GET STARTED

Get Started with JFrog Releases

ARTIFACTORY

Artifactory Release Notes

Artifactory SaaS Releases

Artifactory Self-Managed Releases

About Artifactory Releases

Artifactory Known Issues

Artifactory End of Life

Artifactory Fixed Security Vulnerabilities

Artifactory Deprecations

SECURITY

JFrog Security SaaS

ARTIFACTORY

Artifactory Self-Managed Releases

This section contains the Release Notes for Artifactory Self-Managed releases.

To view a self-managed release's release notes, select the version from the table of contents.

> **Note**
> Release notes for previous releases that have passed their end-of-life date (18 months after the initial release) can be found in Artifactory End of Life.

Important Self-Managed Changes

This section contains crucial notices for:

- Customers using AWS SDK storage.
- Self-Managed users using SAML SSO and basic authentication.

Before upgrading, make sure to review the changes and take the necessary actions.

From version 7.146.7

- **AWS SDK v2 is the Default AWS SDK Storage**
  JFrog Artifactory has officially transitioned its default AWS SDK from v1 to v2 as of Artifactory 7.146.7. If you are setting up new S3 storage integrations or relying on the default configuration, Artifactory will now natively use SDK v2 from version 7.146.7.

> **SDK Storage with KMS Client-Side Encryption**
> Customers using AWS SDK storage with KMS client-side encryption should not use AWS SDK v2. If you are using AWS SDK storage with KMS client-side encryption, ensure that in the `binarystore.xml` file `awsSdkV2` is set it to `false`. For more information, see Amazon S3 Template Parameters.

From version 7.104.5

- **Multiple SAML SSO Provider Configurations**
  The JFrog Platform now supports multiple configurations for SAML SSO providers. Enabling multiple SAML SSO configurations can help large organizations streamline the login and authentication processes for multiple platforms, resulting in a faster and more convenient authentication experience.

> **Note**
> Before creating multiple SAML configurations, JFrog recommends deleting the old configuration and reconfiguring it with a different setting name other than **Default**. If you reconfigure your SAML configuration, you must also update the relevant information in the Identity Provider server.

- **Enabling SSO Disables Basic Authentication By Default**
  Enabling single sign-on authentication now disables internal password authentication by default. For more information, see Disable Basic Authentication Method.

From version 7.98.7

> **Breaking Change for SAML SSO**
>
> As notified in SAML SSO configuration, if you have configured SAML authentication in your environment, make sure to configure a Custom Base URL to prevent a 500 error.

- **Migration of SAML Authentication Provider from Artifactory Service to Access Service**
  As part of enhancements to the JFrog Access Service, which is becoming the primary service for authentication providers, the functionality for the SAML authentication provider has moved to the Access Service.

> **Breaking Change for synchronizeLdapGroups User Plugin**
>
> Following the migration of SAML SSO from Artifactory service to Access service, the deprecated user plugin `synchronizeLdapGroups` will no longer be used for SAML SSO user login. As an alternative, the functionality of the plugin has been implemented as part of the provider. For more information, see Enabling Synchronization of LDAP Groups for SAML SSO.

Artifactory 7.161

This section includes all the Artifactory 7.161 releases.

Artifactory 7.161.26 Self-Managed

Released: 8 September 2026

Resolved Issues

Jira Issue	Component	Severity	Description
INST-24882	General	Medium	Fixed an issue whereby setting `shared.user` and `shared.group` in `system.yaml` applied file ownership as `user:user` instead of `user:group`, which could cause an ownership mismatch.
RTDEV-95512	Packages	High	Fixed an issue whereby NuGet v2 feed responses omitted required package metadata, causing PowerShell package management tools to fail during dependency resolution.
RTDEV-96526	Packages	Medium	Fixed an issue whereby Artifactory returned unnecessary and obsolete npm configuration fields when querying the `/artifactory/api/npm/auth` endpoint or generating `.npmrc` authentication snippets.
RTDEV-97497	Repositories	High	Fixed an issue whereby non-admin users who logged in with Remember Me could not deploy artifacts from the Artifacts UI.

Artifactory 7.161.24 Self-Managed

Released: 5 Sept 2026

This version includes security-driven configuration changes for plugin deployment.

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-97714	Repositories	High	Fixed an issue whereby remote repository downloads could experience a performance degradation in environments where external upstream hostnames are not resolvable locally
RTDEV-97689	General	High	Fixed an issue whereby NuGet package downloads generated misleading WARN log messages referencing Curation On-Demand rejection even when Curation On-Demand was disabled and the package was successfully downloaded.

Artifactory 7.161.20 Self-Managed

Released: 28 Aug 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-82329	General	Critical	Potential authentication bypass leading to administrative access in Artifactory

Artifactory 7.161.19 Self-Managed

Released: 25 August 2026

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-70551	Packages	High	Server-Side Request Forgery Via VCS remote download in JFrog Artifactory.

CVE	Component	Severity	Fix Description
CVE-2026-70550	Packages	Medium	An authorization weakness in JFrog Artifactory Composer repository handling may allow an authenticated user, under specific conditions, to read package metadata from repositories they are not authorized to read.
CVE-2026-70548	Packages	Low	Under specific circumstances, low-level user can run requests to remote CocoaPods repos via JFrog Artifactory External Dependency
CVE-2026-69104	Packages	High	An authenticated user may initiate repository migration operations without required repository permissions, potentially causing partial information disclosure, unauthorized state changes, and service disruption.

Resolved Issues

ID	Component	Severity	Description
RTDEV-93752	Packages	Critical	Fixed an issue whereby NuGet package search in Oracle database environments had slow response times for case-insensitive property lookups.
RTDEV-95374	Repositories	Medium	Fixed an issue whereby when trying to view a repository to which the user doesn't have read permissions, users would get an incomplete or empty directory listing instead of a permissions error.
RTDEV-91181	Federated Repositories	Medium	Fixed an issue whereby when a local repository was created with push replication configured in the same UI action, the replication did not run automatically. This occurred when event-based replication was enabled.
JA-22841	Authentication Providers	Low	Fixed an LDAP issue whereby when editing the settings, the JFrog Platform required entering both the **searchFilter** field and the **userDnPattern** field, not as expected.

Artifactory 7.161.17 Self-Managed

Released: 21 August 2026

Resolved Issues

Jira Issue	Component	Severity	Description
META-3716	Packages	High	Fixed an issue in the metadata service where the update packages endpoint returns a 500 error due to the incorrect use of the limit function for Oracle DB and MSSQL DB.

Artifactory 7.161.16 Self-Managed

Released: 12 August 2026

Feature Enhancements

- **Improved Throughput and Scalability for GCP**
  Artifactory now automatically generates a significantly larger number of temporary upload prefixes on GCS buckets to improve upload throughput and scalability for GCP customers.
- **Improved Azure Blob Storage Access Reliability**
  Artifactory has improved Azure Blob Storage access reliability by introducing a configurable SAS start-time offset (`sasStartTimeOffsetSeconds` , default: `900` seconds) in `binarystore.xml` . This offset prevents intermittent 403 authorization errors caused by clock skew between Artifactory and Azure Blob Storage hosts. For more information, see Azure Blob Storage v2 Binary Provider.
- **Security Hardening for Docker and OCI Referrers API**
  Due to a change that hardened the OCI Referrers API (`GET /v2/ <name>/referrers/<reference>`), the API now returns `403 Forbidden` if the authenticated user does not have read permission on the subject image.
  Users or automations that previously relied on retrieving referrers without read permission on the subject will now receive `403 Forbidden` . Grant read permissions on the relevant repository path to restore access. This change affects local, virtual, remote, and smart remote repositories. For virtual repositories, referrers are aggregated only from member repositories that the user is permitted to read. Related to CVE-2026-66380.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-66376	Authentication Providers	Medium	Deleted users may temporarily retain access to JFrog Artifactory.
CVE-2026-66381	Packages	Medium	Repository readers may access content outside configured upstream paths.
CVE-2026-68753	Packages	Medium	Anonymous users may access restricted Artifactory content under specific configurations.
CVE-2026-68754	Packages	Medium	Publishers without delete permission can overwrite docker layer information.
CVE-2026-66380	Packages	Medium	Authenticated users may access private OCI referrer metadata.
CVE-2026-68755	Release Lifecycle Management	Medium	Bundle writers may alter trusted release information in JFrog Artifactory.
CVE-2026-66377	Packages	Medium	Anonymous users may access restricted Artifactory repository information.
CVE-2026-66379	Packages	Medium	Authenticated users may view private Puppet module metadata.
CVE-2026-66378	Packages	Medium	Authenticated users may access private NuGet metadata.

CVE	Component	Severity	Fix Description
CVE-2026-66382	Packages	Medium	Authenticated users may write files outside the intended Artifactory work directory.
CVE-2026-68756	Database	Medium	Potential insecure deserialization in JFrog Artifactory.
CVE-2026-68760	Authentication Providers	Medium	Potential remember-me authentication bypass in JFrog Artifactory.
CVE-2026-68757	Authentication Providers	High	Potential improper SAML signature verification in JFrog Artifactory.
CVE-2026-66375	General	High	Low-privilege users may remove protected Artifactory metadata.
CVE-2026-68758	General	Medium	Authenticated users may access restricted Artifactory support information.
CVE-2026-66384	Packages	Medium	Authenticated users may write data outside the intended Docker cache path.
CVE-2026-65926	Release Lifecycle Management	Low	Private Release Bundle versions may be disclosed under specific configurations.
CVE-2026-68759	Platform management	High	Integration credential holders may impersonate users in JFrog Access.
CVE-2026-66016	Installation	Medium	Rendered Artifactory Helm manifests may contain generated TLS private keys.
CVE-2026-69105	Packages	High	Potential package cache integrity issue in JFrog Artifactory.
CVE-2026-70547	Packages	Medium	Potential unauthorized metadata exposure in JFrog Artifactory.

Resolved Issues

Jira Issue	Component	Severity	Description
PFED-4928	User Interface (UI)	Medium	Fixed an issue related to Curation Federation whereby, under certain circumstances, when trying to perform any action from the Curation Policies UI, the JFrog Platform returned a 403 Forbidden error.
RTDEV-94633	Repositories	High	Fixed an issue whereby federated repository resource operations returned a 403 error for authorized project admins.

Jira Issue	Component	Severity	Description
RTDEV-90957	Repositories	Medium	Fixed an issue whereby when a Debian virtual repository had priority resolution enabled for one of its members, the merged `Packages` index file was corrupted with literal `\n\n` strings between package entries instead of proper blank-line separators.

Artifactory 7.161.15 Self-Managed

Released: 27 July 2026

Security Notice

This version is designed to fix multiple security vulnerabilities that, when chained together, could result in a critical attack scenario if Anonymous Access is enabled. Anonymous Access is disabled by default and is not recommended for production environments due to the additional security risks it introduces.

Breaking Change for Remote Terraform Repositories

Due to a breaking change whereby Artifactory hardened controls on external Terraform URLs, remote Terraform repositories may return `External URL is not allowed` errors. If this error appears for a credible URL, an administrator must enable external dependency rewrite for the URL in the remote repository settings. For more information, see Remote Terraform Repository.

Embedded OpenJDK Updated to Java 25

Starting with Artifactory version 7.161.15, the embedded OpenJDK has been updated to Java 25 (JDK 25.0.3). Please refer to the Embedded OpenJDK Version page for the complete compatibility matrix.

New Features

- **masterKey and joinKey are now mandatory (Helm Charts only)**
  Both `masterKey` and `joinKey` are now mandatory at install time.
  - **On fresh install:** both keys must be provided before running `helm install`.
  - **On upgrade:** reuse the existing keys from the previous deployment. Do not generate new keys.

  For more information, see Install JFrog Artifactory using Helm.
  To generate, retrieve, and configure the keys, see Manage Keys.
- **Bundled Nginx certificate auto-generation disabled by default**
  Starting with version 7.161, automatic certificate generation for the Nginx bundled with the Artifactory Helm chart is disabled by default. Auto-generated certificates are meant strictly for non-production environments and pose security risks if used in production.
  - **Providing Certificates:** You must supply custom TLS certificates as a pre-created Kubernetes secret managed by the user prior to deployment when HTTPS is enabled.
  - **Upgrades:** Upgrades using existing auto-generated certificates will continue to work, but we strongly recommend migrating to user-managed custom secrets.
  - **Non-Production Environments:** To enable auto-generated certificates for non-production setups, you must explicitly set the `generateSelfSignedCert: true`.
    For more information, see Terminate TLS with Custom Certificate.
- **New services: JFBUS and JFMELT**
  Two new services have been added to Self-Managed Artifactory instances:

- **JFBus** is a service that provides an internal event bus (message queue) for asynchronous communication between JFrog services in the JPD.
- **JFMelt** is a service that collects, processes, and routes audit and operational events generated by JFrog products in the JPD.

These services run as part of the standard platform stack, connect directly to the Artifactory database, and are required for advanced JFrog capabilities to function.
For more information, see Artifactory Product.

- **New operating system support: Debian 13, RHEL 10, SUSE 15.7**
  Artifactory and Distribution now support the following newly validated operating systems for self-managed installations:
  - Debian 13
  - RHEL 10
  - SUSE Linux Enterprise Server 15.7

  See the Supported Platforms and OS Matrix for the full list of supported operating systems and versions.
- **Service pod architecture: Frontend, JFBus, and JFmelt as standalone Deployments**
  Frontend, JFBus, and JFmelt now run as standalone Kubernetes Deployments and are enabled by default:
  - **Frontend** moves out of the Artifactory StatefulSet pod, where it previously ran as a container, and now runs in its own Deployment.
  - **JFBus and JFmelt** have always run as standalone Deployments since their introduction, but are now enabled by default instead of opt-in.

  JFmelt is an event collection and dispatch pipeline for the JFrog Platform (Pro and above; requires JFBus and JFConnect).
- `splitServicesToContainers: false` **no longer supported in Artifactory Helm Charts**
  In Artifactory Helm Charts, `splitServicesToContainers` defaults to `true.`
  Starting with Artifactory 7.161.x, setting `splitServicesToContainers: false` is no longer supported. Helm deployment or upgrade validation will fail if this parameter is explicitly set to `false`.
  For more information, see JFrog Platform Deprecations.
- **Support for Agent Packages Repositories**
  Artifactory now supports using the Agent Package Manager (APM) client to publish and install agent primitives in Agent Packages repositories in Artifactory. Agent Packages Repositories provide a governed, private registry for agent configuration, including skills, plugins, prompts, hooks, Model Context Protocol (MCP) servers, instructions, and agents.
  You can use Agent Packages repositories to distribute resources for harnesses like Claude, Cursor, Codex, and more. For more information, see Agent Packages Repositories.
- **Markdown View in Artifacts Page**
  A view option was added for Markdown (.md) files on the Artifacts page.
- **Support for Agent Plugins Repositories**
  Artifactory now supports Agent Plugins Repositories for secure storage and distribution of agent plugins across harnesses. Agent Plugins repositories in Artifactory provide the following capabilities:
  - **Secure plugin ZIP storage**: Use local Agent Plugins repositories in Artifactory to securely store plugin ZIP files, index metadata, and serve marketplace files for Claude, Cursor, and Codex.
  - **Multi-harness plugins**: Package a single plugin for one agent only, or for multiple agents in one plugin ZIP file using the JFrog CLI.
  - **Native Claude marketplace integration**: Register Artifactory as a plugin marketplace in Claude Code through claude-marketplace.json to download plugins natively.
  - **Broad client support with JFrog CLI**: Use the JFrog CLI to deploy multi-harness plugin directories and install plugins for supported harnesses.

  For more information, see Agent Plugins Repositories.
- **Migration Tool for NuGet repository normalization**
  The Migration Tool is now available in Artifactory Settings to migrate existing repositories to new normalization standards. As of this release, you can use the Migration Tool to migrate NuGet local, remote, and smart remote repositories. Each migration runs a dry run first and produces a report of compliant and non-compliant packages. You can optionally fix non-compliant packages before migration, and specify where to move

remaining non-compliant packages. After migration, all packages left in the repository will be compliant with new artifact and package naming conventions, and `PackageBaseAddress` will be enabled.
For more information, see Migration Tool.

- New REST API for Deleting Multiple Repositories
  A new REST API has been added for deleting multiple repositories. You can indicate which repositories to delete in the body of the request. If a specified repository cannot be deleted, this does not affect the deletion of other repositories specified in the body of the request. For more information, see Delete Multiple Repositories.
  Also, the legacy Delete Repository REST API, which deletes a single repository, has been fixed and now returns JSON instead of plain text in all cases (previously returned JSON only in case of an error). For more information, see Delete Repository.

- New Get Cluster Locks REST API
  Artifactory now provides a REST API that allows you to view locks. Use this REST API instead of the legacy distributed_locks table to troubleshoot stuck replication, indexing, or other operations:

  - `GET /artifactory/api/system/locks`: Returns locks across the cluster
  - `GET /artifactory/api/system/locks/local`: Returns locks held by the current node

  The REST APIs require PostgreSQL database, native DB locks enabled, and admin privileges. For more information, see Get Cluster Locks and Get Node Locks.

- Support for LuaRocks Repositories
  Artifactory now supports LuaRocks repositories, enabling you to manage your Lua dependencies across local, remote, and virtual repositories. This enhancement allows you to securely centralize, discover, and resolve all your LuaRocks packages from a single, controlled platform. For more information, see LuaRocks Repositories.

- Load Healer (Automatic Load Protection)
  This release introduces Load Healer automatic load protection, which protects Artifactory from overload caused by a single activity monopolizing the available worker threads. For more information, see Load Healer (Automatic Load Protection).

Feature Enhancements

Projects

- All Projects and Set Me Up Views Show Only Relevant Virtual Repositories
  The All Projects and Set Me Up views now show only the virtual repositories in projects that you belong to and also global (unassigned) virtual repositories. Virtual repositories from unrelated projects no longer appear in these views. Previously, All Projects and Set Me Up views listed every virtual repository reachable through underlying local and remote repositories, including repositories from projects unrelated to your work. This made the lists long and hard to navigate as the number of projects grew. This change does not affect permissions or your actual access to any repository.

Builds

- Build Search Optimization
  The build search operation has been optimized to provide you with faster results in API calls and the platform UI.

Packages

- Support for Sharded Conda Metadata
  Self-managed instances of Artifactory can now serve sharded repodata for Conda local, remote, and virtual repositories. This increases performance for large packages. To use sharded metadata, configure the Artifactory system property `artifactory.conda.shards.enabled=true` and configure the Conda client with `repodata_use_shards: true` and `solver: libmamba`. For more information, see Enable Conda Metadata Sharding.

- Cache Revalidation for Debian Component Files in Remote Repositories
  Debian remote repositories now support automatic cache revalidation for `Components-{arch}.yml` files in the `dep11` directory. This enhancement ensures that these specific component files stay synchronized with upstream repositories, preventing stale data and hash mismatch errors for clients.

- Syncing Docker Tag Download Statistics for Shared Digests
  Artifactory can now align Docker and OCI tag download statistics when multiple tags point to the same image digest. Administrators can enable Synchronize download statistics for shared digests in Package Settings. When enabled, pulling by tag or digest updates `Number of downloads`, `Last download date`, and `Last downloaded by` for every tag that shares that digest in the same repository and image name. This applies only to tags that you have permissions to read. This enhancement gives a clearer picture of tag usage without

changing how you pull images. For more information, see Enable Synchronized Download Statistics for Shared Digests.

- **Support Added for NuGet v3 repository-signatures in Remote NuGet Repositories**
  Artifactory now supports `repository-signatures` for remote NuGet v3 repositories when the upstream registry also supports `repository-signatures`. This is applicable only to remote NuGet v3 repositories.
- **Support Added for Git Submodules for CocoaPods Packages**
  Artifactory now supports Git submodules for CocoaPods packages fetched from remote repositories. This is also supported for virtual repositories when the pod is resolved through a remote child repository.
- **Improved PyPI Simple JSON Processing Time**
  The response times for `api/pypi/simple` were reduced on PyPI remote repositories by caching the translated package and repository indexes.
- **Enhanced Metadata Support for PyPI Simple JSON API**
  Support has been added for several metadata fields in the PyPI Simple JSON API:
  - `description_content_type`
  - `dynamic`
  - `license_expression`
  - `license_files`
  - `maintainer`
  - `maintainer_email`
  - `project_urls`
  - `provides_extra`
  - `requires_dist`
- **Enhanced Package Details for Skills**
  When viewing package details for items in Skills repositories, the `SKILL.md` file contents now appear in the Packages view.
- **NuGet Remote Metadata Caching Enhancements for Chocolatey**

  Virtual NuGet repositories that connect to Chocolatey now have an enhanced remote caching layer. This cache stores both successful package metadata and "not found" responses (404), enhancing performance and stability during high-volume lookups.
- **Minimum Metadata Retrieval Cache Period Set for NuGet Remote Repositories Pointing to chocolatey.org**
  A four hour minimum has been set as the minimum metadata retrieval cache period for NuGet remote repositories that point to chocolatey.org.
- **Scoped Token Authentication for AI Editor Extensions Repositories**
  Artifactory Set Me Up now generates a scoped reference token for connecting your IDE to an AI Editor Extensions remote repository. You can copy a `serviceUrl` snippet from Set Me Up with the token embedded for manual configuration.
- **Cargo Registries: Unauthenticated `config.json` Returns 401 Error When Anonymous Access is Off**
  For Cargo repositories with Anonymous Access disabled, Artifactory now returns HTTP 401 for unauthenticated requests to the registry `config.json`, so the Cargo client can follow the RFC 3139 flow and retry with credentials instead of receiving a 200 without logging in. Repositories that allow Anonymous Access are unchanged and still serve `config.json` without authentication.
- **End of Support for Cargo Git Indexing**
  As previously announced in JFrog's Deprecations in Process, Cargo Git Indexing is no longer supported. Artifactory now uses the Sparse Index Protocol for Cargo repositories.
- **Improved npm Indexing Performance**
  Indexing for npm has been enhanced, after identifying and improving inefficient per-artifact property retrieval during metadata generation.
- **Added Negative Caching for PyPI Local Repositories**
  A negative cache has been added for PyPI simple-index lookups on local repositories. Repeated requests for non-existent package indexes now skip the database query, significantly reducing database load under high miss traffic.

- **PyPI Curation Performance Improvements**
  PyPI Curation Service performance has been improved by implementing an internal caching mechanism for package index responses. This significantly reduces latency and improves build speeds for curated PyPI repositories.

- **Support for Cryptographic Signing for Nix Repositories**
  Nix repositories in Artifactory now support cryptographic signing with Ed25519 keys. When you add a signing key to your Nix repository, packages in your private binary cache are signed so Nix clients can verify they came from Artifactory and weren't tampered with. For more information, see Configure Cryptographic Signing for Nix Binary Caches.

- **Xet Support for Local and Virtual Repositories**
  Xet support in Hugging Face repositories has been expanded to include local and virtual repositories. The Enable xet protocol option in Packages Settings now enables Xet for all local, virtual, and remote Hugging Face repositories in the organization.
  For more information, see Enable Xet Protocol for Hugging Face Repositories.

  > **Note**
  > If you enabled Xet for remote repositories prior to this update, Xet is automatically enabled for all local and virtual repositories that use the new Machine Learning layout.

- **Ubuntu `amd64v3` Architecture Support Added for Debian Repositories**
  Added support for Ubuntu `amd64v3` architecture variant during the calculation of the coordinates flow for Debian remote repositories, ensuring accurate indexing and caching.

- **Xet Protocol Alignment for Hugging Face Remote Repositories**
  Remote Hugging Face repositories have been updated to align with Hugging Face Xet protocol changes for xorb chunk retrieval. When servicing Xet download requests, Artifactory now searches the repository for existing xorb data before fetching from the upstream registry, reducing redundant upstream traffic and improving download efficiency when the same xorb is referenced across multiple model revisions.
  For more information, see Enable Xet Protocol for Hugging Face Repositories.

- **Support for Tuist Swift Remote Repositories**
  Artifactory now supports Swift remote repositories that connect directly to the Tuist public registry. This enhancement allows you to proxy and cache Tuist registry packages alongside your existing Swift dependencies, improving build reliability and speeding up dependency resolution. For more information, see Swift Repositories.

Access

- **Increased Access Control for Anonymous Users**
  The JFrog Platform now allows selecting specific granular actions that non-admin users with manage permissions can assign to anonymous users in permission targets in the UI, to enhance security and prevent unauthorized privilege escalation. For more information, see Allow Anonymous Access.

- **Enhanced Visibility Controls for OIDC Identity Mappings**
  To strengthen security and improve organizational compliance, you can now restrict project admins from viewing global OIDC identity mappings. Project Administrators will now only view the identity mappings that are directly applicable to their specific, assigned projects. For more information, see OIDC Settings.

- **Nested JSON Claims Support in OIDC Integrations**
  The JFrog Platform now supports mapping nested JSON claims directly within your OIDC identity mappings. This enhancement simplifies your authentication configuration by allowing you to map multiple levels of nesting (for example, `custom_claims.department.group`) without needing to flatten the claims manually. For more information, see Nested JSON Claims.

Release Lifecycle Management

- **Enhanced Evidence Table**
  The evidence table for Release Bundle v2 versions now includes evidence associated with the artifacts contained by the Release Bundle, in addition to the evidence associated with the Release Bundle itself. For more information, see View the Release Bundle Version Evidence Table.

- **Support for Evidence in Remote Repositories**
  You can now attach evidence to artifacts in remote repositories. For more information about evidence, see Evidence Management.

- **Conflict Resolution during Release Bundle v2 Creation**
  A new query parameter, `conflict_resolution`, has been added to the REST APIs for creating and updating Release Bundle v2 versions. Use this query parameter to resolve collisions between source artifacts with the same checksum. Two options are available:
  - `automatic` (default): Resolves collisions using the most recent artifact (taking its properties and evidence).
  - `manual`: Generates an error when a collision is detected. If `fail_fast=true` (default), the error occurs immediately. If `fail_fast=false`, the error is generated only after all collisions are detected. This was the general system behavior before `conflict_resolution` was introduced.

Retention

- **Flexible Retention Policies with Combined Conditions**
  You can now apply Time, Property, and Version criteria within a single policy, enabling precise management of your storage lifecycle. This means you can target outdated packages while ensuring the latest versions are always retained, minimizing data loss risk. For more information, see Cleanup Policies and Smart Archiving.
- **Retention Policy Support for Agent Plugins**
  Cleanup and Smart Archiving policies now support Agent Plugins packages.
- **Release Bundle v2 Cleanup Policies for Enterprise X and Enterprise+ Users**
  Enterprise X and Enterprise+ users can now run cleanup policies that remove eligible Release Bundle v2 versions.
- **Cleanup Policies Performance Improvements for Conan Repositories**
  Cleanup policy performance has been improved to handle duplicate Conan packages without stopping the cleanup run. Duplicate Conan packages are now handled properly so cleanup runs can complete successfully. This enhancement improves reliability for cleanup policies that run on Conan repositories.
- **Detailed Messages for Skipped Packages in Smart Archive Run Reports**
  Archive run reports now provide descriptive messages that explain why a particular package was skipped, as described below. The following messages have been added:

Scenario	Report Message
Package modified since last archive (checksum mismatch, artifact count change, and so on)	Package at source modified since last archive
Package was previously restored from cold storage	Package was restored at 2026-04-28 10:30:00 +0000

  These new messages enable operators who review archive run reports to understand immediately why a package was skipped without digging through Artifactory logs. In addition, the message for restored packages includes the exact UTC timestamp of the restore, making it easier to correlate them with restore operations.
- **Define Stages in Retention Policies**
  You can now limit the scope of Retention policies (Cleanup policies for packages and Smart Archiving policies) to specific lifecycle stages. For example, you can define a Cleanup policy that removes all Docker images more than 2 weeks old from the DEV stage only. Docker images at other stages, such as QA, would be left undisturbed. This new capability makes it possible to tailor your Retention policies to the requirements of each phase of your software development lifecycle.
- **Define Path Patterns in Retention Policies**
  You can now refine the scope of package cleanup policies and Smart Archive policies by optionally defining one or more path patterns (as an addition to the mandatory repository patterns). The use of a wildcard at the beginning or end of each path pattern is supported.

Storage

- **Option to Disable the CRT AWS SDK v2 Client**
  An option has been added to disable the CRT AWS SDK v2 client and use the AWS S3 Async Netty client by setting `<s3UploadStrategy>ASYNC</s3UploadStrategy>` in **binarystore.xml**. For more information, see Amazon S3 Template Parameters.
- **AWS SDK v2 Supports Single-Request Copy**
  AWS SDK v2 now supports a single-request copy inside a bucket by setting the flag `<useSyncClientForCopy>TRUE</useSyncClientForCopy>`. For more information, see Amazon S3

Template Parameters.

General

- **Option Added to UI to Change Block Download Behavior When Curation is Unavailable**
  You can now configure Block Download behavior to allow downloading artifacts from remote repositories even when Curation is unavailable.
- **Xray Configuration Synchronization for Federated Repositories**
  When adding a new member to an existing Federated repository, Artifactory now synchronizes Xray configuration from the source repository to the new member, including **Enable Indexing in Xray**. Changes to Xray settings on existing members are not synchronized. For more information, see Xray Configuration Synchronization.
- **User Context in Webhook Event Payloads**
  Webhook event payloads for artifact-related events now include a `user_context` field that identifies the user or access token that triggered the event. For more information, see Webhook Event Types.
- **CPU Overhead Performance Improvement**
  CPU overhead was reduced for large AQL search queries. Complexity was reduced from $O(N^2 \times M)$ to $O(N \times M)$.
- **High CPU Spikes Eliminated**
  A per-request regex recompilation that caused CPU spikes during request bursts was eliminated.
- **Improved Temporary Memory Allocation**
  Optimizations were made in temporary memory allocation in the download flow.
- **New Worker events: Artifactory Repositories**
  JFrog Workers now supports setting Artifactory repository events to trigger workers, allowing automation of repository management, such as enforcing naming convention. For more information, see Worker Event Types.
- **OneModel GraphQL engine**
  The OneModel Apollo Router engine was replaced by Cosmo Router, providing improved performance and OS compatibility.
- **Artifactory Access APIs Deprecation**
  Artifactory User, Groups, Token, and Permissions management REST APIs are being deprecated and replaced with Access REST APIs, which might require changes to your automations. The deprecation date will be announced in JFrog release notes. For more information, see Deprecated JFrog APIs.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-65617	Packages	High	Designed to prevent unsafe Gems package deserialization that could lead to remote code execution
CVE-2026-65925	Packages	Medium	Designed to validate Cargo sparse index URLs to prevent server-side request forgery
CVE-2026-65921	Builds	High	Designed to prevent build artifact archive paths writing outside intended locations
CVE-2026-65922	General	High	Designed to block unauthorized writes to restricted internal metadata storage locations
CVE-2026-65923	Builds	Medium	Designed to validate Ansible provider URLs to prevent server-side request forgery
CVE-2026-66018	General	Medium	Designed to restrict build environment property access to authorized repository scopes

CVE	Component	Severity	Fix Description
CVE-2026-66014	General	High	Designed to prevent HA authentication fail-open behavior causing privilege escalation
CVE-2026-66015	General	High	Designed to prevent username-based scope injection causing administrative privilege escalation
CVE-2026-65924	Packages	Medium	Designed to validate Terraform external provider URLs to prevent server-side request forgery

Resolved Issues

Jira Issue	Component	Severity	Description
JA-21498	Projects	High	Fixed an issue related to Projects whereby, when deleting a project and attempting to create another project with the same key, the JFrog Platform returned an error.
RTDEV-93599	Packages	Critical	Fixed a high-severity vulnerability in which insufficient validation of user-controlled serialized data could allow a privileged user to trigger unsafe deserialization, potentially leading to remote code execution.
JA-21307	User Interface (UI)	Medium	Fixed an issue related to the Access Tokens page in the JFrog Platform UI whereby, under certain circumstances, when sorting access tokens by project key, the JFrog Platform returned a 400 error.
RTDEV-85657	Packages	Medium	Fixed an issue whereby the After Download Error (ADE) worker failed to trigger when downloading from a local repository using a Docker client.
RTDEV-88344	General	High	Fixed an issue whereby AQL search queries caused significant memory waste under normal download traffic.
RTDEV-87840	Evidence	Medium	Fixed an issue whereby invalid Evidence payloads (for example, no signatures for DSSE envelope or unrecognized payload type) returned 500 errors instead of 400.
RTDEV-87836	Release Lifecycle Management	High	Fixed an issue whereby Xray failed to scan draft Release Bundle v2 versions.
RTDEV-85598	Packages	Medium	Fixed an issue whereby when modifying the `deb.distribution` property on an existing Debian package within a federated repository to add a new distribution, this resulted in a 0-byte package file on the target instance.

Jira Issue	Component	Severity	Description
JA-21124	Authentication Providers	Medium	Fixed an issue related to Access whereby IAM Role Binding did not provide support for the IAM role with path-based prefixes.
RTDEV-85269	Release Lifecycle Management	Medium	Fixed an issue whereby the platform UI failed to display the contents of an OCI package version deployed with Docker when navigating from Release Bundle v2 content screen.
JFUI-21094	General	Medium	Fixed an issue whereby the SAML default REST API was being called even though it was not configured.
RTDEV-84090	Repositories	Medium	Fixed an issue whereby Go `.mod` files triggered Xray scan status polling when copying remote cache items to a local repo that has "Block Unscanned Artifacts" enabled, even though `.mod` is not a supported Xray extension.
RTDEV-65069	Repositories	Low	Fixed an issue whereby a generic remote repository failed to properly follow HTTP 303 redirects from upstream servers when the redirected path ended with a trailing `/`.
JA-20998	User Management	High	Fixed an issue related to access whereby, under certain circumstances, when unsharing a resource from certain users or groups, the JFrog Platform returned an error when anyone with permission tried to access the resource.
JA-20892	Authentication Providers	High	Fixed an issue related to LDAP where, when logging in with a directory containing multiple distinct group entries with identical `cn` values, the JFrog Platform blocks the group population and returns a warning.
JA-20120	User Management	Low	Fixed an issue where, when Disable Internal Password Login was enabled globally, administrators could not set or update a local user's password from the Create/Edit User screens, even for users included in the Internal users allowed to use basic authentication exclusion list.
RTDEV-85481	Builds	Medium	Fixed an issue whereby builds with `/` in the name caused UI failures when appended to aggregate builds.
RTDEV-83999	Repositories	High	Fixed an issue whereby users had limited access to repositories in a default project when using group-scoped access tokens for authorization.
RTDEV-77096	General	Medium	Fixed an issue whereby a project admin with Manage Resources permissions could not manage Xray indexed resources using the User Interface.

Jira Issue	Component	Severity	Description
RTDEV-71186	Builds	Medium	Fixed an issue whereby when a single build published multiple artifacts that shared the same hash sum but were located in different paths, the Build Info UI incorrectly deduplicated these artifacts and displayed only one entry.
RTDEV-82645	General	Medium	Fixed an issue whereby project storage quota notification emails were incorrectly sent to an internal hardcoded address instead of to the actual platform administrators.
JA-20644	Authentication Providers	Critical	Fixed an issue related to SAML SSO whereby, in environments where the JFrog Platform custom CNAME was different from the custom base URL, when trying to perform SAML SSO login, the JFrog Platform returned a 401 error.
JA-20364	Projects	Medium	Fixed an issue related to projects whereby, it was possible to assign Platform Admins the Project Admin role via REST API and not via the UI.
JA-19636	Projects	Medium	Fixed an issue related to projects whereby, under certain circumstances, when creating a project stages, the JFrog Platform created the environment with an incorrect prefix.
RTDEV-84071	Builds	Low	Fixed an issue that caused build-info processing to fail when it contained artifacts referring to directories instead of files. After the fix, those artifacts are ignored.
RTDEV-84078	Builds	Low	Fixed an issue whereby a failed build-info search by artifact returned a 500 error. After the fix, a failed search returns a 400 error.
RTDEV-83357	Release Lifecycle Management	High	Fixed an issue whereby duplicate artifact paths in the request body resulted in a 500 error. After the fix, Artifactory will handle the duplication without it resulting in an error.
RTFE-5068	User Interface (UI)	Medium	Fixed an issue whereby the Artifactory UI tree resolved the wrong path for package types with !-encoded path segments or with path segments that contained a period.
RTDEV-83240	Builds	High	Fixed an issue whereby a Build Cleanup Policy failed to delete builds if the build name contained spaces.
RTDEV-82339	Packages	High	Fixed an issue whereby Artifactory could not resolve Go modules with a major version (v2 and later) from a virtual repository with a remote link to GitHub.

Jira Issue	Component	Severity	Description
RTDEV-82119	Packages	Medium	Fixed an issue whereby a smart remote npm Repository failed to resolve GitHub packages.
RTDEV-80563	Release Lifecycle Management	Critical	Fixed an issue whereby concurrent RBv2 promotions of the same artifact to the same target repository caused an HTTP 500 error. After the fix, concurrent promotions that include the same artifact complete successfully without error.
JFUI-20056	Platform Management	High	Fixed an issue related to the JFrog Platform UI whereby users with the platform auditor role were unable to view Xray scan results
RTDEV-82854	Packages	High	Fixed an issue whereby npm version metadata signatures were stripped from the response after the package tarball was cached, causing installation failures during signature verification.
RTDEV-82256	Packages	Medium	Fixed an issue whereby Go submodule zip downloads could be repacked from the wrong directory when the submodule name matched multiple folder paths in the source archive.
RTDEV-80825	General	Medium	Fixed an issue whereby when a user did not have permission to view a folder in a remote repository (for both smart-remote and regular remote), that user was able to view it in the user interface.
RTDEV-80481	General	Medium	Fixed an issue whereby when attempting to perform deployment by checksum for a generic artifact and providing the sha256 in the headers, the user received the message *Client did not publish a checksum value*.
RTDEV-80066	Packages	Medium	Fixed an issue whereby smart remote PyPI repository requests used an unexpected cache path.
RTDEV-82040	Packages	High	Fixed an issue whereby, after zapping the NuGet metadata cache, a race condition occurred when curation was enabled with Scan from Cache (On-Demand). This caused Artifactory to call Xray with an empty `DownloadURL`, resulting in 400 errors and blocked downloads.
RTDEV-81817	Packages	Medium	Fixed an issue whereby a 401 response was received when using Hugging Face smart remote repositories with the XET protocol enabled.
RTDEV-81767	Packages	Medium	Fixed an issue whereby Go builds failed with a checksum mismatch error when fetching modules from Bitbucket Cloud using tags that contain slashes.

Jira Issue	Component	Severity	Description
JA-20009	Platform Management	Medium	Fixed an issue whereby a specific combination of groups, projects, and lifecycle stages was incorrectly granting delete permissions to non-admin users who should have only had read access to repository artifacts.
RTFS-4094	Federated Repositories	Critical	Fixed a broken authorization service that could permit low-privileged users to read configuration data.
RTDEV-92146	Packages	Critical	Fixed a vulnerability in which weakly validated, request-derived data could be used to poison cached responses.
RTDEV-92966	Packages	High	Fixed an issue whereby a deprecated endpoint caused npm audit queries for smart remote repositories to fail.
RTDEV-90399	General	Critical	Fixed an issue whereby, in certain cases, deprecated services could allow a low-privileged user to retrieve artifacts from repositories they were not authorized to access.
RTDEV-90288	Federated Repositories	Medium	Fixed an issue whereby disabling **Active Replication** on a smart remote repository did not disable **Event-Based Pull Replication**.
RTDEV-90068	Packages	Critical	Fixed an issue whereby Nix remote repositories could not proxy `.nar.zst` NAR files from upstream binary caches, causing 404 errors.
RTDEV-89960	Packages	Medium	Fixed an issue whereby, when using VCS smart remote repositories, the downloadTagFile endpoint failed with a PackageNotFound exception error.
RTDEV-89945	Packages	Medium	Fixed an issue whereby a Docker pull on a Docker smart remote repository did not update the main Artifactory instance download stats.
RTDEV-89767	User Interface (UI)	High	Fixed an issue whereby anonymous UI file downloads via the tree browser could be incorrectly redirected to the native UI instead of downloading the file.
RTDEV-89345	General	Medium	Fixed an issue whereby the repo-layout regex used to resolve module info on every artifact download was being recompiled from scratch on every request instead of being cached.
RTDEV-88337	Storage	Medium	Fixed an issue whereby project storage quota notification emails were being sent too frequently because Artifactory was ignoring the configured notification period property **artifactory.projects.storage.quota.notification.period**.

Jira Issue	Component	Severity	Description
RTDEV-88308	Packages	Medium	Fixed an issue whereby the Maven **Set Me Up** snippet was corrupted when Anonymous Access was enabled.
RTDEV-87580	Repositories	Medium	Fixed an issue whereby, when global **Anonymous Access** was enabled and an anonymous user had explicit read/download permissions, users downloading artifacts via the Web UI or Native Browser layout received the login page HTML source instead of the actual file payload.
RTDEV-87361	Packages	Medium	Fixed an issue whereby an anonymous connection to an upstream repository through a HelmOCI smart remote failed with HTTP 400 when subdomain reverse proxy was enabled.
RTDEV-85594	Packages	Medium	Fixed an issue whereby CocoaPods Smart Remote repositories were missing from the Available Repositories list when configuring a virtual repository.
JA-21766	Authentication Providers	Medium	Fixed an issue related to AWS IAM role mapping whereby, when trying to assign or update an AWS IAM role for a user who already has awsIamRole custom data, the JFrog Platform returned an error.
JA-21745	Projects	Medium	Fixed an issue related to Access whereby, when trying to create new tokens via REST API using Project-scoped Project Admin reference tokens, the JFrog Platform returns a 403 Forbidden error.
JA-21212	User Management	High	Fixed an issue related to custom roles where creating two custom global roles with identical suffixes, differing only by a trailing special character, caused unexpected behavior in the JFrog Platform. Under certain circumstances, when opening the details of the second global role, the details of the first role were displayed instead.
JA-21203	User Interface (UI)	Medium	Fixed an issue related to the GitHub OIDC integration whereby, when selecting a user/group for the first time, in certain circumstances, the JFrog Platform showed an unexpected validation.
RTDEV-92030	General	High	Fixed a privilege-escalation vulnerability that could allow a low-privileged user to obtain elevated permissions.
RTDEV-89766	Builds	Medium	Fixed an issue whereby the Platform UI would fail to display the complete history of promoted builds.

Jira Issue	Component	Severity	Description
RTDEV-88306	Repositories	High	Fixed an issue whereby updating a repository's configuration without specifying an environment reset the repository's assigned stage to the default `DEV` instead of preserving the configured value.
RTDEV-86197	Repositories	Medium	Fixed an issue whereby repository stages could be assigned to build info and release bundle repositories.
JA-20925	Authentication Providers	High	Fixed an issue related to OIDC where GenericOIDC Identity Mappings incorrectly matched OIDC tokens with different claim values when curly-brace-wrapped UUIDs (such as Bitbucket Pipelines) were used.

Artifactory 7.146

This section includes all the Artifactory 7.146 releases.

Artifactory 7.146.39 Self-Managed

Released: 5 Sept 2026

This version includes security-driven configuration changes for plugin deployment.

Artifactory 7.146.38 Self-Managed

Released: 28 Aug 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-82329	General	Critical	Potential authentication bypass leading to administrative access in Artifactory

Artifactory 7.146.36 Self-Managed

Released: 25 August 2026

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-70551	Packages	High	Server-Side Request Forgery Via VCS remote download in JFrog Artifactory.

CVE	Component	Severity	Fix Description
CVE-2026-70550	Packages	Medium	An authorization weakness in JFrog Artifactory Composer repository handling may allow an authenticated user, under specific conditions, to read package metadata from repositories they are not authorized to read.
CVE-2026-70548	Packages	Low	Under specific circumstances, low-level user can run request to remote CocoaPods repos via JFrog Artifactory External Dependency.

Resolved Issues

ID	Component	Severity	Description
JA-20892	Authentication Providers	High	Fixed an LDAP issue where, when logging in with a directory containing multiple distinct group entries with identical cn values, the JFrog Platform blocks the group population and returns a warning.

Artifactory 7.146.35 Self-Managed

Released: 12 August 2026

New Features

- **Package Traffic Controller (PTC)**
  Package Traffic Controller (PTC) is now generally available for Self-Hosted. PTC intercepts public package traffic via your security edge (SASE)—Zscaler ZIA, Netskope, or Cloudflare Gateway—and redirects it through Artifactory Package Reroute, so JFrog Curation and audit apply without changing developer workflows. For more information, see Package Traffic Controller (PTC).
- **Improved Azure Blob Storage Access Reliability**
  Artifactory has improved Azure Blob Storage access reliability by introducing a configurable SAS start-time offset (`sasStartTimeOffsetSeconds` , default: `900` seconds) in `binarystore.xml` . This offset prevents intermittent 403 authorization errors caused by clock skew between Artifactory and Azure Blob Storage hosts. For more information, see Azure Blob Storage v2 Binary Provider.
- **Bundled Nginx certificate auto-generation disabled by default**
  Starting with version 7.161, automatic certificate generation for the Nginx bundled with the Artifactory Helm chart is disabled by default. Auto-generated certificates are meant strictly for non-production environments and pose security risks if used in production.
  - **Providing Certificates:** You must supply custom TLS certificates as a pre-created Kubernetes secret managed by the user prior to deployment when HTTPS is enabled.
  - **Upgrades:** Upgrades using existing auto-generated certificates will continue to work, but we strongly recommend migrating to user-managed custom secrets.
  - **Non-Production Environments:** To enable auto-generated certificates for non-production setups, you must explicitly set the `generateSelfSignedCert: true`.
    For more information, see Terminate TLS with Custom Certificate.
- **Security Hardening for Docker and OCI Referrers API**
  Due to a change that hardened the OCI Referrers API (`GET /v2/ <name>/referrers/<reference>`), the API now returns `403 Forbidden` if the authenticated user does not have read permission on the subject image.
  Users or automations that previously relied on retrieving referrers without read permission on the subject will now receive `403 Forbidden` . Grant read permissions on the relevant repository path to restore access.
  This change affects local, virtual, remote, and smart remote repositories. For virtual repositories, referrers are aggregated only from member repositories that the user is permitted to read. Related to CVE-2026-66380.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-66376	Authentication Providers	Medium	Deleted users may temporarily retain access to JFrog Artifactory.
CVE-2026-68752	Projects	High	Project Resource Managers may escalate privileges in JFrog Artifactory.
CVE-2026-66381	Packages	Medium	Repository readers may access content outside configured upstream paths.
CVE-2026-68753	Packages	Medium	Anonymous users may access restricted Artifactory content under specific configurations.
CVE-2026-68754	Packages	Medium	Publishers without delete permission can overwrite docker layer information.
CVE-2026-66380	Packages	Medium	Authenticated users may access private OCI referrer metadata.
CVE-2026-68755	Release Lifecycle Management	Medium	Bundle writers may alter trusted release information in JFrog Artifactory.
CVE-2026-66377	Packages	Medium	Anonymous users may access restricted Artifactory repository information.
CVE-2026-66379	Packages	Medium	Authenticated users may view private Puppet module metadata.
CVE-2026-66378	Packages	Medium	Authenticated users may access private NuGet metadata.
CVE-2026-66382	Packages	Medium	Authenticated users may write files outside the intended Artifactory work directory.
CVE-2026-68756	Database	Medium	Potential insecure deserialization in JFrog Artifactory.
CVE-2026-68760	Authentication Providers	Medium	Potential remember-me authentication bypass in JFrog Artifactory.
CVE-2026-68757	Authentication Providers	High	Potential improper SAML signature verification in JFrog Artifactory.
CVE-2026-66375	General	High	Low-privilege users may remove protected Artifactory metadata.
CVE-2026-68758	General	Medium	Authenticated users may access restricted Artifactory support information.

