Managed PKI™ v8.4 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 v8.4 release. Managed PKI v8.4 is an automatic upgrade of Managed PKI v8.3 with the following exceptions:

- PKI Client will automatically upgrade to version 2.4 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 Client.

What's New in Managed PKI v8.4

This release of Managed PKI provides the following updates:

Updated Platform Support

Managed PKI v8.4 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 9.0, 10.0
Windows® 7 (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 9.0, 10.0
Windows® 7 (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 9.0, 10.0

PKI Certificate Services

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

OS	Browser
Windows XP SP3	IE 8 (32-bit) Firefox 3.6, 8.0, 10.0 (For Test Drive enrollments, only Firefox 10.0 is supported)
Windows 7 (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 3.6, 8.0, 10.0 (For Test Drive enrollments, only Firefox 10.0 is supported)
Windows 7 (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 8.0, 10.0 (For Test Drive enrollments, only Firefox 10.0 is supported)

PKI Client

- 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
- 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.

User Interface Improvements

The PKI Manager user interface uses a new liquid design that is more streamlined and easier to use, and which supports a wider range of monitor sizes and resolutions.

- Changing your resolution or browser size automatically changes the available workspace. For monitors with larger screens or higher resolution, a larger work area is available. For monitors with smaller screens or resolutions, the interface automatically hides work areas that are not immediately required. However, you can easily show these hidden work areas when you want to see them.
- Most modules have been divided into multiple panels. Each panel allows you to view or act on a different aspect of a workflow:
  - The Search panel allows you to create and run searches for selected criteria.

- The Results pane displays the results of searches, and allows you to select one or more objects to view or act on.
- The Actions panel provides links for available actions for the selected objects in the Results panel.
- The Details panel displays the details of the selected objects, and allows you to perform any required action on the selected objects.

The Dashboard, Authorized User List, and PKI Enterprise Gateway modules do not currently support the multiple-panel model.

- Wherever possible, workflows were moved out of modal widows and integrated into the Details panel.

Support for Granular Administrator Roles

This release of Managed PKI introduces a number of new administrator roles and allows you to configure specific permissions for each.

Table 1-6 Administrator roles and permissions

Role	Permissions Available	Details
User and certificate manager	View users	View user details.
	Manage users	View, create, edit, and delete users. This permission also allows the administrator to enroll users for certificates.
	Approve certificates	Approve or reject user certificate requests.
	Revoke certificates	Permanently revoke user certificates.
	Recover private keys	Recover the private keys for user certificates, allowing the user to recover certificates that were corrupted or otherwise unusable.
Certificate profile manager	Manage profiles	View, create, edit, and delete certificate profiles.
	View profiles	View certificate profiles.

Table 1-6 Administrator roles and permissions (Continued)

Role	Permissions Available	Details
Account manager	Manage account	View and edit details of the account, such as requesting additional seat count and updating contact information.
	View account	View details of the account.
	Manage sub-accounts	View, create, and delete sub-accounts. This permission also allows the administrator to assign other administrators to, and remove them from, sub-accounts.
	View sub-accounts	View details of sub-accounts.
	Enroll for RA certificates	Request and download RA certificates. You will need RA certificates if you are setting up PKI Enterprise Gateway or PKI Web Services.
	Enroll for signing authority certificates	Request and download signing authority certificates. You will need a signing authority certificate if you are setting up PKI Enterprise Gateway for an application that uses the Managed PKI Signing API
Account administrator manager	Manage administrators	View, create, edit, delete, and assign roles to administrators. **Note:** In order to edit an administrator from within a sub-account, this administrator must also have the Account manager role with the Manage sub-account permission.
	Invite administrators	Invite administrators from other PKI Manager accounts to become administrators on this account. This permission also allows the administrator to assign roles to and edit details of the invited administrators. These changes apply only to the administrator for this account; they do not affect the invited administrator's details in the administrator's original account.
	View administrators	View details and roles of administrators.

