Symantec Managed PKI™

Release Notes

V8.3

Symantec Managed PKI™ V8.3 Release Notes

This document may describe features and/or functionality not present in your software or your service agreement. Contact your account representative to learn more about what is available with this Symantec® product.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com/

http://www.symauth.com/support/contact/index.html#support4

Contents

Symantec Managed PKI™ V8.3 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI V8.3 release. Managed PKI v8.3 is an automatic upgrade of Managed PKI v8.2 with the following exceptions:

- PKI Client will automatically upgrade to version 2.3 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.
- The certificate templates in Managed PKI v8.3 support the subject key identifier extension. If you have already created certificate profiles and want to benefit from this update, you must create new certificate profiles to replace your existing ones.

What's New in Managed PKI

This release of Managed PKI provides the following new features:

Updated Platform Support

Managed PKI v8.3 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

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

PKI Certificate Services

OS	Browser
Windows XP SP3	• IE 8 (32-bit) • Firefox 3.6, 8.0
Windows 7 (32-bit)	• IE 8 (32-bit), 9 (32-bit) • Firefox 3.6, 8.0
Windows 7 (64-bit)	• IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) • Firefox 8.0

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 8.0

PKI Enterprise Gateway

For PKI Enterprise Gateway installations:

- 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:

Type	Luna SA	Luna PCI
Driver	4.4.3-1	3.0
Firmware	4.8.1	4.7.1

For Autoenrollment Server installations:

- Server OS: Windows 2008 R2 Server Enterprise (64-bit) or Windows 2008 R2 SP1 Server Enterprise (64-bit)
- HSMs:

Type	Luna SA	Luna PCI
Driver	4.4.3-1	3.0
Firmware	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:

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

PKI Manager Updates

Managed PKI v8.3 includes the following updates to PKI Manager.

Certificate Profiles Updates

- This version of Managed PKI enables you to create certificate profiles that issue certificates to your end users' iOS devices. Your end users can use these certificates to authenticate themselves to VPNs and Wi-Fi networks.

  You can use the basic settings to configure VPN and Wi-Fi certificate profiles. These profiles work for the majority of VPN and Wi-Fi implementations. However, if you require more advanced configurations, you can also use the advanced settings to upload a mobile.config file created by the Apple® iPhone Configuration Utility.
- Additionally, all Managed PK I v8.3 certificate templates support the subject key identifier extension by default. If you have created certificate profiles in an earlier

version of Managed PKI and want to use this extension in your end-user certificates, you must use the new certificate templates to create new certificate profiles to replace your existing ones.

Localization Support for End-user Enrollment Pages

Previously, you could translate standard field labels in the end-user enrollment pages by selecting from a list of supported languages when configuring the certificate template. If you added additional authentication fields, their field labels would display the text exactly as you entered it when configuring the certificate template.

In this release of Managed PKI, you can fully localize the text of all field labels in the end user enrollment page. This allows you to not only localize the field labels, but to also provide label text that more closely aligns with your organizational needs.

Test Drive Enhancements

In this release, if you sign up for a Symantec Managed PKI Service Test Drive account and pick up your administrator certificate using the same browser on the same machine, you will not be prompted for your pick-up code.

General Improvements

Managed PKI v8.3 provides the following user experience and performance improvements:

- Improvements in the response times to searches for certificate profiles, and in certificate profile management in general.
- Continuous scroll has been added to search results across PKI Manager.
- Report formats have been updated to make them easier to read.
- The End user information report now includes a column which contains the user identifier (Seat ID).

Additionally, multiple issues were addressed in this release. Refer to Issues Addressed in This Release on page 5 for a list of these issues.

PKI Client Updates

Managed PKI v8.3 includes the following updates to PKI Client:

- When picking up an administrator certificate, additional administrators can now download PKI Client directly. This eliminates the need for the initial administrators to provide an out-of-band method for delivering PKI Client to the additional administrators.

The initial administrators can still restrict additional administrators from downloading PKI Client directly, by selecting that option when setting up the certificate profile in PKI Manager.

- PKI Client will perform post-processing on both newly-enrolled and imported Wi-Fi certificates to configure the native Microsoft Wi-Fi client to use the new certificate for authentication to a Wi-Fi network.

Documentation

The following documents have been added or revised to incorporate Managed PKI v8.3-specific material:

- *Managed PKI® V8.3 Release Notes* (this document)
- *Managed PKI SCEP Service Integration Guide*
- *PKI Client Administrator's Guide*
- *PKI Client Writing Post-processing Scripts 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.