CVE	Component	Severity	Fix Description
CVE-2026-66384	Packages	Medium	Authenticated users may write data outside the intended Docker cache path.
CVE-2026-65926	Release Lifecycle Management	Low	Private Release Bundle versions may be disclosed under specific configurations.
CVE-2026-68759	Platform management	High	Integration credential holders may impersonate users in JFrog Access.
CVE-2026-66016	Installation	Medium	Rendered Artifactory Helm manifests may contain generated TLS private keys.

Resolved Issues

Jira Issue	Component	Severity	Description
PFED-4928	User Interface (UI)	Medium	Fixed an issue related to Curation Federation whereby, under certain circumstances, when trying to perform any action from the Curation Policies UI, the JFrog Platform returned a 403 Forbidden error.
RTDEV-94633	Repositories	High	Fixed an issue whereby federated repository resource operations returned a 403 error for authorized project admins.

Artifactory 7.146.34 Self-Managed

Released: 27 July 2026

Security Notice

This version is designed to fix multiple security vulnerabilities that, when chained together, could result in a critical attack scenario if Anonymous Access is enabled. Anonymous Access is disabled by default and is not recommended for production environments due to the additional security risks it introduces.

Breaking Change for Remote Terraform Repositories

Due to a breaking change whereby Artifactory hardened controls on external Terraform URLs, remote Terraform repositories may return `External URL is not allowed` errors. If this error appears for a credible URL, an administrator must enable external dependency rewrite for the URL in the remote repository settings. For more information, see Remote Terraform Repository.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-65617	Packages	High	Designed to prevent unsafe Gems package deserialization that could lead to remote code execution
CVE-2026-65925	Packages	Medium	Designed to validate Cargo sparse index URLs to prevent server-side request forgery
CVE-2026-65921	Builds	High	Designed to prevent build artifact archive paths writing outside intended locations
CVE-2026-65922	General	High	Designed to block unauthorized writes to restricted internal metadata storage locations
CVE-2026-65923	Builds	Medium	Designed to validate Ansible provider URLs to prevent server-side request forgery
CVE-2026-66018	General	Medium	Designed to restrict build environment property access to authorized repository scopes
CVE-2026-66014	General	High	Designed to prevent HA authentication fail-open behavior causing privilege escalation
CVE-2026-66015	General	High	Designed to prevent username-based scope injection causing administrative privilege escalation
CVE-2026-65924	Packages	Medium	Designed to validate Terraform external provider URLs to prevent server-side request forgery

Artifactory 7.146.29 Self-Managed

Released: 21 July 2026

Note for Customers Using AWS S3 Storage

Customers using AWS S3 storage should be aware that, starting from this release, AWS SDK v2 strictly enforces `GetObjectVersion` permission.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-70548	Packages	Low	Under specific circumstances, low-level user can run request to remote CocoaPods repos.

Feature Enhancements

- **KMS Client-Side Encryption Compatible with AWS SDK v2 Storage**
  You can now use KMS client-side encryption with AWS SDK v2 storage (resolved known issue RTDEV-86625). The parameter `kmsCryptoMode` is not used in AWS SDK v2.

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-91969	Storage	Low	Fixed an issue whereby a federated member was not deactivated even if not accessible.
RTDEV-93602	Packages	Critical	Fixed an issue whereby NuGet database queries required optimization to improve speed and performance for environments utilizing Microsoft SQL Server.

Artifactory 7.146.28 Self-Managed

Released: 16 July 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-69106	General	High	Potential cache poisoning in JFrog Artifactory

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-92966	Packages	High	Fixed an issue whereby a deprecated endpoint caused npm audit queries for smart remote repositories to fail.
RTDEV-88306	Repositories	High	Fixed an issue whereby updating a repository's configuration without specifying an environment reset the repository's assigned stage to the default `DEV` instead of preserving the configured value.

Artifactory 7.146.27 Self-Managed

Released: 15 July 2026

Security Notice

This version is designed to fix multiple security vulnerabilities that, when chained together, could result in a critical attack scenario if Anonymous Access is enabled. Anonymous Access is disabled by default and is not recommended for production environments due to the additional security risks it introduces.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-65616	General	High	Designed to strengthen refresh token signature validation to prevent privilege escalation

Resolved Issues

Jira Issue	Component	Severity	Description
RTFS-4094	Federated Repositories	Critical	Fixed a broken authorization service that could permit low-privileged users to read configuration data.
RTDEV-92146	Packages	Critical	Fixed a vulnerability in which weakly validated, request-derived data could be used to poison cached responses.
RTDEV-92030	General	High	Fixed a privilege-escalation vulnerability that could allow a low-privileged user to obtain elevated.
RTDEV-91769	Packages	High	Fixed an issue whereby Go remote repositories integrated with self-hosted GitLab failed to resolve non-tag references due to GraphQL service failures and the incorrect treatment of major version suffixes as GitLab subpaths.

Artifactory 7.146.25 Self-Managed

Released: 8 July 2026

Feature Enhancements

- **Configurable Allow Lists for Import, Export, and Backup Path Validations**
  The path validations for import, export, and backup in Artifactory can now be configured to have allow lists, so that import, export, and backup operations are restricted to only explicitly permitted directories. Each operation has its own allow list, so there are 3 separate allow lists. Although these allow lists are not mandatory, JFrog recommends using them for additional security. The allowlist can be configured either with `artifactory.system.properties` or with `system.yaml` (`system.yaml` takes precedence).
  - Configure with `artifactory.system.properties` as follows:

```
artifactory.import.allowed.paths=/tmp/art-import/,/mnt/imports/
artifactory.export.allowed.paths=/tmp/art-export/
artifactory.backup.allowed.paths=/mnt/backups/
```

  - Configure with `system.yaml` as follows:

```
artifactory:
    security:
        import:
            allowedPaths: /tmp/art-import/,/mnt/imports/
        export:
            allowedPaths: /tmp/art-export/
        backup:
            allowedPaths: /mnt/backups/
```

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-89960	Packages	Medium	Fixed an issue whereby, when using VCS smart remote repositories, the downloadTagFile endpoint failed with a PackageNotFound exception error.
RTDEV-90532	Packages	Medium	Fixed an issue whereby Nim remote repositories return the same file-list page when page-size is missing from request parameters.
RTDEV-88743	Packages	Medium	Fixed an issue whereby a NuGet V2 OData query on a virtual repository incorrectly returns HTTP 403 instead of 404 when the user has read access to only some constituents and the requested package does not exist. An unreadable constituent is now treated as "not found" during virtual resolution, so the response is 404 as expected.
RTDEV-87580	Repositories	Medium	Fixed an issue whereby when global Anonymous Access was enabled and an anonymous user had explicit read/download permissions, users downloading artifacts via the Web UI or Native Browser layout received the login page HTML source instead of the actual file payload.
RTDEV-89767	User Interface (UI)	High	Fix an issue whereby anonymous UI file downloads via the tree browser could be incorrectly redirected to the native UI instead of downloading the file.

Artifactory 7.146.22 Self-Managed

Released: 29 June 2026

Forced Use of AWS SDK v1 with KMS Client-Side Encryption

As of this version, customers using AWS S3 storage with KMS client-side encryption can only use AWS SDK v1. Use of AWS SDK v2 with KMS client-side encryption is not possible and customers will be automatically switched to AWS SDK v1.

Feature Enhancements

- **PyPI JSON Version Processing Enhancement**
  PyPI JSON version processing has been optimized to reduce complexity.
- **Cache Revalidation for Debian Component Files in Remote Repositories**
  Debian remote repositories now support automatic cache revalidation for `Components-{arch}.yml` files in the `dep11` directory. This enhancement ensures that these specific component files stay synchronized with upstream repositories, preventing stale data and hash mismatch errors for clients.

Resolved Issues

Jira	Component	Severity	Description
PFED-2163	Federation	Medium	Fixed an issue whereby the JPD registration endpoint `/pfed/api/v1/jpd` exposed by the Platform Federation (PFED) service did not accept private-network IPs as the JPD URL. This prevented registration of Self-managed JPDs to include them in a Curation Federation or other Platform Federations.
RTDEV-85594	Packages	Medium	Fixed an issue where CocoaPods Smart Remote repositories were missing from the Available Repositories list when configuring a virtual repository.
RTDEV-86877	Packages	Medium	Fixed an issue whereby npm package uploads that violated the path-enforcement rule were allowed, resulting in downstream metadata generation failures.
RTDEV-87274	Packages	High	Fixed an issue whereby enabling the settings **Complete list manifest image overwrite** and **Enforce Strict Tag Overwrite** under **Package Settings > Docker, OCI, HelmOCI** was not applied.
RTDEV-87361	Packages	Medium	Fixed an issue whereby anonymous connection to an upstream repository through a HelmOCI smart remote failed with HTTP 400 when subdomain reverse proxy was enabled.
RTDEV-88396	Packages	Critical	Improvements in NuGet Version SortingOptimizations were made in memory consumption of NuGet version sorting.
RTDEV-90068	Packages	Critical	Fixed an issue whereby Nix remote repositories could not proxy `.nar.zst` NAR files from upstream binary caches, causing 404 errors
RTDEV-90290	Packages	High	Fixed an issue whereby publishing Cargo packages to Artifactory failed because the endpoint did not accept the Content-Type: application/octet-stream header, a breaking change introduced in Cargo client version 1.96.0.
RTDEV-89889	Repositories	Medium	Fixed an issue whereby when editing a repository replication configuration, unrelated replications would get validated and sometimes blocked the editing.
RTDEV-85614	User Interface (UI)	Medium	Fixed an issue whereby when browsing repository contents in the Artifacts view using a Windows OS, a Load More option was displayed to show more of the contents in the repository, but when clicking it the same set of artifacts was displayed instead of loading the next batch of entries.

Artifactory 7.146.17 Self-Managed

Released: 10 June 2026

Important Notice for Customers Using AWS SDK Storage with KMS Client-Side Encryption

Customers using AWS SDK storage with KMS client-side encryption should not use AWS SDK v2. If you are using AWS SDK storage with KMS client-side encryption, ensure that in the `binarystore.xml` file `awsSdkV2` is set it to `false`. For more information, see Amazon S3 Template Parameters.

Improved federation flow (metadata negotiation removed)

The standalone Artifactory Federation Service (RTFS) improves the federation flow by decoupling from metadata negotiation to reduce protocol overhead and simplify the connection handshake. The negotiation code is no longer part of RTFS and federation operates as expected without that step.

Repositories that were marked **DISABLED_BY_SYSTEM** under legacy Federation because of failed metadata negotiation may retain that database state after migration. This is not an RTFS negotiation failure. Full Sync is unlikely to resolve it. Contact JFrog Support for guidance.

For more information, see Disabled-by-System Repositories and Metadata Negotiation in Federated Repositories.

Feature Enhancements

- **Upgrade to Apache Tomcat 11.0.22**
  The Apache Tomcat version bundled with Artifactory has been upgraded to version 11.0.22.
- **Support for Opting Out of New SAML Login Redirect Behavior**
  The JFrog Platform now supports reverting to the previous implementation of SAML login redirect, whereas upon automatic logout, users will be redirected to the SAML login URL. For more information, see SAML SSO.
- **Federation**
  - **Configurable Payload Size for RTFS Communication with Access**
    You can now configure how much data the Artifactory Federation Service (RTFS) can receive from the JFrog Access service. Increasing this limit helps prevent federation failures when Access returns large configuration responses, for example, in environments with many Federated repositories. For more information, see Configure RTFS Properties in system.yaml in Federated Repositories.
  - **Federation Configuration Setting Applies to All RTFS Communication with Access**
    A federation configuration setting that controls how much data RTFS can receive from Access now applies to all RTFS communication paths with Access, not only a single path. For more information, see Configure RTFS Properties in system.yaml in Federated Repositories.

Resolved Issues

Jira Issue	Component	Severity	Description
INST-22203	General	Medium	Fixed an issue with the Artifactory Helm chart whereby, when `multiPartLimit`, `multipartElementSize`, `connectionTimeout`, or `socketTimeout` were not explicitly set under `artifactory.persistence.awsS3V3` in `values.yaml`, the Helm chart rendered them as `0` in the generated `binarystore.xml` instead of omitting the tags entirely, silently overriding Artifactory's built-in defaults with `0`.
RTDEV-85530	Packages	Medium	Fixed an issue whereby the Swift reindex process crashed when a repository contained a `.zip` file that wasn't a valid Swift package (that is, missing a `Package.swift` file), causing the entire reindex to fail instead of simply skipping the non-Swift archive.

Jira Issue	Component	Severity	Description
RTDEV-85592	Packages	Medium	Fixed an issue whereby a downloaded module .zip from a smart remote repository that contained executables could lose Unix file permissions.
RTDEV-86957	Packages	Medium	Fixed an issue where connection pool leaks occurred when Artifactory fetched the `Package.swift` release manifest from Swift remote repositories.
RTDEV-88100	Packages	Medium	Fixed an issue whereby Linux binary CRAN packages installed from source instead of as pre-compiled binaries when proxied through an Artifactory remote CRAN repository pointing to a Posit Linux Binary URL.
RTDEV-84352	Release Lifecycle Management	Medium	Fixed an issue whereby Move promotions appeared as Copy promotions in the platform UI of other Federation members.
RTFS-3508	Federated Repositories	High	Fixed an issue whereby adding a second or subsequent remote federation member to an existing federated repository failed with a 400 error stating the repository cannot be added to the federation because it is a member of another federation.

Artifactory 7.146.15 Self-Managed

Released: 26 May 2026

Feature Enhancements

- **Retry Mechanism for AWS SDK v2 Client HTTP Requests**
  A retry mechanism has been added for AWS SDK v2 client HTTP requests.
- **Reference Attributes Added to Composer's `dist` Metadata for Local Repositories**
  Artifactory now supports reference attributes in Composer's `dist` metadata for local repositories. This is useful for identifying dev composer packages and resolving caching issues with clients.

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-91590	Repositories	Medium	Fixed an issue whereby a full repository configuration was returned by the `GET /artifactory/api/repositories/{repoKey}` endpoint when a group-scoped service token was used for authentication, instead of a trimmed, publicly available repository configuration version.
RTDEV-85528	Packages	Medium	Fixed an issue whereby deploying a Debian package with a blank architecture property broke indexing for the repository.
RTDEV-85520	Packages	Medium	Fixed an issue whereby compound Debian component names (for example, `updates/main`) were not handled correctly when the calculate coordinates API ran

Jira Issue	Component	Severity	Description
			on a Debian security remote cache repository, causing virtual repository index calculation to skip resolvable security packages.
RTDEV-83990	Packages	Medium	Fixed an issue whereby it was not possible to publish a new version of a non-public RubyGem to Artifactory due to the YAML document size.
RTDEV-84660	Repositories	High	Fixed an issue whereby restoring a deleted repository root from the Trash Can incorrectly copied its properties onto the restored root folder and all of its child-folders and items.
RTDEV-85935	Storage	Medium	Fixed an issue whereby idle connections were not being closed in the connection pool of the Remote Binary Provider and Federated Binary Provider HTTP clients.
RTDEV-85592	Packages	Medium	Fixed an issue whereby a downloaded module **.zip** from a smart remote repository that contained executables could lose Unix file permissions.

Artifactory 7.146.13 Self-Managed

Released: 20 May 2026

Feature Enhancements

- **Improved Performance for NuGet Repository Database Queries**
  For customers experiencing lock contentions due to heavy_query_cache, it is recommended to set the property `artifactory.db.lock.native.pool.size = 10`. Contentions are seen only when the workload is significantly high. The default size of the pool is 5.
  The following is a typical example as seen in the logs when there is a database contention:

```
Timed out while trying to acquire lock: hqc:nuget_hqc_ ... Couldn't acquire lock for: 120000 milliseconds and locked by: ...
```

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-85999	Packages	Medium	Fixed an issue whereby the Pub repository indexer did not generate `.pub/` metadata index files for packages whose names begin with an underscore `_`, causing resolution failures packages with an underscore prefix.
RTDEV-85727	Packages	Medium	Fixed an issue whereby when **Complete list manifest image overwrite** was enabled, sha256 manifests and layers from previous builds were not deleted when an OCI image tag was overwritten by pushing a new build with the same tag.

Jira Issue	Component	Severity	Description
RTDEV-85316	Release Lifecycle Management	Medium	Fixed an issue whereby Release Bundle v2 REST API endpoints on Artifactory Edge failed with a `500` error for version names longer than 32 characters, preventing deletion of distributed release bundles.
RTDEV-85174	Repositories	Medium	Fixed an issue whereby a custom HTTP header was getting dropped for remote repositories.
RTDEV-84690	Packages	High	Fixed an issue related to the JAX-B parser that led to blocked threads in the NuGet v2 `findPackagesById` endpoint.

Artifactory 7.146.12 Self-Managed

Released: 14 May 2026

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-83615	Authentication Providers	Medium	Fixed an issue whereby when a user tried to download an artifact through the user interface, the user was redirected to the SAML login page and then was logged out of Artifactory.
RTFE-5072	Packages	Medium	Fixed an issue whereby Set Me Up did not display identity tokens as expected.
RTDEV-84875	Packages	Medium	Fixed an issue whereby Hugging Face pagination was not respected and blocked downloads.
RTDEV-83352	Packages	Medium	Fixed an issue where Go v2+ submodules in monorepos could not be resolved through a Go remote repository with a GitHub provider, returning +incompatible versions instead.
RTDEV-85178	Packages	Medium	Fixed an issue whereby xet files are not served in Hugging Face smart repositories.
RTDEV-83969	Release Lifecycle Management	High	Fixed an issue that blocked federation events when the same Release Bundle v2 version was promoted independently on multiple federated sites. Now, update events for artifacts with the same checksum on the receiving site are skipped, preventing queue blockage.
RTFE-4987	Repositories	Medium	Fixed an issue whereby Helm OCI repositories did not have the Enable Redirect Download checkbox.

Jira Issue	Component	Severity	Description
RTDEV-85479	User Interface (UI)	High	Fixed an issue that prevented evidence for artifacts in Federated repositories from appearing in the platform UI.

Artifactory 7.146.10 Self-Managed

Released: 5 May 2026

Resolved Issues

Jira Issue	Component	Severity	Description
JA-20046	General	Medium	Fixed an issue related to Stages whereby under certain circumstances, a misconfigured race condition caused the JFrog Platform to return `500` errors.
JA-20371	General	Medium	Fixed an issue related to AWS whereby the configured regional STS endpoint was ignored, causing the JFrog Kubelet Credential Provider to fail authentication by reaching the global STS endpoint instead.
JFUI-20343	User Interface (UI)	Medium	Fixed an issue whereby the JCR/OSS frontend did not load in the JFrog Platform UI.
JFUI-20497	User Interface (UI)	High	Fixed an issue whereby users could not review Xray logs in the JFrog Platform UI.
JA-20646	User Management	Critical	Fixed an issue whereby when editing the anonymous user page in the JFrog Platform UI, under certain circumstances anonymous users were removed from groups unexpectedly.
JR-10461	Evidence	Medium	Fixed an issue that caused evidence created without a `provider-Id` to be assigned JFrog as the `provider-Id` after promotion, distribution, or federation. After the fix, evidence created without a defined provider will remain without a `provider-Id` throughout the lifecycle of that evidence.
RTDEV-79028	Retention	Medium	Fixed an issue whereby cleanup policies run on Federated repositories on packages present at the root level (`path = repoKey/package_name`) produced unexpected results.
RTDEV-85479	Evidence	High	Fixed an issue that prevented evidence for artifacts in Federated repositories from appearing in the platform UI.

Artifactory 7.146.8 Self-Managed

Released: 28 April 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-42018	General	High	Anonymous token exposure in JFrog Artifactory
CVE-2026-69107	General	Medium	Potential unauthorized artifact access in JFrog Artifactory

Artifactory 7.146.7 Self-Managed

Released: 16 April 2026

AWS SDK v2 is now the default AWS SDK

Following the update in Artifactory 7.133.3, JFrog Artifactory has officially transitioned its default AWS SDK from v1 to v2 as of this release. If you are setting up new S3 storage integrations or relying on the default configuration, Artifactory will now natively use SDK v2.

Why We Made This Change

Amazon Web Services ended support for SDK v1 at the end of 2025. By making v2 the default, JFrog is ensuring that your Artifactory environments are positioned for long-term stability and are protected against the risks of using deprecated software. AWS SDK v2 has the following advantages:

- **Security & Compliance**: Eliminates the security risks associated with running end-of-life software that no longer receives security patches.
- **Performance & Feature Parity**: Unlocks the ability to leverage the latest AWS optimizations, availability improvements, and new features for a more robust storage solution.

This support for AWS SDK v2 and its configuration is added in Artifactory Helm Charts 107.146.x.

For more information, see Integrate Artifactory with AWS SDK v2 for S3 Storage and Fine-Tuning AWS SDK v2 with Artifactory.

Important: Customers using AWS SDK storage with KMS client-side encryption should not use AWS SDK v2. If you are using AWS SDK storage with KMS client-side encryption, ensure that in in the `binarystore.xml` file `awsSdkV2` is set it to `false`. For more information, see Amazon S3 Template Parameters.

Deprecation of the Security Configuration Descriptor (XML export/import via REST API and UI)

The Security Configuration Descriptor, which allows exporting and importing Artifactory's security configuration as raw XML, will be deprecated as of July 1, 2026. This deprecation includes the REST API endpoints `GET/POST /api/system/security` and the Security Descriptor page in the Administration module (Administration > Artifactory Settings > Security Descriptor). Deprecation has been noted on the relevant documentation pages. Security configuration should be managed through the dedicated REST APIs and the Administration UI.

What you need to do : Migrate any automation that uses `GET/POST /api/system/security` to the dedicated Security REST APIs. If you use the Security Descriptor UI page for manual configuration review, use the standard security administration pages instead (Administration > Security). For bootstrap scenarios, use the Access Configuration Bootstrap YAML.

Member Node Deprecation in Artifactory High Availability (HA) Helm Chart

To streamline High Availability (HA) deployments and finalize the transition to a fully masterless architecture , we have officially removed the "Member Node" configuration from the Artifactory HA Helm chart (v7.146.x and later).

What has changed:

- Previously, while Artifactory HA charts defaulted to 3 replicas (3 Primary, 0 Members), legacy code for "Member Nodes" remained for backward compatibility.
- Starting with version 7.146.7, this legacy code has been completely removed. Artifactory now treats all nodes as equals, simplifying scaling and cluster management.

Action Required: Mandatory Configuration Update

If your current values.yaml contains an `artifactory.node` block, your upgrade will fail with the following validation error:

```
'artifactory.node' is no longer supported. Member nodes have been removed from this chart. Please remove the 'artifactory.node' block from your values and use 'artifactory.primary.replicaCount' to scale instead.
```

Steps to Resolve:

- **Remove the Block**: Delete the entire `artifactory.node` section from your `values.yaml`.
- **Scale via Primary:** To define the number of nodes in your cluster, use the `artifactory.primary.replicaCount` parameter instead.

Frontend Microservice Pod Separation

To enhance system resilience and better align with modern cloud-native standards, Artifactory v7.146.7 introduces the ability to decouple the Frontend microservice into its own dedicated pod.

**What's New: ** `frontend.asPod`

Previously, the Frontend service shared resources and lifecycles within the main Artifactory pod. You can now isolate this service by toggling a new flag in your configuration.

- **Parameter**: `frontend.asPod`
- **Default Value**: `false` (Frontend remains within the Artifactory pod)
- **For Standalone**: Set to `true` (Frontend deploys as a standalone pod)

New Features

- **Support for Nix package type**
  You can now use Nix repositories in Artifactory as a high-performance binary cache to ensure fast, reliable, and reproducible builds. This integration allows you to proxy and cache NixOS Search , while also providing a secure platform to host and publish custom internal channels.
  Artifactory enhances the Nix ecosystem by providing unified access through virtual repositories, and global distribution via federated repositories to synchronize artifacts across locations. Artifactory also provides native metadata calculation to logically group related artifacts, improving discoverability and artifact management without compromising Nix's core content-addressed reproducibility. For more information, see Nix Repositories.
- **Skills local repositories**
  Skills repositories are now available in Artifactory as an open beta. You can use Skills repositories as a private skill registry for AI agent capabilities, allowing you to publish, discover, and install skills from one controlled place. Skills repositories offer full integration with JFrog CLI (`jf skills`) v2.98.0 or newer, and a ClawHub v1–compatible REST API for seamless and secure publish and resolve flows.
  For Artifactory instances with JFrog AI Catalog, you can optionally enable semantic scanning to help catch malicious skills before distribution, adding a supply-chain gate to your AI skill lifecycle. A batch deletion feature deletes blocked skills every 30 minutes.
  For more information, see Skills Repositories.
- **NuGet Enforce Layout**
  This version of Artifactory introduces NuGet Enforce Layout. By enabling NuGet Enforce Layout, you will avoid package duplication and bring Artifactory closer in alignment with the nuget.org registry.
  NuGet Enforce Layout has three main uses:

- It allows access to the PackageBaseAddress service, which speeds up NuGet restore operations.
- It normalizes the names of the packages that you deploy based on SemVer, according to the NuGet Normalized Version Numbers convention, supported in NuGet versions 3.4 and above.
- It prevents the upload of duplicate versions or several package versions that are identical according to the Normalized Version Numbers rules.

For more information, see NuGet Enforce Layout.

> **Note**
>
> NuGet Enforce Layout is available only if your Artifactory version has the NuGet Package Handler activated.

- **API for returning all Release Bundle v2 cleanup policies**
  A new REST API returns a list of all existing Release Bundle v2 cleanup policies for either a specific project or for the entire system. For more information, see Get All Cleanup Bundle Policies API.
- **Add Platform Auditor role in REST API** The JFrog Platform now supports assigning users the Platform Auditor role via the user management REST API endpoints. For more information, see Create User, Update User, and Get User Details.

Feature Enhancements

Projects

- **Added support for project admin permissions** The JFrog Platform now supports more granular control over project admin permissions, allowing you to grant project admins **Manage Resources** permissions, but prevent them from creating or managing remote repositories.

Builds

- **Build content displayed in platform UI**
  The platform UI now contains a Content tab that provides a list of all the packages and standalone artifacts (known collectively as releasables) included in the build. For more information, see View Build Number Information.
- **Improved build module performance in platform UI** To enhance the user experience, the time required to display build modules in the platform UI was significantly decreased. This improvement is most noticeable when loading large builds in the UI.

Authentication

- **Webhook management scoped tokens**
  The JFrog Platform now supports creating scoped tokens, allowing access to manage Webhooks endpoints. For more information, see Create Scoped Token.
- **Added a warning message when deleting a SCIM token**
  The JFrog Platform now displays a warning message when attempting to delete a SCIM token, as deletion might disconnect authentication provider integrations.
- **Support for Setting Maximum Token Expiration Value**
  The JFrog Platform now supports setting a maximum value for token expiration in the UI, enabling self-service management and increased platform security.

User management

- **Support for Webhook Creation role** The JFrog Platform now supports a role that allows users who are not platform administrators to create and manage Webhooks. For more information, see Create and Edit Users.

Database

- **AQL limit applied to the Artifactory server to protect the database server from overload**
  An AQL limit has been applied to the Artifactory Server to protect the Database Server from overload caused by excessive AQL search requests issued by end-users. The AQL limit includes concurrency limits at both global and per-user levels. This ensures that the database server has enough remaining capacity to serve other critical activities, such as upload and download.

Packages

- **Improved Helm metadata processing**
  Helm metadata processing has been improved by eliminating redundant version comparison during repository indexing. This optimization reduces CPU overhead during index.yaml generation and virtual repository rewrites, significantly improving performance and scalability for repositories with a large number of chart versions.

- **Improved Pub error handling and status codes**
  For Pub clients older than version 2.15.0, error handling and status codes have been changed to align with proper authorization behavior. When a user without write permissions tries to download a package from a remote, virtual, or smart remote repository, Artifactory will now return HTTP 403 (Forbidden) instead of 404.

- **Enhanced UI Support for DNF Client in RPM Packages**
  This release adds the DNF client option to RPM Set Me Up instructions. While Artifactory has long supported both YUM and DNF clients, the Set Me Up instructions previously only displayed YUM option. Artifactory is prioritizing the DNF client to align with modern RPM-based distributions where DNF is the default package manager.

- **npm metadata protection**
  To avoid potential metadata corruption, Artifactory now blocks writing to the **.npm** directory during copy or move operations to paths in that directory. This limitation prevents source metadata from overwriting the destination's system-generated files, ensuring your npm packages remain correctly indexed after the move.

- **npm attestation support**
  This version of Artifactory introduces support for native npm provenance and attestations in remote and virtual repositories. When running npm audit signatures, the output now includes signatures and attestations for supported packages. This enhancement allows you to retrieve build-source metadata directly from upstream registries and ensure package authenticity. For more information, see Use npm Audit.

- **Support for JSON indexing with PyPI Simple JSON API**
  Artifactory now supports the PyPI Simple JSON API to provide a modernized alternative to traditional HTML-based package metadata. This opt-in feature enables JSON indexing for PyPI repositories via the Accept header, allowing for faster and more efficient dependency resolution by modern Python package managers. For more information, see Enable JSON Indexing in PyPI Repositories.

- **Updated POM validation log level**
  Log entries for POM deployment path mismatches have been updated from Error to Warning to better reflect that these issues typically are not caused by system failure. This change reduces noise in monitoring tools while still reporting incorrect POM metadata.

- **Improved Maven indexing performance**
  Artifactory performance has been improved by optimizing **database indexes for Postgres DB**. By reducing the database load during file upload and deletion operations, this change ensures better system stability and faster response times for Maven repositories.

- **Improved re-indexing process for Opkg repositories**
  The re-indexing process for Opkg repositories has been improved such that a full re-index is no longer required when adding or deleting packages to or from an Opkg repository. Only the affected package entries are added to or removed from the Opkg index file when adding or deleting a package.

Repositories

- **Support for Red Hat Ansible Automation Hub**
  Ansible remote repositories now support proxying Red Hat Ansible Automation Hub. This enhancement lets you cache and serve certified and validated Ansible content collections from Automation Hub through Artifactory, while applying your own access controls and governance policies. For more information about this capability, see Proxying Red Hat Ansible Automation Hub.

- **PyPI Curation Performance Improvements**
  PyPI Curation Service performance has been improved by implementing an internal caching mechanism for package index responses. This significantly reduces latency and improves build speeds for curated PyPI repositories.

- **Support added for Custom HTTP headers in remote repositories**
  Custom HTTP headers can now be configured for all remote repositories directly through Artifactory, without requiring external proxy workarounds. For more information, see Remote Repository JSON Configuration and Repositories Configurations in Artifactory YAML.

- **Support for Smart Remote Repositories over JFrog Bridge Connections**
  Smart remote repositories are now fully supported over JFrog Bridge connections in hybrid environments. Smart remote repository detection occurs when the upstream repository is accessed via a bridge connection,

and properties are properly synced when downloading artifacts through a Smart Remote repository over a bridge.

- **Xet protocol in remote Hugging Face repositories**
  Remote Hugging Face repositories now support Xet protocol, providing enhanced download performance and handling files larger than 50 GB. Xet is supported for repositories that use the new Machine Learning layout. Migrate legacy Hugging Face repositories to the new layout to use Xet. For more information, see Enable Xet Protocol for Hugging Face Repositories.

- **Enhanced Hugging Face compatibility for Xet 1.3.0+ clients**
  Added support for the `/v1/` CAS API path prefix to ensure compatibility with `hf_xet` client version 1.3.0 and later. This update enables successful file reconstruction and xorb chunk retrieval by correctly processing versioned endpoint paths.

- **Strict tag overwrite enforcement configuration**
  Docker, OCI, and Helm OCI repositories now have an **Enforce Strict Tag Overwrite** configuration setting. When enabled, this configuration requires explicit Delete/Overwrite permissions when pushing images with an existing name and tag. This enforcement prevents multiple manifest types under the same tag, maintaining stricter registry integrity.

- **AQL search results now respect repository include and exclude patterns**
  AQL search results now respect repository include and exclude patterns for local, remote, and virtual repositories. Items that do not match a repository's patterns are filtered out for non-admin users, so AQL results align with repository access rules and other search methods. For more information, see Artifactory Query Language.

Release Lifecycle Management

- **Draft Release Bundle v2 versions**
  You can now use the Create Release Bundle v2 Version REST API to create an unlocked, mutable draft. Use the new Update Draft Release Bundle v2 Content REST API to add sources—such as artifacts, packages, builds, or bundles—as needed. When the draft is final, use the new Finalize Draft Release Bundle v2 Version REST API to lock the bundle and make it immutable. Please note that Evidence cannot be added to a draft Release Bundle version until it is finalized. For more information about draft versions, including other limitations, see Create a Draft Release Bundle v2 Version.

- **Artifactory Edge APIs now support Release Bundle v2**
  The following REST APIs, which were developed for Release Bundle v1, can now be used to retrieve information about Release Bundle v2 (RBv2) versions as well:

  - `GET /api/release/bundles?type=target`
  - `GET /api/release/bundles/{name}?type=target`
  - `GET /api/release/bundles/{name}/{version}?type=target&format={format}`
  - `GET /api/release/bundles/{name}/{version}/status?type=target`
  - `GET /api/release/bundles/{name}/{version}/artifacts`
  - `DELETE /api/release/bundles/{name}/{version}`

  This feature enhancement is intended for users who have existing CI/CD processes that include calls to these endpoints and who now require RBv2 support. Users who do not already use these endpoints should use the standard RBv2 endpoints, as described in the Release Lifecycle Management API reference.

- **Performance improvements when exporting Release Bundle v2 versions**
  We are excited to announce significant performance improvements to the export Release Bundle v2 feature. This enhancement provides a more efficient and streamlined experience for users in both self-hosted and SaaS environments. Key improvements include:

  - Faster processing times: Reduced export times for Release Bundles, allowing for quicker access to essential data.
  - Optimized resource usage: More efficient utilization of system resources during the export process, leading to enhanced overall performance.
  - Scalability enhancements: Improved handling of larger datasets, ensuring consistent performance with support for big bundles, allowing users to export extensive Release Bundles without performance degradation.

- **Platform UI searches support Release Bundles v2**

The global search bar at the top of the platform UI now includes support for Release Bundles v2. A toggle switch makes it easy to choose between searching for Release Bundles v1 and Release Bundles v2 (v2 is the default). This enhancement makes it easy to find any Release Bundle quickly without first navigating to a specific window in the application. For more information, see Release Bundles Search.

- **Improved performance of Release Bundles v2 page**
  To improve the user experience, the platform UI page for Release Bundles v2 has been optimized, especially when displaying a long list of Release Bundles.
- **Evidence attachments**
  You can now attach a single, unstructured file — such as a PDF — during the evidence creation process. This feature provides a tamper-proof, signed container for both your structured evidence and unstructured data, ensuring a complete end-to-end audit trail. For more information, see Add an Attachment to Evidence.
- **Evidence distribution for Release Bundle v2 versions**
  JFrog Distribution and Artifactory now support the optional distribution of evidence attached to Release Bundle v2 versions (including package and artifact evidence), allowing security and compliance metadata to be delivered directly to Edge nodes. This ensures that every artifact reaches its destination with a complete, verifiable record of its quality and security posture. This feature completes the "chain of trust" by enabling the relevant users at the Edge to verify signatures, test reports, and compliance data before consumption.

> **Important**
>
> The ability to distribute evidence requires the enhanced distribution engine (introduced in JFrog Distribution release 2.28.1). You must also enable the configuration parameter `evidence-distribution-enable`.

Retention

- **Define path patterns in Retention policies**
  You can now refine the scope of package cleanup policies and Smart Archive policies by optionally defining one or more path patterns (as an addition to the mandatory repository patterns). The use of a wildcard at the beginning or end of each path pattern is supported.
- **Cleanup policies available for Enterprise X subscriptions**
  JFrog cleanup policies are now available to users with an Enterprise X subscription, in addition to those with Enterprise +. Cleanup removes unnecessary files, applications, and configurations to free up storage and improve system performance.
- **Cleanup policies can skip promoted artifacts**
  Package cleanup policies can now skip artifacts that are part of a promoted Release Bundle v2. Such cases are now treated as a warning instead of an error, which enables the cleanup of other packages to proceed smoothly. For more information, see Work with Cleanup.

General

- **Additions to the Artifactory Request Log and Outbound Request Log**
  The Artifactory Request Log (JSON only) and Outbound Request Log (JSON only) have been extended with two new fields that significantly simplify the analysis of traffic patterns:
  - **repo:** The name of the repository as it appears in the URL
  - **repo_type:** The type of the repository (one character). Will be one of the following:
    - **v:** virtual
    - **l:** local (also for federated)
    - **r:** remote

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-70357	Builds	High	Fixed an issue that prevented Xray from scanning artifacts in bu Artifactory Jenkins Plugin (v4.0.8). Builds deployed using the JFrc Plugin were not affected by this issue.
RTFE-4576	Builds	High	Fixed an issue that potentially allowed malicious insiders to exp
JA-19319	General	Medium	Fixed an issue related to Access Federation whereby, under cert were not displayed in the JFrog Platform UI as expected.
JA-19910	General	High	Fixed an issue related to Access whereby, under certain circums caused latency issues in gRPC endpoints.
JA-19924	General	Medium	Fixed an issue related to one-time passwords whereby when try displayed in the verification email as expected.
JA-19972	General	Medium	Fixed an issue related to tokens whereby, when using a non-JFrc against Artifactory, the JFrog Platform returned a 500 error inste
JA-8432	General	Medium	Fixed an issue related to Access Federation whereby, when usin timeout which is not used anymore in platform, the JFrog Platfo not as expected.
RPG-2028	General	Medium	Fixed an issue related to the JFrog Platform UI whereby, when tr Monitor Service page while Topology is enabled, the JFrog Platfc
RTDEV-66866	General	Medium	Fixed an issue whereby a request for a package that was not sca Unscanned enabled, was taking twice as long as the Block Unsc receiving the 403 error.
RTDEV-66255	General	Medium	Fixed an issue whereby objects used by the RubyGems package release their memory allocation, leading to potential Out of Mer
RTDEV-69075	General	Medium	Fixed an issue whereby when customers upgraded Artifactory H "Could not authenticate through LDAP server" appeared for son those LDAP users were still able to log in and access repositorie
RTDEV-73398	General	Medium	Fixed an issue whereby, when executing a curl command throug an empty folder in the upstream, Artifactory returned a 404 erro message.
RTDEV-73812	General	High	Fixed an issue whereby CPU usage using AQL tended to increas methods.
RTDEV-68641	Packages	Medium	Fixed an issue whereby the REST API for retrieving a list versions `https:/<ART_URL>/artifactory/api/gems/<repo_name` was not updated with the latest version.
RTDEV-73811	Packages	Medium	Fixed an issue whereby when the Docker Access Method was cc Set Me Up dialogue for Docker generated an incorrect Docker lc

Jira Issue	Component	Severity	Description
RTDEV-74459	Packages	Medium	Fixed an issue in which an incorrect README was displayed for a Artifactory Packages view.
RTDEV-77242	Packages	High	Fixed an issue whereby AI-Editor Extensions asset URLs from th were not rewritten via Artifactory.
RTDEV-79314	Packages	Low	Fixed an issue whereby when creating a CocoaPods remote rep field contained a trailing space, outbound requests for CDN res URL that always returned a 404 error from the upstream.
RTDEV-79614	Packages	Medium	Fixed an issue whereby the header **x-artifactory-curation-requ** when a smart remote repository was pointing to a remote repo
RTDEV-81215	Packages	Medium	Fixed an issue whereby when a Debian virtual repository includ "main" component and a debian-security remote, packages fror excluded from the merged index due to unsupported compoun updates/main) in the remote's Release file.
RTDEV-77435	Packages	Medium	Fixed an issue whereby when an Opkg package was deployed b delete or overwrite permissions, temporary folders were not de
RTDEV-79597	Release Lifecycle Management	Medium	Fixed an issue whereby a draft Release Bundle v2 version updat sources are invalid. The new behavior in sync mode returns an status as DRAFT. In async mode, the version status still changes
RTDEV-81145	Release Lifecycle Management	High	Fixed an issue whereby Release Bundle v2 versions created fror dependencies, could result in the platform UI linking to an invali dependency artifact.
RTFE-4259	Release Lifecycle Management	Medium	Fixed an issue that prevented users with the correct permission Bundles from the Builds page.
RTDEV-37129	Repositories	High	Fixed an issue whereby directory requests were not forwarded the upstream server by generic remote repositories when the p enabled, and instead returned Artifactory's directory listing.
RTDEV-74757	Repositories	Medium	Fixed an issue whereby Maven, Gradle, and SBT artifacts were s cleanup policy execution, leading to failed deletion attempts an
RTDEV-78662	Repositories	Medium	Fixed an issue whereby remote repository operations could tim resolution when following redirects from the upstream server.
RTDEV-81046	Repositories	Medium	Fixed an issue whereby pushing Docker images through a virtua `Forbidden` instead of a `404 Not Found` during tag existe read permissions on some aggregated repositories.
RTDEV-68312	Repositories	Medium	Fixed an issue with the REST API for checking the status of a rep was returning an OK status and updating the 'last completed' de mismatch of artifacts and the remote repository URL resulted ir

Jira Issue	Component	Severity	Description
RTFE-4702	Repositories	Medium	Fixed an issue whereby remote repositories failed to appear du virtual repository when External Dependency Rewrite is enablec
RTFE-4889	Repositories	Low	Fixed an issue whereby, when creating a smart remote reposito format, the error message displayed in the UI presented an opti correct format, but it was actually not the correct URL path.
RTDEV-80553	Storage	Low	Fixed an issue whereby the `nonProxyHost` parameter was n by AWS SDK v2.
RTDEV-82246	Storage	Medium	Fixed an issue whereby a custom KMS SSE key was not correctly SDK v2.
RTFE-4320	Storage	Medium	Fixed an issue in the repositories storage summary whereby sor folders, or items gave incorrect results.
JFUI-19766	User Interface	Medium	Fixed an issue whereby a user assigned the Platform Auditor rol Distribution historical data.
RTDEV-72622	User Interface	Medium	Fixed an issue whereby repositories of type Build Info were not page in the UI.
JA-16022	User Management	High	Fixed an issue whereby, when a user is part of a group with Mar and that group is included in a Permission Target with Manage p only see that specific Permission Target and was unable to see a expected.
JA-18804	User Management	Medium	Fixed an issue related to Projects whereby, when trying to creat users as a project admin, the JFrog Platform returned a 403 erro
JA-20273	User Management	High	Fixed an issue with Access Federation whereby enabling `allo` could cause permanent permission and user group divergence ((syncBaseline) operations.
JA-19606	User Management	Medium	Fixed an issue related to LDAP whereby, under certain circumst SAML setting containing multiple LDAP group settings that refer group synchronization fails to associate groups.
JA-19661	User Management	Low	Fixed an issue related to the JFrog Platform UI whereby, under c trying to access the User Profile page as an external user, the JF Forbidden error.
JA-19681	User Management	Medium	Fixed an issue with projects whereby, when generating a projec scope via the JFrog Platform UI, the JFrog Platform returned a 4(
MDL-573	General	High	Fixed an issue related to non-Kubernetes and non-Docker instal circumstances, OneModel GraphQL fails to start if the user runr permissions on the system-level certificates folder.

Artifactory 7.133

This section includes all the Artifactory 7.133 releases.

Critical Security Notice

All subversions are vulnerable to multiple non-critical security vulnerabilities that, in some deployments, can be chained into critical-severity attacks. We recommend that all customers upgrade to the latest version. View the latest Self-Managed and SaaS releases.

Important Notice for Customers Using RTFS (Artifactory Federation Service)

A critical issue affects RTFS on all Artifactory 7.133 versions higher than 7.133.12. Customers may see a **Federation service is unable to connect** banner even when RTFS is healthy. Upgrade to **7.146.0** or later (7.146.x, 7.147.x) for a permanent fix. Until then, restart Artifactory pods that log `ALERT: RTFS is enabled ... but the federation service queue does not exist`.

This issue affects RTFS only. Legacy federation is not affected.

For more information, see Troubleshoot RTFS connection banner on Artifactory 7.133.x in Federated Repositories.

Artifactory 7.133.30 Self-Managed

Released: 5 Sept 2026

This version includes security-driven configuration changes for plugin deployment.

Artifactory 7.133.29 Self-Managed

Released: 28 Aug 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-82329	General	Critical	Potential authentication bypass leading to administrative access in Artifactory

Artifactory 7.133.28 Self-Managed

Released: 12 August 2026

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-42018	General	High	Anonymous token exposure in JFrog Artifactory

Artifactory 7.133.27 Self-Managed

Released: 27 July 2026

Security Notice

This version is designed to fix multiple security vulnerabilities that, when chained together, could result in a critical attack scenario if Anonymous Access is enabled. Anonymous Access is disabled by default and is not recommended for production environments due to the additional security risks it introduces.

