Symantec Managed PKI™

Release Notes

V8.1

Symantec Managed PKI™ V8.1 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™ V8.1 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI V8.1 release. Managed PKI v8.1 is an automatic upgrade of Managed PKI v8.0 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.
- Symantec Managed PKI PKI Web Service is a new API for this release. To use it, you must integrate it with your Registration Authority (RA) application.

What's New in Managed PKI

This release of Managed PKI provides the following new features.

Updated Platform Support

Managed PKI v8.1 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.

Component	Platform and OS Requirements
PKI Manager	• OS: Windows XP SP3, Windows 7 (32-bit and 64-bit) • Browsers: IE 7, IE 8 (32-bit and 64-bit), Firefox 6.0
PKI Certificate Service	• OS: Windows XP SP3, Windows 7 (32-bit and 64-bit)

<table>
<tr><th>Component</th><th>Platform and OS Requirements</th></tr>
<tr><td></td><td>• Browsers: IE 6, IE 7, IE 8 (32-bit and 64-bit), Firefox 6.0</td></tr>
<tr><td>PKI Client</td><td>• OS: Windows XP SP3, Windows 7 (32-bit and 64-bit)
• Applications:
o Outlook Client 2003, 2007, 2010 (32-bit and 64-bit)
o Thunderbird 3
o Adobe 9, X
o Word 2003, 2007, 2010 (32-bit and 64-bit)
• Browsers: IE 6, IE 7, IE 8 (32-bit and 64-bit), Firefox 6.0</td></tr>
<tr><td>PKI Enterprise Gateway</td><td>• OS: Windows 2008 R2 64-bit
• Web Server: IIS 7.5, .NET Framework 4.0
• HSMs:
<table>
<tr><td>Type</td><td>Luna SA</td><td>Luna PCI</td></tr>
<tr><td>Driver</td><td>4.3.2 or 4.3.3</td><td>3.0</td></tr>
<tr><td>Firmware</td><td>4.6.8</td><td>4.7.1</td></tr>
</table></td></tr>
</table>

PKI Manager Updates

Support for Managed PKI PKI Web Services API

This release of Managed PKI enables support for the PKI Web Service API. Use this API to develop or integrate certificate lifecycle functionality into your own RA application. You might do this if you will use your own end-user certificate lifecycle pages rather than the PKI Certificate Services provided by Managed PKI.

You can perform the following operations using the PKI Web Services API:

- Obtain the certificate policy for a given certificate profile
- Enroll a user for a certificate (and, if requested, escrow the certificate and private key)
- Renew a certificate
- Revoke a certificate
- Recover an escrowed certificate an private key

Managed PKI PKI Web Service Developer's Guide has been added to the Managed PKI documentation set to assist you with integrating this API into your RA application. Download the PKI Web Service package, including documentation, from PKI Manager's *Resource* page.

Managed PKI Collects Email for all Certificates

Managed PKI now collects the email addresses for all certificate enrollments, even if the email address is not included as part of the certificate. This allows Managed PKI to deliver renewal notices directly to the end user.

If you have created a certificate profile in Managed PKI v8.0 that does not include the email address in the certificate, you must open the certificate profile in PKI Manager, click **Customize options**, and then click **Save**. You do not need to make any edits to the profile to pick up this change.

If using the Active Directory enrollment method, this value is automatically retrieved from the email attribute in your Active Directory. You set which attribute PKI Manager uses when retrieving an email address for a certificate enrollment by setting a custom attribute on the *Customize certificate notification* page.

Support for User Repository in the Cloud

With Managed PKI 8.1 you have the flexibility to host a subset of your enterprise user repository at Symantec. While you can use manage this master list user-by-user, this version of Managed PKI also allows you to perform management operations on multiple users in this master list at one time. Using PKI Manager, you can perform the following operations on multiple users at one time, independent of any certificate profiles:

- Upload users
- Edit user data

PKI Manager also allows you to leverage a common list of users across multiple certificate profiles by performing the following operations on multiple users:

- Enroll users for certificates based on a specified certificate profile
- Manage (reset and download) passcodes for enrolled users

There are two methods you can use to perform multiple operations: either search for users, and then perform the operation on the resulting list of users, or upload a .csv file identifying the users on which to perform the operation.

Optionally, you can search for users and download the resulting list as a .csv file, and then edit the file to upload custom data.

PKI Client Updates

Managed PKI v8.1 includes the following updates to PKI Client.

