# Managed PKI™ v8.5 Release Notes

Symantec

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 Release Notes

# Managed PKI Release Notes

These release notes accompany the delivery of the Symantec Managed PKI v8.5 release. Managed PKI v8.5 is an automatic upgrade of Managed PKI v8.4 with the following exceptions:

- PKI Certificate Manager will automatically upgrade to version 2.5 unless you have manually disabled Live Update for your end users. If you have disabled Live Update, you must enable it to pick up the latest version of PKI Certificate Manager.

## What's New in Managed PKI v8.5

This release of Managed PKI provides the following updates:



### Updated Platform Support

Managed PKI v8.5 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)<br>Firefox 10.0.3, 12 |
| Windows® 7 (32-bit) | IE 8 (32-bit), 9 (32-bit)<br>Firefox 10.0.3, 12 |
| Windows® 7 (64-bit) | IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit)<br>Firefox 10.0.3, 12 |

## PKI Certificate Services

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

| OS | Browser |
|---|---|
| Windows XP SP3 | IE 8 (32-bit)<br>Firefox 10.0.3, 12 |
| Windows 7 (32-bit) | IE 8 (32-bit), 9 (32-bit)<br>Firefox 10.0.3, 12 |
| Windows 7 (64-bit) | IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit)<br>Firefox 10.0.3, 12 |

## PKI Certificate Manager

- OS: Windows XP SP3, Windows 7 (32-bit and 64-bit)
- Applications:
  - Outlook Client 2007, 2010 (32-bit and 64-bit)
  - Thunderbird 3
  - Adobe 9, X
  - Word 2007, 2010 (32-bit and 64-bit)
- Browsers: IE 8 and 9 (32-bit and 64-bit), Firefox 3.6 and 10.0

## 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.XXX
- HSMs:

**Table 1-3** 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 1-4** 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 1-5** iOS device support

| Device | OS |
|---|---|
| 3rd and 4th generation iPhones | iOS 4 or iOS5 |
| 1st and 2nd generation iPads | |

## 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.

## User Interface Improvements

The PKI Manager user interface was updated in Managed PKI v8.4 to use a new liquid design that is more streamlined and easier to use, and which supports a wider range of monitor sizes and resolutions. In this release, the Authorized User List, and PKI Enterprise Gateway modules were updated to support the new design.

## Ability to send Enrollment Code to End Users in Enrollment Email

This release of Managed PKI allows you to configure a certificate profile to send the enrollment code to an end user as part of the enrollment link in the enrollment email. The end user will only need to paste the enrollment link into his or her browser to access and be authenticated to the enrollment request page.

---

**Note:** This enrollment code delivery method is only available for profiles that issue Class 2 certificates, as sending the enrollment link and enrollment code by separate delivery mechanisms is more secure.

---

## Seat Pool Support

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 issued certificates count against that total.

This release of Managed PKI supports three seat types:

- 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 Microsoft Domain Controller certificates

For user seats, you can issue multiple valid certificates to the same seat ID. For device and server certificates, you can issue only one valid certificate to each seat ID. If you revoke all valid certificates assigned to that seat ID, the seat will be credited back to the seat pool.

The PKI Manager dashboard has been updated to show the number of certificates available and used for each seat pool; however, the seat usage graph on the dashboard only displays seats issued from the User seat pool.

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

## Support for Custom Post-processing Scripts

PKI Certificate Manager can run pre-defined scripts for certificates enrolled, imported, or renewed in PKI Certificate Manager, to automate the process of integrating the certificate with third-party applications, such as email clients and VPN devices. This release of Managed PKI allows you to upload and manage your own custom scripts that

perform these post-processing operations for end user certificates in PKI Certificate Manager.

You can write your own script, or download a script template to modify for your needs. You assign which certificate profile templates will use the scripts at the account level. Once assigned to a certificate profile template, you can remove or reassign them for individual certificate profiles.

Refer to *Symantec™ PKI Client Writing Post-processing Scripts Guide* for details on writing your own custom scripts.

### Support for CSR Enrollment

Managed PKI v8.5 allows your end users to enroll for Domain controller certificates using Certificate Signing Requests (CSRs). Managed PKI will only use the public key in the CSR; all other fields will be ignored.

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.

### Enhanced Support for iOS Certificates

Managed PKI v8.3 enabled you to create certificate profiles that issue certificates to your end users' iOS devices. Managed PKI v8.4 provided support for integrating certificates with Microsoft® ActiveSync®. Managed PKI v8.5 provides support for renewal of end user certificates on iOS devices.

*Symantec™ Managed PKI® Integration Guide for ActiveSync®* is available by selecting the Resources icon in the lower left corner of the Managed PKI application.

## PKI Certificate Manager Updates

PKI Certificate Manager 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 Certificate Manager 2.5. For most users, this will happen automatically, unless you have disabled Live Update or cannot access symantec.com. 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 the new custom script upload feature.

## PKI Enterprise Gateway Updates

This release of PKI Enterprise Gateway provides support for Lightweight Directory Access Protocol (LDAP) user stores. You will need to install and configure a separate PKI Enterprise Gateway for each type of user store you will use with Managed PKI.

*Managed PKI® PKI Enterprise Gateway Deployment Guide* has been updated for this new feature, and describes how to install and configure PKI Enterprise Gateway with an LDAP user store.