CVE	Component	Severity	Fix Description
CVE-2026-65617	Packages	High	Designed to prevent unsafe Gems package deserialization that could lead to remote code execution
CVE-2026-65925	Packages	Medium	Designed to validate Cargo sparse index URLs to prevent server-side request forgery
CVE-2026-65921	Builds	High	Designed to prevent build artifact archive paths writing outside intended locations
CVE-2026-65922	General	High	Designed to block unauthorized writes to restricted internal metadata storage locations
CVE-2026-65923	Builds	Medium	Designed to validate Ansible provider URLs to prevent server-side request forgery
CVE-2026-66014	General	High	Designed to prevent HA authentication fail-open behavior causing privilege escalation
CVE-2026-65924	Packages	Medium	Designed to validate Terraform external provider URLs to prevent server-side request forgery

Artifactory 7.133.25 Self-Managed

Released: 16 July 2026

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-92966	Packages	High	Fixed an issue whereby a deprecated endpoint caused npm audit queries for smart remote repositories to fail.

Artifactory 7.133.24 Self-Managed

Released: 15 July 2026

Resolved Issues

Jira Issue	Component	Severity	Description
RTFS-4094	Federated Repositories	Critical	Fixed a broken authorization service that could permit low-privileged users to read configuration data.
RTDEV-92146	Packages	Critical	Fixed a vulnerability in which weakly validated, request-derived data could be used to poison cached responses.

Artifactory 7.133.23 Self-Managed

Released: 29 June 2026

Important Notice for Customers Using AWS SDK Storage with KMS Client-Side Encryption

Customers using AWS SDK storage with KMS client-side encryption should not use AWS SDK v2. If you are using AWS SDK storage with KMS client-side encryption, ensure that in the `binarystore.xml` file `awsSdkV2` is set it to `false`. For more information, see Amazon S3 Template Parameters.

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-90290	Packages	High	Fixed an issue whereby publishing Cargo packages to Artifactory failed because the endpoint did not accept the Content-Type: application/octet-stream header, a breaking change introduced in Cargo client version 1.96.0.
RTDEV-90399	General	Critical	A high-severity vulnerability was fixed in Artifactory. In certain cases, deprecated services could allow a low-privileged user to retrieve artifacts from repositories they were not authorized to access. JFrog recommends that all self-managed customers upgrade to a fixed version as soon as possible, especially those with anonymous user access enabled.

Artifactory 7.133.22 Self-Managed

Released: 10 June 2026

Feature Enhancements

- **Support for Opting Out of New SAML Login Redirect Behavior**
  The JFrog Platform now supports reverting to the previous implementation of SAML login redirect, whereas upon automatic logout, users will be redirected to the SAML login URL. For more information, see SAML SSO.

Artifactory 7.133.21 Self-Managed

Released: 28 April 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

Feature Enhancements

- **Improved npm Indexing Performance**

Indexing for npm has been enhanced, after identifying and improving inefficient per-artifact property retrieval during metadata generation.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-69107	General	Medium	Potential unauthorized artifact access in JFrog Artifactory

Artifactory 7.133.18 Self-Managed

Released: 15 April 2026

Resolved Issues

Jira	Component	Severity	Description
RTDEV-83142	General	High	Fixed an issue whereby Artifactory failed to parse Xray responses after a Jackson library upgrade, affecting repository policy settings and repository diff report APIs.
RTDEV-82854	Packages	High	Fixed an issue whereby npm version metadata signatures were stripped from the response after the package tarball was cached, causing installation failures during signature verification.
RTDEV-80416	Packages	Medium	Fixed an issue whereby when the Docker Access Method was configured as a subdomain, the Set Me Up dialogue for Docker generated an incorrect Docker login URL.

Artifactory 7.133.17 Self-Managed

Released: 1 April 2026

This is a maintenance release with no features or enhancements. CVEs that don't impact Artifactory have been fixed.

Artifactory 7.133.16 Self-Managed

Released: 31 March 2026

Resolved Issues

Jira	Component	Severity	Description
META-2339	General	Medium	Fixed an issue whereby the Metadata service failed to register APIs to OneModel when using a router with a custom port.
RTDEV-80918	Packages	Medium	Fixed an issue whereby pulling Docker images from registry.navops.io failed due to a URL parsing error.
RTDEV-80507	Packages	High	Fixed an issue whereby temporary RPM and Ruby metadata files were not being properly purged from the Tomcat temporary directory after metadata calculation tasks.
RTDEV-81771	Storage	Medium	Fixed an issue whereby the remote binary provider was not releasing a connection when the stream was not fully consumed.
RTDEV-81105	Storage	High	Fixed an issue whereby deleting a folder from a repository incorrectly cleared unrelated items from the trash can if they shared a parent path.
JA-20323	User management	Low	Fixed an issue related to SCIM whereby, the SCIM Get Service Provider Configuration endpoint was incorrectly exposed at the pluralized path `/ServiceProviderConfigs`.

Artifactory 7.133.15 Self-Managed

Released: 18 March 2026

Feature Enhancements

- **Improved AWS SDK v2 CRT Client-Handling of Slow Connections**
  AWS SDK v2 CRT client-handling of slow connections has been improved by exposing the connection health timeout configuration. For more information, see Amazon S3 Template Parameters.

Resolved Issues

Jira	Component	Severity	Description
JFUI-20219	General	Medium	Fixed an issue whereby the frontend continued to communicate via the default port 8046, despite a custom internal port configured in the router.
META-2433	Packages	Medium	Fixed an issue whereby metadata failed to register APIs to OneModel via the router when a custom port is configured in `system.yaml`.
RTDEV-72627	Repositories	Medium	Fixed issue whereby the overlay field in the `source.json` file was missing when requesting a module from a Bazel Modules remote repository.

Jira	Component	Severity	Description
RTDEV-80569	Repositories	Medium	Fixed an issue whereby Artifactory Edge did not send the configured client TLS certificate during Smart Remote repository creation.
RTDEV-78355	Storage	Medium	Fixed an issue whereby the *Too many open files* error message was received when using a combination of the eventual upload mechanism and Filestore Sharding.

Artifactory 7.133.12 Self-Managed

Released: 2 March 2026

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-79785	User Interface (UI)	High	Fixed an issue whereby repositories failed to display on the Repositories UI for OSS and JCR.
JFUI-20068	User Interface (UI)	Medium	Fixed an issue whereby the `Xray Is Unavailable` status messages appeared in the user interface, even though builds were correctly indexed and scanned by Xray.

Artifactory 7.133.10 Self-Managed

Released: 18 February 2026

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-73702	Packages	High	Fixed an issue whereby npm virtual metadata ignored the override base URL for the X-Artifactory-Override-Base-Url header for certain packages.
RTDEV-76892	Repositories	Medium	Fixed an issue whereby HEAD requests for Docker manifests failed if the remote registry returned an incorrect or missing content type.
JA-19609	Projects	High	Fixed an issue whereby OIDC Identity Mappings with a defined Project scope and username pattern in token spec appended a User scope, causing authentication tokens to bypass Project-level permissions and verify user permission can result in 403 errors.
JA-19879	Projects	Low	Fixed an issue where explicit manage resources as false in create projects API made manage remote repo turned on.

Artifactory 7.133.8 Self-Managed

Released: 10 February 2026

Intended Change in Artifactory's Response to Improper Configuration of a Smart Remote Repository

To properly configure a smart remote repository using the Create Repository API, the URL of an Artifactory instance must be used as the URL of the remote repository, and the attribute `contentSynchronisation` must have `enabled = true` in the Repository Configuration JSON. Currently, if a user wants to create a smart remote repository and enables `contentSynchronisation`, but does not set the URL of an Artifactory instance as the URL of the remote repository, Artifactory responds by creating a regular (not smart) remote repository, sends a 200 success message, and disables `contentSynchronisation`. The user does not receive any indication that the smart remote repository that the user tried to create is actually a regular remote repository or that `contentSynchronisation` is disabled. Starting from May 12, 2026, Artifactory will respond differently to this scenario. Instead of creating a regular remote repository, Artifactory will respond with a 400 error message, and no repository will be created.

Artifactory to Stop Allowing Importing a Backup of Repositories with the `-cache` Suffix

Artifactory does not allow creating a repository with the `-cache` suffix, because `-cache` is a reserved string that Artifactory uses internally to create a `-cache` repository for every remote repository. However, currently Artifactory allows importing a backup of repositories even if there are repositories in that backup with a `-cache` suffix. Starting from May 12, 2026, Artifactory will no longer allow a backup of repositories if there are repositories in that backup containing the `-cache` suffix. Ensure that by May 12, 2026, you do not have any repositories with the `-cache` suffix to be backed up for the backup to run successfully.

Note that renaming existing repositories is not possible. Therefore, if you need to rename a repository because it has the `-cache` suffix, the most efficient way to do this is to create a new repository, copy the contents of the repository with the `-cache` suffix into it, then delete the old repository.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-76067	General	Medium	Fixed an issue whereby AQL returned an empty array for a valid build domain query when the `include` method contained 3 fields or less.
RTDEV-63325	General	Medium	Fixed an issue whereby when attempting to download a file via a URL in the native browser, if Allow Anonymous Access was enabled but authorization was still required, a pop-up appeared requesting a username and password to complete the download instead of an auto-redirect to the SAML login page.
RTDEV-71910	General	High	Fixed an issue whereby repository-level JMX attributes `ArtifactsCount` and `ArtifactsTotalSize` were missing from MBeans, preventing remote monitoring of storage metrics via JConsole.
RTFE-4535	User Interface (UI)	High	Fixed an issue whereby non-admin users sometimes experienced failures when uploading large artifacts through the Artifactory user interface.

JIRA Issue	Component	Severity	Description
RTDEV-73816	Release Lifecycle Management	High	Fixed an issue that potentially allowed malicious insiders to exploit a stored XSS vulnerability.

Artifactory 7.133.6 Self-Managed

Released: 3 February 2026

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-71255	Repositories	Medium	Fixed an issue whereby platform-level and Artifactory-level proxy settings were affecting local repository replication settings.
RTDEV-68312	Repositories	Medium	Fixed an issue with the REST API for checking the status of a repository replication where it was returning an OK status and updating the 'last completed' details, when in fact there was a mismatch of artifacts and the remote repository URL resulted in a 404 error.
RTDEV-65623	Platform Management	Low	Fixed an issue where errors occurred during the backup of a federated repository when there was a binary that was not fully federated.
JFUI-20087 and JFUI-20084	User Interface (UI)	High	Fixed an issue whereby certain Administration and Platform menu items, such as Retention Policies and Catalog, failed to display correctly on the initial page load.
JA-19632	User Management	High	Fixed an issue whereby upgrade fails due to LDAP groupDn already existing.
INST-17297	Installation	High	Fixed an issue whereby the JFConfig resource allocation in the `artifactory-2xlarge.yaml` chart sizing template is missing a `0` and could lead to memory errors.
JFUI-20114	User Interface (UI)	High	Fixed an issue related to the Service Status page in the JFrog Platform UI whereby, under certain circumstances, the Service Status page did not display nodes as expected.

Artifactory 7.133.3 Self-Managed

Released: 22 January 2026

Breaking Change for JFrog Platform Logging

From this Artifactory version, two system properties (`audit:enabled` and `db:batch-size`) will be moved from the Access YAML configuration file to the System YAML configuration file, and their values will be reverted to the default value.

This should not impact your environments. However, note that if you have defined a different value for either of these variables or wish to edit them, you can now find and edit them in the `system.yaml` file, located in the `$JFROG_HOME/artifactory/var/etc` folder.

More information about the parameters to be changed:

Parameter name in Access YAML (removed)	Parameter name in System YAML (added)	Description	Default value

`Audit:`
 	
`enabled:`
	`logging:`
	
	`audit:`
	
	`enabled:`
		Toggle logging of changes in Access configuration. It is highly recommended to keep this enabled.	`true`

`db:`
 	
`batch-size:`
	`database:`
	
	`batchSize:`
		Control the number of records in each batch when performing actions on Access resources.	`100`

Transition Default AWS SDK from v1 to v2 (Q2 Update)

In preparation for the sunset of AWS SDK v1 by Amazon Web Services, JFrog Artifactory will transition its default AWS SDK from v1 to v2 by June 30, 2026. This is a proactive step to ensure customers are positioned for long-term stability, security updates, and new features as v1 reached end-of-support at the end of 2025.

Why is JFrog making this change?

- **End of Support for v1**: Amazon Web Services announced that SDK v1 reached end-of-support at the end of 2025. After this date, v1 no longer receives new features, availability improvements, or security updates.
- **Security and Compliance**: Continuing to use v1 beyond 2025 exposes environments to potential security risks due to the lack of ongoing updates.
- **Feature Parity and Optimization**: Integration with v2 allows users to leverage the latest AWS features and optimizations for a more robust and efficient storage solution.

JFrog strongly recommends that all Artifactory customers currently using SDK v1 transition to SDK v2 at this point in time and not postpone this unnecessarily. For instructions on how to do this, see Integrate Artifactory with AWS SDK v2 for S3 Storage.

Timeline for the Sunset of JFrog Legacy Repository Federation

We are officially announcing the sunset plan for Legacy Repository Federation as we transition to the next-generation Artifactory Federation Service (RTFS). Please take note of the following timeline for this change:

Timelines

January 2026 (Current Status)

Official declaration of the sunset plan to all customers.

Migration Window (Now through Mid-2027)

An 18-month period during which customers are requested to migrate to the new Artifactory Federation Service. We encourage all users to begin planning their transition to take advantage of RTFS's superior architecture and enhanced capabilities.

July 2027 (Deprecation)

The actual removal of Legacy Federation from the codebase of new releases.

Note: Older releases will continue to be supported based on JFrog standard support policies.

Important Information

Database Requirements

Please be aware that the new RTFS service explicitly requires a PostgreSQL database connection. However, this requirement applies only to the RTFS service itself; your main Artifactory installation remains completely unaffected and continues to support all currently available databases.

Implementation Options

- If your Artifactory already uses PostgreSQL, you can use the same database instance.
- If your Artifactory uses a different database, you only need to introduce a separate PostgreSQL instance for the RTFS service. There is no need to migrate your entire Artifactory installation.

Why This Change?

The Artifactory Federation Service (RTFS) represents the next generation of repository federation with:

- Superior standalone microservice architecture designed to reduce impact on Artifactory
- All new features (including Unidirectional Sync) are being developed exclusively for RTFS
- Already the default for all JFrog SaaS customers
- Validated by leading enterprise customers with improved stability and performance

Migration Support

The migration from Legacy Federation to RTFS is designed to be seamless:

- Automatic migration tools are provided to ensure configuration and data integrity
- No downtime required during migration
- Hybrid mode supported (RTFS and Legacy can coexist during transition)
- Full rollback capabilities during the transition window
- You do not need to migrate all sites simultaneously

Important

Please note the following regarding certificates:

- The Artifactory Federation Service (RTFS) **supports self-signed certificates and certificates signed by a custom Certificate Authority (CA) starting from Artifactory version 7.133.4**.
- Customers running earlier versions must upgrade to a supported version to use self-signed or custom CA certificates with RTFS.

Note: This sunset applies to **Self-Hosted environments only**.

For detailed information about RTFS features, migration procedures, and FAQs, please refer to the Artifactory Federation Service documentation.

Filebeat Removal

Removed the Filebeat component from all JFrog product installers as part of the JFrog Insight deprecation process.

Action Required: If you utilize the bundled Filebeat application for purposes other than JFrog Insight, you must install a standalone version of Filebeat before upgrading to this version to prevent service disruption.

New Features

- **Application metrics now available to SaaS Users**
  Users working in SaaS (Cloud) environments can now receive a wide variety of application-related metrics (based on the Open Metrics standard) using a new REST API. For more information, see Get Artifactory Application Metrics API.
- **New REST API for preparing evidence for deployment to Artifactory** The new Prepare Evidence for Signing REST API simplifies the evidence creation process for users who do not use the JFrog CLI. The API request contains the predicate, which is a JSON containing claims about the defined evidence subject (for example, a build or artifact), and can include an optional markdown version. The API returns a payload that conforms to the in-toto attestation standard used by the JFrog platform. After signing the payload, you can deploy the evidence to the JFrog platform using the Deploy Evidence REST API. For more information, see Create Evidence using REST APIs.

Feature Enhancements

Release Lifecycle Management

- **Release Bundle v2 creation dry run** You can now use the Create Release Bundle v2 REST API to perform a dry run, which simulates the creation of the Release Bundle and performs all the necessary validations, but without persistence. For more information, see Perform a Release Bundle v2 Creation Dry Run.
- **New REST API for deleting the tag from a Release Bundle v2 version** To improve the user experience, you can use a new, dedicated REST API to delete a tag from a Release Bundle v2 version. For more information, see Delete Release Bundle v2 Version Tag API.
- **Query parameter for returning all errors during Release Bundle v2 creation** To help debug issues you may encounter during Release Bundle v2 creation, a new `fail_fast` query parameter has been added to the Create Release Bundle v2 REST API. When set to `false`, the API will return validation errors that occur during creation as a group instead of failing after the first error. For more information, see Release Bundle v2 Creation Errors Collected by System.
- **RLM promotion rollback from platform UI** To improve the user experience, you can now roll back a Release Bundle v2 version promotion from the platform UI. For more information, see Promotion Rollback. Please note that the UI icon for deleting a promotion has been removed, as rollback replaces this functionality.
- **Audit trail maintained when promoting duplicate Release Bundle artifacts** Previously during Release Bundle v2 promotions, the system skipped artifacts that already existed in the target stage. This behavior prevented the target stage from being updated with evidence associated with those artifacts. This enhancement guarantees that all associated evidence is copied to the target stage, ensuring a complete and verifiable audit trail throughout your SDLC.
- **Improved performance when creating Release Bundles from builds with dependencies** To enhance the user experience, we have implemented significant performance enhancements when creating Release Bundle v2 versions from builds that contain dependencies.

Platform UI

- **Significantly Improved Package Details User Interface** The Package Details user interface (UI) has been significantly improved, and now displays valuable information about package versions in a more user-friendly format, including:
  - When the Package Details view is initially displayed, details on the latest version or tag of the package appear.
  - Use of native terminology, based on the package context (for example, tags for Docker/OCI packages, versions for other package types).
  - Quick selection of a package version, allowing you to easily find the version you need.
  - An All Versions view, allowing quick impact analysis across all versions to see vulnerabilities and where versions are stored.
  - Multi-client install commands: Installation commands are provided for all officially supported clients in every package type.

- More install commands for more package types: The new UI introduces 35 new install commands to help developers use the packages they are looking for.
- Context-sensitive Information tabs, displaying important version information according to the package type. For more information, see The Package Details User Interface.

- **Significant Improvements in the Repositories User Interface** The Repositories user interface has been significantly re-designed, making it much more user-friendly and efficient. When initially opening the Repositories list, there are options to view the 20 most recently viewed repositories and to view inactive repositories. Filtering capability has been added, so that you can now filter the Repositories list according to Repository type, package type, URL (for remote repositories), Project association, stage, and repositories that have a replication (for local and remote repositories). For more information, see View Repositories.
- **Date picker to improve Builds page performance** To improve performance, the Builds page now features a date picker that displays only those builds within a defined timeframe. The default value is the last 7 days. Users can choose a different timeframe as needed.
- **Improved performance of Build Versions page in platform UI** Pagination has been added to the Build Versions page in the platform UI, which makes it faster and more convenient to use when the selected build contains many existing versions.
- **User Management - Permissions** Updated the tooltip for the Include All Builds checkbox to clarify that selecting this option includes all builds and preserves any defined exclude patterns. For more information, see Add Builds.
- **Added a Warning Message When Deleting a SCIM Token** The JFrog Platform now displays a warning message when attempting to delete a SCIM token, as deletion might disconnect authentication provider integrations.

Package Management and Repositories

- **Support for `.dsc` Source packages in local Debian repositories** Local Debian repositories now support Debian source packages. After configuring your sources.list file for source packages, you can deploy the component source package files one by one to your local repository and resolve them as a single package using apt-get source. For more information, see Connect Debian to Artifactory.
- **Performance optimizations in NuGet package manager**
  Artifactory now offers a newer implementation of the NuGet package manager in Self-Managed Artifactory deployments. The new implementation significantly improves performance and efficiency with the following benefits:
  - Improved package resolution speed and download efficiency
  - Resolved legacy memory-related issues
  - Reduced JVM heap memory usage To enable the new NuGet handler, add the following property to the Artifactory system properties file: `artifactory.package.handler.nuget=true`.

  The new handler is opt-in for Self-Managed Artifactory deployments at this time, but it will be the default NuGet handler for all customers in an upcoming release. The new handler is already implemented in SaaS versions of Artifactory.

  > **Note**
  > To ensure optimal performance, it is recommended Artifactory 7.125.0 or later before enabling this feature.

- **New REST APIs for VCS Remote Repositories to Obtain Data from Subgroup Repositories** New REST APIs have been added for VCS remote repositories to obtain data from subgroup repositories. Four new APIs have been added that allow you to:
  - Download a VCS Branch from a Subgroup Repository API
  - Download a VCS Tag from a Subgroup Repository API
  - Download a File in a VCS Branch in a Subgroup Repository API
  - Download a File in a VCS Tag in a Subgroup Repository API
    Also, the legacy APIs Get VCS Tags and Get VCS Branches can be used to obtain VCS tags and branches from subgroup repositories. Currently, branches and tags can be downloaded only in the `tar.gz` format. In this Artifactory version, these APIs can be used to obtain data from the Google Source Git Provider.

- **Google Source Git Provider for VCS Remote Repositories** Support has been added in the Artifactory user interface for the Google Source Git Provider for VCS remote repositories. For more information, see Use VCS to Proxy Git Providers.
- **Improvements in VCS Remote Repositories APIs** The user organization can now be used as the repository for downloading VCS tags, branches, files in a tag, and files in a branch. For more information, see Download a VCS Tag API, Download a VCS Branch API, Download File within a VCS Tag API, and Download File within a VCS Branch.
- Supported Clients and Versions
  - **Support for Kiro with AI Editor Extension repositories** You can now set up AI Editor Extension Repositories in Artifactory to securely proxy and cache the Kiro extension marketplace, and configure your Kiro IDE to download extensions from the Artifactory cache. For more information, see Get Started with AI Editor Extensions.
  - **Support for `pnpm` client with npm repositories** You can now configure the `pnpm` client to connect to npm repositories in Artifactory and use it to manage npm packages. For more information, see pnpm CLI.
  - **Support for `uv` client with PyPI repositories** You can now configure the `uv` client to connect to PyPI repositories in Artifactory and use it to manage Python packages. For more information, see uv client.
  - **Support for Yarn Modern with npm repositories** Artifactory now supports natively managing npm packages with Yarn V2+ (Modern). For more information, see Connect Yarn to Artifactory.
- **JFrog CLI commands for setting up IDEs with AI Editor Extension and JetBrains Plugins repositories** The new `jf ide setup` command automates the process of connecting your IDE to an AI Editor Extensions or JetBrains Plugins repository in Artifactory. You can run the single command to configure any supported client, instead of manually granting permissions and editing configuration files. For more information, see Connect IDE to Artifactory for AI Editor Extensions and Connect JetBrains IDE to Artifactory for JetBrains.
- **Curation Support Added for PHP Composer Remote Repositories** Artifactory now ensures security compliance for Composer repositories protected by JFrog Curation. If a package is blocked by security policy, Artifactory automatically prevents the Composer client from falling back to external source URLs to download.
- **Added Support for the Range Header in Download Requests for PyPI Repositories** Artifactory now supports Range requests when downloading Python packages from local, remote, and virtual PyPI repositories. This improves compatibility with the UV package manager and prevents redundant full-package downloads, reduces unnecessary download counts, and improves performance.
- **Added Support for Proxying the GitHub Enterprise Cloud Private Registry for Go Remote Repositories** Support has been added for proxying the GitHub Enterprise Cloud private registry (`<comanyName>ghe.com`) for Go remote repositories.
- **Curation Support Added for PHP Composer Remote Repositories** Artifactory now ensures security compliance for Composer repositories protected by JFrog Curation. If a package is blocked by security policy, Artifactory automatically prevents the Composer client from falling back to external source URLs to download. This feature requires Xray version 3.137.0 or above.
- **URL Auto-Correct Added to Procedure for Creating a Smart Remote Repository** An auto-correct feature was added to the procedure for creating a smart remote repository for certain package types, to ensure that a correct URL is used. For more information, see Configure a Smart Remote Repository.
- **Bridge URLs in Remote Repositories** Bridge URLs can now be used in remote repositories without additional configuration.

Retention and Cleanup Policies

- **Retention Policies - Package Version Pattern Filtering** Cleanup and Smart Archiving retention policies now support Include and Exclude Package Version Patterns. For more information, see Cleanup Policies and Smart Archiving.
- **Improved the Run reports generated by Retention Policies for packages (Cleanup and Smart Archiving)** The reports now include Package Path, Created Date, Modified Date, and Last Downloaded Date columns under Run Detailed Summary to facilitate better validation and auditing of deleted or archived packages. For more information, see Smart Archiving Run Report Overview, Restore Run Report Overview and Cleanup Run Report Overview.
- **Enhanced Cleanup and Archiving Policy Logic** Cleanup and smart archiving now supports logical AND operators, allowing you to combine time-based and property-based conditions for more granular management.

Workers

- **Updated Payload Code Sample for "Before Download Request Worker"** The payload code sample for Before Download Request Worker has been updated for backward compatibility and to avoid compilation errors. The redundant `repoPath` object has been removed from the root of the event request, and the headers object is now identified as `requestHeaders`. For more information, see Before Download Request Worker Code Sample.

Evidence

- **Evidence system enhancements**
  - **Cosign v3**: The Evidence system now supports automatic evidence creation using the Sigstore bundle format. This includes compatibility with both the `cosign sign` and `cosign attest` commands with the `new-bundle-format` flag. Support remains in place for in-toto attestations (DSSE) created with the legacy Cosign v2 `attest` command.
  - **PSS Padding**: To simplify integration with different systems that produce attestations, the Evidence system now supports secure PSS (Probabilistic Signature Scheme) padding for signatures when creating evidence with APIs. PKCS#1 v1.5 padding is still supported.
  - **Base64 URL encoding**: The Evidence system now supports Base64 URL encoding for the DSSE signature. Standard Base64 encoding is still supported.
- **New REST APIs for evidence queries** Two new REST APIs are available for performing evidence queries. They are intended for users who prefer traditional REST APIs for integration with their existing automation tools instead of using GraphQL. For more information, see Search Evidence (REST API) and Get Evidence by ID (REST API).
- **Evidence GraphQL API for returning evidence by ID** You can now use GraphQL to return the details of a specific evidence item using its ID instead of using its path. For more information, see Get Evidence by ID (GraphQL).

User Integrations

- **Support for Regex in OIDC Integration Dynamic Mapping** The JFrog Platform OIDC integration now supports dynamic mapping creation using regular expressions (regex), which automates and streamlines the process for various use cases.

Platform Management

- **Added a Warning Message When Deleting a SCIM Token** The JFrog Platform now displays a warning message when attempting to delete a SCIM token, as deletion might disconnect authentication provider integrations.
- **Support for New SCIM REST API Endpoints** The JFrog Platform now supports getting more information about your SCIM configuration and schemas via REST API. For more information, see Get Resource Types API, Get Service Provider Configuration, Get Schemas API, and Get Schema by ID.
- **New Support for Password Control Via REST API** The JFrog Platform Access service now enables you to expire and un-expire all passwords via REST API. For more information, see Expire Password for All Users API and Un-Expire Password for All Users API.
- **Support for Filtering Tokens by Scope via REST API** The JFrog Platform now supports filtering the results of the Get Tokens REST API using the scope parameter to get token results for a specific scope, such as group. For more information, see Get Tokens API.
- **Added Support for Project Admin Permissions** The JFrog Platform now offers more granular control over project admin permissions, enabling you to grant **Manage Resources** permissions to project admins while preventing them from creating or managing remote repositories.
- **Logging of Administration Configuration Changes** The JFrog Platform now supports logging of any changes made to the access configuration, such as enabling anonymous access, in the Access audit trail log.
- **Support for Webhook Target Validation** The JFrog Platform now supports creating a whitelist to allow private domains or IP addresses to be used as Webhook targets without needing to disable Artifactory validation.****

Storage

- **Support Added for Decompressing `.xz` and `tar.xz` Files**
  Artifactory now supports decompressing `.xz` and `tar.xz` files, similar to the already supported decompression for `.zip`, `.tar`, and `.gz` files.

Helm Charts

- The Artifactory Helm chart now supports Azure Workload Identity authentication through the new `useInstanceCredentials` parameter. This authentication method replaces the legacy `saasTokens` and `accountKey` configurations. For more information, see Azure Workload Identity
- The Artifactory Helm chart now includes the `rtfs.customCertificatesSecretName` parameter for the RTFS service. This ensures custom certificates are properly copied to the RTFS container's trusted certificates folder.

Resolved Issues

JIRA issue	Component	Severity	Description
RTDEV-66665	Artifactory	Medium	Fixed an issue whereby, event-based push replication configured on a federated repository in the config descriptor could lead to an infinite cyclic event.
JA-18771	Authentication Providers	High	Fixed an issue related to CI integration with OIDC whereby, when using group mapping and dynamic user mapping, the access token was generated without the `applied-permissions/user` scope.
JA-19208	Authentication Providers	Medium	Fixed an issue related to the OIDC integration whereby, when setting two identity mappings with the same name, the JFrog Platform returned a 500 error.
RTDEV-67140	Builds	Medium	Fixed an issue that prevented Project Administrators from defining webhooks for build events within their assigned project.
RTDEV-69072	Federated Repositories	Medium	Fixed an issue whereby it was not possible to remove a disabled federation member.
RTDEV-67129	Federated Repositories	Medium	Fixed an issue whereby replication creation or update could fail at runtime with a "value too long for type character varying" error by adding upfront validation that blocks configurations when the combined include/exclude pattern length exceeds the supported database limit.
RTDEV-65263	General	Medium	Fixed an issue whereby restoring the root folder of a repository deleted any properties that were set on the root folder.
RTDEV-69867	General	Medium	Fixed an issue whereby the JFConnect client did not adhere to the custom router port configuration, thus causing Artifactory to fail upon initialization when the custom router port was set.
RTDEV-69778	General	High	Fixed an issue where it was possible to create a permission with an empty Repositories list.
JA-18497	General	Low	Fixed an issue related to logging whereby, after upgrading Artifactory to version 7.117.16 or later, a warning was logged in the Artifactory log file related to `BeforeTokenExpiryWorkerNotifyTask` that was unnecessary.

JIRA issue	Component	Severity	Description
RTDEV-67058	General	Medium	Fixed an issue whereby the Hex package dependency appeared as 'null' for the opentelemetry package.
RTDEV-65879	General	Medium	Fixed an issue where it was not possible to download a file inside an archive from the UI when the URL contained a period (“.”).
RTDEV-64090	General	Medium	Fixed an issue whereby when an artifact that was marked as filtered was deployed to a repository with password retrieval, the artifact obtained via cURL download contained an encrypted password, whereas the artifact downloaded through the UI did not.
RTDEV-54345	General	High	Fixed an issue whereby during HA cluster startup, a node which acquired the so-called “HA init lock” in order to perform exclusive init operations crashed, leaving the lock in place and blocking other nodes from starting, thus leaving the entire HA cluster in downtime.
EVT-2194	General	Medium	Fixed an issue related to webhooks whereby, when creating a webhook using a proxy and then editing it to remove the proxy, the JFrog Platform prevented leaving the Proxy field empty.
JA-18498	General	Low	Fixed an issue whereby users in view-only mode could click a link that incorrectly opened an OIDC integration/mapping drawer in edit mode, leading to an error when they attempted to save unauthorized changes.
RTDEV-61244	General	Medium	Fixed an issue whereby there was unauthenticated access to a Docker API when anonymous access was disabled.
RTDEV-64461	General	Medium	Fixed an issue whereby Artifactory was not following the RFC 9110 standard regarding the precedence of the precondition headers `If-None-Match` and `If-Modified-Since`.
RPG-1994	General	Medium	Fixed an issue whereby, when using the router metrics REST API endpoint, the JFrog Platform did not include the `content-type` header in the response.
INST-11384	Installation	Medium	Fixed an issue whereby the docker-compose-all.yaml template did not expose Nginx ports by default.
INST-11555	Installation	High	Fixed an issue whereby the command to perform a graceful shutdown was not working for **Jfconfig** and **Topology** services in certain negative scenarios, specifically when the Artifactory service hadn't fully

JIRA issue	Component	Severity	Description
			started. This meant these services would sometimes remain active despite a stop command.
RTDEV-70712	Packages	Medium	Fixed an issue whereby the Artifactory Maven indexer left indexer files open on the JVM even after they were deleted.
RTDEV-70121	Packages	Medium	Fixed an issue whereby Go repositories failed to resolve nested submodules hosted in a monorepo structure on GitHub.
RTDEV-70709	Packages	High	Fixed an issue whereby Artifactory was downloading an empty `.zip` file to a Go directory in a GitLab project, which resulted in the Go client receiving an empty `.zip` file when requesting a package.
RTDEV-70372	Packages	High	Fixed an issue whereby an older retention tag time could have been incorrectly used as the modification time for a later parent image, resulting in premature deletion.
RTDEV-69690	Packages	High	Fixed an issue whereby the download from a Smart Repository was performed using the actual Smart Repository and not the remote repository that it refers to.
RTDEV-68382	Packages	Medium	Fixed an issue in which Docker range uploads returned an incorrect range start offset.
RTDEV-66745	Packages	Medium	Fixed an issue whereby Helm layout enforcement was not working on federated Helm repositories.
RTDEV-65894	Packages	Medium	Fixed an issue in which a user could retrieve certain metadata files from a Debian virtual repository using the anonymous user, even though the user lacked proper permissions.
RTDEV-65622	Packages	Medium	Fixed an issue where Nuget package downloads through a virtual repository could fail when parent and child virtual repositories used different repository layouts.
RTDEV-65854	Packages	Medium	Fixed an issue whereby a RubyGems virtual repository intermittently returned the versions file that included only versions from aggregated local repositories because `UnsupportedReentrantLockException` disrupted metadata calculation and caused the remote handler to fail.
RTDEV-64188	Packages	Medium	Fixed an issue whereby the displayed download count for Conan packages on the Packages tab did not

JIRA issue	Component	Severity	Description
			increase when packages were downloaded, and remained 0.
RTDEV-64026	Packages	Medium	Fixed an issue whereby the npm remote repository with Curation complain version selection enabled would sometimes return the uncurated metadata ETAG header, which caused the npm client to not fetch the curated metadata from the registry even though the metadata was curated and changed.
RTDEV-65895	Packages	High	Fixed an issue whereby a race condition in the Debian indexing code was causing automatic indexing to not occur, which resulted in packages missing from the metadata.
RTDEV-63511	Packages	Low	Fixed an issue whereby the Downloads and Last Downloaded fields were not updated when converting an existing non-v1 Docker manifest to v1 manifest in a local Docker repository.
JA-18318	Projects	Medium	Fixed an issue related to the JFrog Platform WebUI whereby when sorting the results in the Project page by storage quota, the JFrog Platform did not perform as expected.
RTDEV-69828	Release Lifecycle Management	Low	Fixed an issue that prevented users from using multiple filters to exclude specific packages when patching a Release Bundle.
RTDEV-68592	Release Lifecycle Management	Medium	Fixed an issue whereby promotion rollbacks were not displayed correctly in the version timeline. After the fix, the timeline adds an event indicating the rollback succeeded and crosses out the previous event that recorded the promotion.
RTDEV-68310	Release Lifecycle Management	Medium	Fixed an issue whereby Release Bundle v2 promotion would sometimes fail due to HTTP 404 errors.
RTDEV-65239	Release Lifecycle Management	Medium	Fixed an issue whereby the contents of multi-arch Docker/OCI images were sometimes not displayed in the platform UI. After the fix, the contents are displayed correctly.
RTDEV-68303	Release Lifecycle Management	Low	Fixed an issue that prevented the Content Graph from displaying correct information after promotion rollback is performed. After the fix, the graph displays the results of the rollback accurately.

JIRA issue	Component	Severity	Description
RTDEV-66109	Release Lifecycle Management	Medium	Fixed an issue whereby an attempt to create a Release Bundle v2 version with a non-existing artifact resulted in a 500 status code. After the fix, this type of error will result in the expected 404 error, "Release Bundle source artifact not found".
RTDEV-61860	Release Lifecycle Management	Medium	Fixed an issue that prevented users from federating Release Bundle v2 repositories when using the Artifactory Federation Service (RTFS). After the fix, these repositories can be federated without incident.
RTDEV-59638	Release Lifecycle Management	Medium	Fixed an issue whereby deleting the last version of a Release Bundle did not remove the empty folder from the Release Bundle repository.
RTDEV-66254	Release Lifecycle Management	Medium	Fixed an issue whereby Release Bundle v2 creation failed due to a duplicate key error. This error occurred when a Docker image in the Release Bundle contained both a manifest.json and a list.manifest.json. After the fix, Artifactory can handle the duplicate key correctly and create the Release Bundle.
RTDEV-69500	Repositories	Medium	Fixed an issue whereby attempting to delete a non-existing artifact resulted in status code 204 (No Content) rather than 404 (Not Found).
RTDEV-62756	Repositories	Low	Fixed an issue whereby the Create Repository REST API allowed adding a repository of any type (local, remote, or virtual) to a virtual repository with a specific package type (not generic), when the added repository was for a package type that did not match the virtual repository's package type.
RTDEV-63395	Repositories	Medium	Fixed an issue whereby when importing a repository to Artifactory, artifact file statistics, such as `downloadCount`, `lastDownloaded`, `lastDownloadedBy`, were not merged for artifacts that already existed in the target instance.
RTDEV-70880	Storage	Medium	Fixed an issue whereby AWS SDK v2 with the KMS client-side failed to decrypt large objects.
RTDEV-64246	Storage	Low	Fixed an issue whereby binaries pruning was not running when the rootFoldersNameLength wasn't set as the default.
JA-18797	User Interface (UI)	Medium	Fixed an issue related to LDAP whereby, when trying to set up a repository as an LDAP user, the JFrog Platform returned a Forbidden error.
JA-18806	User Interface (UI)	Medium	Fixed an issue related to the JFrog Platform UI whereby, when a user logs in via SAML SSO, the Email

JIRA issue	Component	Severity	Description
			Address field in their Profile page appears as empty and uneditable.
JA-18290	User Interface (UI)	Medium	Fixed an issue whereby it was not possible to revoke the OIDC exchange Access token created with the Project Roles scope.
JA-18801	User Management	Medium	Fixed an issue related to the Administration module on the JFrog Platform UI whereby, when a non-admin user with Manage Resources permissions attempted to access the Permissions page, the JFrog Platform returned an error.
JA-18600	User Management	High	Fixed an issue related to API key whereby, when upgrading from Artifactory version 7.104.14 to 7.117.17 and attempting to regenerate the API Key via the JFrog Platform UI, the JFrog Platform returned an error.
JA-18099	User Management	Low	Fixed an issue whereby, when using the create or update Groups REST API and providing a string exceeding the maximum length, the JFrog Platform returned an incorrect error message.

Artifactory 7.125

This section includes all the Artifactory 7.125 releases.

Critical Security Notice

All subversions are vulnerable to multiple non-critical security vulnerabilities that, in some deployments, can be chained into critical-severity attacks. We recommend that all customers upgrade to the latest version. View the latest Self-Managed and SaaS releases.

Artifactory 7.125.21 Self-Managed

Released: 5 Sept 2026

This version includes security-driven configuration changes for plugin deployment.

Artifactory 7.125.20 Self-Managed

Released: 28 Aug 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-82329	General	Critical	Potential authentication bypass leading to administrative access in Artifactory

Artifactory 7.125.19 Self-Managed

Released: 18 August 2026

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-42018	General	High	Anonymous token exposure in JFrog Artifactory

Artifactory 7.125.18 Self-Managed

Released: 27 July 2026

Security Notice

This version is designed to fix multiple security vulnerabilities that, when chained together, could result in a critical attack scenario if Anonymous Access is enabled. Anonymous Access is disabled by default and is not recommended for production environments due to the additional security risks it introduces.

CVE	Component	Severity	Fix Description
CVE-2026-65617	Packages	High	Designed to prevent unsafe Gems package deserialization that could lead to remote code execution
CVE-2026-65925	Packages	Medium	Designed to validate Cargo sparse index URLs to prevent server-side request forgery
CVE-2026-65921	Builds	High	Designed to prevent build artifact archive paths writing outside intended locations
CVE-2026-65922	General	High	Designed to block unauthorized writes to restricted internal metadata storage locations
CVE-2026-65923	Builds	Medium	Designed to validate Ansible provider URLs to prevent server-side request forgery
CVE-2026-66014	General	High	Designed to prevent HA authentication fail-open behavior causing privilege escalation
CVE-2026-65924	Packages	Medium	Designed to validate Terraform external provider URLs to prevent server-side request forgery

Artifactory 7.125.16 Self-Managed

Released: 15 July 2026

Resolved Issues

Jira Issue	Component	Severity	Description
RTFS-4094	Federated Repositories	Critical	Fixed a broken authorization service that could permit low-privileged users to read configuration data.
RTDEV-92146	Packages	Critical	Fixed a vulnerability in which weakly validated, request-derived data could be used to poison cached responses.

Artifactory 7.125.15 Self-Managed

Released: 29 June 2026

Important Notice for Customers Using AWS SDK Storage with KMS Client-Side Encryption

Customers using AWS SDK storage with KMS client-side encryption should not use AWS SDK v2. If you are using AWS SDK storage with KMS client-side encryption, ensure that in the `binarystore.xml` file `awsSdkV2` is set it to `false`. For more information, see Amazon S3 Template Parameters.

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-90399	General	Critical	A high-severity vulnerability was fixed in Artifactory. In certain cases, deprecated services could allow a low-privileged user to retrieve artifacts from repositories they were not authorized to access. JFrog recommends that all self-managed customers upgrade to a fixed version as soon as possible, especially those with anonymous user access enabled.

Artifactory 7.125.14 Self-Managed

Released: 28 April 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-69107	General	Medium	Potential unauthorized artifact access in JFrog Artifactory

Artifactory 7.125.12 Self-Managed

Released: 27 January 2026

Resolved Issues

JIRA Issue	Component	Severity	Description
JFUI-20084	User Interface (UI)	High	Fixed an issue whereby certain Administration and Platform menu items, such as Retention Policies and Catalog, failed to display correctly on the initial page load.

Artifactory 7.125.11 Self-Managed

Released: 13 January 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-69867	General	Medium	Fixed an issue whereby the JFConnect client did not adhere to the custom router port configuration, thus causing Artifactory to fail upon initialization when the custom router port was set.
RTDEV-65263	General	Medium	Fixed an issue whereby restoring the root folder of a repository deleted any properties that were set on the root folder.
RTDEV-71829	Packages	High	Fix an issue whereby the Artifactory Maven indexer leaves indexer files open on the JVM even after they have been deleted.
RTDEV-70712	Packages	Medium	Fixed an issue whereby the Artifactory Maven indexer left indexer files open on the JVM even after they were deleted.

Artifactory 7.125.10 - Self-Managed

Released: 30 December 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-69690	Packages	High	Fixed an issue whereby Terraform Smart Repositories incorrectly attempted to resolve dependencies by originating the download request from the local instance instead of the configured upstream remote instance.
RTDEV-68382	Packages	Medium	Fixed an issue whereby Docker range uploads returned an incorrect range start offset.

JIRA Issue	Component	Severity	Description
RTDEV-66745	Packages	Medium	Fixed an issue whereby Helm layout enforcement was not working on federated Helm repositories.
RTDEV-65894	Packages	Medium	Fixed an issue whereby a user could retrieve certain metadata files from a Debian virtual repository using the anonymous user, even though the user did not have proper permissions.

Artifactory 7.125.9 Self-Managed

Released: 16 December, 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-65622	Packages	Medium	Fixed an issue where NuGet package downloads through a virtual repository could fail when parent and child virtual repositories used different repository layouts.
RTDEV-66835	Storage	Medium	Fixed an issue whereby the Sharding Balancer was not running as part of the full Garbage Collection.

Artifactory 7.125.8 Self-Managed

Released: 4 December 2025

Feature Enhancements

- **Database Optimizations**
  - Optimized Artifactory's shift events operation by refactoring the internal database process to use bulk inserts, significantly reducing database round trips and improving performance
  - Optimized the performance of node event deletion in Artifactory when using an Oracle Database by adding an optional system property to utilize the primary key index. See Oracle for Artifactory.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-61244	General	Medium	Medium Fixed an issue whereby there was unauthenticated access to a Docker API when anonymous access was disabled.
JA-18600	User Management	High	Fixed an issue related to API key whereby, when upgrading from Artifactory version 7.104.14 to 7.117.17 and attempting to regenerate the API Key via the JFrog Platform UI, the JFrog Platform returned an error.

Artifactory 7.125.7 Self-Managed

Released: 18 November, 2025

Feature Enhancements

- **Retention Policies - Package Version Pattern Filtering**
  Cleanup and Smart Archiving retention policies now support Include and Exclude Package Version Patterns. For more information, see Cleanup Policies and Smart Archiving.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-65895	Packages	High	Fixed an issue whereby a race condition in the Debian indexing code was causing automatic indexing to not occur, which resulted in packages missing from the metadata.
RTDEV-65747	Packages	High	Fixed an issue whereby Cocoapods remote repository gitref files fail to update when external dependency rewrite is enabled, thereby preventing successful pulls of latest packages.
RTDEV-64996	Packages	Medium	Fixed an issue where Terraform module downloads through virtual repositories failed when the module's namespace matched the local repository name. The `X-Terraform-Get` header now correctly includes the complete module path.
RTDEV-65858	Storage	Medium	Fixed an issue whereby a federated member was not deactivated even if not accessible, due to incorrect processing of exceptions that were thrown during ping.

Artifactory 7.125.6 Self-Managed

Released: 4 November, 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-64461	General	Medium	Fixed an issue whereby the `If-None-Match` header was not correctly given precedence over the `If-Modified-Since` header, causing conditional requests to be evaluated incorrectly and not in accordance with RFC 9110.
RTDEV-64151	Release Lifecycle Management	High	Fixed an issue that prevented Release Bundle v2 versions from working properly when Artifactory is configured with an MSSQL database.

