

V2.02.002

Build 000 (16 October 2023)

This release includes the following enhancements:

PTC Enroll Mobile

- Supports Android 13 (API level 33)
- Supports Google Play Store requirements

V2.02.001

Build 000 (02 March 2023)

This release includes the following enhancements:

PTC Enroll Mobile

- Modify the issued certificates permitted key usage
- Supports Android 12 (API level 31)
- Support Google Play Store requirements

V2.2

Build 000 (04 March 2021)

This release includes the following enhancements:

PTC Enroll Mobile

- Support Google Play Store requirements
- The application's self-update feature supports Android API level 29 and 30

This release includes the following components:

PTC Enrollment Web

- PTC Enrollment now supports .NET Framework 4.8
- PTC Enrollment now supports custom encryption in server certificates
- Clicking the online help in the PTC Enrollment Web deployed in both Preprod and Prod environments now displays the online help [CRM98798]

PTC Enroll Client

- The PTC Enroll Client now successfully installs a certificate in both Preprod and Prod environments without issues. The previous issue of the tool not installing the certificate in Production after finding an existing certificate with the same common name in Preprod has been rectified [CRM102406]
- PTC Enroll Client now works properly in computers with a screen resolution less than 1000x1000 pixels. The assembly version has been upgraded to version 4.52.0 and file version to 1.1.0, both of which are displayed at the bottom of the screen [CRM104492]

PTC Enroll Mobile

- PTC Enroll Mobile supports Android 10 (API level 29)

This release includes the following components:

PTC Enrollment Web Services

- It now requires the SAN attribute in certificate requests for server enrollment only
- The PTC Enrollment Web Services now includes a new feature: the **PTC Enrollment Certificate Services** – the web services interface to provide details of valid certificates to enrolled servers with new operations, and to check for:
 - the specific organization code and certificate common name for certificates issued to the organization, and to show these certificates if they exist and are valid (not expired nor revoked)
 - certificates issued previously (if still existing, not expired nor revoked)

PTC Enroll Client

- It now includes the SAN attribute in certificate requests for server enrollment only

PTC Enroll Mobile (2.00.001)

- It does not include the SAN attribute in certificate requests

The new PTC Enrollment suite supersedes the existing PTC Enrollment application. This suite consists of the following components:

- The **PTC Enrollment Web Services** - the web services interface to handle and provide feed-back to client applications
- The **PTC Enroll Client** - the application for enrolling client workstations/servers
- The **PTC Enrollment Web** - the web application to manage all enrollment requests
- The **PTC Enrollment Issuing Services** and the **PTC Enrollment Revoking Services** - the web services interface to handle operations with the subordinate Certificate Authority (CA)
- The **PTC Enroll Mobile** - the application for enrolling client mobile devices
- The **PTC Enrollment Import Export Tool** - the tool for migrating existing enrolled IFS Mobile certificates to PTC Enrollment

Details of these components are listed in the relevant section.

Deployment of all the web services and web application follows the recommended network topology to enhance security. All web services are published via HTTPS.

PTC Enrollment Web Services

First release (replaces the [ClientCertificateServices](#) component of IFS).

The Enrollment Web Services contain the following features:

- Receives enrollment requests, validates and sanitizes them, and stores their details in the database
- Checks if a certificate is available for a specific enrollment request and provides it if available
- Audits web service call activities
- Performs server side validation for the SAN attribute
- Requires the SAN attribute in certificate requests
- SSL settings follow security best practices by removing weak ciphers and protocols

PTC Enroll Client

First release.

This desktop application contains the following features:

- Creates client certificate request and submits it to the PTC Enrollment Web Services
- Checks certificate availability from the PTC Enrollment Web Services when a certificate request has been submitted
- Supports submission of external certificate request for server enrollment
- Displays client certificate details
- Downloads and installs refreshed PTC PKI CA and Intermediate CA certificates
- Validates access to the configuration file. If unavailable, displays an error message and closes the application
- Tests that the installed certificate can establish the correct SSL 2 way connection with the test service
- Copies to the clipboard the subject of the installed certificate to facilitate its use in other PTC applications
- Supports the **Subject Alternative Name (SAN)** attribute
- Tests and validates if the calling client certificate is able to establish the SSL 2 way connection

PTC Enrollment Web

First release.

