Symantec Managed PKI

Release Notes

V8.0

Symantec Managed PKI V8.0 Release Notes

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
http://www.symantec.com

http://www.verisign.com/support/contact/index.html

Contents

Symantec Managed PKI V8.0 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI V8.0 release. Symantec Managed PKI V8.0 release is an optional upgrade for Symantec Managed PKI.

What's New in Managed PKI

This release of Managed PKI includes a greatly redesigned and enhanced service offering designed to streamline the issuance and management of certificates for end users. The following components have been redesigned. Each of the components includes a new, intuitive user interface, and targeted help to make working with the component easier.

- PKI Manager (formerly Control Center)
- PKI Certificate Service (formerly Digital ID Center)
- PKI Client

Additionally, PKI Enterprise Gateway has been added to allow you to use a local Active Directory user store to store user and certificate data.

To take advantage of the redesign, you must install Managed PKI 8.0 as a new service.

PKI Manager

The Managed PKI Control Center has been replaced by PKI Manager. From PKI Manager, you can perform the following administrative tasks:

- Create certificate profiles to enforce your policies that identify how users are authenticated and for what types of certificates they can enroll
- Approve certificate requests and manage certificate lifecycles
- Obtain software and installation documents for PKI Client and PKI Enterprise Gateway

This version of Managed PKI provides five certificate profile templates (Secure Sign-in, Secure Email, Adobe CDS, Windows EFS, and Windows EFS Recovery). This version also supports end-user certificate enrollment using the PKI Client or with native browser enrollment (OS\browser certificate management).

PKI Certificate Service

The Digital ID Center has been replaced by the web-based PKI Certificate Service. Users enroll for, revoke, and renew their certificates using the PKI Certificate Service. The PKI Certificate Service is fully customizable through the PKI Manager.

Once downloaded, your end users can store their certificates in their browser (OS\browser certificate management), or in Symantec's PKI Client.

PKI Client

The PKI Client is software installed on your end-user machines that transparently manages certificates for your end users. This version of PKI Client allows your end users to securely store certificates in the native certificate store or on an Aladdin eToken.

The PKI Client is fully integrated with Symantec's LiveUpdate Service, ensuring that managing distribution and updates to the PKI Client is transparent to your end users.

PKI Enterprise Gateway

PKI Enterprise Gateway is a light-weight replacement for the Registration Authority (RA) Service. Using PKI Enterprise Gateway, you store your end-user certificates and certificate data in a local Active Directory, and use PKI Enterprise Gateway to communicate with the Symantec Certificate Authority. Communications between PKI Enterprise Gateway and Symantec Certificate Authority are secured with an RA certificate.

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.

PKI Manager Issues

- If an administrator clicks **Back** after successfully signing out of PKI Manager, the browser may display a cached version of PKI Manager indicating that the admin is still signed in. (artf91614)

This is a browser issue; the administrator is still signed out of PKI Manager and will need to sign in again in order to perform any actions.

- Adding multiple, additional Subject Domain Name attributes (more than 8), degrades browser performance. Eventually (after more than 19 attributes are added), the browser may prompt you to stop running scripts or the machine may become unresponsive. (artf87958)

  This occurs mainly on Internet Explorer 7. To avoid this issue, use Internet Explorer 8. Optionally, use fewer Subject Domain Name attributes.

- If you edit an administrator's details and save them, then re-edit the administrator's details in the same session but click **Cancel**, the change appears to be saved. (artf91822)

  This is a browser refresh issue; the changes were not saved. Refresh the screen to view the correct administrator details.

- After editing an administrator's first name, the list of administrators in the left pane is not automatically re-sorted. (artf90875)

  Refresh the screen to view administrators in the correct order.

- After editing an end user's first and/or last name, the list of users in the left pane is not automatically refreshed. (artf91047)

  Refresh the screen to view correct user details.

- If you enter too many characters in the **First name**, **Last name**, **Corporate email address,** and **Phone number** fields when adding or editing an administrator's details, you see an error message stating that you entered invalid characters or data, rather than a message stating that you have entered too many characters. (artf91831)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.

- When switching between certificate profiles in the profiles search list (from the *Manage profiles* page), the list of profiles may extend beyond the bottom of the frame. (artf91616)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.

- If you attempt to download the revocation request form to revoke an administrator and your workstation does not have Adobe Reader installed, a blank browser window will open. (artf90874)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.

