Splunk® Enterprise
Securing the Splunk Platform 8.2.1

Install Splunk Enterprise securely

Generated: 7/26/2021 4:46 pm

Install Splunk Enterprise securely

To install Splunk Enterprise securely, you must have an installation package that you have confirmed is authentic and has not been modified in any way since Splunk created it. Splunk provides a Message Digest 5 (MD5) secure hash for every package it generates. You can download this hash to quickly verify that the package you downloaded is authentic and has not been changed since its creation.

You can also compare the Secure Hash Algorithm-512 (SHA-512) hashes by opening a case with Splunk Support.

Prerequisites for verifying package integrity

You must have the following to verify the contents of packages you download:

- The `md5sum` program, which prints the hash of the file that you supply, and comes with most versions of Linux. On Windows, you can use the `certutil` tool to verify MD5 hashes.
- Alternatively, the `sha512sum` program prints SHA512 hashes for the file that you supply.
- The MD5 or SHA512 hashes, in text format, which Splunk provide
- Access to a shell prompt

Verify installation package integrity

After you download the Splunk Enterprise package, verify it by using a trusted version of the OpenSSL suite to compare the MD5 or SHA-512 hashes to the hash of the installation package. If the hash of the package you downloaded matches the hash that Splunk provides, then you have downloaded a valid, secure installation package and can proceed with installation.

Download Splunk Enterprise installation package and MD5 hash

Confirm that you download the MD5 hash that exactly matches the version of installation package that you downloaded. Downloading a different file results in the hashes not matching.

1. Go to the Splunk.com download page.
2. Click **Splunk Enterprise**.
3. Click the tab for the operating system that you want to download Splunk software.
4. Click the **Download Now** link for the OS version and installation package type that you want to install with.
5. On the next page that loads, read the Splunk Software License Agreement.
6. Click the **I have read, understood, and hereby accept the Splunk Software License Agreement** checkbox.
7. Click **Start your download now**. The page refreshes and the download begins.
8. On the next page that loads, in the **Useful tools** box, click **MD5 to verify**. A second file, the MD5 hash, begins to download.
9. After both downloads finish, complete the "Verify hashes" procedure.

Download Splunk Enterprise installation package and request SHA512 hash from Splunk Support

1. Complete Steps 1 through 7 of the "Download Splunk Enterprise installation package and MD5 hash" procedure.
2. Open a case with Splunk Support to receive the SHA512 hash. When you open the case, provide a link to the version, operating system, and type of installation package you downloaded.
3. After you receive a link to the hash, follow the link to download it.
4. After the package and SHA512 hash downloads finish, complete the "Verify hashes" procedure.

Verify hashes

After you download the package, verify it by running either the `md5sum` or `sha512sum` utilities:

1. Open a shell prompt.
2. Change to the directory where you downloaded the installation package and the MD5 hash.
3. Print the contents of the hash file that you downloaded:

MD5	SHA512
`cat splunk-xxxx-release.tgz.md5`	`cat splunk-xxxx-release.tgz.sha512`

4. Run the `md5sum` or `sha512sum` tool on the installation package that you downloaded:

MD5	SHA512
`md5sum splunk-xxxx-release.tgz`	`sha512sum splunk-xxxx-release.tgz`

5. Compare the output from the MD5 or SHA512 hash file against the result from the `md5sum` or `sha512sum` utilities.
6. If the hashes match exactly, then the package you downloaded is authentic and you can continue with the installation. If the hash does not match, try downloading the package again as it's incomplete or has been modified.

Verify Signatures

You can verify the authenticity of the downloaded RPM package using the Splunk GnuPG Public key as follows

1. Download the GnuPG Public key file (yes, this link is over TLS).
2. Install the GnuPG public key:

   ```
   rpm --import <filename>
   ```

3. Verify the package signature using:

   ```
   rpm -K <filename>
   ```

Proceed with installation from your authenticated installation package

After you have successfully verified your installation package as authentic, you can proceed with installation.

- Installation instructions in the *Installation Manual*