Managed PKI™ v8.9 Release Notes

Symantec

Managed PKI™ v8.9 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 July 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 v8.9 Release Notes

Managed PKI v8.9 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI v8.9 release. Managed PKI v8.9 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 v8.9

This release of Managed PKI provides the following updates:

Updated Component Support

Table 1-1 lists the optional components supported by Managed PKI v8.9. All components are available from the *Resources* page of PKI Manager.

Table 1-1 Supported components

Component	Version Supported
PKI Client	v2.9 [a]
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.9
PKI Web Services	v2.3

a.Previous versions of PKI Client will work with Managed PKI v8.9; however, you must be running v2.9 or higher to benefit from the features described in these release notes.

Updated Platform Support

Managed PKI v8.9 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 19, 20
Windows 7 Enterprise edition (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 19, 20
Windows 7 Enterprise edition (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 19, 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 19, 20 Chrome 23[a]
Windows 7 Enterprise edition (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 19, 20 Chrome 23[a]
Windows 7 Enterprise edition (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 19, 20 Chrome 23[a]
Mac OS X v10.7 and 10.8	Safari 5.1.5, 6 Firefox 19, 20
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 (32-bit) Firefox 17, 20 Chrome 23

Table 1-4 PKI Client operating system/browser support (Continued)

OS	Browser
Windows Vista SP 2 (32-bit)[a]	IE 8 (32-bit), 9 (32-bit) Firefox 17, 20 Chrome 23
Windows Vista SP 2 (64-bit)[a]	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-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 Chrome 23
Windows® 8 Desktop Mode (32-bit)	IE 10 (32-bit) Firefox 17, 20 Chrome 23
Windows® 8 Desktop Mode (64-bit)	IE 10 (32-bit and 64-bit) Firefox 17, 20 Chrome 23
Mac OS X v10.7 and 10.8	Safari 5.1.5, 6 Firefox 17, 20

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 Standard	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 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
- 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 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 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

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 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.

General Improvements

Managed PKI v8.9 includes the following general improvements. It:

Ability to Delete Certificate Profiles

This release of Managed PKI allows you to delete unused certificate profiles. Deleting a profile revokes any certificates associated with the profile, and cancels any pending enrollments associated with that profile.

Bulk Certificate Revocation Enhancements

In this release of Managed PKI, administrators can revoke certificates associated with multiple seat IDs. Administrators can revoke these certificates by uploading a comma-separated value file in PKI Manager, or multiple certificates can be revoked using Web Services.

New Certificate Profile Templates

This release adds the following new certificate profile templates under the public CA hierarchy. Contact your Symantec representative to take advantage of these new certificate profile templates.

- **Secure Email Gateway.** This certificate profile template issues certificates that can be used by secure email gateways.
- **Adobe CDS Organization.** This certificate profile template enables an organization to issue certificates that perform digital authentication of Adobe PDF documents.

Additionally, the following certificate profile templates have been added to Managed PKI Test Drive (they were previously offered only to non-Test Drive accounts):

- **MDM.** This certificate profile template enables Mobile Development Management (MDM) vendors to issue device identity certificates down to the mobile devices before pushing the encrypted profile (for VPN, Wi-Fi and so on) to the user's mobile device. These certificates are enrolled for using SCEP requests.
- **MDM (Web Service Client).** This certificate profile enables MDM vendors to issue device identity certificates down to the mobile devices before pushing the encrypted profile (for VPN, Wi-Fi and so on) to the user's mobile device. These certificates are enrolled for using Web Services.

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.

Email Notification Enhancements

Managed PKI v8.9 allows administrators to set email notifications for unique emails across all certificate operations within a profile. For example, administrator can configure Managed PKI to send email for certificate revocation operation to an administrator, and send renewal notification emails to the end user of the certificate.

Strengthening of Non-exportability of Private Keys

This release adds a High security setting to the Native browser enrollment method when creating a certificate profile. This allows an administrator to configure non-exportability of private keys for certificates enrolled using the Native browser enrollment method.

Resource Page Enhancements

The PKI Manager Resources page has been enhanced to better present files and documents. Also, a number of integration guides were added in this release. Refer to Enhanced the PKI Manager Resources page as a central repository of documentation related to PKI Manager. Refer to "Documentation" on page 7 for more information on these new integration guides.

Centralized Account Menu

Basic account functions have been moved to an accounts settings area in the top, right-hand corner of PKI Manager. From this area, you can view which administrator ID you used to log in, view the current account name, switch between sub-accounts, and sign out of PKI Manager.

Link to Managed PKI for SSL

Managed PKI administrators who also have a Managed PKI for SSL account and administrator certificate can now switch to the Managed PKI for SSL Control Center by clicking the Managed PKI for SSL link. The browser will take you to your Managed PKI for SSL Control Center where you will be asked to present your Managed PKI for SSL administrator credentials.

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).

Additionally, Safenet has issued a patch for their client drivers so that keys generated using the CSP client drivers can also be used by applications using KSP client drivers. This version of the PKI Enterprise Gateway supports the use of the same RA certificate keys generated using CSP client drivers for Autoenrollment service as well as the RA service, as long as the patch provided by Safenet is installed on the client machine running EGW service.

This means that you can use the same RA certificate that you generated using the CSP instructions for the Autoenrollment server for the RA Service as well, once you install this patch. Contact Safenet to download the patch.

Note that this information is not reflected in *Symantec™ PKI Enterprise Gateway Deployment Guide* or the *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide*.

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 2.9. 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.

PKI Web Services

PKI Web Services has been updated for the following:

- Ability to get the total count for Web Services search results
- Support for bulk revocation of certificates issued to multiple seat IDs

Language Support

Managed PKI v8.9 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 v8.9-specific material:

- *Managed PKI™ v8.9 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 8.9 in this release:

- *Symantec™ Managed PKI® Integration Guide for AirWatch® MDM Solution*
- *Symantec™ Managed PKI® Integration Guide for Cisco® 3745 Routers*
- *Symantec™ Managed PKI® Integration Guide for Cisco® ASA Series Routers*
- *Symantec™ Managed PKI® Integrating S/MIME Certificates with Microsoft Outlook®*
- *Symantec™ Managed PKI® Integrating Adobe CDS Certificates with Adobe® Reader®*
- *Symantec™ Managed PKI® Integration Guide for Juniper® SA VPN*
- *Symantec™ Managed PKI® Integration Guide for SonicWALL® Aventail® VPN*

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 v8.9** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI v8.9** as the Knowledge Center Search text to obtain a list of the issued addressed.