Managed PKI™ v8.6 Release Notes

Symantec

Managed PKI™ v8.6 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 14, 2012

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 v8.6 Release Notes

Managed PKI v8.6 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI v8.6 release. Managed PKI v8.6 is an automatic upgrade of Managed PKI v8.5, except where described in these release notes.

What's New in Managed PKI v8.6

This release of Managed PKI provides the following updates:

Updated Platform Support

Managed PKI v8.6 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

Table 1-1 PKI Manager operating system/browser support

OS	Browser
Windows® XP SP3	IE 8 (32-bit) Firefox 10.0.3, 14
Windows® 7 (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 10.0.3, 14
Windows® 7 (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 10.0.3, 14

PKI Certificate Services

Table 1-2 PKI Certificate Services operating system/browser support

OS	Browser
Windows XP SP3	IE 8 (32-bit) Firefox 10.0.3, 14
Windows 7 (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 10.0.3, 14
Windows 7 (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 10.0.3, 14
Mac OS X v10.7	Safari 5.1, Firefox 10
Mac OS X v10.8	Safari 6, Firefox 14

PKI Client

Table 1-3 PKI Client operating system/browser support

OS	Browser
Windows XP SP3	IE 8 (32-bit) Firefox 10.0.3, 14
Windows 7 (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 10.0.3, 14
Windows 7 (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 10.0.3, 14
Mac OS X v10.7	Safari 5.1, Firefox 10.0.3, 14
Mac OS X v10.8	Safari 6, Firefox 10.0.3, 14

PKI Client also supports the following applications:

- Outlook Client 2007, 2010 (32-bit and 64-bit)
- Thunderbird 3
- Adobe Reader 9 and X
- Word 2007, 2010 (32-bit and 64-bit)

PKI Enterprise Gateway

For PKI Enterprise Gateway installations:

- Memory: 4 GB RAM and 100 GB hard disk space
- OS: Windows 2008 R2 Server Enterprise/Standard (64-bit) or Windows 2008 R2 SP1 Server Enterprise/Standard (64-bit)
- Web Server: IIS 7.5, NET Framework 4.0
- User Stores: Microsoft Active Directory or Novell eDirectory 8.8.5
- HSMs:

Table 1-4 PKI Enterprise Gateway HSMs

Type	Luna SA	Luna PCI	Luna SA Hybrid (PED Auth)	Luna PCI and PCI Express Cards (3000 Signing)
Driver	4.4.3-1	3.0	4.4.3-1	N/A
Firmware	4.8.1	4.7.1	4.8.1	4.7.1

For Autoenrollment Server installations:

- Memory: 4 GB RAM and 100 GB hard disk space
- Server OS: Windows 2008 R2 Server Enterprise (64-bit) or Windows 2008 R2 SP1 Server Enterprise (64-bit)
- HSMs:

Table 1-5 Autoenrollment Server HSMs

Type	Luna SA	Luna PCI	Luna SA Hybrid (PED Auth)	Luna PCI and PCI Express Cards (3000 Signing)
Driver	4.4.3-1	3.0	4.4.3-1	N/A
Firmware	4.8.1	4.7.1	4.8.1	4.7.1

For Autoenrollment Client OS:

- OS: Windows XP Professional, Windows 2008 Server (64-bit), or Windows 7 Enterprise (64-bit)

iOS Devices

Managed PKI supports issuing digital certificates on the following iOS devices:

Table 1-6 iOS device support

Device	OS
3rd and 4th generation iPhones	iOS 4 and iOS 5
1st and 2nd generation iPads	

Android Mobile Devices

Managed PKI supports issuing digital certificates on the following Android devices:

Note: Additional 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.

Table 1-7 Android device support

Android Device	Android OS
Samsung Galaxy S II and S II Skyrocket Samsung Galaxy Tab 2 7.0 Samsung Galaxy Tab 7.0 Plus, 7.0 Plus Wi-Fi, and 7.7 Samsung Galaxy Tab 10.1 Samsung Galaxy S III Samsung Galaxy Note	ICS 4.0
Nexus 7 Nexus S 4G Galaxy Nexus	
Motorola Xoom Motorola Droid RAZR Motorola XYBOARD 10.1	

See "Support for Android Mobile Devices" on page 5 for more information on Android mobile device support.

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.

Certificate Management Enhancements

Previously, administrators managed certificates in PKI Manager by first searching for the end user to whom the certificate was issued. In this release of Managed PKI, administrators can manage certificates directly by selecting the *Manage certificates* icon or by selecting *Manage certificates* from the **Task** icon (both in the PKI Manager footer).

