Symantec™ Managed PKI 8.13 Release Notes

Symantec™ Managed PKI 8.13 Release Notes

This document includes the following topics:

What's New in 8.13

These release notes accompany the delivery of the Symantec Managed PKI 8.13 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 8.13 supports. All components are available from the **Resources** page of PKI Manager.

Table 1-1 Supported components

Component	Version Supported
PKI Client	v2.13[a]
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.13
PKI Web Services	v1.13

[a]Managed PKI 8.13 supports previous versions of PKI Client. However, you must be running v2.13 or higher to benefit from the features that are described in these release notes.

Updated Platform Support

Managed PKI 8.13 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 8, 9, 11 Firefox 35
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11

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)	Internet Explorer 8 (32-bit), Internet Explorer 9 (32-bit), Internet Explorer 10 (32-bit), Internet Explorer 11[a] Firefox 35 Chrome 39[b]
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 35 Chrome 39[b]
Mac OS X v10.9.5	Safari 7.0.6 Firefox 35
Mac OS X v10.10.1	Safari 8.0.2 Firefox 35

[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.

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 and 64-bit), IE 10 (32-bit and 64-bit), and IE 11 Firefox 35 Chrome 39
Windows® 8.1 (32-bit and 64-bit)	IE 11 Firefox 35 Chrome 39
Mac OS X v10.9.5[a]	Safari 7.0.5 Firefox 35
Mac OS X v10.10.1[b]	Safari 8.0.2 Firefox 35

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

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

Additional PKI Client Support

PKI Client also supports the following applications:

- Outlook Client 2007, 2010 (32-bit and 64-bit)
- Thunderbird 24
- Adobe Reader 9 and X (Windows XP) and Adobe X and XI (all other platforms)
- Word 2007, 2010 (32-bit and 64-bit)

The following platforms are not supported on PKI Client from this release:

- Windows XP
- Windows Server 2003

- OSX 10.7, 10.8

You cannot install the latest version of PKI Client on these platforms. The Managed PKI release will not LiveUpdate to the PKI Client v2.13 on these systems.

PKI Enterprise Gateway

PKI Enterprise Gateway is software installed at the enterprise site that. Working with the enterprise's LDAP directory service, PKI Enterprise Gateway 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), .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 4.4.1[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 4.4.1[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
SafeNet Luna PCI (Model 3.0)[a]	Windows 2008 R2	3.0	4.7.1
SafeNet Luna G5	Windows 2008 R2	5.1.1	6.2.3
SafeNet Luna G5	■ 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

Table 1-6 Supported HSMs *(continued)*

HSM Type	Platform	Driver Version	Firmware Version
SafeNet Luna PCI-E[b]	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]Key generation mechanism on HSM has not been qualified for this device.

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.

iOS Devices

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

Android Mobile Devices

Managed PKI supports issuing digital certificates on many Android devices. New Android mobile devices are constantly being qualified. Refer to https://knowledge.verisign.com/support/mpki-support/index?page=content&id=AR2090&actp=search&viewlocale=en_us for the most up-to-date list of supported devices.

PKI Web Service Updates

PKI Web Services has been updated to include the following:

- Administrators have the ability to send enrollment email to end users when a new or existing user is enrolled using Web Services. The *createOrUpdatePasscodeRequest* API call has been updated to include this change.
- Ability to delete single or multiple users using the PKI Web Service Java Utility. All the certificates associated with the user are also revoked. You can delete up to 25 Seat IDs using this utility. The PKI Web Service Java Utility is updated to include a single key instead of multiple keys which accepts Seat IDs in csv format.

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

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.

Account Structure Enhancement

With this release of Managed PKI, users have the option to choose packages (Standard Private CA, Standard Public CA, and Adobe CA) while creating their account. They also have the option to upgrade their account later by adding more CAs. Contact your Symantec representative to create or upgrade your account.

Issue CA Certificate

This release introduces a new service that supports setting up a CA certificate that your Secure Web Gateway provider can use for SSL decryption.