JIRA Issue	Component	Severity	Description
RTDEV-63395	Repositories	Medium	Fixed an issue whereby when importing a repository to Artifactory, artifact file statistics, such as downloadCount, lastDownloaded, lastDownloadedBy, were not merged for artifacts that already existed in the target instance.

Artifactory 7.125.4 Self-Managed

Released: 30 October, 2025

New Features

- **Support for Sigstore bundle attestations**
  Artifactory now supports the automatic conversion of OCI Sigstore bundle attestations into JFrog evidence.
- **New Parent Manifests API**
  A Parent Manifests API has been added, which allows you to discover all parent manifest lists associated with a specific Docker manifest. For more information, see Find Parent Manifest Lists.
- **New Platform Auditor User Type**
  The JFrog Platform now supports a Platform Auditor user role that allows users to view the entire JFrog Platform Web UI but not perform any actions, which can be useful for auditing or compliance monitoring. To use this feature, enable the following feature flag in your system configuration file:

  ```
  accessPlatformAuditor: true
  ```

  For more information, see The Platform Auditor.
- **Support for signed attestations in OCI images**
  The Evidence Collection service can take signed, 3rd-party attestations uploaded to Artifactory as OCI images and convert them automatically into JFrog evidence. For example, this new feature can successfully convert attestations created using the **cosign attest** command. For the automatic conversion to work, the attestations must conform to both the DSSE and in-toto standards.
- **Cleanup - Builds**
  Artifactory now supports a build cleanup policy to delete unintended builds. For more information, see Cleanup Policies.
- **New Remote Repository Types for IDE Plugins**
  Two new remote repository types, AI Editor Extensions and JetBrains Plugins, are now available to proxy IDE plugin marketplaces. The AI Editor Extensions repository supports proxying extension marketplaces for VSCode, Cursor, and Windsurf. This repository type is integrated with JFrog Curation to enable policy-based blocking of unwanted plugins. The JetBrains Plugins repository supports proxying the JetBrains Marketplace for JetBrains IDEs such as IntelliJ IDEA and PyCharm.
  With both repository types, you can browse and install extensions and plugins natively within each IDE.
  The repositories are available to customers with an Ultimate bundle subscription.
- **New Remote Repository Type for Bazel Modules**
  The new Bazel Modules remote repository type supports caching and proxying the Bazel Central Registry (BCR) in Artifactory. This repository type is designed to support module dependency maknagement in accordance with Bazel 9 requirements. Maintaining a secure cache and proxy of the BCR ensures that developers pull only approved and vetted dependencies, enhancing security and streamlining the development process. For more information, see Bazel Modules Repositories.
- **Update Password Policy Via REST API**
  The JFrog Platform now supports creating and updating your instance's password policy via REST API, for easier access for Cloud instances. For more information, see Password Policy.
- **Artifactory Now Natively Supports the Terraform Provider Registry Protocol**
  Artifactory now natively supports the HashiCorp Terraform Provider Registry Protocol, acting as a fully compliant **Provider Origin Registry** for both Terraform and OpenTofu. This enhancement simplifies client configuration, enhances security with GPG verification, and provides smarter protocol-aware proxying. This

new method applies to local, virtual, and federated repositories and adds to the `network_mirror` approach. For more information, see Documentation.

Feature Enhancements

- Storage
  - **Support for AWS SDK v2 in S3 Storage**
    Artifactory's S3 binary storage provider now supports AWS SDK v2. This integration allows you to leverage the latest AWS features and optimizations for a more robust and efficient storage solution, while maintaining full backward compatibility with your existing S3 configurations. AWS SDK v2 receives all active development, new features, and security updates, ensuring your storage integration remains up-to-date. For more information, click here.

> **Important**
>
> Amazon Web Services has decided to make SDK v1 end-of-life at the end of 2025. Therefore, JFrog strongly recommends that all Artifactory customers currently using SDK v1 transition to SDK v2 at this point in time.

- **Support for Azure Workload Identity**
  Artifactory now supports authentication with Azure Blob Storage using Azure Workload Identity. This method provides a secure, secret-less authentication mechanism for applications running on Azure Kubernetes Service (AKS). It leverages federated identity credentials, eliminating the need to manage and rotate secrets such as SAS tokens or storage account keys within your Artifactory configuration. For more information, click here.
- **Data Sharding Improvements**
  Improvements were made in thread synchronization in sharding and s3-sharding providers.
- **Daily Cleanup Job Added for Cache FS _pre folder**
  A daily job is now triggered on startup to cleanup old `dbRecord*.bin` files in the cache provider's `_pre` folder. The configurations for this job can be modified in the **binarystore.xml** file under the cache-fs provider. For more information, see Cached Filesystem Binary Provider.
- **Additional Configuration for GCP Internal Actions**
  The ability to configure readTimeout was added to Google Cloud Platform (GCP) internal actions.
- Project Administration
  - **Support for webhooks for project-related builds**
    Artifactory now supports the creation of webhooks for builds associated with specific projects. This enables you to receive notifications whenever a build in a particular project is uploaded, promoted, or deleted. To create a build webhook for a specific project, you must be working within the scope of the project (as opposed to All Projects).
    For specific guidelines about creating a build webhook for a specific project, see Domain: Build.
- Evidence Management
  - **Evidence propagation to Federation members**
    This release enhances the Evidence service to enable evidence propagation to all Federation members, regardless of whether they contain the relevant public key for verification. Evidence verification, however, is performed only on those members that have the public key. For more information, see Verify Evidence.
  - **Evidence for artifacts in virtual repositories displayed in Artifacts tree**
    You can now view evidence related to artifacts in a virtual repository in the Artifacts tree. This is particularly useful when attaching evidence to a Docker image created in a tool such as GitHub Actions. In such cases, users typically work with the Docker image as part of a virtual repository in Artifactory. The virtual repository must contain at least one local repository to house the evidence. For more information, see View the Artifact Evidence Table.
  - **Improvements to evidence graph**
    The design of the Release Bundle evidence graph has been improved to make it easier to distinguish between the various elements (builds, packages, etc.) that comprise the Release Bundle. For more information, see View Release Bundle v2 Evidence.
- Federation
  - **Enhanced metadata propagation during RTFS Full Sync operations**

The Artifactory Federation Service (RTFS) now supports the propagation of artifact creation time metadata during a Full Sync operation. To enable this feature:

1. Set the following Artifactory system property to `true` on the target members:
   `artifactory.federated.mirror.events.upload.info.propagate.enabled`
2. Use a new REST API to enable the propagation of this specific metadata. For more information, see Propagate Creation Time Metadata during Full Sync API.

- **Updated Artifactory Worker Events**
  Updated the following Artifactory Worker events:
  - After Copy: The following fields are removed from the Sample Payload: `contentLength`, `trustServerChecksums`, `servletContextUrl`, `skipJarIndexing` and `disableRedirect`.
  - After Delete: The following field is removed from the Sample Payload: `headers`
  - After Property Create: The following fields are removed from the Sample Payload: `contentLength`, `trustServerChecksums`, `servletContextUrl`, `skipJarIndexing`, `disableRedirect` and `headers`.
  - After Move: The following fields are removed from the Sample Payload: `contentLength`, `trustServerChecksums`, `servletContextUrl`, `skipJarIndexing` and `disableRedirect`.
  - Before Move: The following fields are removed from the Sample Payload: `contentLength`, `trustServerChecksums`, `servletContextUrl`, `skipJarIndexing` and `disableRedirect`.
  - **Before Download Request**: The following fields are added in the response: `modifiedRepoPath`, `expired` and `headers`.
  - **Before Create**: The following fields are removed from the Sample Payload: `contentLength`, `trustServerChecksums`, `servletContextUrl`, `skipJarIndexing` and `disableRedirect`.
  - **Before Copy**: The following fields are removed from the Sample Payload: `contentLength`, `trustServerChecksums`, `servletContextUrl`, `skipJarIndexing` and `disableRedirect`.
  - **Before Property Create**: The following fields are removed from the Sample Payload: `contentLength`, `trustServerChecksums`, `servletContextUrl`, `skipJarIndexing` and `disableRedirect`.
  - **Before Property Delete**: The following fields are removed from the Sample Payload: `contentLength`, `trustServerChecksums`, `servletContextUrl`, `skipJarIndexing` and `disableRedirect`.
  - **After Property Delete**: The following fields are removed from the Sample Payload: `contentLength`, `trustServerChecksums`, `servletContextUrl`, `skipJarIndexing` and `disableRedirect`.
  - Updated the following Worker Events with `repoType` Input Parameter:
    - Before Property Replication
    - Before File Replication
    - Before Statistics Replication
    - Before Directory Replication
    - Before Delete Replication
- Smart Archiving
  - **Skips Restore of Artifacts with the Same Name and Path**
    The restore process now skips any artifact that already exists in the target location, preventing accidental overwrites. The existing file will be preserved, and the skipped operation will be noted in the logs and the CSV report.
  - **Supported Archive Packages Search for Project Admins**

Project Admins will now see and be able to use the Archive Search feature. The search results are automatically scoped, ensuring they can only view archived packages that belong to the projects they manage.

- API Updates
  - **Filtering added to Get All Repository Configurations API**
    You can now use query parameters to filter the results of the Get All Repository Configurations API. You can filter by package type (for example, docker, maven) and repository type (for example, local or remote).
  - **Change in API response for Release Bundle v2 tags**
    To correct inconsistent behavior, the following API endpoints have changed the response for Release Bundle v2 tags from `bundle_tag` and `release_bundle_tag` to a standard response of `tag`:
    - Create Release Bundle v2 Version
    - Assign Tag to Release Bundle v2 Version API
    - Get Release Bundle v2 Versions API
  - **Improved Get Federation Sync State REST API performance**
    The performance of the REST API that returns the synchronization state of all Federated repositories in the JPD has been improved.

> **Note**
> This API endpoint is relevant for users operating the legacy Federation service, not the Artifactory Federation Service (RTFS).

- Package Management and Repositories
  - **Virtual Repositories for Hugging Face Packages**
    Virtual repositories can now be created for Hugging Face packages.
    - Local and remote Hugging Face repositories that are associated with a virtual Hugging Face repository must have the Machine Learning Repository Structure.
    - Hugging Face datasets and models can be resolved from a virtual Hugging Face repository only with the snapshot_download API and not by using libraries.

    For more information, see Create a Hugging Face Repository and Resolve Hugging Face Packages.
  - **RPM Package Settings**
    Added support for Administrators to enable/disable RPM package settings for the following:
    - Recommends Tags
    - SHA256

    For enabling/disabling these settings, see Enable/Disable RPM Package Settings.
  - **Improvement to the Vendor Folder for the Private Go Registry and the Go Proxy**
    Checksums in the private Go registry and the Go proxy are now aligned for the Go version 1.24 vendor folder.
  - **NuGet Package Updates**
    - **Curation Support for NuGet Virtual Repositories**
      Extended JFrog Curation capabilities to support NuGet virtual repositories, providing a powerful, centralized way to secure your NuGet package consumption.
    - **NuGet Package - Now Supports .NET CLI**
      NuGet packages now include support for the .NET CLI.
    - **Optimized NuGet Version**
      Tightened validation to require all NuGet packages to use strict Semantic Versioning (SemVer 2.0). See specification.
    - **Nuget Packages - Rate Limit**
      Introduced a new rate-limiting mechanism for search APIs to prevent excessive calls and ensure service stability.
  - **Upgraded Gradle Set Me Up Wizard**

The Gradle Set Me Up wizard has been upgraded to support Gradle 9.

- **Improvement in VCS Remote Repositories**
  The GitHub Server option for Git providers was added for VCS remote repositories. For more information, see Create a VCS Repository.
- **Added Enforcement of Custom Configurations for Certain Remote Docker Repositories**
  When creating a remote Docker repository for an Azure Container Registry (*.azurecr.io) or a Microsoft Container Registry (https://mcr.microsoft.com/), Artifactory makes the following default configuration:
  - **Disable URL Normalization = true**

  When creating a remote Docker repository for a Chainguard Registry (http://cgr.dev/chainguard), Artifactory makes the following default configuration:
  - **Block Mismatching Mime Types = true**

  These default configurations are set upon remote repository creation and can be canceled afterwards. For more information, see Other Advanced Settings for Remote Repositories.
- **Improved npm Search**
  It is now possible to search for up to three search terms in npm local repositories when using the "npm search" command.
- **Enhanced Support for npm Audit**
  In addition to npm virtual repositories, npm Audit is now also enabled by default on npm remote repositories that support npm Audit directly. For more information, see Use npm Audit.
- **Improved Resolving of Subgroups When Accessing Subgroups in Gitlab with Go Remote Repositories**
  When accessing subgroups in GitLab with Go remote repositories (by selecting the Resolve Subgroups checkbox, as explained here), Artifactory now resolves the correct dependency version even if the URL contents contain both subgroups and submodules.
- **New Setting Added to Complete a List Manifest Image Overwrite**
  A new setting has been added under Package Settings called **Complete list manifest image overwrite**. When this setting is enabled, overwriting a list manifest image will asynchronously overwrite all of its sub-manifests.

- **Release Lifecycle Management**
  - **Expanded support for distributing and exporting Release Bundle v2 versions**
    To make distributing and exporting Release Bundle v2 versions easier, you can now use JFrog Distribution with Release Bundle v2 versions signed with the default key in Artifactory. To support this change, the default key type has been changed from RSA to GPG, and the name of the default key has been changed to **default-lifecycle-key**. For more information, see Create Signing Keys for Release Bundles (v2).
  - **Improved visibility for nested Release Bundles**
    The Release Bundle v2 content graph now provides a clear, visual representation of nested Release Bundles. Seeing the complete hierarchy enables you to understand how the Release Bundle is constructed, even when it contains other Release Bundles. For more information, see View Release Bundle v2 Evidence.
  - **Improved aggregated Release Bundle creation**
    Artifactory has improved its handling of aggregated Release Bundles (meaning, a Release Bundle v2 version that is comprised of other Release Bundle versions). If the Release Bundle version you are trying to create contains multiple Release Bundles with the same artifact but different metadata (evidence or properties), Artifactory will create the version successfully using the newer version of the artifact.
  - **Change of status code when creating Release Bundle v2 from build with missing artifact**
    To improve reporting accuracy, errors caused by missing artifacts during Release Bundle v2 creation will be returned as a 422 error (SC_UNPROCESSABLE_ENTITY) rather than a different status code that triggered unnecessary monitoring alerts. The 422 status code represents the event more accurately as it is the expected behavior when an artifact cannot be found.
  - **Performance Improvement in Release Bundle v2 Promotion Flow**
    The performance of the promotion flow for Release Bundle v2 versions has been improved.
  - **Source environment included in Release Bundle v2 promotion GET API results**
    The Get Release Bundle v2 Promotions API and Get Release Bundle v2 Version Promotions API now include the source environment in their responses. This enables you to see at a glance the name of the environment from which the Release Bundle version was promoted.
  - **Redesigned presentation of Release Bundle v2 contents**

The Content tab for Release Bundle v2 versions has been redesigned to show each package and standalone artifact included in the version (known as "releasables") and their source (for example, a build or a different Release Bundle). For more information, see View the Contents of a Release Bundle v2 Version.

- **Release Bundle v2 versions now associated with stages and lifecycles**
  This version replaces environments with the concept of stages and lifecycles, to provide users with more flexibility and control over their SDLC. Administrators can create global and project stages as needed and assign them to different SDLC categories, such as Code and Promote. The administrator then adds selected stages to the lifecycle to represent the progression of release candidates through your SDLC. For more information, see Stages & Lifecycle.

- **Support for webhooks for project-related Release Bundles**
  Artifactory now supports the creation of webhooks for Release Bundle v2 versions associated with specific projects. This enables you to receive notifications whenever a Release Bundle in a particular project is uploaded, promoted, or deleted. To create a Release Bundle webhook for a specific project, you must be working within the scope of the project (as opposed to All Projects).
  For guidelines about creating a Release Bundle v2 webhook for a specific project, see Domain: Release Bundle v2.

- **Created-by information provided for Sigstore evidence**
  To improve understanding and traceability, the API response when creating and deploying Sigstore evidence now includes the username associated with the JFrog token instead of 'internal'.

- **More accurate error messages during Release Bundle promotion**
  To improve user understanding, validation errors during the Release Bundle v2 promotion process will now return a BAD REQUEST error message (HTTP 400) rather than a generic HTTP 500 error.

- **Release Bundle v2 auto-creation feature removed**
  The Release Bundle v2 auto-creation feature, which was introduced to help customers transition from build promotion to the expanded feature set offered by Release Lifecycle Management, has been removed from the platform UI after having served its purpose.

- **Viewing Release Bundles distributed to Edge nodes**
  To align the platform UI with the REST API, only admin users are permitted to view distributed Release Bundle versions (v1 and v2) in the **Received** tab on Edge nodes. For more information, see View Release Bundles on Edge Nodes.

- Cleanup and Retention Policies

  - **Adding days/weeks selection for Time-based Policy Condition - Cleanup Release Bundle V2**
    Enhanced RB V2 cleanup functionality with the addition of **days/weeks** selection for policy condition. You can now configure cleanup conditions, specifying **days/weeks** for the RB V2. For more information, see Create Cleanup Policy - Release Bundle V2.

  - **Retention Policies - Cleanup & Smart Archiving**
    The **Stop All Runs** action is now restricted to Platform Admins only. Project Admins no longer have access to this action.

  - **Run Cleanup policies and Garbage Collection (GC) Simultaneously**
    Enabled cleanup policies to run more reliably by making them health-aware. Jobs will now run concurrently with other tasks only if the system is `HEALTHY` and will automatically stop if load increases, ensuring system stability.
    This can be toggled by the system property: `artifactory.retention.system.health.aware.job.enabled`

- Artifact Management

  - **Improved Artifact Lifecycle Management**
    Artifactory now updates the creation timestamp of an artifact when it is copied or moved to a new repository to the current date and time of the operation. Previously, the original creation timestamp was retained when moving or copying an artifact to another repository, which led to incorrect assumptions about the artifact's age and relevance in the new location. The "last modified" timestamp remains unchanged to preserve the integrity of the artifact's last update. This enhancement helps in the effective adoption of cleanup policies and aligns with industry standards. To ensure backward compatibility, this feature is implemented behind a feature flag and is disabled by default.

  - **New Metadata Properties Added to the manifest.json**
    Metadata properties for the operating system and the operating system architecture will now be added to the **manifest.json** after pushing or caching a new image. These new properties are set in **docker.os** and

docker.architecture, respectively.

- **Prevent accidental removal of referenced sub-architectures in multi-arch images**
  Starting from this Artifactory version, when deleting a multi-architecture image, any sub-architecture variant that is still referenced by another image will be preserved.
- **Context retention in Artifacts browser**
  When you copy or move artifacts in the Artifacts browser, the UI no longer moves automatically to the destination path of the operation but remains in its original context. To move to the destination path after the copy or move operation is complete, click the **Go to path** link in the confirmation message.
- **UI Support for Debian Source Package Search**
  Added support for **Debian Source** package search.

- Caching
  - **Improved Change Artifacts count UI widget caching mechanism**
    Improvements were made to the Change Artifacts count UI widget caching mechanism.
  - **Daily Cleanup Job Added for Cache FS _pre folder**
    A daily job is now triggered on startup to cleanup old `dbRecord*.bin` files in the cache provider's `_pre` folder. The configurations for this job can be modified in the **binarystore.xml** file under the cache-fs provider.
- Platform UI
  - **Redesigned platform UI for Release Lifecycle Management**
    The platform UI for Release Lifecycle Management has been redesigned to provide a clearer, more consolidated view of your Release Bundles. The new design centralizes all critical information for each Release Bundle version, including its timeline, contents, security scans, evidence, and properties, in an accessible and intuitive interface. For more information, see Release Lifecycle Management.
  - **Improved visibility of OCI/Docker multi-arch images in the platform UI**
    To reduce visual clutter and improve comprehension, Artifactory now makes it easier to manage OCI/Docker multi-arch images in the platform UI. For example, if you have a multi-arch image called **my-image:1.0.0** that supports amd64 and arm64 architectures, Artifactory contains 3 distinct package versions, one for the manifest list and one for each architecture:
    - my-image:1.0.0
    - my-image:sha256__f2ca1bb6c7....
    - my-image:sha256__1a8a5828e8....

    Artifactory now displays the version for the manifest list only in the platform UI and suppresses the individual architecture versions (named according to their image tags). This enables you to focus on the multi-arch image as a single entity. Please note that all package versions will be returned when listing the content via the REST APIs.
  - **Platform UI support for displaying larger evidence files**
    The platform UI can now display evidence files up to a maximum size of 3000 lines (compared to 1500 lines in previous versions). Larger evidence files can be downloaded with a single click. For more information, see View Evidence.
  - **Support for Easy Copying of Administration Values**
    The JFrog Platform WebUI now supports a **Copy** button, allowing you to copy values in the Administration module pages with a single click.
    The following values will now be easily copiable:
    - Token ID under Access Tokens
    - Name under Projects, Users, Groups, Permissions, Project Members, Webhooks, and Manage Integrations
    - Auth URL under OAuthSSO
    - URL under Webhooks
    - Group Name under Crowd/ Jira
    - Provider URL under Manage Integrations
    - Project Key under Projects
- Platform Configuration

- **Support for Updating the Access Bootstrap YAML File**
  The JFrog Platform now supports making changes to the access.security.bootstrap.yml file without creating a new configuration or modifying the existing Artifactory YAML file. For more information, see Access Bootstrap YAML File.
- **Improved Configuration Descriptor Validation**
  Configuration descriptor validation was improved to increase system stability.
- **Traefik Version Upgrade**
  The Traefik version embedded in the Router microservice was upgraded from v2 to v3. This should not impact operation. Though if you your deployment depends on specific functionality, review their upgrade notes

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-58782	Archiving/Cold Storage	Medium	Fixed an issue whereby a project admin could not successfully call the **Get all Package Cleanup Policies API** and received a 403 error.
RTDEV-58791	Archiving/Cold Storage	High	Fixed an issue with failed upgrades from Artifactory versions earlier than 7.97 to version 7.97 or later when using a non-enterprise MSSQL license.
RTDEV-61500	Archiving/Cold Storage	Medium	Fixed an issue whereby a cleanup policy would stop running when encountering certain directories.
RTDEV-61647	Archiving/Cold Storage	Medium	Fixed an issue whereby inconsistent naming and compression format for artifactory-cleanup-audit logs caused sync failures and misclassification of logs.
RTDEV-61687	Archiving/Cold Storage	Low	Fixed an issue whereby the Next Run section for Retention Policies (both Cleanup and Archive) sometimes did not update correctly.
JA-17727	Authentication Providers	Low	Fixed an issue where authentication attempts with invalid tokens caused temporary login suspension. Only basic credentials authentication attempts should count toward login suspension.
JA-17902	Authentication Providers	Medium	Fixed an issue whereby a SCIM PATCH request succeeded despite containing an invalid operation.
RTDEV-58433	Builds	Medium	Fixed an issue whereby artifacts with different names but the same checksums showed the wrong repository path in the build browser.
RTDEV-62157	Federated Repositories	High	Fixed an issue that caused the Federation to fail if a proxy was defined at the platform level but the Federated repository was set to `no_proxy`.
RTFE-3634	Federated Repositories	Low	Fixed an issue whereby when converting a local repository to a federated repository, a warning message appeared that “This operation cannot be undone” even though the federated repository can be reverted back to a local repository.

JIRA Issue	Component	Severity	Description
EVT-1706	General	Medium	Fixed an issue whereby a webhook would fail if any of the repositories it was configured to listen to were deleted from the system.
JA-17841	General	Medium	Fixed an issue whereby include/exclude patterns in the Per Repository tab incorrectly displayed the default value '******' when navigating between the All Repositories and Per Repository tabs in the Permission Target UI.
JA-17899	General	Medium	Fixed an issue whereby Access was throwing errors during startup.
JFUI-18900	General	Medium	Fixed an issue whereby a custom message enabled in the UI would cause the "The Federated repository settings are not synchronized between these repositories" notification to negatively impact the user experience by expanding and blocking other elements.
JFUI-18972	General	Medium	Fixed an issue where setting up log rotation for frontend metrics logs in Artifactory's **system.yaml** file didn't work, as the logs did not rotate after a service restart.
JFUI-18973	General	Medium	Fixed an issue whereby the **Show offline node** checkbox under **Administration > Monitoring > Service Status** was not working and preventing users from viewing offline nodes in an HA cluster.
RTDEV-55886	General	Medium	Fixed an issue whereby when sending a request to **ui/api/v1/ui/artifactactions/view** with an empty path, the API returned a 500 error and this led to the disclosure of Java exceptions that described some of the application internals.
RTDEV-57769	General	Medium	Fixed an issue whereby flat copy returned a 409 status code for almost any error.
RTDEV-59666	General	Low	Fixed an issue whereby when setting up Apache as a reverse proxy for Artifactory, the default configuration that was generated from the Artifactory UI did not forward the original user IP address.
RTDEV-60768	General	Medium	Fixed an issue whereby when configuring Artifactory to work with a MySQL database, an unnecessary warning message was received indicating that "No NativeDbLocksService implementation bean exists for DB type".

JIRA Issue	Component	Severity	Description
RTDEV-61179	General	Medium	Fixed an issue whereby Support Bundle status in the UI was reported as **FAILURE** despite successful Support Bundle generation.
RTDEV-62074	General	Medium	Fixed an issue where redundant errors were logged.
RTDEV-62472	General	High	Fixed an issue where a policy for cleaning up unused cached artifacts failed to cleanup any files.
RTDEV-62683	General	Medium	Fixed an issue whereby it was not possible to display HTML contents of a zip file if the zip file name contained the German umlaut character (for example, **ä**).
RTDEV-62928	General	Medium	Fixed an issue whereby Artifactory would fail to start with a partial GPG key configuration.
RTDEV-63693	General	Low	Fixed an issue whereby inconsistent token validation behavior was observed when calling the system/version API with anonymous access enabled.
RTDEV-63869	General	Medium	Fixed an issue whereby a virtual RPM repository was unable to merge metadata when it contained an upstream remote RPM repository with Zstandard compression index files and a local repository containing RPM packages.
RTDEV-60865	General	Medium	Fixed an issue whereby when Artifactory attempted to authenticate a remote Sonatype Nexus repository using Basic Authentication, the request failed with a 401 Unauthorized error if the username contained non-ASCII characters.
INST-11808	Installation	Medium	Fixed an issue where setting a custom `shared.database.url` for embedded DerbyDB in system.yaml led to inconsistent configurations, causing startup failures. To prevent this, a new validation now runs during Artifactory startup, ensuring that if a custom Derby database URL is specified for `shared`, custom URLs must also be provided for all database-connected services (access, topology, jfconfig). This maintains uniform Derby database configuration across the platform.
RTDEV-56935	Packages	Medium	Fixed an issue whereby after saving an NIM remote repository configuration, the test connection failed.
RTDEV-58806	Packages	Medium	Fixed an issue whereby the removal of a child repository from an RPM virtual repository did not trigger metadata calculation.

JIRA Issue	Component	Severity	Description
RTDEV-59071	Packages	Medium	Fixed an issue where an external user could obtain an API key instead of an Identity Token in the Maven Set Me Up tool.
RTDEV-60193	Packages	Critical	Fixed an issue whereby the Go module download process encountered a failure when the MCRP limit was reached, which resulted in an unsuccessful request to the remote resource, and attempts to serve from the cache also failed.
RTDEV-60343	Packages	Medium	Fixed an issue whereby Conan federation did not sync all package properties.
RTDEV-60689	Packages	Medium	Fixed an issue where Artifactory was not honoring include/exclude patterns on a Go remote GitHub repository for **.info** artifacts.
RTDEV-61861	Packages	Critical	Fixed an issue whereby cleanup policies were incorrectly deleting Helm packages with the same prefix name.
RTDEV-62449	Packages	Medium	Fixed an issue whereby passing the **X-JFrog-Override-Base-URL** header during the npm install process from a virtual repository was not always respected.
RTDEV-62985	Packages	Medium	Fixed an issue whereby when deploying a **.pom** file for Maven or Gradle repository types that start with an empty line or used UTF-8 non-breaking spaces in an XML structure, a 409 error was encountered.
RTDEV-64039	Packages	Low	Fixed an issue whereby an incorrect icon for Docker images was displayed in Docker virtual repositories.
RTFE-3459	Packages	Medium	Fixed an issue whereby the setting **Enable Token Authentication** was always checked (set TRUE) for a Helm OCI remote repository and a Docker remote repository, even if the actual value for this setting was false.
RTFE-3636	Packages	Medium	Fixed an issue whereby the Set Me Up repositories list was not showing an empty virtual Maven repository.
RTDEV-59252	Packages	Medium	Fixed an issue whereby the Artifactory Cloud platform did not update the `<latest>` tag in **maven-metadata.xml** upon deployment.
RTDEV-61184	Packages	Medium	Fixed an issue whereby Artifactory was not able to cache the the **drupal/nouislider_js** module and other modules from **git.drupalcode.org**.

JIRA Issue	Component	Severity	Description
RTFE-3603	Projects	Medium	Fixed an issue whereby the "Read Only" check box was not saved when sharing a repository with a project.
RTDEV-39704	Release Lifecycle Management	Medium	Fixed an issue that caused builds to be deleted during build promotion if the customer's storage quota exceeded the configured limit. The status change operation in the build promotion process will now fail if the storage quota has been reached.
RTDEV-57821	Release Lifecycle Management	Medium	Fixed an issue whereby attempts to delete, move, or overwrite a promoted artifact returned a 403 error code (Forbidden). These actions will now return a 409 error code (Conflict).
RTDEV-58946	Release Lifecycle Management	Medium	Fixed an issue where creating a Release Bundle would incorrectly discard duplicate artifacts from different modules. If a build contained the same artifact in multiple paths, only one copy was kept. The process now correctly includes all instances of the artifact, preserving each one in the final Release Bundle.
RTDEV-59525	Release Lifecycle Management	Medium	Fixed an issue whereby creating a Release Bundle with a non-existent project key returned a 500 error. It now returns a 400 error.
RTDEV-59712	Release Lifecycle Management	Medium	Fixed an issue whereby the same event displayed different timestamps in the kanban view and in the timeline.
RTDEV-61209	Release Lifecycle Management	High	Fixed an issue whereby the Get Release Bundle v2 Versions in a Specific Environment API would return data that did not reflect the version's current environment.
RTDEV-61309	Release Lifecycle Management	Critical	Fixed an issue whereby Artifactory was unable to collect all the multi-arch Docker images from a remote cache repository.
RTDEV-61351	Release Lifecycle Management	Medium	Fixed an issue whereby creating a Release Bundle containing two builds with different tags but identical content resulted in the inclusion of just one build.
RTDEV-61511	Release Lifecycle Management	Medium	Fixed an issue whereby promotion to a specific repository would fail due to a race condition caused by the creation of an unrelated repository in the same environment.
RTDEV-61672	Release Lifecycle Management	Medium	Fixed an issue whereby publishing build-info with an empty statuses section caused a 500 error.

JIRA Issue	Component	Severity	Description
RTDEV-62012	Release Lifecycle Management	Medium	Fixed the checksum calculation for Release Bundle (RBv2) by adding an explicit ORDER BY clause.
RTDEV-64239	Release Lifecycle Management	High	Fixed an issue that affected the build promotions process. Previously, when multiple dependencies had the same SHA, only one file would be promoted and the rest would be ignored. Now all dependencies are promoted, even if the files have the same SHA.
RTDEV-64552	Release Lifecycle Management	High	Fixed an issue whereby build dependencies were extracted during Release Bundle v2 creation even when the `include_dependencies` option was set to `false`.
RTDEV-61991	Release Lifecycle Managment	Medium	Fixed an issue whereby, when viewing a build's dependencies within an Artifactory project and selecting Show in Tree for a dependency, the UI redirected to a repository that was not included in the project.
RTDEV-57244	Repositories	Medium	Fixed an issue whereby attempting to create a remote repository with an encrypted password from another Artifactory instance failed with a 500 BadPaddingException.
RTDEV-57737	Repositories	High	Fixed an issue whereby: • When attempting to delete a repository, an unfound artifact caused the deletion to fail. • When attempting to delete a bulk of repositories, an unfound repository caused the deletion to fail.
RTDEV-57893	Repositories	Medium	Fixed an issue whereby artifacts failed to appear in the UI browser after defining an include pattern on the virtual repository.
RTDEV-58624	Repositories	Medium	Fixed an issue whereby the following APIs were accessible to admins only: • Delete Item From Trash Can API • Restore Item from Trash Can API Now, after the fix, these APIs can be accessed by non-admins with the appropriate permissions.
RTDEV-60496	Repositories	High	Fixed an issue whereby the **.jfrog** system folder could not be deleted from local repositories or remote caches.
RTDEV-61165	Repositories	Medium	Fixed an issue whereby the Get All Repository Configurations API API, in certain cases, returned an empty response when using the JSON accept header.

JIRA Issue	Component	Severity	Description
RTDEV-62248	Repositories	Low	Fixed an issue whereby the file-list API would return a 404 error for nested virtual repositories when setting the parameter **?list&deep=1**.
RTDEV-64189	Repositories	Medium	Fixed an issue whereby it was not possible to enable the **List Remote Artifacts** checkbox for Conda smart remote repositories.
RTFE-3619	Repositories	Low	Fixed an issue whereby pressing the Delete button to delete a repository multiple times caused multiple popups.
RTDEV-59159	Repositories	Low	Fixed an issue whereby attempts to test the connection to a remote repository using token authentication fail.
RTDEV-61737	Storage	Low	Fixed an issue whereby stale file descriptors remain from temporary files created when uploading binary with Azure Binary Provider.
JA-18101	User Interface	Medium	Fixed an issue related to the OIDC integration configuration in the JFrog Platform WebUI whereby, when reopening the Identity Mapping configuration following initial setup and saving it again without making any changes, group names containing spaces were not displayed as expected.
RTDEV-60864	User Interface	Medium	Fixed an issue whereby the Artifactory native UI did not display the contents of a VCS remote repository when an include pattern was set.
RTDEV-62995	User Interface	Low	Fixed an issue whereby in the Monitoring Storage UI, there was an unexpected appearance of the ` character.
RTDEV-62997	User Interface	Low	Fixed an issue in the Storage Monitoring UI, whereby when clicking the sort icon in the Percentage column to display the results in ascending order, the results were displayed in descending order (and vice versa).
RTFE-3332	User Interface	Medium	Fixed an issue whereby the Artifactory UI displayed an option to delete properties from virtual repositories, even though it is not possible to delete these properties.
RTFE-3546	User Interface	High	Fixed an issue whereby the warning " `<previous artifact from previous project>` could not be found" was incorrectly appearing in the UI when switching projects.
RTFE-3639	User Interface	Medium	Fixed an issue whereby when navigating to a Storage project in the UI, the Package Type for **npm** appeared

JIRA Issue	Component	Severity	Description
			as “N/A” instead of displaying **npm**.
JA-18037	User Management	High	Fixed an issue whereby clicking **Unlock** on the Edit Profile page was throwing a 403 Forbidden error.
WKS-1799	Workers	Medium	Fixed an issue in the Workers Page in the JFrog Platform WebUI whereby, when creating or editing an event-driven Worker, selecting a timezone, and saving the configuration, the timezone was not saved as expected.

Artifactory 7.117

This section includes all the Artifactory 7.117 releases.

Critical Security Notice

All subversions are vulnerable to multiple non-critical security vulnerabilities that, in some deployments, can be chained into critical-severity attacks. We recommend that all customers upgrade to the latest version. View the latest Self-Managed and SaaS releases.

Artifactory 7.117.29 Self-Managed

Released: 7 Sept 2026

This version includes security-driven configuration changes for plugin deployment.

Artifactory 7.117.28 Self-Managed

Released: 28 Aug 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-82329	General	Critical	Potential authentication bypass leading to administrative access in Artifactory

Artifactory 7.117.27 Self-Managed

Released: 18 August 2026

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-42018	General	High	Anonymous token exposure in JFrog Artifactory

Artifactory 7.117.25 Self-Managed

Released: 27 July 2026

Security Notice

This version is designed to fix multiple security vulnerabilities that, when chained together, could result in a critical attack scenario if Anonymous Access is enabled. Anonymous Access is disabled by default and is not recommended for production environments due to the additional security risks it introduces.

CVE	Component	Severity	Fix Description
CVE-2026-65617	Packages	High	Designed to prevent unsafe Gems package deserialization that could lead to remote code execution
CVE-2026-65925	Packages	Medium	Designed to validate Cargo sparse index URLs to prevent server-side request forgery
CVE-2026-65921	Builds	High	Designed to prevent build artifact archive paths writing outside intended locations
CVE-2026-65922	General	High	Designed to block unauthorized writes to restricted internal metadata storage locations
CVE-2026-65923	Builds	Medium	Designed to validate Ansible provider URLs to prevent server-side request forgery
CVE-2026-66014	General	High	Designed to prevent HA authentication fail-open behavior causing privilege escalation
CVE-2026-65924	Packages	Medium	Designed to validate Terraform external provider URLs to prevent server-side request forgery

Artifactory 7.117.23 Self-Managed

Released: 15 July 2026

Resolved Issues

Jira Issue	Component	Severity	Description
RTFS-4094	Federated Repositories	Critical	Fixed a broken authorization service that could permit low-privileged users to read configuration data.

Jira Issue	Component	Severity	Description
RTDEV-92146	Packages	Critical	Fixed a vulnerability in which weakly validated, request-derived data could be used to poison cached responses.

Artifactory 7.117.22 Self-Managed

Released: 29 June 2026

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-90399	General	Critical	A high-severity vulnerability was fixed in Artifactory. In certain cases, deprecated services could allow a low-privileged user to retrieve artifacts from repositories they were not authorized to access. JFrog recommends that all self-managed customers upgrade to a fixed version as soon as possible, especially those with anonymous user access enabled.

Artifactory 7.117.21 Self-Managed

Released: 28 April 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-69107	General	Medium	Potential unauthorized artifact access in JFrog Artifactory

Artifactory 7.117.19 Self-Managed

Released: 23 October 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-63859	General	Medium	Fixed an issue whereby a virtual RPM repository was unable to merge metadata when it contained an upstream remote RPM repository with Zstandard compression index files and a local repository containing RPM packages.

JIRA Issue	Component	Severity	Description
RTDEV-62683	General	Medium	Fixed an issue whereby it was not possible to display HTML contents of a zip file if the zip file name contained the German umlaut character (for example, ä).
JFUI-18972	General	Medium	Fixed an issue whereby the Go Mod download process encounters a failure when the MCRP limit is reached, resulting in an unsuccessful request to the remote resource and the attempts to serve from the cache also fail.

Artifactory 7.117.18 Self-Managed

Released: 7 October 2025

Feature Enhancements

- **Maintenance Release**
  Released a fix for CVE-2025-41249. For more information see Artifactory Fixed Security Vulnerabilities.

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-17875	User Management	High	Fixed an issue with the Projects user REST API, where a project admin received a 403 error when attempting to retrieve project user details.

Artifactory 7.117.17 Self-Managed

Released: 24 September 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
TOPO-627	User Interface (UI)	Medium	Fixed an issue related to the Service Status page in the JFrog Platform WebUI did not display the Uptime value for the Topology service.
RTDEV-61792	General	Medium	Fixed an issue whereby the OCI referrers.json file was not updated after the distribution of an already existing image.
RTDEV-63240	Packages	Medium	Fixed an issue whereby, copying or moving a Debian package to a path where a package with the same filename but a different checksum already existed caused metadata duplication.

Artifactory 7.117.16 Self-Managed

Released: 16 September 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-62097	Packages	Medium	Fixed an issue whereby a 404 error was received from a request for a package that used a "If-None-Match" header.
RTDEV-61672	Release Lifecycle Management	Medium	Fixed an issue whereby publishing build-info with an empty statuses section caused a 500 error.
RTDEV-61647	Archiving/Cold Storage	Medium	Fixed an issue whereby inconsistent naming and compression format for artifactory-cleanup-audit logs caused sync failures and misclassification of logs.
RTDEV-61500	Archiving/Cold Storage	Medium	Fixed an issue whereby a cleanup policy would stop running when encountering certain directories.
JA-18037	User management	High	Fixed an issue whereby clicking Unlock on the Edit Profile page was throwing a 403 Forbidden error.
INST-12162	Installation	Medium	Fixed an issue where the readOnlyRootFilesystem breaks the functionality of the /app directory.

Artifactory 7.117.15 Self-Managed

Released: 2 September 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
EVT-1706	General	Medium	Fixed an issue whereby a webhook would fail if any of the repositories it was configured to listen to were deleted from the system.
RTDEV-60865	General	Medium	Fixed an issue whereby when Artifactory attempted to authenticate a remote Sonatype Nexus repository using Basic Authentication, the request failed with a 401 Unauthorized error if the username contained non-ASCII characters.
RTDEV-61861	Packages	Critical	Fixed an issue whereby cleanup policies were incorrectly deleting Helm packages with the same prefix name.
RTDEV-56935	Packages	Medium	Fixed an issue whereby after saving an NIM remote repository configuration, the test connection failed.

JIRA Issue	Component	Severity	Description
RTDEV-61184	Packages	Medium	Fixed an issue whereby Artifactory was not able to cache the the drupal/nouislider_js module and other modules from git.drupalcode.org.
RTDEV-62449	Packages	Medium	Fixed an issue whereby passing the X-JFrog-Override-Base-URL header during npm install process from a virtual repository might not be respected.
RTDEV-61165	Repositories	Medium	Fixed an issue whereby the Get All Repository Configurations API, in certain cases, returned an empty response when using the JSON accept header.
RTDEV-61643	Storage	Medium	Improvements were made in thread synchronization in sharding and s3-sharding providers.
RTDEV-62157	Federated Repositories	High	Fixed an issue that caused the Federation to fail if a proxy was defined at the platform level but the Federated repository was set to `no_proxy`.

Artifactory 7.117.14 Self-Managed

Released: 19 August 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RPG-1841	General	Critical	Fixed an issue whereby upgrading existing Artifactory HA installations may fail due to the Router service not starting.
JFUI-18900	General	Medium	Fixed an issue whereby a custom message enabled in the UI would cause the "The Federated repository settings are not synchronized between these repositories" notification to negatively impact the user experience by expanding and blocking other elements.
INST-12162	Installation	Medium	Fixed an issue whereby the `readOnlyRootFilesystem` was breaking the functionality of the `/app` directory.
RTDEV-59071	Packages	Medium	Fixed a bug whereby an external user can get an API key instead of an Identity token in Maven SetMeUp tool.
RTDEV-61351	Release Lifecycle Management	Medium	Fixed an issue whereby adding two content-identical images with different tags to a release bundle would result in one of the images being dropped.

JIRA Issue	Component	Severity	Description
RTDEV-59159	Repositories	Low	Fixed an issue whereby attempts to test the connection to a remote repository using token authentication fail.
RTDEV-57893	User Interface (UI)	Medium	Fixed an issue whereby artifacts failed to appear in the UI browser after defining an include pattern on the virtual repository.

Artifactory 7.117.12 Self-Managed

Released: 5 August 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-58782	Archiving/Cold Storage	Medium	Fixed an issue whereby a project admin could not successfully call the Get all Package Cleanup Policies API and received a 403 error.
RTDEV-60343	Packages	Medium	Fixed an issue whereby Conan federation did not sync all package properties.

Artifactory 7.117.10 Self-Managed

Released: 31 July 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-17875	User Management	High	Fixed an issue with the Projects user REST API, where a project admin received a 403 error when attempting to retrieve project user details.

Artifactory. 7.117.8 Self-Managed

Released: 19 July 2025

Known Issue in this Version

During startup and regular operation, the Artifactory Frontend service attempts to download resources from the public internet endpoint https://grpc.qwak.ai. Therefore, JFrog recommends avoiding the upgrade to this version if your organization's environment restricts access to this endpoint. For more information, see Artifactory Known Issues.

Resolved Issues

JIRA Issue	Component	Severity	Description
JFMC-6021	General	High	Fixed an issue caused by CVE-2025-53506.

Artifactory 7.117.7 Self-Managed

Released: 25 July 2025

Known Issue in this Version

During startup and regular operation, the Artifactory Frontend service attempts to download resources from the public internet endpoint https://grpc.qwak.ai. Therefore, JFrog recommends avoiding the upgrade to this version if your organization's environment restricts access to this endpoint. For more information, see Artifactory Known Issues.

JIRA Issue	Component	Severity	Description
JA-17727	Authentication Providers	Low	Fixed an issue whereby authenticate attempts using invalid tokens caused temporary login suspension. Only basic credentials authentication attempts should count towards login suspension.
RPG-1831	General	High	Fixed an issue whereby upgrading existing Artifactory installations with Router TLS enabled may fail due to the Router service not starting.

Artifactory 7.117.5 Self-Managed

Released: 24 July 2025

New Features

Known Issues in this Version

- During startup and regular operation, the Artifactory Frontend service attempts to download resources from the public internet endpoint `https://grpc.qwak.ai` .Therefore, JFrog recommends avoiding the upgrade to this version if your organization's environment restricts access to this endpoint. For more information, see Artifactory Known Issues.
- When upgrading existing Artifactory installations that have Router TLS enabled (`router.tlsEnabled: true`) in the `system.yaml` file, a common issue has been identified. The upgrade process might fail because the Router service fails to start, displaying the following error: *Error during the build of the default TLS configuration: unknown TLS options: default*. For more information, see Artifactory Known Issues.

Breaking Change for Access REST APIs

From this version, Access REST API responses will be returned as compact JSON and not as pretty-printed JSON. Note that some automatic parsers that rely on the formatting will require an update.

- **New REST API: Get Projects List for a Global Role**
  The JFrog Platform now supports getting a paginated list of projects where a specific global role is used. For more information, see Get Project List for a Global Role API.

