Recast

Certificates

Last Modified on 04.16.26

Certificates are used to secure connections, verify the identity of a third-party and to sign data. The certificate management interface allows you to import, export, generate and delete certificates that are known to the Application Workspace server(s). Certificates are globally stored in the database and are known to all the servers in the same Application Workspace System.

Import new certificate

The following formats can be imported:

- Personal Information Exchange – PKCS #12 (.pfx is the commonly used filename extension)
- Base 64 encoded X.509 (.cer/.crt/.pem are the commonly used filename extensions)
- DER encoded binary X.509 (.der is the commonly used filename extension)

PKCS #12 is the only format supported that can contain a private key. If importing a PKCS #12 certificate format, provide also the password for the private key.

Create self-signed

Description – A description for the newly to be created certificate.
Common name – A valid formatted DNS name, e.g. "www.liquit.com" or "saml-idp".
Days valid – The number of days the certificate is valid from the point of creation.
Key size – The size of the certificate keys, if in doubt, it's recommended to use the default of 2048.

Export certificate

The following formats are supported for exporting:

- Personal Information Exchange – PKCS #12 (.pfx is the commonly used filename extension)
- Base 64 encoded X.509 (.cer/.crt/.pem are the commonly used filename extensions)
- DER encoded binary X.509 (.der is the commonly used filename extension)

PKCS #12 is only available when the certificate contains a private key, it also requires a password to protect the private key in the exported file.

Certificates list

This list displays all certificates currently available in the Application Workspace System.

Selecting multiple rows from the table

- To select multiple adjacent rows, click on the first row, then hold down the Shift key and click on the last row in the range; all rows between will be selected.
- To select multiple non-adjacent rows, hold down the Ctrl key (or "Command" on Mac) and click on each row you want to select individually.
- To select multiple adjacent rows using the mouse only, click and hold the left mouse button on the first row, then drag the cursor up or down across the rows to highlight the desired ones.
- Selecting rows using only the keyboard is not possible.

Table toolbar

To create a new certificate, click on the ✚ **Create** button; to view the details of a certificate or edit it, double-click its entry

or select the certificate and click the **Edit** button.

Views gives you control on how the table is displayed.
The default view contains all your certificates in alphabetic ascending order, and only a few columns: **Subject**, **Issuer**, **Not after** and **Has private key**.
You can create your own personalized view of the table, by filtering the certificates or adding/deleting columns and clicking **Save as** in the drop-down menu of **Views**.

Detailed view of a certificate

See below the description of each screen in the detailed view of a certificate, and what actions you can perform in each of them.

Overview screen

Subject – The full name of the certificate.
Issuer – The full name of the entity that issued this certificate. In case of a self-signed certificate, it will be the same as the **Subject**.
Has private key – If the certificate also contains a private key next to the public key.
Not before – The date when this certificate becomes valid.
Not after – The date when this certificate expires.
Key size – The size of the keys.
Serial number – The serial number of the certificate; this is not per se unique and is decided by the certificate issuer.
Thumbprint – The checksum of the public key; this is a unique identifier for this certificate.
Description – A free fillable field where you can write the description of the certificate.

Tags screen

View, remove or add tags to your certificate. To add a tag, simply start typing in the lookup field for the desired tag and select it from the results lists. Or select the browse button ... at the right of the lookup field to open the **Tags** dialog box and view all the tags available. To view the details of a tag or edit it, double-click its entry.

> Note that the source of a managed tag is a system certificate and it cannot be changed.

Certificate Chain screen

The screen displays a certificate chain, or certification path, which is an ordered list of certificates used to authenticate an entity. The root CA certificate is always signed by the certificate authority (CA) itself and every certificate under it is trusted.

Dependencies screen

This screen displays an overview of the components that are using this certificate, for example identity providers, device registrations, domain or Splunk event collector.

Extensions screen

This will give a simplified overview of the X.509 extensions implemented into this certificate.

These v3 extensions allow certificates to be tailored to specific applications by allowing the inclusion of arbitrary fields to the certificate.

For self-signed generated certificates, this screen will be empty.

Auditing screen

View a comprehensive log of changes to this certificate, displaying the identity behind each modification.
This screen is available only if the auditing is enabled in the Database Event Collector. For more information, see Auditing.