Enhanced ECC Support

This release adds support for Ecliptic Curve Cryptography (ECC)-based keys in Private SSL and Secure Email Gateway certificate templates. Contact your Symantec representative for enabling this option.

New Certificate Profile Templates

This release adds two new standard certificate profile template that let organizations issue digital signing certificates that chain up to Symantec Roots as part of the Adobe Approved Trusted List (AATL). These new standard certificate profile templates are added under the public CA hierarchy.

- **Adobe Individual** - Issues certificates that end users can use to digitally sign and protect Adobe PDF documents.
- **Adobe Organization**- Enables an organization to issue certificates that perform digital authentication of Adobe PDF documents.

This release also introduces another standard certificate profile template:

- **Generic Server**- Enables an organization to issue customized server certificates commonly needed to enable Internet Protocol Security (IPSec), authenticate

computers or other devices to your Active Directory domains, or to issue private server certificates.

User and Administrator Notifications

This release introduces the ability to customize enrollment request notifications for Client Authentication profiles. Administrators now have the option to send email notifications to both the end user and another person such as the administrator.

Allow Administrators to Invite other Administrators

With this release of Managed PKI, the administrators of Class 3 certificate type in a Managed PKI account with invited administrator option can invite other organization's administrators.

Seat Pool Simplification

In this release, the structure of seat pool is simplified and sub-seat pool is merged with the root seat pool. This allows administrators to view the certificates being used by the user against the purchased seats. Seat pool utilization is displayed in the dashboard for the account and for the sub-account.

- Merged existing sub-seat pools count from the Server seat pool (IPSec, Domain Controller, Private SSL) into Server sub-seat pool
- Merged existing sub-seat pools count from the Device seat pool (LTE, MDM) into DEVICE sub-seat pool

PKI Enterprise Gateway Updates

This version of PKI Enterprise Gateway has been updated to support many features. 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).

Symantec™ PKI Enterprise Gateway Deployment Guide and *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide* were updated 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. Additionally, the following enhancements have been made to PKI Client in this release. To obtain the benefits of these updates, your users must upgrade to PKI Client 2.13. 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.

- This release of PKI Client provides support for certificates that are issued with a Wi-Fi certificate profile using software credentials (vtokens).
- Mozilla Firefox is dropping support for the NPAPI plug-in. This release of PKI Client includes an updated browser extension that replaces the NPAPI plug-in for Firefox browsers. Your users will be prompted to install the Firefox extension if they use that browser to access the PKI Certificate Services pages to install a new or replacement certificate.

  If your users have installed an earlier version of PKI Client and are not getting a new or replacement certificate (or are importing a new certificate without accessing the PKI Certificate Services page), they can download the updated extension from https://browser-extension.symauth.com/auth-client/firefox.
- ActivIdentity has removed their CSP from their latest client, version 7.0.2. Versions of this client starting with 7.0.2 use the Microsoft Base CSP, instead. If a user updates their ActivIdentity client to 7.0.2 or newer, the ActivIdentity CSP is not installed. As a result, there is no guarantee that certificates will continue to work. Also, users cannot renew existing certificates, as the renewal process requires the missing CSP.
  - Users can continue to use ActivIdentity client version 6.2 without any issues.
  - Administrators with users that upgrade their ActivIdentity client to 7.0.2 must create a new profile in PKI Manager that specifies the Microsoft Base Smart Card Provider as the CSP. Users will need to re-enroll for their ActivIdentity certificates with the new profile.

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

Language Support

Managed PKI 8.13 components (PKI Manager, PKI Certificate Services, and PKI Client) supports English, French, German, Japanese, Portuguese, Norwegian, Spanish, and simplified Chinese.

These components auto-detect the language setingst 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 8.13-specific material:

- *Managed PKI 8.13 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*
- *Symantec™ Managed PKI SCEP Service Integration Guide*

The following guide was added in the Managed PKI 8.13 release:

- *Symantec™ Managed PKI Integration Guide for Cisco™ Identity Services Engine*

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.verisign.com/support/mpki-support/index.html

- Enter **Managed PKI 8.13** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI 8.13** 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