Managed PKI™ v8.8 Release Notes

Managed PKI™ v8.8 Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated April 10, 2013

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/contact/index.html#support4

Contents

Managed PKI v8.8 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI v8.8 release. Managed PKI v8.8 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 installed at your enterprise location, as described in these release notes.

What's New in Managed PKI v8.8

This release of Managed PKI provides the following updates:

- "Updated Component Support" on page 1
- "Updated Platform Support" on page 1
- "PKI Manager Updates" on page 5
- "PKI Enterprise Gateway Updates" on page 6
- "PKI Client Updates" on page 7
- "Language Support" on page 7

Updated Component Support

Table 1-1 lists the optional components supported by Managed PKI v8.8. All components are available from the *Resources* page of PKI Manager.

Table 1-1 Supported components

Component	Version Supported
PKI Client	v2.8 [a]
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.8
PKI Web Services	v2.3

a.Previous versions of PKI Client will work with Managed PKI v8.8; however, you must be running v2.8 or higher to benefit from the features described in these release notes.

Updated Platform Support

Managed PKI v8.8 supports the following platforms and operating systems (OS).

It is not possible for Symantec to test every combination of third-party client, server, operating system, service pack, and so on. As a result, 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 not listed here.

PKI Manager

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

Table 1-2 PKI Manager operating system/browser support

OS	Browser
Windows® XP SP3	IE 8 (32-bit) Firefox 17, 20
Windows 7 Enterprise edition (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 17, 20
Windows 7 Enterprise edition (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 17, 20

PKI Certificate Services

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

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

OS	Browser
Windows XP SP3	IE 8 (32-bit) Firefox 17, 20 Chrome 23[a]
Windows 7 Enterprise edition (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 17, 20 Chrome 23[a]
Windows 7 Enterprise edition (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 17, 20 Chrome 23[a]
Mac OS X v10.7 and 10.8	Safari 5.1.5 Firefox 17
Mac OS X v10.8 and 10.8	Safari 6 Firefox 17
Windows® 8 Enterprise edition (Desktop mode)	IE 10

a. 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 end-user computer.

Table 1-4 PKI Client operating system/browser support

OS	Browser
Windows XP SP3	IE 8 Firefox 17, 20 Chrome 23
Windows Vista SP 2 (32-bit and 64-bit)[a]	IE 8 (32-bit), 9 (32-bit) Firefox 17, 20 Chrome 23
Windows® 7 Enterprise edition (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 17, 20 Chrome 23
Windows® 7 Enterprise edition (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 17, 20
Mac OS X v10.7	Safari 5.1.5 Firefox 17
Mac OS X v10.8	Safari 6 Firefox 17

[a]Windows Vista users who use hardware tokens must install the manufacturer drivers and should not rely on Windows drivers.

PKI Client also supports the following applications:

- Outlook Client 2007, 2010 (32-bit and 64-bit)
- Thunderbird 3
- Adobe Reader 9 and X (Windows XP) and Adobe X and XI (all other platforms)
- Word 2007, 2010 (32-bit and 64-bit)

PKI Enterprise Gateway

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

For PKI Enterprise Gateway installations:

Table 1-5 Operating Systems and Active Directory supported by PKI Enterprise Gateway

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

- Memory: 4 GB RAM and 100 GB hard disk space
- Web Server: IIS 7.5, NET Framework 4.0
- User Stores: Microsoft Active Directory, Novell eDirectory Server v8.8.5, and Oracle Directory Server 11gR1 11.1.1.5.0.

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 HSMs Supported

HSM Type	Platform	Driver Version	Firmware Version
SafeNet Luna SA with HSM Client software version 4.4.1[a]	Windows 2008 R2	4.4.3-1	4.8.1
SafeNet Luna SA (with remote PED) with HSM Client software version 4.4.1[a]	Windows 2008 R2	4.4.3-1	4.8.1
SafeNet Luna PCI (Model 3.0)[a]	Windows 2008 R2	3.0	4.7.1

a. You must install the client software patch.

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

iOS Devices

Managed PKI supports issuing digital certificates on all devices running iOS 5 and 6.

Android Mobile Devices

Managed PKI supports issuing digital certificates on many Android devices. New Android mobile devices are constantly being qualified. Refer to the PKI Client download page on Google play for the most up-to-date list of supported devices.

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.

General Improvements

Managed PKI v8.8 includes the following general improvements. It:

- The PKI Manager dashboard has been enhanced to reflect seat usages for different seat types.
- The RA certificate enrollment page has been updated to better match the surrounding interface.
- The administrator's experience in setting up third-party CSP tokens (middleware such as Microsoft Base CSP or SafeNet Authentication Client) has been improved.

Key Escrow and Recovery Service

An enterprise must be able to retrieve encrypted data when users lose their private keys. Managed PKI allows you to escrow your users' private keys and recover them in the event they are lost. With this release you can store your user's private keys in a user store at your enterprise location. You must install PKI Enterprise Gateway to use a local user store to escrow and recovery private keys; however, you can manage key escrow and recovery through PKI Manager or through PKI Web Services.

