### Certificates

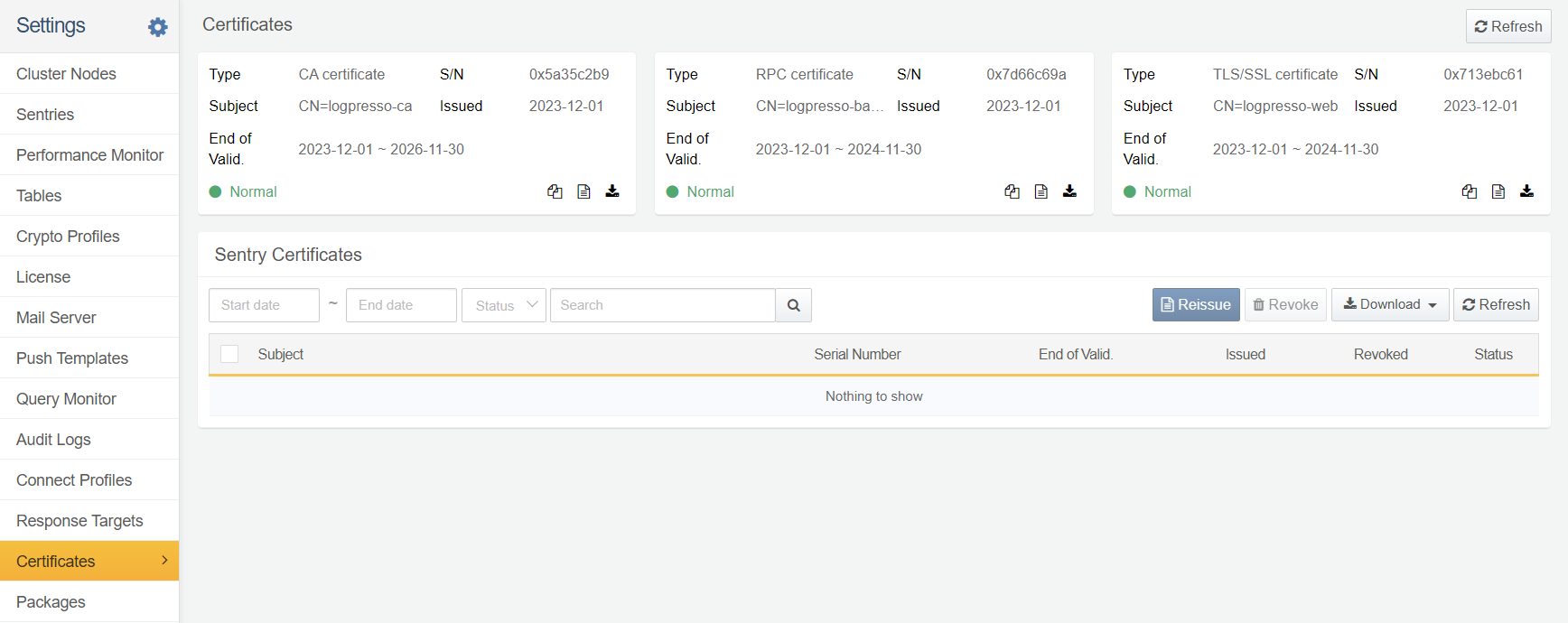
#### Overview

Certificates play a crucial role in modern cryptography and network communication, ensuring the trustworthiness of communication partners or facilitating the exchange of encryption keys for secure communication. The Certification Authority (CA) serves as a central authority that guarantees the trustworthiness of certificates, akin to a central bank in a currency system. Just as the Bank of Korea issues Korean Won (KRW) and regulates the amount of currency in circulation, a CA issues certificates and ensures their authenticity.

Logpresso uses a private CA system for self-signed certificates:

* **CA Certificate** - a certificate containing the CA's public key, which is shared with the Sentry and the user's web browser. It is the top level certificate used by the CA to validate web server certificates, RPC certificates and Sentry certificates signed with its private key.
* **Web Server Certificate** - a certificate used for TLS communication (TCP 443) between the Logpresso server and the user's web browser.
* **RPC Certificate** - a server certificate used for RPC communication (TCP 7140) between the Logpresso server and the Sentry.
* **Sentry Certificate** - a client certificate used in RPC communication (TCP 7140) between the Logpresso server and the Sentry.