This new feature allows enhanced search capabilities, including searching by common name, seat ID, seat pool, validity start/end date, serial number, and Certificate Authority. Administrators can also search by status, such as valid, expired, or revoked. Additionally, this feature allows enhanced certificate management operations, such as exporting certificates, revoking certificates, and recovering private keys.

Support for Organizational Seat Pool Type

Managed PKI certificates are issued against seats. Seats are tracked based on the seat ID, or unique identifiers for each certificate recipient. An organization purchases a number of seats per account, and certificates issues will count against that total.

This release of Managed PKI adds support for Organizational seat pools, bringing the total seat pools types to four:

- User seats for certificates issued directly to users.
- Device seats for certificates issued to machines and devices, such as Microsoft Computer certificates.
- Server seats for certificates issued to servers such as IPSec servers or Microsoft Domain Controller certificates.
- Organizational seats for certificates issued to organizations.

Work with your Symantec Client Manager to purchase seats for the appropriate seat types based on your certificate usage requirements.

Support for Android Mobile Devices

This version of Managed PKI enhances Symantec's mobile device offering by adding support for a number of Android Mobile devices. Whether you provide the device or the end users provide their own, you can configure these Android mobile devices to use Managed PKI certificates for the following purposes:

- Wi-Fi access. The mobile device will use the certificate to authenticate the device to an organizations wireless network. Managed PKI supports the native Wi-Fi capability on Android devices.
- Virtual Private Network (VPN) access. The mobile device will use the certificate to authenticate the device to an organizations VPN, and secure communications over that network.
- Microsoft® ActiveSync support. The mobile device will use the Managed PKI certificate to securely communicate with the enterprise Microsoft® ActiveSync server.

Refer to *Symantec™ Managed PKI® Enterprise Mobility Guide*, available on the PKI Manager *Resources* page for instructions on configuring Managed PKI to issue certificates to Android mobile devices.

PKI Client on Android Mobile Devices

End users must install PKI Client on their Android mobile devices to enroll for Managed PKI certificates. PKI Client acts as a certificate management tool and offers enhanced post-processing capabilities that allows native and third-party applications to consume the Managed PKI certificate automatically.

Note: Managed PKI v8.6 supports Wi-Fi, VPN, and Microsoft® ActiveSync configurations; however, PKI Client should also support certificate functionality for any third-party application that uses Keychain Access to manage certificates. You will need to provide instructions to your end users on how to integrate their certificates with these third-party applications. You can upload these instruction in PKI Manager, and they will be displayed to your end users during enrollment.

If end users have not set a Screen Lock PIN or Swipe Lock swipe, they will need to set this up when they install PKI Client on an Android mobile device.

VPN Clients on Android Mobile Devices

In order to use Managed PKI certificates with PKI Client on Android mobile devices, your end users must install a VPN Client. PKI Client has been qualified on the following Cisco Systems VPN clients.

- AnyConnect ICS+ (all supported devices)
- Samsung AnyConnect (Samsung devices)

Configuration of KU and EKU Certificate Extensions

In this release, an administrator can configure a number of Key Usage (KU) and Extended Key Usage (EKU) extensions for certificates. An administrator can customize specific KU and EKU values, which are used by third-party applications (based on actual usage of the certificate issued).

For example, previously a certificate issued from a VPN certificate profile always included the Digital Signature, Key Encipherment, Non-Repudiation, and Key Agreement key usage extensions. With this release, you can choose to remove the Non-Repudiation, and Key Agreement key usage extensions.

Base Station Security for Long Term Evolution (LTE) Network Support

PKI Manager now includes optional functionality that allows an operator in an LTE network to obtain Managed PKI certificates for their LTE network security. LTE network elements, such as the base station eNodeB and SAE Security Gateway (SEG), use strong public key authentication based on machine certificates in order to establish trust in the network. The certificates are automatically issued and managed using a

standard interface called Certificate Management Protocol (CMP v2) which is also newly supported in this release of Managed PKI.

PKI Manager also provides the ability to assign network IP address ranges for validation during processing automated certificate enrollment requests from LTE network elements.

Contact your Symantec representative for more information on implementing this option.

Support for Non-exportability of Certificates for all Security Levels

Non-exportability means that a certificate cannot be moved from a machine on which it was installed, except by deleting it (making it unusable on any other machine). Previously, only certificate profiles configured for High Security enforced non-exportability. This release of Managed PKI allows a greater range of flexibility for an administrator when setting whether a certificate is non-exportable, based on what private key security level is set for the profile:

- High security: Non-exportability is the default, and cannot be disabled. All certificate issued from these templates will require PIN-protection and cannot be exported. Use High security for your certificate profiles if you want to enforce non-exportability of certificates and PIN-protection.
- Medium Security: Non-exportability is the default, and can be disabled when the profile is created if that profile is also set to use PKI Client as the Enrollment method. In this case, PKI Client will only export a certificate in a proprietary PKI Client format. This format can only be used by other instances of PKI Client (PKI Client enforces PIN-protection). This is the best compromise between PIN-protection and exportability of keys.
- Low Security: Non-exportability is disabled by default, but can be enabled when the profile is created if that profile is also set to use PKI Client as the Enrollment method. This restricts the certificate from being exported for profiles that otherwise require Low security.