PIV/CAC Updates

PKI Client includes support for Personal Identity Verification (PIV) and Common Access Card (CAC) Smart Cards. PKI Client allows administrators to enable the following features for their PIV/CAC users:

- Secure Windows Login. Users can log on to their computers using a certificate stored on their smart cards, if that certificate is enabled for Windows Logon.
- Computer Lock and Unlock. Users can lock and unlock their computers using the certificate stored on their smart cards, if that certificate is enabled for Windows Logon.
- Change PIN. Users can change an existing PIN, if the PIN is not locked. New PINs must be 4-6 alpha-numeric characters.
- Unlock Devices (PIV smart cards only). PIV smart card users can unlock their smart card through PKI Client if the device has become locked due to too many failed PIN attempts. This operation resets the PIN block counter to 0 and resets the users' PINs if they enter a new PIN. This operation does not affect the certificates stored on the smart card.

  CAC smart card users must follow your existing, offline process to reset a locked PIN.
- Choose smart card mode. Users can set whether their smart cards function in PIV or CAC mode.

Support for Friendly Names when Importing and Exporting Certificates

If users set a friendly name for certificate in the PKI Certificate Service, the friendly name will appear as the certificate name in PKI Client. Additionally, the friendly name will appear as the certificate filename when importing or exporting certificates stored in their certificate store (My Computer) using PKI Client. End users must select **For import with PKI Certificate Manager (include Symantec Managed PKI settings)** when exporting certificates to retain certificate friendly names.

Support for Automatic Post-processing of Imported Certificates

PKI Client will automatically perform normal post processing operations on imported certificates. For example, if configured to do so, PKI Client will automatically add the certificate PKCS#11 module to Firefox so the certificate is available to that browser. Note that PKI Client will not run post-processing for Outlook and Active Directory if the certificate being imported is expired.

Disable Support for Storing Certificates in the Certificate Store

By default, if end users do not have a smart card inserted when enrolling for or importing certificates, the certificates will be stored in the end user's certificate store (and visible in PKI Client under **My Computer**). Administrators can disable support for storing the certificate in the end user's certificate store, requiring that the certificate be stored in a smart card. End users will need to have their smart cards inserted when performing certificate operations.

PKI Enterprise Gateway

PKI Enterprise Gateway now includes some internal upgrades to improve logging and to provide better policy enforcement for PKI Client.

While these upgrades do not change its overall functionality, this version of PKI Enterprise Gateway does change the way it supports PKI Client. If you have previously implemented PKI Enterprise Gateway and your end users have installed PKI Client, you must uninstall your current version of PKI Enterprise Gateway and reinstall the latest version (available from the *Resources* page of PKI Manager).

Documentation

The following documents have been added or revised to incorporate Managed PKI v8.1-specific material:

- *Managed PKI V8.1 Release Notes* (this document)
- *Managed PKI v8.1 Web Services Developer's Guide* (new document)
- *PKI Client V2.1 Administrator's Guide*
- *PKI Client V2.1 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: Need handle the error code scenario during renewal where root is deleted (artf92191)
- Make BC extension critical for Symantec Admin and RA certificate (artf92376)
- PKI Manager: Internal server error while trying to view the existing profile (artf91574)
- Need to validate XSS input or url encode input (artf91220)
- Magnum Reports : Search Recent reports issues (artf86896)
- Extension in profile needs to respect NOT-ALLOWED element (artf89141)
- If a sdn attribute is added the CN source includes fixed value field as well in the drop-down (artf93419)
- If dnQualifier value is long it gets hidden and is not displayed on the left pane (artf91483)