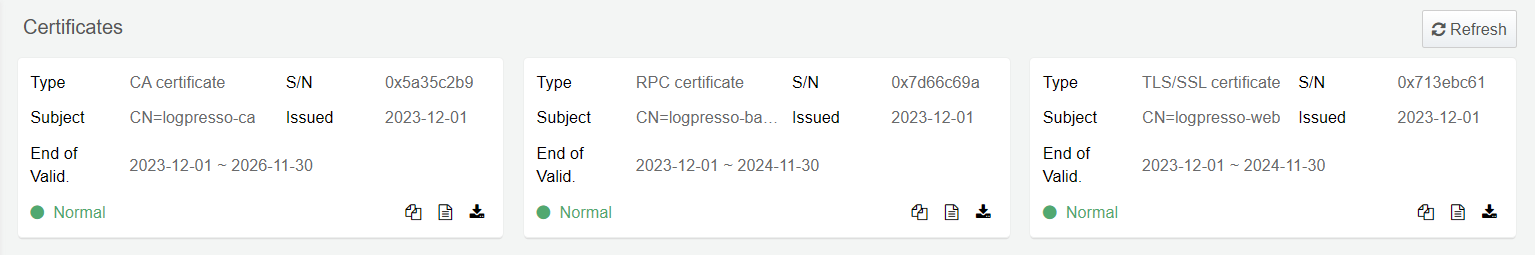
The CA certificate, web server certificates, and RPC certificates are automatically generated when the web installer runs upon a user's (cluster administrator's) first connection to the server. The Sentry certificate is generated when [you create the sentry](https://docs.logpresso.com/en/sonar/4.0/ui/section-sentries). You can manage the issued certificates from the **System** > **Certificates** page.



Logpresso server uses TCP 44300 (network port) to deploy Sentry installation files and certificates.

#### Server Certificate

All certificates issued by Logpresso server are listed in the **System** > **Certificates** page.



* **Type**: the type of certificate (CA certificate, TLS/SSL certificate, RPC certificate)
* **S/N**: a unique identifier assigned to a specific certificate
* **Subject**: Information about the entity to which the certificate is issued (CN, Common Name)
* **Issued**: Date the certificate was issued
* **Validity Period**: The period for which the certificate is valid

The status of the certificate is displayed in the bottom left corner of each certificate card; **Green** indicates that the certificate is valid. In the bottom right-hand corner of the certificate card are buttons for copying certificate information, reissuing and downloading the certificate.

Copy Certificate Information

Click the **Copy** icon to copy the certificate information to the clipboard. The copied information includes the certificate type, serial number, subject and validity period (start time, expiration time).

Reissue Certificate

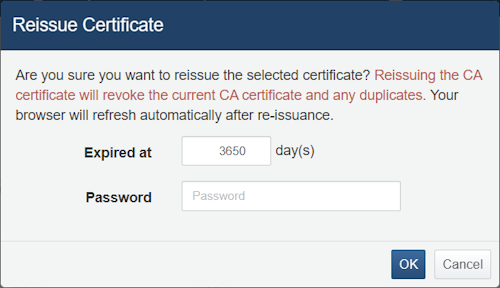
Initial server certificates are generated when the web installer is first run. Server certificates are used in communication with Sentries or when the server communicates with users' web browsers. These certificates have a validity period. All server certificates must be reissued before they expire.

Upon reissuance, RPC Certificates or Web Server Certificates will only replace the certificate used in that communication. However, **when you reissue the CA certificate, all server certificates and Sentry certificates are reissued at the same time.**

To reissue a server certificate:

Click the **Reissue** icon on the certificate card.

In the **Reissue Certificate** dialog, enter the **Expiration Date** and the **Certificate Password**, then click **Confirm**.

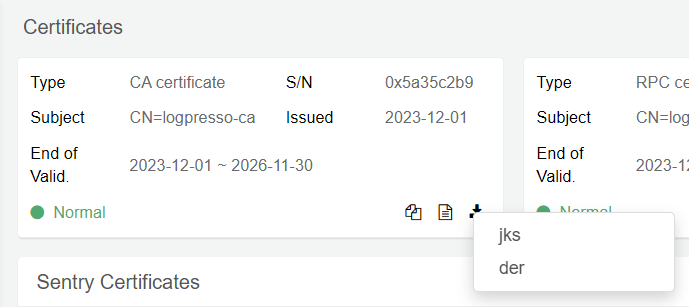


* The CA certificate is generated with a default expiration of 365 days (10 years).
* The default expiration for other server certificates is 365 days (1 year).