- If you customize certificate notifications and select **Set as default for new profiles**, the next time you customize certificate notifications, the **Set as default for new profiles** checkbox is no longer selected. (artf90044)

  There is no workaround for this issue.

- If you customize certificate notifications and enter an invalid email address in the **Other recipients** field, the **Save** button is grayed out. The **Save** button is enabled if a valid email address is entered. (artf90709)

  To avoid this, always enter a valid email address in the **Other recipients** field.
- If you add the registeredID Subject Alt Name attribute to your certificate profile and do not map it to a valid OID value (or map it to an Active Directory object which is not a valid OID value), enrollments will fail with an ambiguous error. (artf89232)

  To avoid this issue, always use an OID value (in the format 1.1.1.1.1) for the registeredID attribute of the Subject Alt Name.
- If you remove an expired, revoked, or active administrator and later re-use the sme email address for a new administrator, the new administrator will appear as *Active* rather than *Pending* before he or she has picked up his or her certificate. Additionally, links to management operations that are not available to Pending administrators will appear in the right pane for this new administrator. (artf91853)

  There is no workaround for this issue.
- PKI Manager allows you to add only 8 Subject Alt Name attributes and 20 Subject Domain Name attributes to a certificate profile. Once you add an attribute, it is added to the total count of attributes; even if you later delete attributes, they will continue to apply towards the total count of attributes. (artf87958)

  There is no workaround for this issue.
- Double-byte character sets in PKI Manager can be hard to read in some areas of the user interface. (artf89328)

  There is no workaround for this issue.
- If you enroll a user for certificates issued by a profile configured to send email notifications to users, and Symantec is unable to send email to the user, you are not notified that the email was not sent if the enrollment completed successfully. (artf91214)

  If your end user does not receive the notification email, resend the enrollment code to this user.
- In some cases when you are enrolling for an end user, the browser will freeze and then throw an internal server error, requiring you to re-start the enrollment process for that user. (artf91214)

  There is no workaround for this issue.
- The list of variables in the drop-down box of the Customize email templates page lists all of the available system variables. However, only those variable that are visible in the active email template (the template you are customizing) will appear in the customized email. If you select a variable that does not already exist in the email template, it will not appear in the customized email. (artf91632)

  There is no workaround for this issue.

- The administrator contact name field does not support Unicode surrogate pairs. (artf89327)

  Use simple Unicode text for administrator names.
- The administrator contact name field does not support international email addresses (email addresses with non-ASCII domains). (artf88248)

  Use simple ASCII characters for administrator names.
- The user email address field does not support international email addresses (email addresses with non-ASCII domains). (artf86485)

  Use simple ASCII characters for domains in user email addresses.
- The date fields in some non-English versions of the PKI Manager Reports page are not localized. (artf89324, artf90055)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.
- 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 update the passcode of an approved administrator before the administrator picks up the certificate, the administrator will not be able to pick up the certificate with this updated passcode. (artf92299)

  The administrator can still pick up the certificate using the old passcode. However, if the old passcode is not available, you will need to delete the administrator and add him again with the new passcode.
- In some cases, the **Continue** button is enabled even if you do not enter a valid email address for a user when enrolling the user from the *Manager* users page. (artf91605)

  You will receive proper validation errors if you click Continue without entering a valid email address. This is a user interface issue; functionality is not impaired.
- In some cases, the email addresses for users do not display in the left or center panes of the *Manage users* page. (artf91868)

  The email address appears in the right pane. This is a user interface issue; functionality is not impaired.
- Your end users may receive duplicate emails after you reset their passcode, resend their enrollment notification, or delete the end user. This occurs intermittently. (artf88360)

  There is no workaround for this issue.

- After entering an email address when enrolling a user, pressing **Enter** on the keyboard cancels the enrollment request rather than continues it. (artf89996)

  To avoid this issue, click the **Continue** button on the screen rather than pressing **Enter** on the keyboard.
- The *Customize certificate options* page loads slowly. (artf86485)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.
- The PKI Manager Welcome screen is not centered if you maximize a Firefox browser window. (artf86485)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.
- When selecting an administrator certificate to log into PKI Manager with a Firefox browser, some images may not appear in the PKI Manager title bar. These images will appear once the administrator certificate is selected. (artf91405)

