Symantec™ Managed PKI 8.17.8 Release Notes

Symantec™ Managed PKI 8.17.8 Release Notes

Symantec Managed PKI (MPKI) is a cloud-hosted service provided by DigiCert, Inc., which acquired Symantec's Website Security and related PKI solutions business on October 31, 2017.

This document includes the following topics:

What's New in 8.17.8

These release notes accompany the delivery of the Symantec Managed PKI 8.17.8 release. MPKI is a cloud-hosted service, so your enterprise receives the latest releases as soon as the service is live.

Table 1-1 New in 8.17.8

New to 8.17.8	Description
Bug fixes	For more information, see “Issues Addressed, Known Issues, and Workarounds” on page 7.
S/MIME Remediation	Modified the Enrollment Code behavior for the S/MIME certificate template, in order to support the migration of Public CAs from Symantec to DigiCert CA hierarchy.
New CSP support for Client Authentication certificates	Support for the new Microsoft Enhanced RSA and AES CSP for Client Authentication certificates using OS/Browser Enrollment Method and enrollment code/manual approval as the Authentication Methods. (available as a Custom certificate template upon request).

Component Support Updates

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

Table 1-2 Optional components that Managed PKI 8.17.8 supports

Component	Version Supported
PKI Client	2.17.7[a]
PKI Enterprise Gateway, including: Autoenrollment Server	1.17
PKI Web Services	1.17.3

[a] Managed PKI 8.17.8 supports previous versions of PKI Client. However, you must run v2.17 or higher to benefit from the features that are described in this release notes.

Platform Support Updates

Managed PKI 8.17.8 supports the following platforms and operating systems.

Note: In addition to the supported platforms and operating systems, Managed PKI 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 Managed PKI administrators to perform account, user, certificate, and key management tasks.

Table 1-3 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 63
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 63
Windows 10 Enterprise edition (32bit and 64-bit)	Internet Explorer 11[a] Firefox 63

[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 1-4 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 63
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 63
Windows 10 (32-bit and 64-bit)	Internet Explorer 11[a, b] Firefox 63
macOS Sierra (10.12)	Safari 11.1.2 Firefox 63
macOS High Sierra (10.13)	Safari 11.1.2 Firefox 63

[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 middleware software for digital signing, authentication, and data protection for desktop-based applications. It uses digital certificates on smart cards, security devices, or users' workstations.

Table 1-5 PKI Client operating systems and browser support

Operating systems	Browsers
Windows 7 SP1 (64-bit)	Internet Explorer 11 Firefox 63 Chrome 71
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11 Firefox 63 Chrome 71
Windows 10 (32-bit and 64-bit)	Internet Explorer 11 Firefox 63 Chrome 71
macOS Sierra (10.12)[a]	Safari 11.1.2 Firefox 63 Chrome 71
macOS High Sierra (10.13)[a]	Safari 11.1.2 Firefox 63 Chrome 71

[a] Managed PKI does not support Government Edition CAC and PIV smart cards on the Mac OS Sierra and macOS High Sierra operating systems.

Mobile Device

Managed PKI supports issuing digital certificates on all devices running iOS 11 and 12.

Documentation

The following documents have been revised to incorporate Managed PKI 8.17.8 specific material:

- *Managed PKI 8.17.8 Release Notes* (this document)

Unless otherwise noted, all Managed PKI documents are available from the **Resources** page within the PKI Manager portal.

Issues Addressed, Known Issues, and Workarounds

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

https://knowledge.digicert.com/

- Enter **8.17.8** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI 8.17.8** as the Knowledge Center Search text to obtain a list of the issues addressed.

Addressed Issues

The following issues have been addressed in this version:

- No bug fixes

Known Issues

The following are the known issues in this version.

- On iOS, certificate renewal after its expiry may not happen as expected. There is no workaround to this issue.
- iOS renewals won't 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.
- PKI Client won't support macOS Mojave.

Legal Notice

DigiCert, Inc.

2801 North Thanksgiving Way, Suite 500

Lehi, UT 84043

https://www.digicert.com