Note: The key escrow and recovery service of the PKI Enterprise Gateway requires Java JRE 1.7. If you have deployed a Web Service client application that will integrate with the key escrow and recovery service of the PKI Enterprise Gateway, make sure that this application is also updated to use JRE 1.7.

The key escrow and recovery service is supported for the following certificate profile templates:

- Secure Email
- Windows EFS
- Windows EFS Recovery

For details on installing and configuring PKI Enterprise Gateway, refer to *Symantec™ PKI Enterprise Gateway Deployment Guide*.

For details on using PKI Web Services to escrow and recover private keys, refer to *Symantec™ Managed PKI PKI Web Services Developer's Guide*.

For details on using PKI Manager to escrow and recovery private keys, refer to PKI Manager and its associated help.

Enrollment Code Display and Configuration

This release of Managed PKI includes the following updates to how enrollment codes are displayed and behave:

- An administrator can now view the enrollment code for users whose enrollment codes are sent as part of the enrollment URL.
- For security reasons, all enrollment codes expire. With this release, an administrator can now set the expiration period of an enrollment code to up to 10 days.

Enhanced Support for Manufacturer Certificates

In this release, Manufacturer certificate batch results are now encrypted using the uploading administrator's certificate, and are only accessible to the administrator who uploaded the batch. Additionally, these batches can only be decrypted by PKI Client, using the uploading administrator's certificate.

This release supports WiMAX and DOCSIS certificate types. If you require additional certificate types, you will need custom templates. Contact your Symantec representative for details on custom certificate profile templates.

Enhanced ECC Support

ECC devices require less storage, power, memory, and bandwidth than other systems. This allows you to implement cryptography in platforms that are constrained, such as wireless devices, handheld computers, smart cards, and thin-clients. It also provides improved efficiency. Smaller-sized ECC keys are equivalent to large-sized RSA keys--something that will be important as stronger security systems become mandated and devices become smaller.

This release adds support for ECC-based keys in PKI Enterprise Gateway and OS/browser enrollments, in addition to the PKI Web Services support added in the previous release.

New Certificate Profile Templates

This release adds the following new certificate profile templates:

- **MDM Device Identity.** This certificate profile template allows you to confirm the identity of a device before pushing an encrypted profile (Client Authentication or Secure Email template) to a device. This template is only available when an MDM is responsible for pushing certificates to a device.
- **Offline IPSec certificate profile template.** This certificate profile template allows you to get a Computer certificate if you are not joined to a domain. These certificates can be issued to any device that supports CSR enrollment.

PKI Enterprise Gateway Updates

This version of PKI Enterprise Gateway has been updated to support many of the features described in these release notes. To obtain the benefits of these updates, you must move to the latest version of PKI Enterprise Gateway (available from the Resources page of PKI Manager).

PKI Client Updates

PKI Client has been updated to support many of the features described in these release notes. To obtain the benefits of these updates, your users must move to PKI Client 2.8. For most users, this will happen 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 and *Symantec™ PKI Client Writing Post-processing Scripts Guide* have been updated to reflect theses new features.

Additionally, PKI Client has been updated for the following new feature:

Autoenrollment for Domain-Joined Macs

In this release, PKI Client supports autoenrollment for OS X Macs that have been joined to a Windows domain. Autoenrollment on a Mac functions the same as on Windows.

Language Support

Managed PKI v8.8 supports the following languages:

- PKI Manager supports English, French, and Japanese
- PKI Certificate Services supports English, French, German, Japanese, Portuguese, Norwegian, Spanish, and simplified Chinese
- PKI Client supports English, French, German, Japanese, Portuguese, Norwegian, Spanish, and simplified Chinese.

These components will auto-detect the languages set 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 v8.8-specific material:

- *Managed PKI™ v8.8 Release Notes* (this document)
- *Symantec™ PKI Client Administrator's Guide*
- *Symantec™ PKI Client Writing Post-processing Scripts 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*

- *Managed PKI® Getting Started with Android Mobile Devices* is a quick reference for integrating Managed PKI certificates with your users' iOS mobile devices.
- *Managed PKI® Configuring an LTE Operator Base Station Solution* (available from your Symantec representative or the Symantec Knowledge Center for Managed PKI)
- *Managed PKI® Configuring a Smart Grid Solution* (available from your Symantec representative or the Symantec Knowledge Center for Managed PKI)
- *Managed PKI® Configuring a Manufacturer Certificate Solution for ZigBee* available from your Symantec representative or the Symantec Knowledge Center for Managed PKI)

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

Issues Addressed and Known Issues and Workarounds

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

https://knowledge.verisign.com/support/mpki-support/index.html

- Enter **Managed PKI v8.8** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI v8.8** as the Knowledge Center Search text to obtain a list of the issued addressed.