  EFS Recovery certificate cannot be made non-exportable.

Once the security level is set and the certificate profile is saved, this setting cannot be changed.

Support for IPSec Server Certificates

This release of Managed PKI allows you to issue IPSec Server certificates. With IPSec Server certificates, you can perform secure authentication on server machines such as Cisco concentrators. You can also configure these certificates to allow IPSec communications with only client authentication.

Enroll for IPSec Server certificates using CSRs or SCEP enrollments.

Support for Custom Attributes in Subject Distinguished Name (DN)

Previously, you could select from a list of common attributes, such as Common Name (CN), Organization (O), and Organization (OU) to configure in the Subject DN for a certificate profile. With Managed PKI v8.6, you can request up to three additional, custom Subject DN attributes. Contact your Symantec representative for details.

Support for Actual Validity Start/End Dates

Previously, the Validity Start and End Dates for certificate issued by Managed PKI was rounded up to 23:59:59 of the day of issuance (UTC). With Managed PKI v8.6, the Validity Start Date for all certificates issued will be the actual date and time of issuance in UTC time format. The Validity End Date will be the actual expiration time, in UTC format, based on the certificate's validity period and Validity Start Date.

As an example, a certificate with a validity period of one year, issued at 14:45:20 on September 20 will have the following Validity Start and End Dates:

- Validity Start Date: 14:45:20, September 20, 2012
- Validity End Date: 14:45:20, September 20, 2013

The Validity Start and End Dates for existing certificates will not change.

PKI Enterprise Gateway Updates

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 will need to uninstall your current version of PKI Enterprise Gateway and upgrade to the latest version.

Additionally, the PKI Enterprise Gateway has been updated to include a GUI-based installer that replaces the more cumbersome, potentially error-prone command-line scripts. This installer will install, repair, or remove PKI Enterprise Gateway.

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 end users must upgrade to PKI Client 2.6. 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 Writing Post-processing Scripts Guide has also been updated to reflect theses new features.

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

PKI Client-based Autoenrollment

Administrators can now configure certificate profiles to allow PKI Client to enroll users for certificates automatically. PKI Client will automatically enroll an end user for any profile or profiles configured for that end user, based on the user data contained in Active Directory. PKI Client autoenrollment is tightly integrated with PKI Enterprise

Gateway, making autoenrollment nearly transparent to end users and administrators alike:

- Depending on how the certificate profile is configured, the enrollments will occur without end-user notification or intervention.
- Administrators will not need to provide an enrollment email, enrollment code, or enrollment link for certificate enrollment.

As before, PKI Client will continue to automate renewals, completing the fully-automated certificate lifecycle experience.

To enable PKI Client autoenrollment, you must:

1. Install PKI Enterprise Gateway. Active Directory must be selected as the user store, and the end-user machines must be joined to the domain configured in PKI Enterprise Gateway. Refer to *Symantec™ PKI Enterprise Gateway Deployment Guide* for details on installing and configuring PKI Enterprise Gateway.
2. Configure your certificate profile for PKI Client-based autoenrollment. Refer to PKI Manager and its associated help for details on creating certificate profiles.
3. Provide group policy settings to PKI Client on your end user machines to initiate the automatic enrollment. Refer to *Symantec™ PKI Client Administrator's Guide* for procedures on defining and pushing group policy settings to PKI Client on your end-user machines.

Support for Check Point VPN Post-processing

In this release, PKI Client supports post-processing for CheckPoint VPN servers. If the Check Point VPN post-processing script is enabled for a certificate profile in PKI Manager, the PKI Client will configure the Managed PKI certificate to work with Check Point VPN servers during enrollment.

Updated Language Support

Managed PKI v8.6 includes support for the following languages:

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

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 v8.6-specific material:

- *Managed PKI™ v8.6 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™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide*
- *Symantec™ Managed PKI® Overview*
- *Managed PKI® Transaction Signing API Developer's Guide*

The following new documents have been added to the Managed PKI documentation set:

- *Symantec™ Managed PKI® Enterprise Mobility Guide* describes how to integrate Managed PKI certificates with your end users' iOS and Android mobile devices.
- *Managed PKI® Getting Started with iOS Mobile Devices* is a quick reference for integrating Managed PKI certificates with your end users' iOS mobile devices.

These, and 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. Enter **Managed PKI v8.6** as the Knowledge Center Search text.

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