  There is no workaround for this issue. This is a browser rendering issue; functionality is not impaired.
- If you select **Don't send renewal reminders** on the *Customize certificate notifications* screen, then change the selection to **Send renewal reminders**, the error *Select at least one renewal reminder* will appear briefly. (artf91618)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.
- If you upload a document or .zip file on the Certificate management options page using an Internet Explorer 8 browser, the following issues occur:
  - The upload window will close momentarily, and then re-open. (artf91252)
  - The progress bar and **Select** button do not display correctly. (artf88322)
  - Once the upload has completed, the **Remove** button may not appear for several seconds. (artf90061)

  There is no workaround for these issues. These are user interface issues; functionality is not impaired.
- After selecting search criteria for a report and successfully generating the report, the search criteria you selected does not remain in the left pane. (artf91298)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.
- History report generation using custom dates will fail. (artf91687)

  There is no workaround for this issue.
- History reports may show data that is one or two days older than the selected report criteria. (artf91081)

When you run a History report, verify that the data range is as expected, and modify the report criteria as needed.

- If you bookmark the Customize certificate profile page and try to return to the page later, you will see an *unexpected error* message. This occurs because the session information is no longer available for that page. PKI Manager only allows you to bookmark the main PKI Manager pages. (artf91833)

  There is no workaround for this issue.
- The list of CAs shown on the left pane of the CA Management page is not listed in hierarchical order. Additionally, all CAs are listed, even if they are shared for a particular hierarchy. (artf90082)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.
- Renewal emails will not be sent to your end users if the following conditions are met: (artf92036)
  - The user data is stored in the enterprise Active Directory
  - The certificate profile is not SMIME
  - The certificate profile is not set to send email notifications to other recipients
  - The email ID is not configured in the Subject Domain Name of the certificate

  There is no workaround for this issue.
- Renewal emails will not be sent to your end users if the certificate validity is less than the maximum renewal window. (artf89897)

  There is no workaround for this issue.
- If you attempt to download a Certificate Revocation List (CRL) from the *CA Management* page and the CRL is blank, you are returned to the *CA Management* page and no CRL is downloaded. No message is displayed showing that the CRL you attempted to download is blank. (artf90549)

  There is no workaround for this issue.

Certificate Profile Issues

- Although PKI Manager will allow you to configure the Windows EFS certificate templates to store certificates in PKI Client, EFS certificates are designed to be stored in your end user's native certificate store. As a result, enrollments using Windows EFS certificate templates with PKI Client will fail. (artf90563)

  To avoid this, always configure Windows EFS certificate templates to store certificates in the end user's certificate store (OS\browser certificate management).

- Although PKI Manager allows you to select 1536 and 4096 key sizes when creating certificate profiles, the Aladdin eToken only supports 2048-bit keys. (artf91459)

  If your end users will store their certificates on Aladdin eTokens, you must configure your certificate profile to issue certificates with 2048-bit keys.
- Although PKI Manager allows you to enter non-ASCII characters for the Domain Name attribute of the Subject Distinguished Name in a certificate profile, this field only supports ASCII characters. If you use non-ASCII characters for this field, certificate enrollments will fail. (artf89222, artf90441)

  Always use ASCII characters for the Domain Name attribute of the Subject Distinguished Name in certificate profiles.
- If you have only one certificate profile, it will appear as selected on the *Manage profiles* page. However, the profile details do not appear in the center pane. You will need to click on the profile to view the profile details. (artf91642)

  There is no workaround for this issue. This is a user interface issue; functionality is not impaired.
- If you select **Hide Profile** for a certificate profile, the Certificate management options for the profile will still appear in the center pane, even if you refresh the page. The issue is resolved once you select another profile or navigate to another page. (artf89157)

  There is no workaround for this issue.
- If you customize a certificate profile, enroll a user for a certificate under that profile, and then click **Done**, the *Customize certificate profile* page displays, rather than the Certificate profile management page. (artf91473)

  There is no workaround for this issue.
- If you lose connection to the PKI Manager while editing a certificate profile, and add a Subject Domain Name attribute, the browser you will see an error dialog box. Clicking OK in the error dialog box will cause the browser to hang. (artf91473)

  There is no workaround for this issue.
- If you customize the Subject DN entries for FirstName, LastName, Email Address, Organization, or Unit attributes in your certificate profile, but have previously added additional Subject DN entries for these attributes through the Customize certificate options screen in PKI Manager, you must delete these attributes and add them again. Otherwise, the labels for these attributes will not display correctly in the PKI Certificate Service. (artf90820)

  There is no workaround for this issue.