When a certificate is reissued, communication using that certificate is paused and restarted based on the new certificate.

Download Certificate

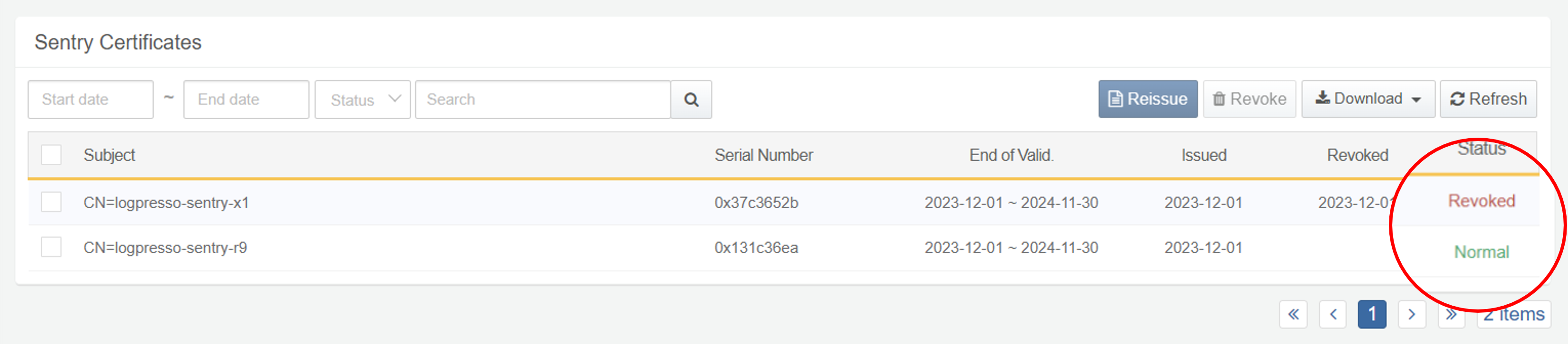
Click the **Download** icon on the certificate card to download the certificate. The file format varies depending on the type of server certificate. CA certificates are available in JKS or DER, while other server certificates are available in PFX.



JKS files are Java KeyStore (certificate) files. You can use keytool to store the certificate in the Java platform keystore. A DER file encodes X.509 certificate and private key data in DER (Distinguished Encoding Rules) format, suitable for use with programs such as openssl.

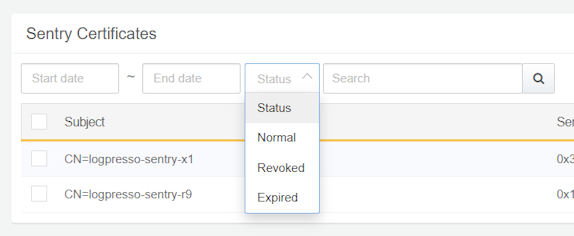
#### Sentry Certificate

A Sentry communicates with Logpresso server via a TLS channel. The Sentry certificate is generated the first time a Sentry is added to the server. You can view the list of the issued Sentry certificates in the **System** > **Certificates** page; This list shows both issued and revoked certificates.



Search for Certificate

You can search for a Sentry certificate by its expiration period, status, and keyword.



* **Start Date**, **End Date**: Search for certificates that expire within a specified range.
* **Status**: Status of the certificate (**Issued**, **Revoked**, **Expired**)
* **Search**: Certificate subject as keyword

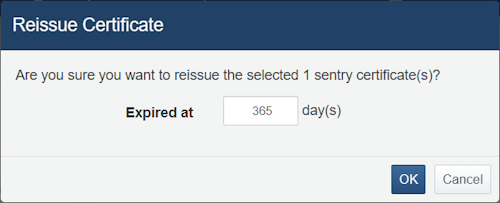
Reissue Certificate

To reissue a Sentry certificate:

From the Sentry certificate list, tick the checkbox of the certificate you want to reissue.

