



Release Notes

7.4.0 Community



2020-11-03



By PrimeKey Solutions AB

PrimeKey is offering EJBCA Community 7.4.0 before its official release in 2021. Take a short [survey about your use of EJBCA](#) to help us continue to develop EJBCA in the future and we will email you a link to download the newest release of EJBCA Community Edition with version 7.4.0.

This release note covers new EJBCA Community features implemented between EJBCA Community version 6.15.2.6 and EJBCA Community 7.4.0. Quite a bit has happened since EJBCA 6.15 - not least 436 bug fixes. This release includes bug fixes resolved relating to EJBCA Community and also contains a few security issue fixes.

1 Highlights

1.1 Technology Jump

With EJBCA Enterprise 7.0 we have done a technology jump and dropped support for JDK7 and JEE6. With this, the new minimum requirements for EJBCA are JDK8 and JEE7, and the earliest supported application server is Wildfly 10. If your current installation is running on an earlier JDK or application server we recommend upgrading those first, going through an intermediate release of EJBCA may be if necessary. To see if this applies to you, see detailed instructions for which workflow to follow in the [EJBCA Upgrade Guide](#).

1.2 CA UI Update

Minor changes in the UI are visible as we are moving away from old JSP pages into the more modern JSF technology. This will lay the foundation for our long-term goal to update and improve the EJBCA UI, so stay tuned.

1.3 Configurable SN Entropy, Default Value Raised to 20 Octets

In EJBCA the serial numbers are cryptographically randomized, and the size is configurable. As serial numbers must be positive, the relative entropy will always be $n-1$ of the serial number size. With [EJBCA Enterprise 7.0.1](#), we increased the default value for new CAs from 8 octets to 20 octets and moved the configuration to be per CA and in the UI. Previously this was set using the property `ca.serialnumberoctetsize` in `cesecore.properties`.

1.4 Downloadable CSRs

CSRs are now stored along with the associated certificate (instead of only the last submitted CSR as it was earlier), allowing you to download and review all CSRs submitted and processed also in the past.

1.5 Partitioned CRLs

Partitioned CRLs can now be activated under the CA configuration. The number of partitions per CRL is dynamically configurable, allowing new partitions to be added as the CRL grows, and assignment to older partitions to be suspended to allow for future growth. CDP partition assignment is random to allow for even distribution of certificates, and partition definition can be looked up in the CDP extension as defined in [RFC 5280](#). For more information, see [Partitioned CRLs](#).

1.6 IPv6 Support

The EJBCA support for Internet Protocol version 6 (IPv6) has been improved. As of [EJBCA 7.2.1](#), IPv6 has been thoroughly tested and improved for certain use cases.

1.7 View Queued Publisher Item Information

Items published with a publisher in EJBCA can be placed in a queue if direct publishing fails or because the publisher is configured to only use a queue for publishing.

The Publisher Queue Status table on the EJBCA CA Web home page has up until now only listed the number of queued events per publisher. Under certain circumstances, entries in the queue may not be able to publish for example, due to a network outage or denied authorization from the target.

You can now view status information about the queued events indicating why they are still queued, information on the latest updates and links to the relevant object. For more information, see [Publishers Overview](#).

1.8 Ed25519 and Ed448 Support

Edwards-Curve Digital Signature Algorithm (EdDSA) is now supported for software crypto tokens, with support for both Ed25519 and Ed448. For more information, see [EdDSA Keys and Signatures](#).

1.9 EJBCA CE Available on Docker Hub

For quite some time now, we've had [a docker container to Docker Hub](#), currently built on EJBCA 6.15 Community Edition, but soon to be upgraded to 7.4 as well. If you're interested in moving your PKI towards containerization, please go ahead and have a look, and feel free to give us any feedback!

2 Upgrade Information

For upgrade instructions and information on upgrade paths, see [Upgrading EJBCA](#). For a complete listing of features and improvements implemented in EJBCA Enterprise releases, see [EJBCA Release Notes Summary](#).