

DigiCert® PKI Platform

Release Notes

Version 8.21.5

October 28, 2021



Legal Notice

Copyright © 2021 DigiCert, Inc. All rights reserved. DigiCert and its logo are registered trademarks of DigiCert, Inc. Other names may be trademarks of their respective owners.

The product described in this document is provided by DigiCert, Inc. and distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of DigiCert, Inc. and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. DIGICERT, INC. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The licensed software and documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the licensed software and documentation by the U.S. Government shall be solely in accordance with the terms of this documentation.

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
<https://www.digicert.com/>

DigiCert® PKI Platform 8.21.5 Release Notes

DigiCert PKI Platform is a cloud-hosted service provided by DigiCert, Inc.

This document includes the following topics:

- [What's New in 8.21.5](#)
- [Component Support Updates](#)
- [Platform Support Updates](#)
- [Documentation](#)
- [Issues Addressed](#)
- [Known Issues](#)

What's New in 8.21.5

This release notes accompany the delivery of the DigiCert PKI Platform 8.21.5 release, henceforth referred to as PKI Platform.

PKI Platform is a cloud-hosted service, so your enterprise receives the latest releases as soon as the service is live.

Table 1 – New in 8.21.5

New to 8.21.5	Description
DigiCert Desktop Client enhancements	<ul style="list-style-type: none"> Support for non-escrow certificates using the Client Authentication and S/MIME (Digital signature only) templates on hardware tokens. Profiles can enforce the use of either a software/browser keystore or a hardware token. When choosing a hardware token, you can select a specific DigiCert-qualified token family to be used. Currently, DigiCert supports Gemalto tokens only. However, there is a profile option to select “Any” token, which will allow testing and use of other tokens, but not formally qualified. PKI Certificate Services portal support for renewal via proof-of-possession of private key flow.
UAA enhancements	<ul style="list-style-type: none"> Support for renewal of certificates via the UAA User portal after authenticating against your SAML IdP. <p>Note: ensure the renewal email template is modified with the correct UAA User portal URL.</p>
Linux support for web flows	<ul style="list-style-type: none"> Browser-based enrollment support for Linux machines, for both escrowed and non-escrowed certificates, for profiles configured with the “OS/Browser” enrollment method.
Resources - KB article for CA hierarchies	<ul style="list-style-type: none"> Update to the Resources area in PKI Manager with a link to a KB article from where to download all CA hierarchies used by Production and Test Drive RA certificates.

Component Support Updates

All software components are available from the **Resources** page within the PKI Manager web portal.

Table 2 – Additional components supported by PKI Platform 8.21.5

Components	Version Supported
PKI Client	2.21.5
PKI Enterprise Gateway, including Autoenrollment Server	1.21.1
PKI Web Services (SOAP API)	8.19
REST API	1.0.36
PKI Client – Android app	2.0.1

Platform Support Updates

PKI Platform 8.21.5 supports the platforms and operating systems detailed in the below sections.

Note: In addition to the supported platforms and operating systems, PKI Platform and its components may work on other platforms or operating systems. However, DigiCert does not guarantee technical support related to issues that may arise on platforms or operating systems that are not listed here.

PKI Manager

PKI Manager is a web portal hosted in DigiCert's data center. It allows PKI Platform administrators to perform account, user, certificate, and key management tasks. In order to access the PKI Manager portal, you need an administrator certificate installed on the PKI Client, which is protected by a PIN (2nd factor).

Table 3 – PKI Manager operating system and browser support matrix

Operating systems	Browsers
Windows 7 Enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer 11 ^a Firefox 93 Chrome 94
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11 ^a Firefox 93 Chrome 94

Operating systems	Browsers
Windows 10 Enterprise edition (32-bit and 64-bit)	Internet Explorer 11 ^a Firefox 93 Chrome 94 Microsoft Edge 94
Mac (Catalina, Mojave, High Sierra)	Firefox 93 Microsoft Edge 94 Chrome 94

^a Edge Mode on Internet Explorer is supported.

PKI Certificate Services

PKI Certificate Services are a set of DigiCert-hosted web pages that enable users to request, install, renew, and recover encryption certificates using a web browser.

The below matrix shows the browsers that have been fully qualified by DigiCert using all supported enrollment and authentication methods, but other browser may also work.

Table 4 – PKI Certificate Services operating system and browser support matrix

Operating systems	Browsers
Windows 7 enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer 11 ^{a, b} Firefox 93
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11 ^{a, b} Firefox 93
Windows 10 (32-bit and 64-bit)	Internet Explorer 11 ^{a, b, c} Firefox 93 Microsoft Edge 94
macOS Sierra (10.12)	Safari 11.1.2 Firefox 93
macOS High Sierra (10.13)	Safari 11.1.2 Firefox 93
macOS Mojave (10.14)	Firefox 93
macOS Catalina (10.15)	Firefox 93

^a The renewal plug-in is not supported in Internet Explorer 11 if Enhanced Protection Mode (EPM) is enabled. EPM is disabled by default in Internet Explorer 11.

^b Renewal of OS browser certificates supported only for Internet Explorer.

