



Get started

Lightwell Network

July 24, 2026

Contents

1 Get started 3

 Get started with the Red Hat Lightwell Network..... 3

 Choose the right repository for your environment..... 3

 Remediated repository version suffixes 4

 Lightwell Network repository access 4

 Create a Lightwell Network service account 4

1 Get started

Get started with the Red Hat Lightwell Network

Get started with Lightwell Network by learning how patched artifacts are versioned, choosing the right repository for your environment, and configuring your artifact repository manager or build tool to consume secure dependencies from Red Hat.

Choose the right repository for your environment

The Lightwell Network provides two repository tiers for each language ecosystem: Validated and Remediated. Both tiers deliver artifacts in the native format for your ecosystem.

Choose the repository that matches your needs, and use the corresponding URL when configuring your build tool.

Repository	Validated	Remediated
Purpose	Trust and verification of upstream code	Delivery of backported security fixes
Contents	Upstream-parity artifacts, signed provenance record, and software bill of materials (SBOM)	Lightwell-patched libraries with <code>.rh1w-0000X</code> suffix
Build standard	SLSA Level 3	SLSA Level 3
When to use	Dependencies that require verified, reproducible builds but do not yet need security patches	Dependencies that need active CVE remediation without version upgrades
Java URL	<code>packages.redhat.com/lightwell/java/validated/</code>	<code>packages.redhat.com/lightwell/java/remediated/</code>
Python URL	<code>packages.redhat.com/lightwell/python/validated/</code>	<code>packages.redhat.com/lightwell/python/remediated/</code>

Related information

[Lightwell Network repositories](#)

Remediated repository version suffixes

If you are using the Lightwell Network Remediated repository, your artifacts include backported security fixes identified by a version suffix.

Red Hat backports fixes to existing upstream versions. You choose the specific version you want to update, and the scope of each security patch is limited to the fix itself.

Patched artifacts are identified by a version suffix appended to the original upstream version:

- `.rhlw-0000X` – A sequential counter tracking cumulative security patches applied to that version.

For example, `5.3.17.rhlw-00001` means:

- The base upstream version is 5.3.17.
- This is the first Lightwell build that contains security patches applied to this version.

A subsequent fix to the same version would produce `5.3.17.rhlw-00002`. These suffixed versions are available to resolve when your build tool is configured to use the Lightwell Network Remediated repository.

Lightwell Network repository access

Access to the Lightwell Network is controlled through Red Hat entitlement certificates. Each certificate is linked to your organization ID, ensuring that your build tool can only resolve artifacts from repositories you are authorized to access.

Every Lightwell Network membership includes an entitlement certificate that you configure in your build tool. This certificate serves two purposes:

- **Authentication:** Confirms your identity as a Lightwell Network member.
- **Authorization:** Scopes your access to repositories based on your organization ID.

Your entitlement certificate scopes access to the repositories included in your membership. Attempts to access repositories not included in your membership are denied with a `403 Forbidden` error.

Create a Lightwell Network service account

Create a registry service account to authenticate your build tools with the Lightwell Network.

Before you begin

- You have a Red Hat account associated with your Lightwell Network membership.

Procedure

1. Navigate to the Registry Service Account Management Application at [Registry Service Accounts](#) and log in with your Red Hat credentials.
2. Click **New Service Account**.
3. Enter a name and description for the service account, and click **Create**.
4. Click the service account you created to view its credentials.
5. Note the following values:
 - a. **Username:** The full string including the prepended portion, in the format `XXXXXXX|service-account-name`.
 - b. **Password/Token:** The token displayed on the service account detail page.
6. Store these credentials securely. You will use them to configure authentication in your build tool or artifact repository manager.

Related information

[Creating Registry Service Accounts](#)