- Navigating from profile to profile in the profile search results on the Manage Profiles page, the list keeps popping out (artf91616)
- PKI Client is termed as Verisign product in the PKI Client admin guide (artf92989)
- PKI Manager: For Medium security level, the text should be revised (artf93905)
- Select Mode, Select Template and CustomizeOptions page takes a long time to render fully every time (artf92077)
- Sign out page text should be updated to not have Sign in again (artf92078)
- The user full name is appended with null in the revocation email (artf92371)
- If application instruction doc is not saved in Windows EFS recovery profile, get a warning in DIDC log during enrollment (artf91909)
- If ip address is more than 20 chars long , its value overflows on the left pane when profile is created (artf91723)
- Log message gets printed in wrong level (ERROR) when user logs into PKI Manager (artf91795)
- The certificate details overflow out of the window in user management when the profile name is long (artf92993)
- [HTA] Help Topics duplicates itself each time the Help File is opened (artf90998)
- Bad positioning on Help Topic in HTA (artf90996)
- EGW: Enrollment fails for Secure-Sign-In/Hybrid/Native profile when CN and OU:VPN are removed and RegisteredId is added in string format (artf89232)
- Enter userid with underscore for user_id sdn attribute in pki-manager (artf93070)
- MagnumWS: Need to include in the magnum WS document the information about Fault Message and Error Handling (artf83304)
- MagnumWS: Need to include the client code to handle soap fault when developing sample application (artf83305)
- PKI Manager : Signature algorithm in preview changed to default after adding Sdn/San attribute (artf93621)
- PKI Manager: some attributes' value not validated artf82425 ()
- Get an improperly formed error message when more than 64 chars are entered for Directory Name (artf91735)
- Get error when 64 characters is enetered for the local part of SDN attribute Email suffixed with domain yahoo.com (artf91714)
- If CN is not populated for WinEFSRecovery Hybrid profile, EMPTY is displayed in Manage users page for the respective use (artf91913)
- If fixed value is entered with 19 characters for Surname field the text in the left pane overflows (artf91731)

- Admin Management : Cancels saves the updates in the session after a successfull edit (artf91822)
- Admin Management: Issue with an admin whose email originally belonged to a removed valid admin (artf91853)
- Admin Management: UI Display for long First and Last Admin Names (artf94778)
- Admin Management: When you edit the first name , the list on the left panel is not sorted automatically (artf90875)
- For Firefox, Go To Pki Manager Link does not work after admin cert installation (artf93760)
- Go To PKI Manager link does not work in FF (artf95087)
- The passcode field in the USR_PASSCODE_T table does not get updated when you edit the passcode for an approved admin (artf92299)
- You should not be able to remove an active admin without revoking the cert (artf93232)
- Admin Approval Email should have "Enterprise PKI Support" in the from name instead of email (artf92221)
- Admin Management:Audit log for Remove for Active, Expired, Revoked shows TRANSACTION_TYPE="ADMIN_USER_CANCEL' (artf92232)
- Revoke Admin: Warn in log file when you have only 1 admin profile active (artf93235)
- dashboard : Intermediate page appears everytime dashboard is loaded (artf90725)
- Get fatal error while trying to create report for WinEFSRecovery native hybrid profile certificate status (artf91920)
- PKI Manager: Download the software from PKI Manager without any user authentication (artf94039)
- Report: The support URL in the email notification of the report being ready has to point to the new symauth URL (artf92440)
- reports : Instant report creation is failing for history reports (artf91687)
- User can download the pki gateway and pki client unauthenticated (artf91486)
- Reports: Incorrect Error String (artf90860)
- User Mgmt: ERROR messages are getting logged even though the user enrollment is successful (artf91759)
- PKI Manager - Add More Graceful Page Loading (artf90830)
- Get signed policy from backend (artf90285)
- [Client VAMA] CacheServer has no max caching size (artf89704)
- [Po-Pro] Ask user to restart FF if P11 not previously installed (artf93676)
- Add new installer image: smart card icon (artf93960)

- Auto-renew window is not aligned correctly (artf88380)
- Beretta - Error Code 1 on FF (artf91612)
- Getting a 1 in front of XML (artf91691)
- Live Update checks for updates even when offline (artf93761)
- Magnum Web Services rejects "2047-bit" key (artf92363)
- Silent Renewal - thread spawned closes out without registering (artf91119)
- [HTA] Add SubjectDN to Cert Details Section (artf89903)
- Change PIN Errors - SAVAGE change-pin support (artf84752)
- Console - Change Reset PIN warning to represrent possibility of No certs/Unidentifiable certs (artf90277)
- Console - Display error when device/cert in use is no longer available (artf89907)
- Console - Hide error notifications on retry (artf91106)
- GPO Published install only installs for the current user. (artf90555)
- Not getting friendly name on renewed certificates (artf91004)
- Progress for eToken (artf88759)
- Auto Renew - 2 tokens get to last pin try on first, second pin dialog is still pink (artf89920)
- Console - Bad sorting of the certs that are in the dropdown (artf91122)
- Investigate NPAPI issue - Intermitent failed firefox enrollments (artf89452)
- JSON encoder improperly attempts to base64 encode object keys (artf90580)
- Location change suggestions for PIN dialog (artf90833)
- PKI Client: Improve User Experience for Reset PIN (artf91409)
- PKI Client: Post Processing Dialog appears in English when default lang is German (artf90335)
- Certificate management API needs to be able to handle mixed datatype for issuer dn (artf87659)
- Magnum WS: Concurrent 'getpolicy' and 'enrollment' calls take longer to process (artf90877)
- Magnum WS: Multiple SQL-FindProfileByOID calls in one webservice operation (artf88233)

