Symantec™ Managed PKI 8.17 Release Notes

Symantec™ Managed PKI 8.17 Release Notes

This document includes the following topics:

What's New in 8.17

These release notes accompany the delivery of the Symantec Managed PKI 8.17 release. Managed PKI is a cloud-hosted service, so enterprises automatically receive the advantage of the latest releases as soon as the service is live. However, you may need to update some components that you have installed at your enterprise location, as described in these release notes.

This release of Managed PKI provides the following updates:

Updated Component Support

Table 1-1 lists the optional components that Managed PKI 8.17 supports.

All components are available from the **Resources** page of PKI Manager.

Table 1-1 Supported components

Component	Version Supported
PKI Client	2.17[a]
PKI Enterprise Gateway (including Autoenrollment Server)	1.17
PKI Web Services	1.17

[a]Managed PKI 8.17 supports previous versions of PKI Client. However, you must be running v2.17 or higher to benefit from the features that are described in these release notes.

Updated Platform Support

Managed PKI 8.17 supports the following platforms and operating systems (OS).

Symantec cannot test every combination of third-party client, server, operating system, service pack, and so on. Managed PKI and its components may work on other platforms or operating systems. However, Symantec is unable to provide support for platform and operating systems that are not listed here.

PKI Manager

PKI Manager is a web portal hosted in Symantec's data center that allows a Managed PKI administrator to perform account, user, certificate, and key management tasks.

Table 1-2 PKI Manager operating system and browser support

OS	Browser
Windows 7® Enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer (IE) 8 (32-bit), 9 (32-bit), 11[a] Firefox 50
Windows 8.1 (32-bit and 64-bit)	IE 11

[a]Edge mode is not supported.

PKI Certificate Services

PKI Certificate Services are the webpages that enable users to request, install, renew, and recover their certificates.

Table 1-3 PKI Certificate Services operating system and browser support

OS	Browser
Windows 7 Enterprise edition SP1 (32-bit and 64-bit)	IE 8 (32-bit), IE 9 (32-bit), IE 10 (32-bit), IE 11[a] Firefox 50 Chrome 54[c]
Windows 8.1 (32-bit and 64-bit)	IE 11[a] Firefox 50 Chrome 54[c]
Windows 10 (32-bit and 64-bit)	IE 11[a, b] Firefox 50 Chrome 54[c]
Mac OS X El Capitan (10.11)	Safari 9.1 Firefox 50
macOS(R) Sierra (10.12)	Safari 9.1 Firefox 50

[a]The renewal plug-in is not supported in IE 11 if Enhanced Protection Mode (EPM) is enabled. EPM is disabled by default in IE 11.

[b]Edge mode is not supported.

[c]The Chrome browser is supported for certificate lifecycle operations using PKI Client only.

PKI Client

PKI Client is middleware for digital signing, authentication, and data protection with desktop-based applications using digital certificates stored on a smart card, security device, or user's computer.

Table 1-4 PKI Client Operating System and Browser Support

OS	Browser
Windows® 7 SP1 (32-bit and 64-bit)	IE 9 (32-bit), IE 10 (32-bit) and IE 11 Firefox 50 Chrome 54
Windows 8.1 (32-bit and 64-bit)	IE 11 Firefox 50 Chrome 54
Windows 10 (32-bit and 64-bit)	IE 11 Firefox 50 Chrome 54
Mac OS X El Capitan (10.11)[a]	Safari 10.0 Firefox 50 Chrome 54
macOS(R) Sierra (10.12)[a]	Safari 10.0 Firefox 50 Chrome 54

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

Additional PKI Client Support

PKI Client also supports the following applications:

- Outlook Client 2013 and 2016
- Adobe Reader DC

- Microsoft Word 2013 and 2016

PKI Enterprise Gateway

PKI Enterprise Gateway is software installed at the enterprise site that, with the enterprise's LDAP directory service, allows an enterprise to programmatically approve certificate requests and publish certificate information back to the enterprise's user store.

For PKI Enterprise Gateway installations:

Table 1-5 Operating systems and Active Directories supported by PKI Enterprise Gateway

OS	Active Directory
Windows 2008 R2 Server Enterprise/Standard (64-bit)	2008
Windows 2008 R2 SP1 Server Enterprise/Standard (64- bit)	2008
Windows Server 2012 R2 Standard	2012

- Memory: 4 GB RAM and 100 GB hard disk space
  Virtual directory: VMware vSphere 4 and 5 or VMware View 5.4
- Web server: IIS 7.5, NET Framework 4.0 (Windows 2008) or IIS 8, NET Framework 4.0 (Windows 2008 R2), .NET Framework 4.5 (Windows 2012 R2)
- User Stores: Microsoft Active Directory 2008, Novell eDirectory Server v8.8.5, Oracle Directory Server 11gR1 11.1.1.5.0 or OpenLDAP 2.4.35
- Key escrow datastore: The key escrow datastore is used to escrow private keys locally, as part of the key escrow and recovery option. The key escrow datastore supports Microsoft SQL Server 2008 and Oracle 10g RDBMS datastore databases.
  Additionally, Symantec has qualified the key escrow datastore on OpenLDAP 2.4.35, Novell eDirectory 8.8.5, and Oracle Directory Server Enterprise Edition 11gR1. Symantec expects that the key escrow datastore also works on other LDAP-based directories.

For Microsoft Autoenrollment Client OS:

- OS: Windows XP SP3, Windows 2008 Server (64-bit), or Windows 7 Enterprise (32- and 64-bit)

HSMs Supported

Table 1-6 Supported HSMs

HSM Type	Client Version	Software Version	Firmware Version
SafeNet Luna SA [a, b]	5.2.1	5.2.1	6.2.1
SafeNet Luna SA [a, b]	5.3.1-1	5.3.1	6.2.1
SafeNet Luna SA[a, b]	6.1	6.1	6.10.9

[a]Both Export and Signing variants were qualified with the supported HSM types.

