Managed PKI™ v8.10 Release Notes

Symantec

Managed PKI™ v8.10 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 December 5, 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

What's New in Managed PKI v8.10 1
Updated Component Support 1
Updated Platform Support 1
PKI Manager Updates 5
PKI Enterprise Gateway Updates 7
PKI Client Updates 7
PKI Web Services 7
Language Support 7
Documentation 7
Issues Addressed and Known Issues and Workarounds 8

Managed PKI v8.10 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI v8.10 release. Managed PKI v8.10 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 v8.10

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 7
- "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 v8.10. All components are available from the *Resources* page of PKI Manager.

Table 1-1 Supported components

Component	Version Supported
PKI Client	v2.10 [a]
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.10
PKI Web Services	v1.10

a.Previous versions of PKI Client will work with Managed PKI v8.10; however, you must be running v2.10 or higher to benefit from the features described in these release notes.

Updated Platform Support

Managed PKI v8.10 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 24, 25
Windows 7 Enterprise edition (32-bit)	IE 8, (32-bit), IE 9 (32-bit) Firefox 24, 25
Windows 7 Enterprise edition (64-bit)	IE 8 (32-bit and 64-bit), IE 9 (32-bit and 64-bit) Firefox 24, 25

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 24, 25 Chrome 30[a]
Windows 7 Enterprise edition (32-bit)	IE 10 (32-bit), 9 (32-bit), IE 8 (32-bit) Firefox 24, 25 Chrome 30[a]
Windows 7 Enterprise edition (64-bit)	IE 10 (32-bit and 64-bit), 9 (32-bit and 64-bit), 8 (32-bit and 64-bit) Firefox 24, 25 Chrome 30[a]
Mac OS X v10.7	Safari 5.1 Firefox 24, 25
Mac OS X v10.8	Safari 6 Firefox 24, 25
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 (32-bit)	IE 8 (32-bit) Firefox 24, 25 Chrome 30
Windows Vista SP 2 (32-bit)[a]	IE 8 (32-bit), 9 (32-bit) Firefox 24, 25 Chrome 30
Windows Vista SP 2 (64-bit)[a]	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 24, 25 Chrome 30
Windows® 7 SP1 (32-bit)	IE 8 (32-bit), 9 (32-bit), 10 (32-bit) Firefox 24, 25 Chrome 30
Windows® 7 SP1 (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit), 10 (32-bit and 64-bit) Firefox 24, 25 Chrome 30
Windows® 8 (32-bit)	IE 10 (32-bit) Firefox 24, 25 Chrome 30
Windows® 8 (64-bit)	IE 10 (32-bit and 64-bit) Firefox 24, 25 Chrome 30
Mac OS X v10.7 and 10.8	Safari 5.1.5, 6 Firefox 24, 25

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 24
- 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 Standard	2012

- Memory: 4 GB RAM and 100 GB hard disk space
- Web Server: IIS 7.5, NET Framework 4.0 (Windows 2008) or IIS 8, NET Framework 4.0 (Windows 2012)
- 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
- Virtual Directory: VMware vSphere 4 and 5 or VMware View 5.4
- Key Escrow Data Store: The key escrow data store is used to escrow private keys locally, as part of the key escrow and recovery option. The key escrow data store supports Microsoft SQL Server 2008 and Oracle 10g RDBMS data store databases.

  Additionally, Symantec has qualified the key escrow data store on OpenLDAP 2.4.35, Novell eDirectory 8.8.5, and Oracle Directory Server Enterprise Edition 11gR1. Symantec expects that the key escrow data store also will work 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	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	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	5.1.1	6.2.1
SafeNet Luna SA5 with HSM Client software version 5.2.1[a]	■ Windows 2008 R2 ■ Windows Server 2012	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	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	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	5.2.1	6.10.1

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

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 need to 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 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 features.

Ability to Migrate Certificate Profiles

This release of Managed PKI allows you to migrate to new profiles when your CAs are ready to expire or need to be re-keyed. The destination profile must be identical to the migrating profile; however, you can change the validity period, the certificate key size, and the signing algorithm of the destination profile.

Certificates issued by the migrating (existing) profile will continue to work through their validity period. New certificates and renewals will be issued using the new profile.

New Seat Pool Types

In this release, Managed PKI displays additional seat pool types under the existing seat pools. This allows you to manage your seat pool allocation more effectively.