Table 1-6 Administrator roles and permissions (Continued)

Role	Permissions Available	Details
Reporting	Manage detail reports	Run, schedule, and delete detailed reports of user, certificate, administrator, and audit activity.
	View detail reports	View detailed reports of user, certificate, administrator, and audit activity.
	Manage summary reports	Run, schedule, and delete summary reports of user, certificate, administrator, and audit activity.
	View summary reports	View summary reports of user, certificate, administrator, and audit activity.

Any existing administrator in your account with the Super administrator role will receive all roles and permissions. Any existing administrator in your account with the PKI administrator role will receive all roles and permissions except the Manage administrators permission.

Support for Hardware Token Enrollment

Managed PKI v8.4 includes additional certificate profile options that allow you to issue certificates that reside on hardware tokens. You can select which Cryptographic Service Provider (CSP) to use for cryptographic operations (such as generating a private key or signing/encrypting emails). Specifically for v8.4, you have two hardware token enrollment options:

Smart Card Logon Support

This release of Managed PKI allows you to issue certificates that are generated and stored on smart cards, tokens, or similar security devices. The user must plug in the device prior to enrolling for the certificate.

Intel® IPT with PEAT Support

This release of Managed PKI allows you to issue certificates for Intel Identity Protection Technology with Platform Embedded Asymmetrical Token (PEAT). These PEAT-compliant certificates are embedded in the PC firmware and managed through PKI Client (PKI Client treats Intel IPT with PEAT as a third-party CSP).

Separation of User Creation from Enrollment

In this release of Managed PKI, the creation of users stored at Symantec has been separated from the enrollment of those users for certificates. Before a user can enroll (or be enrolled) for a certificate against a profile that requires the user to exist at Symantec (for example, against a profile using a public CA), you must first add the user to the Symantec user store. Do this from the **Add users** link on the *Manage users* page.

Note that, if your end user is stored in a user store at your enterprise location, and you want to enroll the user for a profile that requires the user to exist in the Symantec data store, you must first upload the user to Symantec.

Support for ActiveSync-enabled Certificate Profiles

With Managed PKI v8.4, you can configure a certificate profile to issue certificates that support Microsoft ActiveSync® for Secure Sign in.

PKI Client Updates

PKI Client (also known as PKI Certificate Manager) is the desktop middleware that assists your end users manage their certificate lifecycle. This release of Managed PKI includes the following updates to PKI Client:

PKI Client Downloadable from PKI Certificate Services

Previously, you needed to provide PKI Client to your end users (as an installation file or as a GPO push) before they could enroll for certificates. With Managed PKI v8.4, your end users can download PKI Client directly from PKI Certificate Services when enrolling for certificates.

However, if you do not want your users to be able to download PKI Client directly, you can configure for each certificate profile in PKI Manager.

Post-processing Support for Cisco VPN

This release of Managed PKI allows you to write a post-processing script for Cisco VPNs. This script helps automate the integration of Managed PKI certificates into Cisco VPN routers.

Refer to *Symantec™ PKI Client Writing Post-processing Scripts Guide* for instructions on writing a post-processing script for Cisco VPNs. Once written, upload and assign them to certificate profiles using PKI Manager.

PKI Enterprise Gateway Autoenrollment Server Updates

PKI Enterprise Gateway and the optional Autoenrollment server reside on your enterprise site and allow you to act as a local Registration Authority to enroll users for, issue, and perform lifecycle tasks on, certificates. This release of Managed PKI includes the following updates to PKI Enterprise Gateway and the Autoenrollment server:

Additional Luna HSM Support

This version of PKI Enterprise Gateway supports the following additional Luna HSMs:

- Luna SA Hybrid (PED Auth)
- Luna PCI and PCI Express Cards (3000 Signing)

Refer to "Updated Platform Support" on page 1 for driver and firmware requirements.

Support for High Availability

This version of PKI Enterprise Gateway and the Autoenrollment server have been qualified to support multiple instances for high availability. *Managed PKI® PKI Enterprise Gateway Deployment Guide* and *Symantec PKI Enterprise Gateway™ Autoenrollment Server Deployment Guide* have been updated to include configuration information.

Autoenrollment Server Support for Domain Controller Certificates

This version of Autoenrollment server has been qualified to support domain controller certificates.

