Managed PKI™ v8.12 Release Notes

Symantec

Managed PKI™ v8.12 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 September 18, 2014

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 v8.12 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI v8.12 release. Managed PKI v8.12 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 are installed at your enterprise location, as described in these release notes.

What's New in Managed PKI v8.12

This release of Managed PKI provides the following updates:

Updated Component Support

Table 1-1 lists the optional components supported by Managed PKI v8.12. All components are available from the *Resources* page of PKI Manager.

Table 1-1 Supported components

Component	Version Supported
PKI Client	v2.11.0
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.11
PKI Web Services	v1.10

Updated Platform Support

Managed PKI v8.12 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 that are not listed here.

PKI Manager

PKI Manager is a web portal hosted in Symantec's data centers that allow 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 7 Enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer 9, Internet Explorer 11 Firefox 24, 32
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11

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 7 Enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer 11[a], Internet Explorer 10 (32-bit), Internet Explorer 9 (32-bit) Firefox 24, 32 Chrome 37
Windows® 8.1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 24, 32 Chrome 37
Mac OS X v10.8	Safari 6.0.1 Firefox 24, 29
Mac OS X v10.9.4	Safari 7.0.5 Firefox 24, 32

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.

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 Vista SP 2 (32-bit)	Internet Explorer 9 (32-bit) Firefox 24, 29 Chrome 34
Windows Vista SP 2 (64-bit)	Internet Explorer 9 (32-bit and 64-bit) Firefox 24, 29 Chrome 34

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

OS	Browser
Windows 7 SP1 (32-bit)	Internet Explorer 9 (32-bit), Internet Explorer 10 (32-bit), Internet Explorer 11 (32-bit) Firefox 24, 29 Chrome 34
Windows 7 SP1 (64-bit)	Internet Explorer 9 (32-bit and 64-bit), Internet Explorer 10 (32-bit and 64-bit), Internet Explorer 11 Firefox 24, 29 Chrome 34
Windows® 8 (32-bit)	Internet Explorer 10 (32-bit) Firefox 24, 29 Chrome 34
Windows® 8 (64-bit)	Internet Explorer 10 (32-bit and 64-bit) Firefox 24, 29 Chrome 34
Windows® 8.1 (32-bit and 64-bit)	Internet Explorer 11 Firefox 24, 29 Chrome 34
Mac OS X v10.8[a]	Safari 6.0.1 Firefox 24, 29
Mac OS X v10.9.4[a]	Safari 7.0.5 Firefox 24, 29

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

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

You cannot install the latest version of PKI Client on these platforms. The Managed PKI release will not LiveUpdate to the PKI Client v2.11 on these systems.

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 R2 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), .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
- 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 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

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 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 for the following:

- Ability to delete single or multiple users using the Web Service API. All the certificates associated with the user are also revoked. You can delete up to 25 Seat IDs using the multiple user delete API.
- Administrators have the ability to generate audit reports for Web Service operations.
- You can now search for audit operations performed by specific administrators.

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

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.

Download Certificates without the Issuing Chain

In this release, you can customize the certificate template options to include the certificate data, end entity certificate, intermediate CA certificate and root CA certificates. Note that the intermediate CA certificate may not exist for all the certificates. The current template is updated to include a new variable to send email notifications.

Download Manufacturing Certificates in Base64-encoded .pem File Format

With this release of Managed PKI, you now have an ability to download manufacturing certificates in base64-encoded .pem file format. The .pem certificate contains the base64-encoded certificate encoded between the "BEGIN CERTIFICATE" and "END CERTIFICATE" tags.

CSR Based Enrollments in Manufacturing Certificates

With this release of Managed PKI, manufacturing account administrators can generate key pairs at their premises and send public keys as Certificate Signing Requests (CSRs) to generate certificates using batch interface.

By default, email notifications will be sent to the administrator assigned to the certificate profile; however, you can modify this on a per-profile basis on the *Manage certificate profile* page.

Corporate and Technical Contacts for Manufacturing and Private Accounts

With this release of Managed PKI, you can specify a technical contact other than the corporate contact for non-standard accounts. The technical contact, if specified, will receive email notifications related to the Managed PKI Service.

Improvements to Email Templates

This release has a set of new variables to offer more flexibility in customizing email notification templates.

Support for Software Certificates

With this release of Managed PKI, manufacturing account administrators can store their administrator certificates on software (computer) using PKI Client. During the account creation, you need to request to issue manufacturing certificates that reside on software (computer) during enrollment. The hardware tokens will still continue to work on the existing manufacturing accounts.

Enrollment Code Display for Profiles Mapped to Public CA

For client authentication profiles that chain up to a public CA and which use the enrollment code as the Authentication method, administrators now have the option to make the enrollment code available to end users at the time of enrollment. This eliminates the manual effort involved in sending the enrollment code by emails.

Email Address Support in SDN Attribute for Secure Email Gateway Template

Managed PKI now allows organizations to configure the email address in the Subject Distinguish Name (SDN) definition. Previously, RFC822 attribute was required in the SubjectAltName definition. Certificate profiles still only support valid email domains.

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).

Symantec™ PKI Enterprise Gateway Deployment Guide and *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide* have been reflected to reflect these new features.

PKI Client Updates

PKI Client was not updated for this release. However, it has been qualified for use with this version, and with all features that were added in this release.

Documentation

The following documents have been revised to incorporate Managed PKI v8.12-specific material:

- *Managed PKI™ v8.12 Release Notes* (this document)
- *Symantec™ PKI Client Administrator's Guide*
- *Symantec™ PKI Enterprise Gateway Deployment Guide*
- *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide*
- *Symantec™ Managed PKI PKI Web Services Developer's Guide*
- *Symantec™ Managed PKI® Overview*

The following guides are added to Managed PKI 8.12 in this release:

- *Symantec™ Managed PKI Integration Guide for Microsoft Office 365*
- *Symantec™ Managed Integrating Client Authentication Certificates for Web SSO through AD FS*
- *Integrating Symantec™ Managed PKI® with Citrix® XenMobile® Mobile Device Management*

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 v8.12** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI v8.12** as the Knowledge Center Search text to obtain a list of the issued addressed.