Symantec Managed PKI™

Release Notes

V8.2

Symantec Managed PKI™ V8.2 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™ V8.2 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI V8.2 release. Managed PKI v8.2 is an automatic upgrade of Managed PKI v8.1 with the following exceptions:

- PKI Client will automatically upgrade to version 2.1 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.
- If you have previously implemented PKI Enterprise Gateway and want to benefit from the new certificate autoenrollment functionality, you will need to uninstall your existing version of PKI Enterprise Gateway and install the updated version. Refer to the PKI Enterprise Gateway documentation available on PKI Manager for procedures.

What's New in Managed PKI

This release of Managed PKI provides the following new features.

Updated Platform Support

Managed PKI v8.2 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, 6.0
Windows 7 (32-bit)	• IE 8 (32-bit), 9 (32-bit) • Firefox 3.6, 6.0
Windows 7 (64-bit)	• IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 6.0 (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, 6.0
Windows 7 (32-bit)	• IE 8 (32-bit), 9 (32-bit) • Firefox 3.6, 6.0
Windows 7 (64-bit)	• IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) • Firefox 6.0

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 6.0

PKI Enterprise Gateway

For PKI Enterprise Gateway installations:

- OS: Windows 2008 R2, Windows 2008 R2 SP1
- 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, Windows 2008 R2 SP1
- 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 2008 R2, Windows 2008 R2 SP1

Addition of Managed PKI Services Test Drive

With this release, enterprise developers can access a working version of Managed PKI Services to evaluate the service, learn about the functionality, and determine how to configure their certificate solutions. The Test Drive version issues valid PKI certificates from a test CA, and includes all of the functionality of the Managed PKI Service, with the following enforced limitations:

- You are limited to 100 users and 5 scheduled reports.
- You cannot revoke or remove administrators with valid administrator certificates from your Test Drive account. Also, you cannot edit information about an administrator if the administrator has been added but has not yet picked up his or her administrator certificate.
- Certificates are issued under a private test CA, so you will need to provide the Root CA chain to your applications that will consume these certificates.
- PKI Client will not auto-renew test certificates, and renewal emails will not be sent to your end users when their test certificates expire.
- Test Drive accounts are valid for 90 days, by default. If you require additional time to evaluate the Managed PKI Service, you can extend your Test Drive once, to a total of 180 days.

For more information about the Managed PKI Service Test Drive, refer to https://knowledge.verisign.com/support/mpki-support/index?page=content&id=AR1704. To sign up for a Managed PKI Service Teat Drive account, access http://testdrive-pki-account.symauth.com/.

Support for Certificate Autoenrollment through Native Windows® Functionality

Managed PKI now supports certificate autoenrollment using the native Windows autoenrollment feature, through the PKI Enterprise Gateway. If your enterprise uses an Active Directory to store user data, install PKI Enterprise Gateway and the new Autoenrollment server to integrate Managed PKI with your Active Directory and your end user's autoenrollment client. The Autoenrollment server allows the autoenrollment client to automatically request and issue certificates to your end users when your end users start Windows (or when configured to do so in a Group Policy Object push). Use PKI Manager to assign the appropriate certificate template from which to issue certificates.

This feature also allows the Windows autoenrollment client to renew expiring Managed PKI certificates.

If you have already implemented PKI Enterprise Gateway and want to benefit from this new feature, you must uninstall PKI Enterprise Gateway and re-install this version to pick up the new Autoenrollment server.

Ability to Manually Authenticate an End User Enrollment Request

This release of Managed PKI allows you to manually approve a user's or a group of users' certificate enrollment request based on authentication data you define. You can define an optional list of authentication fields to add to the enrollment page, and then provide a common enrollment URL for each certificate profile to your end users. The enrollment page includes any fields that you pre-defined for your end users to complete (the information they provide in these authentication fields does not get added to the certificate).

You can search for users with pending enrollment requests on the *User Management* page, and then approve or reject the request based on the information the users provided.