^c Edge mode is not supported.

PKI Client

PKI Client is a middleware software for digital signing, authentication, and data protection for desktop-based applications. It supports auto-renewal of certificates under management and auto-configuration of third-party applications via Post Processing scripts configured by a PKI Administrator. It uses digital certificates on smart cards, Intel TPM chips, security devices, or users' workstations using its own secure virtual keystore (vToken).

Table 5 – PKI Client operating systems and browser support matrix

Operating systems	Browsers
Windows 7 enterprise edition SP1 (64-bit)	Internet Explorer 11 Firefox 93 Chrome 94
Windows 8.1 enterprise edition (32-bit and 64-bit)	Internet Explorer 11 Firefox 93 Chrome 94
Windows 10 enterprise edition (32-bit and 64-bit)	Internet Explorer 11 Firefox 93 Chrome 94 Microsoft Edge 94
macOS Sierra (10.12) ^a	Safari 11.1.2 Firefox 93 Chrome 94 Microsoft Edge 94
macOS High Sierra (10.13) ^a	Safari 11.1.2 Firefox 93 Chrome 94 Microsoft Edge 94
macOS Mojave (10.14) ^b	Firefox 93
macOS Catalina (10.15) ^c	Firefox 93

^a PKI Platform does not support Government Edition CAC and PIV smart cards on the macOS Sierra and macOS High Sierra operating systems.

^b Safari Version 12 or higher and Client Authentication using eToken is not supported on Chrome & Firefox from macOS Mojave.

^c On macOS Catalina, certificate pickup on Hardware token using Firefox (ONLY) will not work without TokenD enabled in the system. For workaround and details, please refer: [KB article](#).

PKI Client for Android

Table 6 – PKI Client Android version support matrix

Type	Version
Android Pie	9.0
Android Oreo	8.1

Mobile Device

PKI Platform supports issuing digital certificates on all devices running on Android, iOS 11, 12 and 13.

User Authorization Agent (UAA)

The User Authorization Agent (UAA) is a service hosted in DigiCert’s data center. It allows PKI Platform administrators to provide details of SAML IdP configurations to perform authentication/authorization before allowing DigiCert to issue a certificate, based on the certificate profile requirements you have set.

UAA service details:

- The UAA service supports both SAML 2.0 IdP and SP-initiated flows.
- The UAA service is composed of two web portals: UAA Admin and User portals.
- The UAA service is enabled by configuring a supported certificate template with the “Federated Auth” authentication method.

Note: UAA service is not available for Test Drive accounts.

Supported Certificate Templates and Enrollment Methods

List of supported certificate templates and associated enrollment methods that support “Federated Auth”

Table 7 – UAA certificate templates and enrollment method support matrix

Certificate Template	Enrollment Method
All Templates in Device and Server Seat Pools	<ul style="list-style-type: none"> • CSR
Client Authentication S/MIME (Digital Signature only)	<ul style="list-style-type: none"> • Browser PKCS12 • DigiCert Desktop Client

Note: Manual approval flow is supported for all the above Enrollment Methods, when configuring a Device or Server profiles with a private CA, “Federated Auth” as the authentication method and the “Enable manual approval” option is checked within the UAA Admin portal.

UAA Admin Portal

A portal accessed by PKI Administrators using the same administrator certificate securely stored on DigiCert PKI Client used to access PKI Manager. It allows an administrator to configure SAML profiles detailing where certificate data is sourced from (e.g. Fixed values set by an administrator, from a CSR, from a SAML Assertion) and how users go about enrolling/provisioning certificates (e.g. via a Browser PKCS12 flow, or using the DigiCert Desktop Client to interact with browser keystores).

Table 8 – UAA Admin Portal operating systems and browser support matrix

Operating System	Browser
Windows 10	Chrome 94
Mac OS (10.14.6)	Firefox 93
	Microsoft Edge 94

UAA User Portal

A portal accessed by end-users to enroll for certificates based on a profile configured by their administrator. Users can authenticate against their SAML IdP provider and land on a UAA User self-service portal, from where they can perform various operations against profile that been configured by their administrator: enroll, download, revoke a certificate.

Users can also be given a specific URL that is bound to a profile and upon clicking on it, they will be redirected to their SAML IdP provider to authenticate/authorize before returning to the UAA User portal from where they can initiate the enrollment process and get a certificate provisioned via the method set by the administrator within the profile.

Table 9 – UAA User Portal operating systems and browser support matrix

Operating System	Browser
Windows 10	Chrome 94
Mac OS (10.14.6)	Firefox 93
Linux (Ubuntu 18.04)	Microsoft Edge 94(Windows/Mac)
iOS 13	Safari (13.1 or later on Mac)
Android 9 (Pie)	Safari (13 on iOS 13)
	Chrome (69.0 on Android 9)

For UAA configuration details, please refer to the below KB article:

[https://knowledge.digicert.com/solution/User-Authorization-Agent\(UAA\).html](https://knowledge.digicert.com/solution/User-Authorization-Agent(UAA).html)

DigiCert Desktop Client

DigiCert Desktop Client can be used to generate keys and install software certificates across various browsers and platforms (Windows and macOS), when configuring a profile with the “DigiCert Desktop Client” enrollment method using the below certificate templates:

- Client Authentication
- S/MIME (Digital Signature only)

Table 10 – DigiCert Desktop Client operating systems and browser support matrix

Operating systems	Browsers
Windows 10 (32-bit and 64-bit)	Chrome 94 Firefox 93 Microsoft Edge 94
macOS Mojave (10.14.6) macOS Catalina (10.15.2)	Chrome 94 Firefox 93 Microsoft Edge 94 Safari (13.1 or later)

Note: Other browsers may work but have not been formally qualified by DigiCert.

