

DigiCert® PKI Platform

Release Notes

Version 8.20.2

May 27, 2020



Legal Notice

Copyright © 2020 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 8.20.2 Release Notes

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

This document includes the following topics:

- [What's New in 8.20.2](#)
- [Component Support Updates](#)
- [Platform Support Updates](#)
- [Documentation](#)
- [Issues Addressed](#)
- [Known Issues](#)

What's New in 8.20.2

This release notes accompany the delivery of the DigiCert PKI Platform 8.20.2 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 8.20.2

New to 8.20.2	Description
Support for 'evergreen' device certificates	<p>Allows for the issuance of 'evergreen' certificates for devices, expiring on year 9999, using a new Base Certificate Template (BCT) called "Generic Device Authentication (Evergreen validity)".</p> <p>An 'evergreen' CA policy also needs to be applied to the issuing CA, which will also disable CDP and AIA extensions within issued certificates.</p> <p>NOTE: Contact your DigiCert representative to bind the "new BCT" to your chosen private CA on your account.</p>
Support for MacOS using Firefox browser for PKI Manager portal	PKI Manager portal has now been formally qualified and supports the Firefox browser running on MacOS High Sierra, Mojave, and Catalina.
DigiCert Proxy Server support for both SCEP and EST, including renewal flows	<p>SCEP and EST support for the DigiCert Proxy Server, which can be deployed at your organization to proxy both SCEP and EST certificate requests against your DigiCert PKI Platform account. This also includes support for renewal operations.</p> <p>NOTE: Contact your DigiCert representative to gain access to the software.</p>
PKI Client minor enhancements	Minor bug fixes and enhanced usage data tracking.

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 8.20.2 supports

Components	Version Supported
PKI Client	2.20.2
PKI Enterprise Gateway, including Autoenrollment Server	1.19
PKI Web Services	8.19
PKI Client-Android	2.0.1

^a PKI Platform 8.20.2 supports previous versions of PKI Client. However, you must run v2.20.2 or higher to benefit from the features that are described in this release notes.

Platform Support Updates

PKI Platform 8.20.2 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 PKI Manager portal, you need an administrator certificate hosted on the PKI Client agent.

Table 3 - PKI Manager operating system and browser support

Operating systems	Browsers
Windows 7 Enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer 11 ^a Firefox 76 Chrome 83
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11 ^a Firefox 76 Chrome 83

Operating systems	Browsers
Windows 10 Enterprise edition (32-bit and 64-bit)	Internet Explorer 11 ^a Firefox 76 Chrome 83
Mac (Catalina, Mojave, and High Sierra)	Firefox 76

^a Edge Mode on Internet Explorer is supported.

PKI Certificate Services

PKI Certificate Services are webpages hosted in DigiCert's data center that enable users to request, install, renew, and recover encryption certificates.

Table 4 - PKI Certificate Services operating system and browser support

Operating systems	Browsers
Windows 7 enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer 11 ^a Firefox 76
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11 ^a Firefox 76
Windows 10 (32-bit and 64-bit)	Internet Explorer 11 ^{a, b} Firefox 76
macOS Sierra (10.12)	Safari 11.1.2 Firefox 76
macOS High Sierra (10.13)	Safari 11.1.2 Firefox 76
macOS Mojave (10.14)	Firefox 76
macOS Catalina (10.15.2)	Firefox 76

^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 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

Operating systems	Browsers
Windows 7 SP1 (64-bit)	Internet Explorer 11 Firefox 76 Chrome 83
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11 Firefox 76 Chrome 83
Windows 10 (32-bit and 64-bit)	Internet Explorer 11 Firefox 76 Chrome 83
macOS Sierra (10.12) ^a	Safari 11.1.2 Firefox 76 Chrome 83
macOS High Sierra (10.13) ^a	Safari 11.1.2 Firefox 76 Chrome 83
macOS Mojave (10.14) ^b	Firefox 76
macOS Catalina (10.15.2) ^c	Firefox 76

^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

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.

Documentation

The following documents have been revised to incorporate PKI Platform 8.20.2 specific material:

- *DigiCert PKI Platform 8.20.2 Release Notes*

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

For information about fixed issues and other workarounds, see the DigiCert Knowledge Center for PKI Platform at the following URL:

<https://knowledge.digicert.com/>

- Enter **Issues addressed in DigiCert PKI Platform 8.20.2** as the Knowledge Center Search text to obtain a list of the issues addressed.

Known Issues

The following are the known issues in this version:

- 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](#)