

# Symantec™ Managed PKI 8.14 Release Notes



# Symantec™ Managed PKI 8.14 Release Notes

This document includes the following topics:

- [What's New in 8.14](#)
- [Updated Component Support](#)
- [Updated Platform Support](#)
- [PKI Web Service Updates](#)
- [PKI Manager Updates](#)
- [PKI Enterprise Gateway Updates](#)
- [PKI Client Updates](#)
- [Language Support](#)
- [Documentation](#)
- [Issues Addressed and Known Issues and Workarounds](#)

## What's New in 8.14

These release notes accompany the delivery of the Symantec Managed PKI 8.14 release. Managed PKI is a cloud-hosted service, so enterprises automatically receive the advantage of the latest releases as soon as the service is live. However, you may need to update some components that you have installed at your enterprise location, as described in these release notes.

This release of Managed PKI provides the following updates:

- [Updated Component Support](#)
- [Updated Platform Support](#)
- [PKI Web Service Updates](#)
- [PKI Manager Updates](#)
- [PKI Enterprise Gateway Updates](#)
- [PKI Client Updates](#)

## Updated Component Support

[Table 1-1](#) lists the optional components that Managed PKI 8.14 supports. All components are available from the **Resources** page of PKI Manager.

**Table 1-1** Supported components

Component	Version Supported
PKI Client	v2.14 <sup>a</sup>
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.14
PKI Web Services	v1.14

<sup>a</sup>Managed PKI 8.14 supports previous versions of PKI Client. However, you must be running v2.14 or higher to benefit from the features that are described in these release notes.

## Updated Platform Support

Managed PKI 8.14 supports the following platforms and operating systems (OS).

Symantec cannot test every combination of third-party client, server, operating system, service pack, and so on. 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 that are not listed here.

## PKI Manager

PKI Manager is a web portal hosted in Symantec's data center that allows a Managed PKI administrator to perform account, user, certificate, and key management tasks.

**Table 1-2** PKI Manager operating system and browser support

OS	Browser
Windows 7 Enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer (IE) 8, 9, 11 Firefox 38
Windows 8.1 (32-bit and 64-bit)	IE 11

## PKI Certificate Services

PKI Certificate Services are the webpages that enable users to request, install, renew, and recover their certificates.

**Table 1-3** PKI Certificate Services operating system and browser support

OS	Browser
Windows 7 Enterprise edition SP1 (32-bit and 64-bit)	IE 8 (32-bit), IE 9 (32-bit), IE 10 (32-bit), IE 11 <sup>a</sup> Firefox 38 Chrome 43 <sup>b</sup>
Windows 8.1 (32-bit and 64-bit)	IE 11 <sup>a</sup> Firefox 38 Chrome 43 <sup>b</sup>
Mac OS X v10.9.5	Safari 7.1.6 Firefox 38
Mac OS X v10.10.3	Safari 8.0.6 Firefox 38

<sup>a</sup>The renewal plug-in is not supported in IE 11 if Enhanced Protection Mode (EPM) is enabled. EPM is disabled by default in IE 11.

<sup>b</sup>The Chrome browser is supported for certificate lifecycle operations using PKI Client only.

## PKI Client

PKI Client is middleware for digital signing, authentication, and data protection with desktop-based applications using digital certificates stored on a smart card, security device, or user's computer.

**Table 1-4** PKI Client operating system and browser support

OS	Browser
Windows 7 SP1 (32-bit and 64-bit)	IE 9 (32-bit), IE 10 (32-bit), and IE 11 Firefox 38 Chrome 43
Windows® 8.1 (32-bit and 64-bit)	IE 11 Firefox 38 Chrome 43
Mac OS X v10.9.5 <sup>a</sup>	Safari 7.1.6 Firefox 38 Chrome 43
Mac OS X v10.10.3 <sup>b</sup>	Safari 8.0.6 Firefox 38 Chrome 43

<sup>a</sup>Managed PKI does not support Government Edition CAC (Common Access Cards) and PIV (Personal Identify Verification) smart cards on the Mac OS.

<sup>b</sup>Managed PKI does not support any hardware tokens on Mac OS X10.10.x, including Government Edition CAC and PIV smart cards.