Support for Sub-accounts

Managed PKI 8.2 enables administrators with the Super administrator role to create and remove sub-accounts from within PKI Manager. Using sub-accounts, you can group management tasks by many factors such as assigned administrators, available certificate types, user base, and so on.

By default, new sub-accounts inherit the administrators (and their roles) and certificate types of the main account. However, the administrator that created the sub-account can add or remove administrators and certificate types, and modify the roles of administrators assigned to the sub-account.

Once administrators are added to a sub-account, they can directly manage the sub-account, including viewing users and certificates, running reports and, if given the Super administrator role, adding certificate types and additional administrators.

Ability to Assign Administrators from Another Account

By default, the administrators in a Managed PKI account for one organization do not have access to the Managed PKI account in another organization. In some situations, however, it might be useful to allow administrators from one account to be administrators on another account (for example, if a parent company has multiple sub-divisions with separate Managed PKI accounts and wants to consolidate the management to one set of administrators). This release adds the ability for a Super administrator in one account to add administrators from another Managed PKI account.

When an administrator is added from another account, it is important to note:

- The added administrator has already been authenticated by Symantec Verification and Authentication when originally made an administrator.
- Administrators added from another account can only add administrators from the original account (they cannot add administrators to this account from other accounts).
- The Corporate Contact and all Super administrators for the account receive email notification of the added administrator.

Ability to Create and Manage Users and Passcodes Using Managed PKI Web Service

This release of the Managed PKI Web Service includes the User Management Protocol. Integrate this protocol into your RA application to allow it to perform the following administrator operations for your end users:

- Add or modify users. This operation allows you to create new users and upload data for the users. If the users already exist, this operation will modify the user data.
- Obtain user information. This operation returns the user information previously uploaded to your Managed PKI account.
- Generate or replace passcodes. This operation allows you to generate and replace passcodes for users, and update the passcode status (bad attempts counter, expiration date, and so on).
- Obtain passcode information. This operation returns information about an individual passcode assigned to a user.

All other protocols remain the same, for backwards compatibility. *Managed PKI® Web Services Developer's Guide* has been updated with this new information. Additionally, this document has been restructured for better readability.

The Managed PKI Web Service package (including the updated document) is available from the *Resources* page of PKI Manager.

Support for SCEP Certificates

This release of Managed PKI allows you to issue SCEP-compliant certificates to users and devices.

Two New Certificate Template Types Added

Two new certificate template types are added in Managed PKI 8.2:

- Computer certificate templates allow you to issue computer certificates (also known as machine certificates) to devices which enable the devices to authenticate themselves to other machines or applications on your network.
- Wifi certificate templates allow you to enroll devices for certificates that enable Wi-Fi authentication.

Support for 3rd Party CSPs

Managed PKI v8.2 now supports the following operations for 3rd Party Cryptographic Service Providers (CSP) installed in PKI Client:

- Manage certificate lifecycle (enroll for, renew, and delete certificates)
- View certificates in PKI Client
- Enforce certificate policy (if the policy is enforced by the CSP)
- Perform PKI Client operations, such as import certificates and check certificate status
- Perform existing PKI Client post-processing operations.

This release supports the Intel PEAT CSP and the Microsoft CSP (with EFS and Wi-Fi certificates).

PKI Client Updates

Managed PKI v8.2 includes the following updates to PKI Client.

Enhanced Troubleshooting Options

PKI Client includes two new troubleshooting options:

- **Diagnostics mode**. If you configure this for your end users, they can select **Diagnostics mod**e from *Advanced settings*. Diagnostics mode captures detailed information about your end users' certificates, including:
    - Trust –Identifies whether the certificate is part of a trusted CA chain.

  - Policy –Identifies if the certificate complies with the appropriate security policy.
  - Private key –Identifies whether the private key for the certificate is able to perform its intended function (such as digital signing or encryption).

  Diagnostics mode is enabled on a per-session basis. Once the end user closes PKI Client, it exits Diagnostics mode.
- **PKI Client logging**. Previously, logging was available only if enabled by an administrator through a GPO push or by editing the end user's registry settings. Additionally, you could only view logs directly from the log file location. With this release, end users can select **PKI Client logging** from *Advanced settings*. End users will be able to set whether PKI Client writes logs of its activity, and can directly view the logs written by PKI Client.

