DigiCert® PKI Platform

Release Notes

Version 8.21.1

April 15, 2021

Legal Notice

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

DigiCert® PKI Platform 8.21.1 Release Notes

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

This document includes the following topics:

- What's New in 8.21.1

- Component Support Updates

- Platform Support Updates

- Documentation

- Issues Addressed

- Known Issues

What's New in 8.21.1

This release notes accompany the delivery of the DigiCert PKI Platform 8.21.1 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 8.21.1

New to 8.21.1	Description
REST API – Search endpoint	• New REST API endpoint to allow for certificate search operations based on various filters – see REST API documentation for details. • Updated REST API documentation and Swagger with CSR format requirements and SAN extension examples.
Multiple IP addresses in SAN	Support for multiple IP addresses within the SAN extension for the Generic Server certificate template and some custom server templates, when configured with any enrollment method except SCEP and EST.
UAA portal enhancements	Enhancements to the User Authorization Agent (UAA) Admin and User portals, used to authenticate end-user requests via a customer SAML IdP: • UX redesign of the UAA User portal • Support for custom authentication fields • Support for multiple key sizes (set within PKI Manager) • Support for reading multiple dnsName entries from CSR • Support to configure private key not to be exported for profiles configured with DigiCert Deskotp Client (for Windows platforms only)
PKI Enterprise Gateway installer enhancement	The PKI Enterprise Gateway custom installer flow has been updated to enable customers with stringent security policies, to skip the Active Directory changes so that they are reviewed before manually executing by a Domain administrator.

Component Support Updates

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

Table 2 – Optional components that PKI Platform 8.21.1 supports

Components	Version Supported
PKI Client	2.20.7
PKI Enterprise Gateway, including Autoenrollment Server	1.21.1
PKI Web Services	8.19
PKI Client-Android	2.0.1

Platform Support Updates

PKI Platform 8.21.1 supports the platforms and operating systems detailed in the below sections.

<u>Note</u>: 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 PKI Manager portal, you need an administrator certificate hosted on the PKI Client agent.

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 83 Chrome 87
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 83 Chrome 87
Windows 10 Enterprise edition (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 83 Chrome 87

Operating systems	Browsers
Mac (Catalina, Mojave, and High Sierra)	Firefox 83

[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 83
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11[a, b] Firefox 83
Windows 10 (32-bit and 64-bit)	Internet Explorer 11[a, b, c] Firefox 83
macOS Sierra (10.12)	Safari 11.1.2 Firefox 83
macOS High Sierra (10.13)	Safari 11.1.2 Firefox 83
macOS Mojave (10.14)	Firefox 83
macOS Catalina (10.15)	Firefox 83

[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 83 Chrome 87
Windows 8.1 enterprise edition (32-bit and 64-bit)	Internet Explorer 11 Firefox 83 Chrome 87
Windows 10 enterprise edition (32-bit and 64-bit)	Internet Explorer 11 Firefox 83 Chrome 87
macOS Sierra (10.12)[a]	Safari 11.1.2 Firefox 83 Chrome 87
macOS High Sierra (10.13)[a]	Safari 11.1.2 Firefox 83 Chrome 87
macOS Mojave (10.14)[b]	Firefox 83
macOS Catalina (10.15)[c]	Firefox 83

[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 idP and SAML 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

    <u>Note</u>: 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	• CSR
Client Authentication S/MIME (Digital Signature only)	• Browser PKCS12 • DigiCert Desktop Client

<u>Note</u>: 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.

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 Mac OS (10.14.6)	Chrome 87 Firefox 83 Microsoft Edge 87

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 Mac OS (10.14.6) Linux (Ubuntu 18.04) iOS 13 Android 9 (Pie)	Chrome 87 Firefox 83 Microsoft Edge (87 Windows/Mac) Safari (13.1 or later on Mac) Safari (13 on iOS 13) Chrome (69.0 on Android 9)

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 87 Firefox 83 Microsoft Edge 87
macOS Mojave (10.14.6) macOS Catalina (10.15.2)	Chrome 87 Firefox 83 Microsoft Edge 87 Safari (13.1 or later on Mac)

<u>Note</u>: 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	3.2.1

Table 112 – DigiCert Desktop templates and authentication methods support matrix

Certificate Template	Authentication Method
• Client Authentication • S/MIME (Digital Signature only)	• Manual approval • Enrollment Code • Active Directory • Federated Auth

Notes:

a) DigiCert Desktop Client support for the "Active Directory" authentication method is verified only on Windows 10 Operating system.

b) The DigiCert Desktop Client can be downloaded from:
https://pki-ddc.symauth.com/desktopclient

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-208] PKI Enterprise Gateway RA service does not start when using LDAP as a user store

- [DPPC-2673] PKI Client Admin Guide -- Correct the Registry Hive location for AE

- [DPPC-2502] AE, PKI-MGR: Client Authentication Response does not Include ICA

- [DPPC-2503] DigiCert Desktop Client – removed non-relevant renewal email templates for enrollment code profiles

- [DPPC-2274] Alphabetically ordered Enrollment Methods within the dropdown list

- [DPPC-2254] Make SAN IP Address field attribute as optional in Profile creation

- [DPPC-2228] Missing Seat_ID value or incorrect SEAT_ID value on Enrollment/pickup emails

- [DPPC-2172] Certificate email template change in one profile automatically changes other

- [DPPC-1777] Modify unsupported browser page to reflect correct browsers

- [DPPC-250] SAN URI is not available in SAN drop-down list for "Generic Device Authentication for Intune-SCEP" template

- [DPPC-2131] Custom email notification behavior changes for 'set-default' option

- [DPPC-2577] REST: some cert attributes are ignored for Manual approval profiles during enrollment

- [DPPC-2720] Users are not returned when searching for users under Manage Users page in PKI Manager, enrolled in all or specific profiles as search filters

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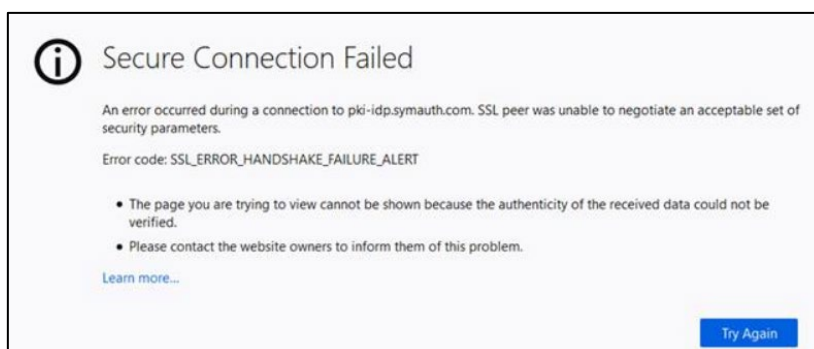
This can be resolved by navigating to the settings of the Security Devices for PKI Client. From the **Open Menu** panel select -> **Options** -> type "Certificate" in **Find in Options** text field -> click on **Security Devices** button, and

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.