Symantec™ Managed PKI 8.15 Release Notes

Symantec™ Managed PKI 8.15 Release Notes

This document includes the following topics:

What's New in 8.15

These release notes accompany the delivery of the Symantec Managed PKI 8.15 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 8.15 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)	v1.15
PKI Web Services	v1.15

[a]Managed PKI 8.15 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 8.15 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, 9, 11 Firefox 42
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 42 Chrome 46[b]
Windows 8.1 (32-bit and 64-bit)	IE 11[a] Firefox 42 Chrome 46[b]
Windows 10 (32-bit and 64-bit)	IE 11[a, c] Firefox 42 Chrome 46[b]
Mac OS X v10.9.5	Safari 9.0 Firefox 42
Mac OS X v10.10.5	Safari 9.0 Firefox 42
Mac OS X v10.11	Safari 9.0 Firefox 42

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

[c]Edge mode is not supported.

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 42 Chrome 46
Windows 8.1 (32-bit and 64-bit)	IE 11 Firefox 42 Chrome 46
Windows 10 (32-bit and 64-bit)	IE 11[c] Firefox 42 Chrome 46
Mac OS X v10.9.5[a]	Safari 9.0 Firefox 42 Chrome 46
Mac OS X v10.10.5[b]	Safari 9.0 Firefox 42 Chrome 46
Mac OS X v10.11[b]	Safari 9.0 Firefox 42 Chrome 46

[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 2012 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	Platform	Driver Version	Firmware Version
SafeNet Luna SA with HSM Client software version 4.5 with patch DOW3797[a]	■ Windows 2008 R2 ■ Windows Server 2012 R2	4.4.3-1	4.8.1
SafeNet Luna SA (with remote PED) with HSM Client software version 4.5 with patch DOW3797[a]	■ Windows 2008 R2 ■ Windows Server 2012 R2	4.4.3-1	4.8.1
SafeNet Luna SA5 with HSM Client software version 5.1.1[a]	■ Windows 2008 R2 ■ Windows Server 2012 R2	5.1.1	6.2.1
SafeNet Luna SA5 with HSM Client software version 5.2.1[a]	■ Windows 2008 R2 ■ Windows Server 2012 R2	5.2.1	6.10.1
SafeNet Luna SA5 (with remote PED) with HSM Client software version 5.1.1[a]	■ Windows 2008 R2 ■ Windows Server 2012 R2	5.1.1	6.2.1
SafeNet Luna SA5 (with remote PED) with HSM Client software version 5.2.1[a]	■ Windows 2008 R2 ■ Windows Server 2012 R2	5.2.1	6.10.1

Table 1-6 Supported HSMs *(continued)*

HSM Type	Platform	Driver Version	Firmware Version
SafeNet Luna PCI (Model 3.0)[a]	Windows 2008 R2	3.0	4.7.1
SafeNet Luna G5[b]	Windows 2008 R2	5.1.1	6.2.3
SafeNet Luna G5[b]	■ Windows 2008 R2 ■ Windows Server 2012 R2	5.2.1	6.10.1
SafeNet Luna 5.3.1 with HSM Client software version 5.3.1-1[a]	Windows 2008 R2	5.3.1-1	6.10.2
SafeNet Luna PCI-E	Windows 2008 R2	5.3	6.2.1

[a]You must contact SafeNet to obtain and install the software patch appropriate to your driver version.

[b]This device can only be used as a USB connector.

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.

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.

Bulk Reject of Manufacturing Certificates

With this release of Managed PKI, administrators of manufacturing certificate accounts can reject certificates if they were issued incorrectly. Administrators have the option to reject an entire batch or select only the certificates that need to be rejected across multiple batches.

If administrators reject an entire batch, all the certificates in the batch are rejected. If administrators reject certificates from multiple batches, only the selected certificates will be rejected. In both cases, the seats corresponding to rejected certificates are returned to the seat pool and the administrator can issue replacement certificates, if needed.

Binding RA Certificates to Certificate Profiles

This release of Managed PKI enhances the management of Registration Authority (RA) certificates and signing authority certificates. Administrators now have the ability to bind RA certificates to certificate profiles. Using this RA certificate, certificate life cycle operations such as enrollment, renewal, and recovery of private key can be accessed only for the certificate profiles bound to that RA certificate.

The option to display Infrastructure certificate is now available for both main and sub-accounts. You can perform all the operations from a main account, but from a sub-account you can only download a certificate and bind a certificate profile.

Contact your Symantec representative for enabling this option.

Displaying Public Key Thumbprint

With this release, the administrator can view MD5, SHA-1, and SHA-256 thumbprint values of the public key at the time of approving the certificate request or after the certificate approval. The public key thumbprint value is a short sequence of bytes used to identify a longer public key and is applicable only for CSR based enrollments. For example, MD5 or SHA-1 thumbprints are only 128 or 160 bits in length.

Performance Improvements for Certificate Batch Services

PKI Certificate Batch Services now includes some internal upgrades to improve the performance of concurrent batches in a node. These changes do not affect the overall functionality.

Allowing Administrators to Invite Other Administrators for Manufacturing Certificate Account

In this release, you can invite administrators from other manufacturing certificate accounts to become administrators on this account. When invited, you can assign roles and edit details of the invited administrators. Contact your Symantec representative to enable this feature.

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.

LKMS now supports HSM slot label for key generation.

Symantec™ PKI Enterprise Gateway Deployment Guide and *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide* were updated to 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 has been updated to support many of the features that are described in these release notes. To obtain the benefits of these updates, your users must upgrade to PKI Client 2.15. 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.

Symantec™ PKI Client Administrator's Guide have been updated to reflect these new features.

Language Support

Managed PKI 8.15 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 8.15-specific material:

- *Managed PKI 8.15 Release Notes* (this document)
- *Symantec™ PKI Client Administrator's Guide*
- *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 8.15** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI 8.15** 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