## Additional PKI Client Support

PKI Client also supports the following applications:

- Outlook Client 2007, 2010 (32-bit and 64-bit)
- Thunderbird 24
- Adobe Reader 9 and X (Windows XP) and Adobe X and XI (all other platforms)
- Word 2007, 2010 (32-bit and 64-bit)

The following platforms are not supported on PKI Client from this release:

- Windows XP
- Windows Server 2003
- OSX 10.7, 10.8

You cannot install the latest version of PKI Client on these platforms. The Managed PKI release will not LiveUpdate to the PKI Client v2.13 on these systems.

## PKI Enterprise Gateway

PKI Enterprise Gateway is software installed at the enterprise site that, in conjunction with the enterprise's LDAP directory service, allows an enterprise to programmatically approve certificate requests and publish certificate information back to the enterprise's user store.

For PKI Enterprise Gateway installations:

**Table 1-5** Operating systems and Active Directories supported by PKI Enterprise Gateway

OS	Active Directory
Windows 2008 R2 Server Enterprise/Standard (64-bit)	2008
Windows 2008 R2 SP1 Server Enterprise/Standard (64-bit)	2008
Windows Server 2012 R2 Standard	2012

- Memory: 4 GB RAM and 100 GB hard disk space  
Virtual directory: VMware vSphere 4 and 5 or VMware View 5.4
- Web server: IIS 7.5, NET Framework 4.0 (Windows 2008) or IIS 8, NET Framework 4.0 (Windows 2012), .NET Framework 4.5 (Windows 2012 R2)
- User Stores: Microsoft Active Directory 2008, Novell eDirectory Server v8.8.5, Oracle Directory Server 11gR1 11.1.1.5.0 or OpenLDAP 2.4.35
- Key escrow datastore: The key escrow datastore is used to escrow private keys locally, as part of the key escrow and recovery option. The key escrow datastore supports Microsoft SQL Server 2008 and Oracle 10g RDBMS datastore databases.  
Additionally, Symantec has qualified the key escrow datastore on OpenLDAP 2.4.35, Novell eDirectory 8.8.5, and Oracle Directory Server Enterprise Edition 11gR1. Symantec expects that the key escrow datastore also works on other LDAP-based directories.

For Microsoft Autoenrollment Client OS:

- OS: Windows XP SP3, Windows 2008 Server (64-bit), or Windows 7 Enterprise (32- and 64-bit)

## HSMs Supported

**Table 1-6** Supported HSMs

HSM Type	Platform	Driver Version	Firmware Version
SafeNet Luna SA with HSM Client software version 4.4.1 <sup>a</sup>	<ul style="list-style-type: none"> <li>■ Windows 2008 R2</li> <li>■ Windows Server 2012 R2</li> </ul>	4.4.3-1	4.8.1
SafeNet Luna SA (with remote PED) with HSM Client software version 4.4.1 <sup>a</sup>	<ul style="list-style-type: none"> <li>■ Windows 2008 R2</li> <li>■ Windows Server 2012 R2</li> </ul>	4.4.3-1	4.8.1
SafeNet Luna SA5 with HSM Client software version 5.1.1 <sup>a</sup>	<ul style="list-style-type: none"> <li>■ Windows 2008 R2</li> <li>■ Windows Server 2012 R2</li> </ul>	5.1.1	6.2.1
SafeNet Luna SA5 with HSM Client software version 5.2.1 <sup>a</sup>	<ul style="list-style-type: none"> <li>■ Windows 2008 R2</li> <li>■ Windows Server 2012 R2</li> </ul>	5.2.1	6.10.1
SafeNet Luna SA5 (with remote PED) with HSM Client software version 5.1.1 <sup>a</sup>	<ul style="list-style-type: none"> <li>■ Windows 2008 R2</li> <li>■ Windows Server 2012 R2</li> </ul>	5.1.1	6.2.1
SafeNet Luna SA5 (with remote PED) with HSM Client software version 5.2.1 <sup>a</sup>	<ul style="list-style-type: none"> <li>■ Windows 2008 R2</li> <li>■ Windows Server 2012 R2</li> </ul>	5.2.1	6.10.1
SafeNet Luna PCI (Model 3.0) <sup>a</sup>	Windows 2008 R2	3.0	4.7.1
SafeNet Luna G5	Windows 2008 R2	5.1.1	6.2.3
SafeNet Luna G5	<ul style="list-style-type: none"> <li>■ Windows 2008 R2</li> <li>■ Windows Server 2012 R2</li> </ul>	5.2.1	6.10.1
SafeNet Luna 5.3.1 with HSM Client software version 5.3.1-1 <sup>a</sup>	Windows 2008 R2	5.3.1-1	6.10.2

**Table 1-6** Supported HSMs (*continued*)

HSM Type	Platform	Driver Version	Firmware Version
SafeNet Luna PCI-E	Windows 2008 R2	5.3	6.2.1

<sup>a</sup>You must contact SafeNet to obtain and install the software patch appropriate to your driver version.