Re-installing the Autoenrollment Server

From this version of Autoenrollment server onwards, you are only able to install one instance of the Autoenrollment server on a machine. If you attempt to install the Autoenrollment server on a machine where an instance already exists, the installer will prompt you to uninstall it (using the uninstall option) before continuing with the installation.

If you have installed multiple instances of an earlier version of the Autoenrollment server, the uninstall option will remove all instances of the Autoenrollment server.

Refer to *Managed PKI® PKI Enterprise Gateway Deployment Guide* for details on installing and uninstalling PKI Enterprise Gateway.

Certificate Validity Period Extensions

The validity period is the period starting when a certificate is issued and ending when it expires (or is earlier suspended or revoked). With Managed PKI v8.4, the following certificate validity periods have been extended. For both, you will need to edit an existing profile or create a new profile to take advantage of the extended validity period. The validity period for certificates that have already been issued will not change.

- Test Drive Expiration Period Extension—The validity period for certificates issued through Managed PKI Service Test Drive has been extended to 90 days.
- Shared Class 2 Public CA—The validity period for certificates issued through Managed PKI Service has been extended to 1095 days (3 years).

Documentation

The following documents have been added or revised to incorporate Managed PKI v8.4-specific material:

- *Managed PKI™ 8.4 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*

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

Issues Addressed in this Release

This release of Managed PKI addressed numerous issues, across multiple components. The following is a list of the general areas of improvement, along with ID numbers for the specific issues addressed. Refer to the accompanying ID number if you call Customer Service with any questions or problems about a specific issue.

Table 1-7 Issues addressed

Component	Issue ID
Certificate Services - Enrollment/Renewal	artf101683, artf102458, artf102498
Certificate Services – General Look and Feel	artf101704, artf101911, artf91465, artf94309, artf97905, artf97911, artf97912
Documentation	artf102025, artf99512
General Localization Issues	artf101595
iOS Service	artf101114, artf101393, artf101395, artf101456, artf101610, artf101615, artf101697, artf101705, artf101706, artf101708, artf102738
Managed PKI Service Test Drive	artf97542, artf98036, artf98486
Managed PKI Web Services	artf101308, artf101938, artf102667
PKI Client	artf100754, artf100823, artf100934, artf100994, artf101183, artf101186, artf101191, artf101351, artf101370, artf101425, artf101427, artf101506, artf101518, artf101553, artf101555, artf101601, artf101603, artf101643, artf101650, artf101651, artf101732, artf101733, artf101743, artf101752, artf101757, artf101758, artf101759, artf101813, artf101814, artf101915, artf101972, artf101973, artf101974, artf102045, artf102186, artf98758, artf99981, artf102044
PKI Enterprise Gateway/Autoenrollment	artf101659, artf99711, artf99942, artf101745
PKI Manager - Manage administrators	artf102218, artf97878, artf99002, artf103099, artf103161
PKI Manager - Dashboard	artf101607, artf91140, artf101580, artf101804, artf101945, artf91886, artf99252
PKI Manager – General UI Improvements	artf100340
PKI Manager – Manage sub-accounts	artf100282, artf101746

Table 1-7 Issues addressed (Continued)

Component	Issue ID
PKI Manager – Manage certificate profiles	artf100342, artf100735, artf100771, artf100996, artf101066, artf101702, artf101912, artf90192, artf91467, artf97468, artf97808, artf97822, artf98606
PKI Manager – Manage users and certificates	artf100012, artf100371, artf100405, artf101626, artf104151, artf89598, artf91606, artf97873, artf98573
PKI Manager – Reporting	artf100364, artf90815, artf90854, artf91298, artf99919

Issues and Workarounds

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 1-8 Known issues and workarounds

Issue	Workaround
General Issues	
Certificates exported from Intel PEAT-enabled devices in PKCS#12 format are not compatible with other applications that require CRT fields, such as Microsoft Certificate Manager. (artf103321)	There is no workaround for this issue.
PKI Manager Issues	
If you click the **Add report** link from the top of the *Manage reports* page while you have an existing scheduled report selected, any changes you make will be saved to the existing report, not to a new report. (artf104362)	Clear the selection in the search results pane (click **Search** again) before attempting to add a new report.
PKI Manager does not honor the **Set as default** selection for a customized email template. (artf104228)	Customize email templates for profiles individually.
If a user is created under a manual approval certificate profile but not yet approved by an administrator, the administrator can enroll the user for a certificate. (artf104231)	You should approve the user before enrolling the user for a certificate.

