

Managed PKI™ v8.11 Release Notes

Managed PKI™ v8.11 Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated [June 13, 2014](#)

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved

Symantec, the Symantec Logo, and the Checkmark Logo 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.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S.

Government shall be solely in accordance with the terms of this Agreement. 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>

What's New in Managed PKI v8.11	1
Updated Component Support	1
Updated Platform Support	1
PKI Web Service Updates	5
PKI Manager Updates	6
PKI Enterprise Gateway Updates	6
PKI Client Updates	7
Support for Extending the Validity of Test Drive Accounts	7
Unified Authentication PKI Migration Support	7
Documentation	7
Issues Addressed and Known Issues and Workarounds	7

Managed PKI v8.11 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI v8.11 release. Managed PKI v8.11 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 are installed at your enterprise location, as described in these release notes.

What's New in Managed PKI v8.11

This release of Managed PKI provides the following updates:

- [“Updated Component Support”](#) on page 1
- [“Updated Platform Support”](#) on page 1
- [“PKI Web Service Updates”](#) on page 5
- [“PKI Manager Updates”](#) on page 6
- [“PKI Enterprise Gateway Updates”](#) on page 6
- [“PKI Client Updates”](#) on page 7

Updated Component Support

Table 1-1 lists the optional components supported by Managed PKI v8.11. All components are available from the *Resources* page of PKI Manager.

Table 1-1 Supported components

Component	Version Supported
PKI Client	v2.11.0
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.11
PKI Web Services	v1.10

Updated Platform Support

Managed PKI v8.11 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 that are not listed here.

Important! Managed PKI will no longer support Windows Vista after this release.

PKI Manager

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

Table 1-2 PKI Manager operating system/browser support

OS	Browser
Windows 7 Enterprise edition SP1 (32-bit and 64-bit)	IE 9 (32-bit), IE 8 (32-bit) Firefox 24, 25
Windows 8.1 (32-bit and 64-bit)	IE 11

PKI Certificate Services

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

Table 1-3 PKI Certificate Services operating system/browser support

OS	Browser
Windows 7 Enterprise edition SP1 (32-bit and 64-bit)	IE 11 ^a , IE 10 (32-bit), IE 9 (32-bit), IE 8 (32-bit) Firefox 29 Chrome 34
Windows® 8 (32-bit and 64-bit)	IE 10 (32-bit) Firefox 29 Chrome 34
Windows® 8.1 (32-bit and 64-bit)	IE 11 Firefox 29 Chrome 34
Mac OS X v10.8	Safari 6 Firefox 29
Mac OS X v10.9.2	Safari 7.1 Firefox 29

a. 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.

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 end-user computer.

Table 1-4 PKI Client operating system/browser support

OS	Browser
Windows Vista SP 2 (32-bit)	IE 8 (32-bit), IE 9 (32-bit) Firefox 24, 29 Chrome 34
Windows Vista SP 2 (64-bit)	IE 8 (32-bit and 64-bit), IE 9 (32-bit and 64-bit) Firefox 24, 29 Chrome 34

Table 1-4 PKI Client operating system/browser support (Continued)

OS	Browser
Windows 7 SP1 (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 24, 29 Chrome 34
Windows 7 SP1 (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 24, 29 Chrome 34
Windows® 8 (32-bit)	IE 10 (32-bit) Firefox 24, 29 Chrome 34
Windows® 8 (64-bit)	IE 10 (32-bit and 64-bit) Firefox 24, 29 Chrome 34
Windows® 8.1 (32-bit and 64-bit)	IE 11 Firefox 24, 29 Chrome 34
Mac OS X v10.8 ^a	Safari 6.0.1 Firefox 24, 29
Mac OS X v10.9.1 ^a	Safari 7.0.3 Firefox 24, 29

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

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

You cannot install the latest version of PKI Client on these platforms. The Managed PKI 8.10.1 release will not LiveUpdate to the PKI Client v2.11 on these systems.

PKI Enterprise Gateway

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

For PKI Enterprise Gateway installations:

Table 1-5 Operating Systems and Active Directory supported by PKI Enterprise Gateway

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

- Memory: 4 GB RAM and 100 GB hard disk space
- Web Server: IIS 7.5, NET Framework 4.0 (Windows 2008) or IIS 8, NET Framework 4.0 (Windows 2012)
- 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
- Virtual Directory: VMware vSphere 4 and 5 or VMware View 5.4
- Key Escrow Data Store: The key escrow data store is used to escrow private keys locally, as part of the key escrow and recovery option. The key escrow data store supports Microsoft SQL Server 2008 and Oracle 10g RDBMS data store databases.