Table 11 – Supported DigiCert Desktop Client version

Components	Version Supported
DigiCert Desktop Client	3.3.0

Table 12 – Supported DigiCert Desktop Client templates and auth methods

Certificate Template	Authentication Method
<ul style="list-style-type: none"> Client Authentication S/MIME (Digital Signature only) 	<ul style="list-style-type: none"> Manual approval Enrollment Code Active Directory Federated Auth

Notes:

- DigiCert Desktop Client support for the “Active Directory” authentication method is verified only on Windows 10 Operating system.
- The DigiCert Desktop Client can be downloaded from:
<https://pki-ddc.symauth.com/desktopclient>

Table 13 – DigiCert Desktop Client supported hardware tokens

Hardware token vendor	Hardware token model
Gemalto	<ul style="list-style-type: none"> eToken 5100 eToken 5110 eToken 5300^a

^a eToken 5300 cannot run alongside the DigiCert PKI Client software for Windows machines.

Note: Other tokens may work, but have not been formally qualified by DigiCert.

Documentation

Unless otherwise noted, all PKI Platform documents are available from the **Resources** page within the PKI Manager portal. Alternatively, you can also download a history of Release Notes from this [KB article](#).

Issues Addressed

Issues addressed within this release include:

- DPPC-3043: fixed issue where revocation emails were sent to end-users when profile was configured with the renewal email template notification set to “Send notification: No”.
- DPPC-3178: modified the format of the Domain Component attributes inside the SAN-DirectoryName extension from PrintableString to UTF8String, except for the Country attribute.
- DPPC-3356: removed “Last 1 year from generation date” and “Last 2 years from generation date” options from all scheduled report types. Instant reports can be used to generate yearly or bi-yearly reports, if required.
- DPPC-3387: change to respect the label used to map a certificate field against a Seat ID during web-based certificate enrollment flow, when clicking the Back button on the web page.
- DPPC-3390: updated the EST Service to also support HTTP Basic Authentication requests using a format of “Authorization: Basic <base64-encoded-global-passphrase-value>” for EST profiles configured with the Global Passphrase authentication method.

Known Issues

The following are the known issues in this release:

- The DigiCert PKI Client for Android application is built using API version 26 best suited for Android Oreo (8.1) and below.

The application functionality has been verified on Android 9 (Pie) and Android Q. In some cases, for Android Pie and Q, while opening the application for the first time, you might get an alert stating, “Detected Problems with API”. Click “OK” and proceed as the functionality has been successfully verified on both these Android versions.

- On iOS, certificate renewal after its expiry may not happen as expected. There is no workaround to this issue.
- iOS renewals will not work if user kicks off the process from the renewal link which is sent in the renewal e-mail. User must renew the iOS certificate from iPhone’s/iPad’s settings by updating the profile.
- While installing certificate on iOS for iPhones, although the certificate profile gets downloaded, the DigiCert UI displays a message showing “Your Certificate is not installed”.
- User/Admin enrollment on any Browser, any Operating System, may result into a Blank Page without any progress if the Symantec branded Browser extension is not removed from the Browser from where enrollment is attempted. Please manually remove the Symantec branded browser extension and install the DigiCert branded browser extension as provided on our instructions page and then restart the browser. Certificate enrollment should work fine after this procedure.
- Safari version 12 or higher is not supported on any macOS, due to an Apple API change affecting the PKI Client Safari extension.
- Client Authentication using eToken is currently not supported on Chrome & Firefox from macOS.
- For Mac and Windows OS, while accessing the PKI Manager portal using the PKI Client in Firefox browser, an error message may be displayed with the error code: **SSL_ERROR_HANDSHAKE_FAILURE_ALERT**.



This can be resolved by navigating to the settings of the Security Devices for PKI Client. From the **Open Menu** panel select -> **Options** -> type "Certificate" in **Find in Options** text field -> click on **Security Devices** button, and

1. Click the **Load** button and select the **PKCS 11** module.
2. Browse to the path where the PKCS 11 module is located:

For Mac: /usr/local/lib/tblive-4/PKCS11.so

For Windows: C:\Program Files\DigiCert\PKI Client\PKCS11.dll

3. Click **OK**.

You will be able to access the PKI Manager portal successfully.

For more details on the steps, please refer: [KB article](#)

- Certificate information report will not include **Other Name (GUID)** information for historic certificate data. This data will only be included within the report for certificates issued after the 30th Sep 2020, since this enhancement was delivered as part of the DigiCert PKI Platform v8.20.5 release.