Table 1-8 Known issues and workarounds (Continued)

Issue	Workaround
If you enter an invalid setting for the otherName(GUID) attribute in a SubjectAltName field, the profile will be saved but users will not be able to enroll for certificates. (artf104136)	Always use a valid value for the otherName(GUID) attribute when configuring a certificate profile.
When you enroll a user for a certificate from the *Manage profiles* page, the **User identifier** field does not always appear, and you cannot continue with the enrollment. (artf104271)	This is an intermittent issue. Return to the *Manage profile* page and begin the enrollment process again.
If you select all items in the search results pane, the count of users is correct; however, if you deselect one or more users manually, the count is not displayed correctly. (artf104178)	There is no workaround for this issue.
The revocation reason and date are not always displayed for revoked certificates. (artf103700)	There is no workaround for this issue.
Certificate Services Issues	

An end user enrolling for a certificate may experience an unexpected error under the following conditions: (artf104093)
■ The end user is running Internet Explorer 9 on Windows 7.
■ ActiveX Controls are not enabled
■ The certificate profile is configured as follows:
  ■ Enrollment method: OS/browser
  ■ Authentication method: Passcode
  ■ Key escrow: No
	Have the user enable ActiveX Controls from Internet Options, and retry the enrollment operation.

An end user enrolling for a certificate will experience errors if he or she attempts to download PKI Client more than once in the same browser session (for example, if he or she clicks the browser's **Cancel** button and attempts to download PKI Client again). (artf102467)	Instruct the user not to attempt to download PKI Client more than once from the same browser session.
An end user may experience errors if he or she attempts to install multiple certificates simultaneously (using different tabs or different browsers). (artf102258)	Instruct the user to complete one certificate enrollment at a time.
iOS Profile Issues	

Table 1-8 Known issues and workarounds (Continued)

Issue	Workaround
When configuring a certificate profile with iOS as the enrollment method, you will see a message that you need to configure the device profile. However, the message does not disappear after uploading a valid device profile. (artf104224)	There is no workaround for this issue; however, functionality is not affected.
PKI Client Issues	
When PKI Client is upgraded, the PKI Client process does not automatically restart. (artf104126)	Have the user restart PKI Client after an upgrade (for example, **Start** → **Programs** → **Symantec** → **Symantec PKI Client**). Otherwise, the process will restart the next time the user starts Windows.
If a user imports a certificate into PKI Client, deletes it, and then attempts to return to it but does not remember the PIN, the user will not be able to reset the PIN. (artf104149)	There is no workaround for this issue.
If a user's device requires a minimum PIN length that is greater than the value you choose for the maximum PIN length in the PIN policy of PKI Client, the maximum PIN length will be lower than the minimum PIN length.	Either have the user reset the minimum PIN length in his or her device, or set the maximum PIN length higher in the PIN policy.
Documentation	
Page 4 of PKI Client Administrator Guide states that, for SSL web authentication, users can be authenticated to web sites using a certificate stored on their smart card. However, SSL web authentication is also available to certificates stored in PKI Client.	There is no workaround for this issue; however, functionality is not affected.

Additionally, there are a number of minor user interface and localization issues that do not affect functionality. (artf104017, artf103929, artf104210, artf103552, artf104134, artf103663, artf103952, artf103235, artf103305, artf103075, artf103540, artf103299. artf103864, artf103893, artf104393, artf103977, artf103945, artf103534, artf103535, artf103533, artf103537, artf103538, artf103849, artf104414, artf103728, artf102181, artf102180, artf102175, artf103962, artf104036, artf103930, artf103565, artf104013, artf103965, artf104005, artf104106, artf103983, artf104319, artf103813, artf103653, artf104346, artf103282, artf102720, artf103933, artf104013, artf103297, artf104389, artf103760, artf103163, artf104302, artf104068, artf103629, artf102783, artf104293, artf102423, artf104152, artf104123.)