Feature Enhancements

- **RTFS Breaking Change**
  The version of the Artifactory Federation Service (RTFS) that comes with this Artifactory release changes the context path from **/artifactory/service/rtfs** to `/rtfs`. This is a breaking change for users who have multiple sites (JPDs) using RTFS. (Users who run RTFS on only one site, and sites that use the legacy Federation service, are unaffected by this change.)
  Users in Self-Managed environments who have sites running an older version of RTFS should upgrade them to the new version of RTFS as soon as possible to accommodate the new context path. As an interim solution, a set of commands can be added as a workaround to bridge the context path differences between sites using the new version of RTFS and sites using an older version, as described below.
  Nginx Configuration
  Add this command to the Nginx configuration of a site using the **new** version of RTFS:

```
location /artifactory/ {
    if ($request_uri ~ ^/artifactory/service/rtfs/(.*) $ ) {
      proxy_pass       http://router/rtfs/$1;
      break;
    }
    if ( $request_uri ~ ^/artifactory/(.*) $ ) {
      proxy_pass       http://artifactory/artifactory/$1;
    }
    proxy_pass         http://artifactory/artifactory/;
  }
```

  This command instructs Nginx to redirect requests from sites that use the old RTFS context path to the new context path.
  Add this command to the Nginx configuration of a site using the **old** version of RTFS:

```
location /rtfs/ {
  if ($request_uri ~ ^/rtfs/(.*) $ ) {
      proxy_pass       http://router/artifactory/service/rtfs/$1;
      break;
    }
```

  This command instructs Nginx to redirect requests from sites that use the new RTFS context path to the old context path.
  Apache Configuration
  Use the following Apache rewrite rule to redirect requests between sites that have a mix of old and new context paths:

```
RewriteRule "^/artifactory/service/rtfs/(.*) $"
"balancer://artifactory/artifactory/service/rtfs/$1" [P,L]
```

  Important Migration Note
  When migrating from the legacy Federation service to RTFS, be sure to use **version 2.0** of the CLI, which implements the new context path.

Release Bundles

- **Create Release Bundle v2 version from multiple sources**
  You can now create a Release Bundle v2 version from multiple sources, for example, a combination of artifacts, builds, and existing Release Bundles. For more information, see Create Release Bundle v2 Version.
- **Create a Release Bundle v2 version from packages**
  You can now create a Release Bundle v2 version by defining one or more packages to include in the Release Bundle. The Release Bundle can include packages of every type supported by Artifactory. For more information, see Create Release Bundle v2 Version.
- **Create a Release Bundle v2 version using items in remote-cache repositories**
  You can now create a Release Bundle v2 version that includes packages and artifacts located in remote-cache repositories. For more information about Release Bundle creation, see Create Release Bundle v2 Version.

- **SBOMs containing remote-cache dependencies**
  Release Bundle v2 versions created from **build-info** can now include build dependencies located in remote-cache repositories, provided you have used the option for including dependencies in the Release Bundle. If this option has not been used, the remote-cache dependencies will not be included in the Release Bundle, but the SBOM used by Xray will still contain metadata about those dependencies.

- **Release Bundle v2 – support for SBOMs with remote dependencies**
  Previously, Release Bundle v2 did not include information about dependencies from remote repositories, which prevented the generation of a complete SBOM (software bill of materials) by Xray. This limitation hoas now been removed, which means that information about these dependencies will be included in the SBOM, and Xray (version 3.121.7 and above) can scan them. Having a complete SBOM increases transparency and security by providing insight into all components involved in the Release Bundle, and helps with auditing and compliance.

> **Note**
>
> Although information about remote dependencies is included in the SBOM, the dependencies themselves are not included in the Release Bundle in the current version.

- **Source environment of Release Bundle v2 promotions**
  The source environment of a Release Bundle v2 promotion is now included in the API response, making it easier for users to identify the start and end points of the promotion. For more information about promotion, see **Promote Release Bundle v2 Version**.

- **Adding properties to Release Bundle v2 versions**
  You can now add **properties** and **property sets** to Release Bundle v2 versions. Properties are user-defined, key-value pairs that are added to the Release Bundle v2 version's manifest file. For more information, see **Add Properties to a Release Bundle v2 Version**.

- **New search and filtering options for Release Lifecycle Management kanban board**
  The Release Lifecycle Management kanban board now features options for searching through and filtering the displayed Release Bundle versions. These options make it easier for you to focus on the versions of greatest interest.

- **Release Bundle v2 promotion rollback**
  You can now use the **REST API** to roll back the latest promotion of a Release Bundle v2 version. Rollback deletes the contents of the latest promotion (including its artifacts, properties, and evidence) and restores the version to its previous environment, including the properties and evidence it contained when the version was first created. For more information, see **Promotion Rollback**.

- **Release Bundle v2 version supports plus sign character**
  You can now include a plus sign (+) when defining the version of a Release Bundle v2. This change was made to achieve alignment with the SemVer 2.0.0 specification. For more information, see **Create Release Bundle v2 Version**.

- **Assigning a tag when creating a Release Bundle v2 version**
  You can now assign a tag when creating a Release Bundle v2 version with the **REST API**. Use the tag to identify the version quickly. For example, you can create tags such as nightly-build, release-candidate, bugfix-2025-33124, and so on. The tag will appear on the card for the Release Bundle version on the Release Lifecycle stages board.

> **Note**
>
> You can continue using the **Assign Tag API** to tag existing Release Bundle versions.

- **Version counter on Release Lifecycle stages board**
  The Release Lifecycle stages board now includes a counter so that you can see at a glance how many versions of the selected Release Bundle currently exist.

- **Improved error codes during Release Bundle v2 creation**
  Artifactory will now return 404 when an artifact or package is missing from the defined artifact or package list during Release Bundle v2 creation. In addition, Artifactory will return 403 when an artifact or package is filtered out due to a user permissions issue.

- **Evidence provider logo displayed on stages board**

Each evidence item displayed on the Release Lifecycle stages board now includes a logo to indicate the provider of that evidence, whether it is evidence provided by the JFrog platform or evidence originating from other providers, such as GitHub or Sonar. The logo is also displayed prominently when the contents of the evidence item are opened.

- **Cleanup and Retention Policies**
- **Support for Composer Packages in Cleanup Policies and Smart Archiving**
  Cleanup Policies and Smart Archiving now support Composer package type.
- **Support for Chef and Puppet Packages in Cleanup Policies**
  Cleanup Policies now support Chef and Puppet package types.
- **Support for N versions in Retention Policies**
  Cleanup Policies and Smart Archiving now support N versions for Docker, OCI and Helm OCI. For more information, see Cleanup Supported Packages and Smart Archiving Supported Packages.
- **API Run Summary Reports for Cleanup and Smart Archiving**
  Added new API endpoints for cleanup and smart archiving that provide detailed run summary reports in JSON format. For more details, refer toView Package Cleanup Policy Run Summary Report API and View Smart Archiving Policy Run Summary Report API.
- **Smart Archiving Packages: Evidence**
  Added support for the archival of evidence associated with any packages. This enhancement ensures that relevant evidence is preserved as part of your archiving strategy, streamlining your package management process. For more information, refer to Smart Archiving.
- **Property-based Policy Condition - Smart Archiving Packages**
  Enhanced package-archivie functionality with the addition of a property-based policy condition. You can now include or exclude specific package versions from archive by applying a property-based policy condition. This allows for more granular control over which packages are retained or archived during archive actions. For more information, see Create Smart Archiving Policy.
- **Packages and Repositories**
- **Default Socket Timeout for Federated Repositories**
  The default socket timeout for Federated repositories has been changed to 300000 milliseconds (5 minutes). This value can be adjusted, if required, using an Artifactory system property. For more information, see Increase the Predefined Socket Timeout for Larger Repositories.
- **CocoaPods Smart Repositories**
  The **CocoaPods Settings** section has been removed from the smart repository creation page. Smart repositories automatically inherit configuration from their source repository, making manual settings unnecessary.
- **Cocoapods CDN Smart Repository Support**
  Added smart repositories support for CocoaPods CDN.
- **Improvement in Promoting Docker Images**
  Starting from this Artifactory version, when Docker image promotion overrides an existing image tag in the target repository, shared layers from other tags of the same image will not be deleted. In versions prior to 7.117.1, these shared layers may be deleted.
- **Support for Oracle 23c**
  Artifactory is now certified to work with the Oracle 23c database.
- **Improved Get Federation Sync State REST API performance**
  The performance of the REST API that returns the synchronization state of all Federated repositories in the JPD has been improved.

> **Note**
>
> This API endpoint is relevant for users operating the legacy Federation service, not the Artifactory Federation Service (RTFS).

- **JFrog Platform**
- **Removal and Backup of Mission Control Plugins**
  The following Mission Control plugins, which were created during the initial days specifically for Mission Control, are no longer required by any JFrog products. As a result, these plugins will be removed in this version

and backup files are created with a `.backup` extension.

- `internalUser.groovy`
- `ldapSettingsConfig.groovy`
- `ldapGroupsConfig.groovy`
- `haClusterDump.groovy`
- `repoLayoutsConfig.groovy`
- `proxiesConfig.groovy`
- `propertySetsConfig.groovy`
- `requestRouting.groovy`
- `httpSsoConfig.groovy`
- `pluginsConfig.groovy`

For more information, see User Plugins documentation.

- **Support for Reading Permissions Scoped Tokens**
  It is now possible for non-admin users to use the Get Projects List API, Get Project Users API, Get Repository Configuration API , HA License Information API , and Get Storage Summary Info API endpoints using a scoped token. For more information, see Create Scoped Token.
- **Secure Cloud Storage Credentials in Helm**
  We have introduced a new feature that allows you to supply cloud storage identity and credentials as a Kubernetes secret within your `values.yaml` file for Artifactory Helm deployments. This capability extends to: *AWS S3V3: Securely provide your AWS S3V3 access keys and secret keys.* Azure Blob Storage: Securely provide your Azure storage account name and access key.
- **Improved Builds table**
  The Builds table features two important enhancements:
  The maximum of 100 builds displayed in the table has been removed. The table can now display all the builds that exist in your Artifactory instance. A search window has been added to make it easier to focus on the builds of greatest importance to you. (This new search window works in coordination with the platform search window at the top of the UI.)
- **Additions to Artifactory Request Log (JSON version)**
  The JSON version of the Artifactory request log has been enhanced to include additional metrics for improved tracking of request and response performance. These enhancements provide insights into response timing, data size, processing duration, and request specifications.
- **Expanded support for scoped tokens in Deploy Evidence API**
  The Deploy Evidence REST API now supports scoped tokens based on specified artifacts in addition to its previous support for scoped tokens based on a specified repository. In both cases, the scoped token must include the Annotate action. For more information, see Create Scoped Token.
- **Filter Users and Groups by Role Within a Repository Via REST API** The JFrog Platform now supports filtering users and groups by role within a specific repository via REST API. For example, you can easily retrieve a list of admins for a specific repository to streamline permissions management. For more information, see Get User List API and Get a List of Groups API.
- **Allow Granting Manage Permissions in Permissions V2**
  The JFrog Platform now supports allowing users with `manage` permissions to grant `manage` and other permissions to other users in Permissions V2, although it is not recommended. For more information, see Permissions.
- **Add Unlimited Groups to a Reference Token in SAML** The JFrog Platform now supports adding an unlimited number of groups in SAML user-scoped reference tokens, as the number of groups does not affect the payload. For more information, see Create Token.
- **Improved Robustness of Binary Uploads to Google Cloud Storage (GCS)**
  The robustness of binary uploads to GCS has been improved by enhancing recovery mechanisms.
- **Daily Notification Emails for Token Expiration**
  The JFrog Platform now supports setting intervals for email notifications about tokens that are about to expire, either once or daily during the notice period. For more information, see Token Expiration Notification.
- **JFrog Platform WebUI Breadcrumbs**

From Artifactory version 7.116.3, breadcrumbs allowing you to orient yourself in the JFrog Platform WebUI will gradually be rolled out to all pages. For more information, see JFrog Platform Navigation.

- Workers
- Get Worker Code Samples with Worker Code Gallery
  The JFrog Platform now supports populating new Workers with GitHub code samples, directly from the JFrog Platform WebUI. For more information, see Configure Workers in the UI.
- Rerun Worker Runs
  The JFrog Platform now supports a Rerun feature to troubleshoot Worker runs. For more information, see Workers Troubleshooting.
- Updated Type Definitions for Event-Driven Workers' Response
  Refined TypeScript type definitions for event-driven workers' response to improve the developer experience.

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-7684	Archiving/Cold Storage	Medium	Fixed an issue whereby SaaS customers were able to execute the Access Export API.
RTDEV-56961	Archiving/Cold Storage	Medium	Fixed an issue whereby the next token was included in the Maven/Gradle cleanup results even if the number of results was less than the limit.
JA-16308	Authentication Providers	Medium	Fixed an issue whereby the JFrog CLI refresh token was failing for non-admin SAML users when their token scope included additional permissions beyond the default.
JA-17630	Authentication Providers	Low	Fixed Fixed an issue where the `access/api/v1/ldap/groups/ldap-groups/refresh?operation=UPDATE_AND_IMPORT` endpoint failed to work correctly when authenticated with an access token. This fix ensures that users can now successfully refresh LDAP groups using an access token.
RTDEV-56222	Authentication Providers	Medium	Fixed an issue whereby customers could sometimes mistakenly deploy artifacts using a FULL ACCESS TOKEN because the FULL ACCESS TOKEN did not take into account the scoped group of the token.
RTFE-2989	Authentication Providers	Medium	Fixed an issue whereby, it was possible to generate a valid token on the Set Me Up page when entering any password in the Password field when logging in by means of Authentication Provider.
JA-17696	Database	Critical	Fixed an issue whereby when Artifactory was configured to use a non-public PostgreSQL schema and a **search_path** that included the user's schema (default Postgres setting), Access incorrectly defaulted to using the non-public schema for its tables.
RTDEV-57265	Evidence Management	High	Fixed an issue that prevented users from deleting a repository containing evidence files.

JIRA Issue	Component	Severity	Description
RTDEV-55125	Federated Repositories	Low	Fixed an issue whereby when using the JMX exporter to see mBean metrics, errors were encountered.
RTDEV-57406	General	Low	Fixed an issue whereby an error warning was received when converting a RepoDescriptor URL to URI when the upstream URL in the remote repository settings had a '/' at the end of the URL.
RTDEV-58470	General	Medium	Fixed an issue whereby when the client requested an incorrect HTTP range, Artifactory returned an invalid HTTP content range.
JA-17181	General	High	Fixed an issue whereby the OIDC token exchange would fail when the Organization field was set and the Enable Permissive Configuration setting was disabled.
META-1873	General	Medium	Fixed an issue whereby metadata was unable to handle non-existent packages requested by Xray.
RPG-1799	General	High	Fixed an issue whereby when upgrading Artifactory in Windows to newer versions, Xray was unavailable.
RTDEV-54362	General	High	Fixed an issue whereby when calling the zap cache API, the zap repository cache was holding all artifact locks in a single long transaction.
RTDEV-56440	General	Medium	Fixed an issue whereby the internal repository **jfrog-usage-logs** was included by default in the system backup, and was excluded from export/import repositories and export/import system flows.
RTDEV-57054	General	Low	Fixed an issue whereby the Audit Event popup that is displayed in the Curation User Interface was showing a name for the Origin Server that was sometimes a random string of characters, which was not useful to the user.
RTDEV-57123	General	Medium	Fixed an issue whereby when creating or updating properties for a package with an emoji, if the database did not support emojis the action failed with 500 error message and the user was navigated to the 500 error page. Now, the user will receive a 422 error code and the properties will not be created/updated.
RTDEV-57267	General	High	Fixed an issue whereby Artifactory was still picking up the https port for router registration, and did not pick up the port from system configuration.
RTDEV-57293	General	Medium	Fixed an issue whereby an AQL transitive query on a virtual repository failed and returned a HTTP 500 response when the query was performed on a virtual repository that had an offline remote repository.

JIRA Issue	Component	Severity	Description
RTDEV-57400	General	Medium	Fixed an issue whereby Artifactory incorrectly displayed an old license expiration date even after a new license key was applied, due to persistent cached entitlements overriding new license information.
RTDEV-55275	General	Medium	Fixed an issue whereby, when searching for artifacts using the underscore (_) , the underscore was considered a wildcard and lead to undesirable results. This has been changed so that when using the underscore, it will be treated as an underscore character and not a wildcard.
RTDEV-58129	General	Low	Fixed an issue whereby, a new permission target called INTERNAL_default appeared in the list of Permission Targets after upgrading Artifactory.
INST-10787	Installation	Medium	Fixed an issue whereby the Artifactory Helm chart was misconfigured to read the `nodePort` value from `artifactory.nodePort` instead of the intended `artifactory.service.nodePort`, causing fixed `nodePort` settings to be ignored during deployments.
INST-11384	Installation	Medium	Fixed an issue whereby the `docker-compose-all.yaml` template for Artifactory did not expose Nginx ports (80 and 443) by default, preventing customer access to the Nginx container.
INST-9279	Installation	Medium	Fixed an issue where the **serviceName** in the **artifactory-statefulset.yaml** and the **artifactory-service.yaml** files were not identical, causing DNS resolution failures.
RTDEV-59631	Packages	Medium	Fixed an issue whereby Docker referrers were not passed to the federated repository.
RTDEV-55520	Packages	High	Fixed an issue whereby after resolving the release or InRelease file using a Debian virtual repository, the merged release file didn't include components from all repositories aggregated in the virtual repository.
RTDEV-56028	Packages	Medium	Fixed an issue whereby the npm search on an npm repository with more than 20 artifacts did not provide the correct latest version.
RTDEV-56101	Packages	Medium	Fixed an issue whereby corrupted cache from an npm remote repository was breaking the resolution of packages.

JIRA Issue	Component	Severity	Description
RTDEV-56651	Packages	Medium	Fixed an issue whereby an empty string in the **noarch** element in the Conda **repodata.json** metadata file caused a failure when downloading artifacts from a Conda repository with a pixi client.
RTDEV-57071	Packages	Medium	Fixed an issue whereby the **nuget search** command returned an empty response when searching for packages in a NuGet virtual repository that contained a remote GitHub packages repository.
RTDEV-57187	Packages	Medium	Fixed an issue whereby a 500 error was received when executing the Get RubyGem Version List REST API on a virtual repository.
RTDEV-57309	Packages	Medium	Fixed an issue whereby it was not possible to delete an improper **list.manifest.json** in a Docker repository.
RTDEV-57815	Packages	Medium	Fixed an issue in the max unique tags Docker cleanup feature where tags were removed out of order.
RTDEV-57859	Packages	Medium	Fixed an issue whereby, the SAX parser failed when parsing filtered XML resources.
RTDEV-58355	Packages	High	Fixed an issue whereby the upload of large files failed with Azure cloud providers.
RTDEV-58640	Packages	Medium	Fixed an issue whereby some versions of certain composer packages were not listed or downloadable when using a composer remote repository configured with default settings.
RTFE-3107	Packages	Medium	Fixed an issue whereby the option to “Enable Indexing in Xray” appeared in the configuration of Machine Learning repositories.
RTFE-3137	Packages	Low	Fixed an issue whereby an exclamation mark incorrectly appeared in the code snippet for manually setting credentials in the Set Me Up procedure for OCI repositories.
JA-17278	Platform Management	Medium	Fixed the issue whereby a global role created at the Platform level was unexpectedly automatically appearing under project roles.
JA-17177	Projects	High	Fixed an issue whereby project-level access tokens were circumventing the Read-Only restriction in a shared repository.
RTDEV-45715	Release Lifecycle Management	Medium	Fixed an issue whereby a build rename failed (because the build was not found in the defined project), but the operation was still reported as successful. After the fix, an error message is returned

JIRA Issue	Component	Severity	Description
			if a build with the specified name is not found in the defined project.
RTDEV-54817	Release Lifecycle Management	Medium	Fixed an issue that prevented webhook notifications from being triggered for each artifact in a Release Bundle v2 promotion. After the fix, users who have configured artifact copy/move webhook notifications (and include `<project-key>-release-bundles-v2` repositories) will receive notifications about each artifact when Release Bundles are promoted.
RTDEV-55410	Release Lifecycle Management	Medium	Fixed an issue whereby when trying to append an artifact to an empty build via the Build Append REST API, an error was encountered.
RTDEV-56117	Release Lifecycle Management	Medium	Fixed an issue that caused the platform UI to show an inaccurate number of items inside the packages contained in a Release Bundle.
RTDEV-56347	Release Lifecycle Management	Medium	Fixed an issue whereby only the latest piece of evidence was preserved when promoting a release bundle with Move.
RTDEV-57055	Release Lifecycle Management	Medium	Fixed an issue that caused the build cleanup procedure to fail after the associated project was deleted.
RTDEV-59330	Release Lifecycle Management	High	Fixed an issue that caused artifacts to be deleted when a Release Bundle was promoted using the `move` option to the environment in which it already resides.
RTDEV-58079	Release Lifecycle Management	High	Fixed an issue that prevented the creation of a Release Bundle v2 version from a build containing multiple images that share a layer.
JA-16404	Repositories	Medium	Fixed an issue related to Generic Repository Set-Me-Up whereby, when creating an identity token, the JFrog Platform did not include all required scopes.
RTDEV-60496	Repositories	High	Fixed an issue whereby the **.jfrog** system folder could not be deleted from local repositories or remote caches.
RTDEV-55094	Repositories	Low	Fixed an issue whereby, when a remote repository pointed to a blocked URL, the **Disable Artifact Resolution in Repository** setting could not be disabled even though the update request returned a 200 status code.
RTDEV-55756	Repositories	Medium	Fixed an issue where, after encountering a connection error with a remote repository, Artifactory

JIRA Issue	Component	Severity	Description
			prematurely reset the repository's offline status before completing an online check.
RTDEV-46823	Repositories	Medium	Fixed an issue whereby, when setting members in a virtual repository the order in the YAML configuration file was not maintained.
RTDEV-55298	Repositories	Low	Fixed an issue whereby, when trying to create a repository using the Create Repository Rest API without an "include pattern" in the input JSON, the repository was created with an empty string for the "include pattern" field.
RTDEV-55808	Repositories	Medium	Fixed an issue whereby when a Smart-Remote repository on Edge was pointing to another Artifactory instance and had artifacts in the cache, if the Main instance was up but had returned an unexpected error code, artifacts could not be resolved even if they were in the cache.
RTDEV-55932	Storage	Low	Fixed an issue whereby the storage summary graph that appears under Monitoring > Storage showed incorrect usage.
JA-17192	User Interface	Low	Fixed an issue whereby the **Disable Internal Password Login** setting was not functioning correctly when configured globally.
JA-17258	User Interface	High	Fixed an issue whereby, when creating a group via the JFrog Platform WebUI, the **Read Policy** role was not displayed.
JFUI-18147	User Interface	Medium	Fixed an issue whereby after clicking a URL to a specific package and needing to log in, users were directed to the general package page instead of the package referred to in the URL.
RTFE-3191	User Interface	High	Fixed an issue whereby the Trash Can could not re-enabled after disabling it via the User Interface.
TOPO-592	User Interface (UI)	High	Fixed an issue related to monitoring whereby, under certain circumstances, the Service Status page in the JFrog Platform WebUI displayed inaccurate uptime information for services.
JA-17040	User Management	Medium	Fixed a issue with synchronization in Access Federation for groups containing the 'anonymous' user, as the user's membership wasn't getting replicated.
JA-17058	User Management	Medium	Fixed an issue whereby when creating a user scoped token in the UI, then changes it during creation to a group scoped token, the token is created including

JIRA Issue	Component	Severity	Description
			the username previously selected (in user scoped token UI) instead of the logged in user's username required for group scoped token.
RTDEV-57047	User Management	Medium	Fixed an issue whereby an access project scoped token with the "Viewer" role allowed artifact deployment.

Artifactory 7.111

This section includes all the Artifactory 7.111 releases.

> **Critical Security Notice**
>
> All subversions are vulnerable to multiple non-critical security vulnerabilities that, in some deployments, can be chained into critical-severity attacks. We recommend that all customers upgrade to the latest version. View the latest Self-Managed and SaaS releases.

Artifactory 7.111.22 Self-Managed

Released: 7 Sept 2026

> This version includes security-driven configuration changes for plugin deployment.

Artifactory 7.111.21 Self-Managed

Released: 28 Aug 2026

> This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-82329	General	Critical	Potential authentication bypass leading to administrative access in Artifactory

Artifactory 7.111.20 Self-Managed

Released: 18 August 2026

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-42018	General	High	Anonymous token exposure in JFrog Artifactory

Artifactory 7.111.18 Self-Managed

Released: 27 July 2026

Security Notice

This version is designed to fix multiple security vulnerabilities that, when chained together, could result in a critical attack scenario if Anonymous Access is enabled. Anonymous Access is disabled by default and is not recommended for production environments due to the additional security risks it introduces.

CVE	Component	Severity	Fix Description
CVE-2026-65617	Packages	High	Designed to prevent unsafe Gems package deserialization that could lead to remote code execution
CVE-2026-65925	Packages	Medium	Designed to validate Cargo sparse index URLs to prevent server-side request forgery
CVE-2026-65921	Builds	High	Designed to prevent build artifact archive paths writing outside intended locations
CVE-2026-65922	General	High	Designed to block unauthorized writes to restricted internal metadata storage locations
CVE-2026-65923	Builds	Medium	Designed to validate Ansible provider URLs to prevent server-side request forgery
CVE-2026-66014	General	High	Designed to prevent HA authentication fail-open behavior causing privilege escalation
CVE-2026-65924	Packages	Medium	Designed to validate Terraform external provider URLs to prevent server-side request forgery

Artifactory 7.111.16 Self-Managed

Released: 15 July 2026

Resolved Issues

Jira Issue	Component	Severity	Description
RTFS-4094	Federated Repositories	Critical	Fixed a broken authorization service that could permit low-privileged users to read configuration data.
RTDEV-92146	Packages	Critical	Fixed a vulnerability in which weakly validated, request-derived data could be used to poison cached responses.

Artifactory 7.111.15 Self-Managed

Released: 29 June 2026

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-90399	General	Critical	A high-severity vulnerability was fixed in Artifactory. In certain cases, deprecated services could allow a low-privileged user to retrieve artifacts from repositories they were not authorized to access. JFrog recommends that all self-managed customers upgrade to a fixed version as soon as possible, especially those with anonymous user access enabled.

Artifactory 7.111.14 Self-Managed

Released: 28 April 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-69107	General	Medium	Potential unauthorized artifact access in JFrog Artifactory

Artifactory 7.111.12 Self-Managed

Released: 13 July 2025

Breaking Change for Artifactory Federation Service

The version of the Artifactory Federation Service (RTFS) that comes with this Artifactory release changes the context path from **/artifactory/service/rtfs** to `/rtfs`. This is a breaking change for users who have multiple sites (JPDs) using RTFS. (Users who run RTFS on only one site, and sites that use the legacy Federation service, are unaffected by this change.)

Users in Self-Managed environments who have sites running an older version of RTFS should upgrade them to the new version of RTFS as soon as possible to accommodate the new context path. As an interim solution, a set of commands can be added as a workaround to bridge the context path differences between sites using the new version of RTFS and sites using an older version, as described below.

Nginx Configuration

Add this command to the Nginx configuration of a site using the **new** version of RTFS:

```
location /artifactory/ {
    if ($request_uri ~ ^/artifactory/service/rtfs/(.*) $ ) {
      proxy_pass       http://router/rtfs/$1;
      break;
    }
    if ( $request_uri ~ ^/artifactory/(.*) $ ) {
      proxy_pass       http://artifactory/artifactory/$1;
    }
    proxy_pass         http://artifactory/artifactory/;
  }
```

This command instructs Nginx to redirect requests from sites that use the old RTFS context path to the new context path.

Add this command to the Nginx configuration of a site using the **old** version of RTFS:

```
location /rtfs/ {
  if ($request_uri ~ ^/rtfs/(.*) $ ) {
      proxy_pass       http://router/artifactory/service/rtfs/$1;
      break;
    }
```

This command instructs Nginx to redirect requests from sites that use the new RTFS context path to the old context path.

Apache Configuration

Use the following Apache rewrite rule to redirect requests between sites that have a mix of old and new context paths:

```
RewriteRule "^/artifactory/service/rtfs/(.*) $"
"balancer://artifactory/artifactory/service/rtfs/$1" [P,L]
```

Important Migration Note

When migrating from the legacy Federation service to RTFS, be sure to use **version 2.0** of the CLI, which implements the new context path.

Feature Enhancements

- Improved Get Federation Sync State REST API performance

The performance of the REST API that returns the synchronization state of all Federated repositories in the JPD has been improved.

> **Note**
>
> This API endpoint is relevant for users operating the legacy Federation service, not the Artifactory Federation Service (RTFS).

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-58470	General	Medium	Fixed an issue whereby when the client requested an incorrect HTTP range, Artifactory returned an invalid HTTP content range.
INST-11555	Installation	High	Fixed an issue whereby the command to perform a graceful shutdown was not working for **JFConfig** and **Topology** services in certain negative scenarios, specifically when the Artifactory service didn't start completely. This means that these services would sometimes remain active even with a stop command.
RTDEV-60193	Packages	Critical	Fixed an issue whereby the Go Mod download process encounters a failure when the MCRP limit is reached, resulting in an unsuccessful request to the remote

JIRA Issue	Component	Severity	Description
			resource and the attempts to serve from the cache also fail.

Artifactory 7.111.11 Self-Managed

Released: 3 July 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-58622	General	Medium	Fixed an issue whereby changing the value of a system property in the "artifactory.properties" file was ignored.
RTDEV-57293	General	Medium	Fixed an issue whereby an AQL transitive query on a virtual repository failed and returned a HTTP 500 response when the query was performed on a virtual repository that had an offline remote repository.
RTDEV-57859	Packages	Medium	Fixed an issue whereby the SAX parser failed when parsing filtered XML resources.

Artifactory 7.111.10 Self-Managed

Released: 17 June 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-46823	Repositories	Medium	Fixed an issue whereby when setting members in a virtual repository, the order in the YAML configuration file was not maintained.
JFUI-18147	User Interface (UI)	Medium	Fixed an issue whereby after clicking a URL to a specific package and needing to log in, users were directed to the general package page instead of the package referred to in the URL.

Artifactory 7.111.9 Self-Managed

Released: 3 June 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-57815	Packages	Medium	Fixed an issue in the max unique tags Docker cleanup feature where tags were removed out of order.

JIRA Issue	Component	Severity	Description
RTDEV-57187	Packages	Medium	Fixed an issue whereby a 500 error was received when executing the Get RubyGem Version List REST API on a virtual repository.
RTDEV-57071	Packages	Medium	Fixed an issue whereby the Nuget search command returned an empty response when searching for packages in a NuGet virtual repository that contained a remote GitHub packages repository.

Artifactory 7.111.8 Self-Managed

Released: 20 May 2025

Feature Enhancements

- Default Socket Timeout for Federated Repositories

The default socket timeout for Federated repositories has been changed to 300,000 milliseconds (5 minutes). This value can be adjusted, if required, using an Artifactory system property. For more information, see Increase the Predefined Socket Timeout for Larger Repositories.

Resolved Issues

JIRA Issue	Component	Severity	Description
INST-11375	Installation	Medium	Fixed an issue whereby when JFConfig was added to the Artifactory-HA chart, the `volumeMounts` section was not included in the `statefulset.yaml`, causing the upgrade to fail.
RTDEV-57644	Packages	Medium	Fixed an issue whereby when executing the PyPI JSON API against a PyPI remote repository pointing to 'https://pypi.org', Artifactory returned a 500 error status code.
RTDEV-57309	Packages	Medium	Fixed an issue whereby it was not possible to delete an improper list.manifest.json in a Docker repository.
RTDEV-56651	Packages	Medium	Fixed an issue whereby an empty string in the noarch element in the Conda repodata.json metadata file caused a failure when downloading artifacts from a Conda repository with a pixi client.
RTDEV-55808	Repositories	Medium	Fixed an issue whereby when a Smart-Remote repository on Edge was pointing to another Artifactory instance and had artifacts in the cache, if the Main instance was up but had returned an unexpected error code, artifacts could not be resolved even if they were in the cache.
RTDEV-56961	Archiving/Cold Storage	Medium	Fixed an issue whereby the next token was included in the Maven/Gradle cleanup results even if the number of results was less than the limit.

Artifactory 7.111.7 Self-Managed

Released: 8 May 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
INST-10962	Installation	High	Fixed an issue where the One Model registry service was not starting when upgrading Artifactory installations for Linux Archive, Debian, and RPM in service mode, with `console.log` being disabled (`shared.logging.consoleLog.enabled: false`) in `system.yaml` .
JA-17177	Projects	High	Fixed an issue where the project level access tokens were bypassing the Read-Only restriction in shared repository.
RTDEV-56117	Release Lifecycle Management	Medium	Fixed an issue that caused the platform UI to show an inaccurate number of items inside the packages contained in a Release Bundle.
RTDEV-56101	Packages	Medium	Fixed an issue whereby corrupted cache from an npm remote repository was breaking the resolution of packages.
RTDEV-56028	Packages	Medium	Fixed an issue whereby the npm search on an npm repository with more than 20 artifacts did not provide the correct latest version.,

Artifactory 7.111.4 Self-Managed

Released: 23 April 2025

Important Announcements

- Pre-Upgrade Checks for Bundled PostgreSQL

If you are using the bundled postgresql with the Artifactory Helm chart during the upgrade to Artifactory version 7.111, it is essential to perform some pre-upgrade checks to ensure a smooth upgrade.

Breaking Changes in Bundled PostgreSQL Upgrade

Starting from Artifactory version 7.111.x, the bundled postgresql chart is upgraded to version 15.5.20. This update is available in the latest artifactory and artifactory-ha Helm charts.

If you upgrade Artifactory from any older version to 7.111.x directly, there may be some challenges during the upgrade if you are using the bundled postgresql in the Helm chart. Customers using an external postgresql will not be affected.

For more information about the pre-upgrade checks to be performed, see Pre-Upgrade Checks for Bundled PostgreSQL in Artifactory.

- Verify Database Configurations for Go Services

If you have customized the database URL for the Metadata microservice, it is essential to configure the Evidence database URL as well for a smooth upgrade, as both are GO services.

Database Configuration Checks for Smooth Upgrade

Similar to Metadata, Evidence is also a Go service with a direct connection to the Artifactory database. Note that, JFrog provides a JDBC to Go URL converter within the Artifactory application to facilitate this connection.

However, in some cases, the converter may be unable to connect, which could affect Go services like Metadata and Evidence.

Customers who have previously configured `metadata.database.url` must also add `evidence.database.url` before upgrading to version 7.111.x. This step is essential to maintain database connectivity after the upgrade.

New Features

- Packages: Hex Repositories

Hex repositories in Artifactory allow you to deploy and resolve Hex packages. For more information, refer to Hex Repositories. (GA for all customers)
- Packages: NVIDIA NIM Models

JFrog Artifactory now integrates with NVIDIA NIM, allowing you to cache NVIDIA NIM models in Artifactory via a remote repository. NVIDIA NIM is a set of microservices designed to accelerate the deployment of foundation models across any cloud or data center, ensuring data security. It provides production-grade runtimes with ongoing security updates and stable APIs, backed by enterprise-grade support. For more information, refer to NVIDIA NIM Repositories.
- API Key Deprecation Control

As part of the deprecation process, API Key has reached End of Life in Q4.24. This version includes a checkbox in the JFrog platform UI allowing you to control the API Key usage deprecation. This checkbox will be deselected by default: to block API key usage in your environment, select the **Disable API Key Usage** checkbox under **Administration** > **Security** > **General**. For more information, see JFrog API Key Deprecation Process.
- New Service - JFConfig

We have added a new service to our Self-Managed instances. JFConfig is a service that can be used by other JFrog services to store configuration in a key-value format in DB in a centralized way.

For more information, see Artifactory Product.
- Support `readOnlyRootFilesystem` in Artifactory Containers

Support has been added for `readOnlyRootFilesystem` in Artifactory containers, which is a Kubernetes security context feature. This feature enhances security by allowing Artifactory to operate in environments where containers are configured with `readOnlyRootFilesystem=true`. In this configuration, the entire file system of the container is set to read-only, preventing modifications to files or directories. This setting serves as a security measure to protect the application and its data from unauthorized changes.

For more information on how to configure this setting, see Configure readOnlyRootFilesystem in Artifactory Containers.
- Enable Logging to `STDOUT` and `STDERR`

In the Artifactory Helm charts, container logs are supported through `STDOUT` and `STDERR`. This feature can be enabled by setting the feature flag `logging.logToStdoutJson=true`. When the feature is enabled, container logs will be output in JSON format via console logging, while service logs inside the container will be available only in text format, such as `artifactory-service.log`.

Feature Enhancements

- Packages and Repositories

- New Machine Learning Layout for Hugging Face Repositories

All new Hugging Face repositories are now created with the new unified Machine Learning layout. Users can also migrate legacy Hugging Face repositories to the new Machine Learning layout on a manual basis. The Hugging Face repositories legacy layout will be deprecated in July 2025 when all repositories with the legacy layout will be automatically upgraded to the Machine Learning layout. For more information, click here.

- Added Support for Chocolatey and PowerShell Clients in Nuget Repositories

Added support for PowerShell (minimum version 1.0.5) to interact with NuGet repositories. Added support for Chocolatey (minimum version 1.2.0) to interact with Nuget repositories.

For more information, see NuGet Repositories.

- **Hex Virtual Repositories**

Artifactory now supports Hex Virtual Repository. A Hex virtual repository aggregates Hex local and remote repositories, enabling more efficient package management. To learn more, see Hex Repositories.

- **Easier Configuration of the NimModel Redirect Download Form**

The NimModel redirect download form can now be configured through the User Interface.

- **Complete Docker and OCI List Manifest Image Overwrite**

When overwriting a **list.manifest** file with a new one, all previous sub-manifests will be removed, enhancing storage efficiency and reducing the need for manual cleanup. For more information, click here.

- **Support Added for the PyPI JSON API in Remote and Virtual Repositories**

Artifactory now supports PyPI's JSON API in remote and virtual repositories.

- **Support Added for PyPI JSON API in Local Repositories**

Artifactory now supports the PyPI JSON API in local repositories with most attributes. The following attributes (JSON keys) are not supported:

- Deprecated keys (releases, downloads, has_sig, bugtrack_url) as described in PyPI JSON API
The following info sub keys: description_content_type, dynamic, license_expression, license_files, maintainer, maintainer_email, project_urls, provides_extra, requires_dist Vulnerabilities key

- **Permissions Added for Using Zapping Cache on Remote Repositories**

The Zapping Cache action on remote repositories now requires **Manage** or **Delete** permissions, either via the UI or API. This change is backward-compatible. For more information on UI changes, click here, and for API changes, click here.

- **Repositories can now be assigned to more than one environment**

For more information, see Assign Environments to Repositories.

- **Added Tags for RPM local repositories**

Added support for the `Recommends` and `Suggests` dependency tags in the `primary.xml` metadata of RPM local repositories enhancing package management for clients like `dnf` and `yum` by recognizing optional dependencies.

Feature Flag Control: The inclusion of Recommends tags in `primary.xml` can now be configurable via a feature flag

`yum.local.install.recommended.dependencies.enabled`.

To learn more, refer to Install RPM Packages Using Yum.

- **Added Support for Listing Folder Items in Conan Smart Remote Repositories**

- A new setting, **List Folder Items**, is now available for Conan Smart Remote Repositories.
- Enabling the **List Remote Artifacts** checkbox during repository creation allows folder items to be listed.

- **Improved Access for Go Remote Repositories**

Go remote repositories now support the ability to access subgroups in GitLab.

- **Bearer Authentication for Remote Repositories**

Added Bearer Authentication support for remote repositories.

- **Properties Tab for RPM Remote Packages**

Added functionality to calculate and display the properties of an RPM package after it is downloaded from a remote RPM repository. The package properties are now shown in the **Properties** tab on the UI.

- RPM Repositories - SHA-256 checksums have been integrated into Local and Virtual repositories

Added SHA-256 checksums to the `repomd.xml` files of local and virtual repositories. This improvement ensures package integrity verification aligns with remote repositories' security standards.

Local repositories previously do not have SHA-256 checksums in their `repomd.xml` files, increasing the risk of undetected package tampering or corruption.

Enable SHA-256 for enhanced security in package integrity verification. To enable SHA-256 checksums, update the configuration by setting `yum.local.repomd.calculate.sha2.enabled = true`

- Improved Performance of the Repository Selection Field in Set-Me-Up

The performance of the repository selection field in Set-Me-Up has been improved by promoting a search-first approach.

- Improvement to Maven Set-Me-Up Placeholders

Maven set-me-up placeholders will now automatically populate.

- Cleanup Policies

- Support for Vagrant and Hex in Cleanup and Archive

Vagrant packages are now supported in Cleanup and Archive. Hex packages are now supported in Cleanup and Archive.

- Support for Alpine and SBT in Cleanup and Archive

Alpine packages are now supported in Cleanup and Archive. SBT packages are now supported in Cleanup and Archive.

- Improved Cleanup Release Bundle V2 Report

The Cleanup Release Bundle V2 report has been improved. For more information, refer to Cleanup Run Report Overview.

- Support for Conda in Cleanup and Archive

Conda packages are now supported in Cleanup and Archive.

- Policy Conditions - Cleanup Packages

- Adding Property-based Policy Condition

Enhanced package-cleanup functionality with the addition of a **property-based** policy condition. You can now include or exclude specific package versions from cleanup by applying a property-based policy condition. This allows for more granular control over which packages are retained or removed during cleanup actions. For more information, see Create Cleanup Policy - Package.

- Adding days/weeks selection for Time-based Policy Condition

Enhanced package-cleanup functionality with the addition of **days/weeks** selection for **Time-based** policy condition. You can now configure by specifying **Time-based** cleanup conditions based on days/weeks for the packages. For more information, see Create Cleanup Policy - Package.

- Federation

- Compile list of inconsistent Federated repositories

A new API enables you to return a list of all Federated repositories in your local Artifactory instance that have a configuration mismatch with one or more remote members. After getting the list of mismatches, you can use the Synchronize Federated Member Configuration REST API on each mismatch to synchronize the members. For more information, see Get List of Inconsistent Federated Repositories API.

- New API for removing Federation members

A new REST API enables you to remove a member from all repository Federations to which it belongs. This can be used, for example, when a site is taken out of commission. This API removes the member on this site from all the Federations in which it was a part. For more information, see Remove Federation Member API.

- Release Lifecycle Management

- Improved Release Lifecycle Management Kanban board

The Release Lifecycle Management kanban board has been redesigned to provide more information at a glance, including clear indications of failed promotions. For more information, see Promote a Release Bundle v2 Version in the Platform UI.

- Auto-creation of Release Bundle v2 versions after build promotion

By default, Artifactory now creates a Release Bundle v2 version automatically when you promote a build using the JFrog CLI or REST API. It also promotes the Release Bundle to the environment associated with the build's target repository, if defined. Both copy promotions and move promotions are supported. Having a Release Bundle provides better visibility and control over your release candidate as it progresses through your SDLC.

- Creating project-specific environments during build promotion

When promoting a build, if the target repository (`targetRepo`) is part of a project, a project-specific environment is created for the auto-created Release Bundle v2. The environment is named after the `status` value of the build.

- Giving build status priority over an existing target environment during build promotion

If the `status` is defined for a build, the environment represented by that status is always given priority during promotion. For example, if an environment assigned to the `targetRepo` matches the `status` , the auto-created Release Bundle v2 is promoted to that environment. (That is, it is given priority over other environments that might also be assigned to the `targetRepo` .) If no environment exists for the `status` , a new environment is created for the promoted Release Bundle v2 with the name of the status, even when other environments are available.

- Searching for distributed Release Bundle versions containing a specific artifact

The Get Release Bundle v2 Versions by Artifact REST API (introduced in 7.107.1) has a new query parameter has a new query parameter that can return distributed Release Bundle versions (`origin=target`) containing the artifact in addition to created Release Bundle versions (`origin=source`). This new query parameter makes it possible to run the API on Edge nodes in addition to standard Artifactory instances.

- Moving artifacts during Release Bundle v2 promotion

When promoting a Release Bundle v2 version, you can optionally move the contents of the Release Bundle from the source to the destination instead of copying them (the behavior until now). For example, if you promote a Release Bundle v2 version from the DEV environment to the QA environment and select the Move option, the artifacts are removed from the repositories associated with DEV and moved to the repositories associated with QA. The option to move artifacts can be executed using the JFrog CLI, API, or platform UI.

- Release Bundle v2 version creation using artifacts in virtual repositories

You can now create a Release Bundle v2 version using artifacts located in a virtual repository, provided the source path of the artifacts points to a local repository (not a remote repository) aggregated by the virtual repository. This feature is relevant when creating a Release Bundle version from a list of artifacts.

- Support for SemVer sorting in Release Bundle v2 APIs

SemVer sorting support has been added to the Get Release Bundle v2 Versions API and Get Release Bundle v2 Versions in a Specific Environment API. This support is limited to the 1000 latest records and does not support pagination. This option pulls the latest 1000 records only and does not support pagination. Versions that do not conform to SemVer rules are sorted afterward lexicographically.

- New API for returning all Release Bundle v2 versions containing a specified artifact

A new REST API endpoint is available that returns a list of Release Bundle v2 versions containing a specified artifact. The `origin` query parameter enables you to distinguish between versions created on a device (`origin=source`) as opposed to versions distributed to a device (`origin=target`). This enables you to run this API on Edge nodes in addition to standard Artifactory instances. For more information, see Get Release Bundle v2 Versions by Artifact API.

- New API for returning all Release Bundle v2 promotions containing a specified artifact

A new REST API endpoint is available that returns a list of promoted Release Bundle v2 versions containing a specified artifact. For more information, see Get Release Bundle v2 Version Promotions with a Specific Artifact API.

- New API for returning all Release Bundle v2 versions in a specified environment

A new REST API endpoint is available that returns all Release Bundle v2 versions associated with a specified environment, for example, DEV or PROD. For more information, see Get Release Bundle v2 Versions in a Specific Environment API.

- New API for adding tags to Release Bundle v2 versions

You can now add a descriptive tag to a Release Bundle v2 version via REST API to help identify Release Bundle versions quickly. The tag will appear on the stages board in the platform UI to enhance visibility and organization. For example, you can create tags such as `nightly-build`, `release-candidate`, `bugfix-2025-33124`, and so on. For more information, see Assign Tag to Release Bundle v2 Version API.

- Get Release Bundle v2 Versions API returns tag information

The Get Release Bundle v2 Versions REST API now returns the descriptive tag assigned to a Release Bundle version. For more information about tagging, see Assign Tag to Release Bundle v2 Version API.