Automatic Certificate Status Checking

PKI Client now automatically checks the status of any certificate issued to your user through Managed PKI. PKI Client displays one of the following statuses, based on the response:

- Valid – The certificate is valid and ready for use.
- Expiring – The certificate is about to reach its expiration date.
- Expired – The certificate has expired and is no longer usable except to unencrypt emails previously encrypted using this certificate.
- Revoked – The certificate has been made invalid by an administrator and is no longer usable.
- Checking... - PK Client is attempting to determine the status of the certificate.
- Unable to determine – PKI Client could not determine the status of the certificate. This could be because the PKI Client could not find an Internet connection.
- Invalid – The certificate is corrupted or otherwise not usable.

Support for Silent Updates

PKI Client can now use LiveUpdate to automatically upgrade itself to the latest version without interaction from an administrator or user.

Documentation

The following documents have been added or revised to incorporate Managed PKI v8.2-specific material:

- *Managed PKI® V8.2 Release Notes* (this document)
- *Managed PKI® Web Services Developer's Guide*

- *Managed PKI® PKI Enterprise Gateway Deployment Guide*
- *Symantec PKI Enterprise Gateway™: Autoenrollment Server Deployment Guide* (new document)
- *Managed PKI SCEP Service Integration Guide* (new document)
- *PKI Client Administrator's Guide*
- *PKI Client Writing Post-processing Scripts Guide*

All documents are available from the *Resources* page of PKI Manager.

Issues Addressed in This Release

In addition to a number of user interface and localization issues, the following issues have been fixed in this release. Refer to the accompanying ID number, in parentheses, if you call Customer Service with any questions or problems about the associated issue.

- DIDC Renew: Unable to install renewal plugin using IE9 in Win7 (artf99001)
- MSTSC has cache issues (artf97461)
- [Client VAMA] Verify all memory is freed (artf89712)
- Cap Log file sizes (artf97005)
- [LiveUpdate] Log file size needs to be managed. (artf97096)
- New GPO setting to disable LUE (artf96575)
- CSP & PKCS#11 – Performance (artf98795)

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	
PKI Manager does not honor the values set for LDAP CRLDistribution Point (CDP) in your CA Policy. These values are not populated in the autoenrollment configuration file downloaded from PKI Manager, so the Autoenrollment server cannot publish CRLs to a custom location	You can configure the Autoenrollment server to publish CRLs to the default location in Active Directory. Add the following string to the CA-Config section of the autoenrollment configuration file for each CA for which you will publish CRLs. Obtain the autoenrollment configuration file from PKI Manager.

Issue	Workaround

in your Active Directory. (artf98176)	`LdapCDP: default`
	This will publish your CRLs to your Active Directory in the following location:
	`CN=<Service-CN>,CN=<machinename>,CN=CDP, CN=Public Key Services,CN=Services,CN= Configuration, DC=<domain>`
	This location must already exist in your Active Directory. Also, make sure that the Autoenrollment server is a member of the Cert Publisher group in Active Directory, and that the Cert Publishers group has write permissions to the default LDAP CDP.

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.
PKI Manager does not automatically clean up old javascript files that were removed or updated with this release. In some rare cases, these files might cause some visual or performance issues. (artf98079)	If you see visual or performance issues, try clearing your browser cache and access PKI Manager again. This may resolve the issue.
If you create a Microsoft® Autoenrollment certificate template with a 1536-bit key size, certificate enrollments will fail. The following message is written to you Autoenrollment server log file (artf99247): `ERROR 2011-10-19 21:07:11.570 216.168.255.62 e7c22e6fbff888ce 0xa508 magnum2be-m1-ap 'text=RSA key length does not match policy. Key length in the request is 2048 Key length from policy is 1536, class.method=CAImpl.verify KeyInfo' "ajp-bio-9009"-exec-33`	The Autoenrollment server supports only 2048-bit or higher key size. You must select a 2048-bit or higher for key size for this certificate template.
In some rare cases, if you return to a workflow in progress after an extended	Refresh your browser or close the workflow, and begin the workflow again.