This PTC hosted web site contains the following features:

- Lists every enrollment request for the business partner of the current user with the details listed below:
 - Identifier
 - Organization
 - Client type
 - Name (public URL for a server/name for a mobile device/Machine Fully Qualified Name for a workstation)
 - Status date
 - Enrollment status
 - User name
- Issues certificates or rejects enrollment requests
- Revokes currently enrolled certificates
- Audits enrollment activities
- Integrates Active Directory (AD) authentication with the current PTC AD infrastructure

- Allows the PTC Enrollment Manager to automatically update expired certificates
- Allows only the PTC Enrollment Manager to issue server certificates for any organization
- Allows only the DO Enrollment manager to issue client certificates for their own organization
- Uses a specific Active Directory (AD) group `ENR_J1CXXX`, where `XXX` is the organization code, to identify the user's DO
- SSL settings follow security best practices by removing weak ciphers and protocols

PTC Enrollment Issuing Services and PTC Enrollment Revoking Services

First release (replaces the `EnrollServices` from Enrollment Subordinate CA specific to IFS).

The CA Web Services contain the following features:

- Receives instruction to issue a new certificate, validates and sanitizes the instruction, issues the certificate in the Subordinate CA, and updates the certificate status in the database
- Receives instruction to revoke a certificate, validates and sanitizes the instruction, revokes the certificate in the Subordinate CA, publishes the Certificate Revocation List (CRL), and updates the certificate status in the database
- Publishes the CRL hourly, and the delta CRL every half hour
- The Issuing service can only be accessed internally from the PTC network

PTC Enroll Mobile (2.00.000)

- PTC Enroll Mobile is now compliant with the new PTC Enrollment suite, as per the following changes:
 - It now collects additional information such as the hardware and software specifications of the enrolling mobile device
 - A new screen has been added for users to specify the details of the fields listed below when creating/importing a certificate request
 - Country
 - State/Province
 - Locality/City
 - Email
 - Phone
 - Request Description
 - Displays more information to the user, such as the status of the certificate, during enrollment
 - Checks for enrollment application update requirement and prompts the user to update if an update is available

- Highlights the required fields in the enrollment request form and alerts the user if these have not been filled out
- Supports the SAN attribute

PTC Enrollment Import Export Tool

First release.

This tool exports certificates from the operator's IFS database and into PTC Enrollment.

PTC Enroll Mobile Version 1.00

V1.01, Build 001 (11 November 2016)

The enhancement and fixes listed here are shown with their associated PRCR numbers in brackets.

Fixes

- The PTC Enroll app now first verifies enrollment password before trying to get the certificate [PTC17]

V1.00, Build 001 (31 October 2016)

The enhancement and fixes listed here are shown with their associated PRCR numbers in brackets.

Enhancements

- The PTC Enroll app now complies with the new Enrollment Services and the new PTC CA authorities
- Client certificate and private key now have:
 - 2048 length private key [PTC61]
 - SHA512 as signature algorithm [PTC40]
 - SHA256withRSA as certificate request digest algorithm [PTC59]
- The application now includes the mobile device's Android ID in **Common name** attribute, business partner code in **Organization** attribute and Mobile Enroll as **Organization Unit** attribute of the certificate [PTC65]
- The PTC Enroll app now checks that the device ID of the mobile device running the application matches the client certificate common name [PTC52]
- CRL validation is now enabled [PTC73]

Fixes

- It is no longer possible to send a certificate request before checking the lock screen settings [PTC91]
- The PTC Enroll app now runs only on a mobile device that is not rooted or jail broken [PTC74]
- Before installation, the PTC Enroll app now checks the device's Android version if it is above 16 to prevent installation on non-supported Android devices [PTC80]

First release.

This release is a mobile application which contains the following features:

Enrollment process from IFS 4.15 which is composed of the functionality to:

- Submit client certificate request to IFS **ClientCertificatesServices** with 1024 length private key and SHA1 algorithm
- Collect client certificate from IFS **ClientCertificatesServices**
- Store the client certificate and its private key in a secure container of the mobile application, preventing backup of the key [PTC51]
- Run only on a mobile device with screen lock in place (PIN or password) [PTC75], not rooted or jail broken device [PTC37]

The PTC Enroll app also includes the following new features:

- Allow capture and storage of settings which include:
 - enrollment password with minimal strength validation [PTC84] and without allowing password change [PTC50]
 - setting URL
- Provide access to client certificate and its private key to other mobile applications installed on the device under the condition of providing enrollment password
- Automatic update feature with dedicated setting file [PTC83]
- English and French localization