Click **Reissue** on the toolbar.

In the **Reissue Certificate** dialogue box, enter the **expiration date**. The default is 365 days.



Click **OK** to reissue the certificate. If you do not want to reissue the certificate, click **Cancel**.

* Clicking **OK** sends the reissued certificate to the Sentry and revokes the old certificate.
* The Sentry will reboot when it receives the new certificate.

Check the Sentry's connection status in **System > Sentries**.

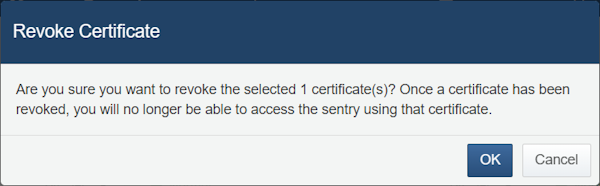
Revoke Certificate

To revoke a Sentry certificate:

From the Sentry certificate list, tick the checkbox of the certificate you want to revoke.

Click **Revoke** on the toolbar.

When the **Revoke Certificate** dialogue box appears, click **OK** to revoke the certificate. If you do not want to, click **Cancel**.



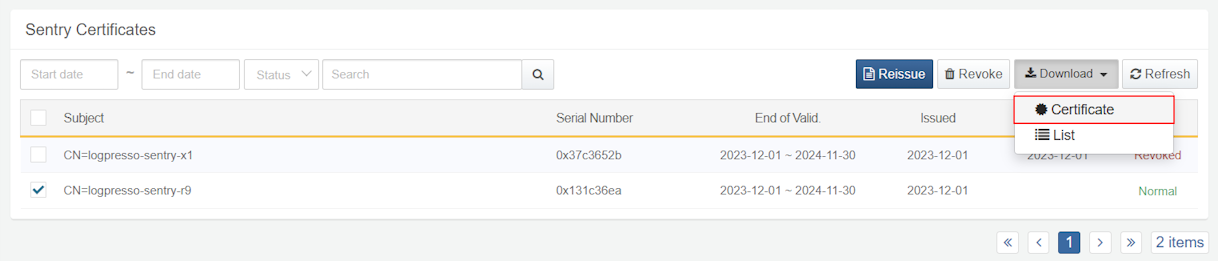
Check the Sentry's connection status in **System > Sentries**. If necessary, [remove the sentry](https://docs.logpresso.com/en/sonar/4.0/ui/section-sentries) from the Sentry list.

Download Certificate

To download a Sentry certificate:

From the Sentry certificate list, tick the checkbox of the certificate you want to download. Selecting the checkbox at the top of the list will select all certificates on the page you are viewing.

Click **Download > Certificates** from the toolbar.

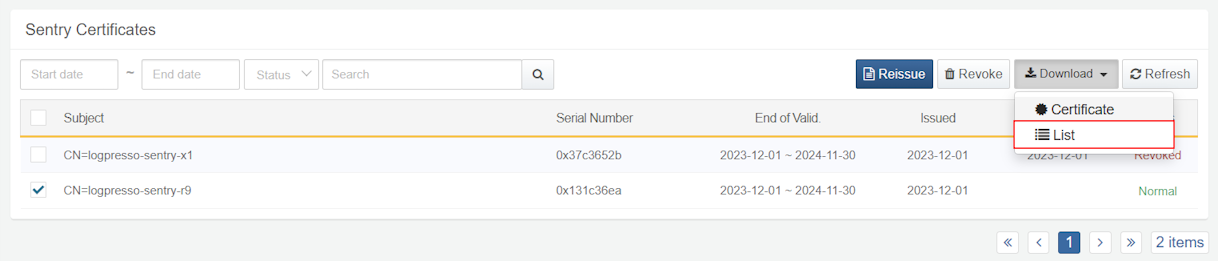


* The file is provided as a ZIP file containing the Sentry Certificate PFX file.
* Even if you select only one Sentry certificate, it will still provided as a ZIP file.

Download Certificate List

To download the Sentry certificate list:

Click on **Download > List** from the toolbar.



In the **Download Sentry Certificate List** dialog, specify the **File Name**, **Columns**, **File Format**, **Encoding**, and **Range**, then click **Confirm**.