- Increased limits for Release Bundle v2 names and versions

The maximum length of the name (`release_bundle_name`), version (`release_bundle_version`), and creator (`created_by`) of a Release Bundle v2 has been increased to 255 characters when working with the REST API.

- New promotion icons on RLM Kanban board and timeline

New icons have been introduced to the Release Lifecycle Management stages board and timeline. These icons indicate at a glance what type of Release Bundle promotion was performed (copy artifacts or move artifacts). Hovering over the icon provides a tooltip reminder. For more information, see Promote a Release Bundle v2 Version in the Platform UI.

- Evidence

- Evidence management – support for additional databases and installation types

The Evidence service now supports all databases that Artifactory supports. For the complete list, see Artifactory Database Requirements. In addition, the Evidence service is now enabled by default for all installation types. For more information, see Installing Artifactory.

- Attach external evidence to artifacts in the local part of a virtual repository

You can now attach external evidence to artifacts located in a local repository that is aggregated inside a virtual repository. For more information about attaching external evidence, see Evidence Service.

- Changes to Evidence GraphQL APIs

The `repositoryKey` and `path` fields have been deprecated from the Get Evidence API and Search Evidence API, and `subject` (which contains `repositoryKey`, `path`, `name`, and `sha256`) has been added.

- Viewing Evidence in the Packages Screen

You can now view a list of the evidence files associated with a specific package version in a selected repository. For more information, see View the Package Evidence Table.

- Enable Evidence for All Installations

Starting from Artifactory version 7.111, Evidence service is available for all installations.

- JFrog Platform

- Performance Improvements with Artifactory Helm Charts bundled with Nginx

A number of performance improvements have been made when using Artifactory Helm Charts bundled with Nginx. These items can be configured in the Helm chart's values.yaml file. The enhancements include:

Improved performance with throughput improvements of up to 59% Increased number of available Nginx workers connections: from 1024 to 8192 (worker_connections 8192)
Auto-scaling of the number of workers: based on the number of available CPUs (worker_processes auto) The ability to use keep-alives: for reusing the Nginx > Artifactory connections

- **Added Memory Target Trigger to Artifactory Charts using HPA**

Custom metrics support for Horizontal Pod Autoscaler (HPA) has been incorporated into the Artifactory Helm chart. With these metrics, you can configure custom auto-scaling behavior for HPA.

For the Artifactory chart, HPA will function only when the replica count is a minimum of 2 (i.e., in High Availability mode). For the Artifactory HA chart, HPA will operate as expected.

For more information, see Add Memory Target Trigger to Artifactory Charts using HPA.

- **Improved Project Navigation**

The Projects navigation menu now includes UI usability enhancements: it is now located in the sidebar and highlights Projects filtering to clarify context switching between Project and All Projects scope.

- **Blocking Blob Uploads If a Digest Does Not Match the Blob's SHA-256 Checksum**

Added a flag to block blob uploads if a provided digest does not match the blob's SHA-256 checksum. This flag is disabled by default but can be enabled as needed.

- **Docker Repository Key Length Limitation on Cloud Platforms**

Artifactory cloud customers using the Docker Subdomain method will now receive a warning when creating a repository if their repository key is too long for DNS record creation. This could lead to accessibility issues if DNS is not managed internally. However, exceeding the character count does not prevent creating the repository. For more information, see Docker Limitations in Artifactory.

- **Support for Triggering Partial Reindexing of Helm Charts**

Added support for triggering partial reindexing of Helm charts, enabling more efficient and targeted **index.yaml** updates. This improvement reduces processing time and resource usage. For more information, see Helm Charts Partial Re-Indexing .

- **Access Token Expiration Email Now Points to the CNAME Domain**

The JFrog platform will send users Access token expiration reminder emails which include the CNAME URL instead of the JFrog instance URL.

- **SCIM Token Expiry Configuration**

The JFrog Platform now supports the creation of SCIM tokens with configurable expiry times. To learn more, see Generate a Scoped Token for SCIM.

- **Get Token Last Used Information**

The JFrog Platform now supports getting a token's 'last used' timestamp when using Get Tokens and Get Token By ID REST APIs.

- **Support for Reading Permissions Scoped Tokens**

It is now possible for non-admin users to use the Get User List API, Get a List of Groups API, and Get All Permissions API endpoints using a scoped token. For more information, see Create Scoped Token.

- **Maximum placed on bad checksum search responses**

Responses to the Bad Checksum Search REST API are now limited to a maximum of 10,000 results.

- **Storage**

- **New Metric for Obtaining Shard Accessibility Status**

For Artifactory instances configured to use shards, a new metric (`jfsh_shard_accessibility_status_total`) has been introduced for obtaining the accessibility status of each shard. The possible values are:

1: a shard is accessible 0: a shard is inaccessible

- -1: a timeout occurred while checking the accessibility status of a shard

For more information, click here.

- **New Metric for Counting Binaries Not Cached Due to Their Large Size**

A new metric (`jfsh_cache_bypass_large_binary_total`) has been added for counting binaries that were not cached due to their large size. For more information, click here.

- **Supported Worker Features**

- **New Worker Event: Before Token Expiry**

JFrog now supports creating event-driven workers to trigger before a token expires. Learn more

- `Alt Response` event is now supported.
- `Alt All Responses` event is now supported.
- `Alt Remote Content` event is now supported.
- `After Download Error` event is now supported.
- `Before Download Request` event is now supported.
- `Before Build Info Save` event is now supported.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-55463	Archiving/Cold Storage	Medium	Fixed an issue whereby Artifacts that were never downloaded from Artifactory were not deleted by Time-Based Cleanup Policies.
JFUI-17125	Authentication Providers	Medium	Fixed an issue whereby when using SAML with “Auto Redirect Login Link To SAML Login” enabled, logout from another realm logged you into SAML instead of logging out completely.
RTDEV-51424	Builds	Low	Fixed an issue whereby on the Builds Tab of an artifact in the artifacts tree, the "Go to Build" button would not work if the build name contained a slash hyphen (/-).
RTDEV-52470	Builds	Medium	Fixed an issue where by when refreshing the UI, the projects build page would display different results.
RTDEV-54283	Builds	High	Fixed an issue that caused Build Uploaded and Build Deleted webhook notifications to be sent when these operations began instead of waiting for the operations to complete. This meant that if the operations failed and were rolled back, the rollback occurred after the notification indicating completion was already sent.
RTDEV-53064	Database	Medium	Fixed an issue whereby MariaDB JDBC driver 3.4.1 was not working with Artifactory 7.98.9 after upgrading from Artifactory 7.84.21.
RTDEV-54017	Federated Repositories	High	Fixed an issue in the legacy Federation service whereby, after an upgrade, repositories that failed Federated Metadata Negotiation had their status updated incorrectly from DISABLED_BY_SYSTEM to

JIRA Issue	Component	Severity	Description
			DISABLED, which prevented the auto-healing mechanism from performing recovery.
JA-16359	General	Medium	Fixed an issue whereby group information for a selected user was not displayed.
JA-16503	General	Medium	Fixed an issue whereby when the Authentication provider name contained a space character it did not render the configuration page.
JFUI-17179	General	High	Fixed an issue where the Select Log File dropdown list was not displayed properly in the UI when the screen width was too small.
RTDEV-48643	General	Medium	Fixed an issue whereby an error was returned after upgrading to the latest Artifactory version, even though the upgrade was successful.
RTDEV-51363	General	Medium	Fixed an issue whereby Apache Tomat version 10.1 that was bundled in Artifactory 7.98.7 contained an issue whereby when sending HEAD requests where the resource size was unknown, the server returned a content-length=0 header instead of omitting the header.
RTDEV-52983	General	High	Fixed an issue whereby when upload to S3 storage failed for an aritfact, a 200 OK message was entered in the **artifactory-request.log**.
RTDEV-53694	General	Medium	Fixed an issue whereby calling the Create or Update Reverse Proxy Configuration API with invalid data led to a broken Artifactory configuration.
RTDEV-54115	General	Medium	Fixed an issue whereby multipart uploads were failing to virtual repositories for a non-admin user even if the user had deploy permission.
RTDEV-54667	General	Medium	Fixed an issue whereby the email date format was displaying as YYYY instead of yyyy.
RTDEV-55208	General	Low	Fixed an issue whereby the Artifact count temporarily displayed '0' while the HQC was being refreshed.
RTDEV-55266	General	Medium	Fixed an issue whereby when trying to retrieve a package from a remote Maven repository, a 404 Forbidden error was encountered.
RTDEV-50192	General	High	Fixed an issue whereby when downloading files with Chinese characters in the file name via the "File URL", a 500 error was received.

JIRA Issue	Component	Severity	Description
RTDEV-50750	General	Medium	Fixed an issue whereby when a non-admin user using an include pattern would attempt to delete or overwrite a repository with an artifact in it that is already in the trash can, the action would fail.
RTDEV-50452	Packages	Medium	Fixed an issue whereby Debian virtual metadata requests were triggering extra metadata calculations even if the cache had not expired.
RTDEV-50987	Packages	Medium	Fixed an issue whereby when working with a Gems virtual repository and running the API "/api/v1/versions/" a 500 error was displayed.
RTDEV-51247	Packages	High	Fixed an issue that prevented locally-generated properties of various package types from being replicated.
RTDEV-52654	Packages	Medium	Fixed an issue whereby when the “Hide Existence of Unauthorized Resources” option was enabled on a local repository and Python packages were uploaded to a virtual repository associated with that local repository, a 400 error response was received instead of a 404 error response.
RTDEV-52844	Packages	Medium	Fixed an issue whereby all Docker image layers appeared as RUN layers.
RTDEV-53162	Packages	Medium	Fixed an issue whereby uploading a batch of pub packages sometimes resulted in missing versions within the generated metadata.
RTDEV-53745	Packages	Low	Fixed an issue whereby when configuring a Hugging Face smart remote repository with the prefix api/huggingfaceml, clicking the test button resulted in a 404 error even though the test was actually successful.
RTDEV-53823	Packages	Medium	Fixed an issue whereby there was inconsistent resolution behavior when multiple remote repositories were aggregated in a Terraform virtual repository.
RTDEV-53840	Packages	Medium	Fixed an issue whereby when performing an Artifactory upgrade, updating of existing Helm local repositories failed with a 400 response code.
RTDEV-53903	Packages	Medium	Fixed an issue whereby when uploading very large files with 1,000+ parts using multipart upload, the upload would not complete.
RTDEV-54091	Packages	Medium	Fixed an issue whereby a user who does not have delete permissions would receive a 200 successful status code when calling the Promote Docker Image

JIRA Issue	Component	Severity	Description
			API with a copy:false parameter, even though certain artifacts were not removed from the source repository. Now, when this happens, the API returns a 206 status code, indicating partial success because the promotion was executed successfully but insufficient permissions prevented the deletion of certain artifacts from the origin repository.
RTDEV-54260	Packages	Medium	Fixed an issue whereby non-admin users were unable to create a Debian snapshot for a virtual repository.
RTDEV-54891	Packages	Medium	Fixed an issue whereby 'symbols.nupkg' was getting indexed post calling reindex endpoint and then restarting the Artifactory instance.
RTDEV-55270	Packages	Medium	Fixed an issue where maven set-me-up generated settings.xml did not support OIDC integration for use with Github actions.
RTDEV-55450	Packages	Medium	Fixed an issue whereby the Promote Docker Image API renamed sub-manifest tags according to their architectures.
RTDEV-55696	Packages	High	Fixed an issue whereby triggering indexing in a nested virtual Debian repository also triggered indexing in all parent virtual repositories.
RTDEV-55754	Packages	High	Fixed an issue whereby when trying to override an image with the exact same image, by a user without delete permission, a 403 error was encountered.
RTFE-1637	Packages	Medium	The Graph view was removed from the Packages tab.
RTFE-2467	Packages	Medium	Fixed an issue whereby when the cache retrieval period for metadata was updated via the UI, the values were not applied.
RTFE-2532	Packages	Medium	Fixed an issue whereby Gradle repositories did not have the Enable Redirect Download checkbox.
RTFE-2534	Packages	Medium	Fixed an issue whereby in the All Packages view the same data was loaded infinitely and new data was not displayed.
RTFE-2586	Packages	Medium	Fixed an issue whereby when in the Packages window and sorting by the security column, an error would be encountered.
RTFE-2641	Packages	Medium	Fixed an issue whereby when trying to create a repository in the Create a Repository window, Pub, Swift and Terraform repositories were not available.

JIRA Issue	Component	Severity	Description
RTFE-2648	Packages	Medium	Fixed an issue whereby when trying to use the Set me up functionality from inside the JFrog Platform Deployment with Pub, Swift, and Terraform package types, configuration options were not displayed.
RTFE-2658	Packages	Medium	Fixed an issue whereby when using a custom CNAME for a cloud instance configured using the My JFrog Portal, the instructions on the Docker repository's Set Me Up page had a blank space instead of the URL.
RTFE-2714	Packages	Medium	Fixed an issue whereby when searching for packages and applying a filter, the page flickers and no results are displayed.
RTFE-2525	Packages	Medium	Fixed an issue whereby when switching from Recently Viewed packages to a packages custom view, the custom view was not applied and instead all packages were listed.
RTDEV-53104	Packages	Low	Fixed an issue whereby the "deprecated" field type returned by the npm view via the Artifactory npm repository was inconsistent with the npm source register.
RTDEV-53251	Packages	Medium	Fixed an issue whereby missing Vagrant .box properties caused 500 internal server errors when resolving boxes.
RTDEV-53268	Packages	Medium	Fixed an issue whereby users could not download NuGet packages from an upstream Beckhoff TwinCAT Package Manager repository through Artifactory.
RTDEV-53371	Packages	Medium	Fixed an issue whereby when configuring a NuGet Remote Repository targeting **community.chocolatey.org**, no metadata was cached when executing the "choco outdated" command.
RTDEV-53839	Packages	Critical	Fixed an issue whereby an unannounced change that was introduced by Conda Forge upstream impacts Artifactory's ability to resolve package metadata and dependencies with virtual Conda repositories.
RTDEV-54026	Packages	Medium	Fixed an issue whereby Cargo repositories failed to calculate the index of the repository if the package name contained more than one hyphen.
RTDEV-54861	Packages	Medium	Fixed an issue whereby when retrieving the Packages.gz file from a virtual repository, sometimes old package information was retrieved, which lead to certain tools reporting old packages that no longer existed in the upstream.

JIRA Issue	Component	Severity	Description
RTDEV-55484	Packages	Medium	Fixed an issue whereby triggering the Recalculation Index on an empty Conan local repository resulted in an error, increased the Conan metadata stuck tasks, and all packages that were uploaded after the reindexing were not indexed.
JFUI-17179	Platform Management	Medium	Fixed an issue where the **Select Log File** drop-down list is not displayed properly in the UI when the screen width is too small.
JA-16046	Platform Management	Medium	Fixed an issue whereby federated reference token authentication was not working correctly in Event APIs.
JA-16274	Platform Management	Medium	Fixed an issue where project access tokens were not getting revoked when the user who created them was removed.
JA-16151	Projects	Medium	Fixed an issue whereby project scope access tokens were visible from the Project Admins profile.
JA-16710	Projects	Medium	Fixed an issue whereby when calling the **Update Existing Project Properties REST API**, the project storage quota was set to 0 and the project description was removed.
RTDEV-53914	Release Lifecycle Management	Medium	Fixed an issue whereby Release Bundle promotion failed when the Release Bundle contained artifacts in a local repository aggregated by a virtual repository.
RTDEV-54887	Release Lifecycle Management	Low	Fixed an issue that caused the evidence graph to fail when the Release Bundle contains an artifact from a build whose **build.number** property contains multiple values.
RTDEV-48297	Release Lifecycle Management	Medium	Fixed an issue whereby when creating a Release Bundle v2 for an OCI Helm Image, SHA files for layers were missing.
RTDEV-54151	Release Lifecycle Management	Medium	Fixed an issue that prevented certain commands from being executed on builds containing the `originalDeploymentRepo` field that were promoted using the `--copy` flag.
RTDEV-55692	Release LIfecycle Management	Medium	Fixed an issue whereby the Xray scan of a Release Bundle v2 version would fail if any item in the Release Bundle contained a property whose value included a surrogate pair (a way to represent special characters in UTF-16, such as an emoji). Artifactory now normalizes the surrogate pair into a string that Xray can process.

JIRA Issue	Component	Severity	Description
RTDEV-50832	Repositories	Low	Fixed an issue whereby non-admin user selecting "Show All Included" on a virtual repository that contains another virtual repository don't see the other virtual repository.
RTDEV-52748	Repositories	Medium	Fixed an issue where Artifactory only processed the first value for multi-value query parameters in HTTP requests to remote repositories.
RTDEV-54849	Repositories	Medium	Fixed an issue whereby the Artifactory API for creating a repository would create a Release Bundle repository instead of returning an error if an unknown or misspelled repository type was sent in the input.
RTDEV-54909	Repositories	High	Fixed an issue whereby a remote repository would remain offline even when it appeared to be back online.
RTDEV-54601	Repositories	Low	Fixed the following two issues related to using **Delete Content** on a repository: • When a user with delete permissions on a repository attempted to use **Delete Content** on the repository, the user was denied permission to delete. • When a project admin attempted to use **Delete Content** on a repository shared into a project, the project admin was denied permission to delete.
RTDEV-52751	Storage	Medium	Fixed an issue whereby the cache-fs synchronization process was stopped prematurely if an entry in the cache folder was inaccessible and resulted in the actual cache size being larger than the displayed cache size.
RTDEV-53825	Storage	Medium	Fixed an issue whereby when using Artifactory with S3 storage, enabling redirect download in the **binarystore.xml** file and setting **signedUrlExpirySeconds** to 0 or a negative value sometimes resulted in download failure.
RTDEV-54831	Storage	Low	Fixed an issue whereby when attempting to perform multipart upload with the wrong repository key, the upload would get stuck when getting the upload URLs and would not complete.
JA-13245	User Interface	Medium	Fixed an issue whereby a Crowd user would get an internal server error when trying to unlock a user profile with a dummy or incorrect password.
JA-15292	User Interface	Medium	Fixed an issue whereby there was no syntax validation for the OIDC provider URL.

JIRA Issue	Component	Severity	Description
RTFE-2445	User Interface	Low	Fixed an issue whereby when the "filter by" option was selected in the Artifactory Artifacts view, then switching from one project to another, the selection remained but Artifactory did not actually update the filter results as required to reflect the selected project.
RTFE-2543	User Interface	Medium	Fixed an issue whereby the Artifacts search window displayed erratic behavior when interacting with the drop-down menu and scroll bar.
RTFE-2577	User Interface	Low	Fixed an issue whereby when switching to compact mode on an expanded folder, an unexpected " file/folder not found" error was thrown, even though the file/folder did exist .
RTFE-2521	User Interface	Low	Fixed an issue whereby the option to select multiple versions to delete in the 'Delete Versions' feature was not available.

Artifactory 7.104

This section includes all the Artifactory 7.104 releases.

Critical Security Notice

All subversions are vulnerable to multiple non-critical security vulnerabilities that, in some deployments, can be chained into critical-severity attacks. We recommend that all customers upgrade to the latest version. View the latest Self-Managed and SaaS releases.

Artifactory 7.104.17 Self-Managed

Released: 29 June 2026

Resolved Issues

Jira Issue	Component	Severity	Description
RTDEV-90399	General	Critical	A high-severity vulnerability was fixed in Artifactory. In certain cases, deprecated services could allow a low-privileged user to retrieve artifacts from repositories they were not authorized to access. JFrog recommends that all self-managed customers upgrade to a fixed version as soon as possible, especially those with anonymous user access enabled.

Artifactory 7.104.16 Self-Managed

Released: 28 April 2026

This patch includes security bug fixes. Customers with Self-Managed deployments are strongly recommended to upgrade to the latest patch for this version.

CVEs Addressed

CVE	Component	Severity	Fix Description
CVE-2026-69107	General	Medium	Potential unauthorized artifact access in JFrog Artifactory

Artifactory 7.104.15 Self-Managed

Released: 9 April 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-56035	Storage	Low	Fixed an issue whereby Full Garbage Collection was working in only one thread.
RTDEV-55125	Federated Repositories	Low	Fixed an issue whereby when using the JMX exporter to see mBean metrics, errors were encountered.
RTDEV-55119	Federated Repositories	Medium	Fixed an issue whereby Artifactory initialization sometimes failed due to delays while Access checks if the customer has migrated to the Artifactory Federation Service (rtfs).
RTDEV-55275	General	Medium	Fixed an issue whereby when searching for artifacts using the underscore (_) , the underscore was considered a wildcard and lead to undesirable results. This has been changed so when using the underscore, it will be treated as an underscore character and not a wildcard.
RTDEV-55298	Repositories	Low	Fixed an issue whereby when trying to create a repository using the Create Repository Rest API without an "include pattern" in the input JSON, the repository was created with an empty string for the "include pattern" field.
RTDEV-55410	Release Lifecycle Management	Medium	Fixed an issue whereby when trying to append an artifact to an empty build via the API, an error was encountered.

Artifactory 7.104.14 Self-Managed

Released: 27 March 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-54891	Packages	Medium	Fixed an issue whereby 'symbols.nupkg' was getting indexed post calling reindex endpoint and then restarting the Artifactory instance.
RTDEV-52654	Packages	Medium	Fixed an issue whereby when the "Hide Existence of Unauthorized Resources" option was enabled on a local repository and Python packages were uploaded to a virtual repository associated with that local repository, a 400 error response was received instead of a 404 error response.
RTDEV-55754	Packages	High	Fixed an issue whereby when trying to override an image with the exact same image, by a user without delete permission, a 403 error was encountered.
RTDEV-53839	Packages	Critical	Fixed an issue whereby an unannounced change that was introduced by Conda Forge upstream impacts Artifactory's ability to resolve package metadata and dependencies with virtual Conda repositories.,

Artifactory 7.104.13 Self-Managed

Released: 24 March 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-51247	Packages	High	Fixed an issue that prevented locally-generated properties of various package types from being replicated.
RTDEV-55266	General	Medium	Fixed an issue whereby when trying to retrieve a repository from maven.oracle.com, a 404 Forbidden error was encountered.
RTDEV-50750	General	Medium	Fixed an issue whereby when a non-admin user using an include pattern would attempt to delete or overwrite a repository with an artifact in it that is already in the trash can, the action would fail.
JA-16503	General	Medium	Fixed an issue whereby when the Authentication provider name contained a space character it did not render the configuration page.
RTFE-2586	Packages	Medium	Fixed an issue whereby when in the Packages window and sorting by the security column, an error would be encountered.
RTDEV-55484	Packages	Medium	Fixed an issue whereby triggering the Recalculation Index on an empty Conan local repository resulted in

JIRA Issue	Component	Severity	Description
			an error, increased the Conan metadata stuck tasks, and all packages that were uploaded after the reindexing were not indexed.
RTDEV-54260	Packages	Medium	Fixed an issue whereby non-admin users were unable to create a Debian snapshot for a virtual repository.
RTDEV-53371	Packages	Medium	Fixed an issue whereby when configuring a NuGet Remote Repository targeting *community.chocolatey.org*, no metadata was cached when executing _the "_choco outdated" command.
RTDEV-54053	Repositories	Medium	Fixed an issue whereby the Artifactory traffic log v2 was logging every outgoing "put" request as a download, regardless of whether the request was successful or not.
RTFE-2579	User Interface (UI)	Medium	Fixed an issue whereby erratic behavior was encountered when making changes to artifact properties via the properties grid in the properties tab.
JA-13245	User Interface (UI)	Medium	Fixed an issue whereby a Crowd user would get an internal server error when trying to unlock a user profile with a dummy or incorrect password.

Artifactory 7.104.12 Self-Managed

Released: 12 March 2025

Feature Enhancements

- Maximum placed on bad checksum search responses

Responses to the Bad Checksum Search REST API are now limited to a maximum of 10,000 results.
- Permissions Added for Using Zapping Cache on Remote Repositories

The Zapping Cache action on remote repositories now requires **Manage** or **Delete** permissions, either via the UI or API. This change is backward-compatible. For more information on UI changes, click here, and for API changes, click here.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-54909	Repositories	High	Fixed an issue whereby a remote repository would remain offline even when it appeared to be back online.
RTDEV-53162	Packages	Medium	Fixed an issue whereby uploading a batch of pub packages sometimes resulted in missing versions within the generated metadata.

JIRA Issue	Component	Severity	Description
INST-10187	Installation	Medium	Fixed an issue where Nginx log rotation failed due to Supercronic not being installed correctly.
INST-9992	Installation	High	Upgraded `NodeJS` to version `22.14.0`.

Artifactory 7.104.10 Self-Managed

Released: 26 February 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-53694	General	Medium	Fixed an issue whereby calling the Create or Update Reverse Proxy Configuration API with invalid data led to a broken Artifactory configuration.
RTDEV-53268	Packages	Medium	Fixed an issue whereby users could not download NuGet packages from an upstream Beckhoff TwinCAT Package Manager repository through Artifactory.
RTFE-2714	Packages	Medium	Fixed an issue whereby when searching for packages and applying a filter, the page flickers and no results are displayed.

Artifactory 7.104.9 Self-Managed

Released: 20 February 2025

Known Issue in this Version

There is a known issue that causes an infinite loop when searching for packages by name in the top search bar on the Packages screen. Users should avoid installing this version and move directly to version 7.104.10.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-53694	General	Medium	Fixed an issue whereby calling the Create or Update Reverse Proxy Configuration API with invalid data led to a broken Artifactory configuration.
RTDEV-53268	Packages	Medium	Fixed an issue whereby users could not download NuGet packages from an upstream Beckhoff TwinCAT Package Manager repository through Artifactory.

Artifactory 7.104.7 Self-Managed

Released: 13 February 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-53840	Packages	Medium	Fixed an issue whereby when performing an Artifactory upgrade, repositories failed with a 400 response code.
MDL-483	General	High	Fixed an issue where, under certain circumstances, when running the `$JFROG_HOME/artifactory/var/data` and `$JFROG_H` located on different partitions (using mounted volumes), the One publish the supergraph, resulting in a failure during the Artifacto

Artifactory 7.104.6 Self-Managed

Released: 1 February 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-53839	Packages	Critical	Fixed an issue whereby an unannounced change that was introduced by Conda Forge upstream impacts Artifactory's ability to resolve package metadata and dependencies with virtual Conda repositories.

Artifactory 7.104.5 Self-Managed

Released: 29 January 2025

Important Announcements

- Updated Minimum System Requirements

To support the new services for our self-Managed customers, we have increased the minimum system resources required to run JFrog Artifactory.

> **Warning**
>
> Review the resources and make adjustments to your environment to ensure effective support for the new services in JFrog Artifactory. For more information, see System Requirements.

- Java 21 Compatibility

Artifactory now officially supports JDK 21. All Artifactory distributions are pre-packaged with JDK 21.

> **Breaking Change for Groovy**
>
> Java 21 is compatible with Groovy version 4.x, which includes several improvements and breaking changes compared to Groovy 3. If you have developed custom JFrog user plugins using Groovy, review your code and ensure it is compatible with Groovy 4.x.
>
> If you are using the Promotion User plugin, ensure that you are using the latest plugin version. For more information, see Upgrade Notice: Groovy 4 Compatibility.

Breaking Change for LDAP Authentication Rollback

Starting from Artifactory version 7.71.x, LDAP authentication has been moved to the Access Service.

The LDAP implementation on the Artifactory service will only work if the **Secure LDAP Search** (Poisoning Protection) feature is enabled. If you have rolled back to the previous implementation, you must remove this rollback. This will help you to avoid conflicts.

If you are using LDAP authentication via Access Service, you will not have any impact.

- **New Services - Topology and One Model**

We have added some new services for our Self-Managed instances:

JFrog Topology is a service registry that streamlines platform topology management. One Model is a service that acts as a centralized hub for all GraphQL APIs. This also includes a third-party service called Apollo Router.

For more information, see Artifactory Product.

- **New Validation for Creating and Updating Repositories**

There is a new validation for creating and updating repositories.

New Features

- **Evidence service**

JFrog's new Evidence service generates an audit trail that documents all the security, quality, and operational steps taken to produce a production-ready software release. It enriches artifacts, packages, builds, and Release Bundles with signed attestation metadata (based on the in-toto Attestation Framework) that can be tracked and verified easily for governance and compliance. The Evidence service enables you to seamlessly consolidate information from all the tools and platforms used in software development into a trusted single source of truth. It also integrates seamlessly with Release Lifecycle Management, providing a graphical interface for viewing the evidence generated at each stage of your SDLC.

Artifactory creates signed evidence automatically when Release Bundles are promoted and distributed. When used in conjunction with JFrog Xray, additional evidence is created in the form of SBOMs and vulnerability reports.

In addition, Enterprise+ users can attach externally-produced evidence to artifacts, packages, builds, and Release Bundles using the JFrog CLI.

For more information, see Evidence Management.

Important

The current release of the Evidence service is subject to the following limitations in Self-Managed environments:

- Kubernetes is required. Support for non-Kubernetes installations is planned for late Q1 2025.
- The Evidence service requires PostgreSQL 12 or later. (Please note that Artifactory can continue working with any supported database. There is no need to migrate Artifactory to PostgreSQL to support the Evidence service.)

- **Artifactory Federation Service**

To meet the growing needs of customers, JFrog has moved the Federated repositories feature into a standalone, multi-tenant service to ensure the timely synchronization of huge volumes of artifact metadata between customer sites. The new standalone service offers the following benefits:

- **Scalability**: The Federation service is designed from the ground up to grow as the needs of our customers grow.

- **Automatic Federation recovery**: The Federation service features an improved auto-healing mechanism that can identify synchronization problems between members due to an exhausted queue (a queue that has exceeded the maximum number of attempts to send metadata events to other members), reset the

failed events, and retry synchronization. This capability is particularly useful in the event a Full Sync operation is interrupted by a restart of one of the Artifactory instances that host a Federation member. For more information, see Federation Recovery and Auto-Healing.

- **Improved monitoring using the Federation dashboard**: The new Federation dashboard enables you to:

- Understand the health status of all your repository Federations at a glance. The dashboard makes it particularly easy to see how many repositories are in error or delayed. For more information, see View the Status of All Repository Federations.
- Drill down into a selected Federation to see the state of each member at a glance. For more information, see View the Status of a Selected Repository Federation.
- Give selected repositories priority to system resources to help ensure all their metadata events are synchronized with other Federation members. For more information, see Prioritize Federated Repository API.

> **Important**
>
> The current release of the standalone Artifactory Federation service is subject to the following limitations in Self-Managed environments:
>
> - Kubernetes is required. For more information, see Installing Artifactory Federation Service. Support for non-Kubernetes installations for early adopters is planned for late Q2 2025.
> - The Artifactory Federation service requires PostgreSQL 12 or later. (Please note that Artifactory can continue working with any supported database. There is no need to migrate Artifactory to PostgreSQL to support the Artifactory Federation service.)
> - Providing support for other databases is under consideration.

- **Using the Federation Comparison Tool on Federated Repositories**

Users who have the Artifactory Federation Service installed can use the Federation Comparison Tool to compare the state of a Federated repository with one or more remote members to detect missing artifacts in those remote members. This enables you to simulate the results of a Full Sync operation before you perform it. The Federation Comparison tool is invoked using a new query parameter in the Federated Repository Full Sync API. For more information, see Use the Federation Comparison Tool.

- **Machine Learning Repositories**

Machine Learning Repositories with the FrogML SDK is a local management framework tailored for machine learning projects, serving as a central storage for models and artifacts, featuring a robust version control system. It offers local repositories and an SDK for effortless model deployment and resolution.

Machine Learning Repositories offer the following benefits to your system:

- **Secure Storage:** Protect your proprietary information by deploying models and additional resources to Artifactory local repositories, giving you fine-grain control of the access to your models.

- **Easy Collaboration:** Share and manage your machine learning projects with your team efficiently.

- **Easy Version Control:** The Machine Learning Repositories SDK (FrogML) provides a user-friendly system to track changes to your projects. You can name, categorize (using namespaces), and keep track of different versions of your work.

For information on Machine Learning Repositories, click here.

- **Helm Enforce Layout**

Helm Enforce Layout is designed to maintain the integrity and organization of Helm charts within your repositories. It consists of two key functionalities that promote structure and reduce errors during deployments:

Preventing duplicate chart paths: Prevents the deployment of charts with the same name and version to different paths within the same repository, by ensuring that only a single instance of a chart is indexed. This maintains the integrity and accessibility of Helm charts, ensuring that users can easily identify and deploy the desired version without confusion. Enforcing chart names and versions: Ensures that the chart name and version specified in the packaged file name match the values in Chart.yaml and adhere to Semantic Versioning (SemVer)

standards adopted by the Helm official specification. Enforcing these rules promotes uniformity, allowing teams to adopt clear naming conventions that foster better collaboration and understanding of changes across different versions.

For more information on Helm Enforce Layout, click here.

> **Note**
>
> Helm Enforce Layout is forward-compatible only, it will not work on repositories created prior to Artifactory 7.104.2. This means that even if you upgrade to Artifactory 7.104.2, any repositories created prior to the upgrade are not compatible with this feature. Enforcement is set only upon repository creation.

- Cleanup Policies: Release Bundle v2

JFrog Cleanup Policies for Release Bundle v2 enable Platform and Project Administrators to define and customize policies based on specific criteria for removing unused Release Bundles across their JFrog platform. This provides optimal system performance. Administrators can customize a repeatable cleanup process that aligns with their organization's requirements by setting specific criteria and rules. For more information, refer to CLEANUP POLICIES API.

Feature Enhancements

- Packages and Repositories

- New REST API for Checking Repository Existence

A new REST API has been added to check whether a repository exists based on the project key and repository type. For more information, see the Check If Repository Exists API.

- Improvements to Conan Reindexing Speed on Large Repositories

The process for reindexing large Conan repositories has been optimized and is now half the time from what it was previously. Added Conan packages are available for indexing immediately even during the reindexing process.

- Added Clients for PyPI Repositories

PyPI repositories now support Poetry and Twine clients. For more information, click here.

- Updating multiple repositories using a batch request

It is now possible to update the configuration of multiple repositories using a single batch request. The request can contain a mixture of package types (for example, Docker and Maven) and repository types (for example, local and remote). For more information, see Update Multiple Repositories API.

- Viewing contents of Release Bundle v2 versions by package type

The window for viewing the contents of a Release Bundle v2 version has been redesigned to organize the contents according to package type. You can drill down from a package type to individual packages and from there, click a link to see the individual artifacts. For more information, see View the Contents of a Release Bundle v2 Version.

- Promoting Release Bundle v2 versions to virtual repositories

You can now promote a Release Bundle v2 version to a virtual repository, provided it contains at least one local repository assigned to the same environment as the virtual repository (or no environment at all). For more information about promotion, see Promote a Release Bundle v2 Version in the Platform UI.

- Virtual repositories can include repositories not assigned or shared to the same project

You can now edit a virtual repository configuration that contains local and remote repositories which are not assigned to, or shared with, the same project as the virtual repository. If such repositories are aggregated, a message appears in the UI. Click the button next to the message to display a list of these repositories. You can export this list to a CSV file. For more information, see Virtual Repositories and Projects.

Note

Users who can perform actions on the virtual repository (based on their assigned roles in the relevant project) are not automatically granted permissions to aggregated repositories not assigned or shared with the same project.

- Storage

- Improved Retry Mechanism for the google-storage-v2 Provider

The **google-storage-v2** provider now supports an improved retry mechanism when Google Cloud Storage returns 50x errors during binary download. The retry behavior is controlled by the `maxRetries` and `retryIntervalMillis` configuration parameters. For more information, click here.

- Improved Optimize System Storage REST API

The Optimize System Storage REST API now triggers the balancing mechanism immediately instead of raising a flag to indicate that Artifactory should run the balancing mechanism in the next Full Garbage Collection cycle. If balancing is already running, the API skips the process. For more information, see the Optimize System Storage REST API documentation.

- Release Lifecycle Management

- New Content tab in Release Lifecycle Management timeline

The Release Lifecycle Management timeline contains a new Content tab that lists the artifacts in the selected Release Bundle v2 version. For more information, see View the Contents of a Release Bundle v2 Version.

- Support for default key creation for Release Bundles v2 via REST API

It is now possible to create a Release Bundle v2 using the REST API without specifying an existing signing key. In such cases, Artifactory creates a default GPG key that is used to sign the Release Bundle. This default key is then used for future Release Bundles unless a different key is selected during Release Bundle creation. The default key created by Artifactory is displayed in the Keys Management table.

Note

In the current release, a default key is created only when creating the Release Bundle v2 using the REST API. It is still mandatory to select an existing signing key when using the JFrog CLI or platform UI.

- Support for default key creation for Release Bundles v2 in the platform UI

It is no longer mandatory to select a signing key when creating a Release Bundle v2 with the platform UI. If you do not select a key, Artifactory uses a default GPG key that it creates automatically. The default key is then used for future Release Bundles unless a different key is selected during Release Bundle creation. The default key created by Artifactory is displayed in the Keys Management table.

Note

Support for the default key will be added to the JFrog CLI in an upcoming release.

- Federated Repositories

- Performance enhancement for Federated repositories

A new system property enables event properties to be fetched in bulk from the database, which improves overall performance when mirroring among Federation members. For more information, see Configure Federated Repositories for Bulk Mirroring and Parallel Processing.

- Converting Federated repositories back to local

You can now convert a Federated repository back to a local repository using a REST API, provided it is not part of a Federation containing additional members. For more information, see Convert Federated Repository to a Local Repository API.

- **OCI and Docker Related Changes**

- **Enhanced Docker List Tags REST API Compatibility**

The Docker List Tags REST API has been enhanced to support both the full and shorthand conventions for referencing official Docker images. Users can now retrieve tags using either the complete path (including /library/) or the shorter version without it. For more information about the API see List Docker Tags API.

- **Enhanced Webhook Event Support for OCI and Docker Images**

In this release, the Webhook events functionality for Docker images has been expanded to include support for OCI repositories and images. These enhancements made include:

- **Support for OCI Repositories:** Webhook events can now be triggered for OCI repositories, broadening the integration capabilities.

- **Support for OCI Images:** Events related to OCI images are now fully supported, ensuring that actions on these images are captured.

- **New `image_type` Key:** A new `image_type` key has been added to the event action payload, indicating whether the action was performed on an OCI or Docker image.

For more information, click here.

- **Additional Keys Added to the Webhook Promoted Event in the Docker Domain**

The Image Promotion Webhook in the Docker domain has been expanded with two additional keys:

- **targetRepo:** The repository where the image is promoted to.

- **targetTag:** The new tag of the promoted image.

JFrog Platform

- **Setting upper limits on property updates**

A new system parameter has been introduced (**artifactory.max.artifacts.set.properties.recursive**) for setting an upper limit on the number of artifacts on which recursive property updates can be performed. For example, if you revise a folder property and the folder contains more items than the limit defined in this system parameter, the operation will fail. This property can be used to throttle the number of update requests, which can put a heavy load on the database and in extreme cases lead to crashes. By default, this feature is off. There is no default value when turned on.

- **Platform Chart 11.x Release**

We have released the JFrog Platform Helm Chart 11.x, which includes some of the important changes:

- *Removal of Insight and Pipelines*: We have removed the Insights and Pipelines chart dependencies from the JFrog Platform chart 11.x.
- *Upgrade of Bitnami PostgreSQL and RabbitMQ Helm Charts*: Upgraded the RabbitMQ chart version and the image version of PostgreSQL and RabbitMQ.

The JFrog Platform chart 11.x also includes multiple breaking changes. For more information, see Platform chart 11.x: Breaking Changes.

- **OIDC Multiple Token Scopes**

The Jfrog Platform now supports adding multiple scopes to OIDC identity mapping tokens, enabling you to use both user and group scopes for the same token.

- **Enabling SSO Disables Basic Authentication By Default**

Enabling single sign-on authentication now disables internal password authentication by default. For more information, see Disable Basic Authentication Method.

- **Improvements in Obtaining AQL Results**

The Search AQL API was improved such that AQL results are complete and not missing properties. A notification is now provided informing the client when the AQL limit has been reached.

- **Improved Performance for the Fetching Process**

Performance of the fetching process has been improved, based on the count of manifests relative to the Max Unique Tags configuration.

- **Cleanup Policies**

- **Terraform**: Terraform packages are now supported in Cleanup.

- **Terraform BE Packages** : Terraform BE packages are now supported in Cleanup and Archive.

- **CocoaPods**: CocoaPod packages are now supported in Cleanup.

- **Hugging Face**: Hugging Face packages are now supported in Cleanup.

- **OCI**: Helm OCI and OCI packages are now supported in Cleanup and Archive.

- **Cargo**: Cargo packages are now supported in Cleanup and Archive.

- **Frog ML**: Frog ML models are now supported in Cleanup and Archive.

- **Ansible**: Ansible packages are now supported in Cleanup and Archive.

- **Support for Scheduled Workers**

JFrog now supports creating scheduled workers to trigger at predefined times or intervals, which you can define using Cron expressions. Learn more

- **Worker Events**

- **Replication: Before Directory Replication** event is now supported.

- **Storage: After Copy** event is now supported.

- **Storage: After Property Delete** event is now supported.

- **Storage: After Property Create** event is now supported.

- **Storage:beforeCreate**: `beforeCreate` event is now supported.

- **Storage:beforeCopy**: `beforeCopy` event is now supported.

- **Before Build Info Save**: `Before Build Info Save` event is now supported.

- **Before Download Request**: `Before Download Request` event is now supported.

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-17217	Authentication Providers	Medium	Fixed an issue whereby the mTLS authentication was not working with an Edge license in Artifactory.
JA-15134	Authentication Providers	High	Fixed an issue whereby Oauth user was not able to login to Artifactory.
JA-14599	Authentication Providers	High	Fixed an issue to convert group names to lowercase during synchronization and resolve groups based on their external IDs.
JA-14625	Authentication Providers	Medium	Fixed an issue whereby the OAuth configuration in cloud instances incorrectly included the **Use Default Proxy Configuration** checkbox, which can only be used in on-prem environments.
JA-14560	Authentication Providers	Low	Fixed an issue whereby the LDAP settings got reordered when editing the settings.

JIRA Issue	Component	Severity	Description
JA-14557	Authentication Providers	Low	Fixed an issue whereby LDAP users had access to the 'Change Password' option in the Edit Profile page.
JA-14496	Authentication Providers	Medium	Fixed an issue whereby attempting to set up Azure OIDC integration with Artifactory resulted in an error message stating, "Failed to find public key matching the kid."
JA-14599	Authentication Providers	High	Fixed an issue to convert group names to lowercase during synchronization and resolve groups based on their external IDs.
RTDEV-48758	Builds	Medium	Fixed an issue whereby when creating a project, deleting it, and creating a new project with the same key as the deleted project, the build-info repository of the deleted project was not associated with the new project that has the same key.
RTDEV-49437	Builds	Medium	Fixed an issue whereby when clicking the build info link in the user interface for a VCS build, the link was inactive.
RTDEV-53064	Database	Medium	Fixed an issue whereby MariaDB JDBC driver 3.4.1 was not working with Artifactory 7.98.9 after upgrading from Artifactory 7.84.21.
JA-14805	Database	Low	Fixed an issue whereby duplicate resources existed during import and migration.
RTDEV-51529	Federated Repositories	Medium	Fixed an issue during pull replications that caused changes to property values to be added to existing property values on the target instead of overriding the existing values.
RTDEV-52453	Federated Repositories	Medium	Fixed an issue whereby a binary task was sometimes not created for a federated repository.
JA-15155	General	Medium	Fixed an issue where certain global roles could not be edited or were grayed out.
RTDEV-53176	General	Medium	Fixed an issue whereby Artifactory could not retrieve an artifact from a remote repository if there were square brackets "[]" in the artifact name.
RTDEV-51363	General	Medium	Fixed an issue whereby Apache Tomat version 10.1 that was bundled in Artifactory 7.98.7 contained an issue whereby when sending HEAD requests where the resource size was unknown, the server returned a content-length=0 header instead of omitting the header.

JIRA Issue	Component	Severity	Description
RTDEV-48398	General	Medium	Fixed an issue whereby the Multipart upload status API **/uploads/status** returned a 503 error message.
RTDEV-48039	General	Medium	Fixed an issue whereby the Permission Target and Groups did not appear under the Effective Permissions tab of a remote cache repository.
RTDEV-48522	General	Medium	Fixed an issue whereby after configuring an include/exclude pattern on a virtual repository, the pattern was not applied and items weren't included in the Artifact tree.
RTDEV-49088	General	Medium	Fixed an issue whereby when a user had permission to a repository that was aggregated to a virtual repository, the user was able to see repositories for which he did not have permission in the "Included Repositories" section of the virtual repository.
RTDEV-49236	General	Medium	Fixed an issue whereby the REST API for updating project and environment information for a repository did not update this information.
RTDEV-49231	General	Medium	Fixed an issue whereby after unused artifacts cleanup, empty folders in the remote-cache repository were not removed during the empty folder pruning global job.
JA-14648	General	High	Fixed an issue whereby permission targets having “per repository” patterns were not federated properly with Access Federation when having more than 2 repositories with patterns.
RTDEV-51199	General	Medium	Fixed an issue whereby when viewing a virtual repository in a tree browser, the message **This item is not cached.** appeared for an artifact in that repository even though it was cached.
RTDEV-50995	General	Medium	Fixed an issue whereby Artifactory was sending an empty project key instead of the default project key.
RTDEV-49625	General	Medium	Fixed an issue whereby internal users with “Disable Internal Password” enabled were getting password expiration emails.
INST-8369	Installation	Medium	Fixed an issue related to Helm installation whereby, the ‘cacheProviderDir’ and ‘maxCacheSize’ properties were swapped in the "google-storage-v2-direct" binarystore.xml template.
INST-7815	Installation	Medium	Fixed an issue whereby the router service was not shutting down gracefully before starting Tomcat.