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 you make any updates to information for an existing Managed PKI 8.0 account after upgrading to Managed PKI 8.1, the country field will not be populated. (artf93682)	You will need to manually update this field.
Administrators using the Firefox browser may be prompted to select credentials to log in immediately after signing out of the PKI Manager. If the administrator selects his or her certificate, the prompt will close but the administrator will remain signed out. Additionally, administrators using the Firefox browser may be prompted to select credentials twice when logging in. (artf92076)	To avoid these prompts, clear the browser cache.
If you do not include the @ symbol in the email address for users you enroll from **the Enroll a user** link, PKI Manager does not validate the email address, and the administrator will not be able to complete the user enrollment process. PKI Manager does not display any error notification (appropriate errors are written to the log file). (artf91605)	Always enter email addresses in correct format: <user name>@<domain>.<extension>.
If no value is provided for user data fields, any report generated for the user data will display NULL for those fields. (artf95775)	There is no workaround for this issue; however, it has no affect on report functionality.
Subject DN values cannot include an underscore. PKI Manager will validate this entry when an administrator sets the Subject DN in the certificate profile in PKI Manager; however, PKI Certificate Service does not validate this if you configure the profile to allow the user to manually enter it during enrollment. If a user enters an underscore, the enrollment request will succeed, but the certificate issuance will fail. (artf96127)	You will need to educate your users that underscores are not valid in the Subject DN.
When editing a certificate profile, clicking on Cancel returns the administrator to the Managed profile page, but the profile previously selected is no longer highlighted. (artf95660)	There is no workaround for this issue.

Issue	Workaround
By default, certificate profiles configured for PKI Enterprise Gateway use mail_email to collect users' email addresses for inclusion in the certificate and for sending renewal emails. However, if you configure the profile to include multiple email attributes in the Subject DN, save the profile, and then remove the first email attribute (mail_email) from the Subject DN, the user will not receive renewal emails. (artf95646)	There is no workaround for this issue. However, the correct attributes are used to populate the Subject DN in users' certificates.
PKI Certificate Service Issues	
The filename of a PDF uploaded by the PKI Manager administrator is truncated when a user downloads it from the PKI Certificate Service using the Firefox browser. This occurs if there is a space in the filename. For example, the file **Install Guide.pdf** will be downloaded by the browser as **Install**.	This is a known issue with the Mozilla Firefox browser. To avoid this issue, make sure that the filename of PDFs that you upload do not include spaces.
When an end user initially accesses PKI Certificate Service to enroll for a certificate, the first field that the user should complete is not selected by default. This also occurs in the second enrollment page. (artf95336)	The user will need to manually select the fields to complete in the enrollment pages.
PKI Client Issues	
If an end user is running the 64-bit version of Microsoft Office and has configured Outlook to use the certificate stored on his or her smart card as an S/MIME certificate, Outlook will not pick up the S/MIME security settings when the user inserts his or her smart card for the first time. (artf95831)	These users must manually set their Outlook to use the certificate on the smart card as their S/MIME certificate the first time they insert their smart card.
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 icon displayed for an unsupported smart card is the same as the icon for a supported smart card. (artf94157):	Although the icon is the same for both supported and unsupported smart cards, PKI Client displays prominent messaging when an unsupported smart card is inserted.

Issue	Workaround
When importing or exporting a certificate, PKI Client will honor the file type the user selects in the **File of type** drop-down box (such as .p12 or .glck), even if the user selects the wrong one. (artf95421)	If the user is importing a certificate and selects a different extension in the **File of type** drop-down box than the actual format of the certificate file, the user will encounter an error during the import process. If the user is exporting a certificate and enters a different extension in the **Filename** field than the file type selected in the **File of type** drop-down box, the certificate file will be saved in the format selected in the drop-down box.

Additionally, there are a number of minor user interface and localization issues that do not affect functionality. (artf95839, artf95267, artf95485, artf95059, artf96085, artf94157, artf95229, artf96072, artf91897, artf95300, artf95298, artf95299, artf95301, and artf95302)