- Microsoft Computer AutoEnrollment
- MDM
- Domain Controller
- Private SSL
- IPSEC Server
- Adobe Organization
- Secure Gateway Organization
- Code Signing

Contact your Symantec representative for more information about these seat pool types.

Support for MAC Address and Device ID Ranges in Manufacturing Accounts

In this release of Managed PKI, Manufacturer accounts can generate batches of certificates based on a range of MAC addresses or device IDs.

New Certificate Profile Templates

This release adds a new custom certificate profile template and four new standard certificate profile templates under the public CA hierarchy. Contact your Symantec representative to take advantage of this new custom certificate profile template.

- **Generic Device Authentication.** This custom certificate profile template enables an organization to issue customized device certificates commonly needed for computer client to server, server to server, and device to server authentication. You can choose the "allow duplicate certificate" option and add or remove some optional extensions with this custom certificate profile template.
- **OpenADR.** This standard certificate profile template issues OpenADR VEN device certificates to manufacturers for products that are compliant with the OpenADR Alliance specification. OpenADR certificate serves as an identity certificate for each device as it gets enrolled on the network.

  Managed PKI also supports OpenADR VTN server certificates, using a separate Managed PKI account. Contact your Symantec representative for information about these accounts.
- **OpenCable.** This standard certificate profile template issues device certificates that get embedded in the OpenCable compliant devices at the time of manufacture. OpenCable certificates provide the basis for a number of security services including data confidentiality, content integrity, and hardware authentication for the devices.
- **PacketCable**. This standard certificate profile template issues device certificates that get embedded in the PacketCable compliant devices at the time of manufacture. PacketCable certificates provide the basis for a number of security services including data confidentiality, content integrity, and hardware authentication for the devices.
- **CableHome**. This standard certificate profile template issues device certificates that get embedded in the CableHome compliant devices at the time of manufacture. CableHome certificates provide the basis for a number of security services including data confidentiality, content integrity, and hardware authentication for the devices.

Enhanced Reporting

This release of Managed PKI v8.10 allows administrators to run reports to obtain a count for the number of seats assigned to each profile. This reporting functions for both Cloud and hybrid profiles. Reporting was also enhanced to allow faster and smoother performance for large data sets (>50K records per profile). Reporting is now available in both .xls and .xlsx formats.

PKI Enterprise Gateway Updates

This version of PKI Enterprise Gateway includes minor internal updates. Updating to this version of PKI Enterprise Gateway os optional, but recommended.

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

PKI Client Updates

PKI Client has been updated to support many of the features 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 move to PKI Client 2.10. 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.

- **Secure Email.** Users can use a certificate stored on their computer or smart card to digitally sign, encrypt, and decrypt email in Outlook on Windows. The settings are set so their certificate will only match their Outlook profile.
- **Administrator Credential Support for 3rd-party CSPs.** For CI Plus administrator certificates, PKI Client supports SafeNet eToken, Microsoft Base Smart Card, and Symantec CSPs.
- **Improved Logging by Default.** PKI Client logging is now always enabled by default. Logging now writes to a set location and automatically cleans up logs according to a schedule. Logs older than two weeks are compressed. Logs are kept for the current and prior calendar year, and others are deleted.

Symantec™ PKI Client Administrator's Guide and *Symantec™ PKI Client Writing Post-processing Scripts Guide* have been updated to reflect these new features.

PKI Web Services

PKI Web Services has been updated for the following:

- Includes the enrollment URL in the responses from createPasscode and getPasscodeInformation API calls.
- Support for recovering private keys for certificates imported into PKI Manager.

Symantec™ Managed PKI PKI Web Services Developer's Guide has been updated to reflect these new features.

Language Support

Managed PKI v8.10 components (PKI Manager, PKI Certificate Services, and 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 v8.10-specific material:

- *Managed PKI™ v8.10 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*

The following guides were added to Managed PKI 8.10 in this release:

- *Symantec™ Managed PKI® Integration Guide for MobileIron® Virtual SmartPhone Platform*
- *Symantec™ Managed PKI® Integrating Secure Email Gateway Certificates with Clearswift SECURE Email Gateway*
- *Symantec™ Managed PKI® Integrating Adobe® CDS Organization Certificates with Adobe® LiveCycle® Enterprise Suite for Adobe® Reader®*

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 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 v8.10** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI v8.10** as the Knowledge Center Search text to obtain a list of the issued addressed.