PKI Certificate Service Issues

- PKI Certificate Service does not support international email addresses (email addresses with non-ASCII domains). Although an end user can enter non-ASCII

characters in the email domain when enrolling for a certificate, the end user will not receive notification of certificate enrollment and the enrollment will fail. (artf88650)

Do not use non-ASCII characters in the email address field for certificate enrollments.

- The Terms of Use field in the certificate enrollment details page for non-English versions of the PKI Certificate Service is in English. (artf90680)

  There is no workaround for this issue.

PKI Client Issues

- If you install PKI Client to a custom installation directory in the C:\ drive on a 64-bit Windows machine, the installer will install some PKI Client files in the default installation directory (C:\Program Files (x86)\Symantec\PKI Client). This does not occur if the default Program Files directory is on another drive. (artf90541)

  There is no workaround to this issue.

- If your end user renews multiple certificates on an Aladdin token simultaneously, the end user will see post-processing error 1 after a successful renewal. (artf91703)

  The end user can safely ignore this issue.

- If your end user manually adds the PKCS11 module into his or her Firefox browser, the end user will always see post-processing error 196 after a successful enrollment. (artf90766)

  The end user can safely ignore this issue; however, Symantec recommends that the PKI Client be installed using the installation scripts. Refer to *Symantec PKI Client V2.0 Administrator's Guide* for instructions on installing PKI Client.

- If an end user chooses his or her own friendly name over the default friendly name when enrolling for a certificate using PKI Client, then later renews the certificate, the renewed certificate reverts to the default friendly name. (artf91007)

  If your security policies allow, the end user can change the friendly name in the browser directly:

  1. Click on **Tools → Internet Options**, and then select the **Content** tab.
  2. Click **Certificates** under *Certificates.* The *Certificates* dialog box appears.
  3. On the *Personal* tab, double-click the certificate. A new *Certificates* dialog box appears.
  4. Click the **Details** tab and click **Edit Properties**.
  5. Add a friendly name and click **OK**.
  6. Close the open dialog boxes.

- If an administrator resets an end user's password in PKI Manager, all of the user's certificates that were previously encrypted with this password will become unusable.

The next time the end user accesses PKI Client to view his or her certificates, the end user will see a javascript error. (artf91794)

The end user will need to delete the virtual token file and re-enroll for his or her tokens. To delete the virtual token file:

- On Windows 7, delete the following folder:

  C:\Users\< user>\AppData\LocalLow\PKI Client\4\vTokens
- On Windows XP, delete the following folder:

  C:\Documents and Settings\< user>\Local Settings\Application Data\PKI Client\4\vTokens

OS\Browser Certificate Management Issues

- An end user enrolling for a certificate using OS\browser certificate management will not be able to set his or her own friendly name if using Internet Explorer 7 or higher in Protected Mode. (artf91474)

  This is a feature of Internet Explorer. If your security policies allow, the end user can change the friendly name in the browser directly:

  1. Click on **Tools → Internet Options**, and then select the **Content** tab.
  2. Click **Certificates** under *Certificates.* The *Certificates* dialog box appears.
  3. On the *Personal* tab, double-click the certificate. A new *Certificates* dialog box appears.
  4. Click the **Details** tab and click **Edit Properties**.
  5. Add a friendly name and click **OK**.
  6. Close the open dialog boxes.
- If an end user running the 64-bit version of Windows 7 attempts to install a certificate from the PKI Certificate Service and does not have that certificate's root CA certificate installed, an error will display stating that the trusted chain could not be built to a trusted authority, or that the trusted root could not be found. The PKI Certificate Service will prompt the end user to download the certificate to his or her workstation. (artf92021)

  The end user will need to contact you to obtain and install the root CA certificate. Once the root CA certificate is installed, the end user should install the downloaded certificate (by double-clicking it and following the onscreen prompts).
- If your end users install the renewal plug-in (symantec-pki-client-plugin-win-x86_64.exe) on Windows 7 running Internet Explorer, they may see a *This program might not have installed correctly* error.

  This is an issue with Windows 7. The plug-in installed correctly, and your end user can safely ignore this error. However, if you wish to avoid this issue, ensure that your end users' version of Windows 7 is updated with all of the latest patches.

Documentation

The following Managed PKI V8.0 documents are available on PKI Manager:

- *Managed PKI V8.0 Release Notes* (this document)
- *PKI Enterprise Gateway Installation and Configuration Guide*
- *PKI Client V2.0 Administrator's Guide*
- *PKI Client V2.0 Writing Post-processing Scripts Guide*