JIRA Issue	Component	Severity	Description
INST-8592	Installation	Medium	Fixed an issue whereby the JVM configuration could not properly apply the `InitialRAMPercentage` and `MaxRAMPercentage` values because they were being overridden by `Xms` and `Xmx` settings.
INST-9172	Installation	Medium	Fixed an issue whereby the `pathType` for Artifactory ingress was hardcoded to `ImplementationSpecific`, preventing users from customizing it through `values.yaml`. This fix now allows users to utilize different types of ingresses effectively.
RTDEV-51535	Packages	Medium	Fixed an issue whereby it was not possible to download and install a Go nested module from a private GitLab using a Go remote repository, and when trying to do this it resulted in a 404 error.
RTDEV-50700	Packages	Medium	Fixed an issue whereby webhooks were not being triggered by the npm deprecate command.
RTDEV-50241	Packages	Medium	Fixed an issue where reindexing did not happen automatically after distributing a Release Bundle for Cocoapods.
RTDEV-50220	Packages	Medium	Fixed an issue whereby a Debian virtual repository was generating a packages metadata file in gz format when requested for a plain text file.
RTDEV-48779	Packages	Critical	Fixed an issue whereby in some packages, X-Artifactory-Xray-Origin: true was not returned correctly for blocked package, resulting in a wrong status code for smart remote repositories
RTDEV-49156	Packages	Medium	Fixed an issue whereby Xray failed to scan Hugging Face local models when the model ID was missing from the README file.
RTDEV-42940	Packages	Medium	Fixed an issue related to Cargo whereby, under certain circumstances, Artifactory failed to install a package from a local repository after copying it from a remote cache.
RTDEV-34149	Packages	Medium	Fixed an issue whereby, when pushing a multi-architecture layer that already exists in the system, Artifactory created a redundant appearance of the layer with its architecture name.
RTDEV-49462	Packages	Medium	Fixed an issue whereby when installing NuGet packages that contain a '+' in the version, the installation failed and 404 error messages were returned.

JIRA Issue	Component	Severity	Description
RTDEV-48638	Packages	Medium	Fixed an issue whereby when using Artifactory as a CDN, packages like PLCrashReporter with additional keys in the podspec 'source' field (alongside HTTP) could not be downloaded.
RTDEV-48363	Packages	Medium	Fixed an issue whereby when “Block unscanned artifacts” was selected in Xray’s policy and a package had violations, that package did not appear in the Packages list in Artifactory.
RTDEV-49017	Packages	Medium	Fixed an issue whereby the Cocoapods parser was only able to parse a podspec file when the file was started with 's' and was not able to read the file when it was starting with 'spec'.
RTDEV-49810	Packages	Medium	Fixed an issue whereby failure occurred when clicking Test Connection with OAUTH enabled and using an NPM Smart Remote Repository, and displayed a 500 error.
RTDEV-49228	Packages	Medium	Fixed an issue whereby it was not possible to publish an Ansible-Galaxy pre-release collection if it contained a hyphen in the file name.
RTDEV-49209	Packages	Medium	Fixed an issue whereby when running the group list command on a YUM/RPM virtual repository that contained both local and remote repositories, no groups were listed.
RTDEV-50095	Packages	High	Fixed an issue whereby when Artifactory is operating on Windows and a user attempted to deploy a Maven project, deployment failed.
RTDEV-50568	Packages	Medium	Fixed an issue with RPM packages, whereby if one of the *provides* versions was '-', indexing of the package failed.
RTDEV-50076	Packages	Low	Fixed an issue whereby, the **/npm/auth** endpoint did not return the user email when using an access token for authentication.
RTFE-2586	Packages	Medium	Fixed an issue whereby when in the Packages window and sorting by the security column, an error would be encountered.
JA-13448	Platform Management	High	Fixed an issue whereby unused licenses that were removed from the access configuration were not removed from the platform configuration.
JA-14796	Projects	Medium	Fixed an issue whereby deleting a project caused the read-only access of the shared repository to be reset for other projects as well.

JIRA Issue	Component	Severity	Description
RTDEV-50571	Release Lifecycle Management	Medium	Fixed an issue whereby, the REST API **Promote Release Bundle v2 Version** was missing the included repositories validation.
RTDEV-50824	Release Lifecycle Management	High	Fixed an issue that prevented a Release Bundle v2 from resolving dependencies located in a remote cache repository. Users must first copy the dependency artifacts from the remote cache repository to a local repository. When the Release Bundle is created, the dependency artifacts will be resolved with preference to the local repository instead of the remote cache repository.
RTDEV-49456	Repositories	Low	Fixed an issue whereby when trying to create a remote Gradle repository with the "Quick Repository Creation" option, the remote repository that was created was a Maven repository instead of Gradle.
RTDEV-49436	Repositories	Medium	Fixed an issue whereby the Smart Remote Repository options were automatically enabled even after disabling those options in the user interface.
RTDEV-49391	Repositories	Medium	Fixed an issue whereby users were unable to add an environment to an existing repository in the Repository Configuration page.
RTDEV-50682	Repositories	Medium	Fixed an issue whereby there was no option in the UI to disable the “List Remote Artifacts” option for Maven remote repositories.
RTDEV-49674	Storage	High	Fixed an issue whereby when Artifactory was configured with Cloudfront (AWS CDN), and a file larger than 50 GB was requested, the client received a 400 error.
RTDEV-48544	Storage	Medium	Fixed an issue whereby the API for getting a list of failed binary tasks would return a 200 status for non-existing repositories.
RTDEV-51525	User Interface	Medium	Fixed an issue whereby the trash can could not be disabled through the User Interface with a Pro license.
JA-15109	User Interface	High	Fixed an issue where the Manage Intergrations (Administration | General Management | Manage Integrations) page was unavailable in the UI for hybrid deployments with Edge license.

JIRA Issue	Component	Severity	Description
RTFE-2043	User Interface	Medium	Fixed an issue whereby when configuring a virtual repository, if a repository was the "Default Deployment Repository" and then was removed from the virtual repository, the removed repository remained as the "Default Deployment Repository".
RTFE-2579	User Interface	Medium	Fixed an issue whereby erratic behavior was encountered when making changes to artifact properties via the properties grid in the properties tab.
META-1854	User Interface	Medium	Fixed an issue whereby some of Digest IDs for Docker tags did not appear in the packages view in the Artifactory user interface.

Artifactory 7.98

This section includes all the Artifactory 7.98 releases.

Artifactory 7.98.19 Self-Managed

Released: 11 May 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-55754	Packages	High	Fixed an issue whereby when trying to override an image with the exact same image, by a user without delete permission, a 403 error was encountered.

Artifactory 7.98.18 Self-Managed

Released: 27 March 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-55754	Packages	High	Fixed an issue whereby when trying to override an image with the exact same image, by a user without delete permission, a 403 error was encountered.

Artifactory 7.98.17 Self-Managed

Released: 18 March 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-50656	Packages	High	Fixed an issue whereby NPM metadata request to a virtual repository can cause a DB query that will outcome with high database CPU.

Artifactory 7.98.15 Self-Managed

Released: 1 February 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-53839	Packages	Critical	Fixed an issue whereby an unannounced change that was introduced by Conda Forge upstream impacts Artifactory's ability to resolve package metadata and dependencies with virtual Conda repositories.

Artifactory 7.98.14 Self-Managed

Released: 21 January 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-15109	User Interface (UI)	High	Fixed an issue where the Manage Integrations (**Administration** | **General Management** | **Manage Integrations**) page was unavailable in the UI for hybrid deployments with Edge license.
JFUI-17059/JFUI-17173	User Interface (UI)	Medium	Fixed an issue where the navigation tour guide pop-up was displaying automatically. Since it was appearing multiple times for some users, we disabled the automatic display, and now it can only be triggered manually.

Artifactory 7.98.13 Self-Managed

Released: 6 January 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-52354	Packages	Medium	Fixed an issue whereby performing a publish with Swift Registry using the –metadata-path flag resulted in the metadata files being owned by the user rather than the system.

JIRA Issue	Component	Severity	Description
RTDEV-51525	User Interface (UI)	Medium	Fixed an issue whereby the trash can could not be disabled through the User Interface with a Pro license.
RTDEV-50700	Packages	Medium	Fixed an issue whereby webhooks were not being triggered by the npm deprecate command.
RTDEV-48039	General	Medium	Fixed an issue whereby the Permission Target and Groups did not appear under the Effective Permissions tab of a remote cache repository.

Artifactory 7.98.12 Self-Managed

Released: 24 December, 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-14796	Projects	Medium	Fixed an issue whereby deleting a project caused the read-only access of the shared repository to be reset for other projects as well.

Artifactory 7.98.11 Self-Managed

Released: 16 December 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-51529	Federated Repositories	Medium	Fixed an issue during pull replications that caused changes to property values to be added to existing property values on the target instead of overriding the existing values.
RTDEV-50398	General	High	Fixed an issue whereby downloads failed when coming from AWS and CloudFront cloud providers.
RTDEV-50824	Release Lifecycle Management	High	Background: Since a Release Bundle v2 cannot resolve dependencies located in a remote cache repository, users must first copy the dependency artifacts to a local repository. Fixed an issue during Release Bundle creation that prevented Artifactory from giving preference to the local repository that contains the dependencies instead of the remote cache repository.
JOBS-602	General	Low	Fixed an issue whereby the 403 error "No permissions to access the resource" was encountered when running

JIRA Issue	Component	Severity	Description
			"/observability/api/v1/metrics" with a metrics scoped token.

Known Issue with Pull Replications

There is a known issue whereby properties generated locally by Artifactory are deleted during pull replications when the properties are unchanged from the previous replication execution. The current workaround is to add a custom property to the package. This is sufficient to prevent the locally-generated properties from being deleted.

Artifactory 7.98.10 Self-Managed

Released: 9 December 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-51064	Federated Repositories	Medium	Fixed an issue where binary tasks were not being removed correctly when there was no binary present due to unneeded iterations over remote binary providers.
RTDEV-49625	General	Medium	Fixed an issue whereby internal users with "Disable Internal Password" enabled were getting password expiration emails.
RTDEV-49236	General	Medium	Fixed an issue whereby the REST API for updating project and environment information for a repository did not update this information.
JA-15004	Authentication Providers	Medium	Fixed an issue whereby users were unable to create OIDC integrations when using an ENT_PLUS_HYBRID license with Artifactory Edge on-premises instances.

Artifactory 7.98.9 Self-Managed

Released: 25 November 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-14560	Authentication Providers	Low	Fixed an issue whereby the LDAP settings got reordered when editing the settings.
JA-14557	Authentication Providers	Low	Fixed an issue whereby LDAP users had access to the **Change Password** option in the *Edit Profile* page.

JIRA Issue	Component	Severity	Description
RTDEV-46982	Federated Repositories	Medium	Fixed an issue whereby out-of-sync and exhausted Federations were presented as Federated in the Federation Sync Status page. These Federations are now given a status of Delayed.
RTDEV-49236	General	Medium	Fixed an issue whereby the REST API for updating project and environment information for a repository did not update this information.
JA-14648	General	High	Fixed an issue whereby permission targets having *per repository* patterns were not federated properly with Access Federation when having more than 2 repositories with patterns.
INST-9282	Installation	Medium	Fixed an issue where the `signedUrlExpirySeconds` parameter in the Artifactory Helm Chart defaults to false instead of being a number.
INST-9289	Installation	Medium	Fixed an issue where the attribute `encodedSolidusHandling=DECODE` goes missing in the `server.xml` file when Mission Control is enabled. The suggested workaround is not supported as the configuration is incorporated by default in `server.xml` file. For more information, see Known Issue (INST-9289).
INST-9333	Installation	Low	Fixed an issue where several secrets in the Evidence container of the Artifactory-HA Helm Chart are configured with `artifactory.fullname` instead of `artifactory-ha.fullname`.
INST-9286	Installation	Medium	Fixed an issue where the crontab file increases in size with every restart of the Nginx container in a Docker Compose installation, leading to storage issues.
RTDEV-49209	Packages	Medium	Fixed an issue whereby when running the group list command on a YUM/RPM virtual repository that contained both local and remote repositories, no groups were listed.

Artifactory 7.98.8 Self-Managed

Released: 6 November 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-48758	Builds	Medium	Fixed an issue whereby when creating a project, deleting it, and creating a new project with the same key as the deleted project, the build-info repository of the deleted project was not associated with the new project that has the same key.
RTDEV-49810	Packages	Medium	Fixed an issue whereby when clicking Test Connection with OAUTH enabled and using an NPM Smart Remote Repository failed, displaying error 500.
RTDEV-50095	Packages	High	Fixed an issue whereby when Artifactory was operating on Windows and a user attempted to deploy a Maven project, deployment failed.
RTFE-2043	User Interface (UI)	Medium	Fixed an issue whereby when configuring a virtual repository, if a repository was the "Default Deployment Repository" and then was removed from the virtual repository, the removed repository remained as the "Default Deployment Repository."
RTFE-2128	Repositories	Medium	Fixed an issue whereby when changing the “Metadata Retrieval Cache” value via the UI for Helm OCI remote, after saving the value was not changed.

Artifactory 7.98.7 Self-Managed

Released: 29 October 2024

Important Announcements

Note

Artifactory Release Notes Structural Update

The Artifactory Release Notes (that appear in the JFrog Release Notes) has been updated to separate the Self-Managed and SaaS Releases into separate areas. Self-Managed content for minor releases now lists aggregated bugs and features previously only reported as part of Cloud Releases. This enables users to better see content only relevant to their deployment type, and for Self-Managed users to more easily review the changes between versions, providing better visibility in preparation for upgrade.

Note

JFrog Workers Release Notes

We are pleased to announce that JFrog Workers is now in general availability with separate release notes, see JFrog Workers Release Information.

Classic Navigation Sunset

The classic navigation has reached its end of life, therefore users will no longer be able to switch back to the classic navigation. For more information about how navigation menus are organized, see JFrog Platform Navigation.

API Key Creation is Disabled

The creation of new API keys has now been disabled. You can use identity tokens instead, which replace API keys and offer enhanced security. The usage of API Keys will be disabled at the end of Q4 2024. For more information, see JFrog API Key Deprecation Process.

Breaking Change for Oracle 11 Users

Artifactory has replaced the Oracle-specific ROWNUM pseudo-column with the SQL-standard FETCH FIRST clause when generating AQL queries that include the ORDER BY clause. This change breaks compatibility with users of Oracle 11 and earlier (which are Oracle versions not officially supported by Artifactory).

Breaking Change when Using Get User Details API for Details of Non-Logged-In Users

When retrieving user details for non-logged-in users via the Rest API, a random date in the distant past was returned, now a `null` value will be returned. Previously, if a user never logged, in the response to the Get User Details API, the value of `last_logged_in` was `1970-01-01T00:00:00.000Z`. Now, if a user never logged in, the value of `last_logged_in` will be `null`.

Breaking Change for SAML SSO

As notified in SAML SSO configuration, if you have configured SAML authentication in your environment, make sure to configure a Custom Base URL to prevent a 500 error.

Known Issue in Tomcat 10.1

Apache Tomcat version 10.1 that is bundled in Artifactory 7.98.7 contains an issue whereby, when sending HEAD requests where the resource size is unknown, the server returns a `content-length=0` header, instead of omitting the header.

New Features

- Cleanup Policies

JFrog Cleanup Policies enable Platform and Project Administrators to define and customize policies based on specific criteria for removing unused binaries from across their JFrog platform. This provides control over storage utilization and ensures optimal system performance. By setting specific criteria and rules, administrators can customize a repeatable cleanup process that aligns with their organization's requirements. For more information, click here.

Also, this release includes a number of internal database indexing enhancements that improve performance during the cleanup process. JFrog recommends creating database indexes prior to upgrading, as explained in the article Database Index Optimizations for Improved Cleanup Policy Performance.

- Support for GitHub Enterprise in Self-Managed Environments

Users working in a Self-Managed environment can now select GitHub Enterprise as the Git provider for Go remote repositories. When using this option, you should configure the Go remote repository with the URL of the GitHub Enterprise server located at your site. This feature requires Enterprise Server 3.10 and above.

- Upgrade to Apache Tomcat 10.1.x

The Apache Tomcat version bundled with Artifactory has been upgraded to version 10.1.x.

- Support for Multi-Architecture Tag Deletion

Artifactory now supports deleting multi-architecture Docker and OCI image tags with one action. For more information, see Delete Multi-Architecture Docker Tags.

- Support for PostgreSQL 16

Artifactory is now certified to work with the PostgreSQL 16 database.

Feature Enhancements

- Significant Changes to the Packages User Interface

Significant changes have been made to the Packages User Interface (UI). From the Packages home page, you can now view a list of the most recently viewed packages, and an upgraded filter option has been added that allows you to create refined filters on the packages list to easily see the packages that interest you. After creating the filter, you can save it as a customized view for later use and reference. For more information, click here.

- Authentication Related Enhancements

- OpenID Connect Integration

The JFrog Platform now includes project support, multiple values, wildcard values, and dynamic mapping for OpenID Connect integrations. Project Admins can now create identity mappings associated with specific projects. Multiple values and wildcard values are now supported for JSON Claims in identity mappings associated with OpenID Connect Integrations. Identity mappings can contain dynamic mappings that support the verification or modification of a username or group name in the token subject based on a pattern.

- Multiple SAML SSO Provider Configurations

Starting from Artifactory version 7.98.7, the JFrog Platform now supports multiple configurations for SAML SSO providers. Enabling multiple SAML SSO configurations can help large organizations streamline the login and authentication processes for multiple platforms, resulting in a faster and more convenient authentication experience.

> **Note**
>
> Before creating multiple SAML configurations, JFrog recommends deleting the old configuration and reconfiguring it with a different setting name other than **Default**. If you reconfigure your SAML configuration, you must also update the relevant information in the Identity Provider server.

- Migration of SAML Authentication Provider from Artifactory Service to Access Service

As part of enhancements to the JFrog Access Service, which is becoming the primary service for authentication providers, the functionality for the SAML authentication provider has moved to the Access Service.

> **Breaking Change for synchronizeLdapGroups User Plugin**
>
> Following the migration of SAML SSO from Artifactory service to Access service, the deprecated user plugin `synchronizeLdapGroups` will no longer be used for SAML SSO user login. As an alternative, the functionality of the plugin has been implemented as part of the provider. For more information, see Enabling Synchronization of LDAP Groups for SAML SSO.

- Temporary Login Suspension Moved to Access Service

As part of enhancements to the JFrog Access Service, which is becoming the primary service for authentication and authorization, the implementation of Temporary Login Suspension has been moved to the Access Service starting from Artifactory version 7.98.x. For more information, see User Lock and Login Suspension.

- Proxy support for OAuth Authentication Provider

The OAuth authentication provider now supports the platform default proxy. To enable this functionality, select the **Use Default Proxy Configuration** checkbox in the Provider Settings section.

- Support for OIDC Forward Proxy Configuration

The JFrog Platform OIDC integration now supports the configuration of a forward proxy. For more information, see Manage Proxy Servers.

- Release Bundles Enhancements

- **Cannot modify or delete files that belong to a promoted Release Bundle v2**

To protect the immutability of Release Bundle v2, users are now blocked from modifying or deleting a file that belongs to a promoted Release Bundle. Users must first delete the promotion or delete the Release Bundle version altogether before the files can be modified or deleted.

- **Release Bundles v2 protected from expired GPG keys**

When a user attempts to create, promote, or distribute a Release Bundle v2 version, the action is now blocked if the GPG key has expired.

- **Adding pagination to Release Bundle v2 Version Details REST API**

The Get Release Bundle v2 Version Details REST API now includes the ability to paginate the results using the `offset` and `limit` query parameters. In addition, the response now includes the `total_artifacts_count`.

- **Improved UI for deleting Release Bundle v2 versions and promotions**

The UI offers improved options for deleting Release Bundle v2 versions and promotions, including versions distributed to Edge nodes.

- **Federated Repository Related Enhancements**

- **Improved Federated Repository validation**

There is an improved validation check when creating Federated repositories that provides a clear error message if a Federated repository with the same name already exists on a different Federation member.

- **Federation recovery and auto-healing of binary tasks**

The auto-healing mechanism used by Artifactory to recover synchronization of metadata events among repository Federation members now includes support for binary tasks as well. The mechanism will check periodically for any binary tasks that are in a retry or error state and use the checksum to identify whether the file was deleted from its source. If the binary was deleted, the task is deleted.

- **Change to Federated Repository Artifactory System Parameter**:

- Old name (7.90.5): `artifactory.federated.mirror.events.metadata.enabled`
- New name (7.92.3 and above): `artifactory.federated.mirror.events.upload.info.propagate.enabled`

- **Cargo Related Enhancements**

- **Cargo `index/config.json` REST API Aligned with the Cargo Specs**

The Cargo index/config.json REST API has been aligned to the Cargo specs so that it now returns a response even if a user has no permissions on a repository and invokes an auth-challenge.

- **Improved Cargo Status Code Responses**

Cargo status code responses are now aligned with the cargo registry according to the Cargo specification.

- **Improvements to authenticated requests on Cargo repositories**

Authenticated requests on Cargo repositories are now allowed with anonymous access.

- **Hugging Face Related Enhancements**

- **The Hugging Face `readme.md` file is now accessible**

The Hugging Face `readme.md` file can now be viewed with an MD viewer for Hugging Face packages.

- **Support for Hugging Face Modifying Deployment Expiration**

Artifactory now supports using a system property to modify the expiration time for models and datasets deployment, so that you can upload larger models without encountering errors.

- **Projects Support for Webhooks**

Artifactory now supports creating and viewing webhooks associated with a specific project.

- **Artifactory Performance Improvement**

This version includes improvements in response time with a reduction of up to 12%. This results in an overall improvement in performance.

- **Added option to configure an absolute path for tempDir for certain binary providers**

It is now possible to configure an absolute path for tempDir (_pre folder) for the following binary providers: cache-fs, s3-storage-v3, azure-blob-storage-v2, and file-system (or state-aware when using sharding). Before this change, tempDir was always relative to the baseDataDir, and if tempDir had an absolute path in `binarystore.xml` (for example: `/tmp`), tempDir was set to `$BASEDATADIR/filestore/tmp`. Now, it will be set to `/tmp`, which will be a breaking change. To revert to the old behavior, use a relative path "`tmp`". Configuring an absolute path allows for improved performance when baseDataDir is located in a NFS.

- **Reduced Calls to the Database When Interacting with Virtual Generic Repositories**

The number of calls to the database was significantly reduced when interacting with a virtual generic repository containing more than 3 sub-repositories, which results in improved system performance.

- **Logging Outgoing Requests**

Introduced logging for outgoing requests in the JFConnect service to enhance debugging capabilities.

- **Significant Improvements in Deploying Artifacts from Archives**

The Deploy Artifacts from Archive REST API now supports deploying artifacts in parallel threads as well as sequentially, significantly reducing the time it takes to deploy. For more information, see Deploy Artifacts from Archive API.

- **Improved Failure Retry Mechanism When Working With Google Cloud Storage**

The `google-storage-v2` provider now supports an improved retry mechanism when Google Cloud Storage returns 50x errors. Two new parameters have been added to the provider (`maxRetries` and `retryIntervalMillis`) to allow configuring this. For more information, click here.

- **List Docker Images REST API Performance Improvements**

The REST API List Docker Images now delivers faster results and uses less resources. For more information, see List Docker Images API.

- **Support for PyPI Etag Headers**

Artifactory now supports Etag headers for Pypi Package Indexes, minimizing the bandwidth used for installation flows.

- **Table of public keys now includes the key type**

The table of public keys available to administrators in the Public Keys tab of the Keys Management window now includes the key type. For more information, see Manage Public Keys.

- **Tree Browser Performance Improvements**

The following performance improvements were made in the artifacts tree/native browser. For information on this change and why the **List Remote Folder Items** function is turned off by default, see Why Remote Folder Listing Is No Longer Available:

Expanding a folder with a long list of artifacts is now much faster. The displayed list of artifacts is now limited to a maximum of 20K. Artifacts that are not displayed are accessible through the Search. Display of repository and artifact details is now faster

- **Improvements to Metadata Retrieval Performance** Performance of metadata retrieval was improved following recent changes made to the npm client.

- **Improvements to Tree Browser Performance**

For users with limited permissions, loading the list of repositories at the root level of the tree browser is now much faster

Improvements were made to tree browser performance such that the time it takes to list artifacts from remote repositories was significantly reduced. For more information, see Why Remote Folder Listing Is No Longer Available.

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-14175	Authentication Providers	Medium	Fixed an issue whereby the Crowd login failed when the Crowd server was unavailable during Artifactory restart. It may take a few minutes for the Crowd login to become available once the Crowd server restarts.
JA-14274	Authentication Providers	High	Fixed an issue whereby, when mTLS is enabled in Artifactory and the Router port (8082) is accessed, the mTLS user is not created in the Artifactory users list. However, the user is created when accessing the Artifactory port (8081).
JA-14426	Authentication Providers	Normal	Fixed an issue whereby encrypted passwords could not be created for SAML users.
JA-14599	Authentication Providers	High	Fixed an issue to convert group names to lowercase during synchronization and resolve groups based on their external IDs.
RTDEV-44073	Authentication Providers	Medium	Fixed an issue whereby downloading artifacts using an identity token or reference token from Maven virtual repositories with “Force Authentication” enabled and anonymous access enabled resulted in “401 Unauthorized” errors.
EVT-1211	Builds	Medium	Fixed an issue whereby selecting the Any Build checkbox in the UI caused the complete list of builds to be injected instead of simply setting the **anyBuild** parameter to **true**.
RTDEV-47671	Builds	Low	Fixed an issue whereby build promotion failed when the same artifact was used in the build more than once.
RTFE-1665	Builds	Medium	Fixed an issue whereby, users were unable to select text in the table of published modules for the artifacts under the **Build** tab in the JFrog Platform UI.
RTDEV-41201	Database	Medium	Fixed an issue where Artifactory failed to verify the signatures of the signed repository when working with Debian packages and displayed an error.
RTDEV-41232	Database	Medium	Fixed an issue whereby when Artifactory runs with an Oracle database, database conversion errors occur when creating new indexes.
RTDEV-45055	Federated Repositories	Medium	Fixed an issue that caused the keys for local repositories (for example, RPM) to become unavailable after converting the repositories to Federated repositories.

JIRA Issue	Component	Severity	Description
RTDEV-48547	Federated Repositories	Medium	Fixed an issue where the pairing token was using base URL for federated repo binding end point instead of federated base URL.
EVT-1211	General	Normal	Fixed an issue whereby, selecting the **Any Build** checkbox in the UI caused the complete list of builds to be injected instead of simply setting the `anyBuild` parameter to `true`.
JA-14046	General	Medium	Fixed an issue whereby OIDC token exchange failed after key rotation.
JA-14247	General	Normal	Fixed an issue where in some cases the modified timestamp was not being updated when an existing permission was modified, causing issues with the federation sync events.
JA-14387	General	Medium	Fixed an issue whereby when creating a new OIDC integration with a name that is a prefix of an existing integration, all the mappings from the existing integration were automatically copied over to the new integration.
JFCON-986	General	Normal	Fixed an issue where JFConnect was unable to read certificates from the TRUSTED folder.
RTDEV-45910	General	Medium	Fixed an issue whereby slowness with the `/auth/current` endpoint was causing rendering issues.
RTDEV-46817	General	Medium	Fixed an issue whereby when a storage quota notification could not be sent to a project admin because there was no email address for the project admin, the notification was also not sent to other project members who did have email addresses.
RTDEV-47455	General	Medium	Fixed an issue whereby certain RPM Packages were not listed in a remote repository when pointing to the Rockylinux registry.
RTDEV-47968	General	High	Fixed an issue whereby after upgrading to 7.90.9, users could not retrieve the latest artifact and would receive a '404 file not found' error.
RTDEV-48199	General	Medium	Fixed an issue whereby requests reaching Artifactory that contained no headers or null values returned a 500 error and “java.lang.NullPointerException” appeared in Tomcat logs.
RTDEV-48398	General	Medium	Fixed an issue whereby the Multipart upload status API **/uploads/status** returned a 503 error message.

JIRA Issue	Component	Severity	Description
RTFE-1502	General	Medium	Fixed an issue whereby when setting an artifact property that includes a URL as the value, the property value did not appear in the user interface.
RTDEV-46500	General	High	Fixed an issue whereby downloading files containing '%' in the filename caused UI Errors.
RTDEV-48443	General	Medium	Fixed an issue whereby, items were not displayed in a native browser in virtual repositories but were displayed in a native browser in local repositories.
INST-6822	Installation	Medium	Fixed an issue whereby Artifactory failed to identify an application running inside a container while using Kubernetes clusters without a Docker engine.
INST-8061	Installation	Medium	Fixed an issue whereby the `artifactory-ha` chart had hard-corded values of `--max-time` 1 for `livenessProbe` and `startupProbe`.
RTDEV-33287	Packages	Low	Fixed an issue related to Conan whereby, when creating a user without read permissions the user was able to view search results instead of receiving a 404 error.
RTDEV-44330	Packages	Medium	Fixed an issue related to Conda whereby, under certain circumstances, users could access the full metadata from a virtual repository even if they did not have the appropriate permissions.
RTDEV-45528	Packages	High	Fixed an issue whereby, attempting to download a model or dataset with a letter case that does not match the exact case as in huggingface.co, failed to download.
RTDEV-45666	Packages	Medium	Fixed an issue related to Cocoapods whereby, Artifactory installed certain packages via a remote repository but then did not support subsequent installations.
RTDEV-46304	Packages	Medium	Fixed an issue where Terraform anonymous requests were causing 401 errors for other anonymous requests that were made during the same time period.
RTDEV-46343	Packages	Medium	Fixed an issue whereby Artifactory's "reject invalid jars" feature was incorrectly rejecting archives with a payload before the zip structure.
RTDEV-46661	Packages	Critical	Fixed an issue where the blob upload range header returned the wrong byte size. This resulted in a malformed `manifest.json` file and caused the error "failed to read expected number of bytes:

JIRA Issue	Component	Severity	Description
			unexpected EOF" when pulling the image using containerd.
RTDEV-46682	Packages	Medium	Fixed a status code response for Cargo smart remote repositories.
RTDEV-47144	Packages	Low	Fixed an issue whereby when attempting to download an artifact from a VCS remote repository in Artifactory with an `exclude/include` pattern set, the download request failed with a 404 Not Found error but the error message did not state that the artifact was not downloaded due to the `exclude/include` pattern.
RTDEV-47286	Packages	Medium	Fixed an internal logging issue with PyPI metadata uploads.
RTDEV-47967	Packages	Medium	Fixed an issue whereby installation of Hugging Face modules was not working when using smart repository configuration.
RTDEV-48273	Packages	Medium	Fixed an issue whereby default features in `Cargo.toml` files were overwritten as true when the JSON file was deleted from the .cargo folder in the repository.
RTDEV-48822	Packages	Medium	Fixed an issue whereby the npm package indexing would fail after upload when the Xray setting to block the download of unscanned artifacts was enabled.
RTFE-1260	Packages	Medium	Fixed an issue whereby, when sorting package versions according to the modified timestamp in the Packages page in the JFrog Platform WebUI, when there were over 100 versions of the same package, Artifactory did not perform as expected.
RTFE-1790	Packages	Medium	Fixed an issue whereby the command to install a Go package on the Package Version Details was incorrect.
RTDEV-44299	Packages	Medium	Fixed an issue whereby search results in virtual repositories were not sorted by relevance.
RTDEV-46051	Packages	Medium	Fixed an issue related to CRAN whereby, when trying to install local packages from a virtual repository using the R client, Artifactory returned an error.
RTDEV-46298	Packages	Low	Fixed an issue whereby the Artifactory webhook did not trigger an event for `list.manifest.json` after pushing a multi-arch Docker image.

JIRA Issue	Component	Severity	Description
RTDEV-46647	Packages	Medium	Fixed an issue whereby a Go remote repository was not able to proxy Go providers with package versions similar to v2.0.0-beta.1.
RTDEV-46766	Packages	Medium	Fixed an issue whereby Artifactory returned a 400 error for a valid tag in certain circumstances when using the Docker Promote REST API to promote a Docker image.
RTDEV-48144	Packages	Medium	Fixed an issue whereby a Yum virtual repository was unable to merge data from its repositories when one of the repositories specified the location of index files in `repomd.xml` using end tags instead of self-closing tags.
JFMC-5431	Platform management	Low	Fixed an issue where the Register Platform Deployment page displayed unclear error messages and presented confusing UI behavior when an invalid URL was used for the connection. Following this fix, registering legacy instances (version 6.x and below) is no longer supported in the web UI and can only be done using the Add JPD REST API.
JFMC-5764	Platform management	Medium	Fixed an issue whereby when Mission Control tries to prepare a database request as part of its monitoring work, an SQL error occurs. This error (`RunTime SQLException`) causes the monitoring jobs to stop functioning properly.
JA-14163	Platform Management	Medium	Fixed an issue whereby when retrieving user details for non-logged-in users via the Rest API, a random date was returned for the time of the last login. Now **null** is returned for a non-logged-in user.
JA-13470	Platform Management	Medium	Fixed an issue whereby the Access REST API returned a "403 Forbidden" error when attempting to delete an AWS IAM Role.
JA-13994	Projects	Medium	Fixed an issue whereby moving a repository using the Move Repository REST API caused users with read-only permissions to lose access to that repository.
RTDEV-45671	Release Lifecycle Management	Medium	Fixed an issue whereby long usernames caused an error when creating a Release Bundle v2. Artifactory now truncates the username to 64 characters and saves the truncated name to its database.
RTDEV-43590	Repositories	Medium	Fixed an issue whereby the cleanup of unused cached artifacts was deleting configuration files in remote repositories.

JIRA Issue	Component	Severity	Description
RTDEV-44724	Repositories	Medium	Fixed an issue that allowed users to migrate system repositories to Federated repositories.
RTDEV-46832	Repositories	High	Fixed an issue whereby cleanup cron jobs were causing Out-of-Memory crashes in Artifactory.
RTDEV-47642	Repositories	Medium	Fixed an issue where when using Terraform with remote Terraform repositories and anonymous access enabled, permissions did not behave as expected. This may impact users ability to access these repositories.
RTFE-1593	Repositories	Medium	Fixed an issue related to Helm OCI whereby, the repositories were not displayed on the Repositories page in the JFrog Platform WebUI Administration module as expected.
RTFE-1940	Repositories	Medium	Fixed an issue whereby the Set Me Up page showed the wrong URL for Docker repositories with a sub-domain method configured in SaaS.
RTDEV-44388	Repositories	Low	Fixed an issue whereby when attempting to update includePatterns to an empty string using the REST API, the operation reverted to the default value instead of removing the pattern entirely.
RTDEV-44694	Repositories	Medium	Fixed an issue related to Smart Remote repositories whereby, when enabling the **Propagate Query Params** setting and then updating the repository, Artifactory saved the '?trace' report as an artifact and saved this report as a cached file regardless of the valid response status.
RTDEV-39831	Storage	Medium	Fixed a bug where upload failed when using mixed storage types filesystem and s3 in the same Sharding configuration.
RTDEV-46671	Storage	High	Fixed an issue related to S3 Cold Storage whereby Artifactory failed to move packages to the Glacier Tier.
RTFE-1908	User Interface	Medium	Fixed an issue whereby users could not access the Artifactory Artifacts tab when upgrading to a new Artifactory version.
RTFE-1918	User Interface	Medium	Fixed an issue whereby the Set Me Up page would get stuck when clicking **Generate Token & Create Instructions**.

JIRA Issue	Component	Severity	Description
RTDEV-44363	User Interface	Medium	Fixed an issue whereby when a user navigated in the native browser UI to view or download artifacts that are in ZIP files without folders, the system returned a “404 item does not exist” error.
RTFE-1736	User Interface	Low	Fixed an issue whereby the **Configure** tab did not appear in the Set Me Up instructions for certain repositories for SAML users.
RTFE-1614	User Interface (UI)	Medium	Fixed an issue related to Docker whereby, when trying to view image information on the Packages page on the JFrog Platform WebUI, Artifactory returned an error.
RTFE-1748	User Interface (UI)	Medium	Fixed an issue with the Artifactory native browser whereby, when clicking **Load More** in the WebUI, there was a missing trailing slash (/) after the `recordNum` parameter in the request URL.
RTFE-1721	User Interface (UI)	Low	Fixed an issue related to the Tree Browser repositories search input textbox, whereby, when writing unnecessary spaces in the search input, Artifactory did not remove the white spaces from the query string and returned an empty result.
JA-13021	User Management	High	Fixed an issue whereby password-less access to EKS did not work with AWS GovCloud.
JA-13226	User Management	Critical	Fixed an issue where a disabled user can change his/her status to locked when trying to login to Artifactory multiple times.

Artifactory 7.90

This section includes all the Artifactory 7.90 releases.

Artifactory 7.90.19 Self-Managed

Released: 2 February 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-53839	Packages	Critical	Fixed an issue whereby an unannounced change that was introduced by Conda Forge upstream impacts Artifactory's ability to resolve package metadata and dependencies with virtual Conda repositories.

Artifactory 7.90.17 Self-Managed

Released: 25 November, 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-49462	Packages	Medium	Fixed an issue related to Nuget whereby, under certain circumstances, a 404 error was returned during package installation. The fix is disabled by default and can be controlled through Artifactory System Properties.

Artifactory 7.90.15 Self-Managed

Released: 21 October 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTFE-1918	User Interface (UI)	Medium	Fixed an issue whereby the Set Me Up page would get stuck when clicking on “Generate Token & Create Instructions.”
RTFE-1908	User Interface (UI)	Medium	Fixed an issue whereby users could not access the Artifactory > Artifacts tab when upgrading to a new Artifactory version.
RTFE-1790	Packages	Medium	Fixed an issue whereby the command to install a Go package on the Package Version Details was incorrect.
RTFE-1486	General	Medium	Fixed an issue whereby in the artifact tree under the Docker repository, the Layers Visualization section is empty and didn't display the entire set of commands used to generate the selected tag.

Artifactory 7.90.14 Self-Managed

Released: 8 October, 2024

> **Warning**
>
> When upgrading to Artifactory 7.90.14 from a previous version, API Key creation is enabled, even if you had disabled API Key creation in the previous version.

Feature Enhancements

- Cargo index/config.json API Aligned with the Cargo Specs

The Cargo index/config.json API has been aligned to the Cargo specs so that it now returns a response even if a user has no permissions on a repository and invokes an auth-challenge.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-48779	Packages	Critical	Fixed an issue where in some packages, X-Artifactory-Xray-Origin: true was not returned correctly for blocked package, resulting in a wrong status code for smart remote repositories.
RTDEV-48547	Federated Repositories	Medium	Fixed an issue where the pairing token was using base URL for federated repo binding end point instead of federated base URL
RTDEV-48443	General	Medium	Fixed an issue whereby items were not displayed in a native browser in virtual repositories but were displayed in a native browser in local repositories.
RTDEV-48100	General	High	Fixed an issue whereby clicking an artifact and selecting Show in Tree / Direct URL" was not working as expected.
JOBS-559	General	Normal	Fixed an issue whereby, the `# UPDATED` tag was removed from the OpenMetrics response in Artifactory as it was not aligned with the OpenMetrics spec.

Artifactory 7.90.13 Self-Managed

Released: 25 September, 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-48199	General	Medium	Fixed an issue whereby requests reaching Artifactory that contained no headers or null values returned a 500 error and “java.lang.NullPointerException” appeared in Tomcat logs.
RTDEV-47968	General	High	Fixed an issue whereby after upgrading to 7.90.9, users couldn't retrieve the latest artifact and would receive a '404 file not found' error.
RTDEV-47671	Builds	Low	Fixed an issue whereby build promotion failed when the same artifact was used in the build more than once. Note that this fix changes the default behavior and may result in Build Publish Info failing with an error if it contains duplicate artifacts. This behavior can be turned off starting with Artifactory 7.90.15 by setting the flag `artifactory.build.block.duplicate.entries` to `false`. For more information see the issue RTDEV-47671 in Artifactory 7.90.
RTFE-1831	General	Medium	Fixed an issue whereby entering credentials into Set Me Up, logging in using the instructions provided didn’t work

JIRA Issue	Component	Severity	Description
			as the encoding of username and password wasn't working properly.

Artifactory 7.90.10 Self-Managed

Released: 11 September, 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-46298	Packages	Low	Fixed an issue whereby the Artifactory webhook did not trigger an event for **list.manifest.json** after pushing a multi-arch Docker image.
JA-13470	Platform Management	Medium	Fixed an issue whereby the Access REST API returned a 403 Forbidden error when attempting to delete an AWS IAM Role.
RTDEV-46343	Packages	Medium	Fixed an issue whereby Artifactory's "reject invalid jars" feature was incorrectly rejecting archives with a payload before the zip structure.
RTDEV-45910	General	Medium	Fixed an issue whereby slowness with the **/auth/current** endpoint was causing rendering issues.
RTFE-1412	Repositories	Medium	Fixed an issue whereby "Set me up" for Docker repositories did not generate the correct docker login URL as required per docker access methods.
INST-8978	Installation	High	Fixed an issue whereby, the **tomcat/lib** directory was incorrectly placed in **bootstrap/artifactory/access/tomcat/lib** instead of **bootstrap/artifactory/tomcat/lib.**
INST-8700	Installation	Medium	Fixed an issue whereby, under certain circumstances, when running an Artifactory non-containerized installation with a container engine available on the same virtual machine, the **isRunningInsideAContainer** function falsely identified the installation as in a container, which resulted in Artifactory startup failure.

Artifactory 7.90.9 Self-Managed

Released: 28 August, 2024

Feature Enhancements

- **Performance Improvements**

The following performance improvements were made in the artifacts tree/native browser:

For users with limited permissions, loading the list of repositories at the root level of the tree browser is now much faster Expanding a folder with a long list of artifacts is now much faster. The displayed list of artifacts is now

limited to a maximum of 20K. Artifacts that are not displayed are accessible through the Search

- Display of repository and artifact details is now faster

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-46858	Storage	High	Fixed an issue whereby redirect signed URLs were not working when using the cluster-sharding provider with a cloud provider in the binarystore chain and templates such as: cluster-s3-storage-v3, cluster-google-storage-v2 and cluster-azure-blob-storage-v2.
RTDEV-46766	Packages	Medium	Fixed an issue related to Docker whereby, under certain circumstances, when using the Docker Promote REST API to promote a Docker image, Artifactory didn't follow the OCI distribution specification when retagging valid tags.
RTDEV-46500	General	High	Fixed an issue whereby downloading files containing '%' in the filename caused UI errors.
RTDEV-44694	Repositories	Medium	Fixed an issue related to Smart Remote repositories whereby, when enabling the Propagate Query Params setting and then updating the repository, Artifactory saved the '?trace' report as an artifact and saved this report as a cached file regardless of the valid response status.
RTDEV-45055	Federated Repositories	Medium	Fixed an issue that caused the keys for local repositories (for example, RPM) to become unavailable after converting the repositories to Federated repositories.
RTDEV-46832	Repositories	High	Fixed an issue that caused out-of-memory crashes due to Artifactory cleanup cron jobs.
JA-13994	Projects	High	Fixed an issue whereby, when moving a repository using the Move Repository REST API, users with read-only permissions lost access to that repository.

Artifactory 7.90.8 Self-Managed

Released: 14 August, 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-44073	Authentication Providers	Medium	Fixed an issue whereby downloading artifacts using an identity token or reference token from Maven virtual repositories with "Force Authentication" enabled and anonymous access enabled resulted in "401 Unauthorized" errors.

JIRA Issue	Component	Severity	Description
RTDEV-46671	Storage	High	Fixed an issue whereby S3 Cold storage failed to put binaries in the Glacier Tier.
RTDEV-46659	Storage	High	Fixed the following issues: • When redirecting to S3, downloads were served directly from Artifactory instead of the S3 bucket. • When using CloudFront, redirect failed and download did not work.

Artifactory 7.90.7 Self-Managed

Released: 9 August, 2024

New Feature

- Deploy Large Files Using Multi-Part Upload

Artifactory now implements a fast and reliable multi-part upload approach for large files with the JFrog CLI. The new multi-part upload is designed so that in the case of an upload failure a retry mechanism resumes uploads from the point of failure, thus preserving all content that was uploaded before the failure. In contrast, with the standard upload, an upload failure will result in the loss of all data and require a restart from the beginning.

Multi-part Upload is available using S3 and GCP storage types. The default value for the minimum file size requiring multi-part upload is 200 MB, although this value can be changed. For more information, click here.

Change to Existing Feature

The system property for synchronizing metadata in Federated repositories (introduced in release 7.90.5) has been renamed:

- Old name (7.90.5 & 7.90.6): `artifactory.federated.mirror.events.metadata.enabled`
- New name (7.90.7 and above): `artifactory.federated.mirror.events.upload.info.propagate.enabled`

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-46304	Packages	Critical	Fixed an issue where Terraform anonymous requests were causing 401 errors for other anonymous requests that were made during the same time period.
RTDEV-45842	Installation	High	Fixed an issue whereby Upgrading self-managed deployments from version 7.71 directly to 7.90.5 and 7.90.6 failed due to a problematic Artifactory revision number.

Artifactory 7.90.6 Self-Managed

Released: 05 August, 2024

Known Issue in this Version

Artifactory version 7.90.6 has an issue that affects Pub package deployments due to a Tomcat upgrade. To avoid this issue, customers are advised to upgrade to Artifactory 7.90.7. For more information, see Artifactory Known Issues.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-45824	General	Critical	Fixed an improper path validation issue that could potentially lead to cache poisoning.
RTDEV-45626	General	High	Fixed an improper token validation issue that could potentially lead to privilege escalation.
RTDEV-41232	Database	Medium	Fixed an issue whereby when Artifactory runs with an Oracle database, database conversion errors occur when creating new indexes.

Artifactory 7.90.5 Self-Managed

Released: 25 July, 2024

This topic describes the new features, feature enhancements, and resolved issues that are part of the Artifactory 7.90.5 release for Self-Managed environments. It includes all improvements since Artifactory 7.84.

Highlights

Known Issue in this Version

Upgrading self-maanaged deployments from version 7.71 directly to 7.90 or higher fails due to a problematic Artifactory revision number in 7.71 causing converters not to run. To avoid this issue, upgrade to Artifactory version 7.90.7 or above.

- New Platform Navigation

JFrog is launching the new platform UI navigation for Self-Managed instances.

This will be the default experience when using version number 7.90.x.

To find out more about this change, see JFrog Platform Navigation.

Classic UI Navigation Sunset

Classic UI navigation is planned to be deprecated with the Self-Managed release of October 2024.

For more information, see JFrog Platform Deprecations.