[b]Luna SA, Luna PCI, and Luna G5 are functionally identical and the qualified versions of Luna SA should work with Luna PCI and Luna G5.

For PKI Enterprise Gateway without the key escrow and recovery service, use the key signing variant of the HSM (the default). If using the optional key escrow and recovery service, you must obtain the key generation (key export) variant of the HSM from SafeNet, which includes the key signing variant.

Mobile Devices

Managed PKI supports issuing digital certificates on all devices running iOS 6, 7, 8.1, 9, and 10. Beginning with this release, Symantec is announcing the end of life for the PKI Client app for Android systems.

See "Announcement of End of Life for PKI Client Android app" on page 9.

PKI Manager Updates

PKI Manager is the portal you use to configure your Managed PKI account and perform the daily certificate lifecycle tasks. This release of Managed PKI includes the following updates to PKI Manager. Refer to PKI Manager and the online Help for more information about these new features.

Ability to support IPv6 capabilities in DNS and Additional DNS names

This version of Managed PKI supports IPv6 in DNS and Additional DNS names.

The IPv6 support is available only for profiles having Enrollment method as CSR and Authentication method as Manual approval. The Generic Server, Private Server, and IPSEC Server certificate profiles have been qualified to support IPv6.

General Improvements

A number of messages and UI text strings were updated based on customer feedback.

PKI Enterprise Gateway Updates

PKI Enterprise Gateway includes some minor updates, but does not include new functionality. PKI Enterprise Gateway is an optional update in this release.

Symantec™ PKI Enterprise Gateway Deployment Guide and *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide* were updated to reflect these updates and fix minor issues.

Announcement of End of Life for the Transaction Signing API

Symantec is announcing the end of life for the Transaction Signing API. *Managed PKI® Transaction Signing API Developer's Guide* and other references are removed from the PKI Enterprise Gateway package.

PKI Web Service Updates

PKI Web Services includes some minor updates, but does not include new functionality. PKI Web Services is an optional update in this release.

Symantec™ Managed PKI PKI Web Services Developer's Guide has been updated to reflect these updates and to fix minor issues.

PKI Client Updates

PKI Client supports new operating systems and platforms. Specifically, PKI Client supports:

- Mac OS El Capitan and macOS Sierra. Mac OS Mavericks (10.9) and Mac OS Yosemite (10.10) are no longer supported.
- Microsoft Office 2013 and 2016. Microsoft Office 2010 and 2011 are no longer supported.
- SafeNet Authentication Client 10.x. SafeNet Authentication Client 8 is no longer supported,

Additionally, PKI Client no longer supports the Cisco VPN client.

PKI Client has been qualified against the latest supported platforms. See PKI Client.

For most users, upgrades occur automatically, unless you have disabled Live Update. Refer to *Symantec™ PKI Client Administrator's Guide* for instructions on how to disable Live Update.

Updated Token Support

SafeNet has ended support for the Gemalto SA .NET Dual and the SafeNet iKey 4000 tokens. Symantec recommends that your customers move to the latest supported tokens. PKI Client is qualified on the following tokens:

- SafeNet 5100
- SafeNet 5110

See *Symantec™ PKI Client Administrator's Guide* for details on token support.

Note: *Symantec™ PKI Client Administrator's Guide* erroneously states, "Managed PKI does not support any hardware tokens on the Mac OS El Capitan and Mac OS Sierra operating systems, including Government Edition CAC and PIV smart cards". With this release of PKI Client, that statement should read, "Managed PKI does not support Government Edition CAC and PIV smart cards on the Mac OS El Capitan and macOS Sierra operating systems."

PKCS 11 Module Changes

The 64-bit PKCS#11 DLL named TBPKCS11.dll has been renamed to PKCS11.dll. If your 64-bit applications point to TBPKCS11.dll as the 64-bit PKCS #11 DLL, you must configure the application to point to PKCS11.dll.

Due to changes in how Adobe Reader DC handles the PKCS#11 module, PKI Client no longer supports the PKCS#11 module.

Announcement of End of Life for PKI Client Android app

Symantec is announcing the end of life for the PKI Client app for Android systems. The PKI Client Android app for ICS 4.0 and the PKI Client Android app for Android 4.4/5.0 will no longer be supported, effective February 2017. These apps will be removed from the Google Play store in March of 2017.

If your users have downloaded one of these apps, inform them of this end of life announcement.

Language Support

Managed PKI 8.17 components (PKI Manager, PKI Certificate Services, and PKI Client) support English, French, German, Japanese, Portuguese, Norwegian, Spanish, Simplified Chinese, Korean, Traditional Chinese, and Italian.

These components auto-detect the language settings in the browser and display the correct language. The browser must have the appropriate language packs installed.

Documentation

The following documents have been revised to incorporate Managed PKI 8.17-specific material:

- *Managed PKI 8.17 Release Notes* (this document)
- *Symantec™ PKI Enterprise Gateway Deployment Guide*
- *Symantec™ Managed PKI PKI Web Services Developer's Guide*
- *Symantec™ Managed PKI® Overview*
- *Symantec™ PKI Client Administrator's Guide*
- *Symantec™ PKI Client Writing Post-processing Scripts Guide*

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

Issues Addressed and Known Issues and Workarounds

For information about issues fixed in this release and about the workarounds related to known issues in this release, access the Symantec Knowledge Center for Managed PKI at the following URL.

https://support.symantec.com/support/mpki-support/index.html

- Enter **Managed PKI 8.17** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI 8.17** as the Knowledge Center Search text to obtain a list of the issued addressed.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com