For PKI Enterprise Gateway without the key escrow and recovery service, use the key signing variant of the HSM (the default). If using the optional key escrow and recovery service, you must obtain the key generation (key export) variant of the HSM from SafeNet, which includes the key signing variant.

## iOS Devices

Managed PKI supports issuing digital certificates on all devices running iOS 6, 7, and 8.1.

## Android Mobile Devices

Managed PKI supports issuing digital certificates on many Android devices. New Android mobile devices are constantly being qualified. Refer to [https://knowledge.symantec.com/support/mpki-support/index?page=content&id=AR2090&actp=search&viewlocale=en\\_us](https://knowledge.symantec.com/support/mpki-support/index?page=content&id=AR2090&actp=search&viewlocale=en_us) for the most up-to-date list of supported devices.

## PKI Web Service Updates

PKI Web Services has been updated to include the following:

- Webservice includes enhancement to the performance of queries.
- Subject Alternative Name (SAN) Uniform Resource Identifier (URI) Support is enabled for the following:
  - Custom Generic Server and Custom Generic Device Profile certificate profile templates now support *Webservice* as an enrollment method.
  - *CreateorUpdatePasscode* API has been updated to include the URI attribute.
  - You can now select multiple Organization Unit (OU) for SCEP-based enrollments.

*Symantec™ Managed PKI PKI Web Services Developer's Guide* has been updated to reflect these new features and to fix minor issues.



# 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. Refer to PKI Manager and the online help for more information about these new features.

## Performance Enhancements

As Managed PKI generates more certificates, the time that is required to retrieve certificate and user information in PKI Manager increases. Managed PKI includes enhancements to the performance of queries and data searches in the portal. In addition to streamlining the performance of queries, this release includes some UI enhancements to make data retrieval faster. These enhancements are designed to provide guidance when performing intelligent searches so that only pertinent data is returned.

These changes are to the PKI Manager portal only. The behavior of PKI Web Services has not changed.

### General Performance Enhancements

This release includes the following general changes to enhance performance:

- The Manage Users and Manage Certificate pages no longer load user or certificate data automatically. You must perform a search before any data appears.
- For Manage Users, only the first 1000 results are returned. If a search returns more than 1000 results, PKI Manager displays the first page of results and a message requesting that you refine your search criteria.

### Performance Enhancements to the Manage Users Pages

In general, the Manage Users pages are meant to perform user management tasks. This release enhances that behavior by restricting search results to user details and the details about any certificates issued from the User seat pool. Specifically, this release includes the following changes to the User management pages to enhance performance:

- Two new search criteria have been added:
  - **All profiles (this account)** returns details about users assigned to any certificate profile in the account
  - **No Profiles** returns details about users that exist but that are not yet assigned to any certificate profiles

If you have selected the All profiles (this account) search criteria, you must enter a minimum of three characters in search fields. Open-ended searches are not supported if this option is selected.

- Depending upon your search criteria, the **Only users stored in issuing center** check box displays. Beginning with this release, this check box is checked by default. Deselect it to search for certificates stored in your local data center.
- The option to select profiles that issue Device certificates is available only in Seat ID and Date filters.
- The values displayed in the Enrolled in filter is based on the following search selection:
  - When **Name** filter is selected, Enroll in displays all the profiles that belongs to User Seat Pool.
  - When **Email address** filter is selected, Enroll in displays all the profiles except for Device Seat Pool.
  - When **Seat ID** or **Date** is selected, Enroll in displays all the profiles.
  - When **User with pending request** is selected, Enroll in displays all the profiles having Authentication Method as Manual Approval.
- If you view details for a user on the Manage Users page, it displays all the certificates from all the seat pool.

## Performance Enhancements to the Manage Certificate Pages

In general, PKI Manager is designed to manage the certificates issued from the User seat pool. This release enhances that behavior by restricting search results in the Manage Certificate pages to details for the certificates issued from the User seat pool. Specifically, this release includes the following changes to the Manage Certificate pages to enhance performance.