Component	Issue ID
PKI Manager - Dashboard	artf88637, artf98662
PKI Manager – Manage users and certificates	artf99687, artf97885, artf91581, artf99025, artf88360, artf91868, artf99332, artf91212, artf91213, artf96228, artf97138, artf96457, artf96458, artf95478, artf94045, artf96667, artf91263, artf91047, artf96248
PKI Manager – Bulk user management	artf95063, artf96229, artf96569, artf96806, artf96008
PKI Manager – Manage accounts	artf98866, artf99183, artf100489, artf99158
PKI Manager – Manage certificate profiles	artf97743, artf92036, artf91605, artf90751, artf96470, artf90820, artf89222, artf98999, artf99247, artf99267, artf99897, artf99416, artf99086, artf99829, artf85946
PKI Manager – Reporting	artf95775, artf98874, artf88653, artf92508, artf96322,

	artf99443, artf99686, artf87173
PKI Manager - Audit trail	artf91846, artf92370, artf91084, artf91381, artf90990
PKI Manager – General Performance Improvements	artf98079, artf98462
PKI Manager – General UI Improvements	artf95301, artf95299, artf98761, artf98959, artf89197, artf88665, artf99103, artf96143, artf99105
Managed PKI Services Test Drive	artf98123, artf99120, artf99984, artf99756, artf99487
PKI Client	artf99152, artf91806, artf99159, artf98914, artf99049, artf99303, artf97990, artf98439, artf99292, artf99385, artf97915, artf98677, artf99489, artf99095, artf100083, artf98856, artf99713, artf99309, artf98833, artf99478, artf98692, artf98790, artf99453, artf99101, artf97980
Certificate Services - Enrollment	artf96509
Certificate Services – General Look and Feel	artf99251, artf97928, artf99456, artf98707
Managed PKI Web Services	artf100961
General Localization Issues	artf90680, artf99490, artf91324, artf96031, artf98329, artf98547, artf95267

Known 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.

Issue	Workaround
PKI Manager Issues	
If an end user whose user data is stored at Symantec receives a passcode for a Secure Email certificate enrollment and does not use it (allows it to expire), the enrollment request appears as an expired certificate on the *Manage users* page. (artf97885)	This is a UI error only; no certificate has yet been issued to the user. Click **Reset enrollment** to generate a new passcode and provide it to the user so that the user can pick up his or her new certificate.
When you (as an administrator) manually enroll a user for a certificate in an Adobe CDS profile, you are prompted to include a user identifier and	There is no workaround for this issue.

Issue	Workaround
then an email address for the user. If you enter a valid email address as the user identifier, the certificate will be issued using this email address, regardless of the email address you enter later. (artf100012)	
Certificates for iOS devices do not include the user's email address by default, even if the email address is provided during enrollment. (artf101114)	This is the expected behavior for iOS devices. To include the email address in the certificate, configure the profile to use UPN in the Subject AltName, and have the user provide the same email address for both the Email and UPN values.
If you enter unsupported characters when editing user details, PKI Manager will correctly identify that the characters are invalid, but displays inconsistent error messages. (artf101488)	There is no workaround for this issue; however, functionality is not affected.
In some situations, when searching for users on the *Manage users* page using the Firefox browser, using the **Enter** key appears to submit your search, but no results will display. (artf100371)	Use the **Search** button to submit your search.
If you upload a CSV file that has no data, PKI Manager displays an error stating that the file was not a valid CSV file, rather than that the file was empty. (artf101174)	There is no workaround for this issue; however, functionality is not affected.
Reports with long names do not always display correctly in the right panel of the *Report details* page and in the search results panel. (artf99919 and artf100364)	There is no workaround for this issue; however, functionality is not affected.
Searches for records in the audit trail for the last seven days returns records for the last eight days. (artf99928)	There is no workaround for this issue.
Certificate Service Issues	
In some situations, if a user clicks the **Back** button on his or her browser after successfully enrolling for a certificate, the user is able to submit a request for a second certificate using the same enrollment code. (artf101393)	There is no workaround for this issue; however, Certificate Services will correctly deny the request and display an error to the user.
iOS Profile Issues	

Issue	Workaround
If you upload a mobile.config file for an iOS certificate profile and required values are not present in the file, the certificate profile will not correctly install and configure the certificate on the end user's iOS device.	Your mobile.config file must include all values required by the iPhone Configuration Utility, even if you do not use this utility to create your mobile.config file Symantec recommends that you use this utility and work with your Symantec representative if you will upload a mobile.config file to PKI Manager.
PKI Client Issues	
PKI Client displays the status of a certificate based, in part, on the response from the OCSP responder. However, there is a delay of up to 5 minutes between the time a certificate is initially picked up and the OCSP responder receives the status of the new certificate. As a result, the certificate status will appear as Unable to determine until the OCSP responder is made aware of the new certificate. (artf99621)	Have the end user wait for five minutes before viewing the status of the certificate again.
During installations or upgrades, PKI Client will be installed to the default installation directory, even if a different directory is specified. (artf101351)	There is no workaround for this issue.
If an end user inserts an unrecognized smart card and attempts to enroll for a certificate, the certificate enrollment will fail. (artf101506)	The user should ensure that only supported smart cards are inserted when enrolling for certificates.
If a user attempts to repair an installation of PKI Client using an MSI file with a different name than the MSI file used to originally install PKI Client, the repair will fail and display an error.	The user should repair the installation of PKI Client using the Windows Control Panel, or rename the MSI file to match the original MSI file name.
In some situations, when a user begins to install PKI Client the installer may take a long to move past the initial progress screen, giving the impression that the installation has frozen. (artf100944)	The installer is preparing the installation but does not provide notification of this. The user should wait until the installer finishes its preparation (in rare cases this may take as long as two minutes).

Additionally, there are a number of minor user interface and localization issues that do not affect functionality. (artf100359, artf100339, artf100342, artf100343, artf100340, artf100282, artf100284, artf100286, artf101427, artf100934, artf99855, artf101425, artf100716, artf101502, artf101496, and artf101492)