Symantec™ Managed PKI 8.16 Release Notes

Symantec

Symantec™ Managed PKI 8.16 Release Notes

This document includes the following topics:

What's New in 8.16

These release notes accompany the delivery of the Symantec Managed PKI 8.16 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 8.16 supports.

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

Table 1-1 Supported components

Component	Version Supported
PKI Client	v2.15[a]
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.16
PKI Web Services	v1.16

[a]Managed PKI 8.16 supports previous versions of PKI Client. However, you must be running v2.15 or higher to benefit from the features that are described in these release notes.

Updated Platform Support

Managed PKI 8.16 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 46
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 46 Chrome 50[c]
Windows 8.1 (32-bit and 64-bit)	IE 11[a] Firefox 46 Chrome 50[c]
Windows 10 (32-bit and 64-bit)	IE 11[a, b] Firefox 46 Chrome 50[c]
Mac OS X v10.10.5	Safari 9.1 Firefox 46
Mac OS X v10.11.4	Safari 9.1 Firefox 46

[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 (64-bit)	IE 9 (32-bit), IE 10 (32-bit), and IE 11 Firefox 46 Chrome 50
Windows 8.1 (32-bit and 64-bit)	IE 11 Firefox 46 Chrome 50
Windows 10 (32-bit and 64-bit)	IE 11[c] Firefox 46 Chrome 50
Mac OS X v10.9.5[a]	Safari 9.1 Firefox 46 Chrome 50
Mac OS X v10.10.5[b]	Safari 9.1 Firefox 46 Chrome 50
Mac OS X v10.11.4[b]	Safari 9.1 Firefox 46 Chrome 50

[a]Managed PKI does not support Government Edition CAC (Common Access Cards) and PIV (Personal Identify Verification) smart cards on the Mac 10.9.x operating system.

[b]Managed PKI does not support any hardware tokens on Mac OS X10.10.x and Mac OS X10.11, including Government Edition CAC and PIV smart cards.

[c]Edge mode is not supported.

Additional PKI Client Support

PKI Client also supports the following applications:

- Outlook Client 2010 and 2013
- Adobe Reader DC
- Word 2010 and 2013

PKI Enterprise Gateway

PKI Enterprise Gateway is software installed at the enterprise site that, in conjunction 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 above 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

Symantec tests Managed PKI on common mobile devices and OS. Symantec cannot test all combinations; however, Symantec expects that Managed PKI will work on other devices that run a qualified OS.

iOS Devices

Managed PKI supports issuing digital certificates on all devices running iOS 6, 7, 8.1, and 9.

Android Mobile Devices

Managed PKI supports issuing digital certificates on devices running Android 4.5 and 5.1.1.

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.

Allow Administrators to Change Self Service Portal Contact

Self Service Portal now allows you to modify your technical contact from an existing administrator to another administrator within the account. If you do not want to use any existing administrators, you can choose to create a new administrator.

Support for CSR-Based Enrollment for Client Authentication

This release of Managed PKI supports CSR-based enrollment for client authentication that allows you to issue certificates that end users can use to authenticate themselves to your enterprise resources (VPNs, web sites, or similar services).

Improvement to Email Templates

The certificate email template now has a system variable that allows administrators to include DER encoded PKCS7 formatted certificates in emails to end users. This system variable is applicable only for certificate profiles that support CSR-based enrollments.

Addition of Certificate Profile Templates to Test Drive

The following certificate profile templates have been added to Managed PKI Test Drive. These profiles were previously offered only to non-Test Drive accounts. You can use these profiles to issue valid PKI Certificates from a test CA solution.

- Generic device - Enables an organization to issue customized device certificates commonly needed for computer client to server, server to server, and device to server authentication
- Private Server SSL - Enables certificate to authenticate servers under a private enterprise CA hierarchy.

- Adobe Organization - Enables an organization to issue certificates that perform digital authentication of Adobe PDF documents.
- Adobe CDS Organization - Enables an organization to issue certificates that perform digital authentication of Adobe PDF documents.
- Secure Email Gateway - This certificate profile template issues certificates that can be used by secure email gateways.
- Code Signing - This certificate profile template issues Code Signing certificates to digitally sign code under your enterprise. Code Signing certificate provides verification that the code has come from an internally trusted source.
- Client Authentication - This certificate profile template issues certificates that enable standard Wi-Fi, VPN, or website access for any device (including iOS and Android mobile devices).

Updates to Managed Users Search

This release enhances the search behavior of the Manage Users page. If you have selected the **All Profiles (this account)** search criteria for User with pending requests, you no longer need to enter three characters in the search field. Leave the field blank to search for all users with pending requests across all the profiles.

Manufacturing Account Certificate Changes

This release has the following updates for Manufacturing accounts:

- Account Renewal - Unused manufacturing seats now expire during the account renewal period. Seats must be repurchased when the account is renewed. After the account is renewed, you can view available seat pool usage in the PKI Manager dashboard.
- Account Expiry -If your Manufacturing account expires, you will no longer be able to access the account. You must contact your Symantec representative to renew your account.

  To avoid this, make sure to renew your account before it expires. Your expiration date is available on the PKI Manager dashboard.

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.

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 does not include new functionality and does not require an update. 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.

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

Language Support

Managed PKI 8.16 components (PKI Manager, PKI Certificate Services, and PKI Client) support English, French, German, Japanese, Portuguese, Norwegian, Spanish, and simplified Chinese.

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 8.16-specific material:

- *Managed PKI 8.16 Release Notes* (this document)
- *Symantec™ PKI Enterprise Gateway Deployment Guide*
- *Symantec™ Managed PKI PKI Web Services Developer's Guide*
- *Symantec™ Managed PKI® Overview*
- *Managed PKI® Transaction Signing API Developer's 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://knowledge.symantec.com/support/mpki-support/index.html

- Enter **Managed PKI 8.16** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI 8.16** 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