- Support for Ansible Repositories

You can now use Artifactory to manage and store your Ansible collections (including Roles, Playbooks, Plugins, Modules, etc.), providing full flexibility and usability. You can store and distribute your own collections through secure local repositories, and cache remote resources from the Ansible Galaxy registry for reliable access. For more information, see Ansible Repositories.

- Support for Hugging Face Datasets

Artifactory now supports storing and caching of Hugging Face ML datasets, allowing you to manage all stages of the ML development lifecycle. For more information, see Hugging Face Repositories.

- Individual JVM for Access Service

The Access service will now run on a dedicated Java Virtual Machine (JVM), separated from the main Artifactory JVM. While the Access JVM will utilize additional resources, this change is anticipated to decrease the memory usage of the Artifactory JVM. Additional configuration steps might be required for customers using the Derby database. For more information, see Individual JVM for Access Service

- Breaking Change for JFrog Access REST API Endpoints

> **Warning**
>
> As a result of the Individual JVM for Access Service, the previously used Access REST API endpoint, `https://<JFROG_PLATFORM_URL>/artifactory/api/access`, is no longer supported, and you must now use the new endpoint, `https://<JFROG_PLATFORM_URL>/access`.
>
> If your Access Federation URL is currently configured with `https://<JFROG_PLATFORM_URL>/artifactory/api/access`, update it to prevent service interruptions.

- Major Performance Improvements for Alpine

This version includes up to an 87% improvement in the response time in Alpine-related use cases, such as downloading from a virtual repository.
- Reduced Load When Reading Global Exclude Properties

An improvement was introduced in this version to reduce the load when reading global exclude properties. Any properties added to the **artifactory.repo.includeExclude.globalExcludes** parameter are now controlled by the flag **artifactory.repo.default.includeExclude.globalExcludes.empty.list**, which is set to **true** by default. When this flag is **true**, the list is treated as empty, meaning that the global exclude patterns are not considered. Therefore, it is necessary to set **artifactory.repo.default.includeExclude.globalExcludes.empty.list = false** for the global exclude patterns to be taken into account.

New Features

- Security Hardening for Artifactory Container Images

As part of JFrog's commitment to maintain the security and reliability of our products, JFrog Artifactory container images are now enforced with read-only permission to `webapps` and `conf` folders located in the `app/artifactory/tomcat` and `app/access/tomcat` directories.
- Support for PyPI Name Normalization and Enforce Layout

Artifactory now supports the PyPI package features name normalization and enforce layout, as specified in PEP-440. These features help you keep a consistent naming method for PyPI packages and avoid issues. For more information, see Use PyPI File Path Name Normalization, Use PyPI Enforce Layout, and Using Both PyPI File Path Naming Normalization and Enforce Layout.
- Support for OCI Referrers API

You can view the connection between images and their related information, such as signatures and attestations, for better visibility and management. For more information, see Use Referrers REST API to Discover OCI References.
- Get Status of Project Repository API

A new API allows users to obtain the status of a repository and whether it was assigned and/or shared to a project, to multiple projects, or to all projects. For more information, see Get Status of Project Repository API.

Feature Enhancements

Installation

- Improved User Experience for Helm Installations

Artifactory now supports the following Helm improvements:

- The `nginx.artifactoryConf` and `nginx.mainConf` fields have been reallocated to the 'files' directory.
- The `artifactory.openMetrics` field has been renamed as `artifactory.metrics`.
- Added `nginx.hosts` field to use as `server_name` directive on the embedded Nginx instead of `ingress.hosts` field.
- Changed `migration.enabled` flag to false by default. For Artifactory 6.x to 7.x migration, this flag needs to be set to `true`.

Authentication

- **Temporary Login Suspension Configuration Moved to Access Service**

As part of enhancements to the JFrog Access Service to make it the primary service for Authentication and Authorization, from Artifactory version 7.90, the configuration management for Temporary Login Suspension has moved to the Access Service. For more information, see User Lock and Login Suspension.

- **Project Admin Scoped Access Token**

Now in addition to an API that was released in Artifactory version 7.84, you can also generate project admin access tokens using the JFrog Platform UI. For more information, see Create a Project Admin Scoped Token.

Integrations

- **OpenID Connect Integration**

OIDC integration in the JFrog Platform allows you to use services including GitHub Actions and Azure with OpenID Connect to work on the JFrog Platform.

OpenID Connect Integration now supports Azure.

Database & Storage

- **Project Storage Quotas**

You can now view and manage project storage quotas. A table view with project details is now the default All Project View, and a new Storage Quota column with a usage bar has been added. You can now perform actions such as Edit Storage to manage and change the storage quota from the table view. For more information, see Manage Storage Quotas.

- **Enhanced Performance for Get Storage Summary Info REST API**

The time needed to return the storage summary information using a REST API has been significantly reduced for virtual repositories. For more information, see the Get Storage Summary Info REST API.

Archiving & Cold Storage

- **Additional Package Types Now Support Package Archiving**

Additional package types have been added to support package archiving. The full list of all package types that now support package archiving is: Docker, Maven, npm, Gradle, YUM, generic, NuGet, Conan, and Helm. For more information on package archiving, see Working with Cold Storage.

- **Improved Performance with Storage Summary Queries**

A flag was added to the Artifactory System Properties (`artifactory.db.operations.totalSize.mysql.noIndex`) that changes the storage summary queries (file count and repository table) to not use indexes in MySQL DB and hence improves query performance. By default, this flag is `false` and can be set to `true` in the system properties.

Federated Repositories

- **Additional synchronized metadata in Federated repositories**

It is now possible to synchronize the following artifact metadata with all Federation members:

- **createdBy**: The name of the user who uploaded the artifact to Artifactory (including the suffix '`federated`'.) The name is mirrored to other members even if the user does not exist on those members.

- **deploymentDate**: Defines when the artifact was deployed. Synchronizing this metadata is important for features such as the Max Unique Snapshot policy in Maven.

- **modifiedDate**: Defines when the artifact was last modified.

A new Artifactory system property controls the inclusion of this metadata:

`artifactory.federated.mirror.events.metadata.enabled`

By default, this flag is set to `false`. To mirror this metadata to other Federation members, change the flag setting to `true` on each relevant member. The metadata is mirrored only if the flag is activated on both the source and target JPD.

- **Cleanup Job for Removing Orphaned Cursors**

A new job cleans up orphaned cursors from the Federated repository database. This was done to optimize the auto-healing process.

Package Management

- **Support for new CocoaPods CLI Commands**

Artifactory now supports using the `pod search` and `pod list` commands for virtual CDN repositories.

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-8230	Access	Medium	Fixed an issue whereby, newly created generic repositories intermittently disappeared under projects.
JA-8346	Access	Medium	Fixed an issue whereby, Release Bundle did not appear as a resource in the Permissions UI for JFrog Pro subscriptions.
JA-8600	Access	High	Fixed an issue whereby, SAML login with Azure failed on multi-SAML SSO.
JA-8655	Authentication Providers	Medium	Fixed an issue whereby, LDAP user refresh failed when the lock time was set without setting a lockout duration.
JA-8655	Authentication providers	Medium	Fixed an issue whereby, LDAP user refresh failed when the lock time was set without setting a lockout duration.
JA-8980	General	Medium	Fixed an issue whereby, when starting the Access service, an unnecessary warning related to `application.yaml` was added to the logs.
JA-9056	Database	Medium	Fixed an issue whereby, Artifactory did not support updating a Permission Target with empty repository scope JSON when using Oracle Database.
JFUI-15366	Packages	Medium	Fixed an issue whereby, when using a URL to access the JFrog Platform WebUI, and logging in using HTTP SSO, Artifactory was redirected to the incorrect URL.
RTDEV-40320	Repositories	Medium	Fixed an issue whereby, Artifactory Export failed on Windows due to unsupportable characters in a file name or restricted file names.

JIRA Issue	Component	Severity	Description
RTDEV-40507	Storage	High	Fixed an issue whereby when CDN Download was enabled, if contentType contained a special character (such as '+') it was omitted and caused a failure with the redirect URL.
RTDEV-40750	Repositories	Medium	Fixed an issue that prevented the creation of a federated Release Bundle v2 repository with multiple members using a single API call (`PUT api/repositories/{repoKey}`).
RTDEV-41067	Packages	Medium	Fixed an issue relate to NuGet whereby, `*.symbols.nupkg` packages were indexed, causing search errors.
RTDEV-41317	Packages	Medium	Fixed an issue related to Helm whereby, when trying to use a virtual repository containing a remote repository pointing to the `https://wiremock.github.io/helm-charts/` registry, Artifactory returned a 500 error.
RTDEV-41390	User Interface (UI)	Medium	Fixed an issue related to OCI whereby, when creating a repository using the JFrog Platform WebUI, it is possible to use a repository key containing uppercase characters, but when trying to use the repository through the REST API, Artifactory returned a 400 error.
RTDEV-41630	Packages	High	Fixed an issue related to Docker whereby, under certain circumstances, Artifactory failed to generate the docker tags list when the registry returned a full URL instead of a relative URL in the link header as expected.
RTDEV-41714	General	High	Fixed an issue whereby, under certain circumstances, when trying to perform pull replication, Artifactory created an infinite loop and failed to complete the operation.
RTDEV-41880	Packages	Medium	Fixed an issue whereby, under certain circumstances, Artifactory failed to index NuGet packages.
RTDEV-42061	Packages	Medium	Fixed an issue related to PyPI whereby, when resolving packages via Artifactory Cloud, the `cache-control` header was not returned, causing possible duplicate resolving of packages.
RTDEV-42072	General	Medium	Fixed an issue related to the Mail Server page whereby, when setting up a mail server without configured password, users encountered an error to re-enter the password, when editing the mail server configuration or testing the connection.

JIRA Issue	Component	Severity	Description
RTDEV-42350	Packages	Medium	Fixed an issue related to Gradle whereby, the Set Me Up menu in the JFrog Platform WebUI showed incorrect instructions.
RTDEV-42560	Repositories	Medium	Fixed an issue whereby Artifactory Export overwrites a file with the same name but written in a different case.
RTDEV-42772	Packages	High	Fixed an issue related to Conda whereby, under certain circumstances, when trying to resolve a package from a virtual repository, Artifactory returned a 500 error.
RTDEV-43090	Packages	Medium	Fixed an issue related to Generic repositories whereby, when deploying `*.crate` files in the repositories, Artifactory attempted to calculate metadata for the file which may result in a crash.
RTDEV-43533	Repositories	Medium	Fixed an issue whereby, when clicking Load More in the Tree View menu in the JFrog Platform WebUI, Artifactory did not perform as expected.
RTDEV-43850	Repositories	Medium	Fixed an issue whereby remote repositories were not set to an “assumed offline” state in certain situations.
RTDEV-44031	Packages	Medium	Fixed an issue related to Cargo whereby, updating or creating repository settings through the YAML configuration did not work as expected.
RTDEV-44298	General	Medium	Fixed an issue whereby, from Artifactory version 7.84, AQL searches will undergo throttling, potentially resulting in 429 errors. for more information, see the Known Issues.
RTDEV-44325	Repositories	Medium	Fixed an issue related to npm whereby, when performing metadata processing, a connection leak might occur.
RTDEV-4982	Repositories	Medium	Fixed an issue related to Helm whereby, when turning off the ‘List Remote Folder Items’ setting for smart remote repositories, it was still enabled.
RTDEV-39492	Repositories	Medium	Fixed an issue related to P2 whereby, creating a local repository was allowed using repository creation REST API, even though only remote and virtual P2 repositories are supported.
RTDEV-40535	Packages	Medium	Fixed an issue related to Terraform whereby, when trying to resolve modules from a virtual repository containing a smart remote repository in an air-gapped environment, Artifactory returned a 404 error.

JIRA Issue	Component	Severity	Description
RTDEV-41066	Packages	Medium	Fixed an issue whereby, when trying resolving artifact metadata from a virtual repository, Artifactory did not merge metadata files of `xml.bz2` format from a nested remote repository, which caused longer resolution times and an inability to view or resolve artifacts from the nested remote repository.
RTDEV-41095	Packages	Medium	Fixed an issue related to PyPI whereby, when trying to access the simple index of a smart remote repository that is offline, Artifactory returned a 404 error.
RTDEV-41189	Repositories	High	Fixed an issue whereby, when attempting to create a Smart Remote Repository on Edge instance that has Platform Proxy configured, Artifactory did not create the repository.
RTDEV-41547	General	Medium	Fixed an issue whereby, when setting up a webhook to monitor `artifact-property-added` events and then adding a property recursively at the folder level, Artifactory did not perform as expected.
RTDEV-41633	Packages	Medium	Fixed an issue related to Go whereby, when trying to download a Golang package in a major version higher than 10 from a remote repository proxying GitHub, Artifactory did not perform as expected.
RTDEV-42300	Packages	Medium	Fixed an issue related to Hugging Face whereby, the 'Store Artifacts Locally' checkbox was visible for remote repositories via the JFrog Platform WebUI.
RTDEV-42319	Release Lifecycle Management	Medium	Fixed an issue whereby, a Release Bundle v2 could not be created from a build that has dependencies lacking a SHA-256.
RTDEV-42905	Packages	Low	Fixed an issue related to Docker whereby, when trying to promote a multi-architecture image more than once in the same repository with the same source tag and destination tag, Artifactory returned a 400 error.
RTDEV-43447	Packages	Medium	Fixed an issue related to npm whereby, when requesting package metadata, Artifactory returned the same response headers for JSON and abbreviated JSON files.
JA-9584	General	Medium	Fixed an issue whereby, when trying to edit or delete project roles with names containing special characters, Artifactory returned a 400 error.
RTDEV-44444	Medium	Medium	Fixed an issue whereby a project admin could not delete a repository associated with a project.

JIRA Issue	Component	Severity	Description
RTFE-1341	Repositories	Medium	Fixed an issue whereby the Run Now option was available when adding a replication configuration to a new local repository that was still being created in the UI.
RTFE-1593	Repositories	Medium	Fixed an issue related to Helm OCI whereby, the repositories were not displayed on the Repositories page in the JFrog Platform WebUI Administration module as expected.

Artifactory 7.84

This section includes all the Artifactory 7.84 releases.

Artifactory 7.84.23 Self-Managed

Released: 2 February 2025

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-53839	Packages	Critical	Fixed an issue whereby an unannounced change that was introduced by Conda Forge upstream impacts Artifactory's ability to resolve package metadata and dependencies with virtual Conda repositories.

Artifactory 7.84.21 Self-Managed

Released: 26 August, 2024

New Features

- Specifying a Dedicated HA Node for Shift Events

Users working in a Self-Managed HA environment can now designate which node will be responsible for all shift events, which is an internal process used by Artifactory to organize events in the correct order. The node is configured by specifying the system parameter, `artifactory.shift.events.isolated.member` with the name of the dedicated node on each HA member.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-47226	Packages	High	Fixed an issue related to Conda whereby, when installing packages with a `noarch` value set to `null`, Artifactory did not perform as expected.

Artifactory 7.84.20 Self-Managed

Released: 5 August, 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-45824	General	Critical	Fixed an improper path validation issue that could potentially lead to cache poisoning.
RTDEV-45626	General	High	Fixed an improper token validation issue that could potentially lead to privilege escalation.

Artifactory 7.84.18 Self-Managed

Released: 29 July, 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-45634	General	High	Fixed an issue whereby Artifactory would lose all memory and crash due to an AQL query with a limitless dataset.

Artifactory 7.84.17 Self-Managed

Released: 9 July, 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-44444	Projects	Medium	Fixed an issue whereby a project admin was unable to delete a repository associated with a project.
RTDEV-44325	Repositories	Medium	Fixed an issue that caused a potential connection leak during npm metadata requests.
RTDEV-43241	Repositories	Medium	Fixed an issue whereby Generic repositories configured with the `retrieveSha256FromServer` property set to `true` were unable to download SHA256 files from a remote registry due to a URL modification that resulted in 404 errors.

Artifactory 7.84.16 Self-Managed

Released: 28 June, 2024

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-44298	General	Medium	Fixed an issue whereby, from Artifactory version 7.84, AQL searches will undergo throttling, potentially resulting in 429 errors. For more information, see Artifactory Known Issues.

Artifactory 7.84.15 Self-Managed

Released: 18 June, 2024

Known Issue in this Version

Starting from Artifactory version 7.84, AQL searches will undergo throttling, potentially resulting in 429 errors. The default setting for the parameter below will be TRUE. You can opt to set it to FALSE to disable the throttling:

```
artifactory.aql.queries.limit.enabled
```

To avoid this issue, upgrade to Artifactory version 7.84.16 or later.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-42905	Packages	Low	Fixed an issue related to Docker whereby, when trying to promote a multi-architecture image more than once in the same repository with the same source tag and destination tag, Artifactory returned a 400 error.
RTDEV-42940	Packages	Medium	Fixed an issue related to Cargo whereby, under certain circumstances, Artifactory failed to install a package from a local repository after copying it from a remote cache.
RTDEV-42772	Packages	Medium	Fixed an issue related to Conda whereby, under certain circumstances, when trying to resolve a package from a virtual repository, Artifactory returned a 500 error.

Artifactory 7.84.14 Self-Managed

Released: 6 June, 2024

Known Issue in this Version

Starting from Artifactory version 7.84, AQL searches will undergo throttling, potentially resulting in 429 errors. The default setting for the parameter below will be TRUE. You can opt to set it to FALSE to disable the throttling:

```
artifactory.aql.queries.limit.enabled
```

To avoid this issue, upgrade to Artifactory version 7.84.16 or later.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-42300	Packages	Medium	Fixed an issue related to Hugging Face whereby, the 'Store Artifacts Locally' checkbox was visible for remote repositories via the JFrog Platform WebUI.
INST-8369	Installers	Medium	Fixed an issue related to Helm installation whereby, the `cacheProviderDir` and `maxCacheSize` properties were swapped in the `azure-blob-storage-v2-direct` binarystore.xml template.

Artifactory 7.84.12 Self-Managed

Released: 23 May, 2024

Known Issue in this Version

Starting from Artifactory version 7.84, AQL searches will undergo throttling, potentially resulting in 429 errors. The default setting for the parameter below will be TRUE. You can opt to set it to FALSE to disable the throttling:

```
artifactory.aql.queries.limit.enabled
```

To avoid this issue, upgrade to Artifactory version 7.84.16 or later.

Resolved Issues

JIRA Issue	Component	Severity	Description
RTDEV-39492	Repositories	Medium	Fixed an issue related to P2 whereby, creating a local repository was allowed using repository creation REST API, even though only remote and virtual P2 repositories are supported.
RTDEV-41547	General	Medium	Fixed an issue whereby, when setting up a webhook to monitor `artifact-property-added` events and then adding a property recursively at the folder level, Artifactory did not perform as expected.
INST-8316	Installation	High	Fixed an issue related to Helm installation whereby, the Nginx deployment failed to render when loggers sidecar containers were set.
INST-8320	General	High	Upgraded NodeJS to version 20.12.2
RTDEV-4982	Repositories	Medium	Fixed an issue related to Helm whereby, when turning off the 'List Remote Folder Items' setting for smart remote repositories, it was still enabled.
RTDEV-40319	Packages	Medium	Fixed an issue related to Helm whereby, charts with external dependencies were not resolved properly using smart remote repositories.

JIRA Issue	Component	Severity	Description
RTDEV-42030	Packages	Low	Fixed an issue related to npm whereby, when performing metadata processing, a connection leak might occur.

Artifactory 7.84.11 Self-Managed

Released: 17 May, 2024

Known Issue in this Version

Starting from Artifactory version 7.84, AQL searches will undergo throttling, potentially resulting in 429 errors. The default setting for the parameter below will be TRUE. You can opt to set it to FALSE to disable the throttling:

```
artifactory.aql.queries.limit.enabled
```

To avoid this issue, upgrade to Artifactory version 7.84.16 or later.

Resolved Issues

JIRA Issue	Component	Severity	Description
INST-8316	Installation	High	Fixed an issue related to Helm installation whereby, the Artifactory statefulset failed to render when loggers sidecar containers were set.
INST-8301	Installation	Medium	Fixed an issue related to Helm installation (artifactory-HA chart) whereby, the statefulset failed to render when imagePullPolicy on copy-circle-of-trust-certificates container were set.
INST-8366	Installation	High	Fixed an issue related to Helm installation whereby, when using artifactory-unified-secret, Artifactory did not support installing multiple instances in a single namespace.

Artifactory 7.84.10 Self-Managed

Released: 26 August 2024

This topic describes the new features, feature enhancements, and resolved issues that are part of the Artifactory 7.84.10 release for Self-Managed environments. It includes all improvements since Artifactory 7.77.

Change to AWS S3 Storage Direct Download Option

From this version and on, the direct download option no longer works with eventual and cluster providers. If you want to continue using direct download, use the **s3-storage-v3-direct** template.

Replicator Sunset

The Replicator service for Release Bundles v1 has been deprecated. For more information, see Artifactory Deprecations.

Known Issue in this Version

Starting from Artifactory version 7.84, AQL searches will undergo throttling, potentially resulting in 429 errors. The default setting for the parameter below will be TRUE. You can opt to set it to FALSE to disable the throttling:

```
artifactory.aql.queries.limit.enabled
```

To avoid this issue, upgrade to Artifactory version 7.84.16 or later.

Cargo Git Indexing Deprecation

Starting at the end of Q2, 2024, Cargo indexing will only be enabled using Sparse indexing, and the use of Git indexing will be discontinued. For more information, see Deprecations in Process.

Highlights

- **PostgreSQL is the Recommended Database for Artifactory Installation**

After a comprehensive evaluation of leading database providers' capabilities, scalability, and support, JFrog selected PostgreSQL as the preferred database solution for all its product offerings.

Organizations can still choose to use any database in the list of Artifactory-supported databases, however, there is a minor new configuration step that will need to be performed for new installations. When installing a new Artifactory instance with any database other than PostgreSQL, you are required to specify the configuration in the `system.yaml` file.

For more information, see Choose the right database.

- **Major Performance Improvements for PyPI, NuGet, and npm**

This version includes significant reductions in response time, as well as simplified and reduced database calls from the previous Self-Managed version (7.77). These improvements apply to several important use cases, including virtual package resolution and external dependency resolution, among others. We have measured:

Up to 24% response time reduction in PyPI-related use cases Up to 23% response time reduction in NuGet-related use cases

- Up to 84% response time reduction in npm-related use cases

New Features

- **APIs for Creating & Retrieving Batches of Repositories**

A new API enables you to create multiple repositories using a batch request. The batch request can contain a mix of different package types and repository types. For more information, see Create Multiple Repositories API. Another new API enables you to retrieve the configurations for a batch of repositories based on the repository names. For more information, see Get Batch of Repositories by Name API.

- **Oracle RAC support for Federated repositories**

Customers who use Oracle Real Application Clusters (RAC) must configure the following Artifactory system property to support Federated repositories:

```
artifactory.oracle.node.events.sequence.is.no.cache
```

Setting this property to `true` enables a converter that fixes the Oracle node events sequence definition for RAC instances.

Note

For additional prerequisites, see Setup Prerequisites for Federated Repositories.

- Support for OpenTofu Terraform Client

Artifactory now supports the OpenTofu registry and client, which provides an alternative to Hashicorp's Terraform Provider Registry.

For more information, see Configure OpenTofu to Work With Artifactory.
- Support for CocoaPods Virtual Repositories

Artifactory now supports using CocoaPods virtual repositories, only for repositories using CDN- allowing you to access both local and remote CocoaPods resources through a single URL.

For more information, see Set Up Virtual CocoaPods Repositories and Use CocoaPods CDN for Virtual Repositories.
- CocoaPods CDN Now Supported for Local Repositories

CocoaPods CDN expedites the workflow by creating a static copy of the CocoaPods Specs repository, reducing the time required for adding repositories. For more information, see Use CocoaPods CDN.

Feature Enhancements

Installation

- Helm Installation Updates

- The `setSecurityContext` field in Helm installation has been renamed as `podSecurityContext`.
- Added a dedicated image section for `initContainers` instead of `initContainerImage`
- Added `unifiedSecretInstallation` flag, which enables single unified secret holding all chart secrets to **true** by default.

Authentication

- Automatically pair OAuth SSO users with JFrog Platform users

You can now automatically pair OAuth SSO users when they log in to the JFrog Platform with their JFrog Platform user based on their email address. No configuration change is required to enable the feature. For more information on OAuth SSO, see OAuth SSO.
- Access Token Creation by Project Admins

Project admins can create access tokens that are tied to the projects in which they hold administrative privileges. For more information, see Access Token Creation by Project Admins.
- Changes to Anonymous Access

Starting from Artifactory 7.84.3, the anonymous user is removed from the **Anything** and **Any Remote** permissions by default. To grant permissions to anonymous users, the best practice is to create a new permission target containing the anonymous user, and to assign it with read-only access to the relevant repositories.

For more information, see Allow Anonymous Access.

General

- Availability Zone Affinity

You can configure a preferred availability zone in the router section of the Artifactory System YAML file. If a service is available in the local zone, traffic is sent to this local service. However, if a service is not available locally, traffic is sent to a service in another zone using a round robin strategy.

For more information, see JFrog Router Service.

Storage

- Storage Improvements

This release contains the following storage improvements:

When using Azure Blob storage with a SAS token, the SAS token is now encrypted at rest in the the binarystore.xml file. When using the state-aware-s3 binary provider, sensitive properties are now encrypted in the same manner as they are for the s3-storage-v3 binary provider.

Federated Repositories

- Federated repository support for projects

In versions before 7.78.1, new Federation members ignored the association of a Federated repository with a specific project. For example, if a Federated repository in existing members was associated with **myProject**, new Federation members would lack the project association.

Starting with version 7.78.1, Artifactory will check whether the associated project in existing members is defined in the site of the new Federation member. If the project exists, the new member will be associated with this project automatically. If the project does not exist, the new member will not be associated with the project.

> **Note**
>
> A current limitation of this feature is that if the project association later changes in one Federation member, this change is not synchronized with the other members.

- Full Sync improvements for Federated repositories

This release contains an option for generating the file list for a Full Sync operation using multiple SQL queries (paging) instead of a single AQL query. Dividing the database query into pages helps prevent the operation from crashing when retrieving a large file list (by default, more than 400000 artifacts). In addition, several new system properties have been introduced for managing this paging feature. For more information, see System Properties for Full Sync File List Queries. For more information about Full Sync, see Perform Full Sync on Federated Repositories.

- Solutions for resolving 'stuck' Full Sync operations on Federated repositories

Two new options have been introduced for resolving Full Sync operations that have become 'stuck', meaning the operation persists in the database but is not active in memory. For example, this situation can arise if a user restarts an Artifactory instance while a Full Sync operation is in progress.

1. A new async task defined in the `system.properties` file (`artifactory.reset.stale.full.sync.job.interval.min`) can reset the status of a Full Sync operation that has become 'stuck', enabling the operation to restart.
2. A new Force Full Sync API enables you to force a Full Sync operation between the Federated repository members, interrupting another Full Sync operation that is already in progress.

- Auto Healing of Federated repositories enabled by default

The auto-healing mechanism introduced in version 7.71.1 is now permanently enabled for all customers who work with Federated repositories. This mechanism checks Federated repositories at regular intervals for exhausted queues (queues that have exceeded the maximum number of attempts to send events to other Federation members), resets the failed events automatically, and tries again to sync with the target mirror. For more information, see Federation Recovery and Auto-Healing.

- Perform recovery on repository Federation

It is now possible to perform a recovery operation on an entire Federation at once by leaving off the `{repo-key}` parameter when invoking the REST API. For more information, see Federation Recovery API.

- Open Metric for Federated Repository status

A new Open Metric records the number of Federated repositories that have the indicated status. For more information, see Federated Repository Metrics.

- Get Federated Repository Status V2 API

This enhanced version of the existing API endpoint supports a wider range of statuses. For more information, see Get Federated Repository Status (v2) API.

Release Lifecycle Management

- Updates to Release Lifecycle Management APIs

Several changes have been made to the Release Lifecycle Management APIs. Among the changes:

- For all relevant APIs, the status value of `PROCESSING` has been changed to `STARTED`.
- For all relevant APIs, the `messages[].source` and `messages[].created` properties have been deprecated.
- The `X-JFrog-Signing-Key-Name` request header has been made optional instead of mandatory when promoting a Release Bundle v2 version using the Promote Release Bundle v2 Version API.
- **New menu options for creating Release Bundle v2 versions**

The Actions menu for Release Lifecycle Management now includes options for creating a new version of the selected Release Bundle v2 from builds or other Release Bundles. For more information, see Create a New Version of an Existing Release Bundle.
- **Local Deletion of Distributed Release Bundles v2 from Edge Nodes Reported in Source Timeline**

When a distributed Release Bundle v2 version is deleted locally from the target (typically an Edge node), as opposed to being deleted remotely from the source Artifactory, a new service provided by JFrog Distribution informs the source Artifactory of the operation. An event that describes the deletion is then added to the Release Bundle timeline for maximum visibility.

The behavior of this functionality is configurable in both Distribution (requires 2.24.x and higher) and Artifactory. For more information, see Configure Deleted-at-Target Scraping Service.
- **Support for Release Lifecycle Management in Federated Environments**

It is now possible to work with Release Bundles v2 in a Federated environment as part of managing your release lifecycle. This is particularly useful when Federations are employed in a DR (disaster recovery) or Active/Active multi-site framework, as it ensures that your releases (as contained in an immutable Release Bundle) are replicated across all sites. For more information, see Release Lifecycle Management in Federated Environments.
- **Project Key Validator for Federated Release Bundle Repositories**

A validator has been added to ensure that Release Bundle repositories related to a specific project can be Federated only if the same project key exists on the other JPDs in the Federation.
- **Lifecycle System YAML**

There is a new section in the Artifactory YAML file for configuring parameters related to Release Lifecycle Management. This replaces the Configuration APIs that were used previously and have now been deprecated. For more information, see Lifecycle System YAML.
- **Improved Tracking of Distribution Task Progress**

JFrog Distribution now uses an improved method for tracking distribution tasks, which enables more accurate updates about the progress of each task.

Package and Repository Management

- **Support for new CocoaPods CLI Commands**

Artifactory now supports using the `pod search` and `pod list` commands for local and remote CDN repositories.
- **Helm Virtual `index.yaml` Resolution Improvements**

We have improved our index calculation mechanism for virtual repositories to minimize potential OOM issues. We recommend setting the **Metadata Retrieval Cache Period (Sec)** in the repository page in the JFrog Platform WebUI to 60 seconds or more. For more information, see Helm Virtual Repository Index Improvements.
- **Go Virtual Repositories Performance Improvement**

Added Go Remote VCS repositories requests caching using local cache to reduce remote API calls and avoid rate limits.
- **Support for `.zip` Package Format in CocoaPods Remote CDN Repositories**

Artifactory now supports resolving and caching `.zip` format packages in CocoaPods remote CDN-enabled repositories, in addition to `.tgz` format.

User Interface

- **Improved Artifact Tree View**

The Artifact Tree view has been significantly improved such that when opening a node on a repository, a specific (configurable) number of artifacts will be displayed instead of the entire contents of the repository. This significantly reduces loading time for repositories containing a large number of artifacts. The default

display number is 500, but this number can be changed in the Aritfactory UI. If there are more artifacts to display beyond the current list, a **Load more** option appears at the end of the list and when clicked displays more items.

The enhanced Artifact Tree View is available both in a Tree Browser and a Native Browser.
- **Display List Manifest Content on the Artifacts Page**

Artifactory now displays the manifests under a `list.manifest` file directly in the Artifacts page in the JFrog Platform WebUI. For more information, see List Manifest Content.

Xray

- **New Default Timeout Value for Blocking Operations After Unfinished Scans**

The default timeout value for the `blockUnfinishedScansTimeoutSeconds` property has been changed from 600 seconds (10 minutes) to 1800 seconds (30 minutes). This property defines how long Artifactory waits for Xray to finish scanning before blocking operations automatically if the scan is still unfinished.

Resolved Issues

JIRA Issue	Component	Severity	Description
JA-7939	Authentication Provider	Low	An error occurs with the group scope token when attempting to set up identity mapping.
JA-8655	Authentication Providers	Medium	Fixed an issue whereby, LDAP user refresh failed when the lock time was set without setting a lockout duration.
RTDEV-39111	Authentication Providers	Medium	Fixed an issue whereby, when a transient user was created the API security.currentUser().isTransientUser() returned **false**
RTDEV-40549	Authentication Providers	Medium	Fixed an issue that enabled a Release Bundle v2 to be created successfully even when the GPG key assigned to the Release Bundle was provided with the wrong passphrase.
RTDEV-39382	Authentication Providers	Medium	Fixed an issue whereby, when trying to remove an SSH key from Artifactory, the key was not completely removed.
RTDEV-37193	Federated Repositories	High	Fixed an issue that caused fetch failures from deleted Federated repositories to persist indefinitely in the database.
RTDEV-38116	Federated Repositories	Medium	Fixed an issue that prevented sites using Oracle RAC from supporting Federated repositories. For more information, see Oracle RAC support for Federated repositories.
RTDEV-38558	Federated Repositories	Medium	Full Sync operations on Federated repositories now always update the timestamp in the node_event_cursor table.
RTDEV-37757	Federated Repositories	Medium	Fixed an issue that enabled users to Federate two repositories on the same Artifactory instance and to create a Federation with an Edge node as a target instance.
JA-8461	General	High	Fixed an issue related to Helm whereby, when using an Oracle database with only one repository with permissions, cannot remove this repository from permissions.

JIRA Issue	Component	Severity	Description
RTDEV-38572	General	Low	Fixed an issue whereby, when using a curl command with a 'range' HTTP header to fetch bytes from the end of a text file, Artifactory fetched bytes from the beginning of the file instead.
RTDEV-38828	General	Medium	Fixed an issue whereby the process of reading the same binary multiple times simultaneously to the Cached Filesystem Binary Provider was getting stuck and caused high CPU processing.
RTDEV-40089	General	Medium	Fixed an issue whereby the backup would fail when Artifactory attempted to verify if enough disk space was available for the backup and a remote repository was selected for backup.
RTDEV-40166	General	Medium	Fixed an issue whereby, when applying Artifactory YAML Configuration with mail server changes containing quotation marks, Artifactory returned an error and became unresponsive.
RTDEV-42076	General	Critical	Fixed an improper input validation issue that could potentially lead to privilege escalation.
RTDEV-39697	General	Medium	Fixed an issue where YAML configuration changes couldn't be applied if the file size exceeded 3 MB.
RTDEV-36400	Packages	Medium	Fixed an issue related to Conan whereby, under certain circumstances, when copying Conan artifacts from one repository to another, Artifactory did not update the `conan/packages.ref.json` file as expected.
RTDEV-37586	Packages	Medium	Fixed an issue related to Conda whereby, under certain circumstances, some packages were not indexed as expected.
RTDEV-37982	Packages	Medium	Fixed an issue whereby, when using a dotnet NuGet client with incorrect authentication credentials, Artifactory returned a 500 server error instead of a 401 error.
RTDEV-38770	Packages	High	Fixed an issue related to Terraform whereby, under certain circumstances, modules from remote repositories could not be resolved.
RTDEV-38815	Packages	Medium	Fixed an issue related to Go and PyPI whereby, when resolving artifacts from remote repository using a plugin that uses the `org.artifactory.exception.CancelException` class, Artifactory returns an incorrect error.
RTDEV-39036	Packages	Medium	Fixed an issue related to npm whereby, Artifactory did not support installing external dependencies with URLs containing question marks (?).

JIRA Issue	Component	Severity	Description
RTDEV-39105	Packages	Medium	Fixed an issue related to Maven whereby, Artifactory did not force authentication for unavailable artifacts in virtual repositories in the native JFrog Platform WebUI even when the Force Authentication checkbox was selected.
RTDEV-39551	Packages	Low	Fixed an issue related to PyPI whereby, under certain circumstances, the `yanked` property was not applied to packages' simple index files as expected.
RTDEV-39600	Packages	Medium	Fixed an issue related to Terraform whereby, Artifactory did not support dereferenced commits for Terraform modules when proxying remote registries.
RTDEV-39764	Packages	Medium	Fixed an issue related to RPM whereby, when adding GPG keys without extension with a file name containing 'GPG', Artifactory did not support making the keys expirable.
RTDEV-40052	Packages	High	Fixed an issue related to Helm whereby, when trying to use the dependencies commands in virtual repositories, Artifactory returned an error.
RTDEV-40083	Packages	Medium	Fixed an issue related to Hugging Face whereby, Artifactory did not support the `/api/validate-yaml` endpoint that was added in client version 0.21.0, causing upload failures.
RTDEV-40221	Packages	High	Fixed an issue related to npm whereby, under certain circumstances, Federated repository instances overwrote the latest dist-tag to the wrong version during package indexing instead of excluding the dist-tag from the mirror.
RTDEV-40543	Packages	Medium	Fixed an issue related to Maven whereby, when trying to configure a Maven client with the "Mirror Any" option checked, Artifactory did not generate the `settings.xml` file as expected.
RTDEV-41317	Packages	Medium	Fixed an issue related to Helm whereby, when trying to use a virtual repository containing a remote repository pointing to the `https://wiremock.github.io/helm-charts/` registry, Artifactory returned a 500 error.
RTDEV-41630	Packages	High	Fixed an issue related to Docker whereby, under certain circumstances, Artifactory failed to generate the docker tags list when the registry returned a full URL instead of a relative URL in the link header not as expected.
RTDEV-41685	Packages	High	Fixed an issue related to PyPI whereby, under certain circumstances, a persistent connection leak caused slowness in Artifactory.
RTDEV-41880	Packages	Medium	Fixed an issue whereby, under certain circumstances, Artifactory failed to index NuGet packages.

JIRA Issue	Component	Severity	Description
RTDEV-35895	Packages	Medium	Fixed an issue related to NuGet whereby, Artifactory did not support searching for specific packages in a virtual repository using the PowerShell client.
RTDEV-36665	Packages	Medium	Fixed an issue related to Helm whereby, when deleting a build and its multiple related Helm artifacts, the `Helm index.yaml` file was not updated accordingly.
RTDEV-36736	Packages	High	Fixed an issue related to RPM whereby, when trying to resolve artifacts from an upstream repository through a virtual repository, Artifactory did not work as expected at first attempt.
RTDEV-37593	Packages	Medium	Fixed an issue related to npm whereby, when copying a package to a different repository, after removing the package with the `disttag=latest`, the `package.json` metadata file was copied as empty.
RTDEV-37776	Packages	Medium	Fixed an issue related to CocoaPods whereby, when configuring a remote repository using Cocoapods CDN, Artifactory did not support the 'pod repo update' command.
RTDEV-38467	Packages	Medium	Fixed an issue related to RPM whereby, when deploying a package with a name containing the substring `_tmp_`, Artifactory did not index it as expected.
RTDEV-38691	Packages	Low	Fixed an issue related to P2 whereby, Artifactory did not support creating a Smart Remote repository with a key containing special characters.
RTDEV-38921	Packages	Low	Fixed an issue related to NuGet whereby, under certain circumstances, Artifactory did not support resolving artifacts through a virtual repository containing a large number of remote repositories.
RTDEV-38923	Packages	Low	Fixed an issue related to Maven whereby, when deploying a snapshot to a local repository with the `artifactory.maven.authentication.nonPreemptive` property enabled, Artifactory did not perform as expected.
RTDEV-39342	Packages	Medium	Fixed an issue related to Docker whereby, when running a ‘docker push’ command on a new image, the ‘docker tag promoted’ webhook was incorrectly triggered.
RTDEV-39456	Packages	Medium	Fixed an issue related to Conda whereby, when trying to deploy an artifact with an empty `noarch` metadata value, Artifactory did not calculate the package metadata as expected.
RTDEV-39903	Packages	Low	Fixed an issue whereby, Artifactory did not support setting a Cargo registry URL via the configuration YAML file.

JIRA Issue	Component	Severity	Description
JFUI-14974	Packages	Medium	Fixed an issue whereby, when navigating to the package version details page and clicking the **Show In Tree** button near a package artifact while moving to the Artifacts page, Artifactory returned an error.
RTDEV-39948	Packages	Medium	Fixed an issue related to Terraform whereby, when trying to resolve versions of modules that were already cached, the gitref files were not updated as expected and Artifactory returned a 404 error or an incorrect latest version.
RTDEV-40074	Packages	High	Fixed an issue related to Cargo whereby, after calculating repository metadata, Artifactory did not support resolving packages from local repositories.
RTDEV-41066	Packages	Medium	Fixed an issue whereby, when trying resolving artifact metadata from a virtual repository, Artifactory did not merge metadata files of xml.bz2 format from a nested remote repository, which caused longer resolution times and an inability to view or resolve artifacts from the nested remote repository.
RTDEV-41068	Packages	Medium	Fixed an issue related to Pub whereby, when trying to resolve an artifact with a version containing a '+' character from a virtual repository, Artifactory did not include the metadata as expected.
RTDEV-41095	Packages	Medium	Fixed an issue related to PyPI whereby, when trying to access the simple index of a smart remote repository that is offline, Artifactory returned a 404 error.
RTDEV-41633	Packages	Medium	Fixed an issue related to Go whereby, when trying to download a Golang package in a major version higher than 10 from a remote repository proxying GitHub, Artifactory did not perform as expected.
RTDEV-41970	Packages	Medium	Fixed an issue related to npm whereby, when using Yarn 2 to publish a scoped npm package to Artifactory, Artifactory did not perform as expected.
RTDEV-37678	Release Lifecycle Management	Medium	Fixed an issue that caused the promotion and distribution filters on the Release Lifecycle dashboard to present Release Bundle versions created during the selected timeframe instead of versions that were promoted or distributed during that timeframe.
RTDEV-37966	Release Lifecycle Management	Medium	Established a limit to the number of versions (default = 200) that can be displayed for one Release Bundle v2 on the Release Lifecycle dashboard.
RTDEV-38849	Release Lifecycle Management	Medium	Fixed an issue that caused an unexpected server error when deleting a Release Bundle v2.

JIRA Issue	Component	Severity	Description
RTDEV-38927	Release Lifecycle Management	Medium	Fixed an issue that prevented failed Release Bundle v2 promotions from appearing with the correct icon on the Release Lifecycle dashboard.
RTDEV-38928	Release Lifecycle Management	Medium	Fixed an issue that caused errors in the Release Lifecycle dashboard due to Release Bundle v2 promotions to a renamed or deleted environment.
RTDEV-39037	Release Lifecycle Management	Critical	Fixed an issue that prevented a Release Bundle v2 from collecting all artifacts of the same name from within a single build-info module.
RTDEV-39093	Release Lifecycle Management	Critical	Fixed an issue that excluded certain properties by default (`build.name` , `build.number` , `build.timestamp`) when promoting a Release Bundle v2 version.
RTDEV-39724	Release Lifecycle Management	Medium	Fixed a permissions issue that prevented users with a license other than Enterprise+ from creating Release Bundles v2 from the Release Lifecycle Management dashboard.
RTDEV-42319	Release Lifecycle Management	Medium	Fixed an issue whereby, Release Bundle V2 could not be created from a Build having dependencies without SHA-256.
RTDEV-36586	Repositories	Medium	Fixed an issue whereby, virtual repositories containing remote repositories with no metadata were not visible to non-admin users.
RTDEV-40796	Repositories	Medium	Fixed an issue related to OCI and HelmOCI whereby, the JFrog Platform WebUI displayed the 'enable indexing in Xray' option, even though Xray indexing is not supported for OCI and HelmOCI repositories.
RTDEV-37909	Repositories	Low	Fixed an issue whereby, when running the Update Repository Configuration REST API using a mismatched `rclass` parameter, Artifactory returned a 400 error specifying the `rclass` always as 'local', regardless of the repository type.
RTDEV-38679	Repositories	Medium	Fixed an issue whereby, when enabling the "Disable Artifact Resolution in Repository" setting at the repository level, it was still possible to download the entire repository's content as a ZIP file.
RTDEV-39623	Repositories	Low	Fixed an issue whereby, when trying to resolve an un-cached artifact from a remote repository pointing to a registry that does not allow content browsing through the Native Browse, Artifactory returned a 404 error.
RTDEV-40538	Repositories	Medium	Fixed an issue related to Go whereby, when trying to set up a remote repository using the Set Me Up instructions in the JFrog Platform WebUI, Artifactory returned a 404 error.

JIRA Issue	Component	Severity	Description
RTDEV-41189	Repositories	High	Fixed an issue whereby, when attempting to create a Smart Remote Repository on Edge instance that has Platform Proxy configured, Artifactory did not create the repository.
RTDEV-39396	Storage	Medium	Fixed an issue whereby, `enableSignedUrlRedirect` in the **state-aware-s3** provider (in **binarystore.xml**) did not follow the read order of zones that were configured in the sharding provider.
RTDEV-40507	Storage	High	Fixed an issue whereby when CDN Download was enabled, if contentType contained a special character (such as '+') it was omitted and caused a failure with the redirect URL.
RTDEV-41125	Storage	Medium	Fixed an issue whereby initiating the process for pruning unreferenced data with a federated repository configured resulted in 403 forbidden errors.
JFUI-14838	User Interface (UI)	Low	Fixed an issue whereby, `frontend-request.log` did not have the same structure as other log files in the JFrog Platform.
JFUI-14956	User Interface (UI)	Medium	Fixed an issue whereby, when modifying the `timeoutMinutes` property within the `values.yaml` file to a value higher than 5 minutes, the Artifactory Frontend service did not behave as expected.
RTDEV-38945	Xray	Medium	Fixed an issue whereby, Xray did not support scanning builds with names containing German umlaut characters (ü).

Previous Artifactory Releases

For more information about previous Artifactory releases, see Artifactory End of Life.

To download previous release notes, see the Legacy PDF archive.

Updated 1 day ago

← Artifactory SaaS Releases

About Artifactory Releases →

Did this page help you?

Yes No

Artifactory
Distribution
Xray
Advanced Security
Runtime
AppTrust
Curation
ML
AI Catalog

Events
Integrations
Software Supply Chain Topics
Open Source
JFrog Trust
Compare JFrog
JFrog Academy

Company

About
Management
Investor Relations
Partners
Customers
Careers
Press
Contact Us
Brand Guidelines

Developer

Community
Downloads
Community Events
Community Forum

Follow Us

© 2026 JFrog Ltd All Rights Reserved



© 2026 JFrog Ltd All Rights Reserved

Terms of Use Privacy Policy Cookies Settings Cookies Policy