Issue	Workaround
period of time, the action buttons may no longer work or may no longer behave as expected. (artf99183)	
Administrators cannot search for users with pending enrollment requests by Common Name if the user enrolled for a certificate under a Manual Authentication certificate template. (artf98573)	Use different criteria when searching for these users.
On Internet Explorer browsers, if you click Open (rather than Save) when downloading the autoenrollment configuration file, and you have set Internet Explorer to open .cfg files, Internet Explorer will open the file in the same browser window as PKI Manager is in. You will need to close the browser to access PKI Manager again. (artf99270)	There is no workaround for this issue. This is the expected behavior of Internet Explorer.
When viewing the audit report for sub-accounts created, the Notes column is empty on the first page. When you return to the first page after viewing another page, the expected notes appear.	There is no workaround for this issue; however, the notes are being saved to the audit correctly.
Test Drive Issues	
The Download button still appears if your search for audit trail records returns no results. Clicking the button returns an empty file. (artf98123)	There is no workaround for this issue; however, functionality is not affected.
PKI Client Issues	
If an end user is connected to a domain, PKI Client will not recognize any changes to the group policy that are made locally on the end user's machine.	This is a requirement of Microsoft's domain server. When connected to a domain, the end user's policy changes should be directed by a GPO push from the domain server.
The following features will not be available after LiveUpdate successfully updates PKI Client until the user reboot his or her computer: • Certificate Propagation	These features will become available as soon as the user reboots the computer.

Issue	Workaround
• Automatic Renewal • Log Cleanup	
If you have configured your certificate profile to use 3rd party CSPs and to delete end user certificates that have been renewed, PKI Client will delete the private key from PKI Client, but will not delete the certificate from the certificate store. (artf98692)	There is no workaround for this issue. The certificate is no longer usable, but will remain in the user's certificate store until manually deleted.
When importing a certificate to an uninitialized token, you cannot select the text in the Import field. This is possible when importing certificates to other devices. (artf97980)	There is no workaround for this issue; however, functionality is not affected.
The Alt+a hotkey does not select the End User License Agreement checkbox in some localized versions of the PKI Client installer. (artf97901)	Use another method to select this checkbox (such as the spacebar).
If your users' signing/encryption certificates were set up in Outlook's Trust Center during post-processing, Outlook will not display the AES and SHA-2 hash and the encryption options.	The user must manually select the certificate in Outlook's Trust Center for both the Signing and Encryption certificate options. This will propagate the AES and SHA-2 algorithms to the hash and encryption dropdowns for use.
If a user enters the correct PIN in a client application to access certificates stored in the Software Certificate Store, the incorrect PIN counter is not reset (it will be reset if the user enters the correct PIN in PKI Client). (artf99309).	There is no workaround for this issue; however, if the user locks the Software Certificate Store due to too many bad PIN attempts, PKI Client blocks the use of the associated certificates for 60 minutes, and not permanently.
If Configure PIV/CAC mode is enabled for end users' smart cards and you disable Configure Windows Logon\Device Unblock using a GPO push, the link to configure smart card settings appears, but no settings are shown when you click the link. (artf99309)	There is no workaround for this issue; however, functionality is not affected.
If a user checks the status of a certificate in PKI Client before the certificate has been populated to the OCSP Responder, the OCSP Responder will return a status	There is no workaround to this issue.

Issue	Workaround
of Unable to determine. The certificate will appear as valid once the OCSP Responder is updated with the certificate information. (artf99150)	

Additionally, there are a number of minor user interface and localization issues that do not affect functionality. (artf98329, artf98707, artf98662, artf97990, artf98677, artf99267, artf99301, artf96841, artf99105, artf99103, artf99251, artf99306, artf99002, artf97990, artf99088, artf99292, artf96841, artf99122, artf98874, artf98450, artf97928, artf98796, artf99159, artf98959, artf99252, and artf99025)