- You must select a certificate profile before performing any search, except for those using the **Search by** criteria. Additionally:
  - Certificate profiles that issue certificates from the device seat pool do not display when searching using the **Certificate profile** criteria.
  - If the **Status** criteria is selected, **Certificate profile** is required.
- The following Search by filters have been changed:
  - The **Validity start/end date** filter is only available if searching with the **Certificate profile** criteria.
  - CAs that issue certificates from the device seat pool do not display when searching using the **Certificate Authority** filter.

- The option to display the certificates imported from other certificate solutions (Non-managed Certificates) is no longer available in searches.

## Certificate Information Report Generation Utility

In this release, the Certificate information report provides options to generate a full or delta report. If you select the full report option, reports are generated at the beginning of the month. If you need a report on a daily basis, you can select the delta report. All these reports will be available for 35 days from the date of generation. You can generate full and delta reports once in a day. However, you can generate an individual report at any time of a day. Contact your Symantec representative for more information about this utility.

## Updates to Third-Party Support Applications

The following third-party support application is updated in this release:

This release of Managed PKI 8.14 uses Java JDK 8 (1.8.0\_40) and this is applicable only to PKI Web Services. You perform this upgrade when you upgrade to Managed PKI 8.14. You may then choose to remove Java JDK 1.7 from your system.

## Delete Older Reports

In this release, you cannot view reports whose expiry is 180 days from the report generation date. These reports will be automatically deleted. Once the report is deleted, you cannot view these reports.

## PKI Enterprise Gateway Updates

The 2.14 version of PKI Enterprise Gateway includes some minor updates. However, there are no new functionality changes since the previous release and you do not need to update it.

*Symantec™ PKI Enterprise Gateway Deployment Guide* and *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide* were updated to fix minor issues.

## PKI Client Updates

PKI Client has been updated to support many of the features that are described in these release notes. Additionally, the following enhancements have been made to PKI Client in this release. To obtain the benefits of these updates, your users must upgrade to PKI Client 2.14. For most users, upgrades occur automatically, unless

you have disabled Live Update. Refer to *Symantec™ PKI Client Administrator's Guide* for instructions on how to disable Live Update.

- This release of PKI Client allows users to access resources behind a proxy that uses Basic Authentication (that is, protected by a user name and password). Refer to *Symantec™ PKI Client Administrator's Guide* for instructions on how to configure PKI Client to recognize an authenticated proxy.
- PKI Client now supports the Chrome browser on the OS X platform. See “[PKI Client](#)” on page 4. for a list of supported operating systems and versions.
- This release of PKI Client enhances how it exports and imports certificates. When a user exports a certificate from PKI Client, the GLCK export file containing the certificate now includes copies of the appropriate post-processing scripts. As a result, PKI Client can correctly process the certificate even if the user is not online when importing the certificate.

Additionally, *Symantec™ PKI Client Administrator's Guide* has been updated to include more information about using PKI Client with the Chrome browser, and about installing certificates on Android.

## Language Support

Managed PKI 8.14 components (PKI Manager, PKI Certificate Services, and PKI Client) support English, French, German, Japanese, Portuguese, Norwegian, Spanish, and simplified Chinese.

These components auto-detect the language settings in the browser and display the correct language. The browser must have the appropriate language packs installed.

## Documentation

The following documents have been revised to incorporate Managed PKI 8.14-specific material:

- *Managed PKI 8.14 Release Notes* (this document)
- *Symantec™ PKI Client Administrator's Guide*
- *Symantec™ PKI Enterprise Gateway Deployment Guide*
- *Symantec™ Managed PKI PKI Web Services Developer's Guide*
- *Symantec™ Managed PKI® Overview*
- *Managed PKI® Transaction Signing API Developer's Guide*
- *Symantec™ Managed PKI SCEP Service Integration Guide*

The following guide was added in the Managed PKI 8.14 release:

- *Symantec™ Managed PKI Integration Guide for Citrix NetScaler VPN*

Unless otherwise noted, all Managed PKI documents are available from the **Resources** page of PKI Manager.

## Issues Addressed and Known Issues and Workarounds

For information about issues fixed in this release and about the workarounds related to known issues in this release, access the Symantec Knowledge Center for Managed PKI at the following URL.

<https://knowledge.symantec.com/support/mpki-support/index.html>

- Enter **Managed PKI 8.14** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI 8.14** as the Knowledge Center Search text to obtain a list of the issued addressed.

# Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved

Symantec, the Symantec Logo, and the Checkmark Logo and are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043

<http://www.symantec.com>