## Web Services Improvements

The Managed PKI Web Service has been improved to include the following:

- Ability to search for certificates by multiple criteria, including the certificate's Common Name, status, email address, issuing CA, and validity dates.
- Ability to revoke certificates by seat ID or certificate serial number.

*Symantec™ Managed PKI  PKI Web Services Developer's Guide* has been updated to describe these improvements and how to integrate them with your client applications.

## Transaction Signing API

This release of Managed PKI includes a new Transaction Signing API that you can integrate with your web applications to provide your end users the ability to securely authenticate and sign transactions.

A new document, *Managed PKI® Transaction Signing API Developer's Guide* is available in the PKI Enterprise Gateway package. This new document describes this new API and how to integrate it with your web applications.

## Miscellaneous Improvements

Managed PKI v8.5 includes the following minor updates:

- Changed the sender address for production and Test Drive Managed PKI accounts from noreply@symantec.com to noreply@pki.symantec.com and enterprise_pkisupport@symantec.com to support@pki.symantec.com, so that enterprise email applications are less likely to block these emails.
- The format of certificates issued by Managed PKI now includes an issuing URL that identifies the certificates' issuing CA.
- A number of messages and UI text strings were updated based on customer feedback.
- The PKI Manager and PKI Certificate Service has been updated to support the French language.

# Documentation

*Symantec™ Managed PKI® Overview* has been added to the Managed PKI documentation set. This guide provides an overview of the Managed PKI service, as well as information that you will need to get started with configuring your Managed PKI account and certificate profiles.

Additionally, the following documents have been revised to incorporate Managed PKI v8.5-specific material:

- *Managed PKI™ v8.5 Release Notes* (this document)
- *Symantec™ PKI Client Administrator's Guide*
- *Symantec™ PKI Client Writing Post-processing Scripts Guide*
- *Managed PKI® PKI Enterprise Gateway Deployment Guide*
- *Symantec PKI Enterprise Gateway™ Autoenrollment Server Deployment Guide*
- *Symantec™ Managed PKI® Integration Guide for ActiveSync®*

These, and all other Managed PKI documents, are available from the *Resources* page of PKI Manager.

# Known Issues and Workarounds

The release of Managed PKI addressed numerous issues, across multiple components. For a list of the issues addressed and their ID numbers, as well as a list of the open issues and workarounds related to this release, access the Symantec Knowledge Center for Managed PKI at the following URL. Enter **Managed PKI v8.5** as the Knowledge Center Search text.

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

This section describes known issues and solutions at the time of this release. Refer to the accompanying ID number, in parentheses, if you call Customer Service with any questions or problems about the associated issue.

**Table 1-6** Known issues and workarounds

| Issue | Workaround |
|---|---|
| The PKCS #11 module has an issue with Mozilla Firefox and Thunderbird. If the PKCS #11 module is imported manually into either application and no PIN has been initialized on My Computer, a PIN prompt will still appear for the uninitialized token. (artf106892) | If the module was added manually, then it should be removed. This can be done manually in Firefox via Options>Advanced>Encryption>Security Devices>Unload.<br><br>You should add a module during post-processing of any enrollment, renewal, or import operation.<br><br>In order to do this via the command line, the user needs to know the path to the Firefox installation, the PKI Certificate Manager installation, the user's Firefox profile, and the name of the manually-added module.<br><br><u>To list existing modules:</u><br><br>cd [Firefox Install - C:\Program Files (x86)\Mozilla Firefox]<br><br>"[PKI Client Path - C:\Program Files (x86)\Symantec\PKI Client]\BERETTA\bin\modutil.exe" -list -dbdir "[User's Firefox Profile - C:\Users\USERNAME\<br><br>AppData\Roaming\Mozilla\Firefox\Profiles\5lkfw1vx.default]"<br><br><u>To delete a module:</u><br><br>cd [Firefox Install]<br><br>"[PKI Client Path]\BERETTA\bin\modutil.exe" -delete "[Module Name - Symantec Security Module]" -dbdir "[User's Firefox Profile]"<br><br><u>To add a module:</u><br><br>cd [Firefox Install]<br><br>"[PKI Client Path]\BERETTA\bin\modutil.exe" -add "Symantec Security Module" -dbdir "[User's Firefox Profile - C:\Users\USERNAME\AppData\Roaming\<br><br>Mozilla\Firefox\Profiles\5lkfw1vx.default]" -libfile "[PKI Client Path]\PKCS11.dll" -mechanisms FRIENDLY -force |

**Table 1-6** Known issues and workarounds (Continued)

| Issue | Workaround |
|---|---|
| In single user enrollment, if all the required user attributes had not been previously entered, the administrator will receive an error message stating that all the values were not entered. (artf104765) | The administrator must know all the user attributes ahead of time and enter them. |
| On the client's Private CA, there is not an option to download the Certificate Revocation List (CRL), and the CRL Distribution Point (CDP) is not shown. (artf106942) | The administrator can issue a certificate and extract the CDP from within it. |
| PKI Manager does not assign the right name for email. (artf105023) | A certificate is still issued, but it shows it was issued by the email address DNemail@att.com |
| If the user has no network connectivity and imports a glock certificate in the PKI Client, post processing will not be run. | The user must ensure network connectivity before importing a certificate. |