Additionally, Symantec has qualified the key escrow data store on OpenLDAP 2.4.35, Novell eDirectory 8.8.5, and Oracle Directory Server Enterprise Edition 11gR1. Symantec expects that the key escrow data store also will work 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 ^a	<ul style="list-style-type: none"> Windows 2008 R2 Windows Server 2012 	4.4.3-1	4.8.1
SafeNet Luna SA (with remote PED) with HSM Client software version 4.4.1 ^a	<ul style="list-style-type: none"> Windows 2008 R2 Windows Server 2012 	4.4.3-1	4.8.1
SafeNet Luna SA5 with HSM Client software version 5.1.1 ^a	<ul style="list-style-type: none"> Windows 2008 R2 Windows Server 2012 	5.1.1	6.2.1
SafeNet Luna SA5 with HSM Client software version 5.2.1 ^a	<ul style="list-style-type: none"> Windows 2008 R2 Windows Server 2012 	5.2.1	6.10.1
SafeNet Luna SA5 (with remote PED) with HSM Client software version 5.1.1 ^a	<ul style="list-style-type: none"> Windows 2008 R2 Windows Server 2012 	5.1.1	6.2.1
SafeNet Luna SA5 (with remote PED) with HSM Client software version 5.2.1 ^a	<ul style="list-style-type: none"> Windows 2008 R2 Windows Server 2012 	5.2.1	6.10.1
SafeNet Luna PCI (Model 3.0) ^a	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"> Windows 2008 R2 Windows Server 2012 	5.2.1	6.10.1

a. 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 need to 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 and 7.

Android Mobile Devices

Managed PKI supports issuing digital certificates on many Android devices. New Android mobile devices are constantly being qualified. Refer to the [PKI Client download page](#) on Google Play™ for the most up-to-date list of supported devices.

PKI Web Service Updates

This release of Managed PKI allows administrators to suspend and revoke certificates using Certificate Revocation Lists (CRL). This feature is only supported using Managed PKI Web Services. Although this feature is optional for both public and private CA hierarchies, Symantec recommends that you enable this feature for private CAs. For more information on this feature, including instructions for enabling it, contact your Symantec representative.

Symantec™ Managed PKI PKI Web Services Developer's Guide has been updated to reflect these new features.

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.

Self Service Portal

This release provides a Self Service Portal that allows your end users to manage their own certificate lifecycle operations (such as viewing, enrolling for, renewing, and revoking certificates, and downloading root CAs). Refer to the PKI Manager online help for instructions on enabling the Self Service Portal.

Certificate Service Search

This release allows your end users to search for certificates (using email address, name, or serial number) and can download the public key of these certificates.

Infrastructure Certificate

This release of Managed PKI enhances the management of Registration Authority (RA) certificates and signing authority certificates:

- Administrators now have the ability to search for, revoke, and download RA certificates and signing authority certificates.
- Administrators can add friendly names when enrolling for RA certificates or signing authority certificates.

Support for Non-email Address as Seat IDs

This release allows administrators to assign values other than email addresses to seats IDs for cloud profiles.

Support for Date Ranges in Reports

This release has added a date range filter for the End User Certificate Status and Certificate Information reports. This feature allows you to generate reports based on the selected date range.

Account Renewal Notification

Managed PKI v8.11 will send a renewal notice for Managed PKI accounts that are about to expire. The renewal emails will be sent on 30/60/90/120 days before the account expiration.

PKI Enterprise Gateway Updates

This version of PKI Enterprise Gateway has been updated to support many features described in these release notes. To obtain the benefits of these updates, you must move to the latest version of PKI Enterprise Gateway (available from the Resources page of PKI Manager).

Symantec™ PKI Enterprise Gateway Deployment Guide and *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide* have been reflected to reflect these new features.

PKI Client Updates

PKI Client has been updated for the following new features. To obtain the benefits of these updates, your users must move to PKI Client 2.11. For most users, this will happen automatically, unless you have disabled Live Update. Refer to *Symantec™ PKI Client Administrator's Guide* for instructions on how to disable Live Update.

Symantec™ PKI Client Administrator's Guide has been updated to reflect these new features.

Support for LiveUpdate through Proxy Servers

With this release of Managed PKI, PKI Client has been enhanced to extend LiveUpdate support through proxy servers on Windows environments. Users running PKI Client on Windows can now connect to the Symantec LiveUpdate service through proxy servers. The user must be logged into their computer in order for PKI Client to connect to LiveUpdate through a proxy server.

Support for Extending the Validity of Test Drive Accounts

This release supports the extension of a test drive account beyond 90 days. Contact your Symantec representative for more information about extending the test drive account.

Unified Authentication PKI Migration Support

This release provides a tool to migrate PKI Certificates from your Unified Authentication solution to Managed PKI's Local Key Escrow solution. This tool allows you to export user's certificate to a zip archive file. Contact your Symantec representative for more information about this migration tool.

Documentation

The following documents have been revised to incorporate Managed PKI v8.11-specific material:

- *Managed PKI™ v8.11 Release Notes* (this document)
- *Symantec™ PKI Client Administrator's Guide*
- *Symantec™ PKI Enterprise Gateway Deployment Guide*
- *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide*
- *Symantec™ Managed PKI PKI Web Services Developer's Guide*
- *Symantec™ Managed PKI® Overview*

The following guide is added to Managed PKI 8.11 in this release:

- *Symantec™ Managed PKI Integration Guide for Fiberlink® MaaS360® Mobile Device Management*

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

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

- Enter **Managed PKI v8.11** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI v8.11** as the Knowledge Center Search text to obtain a list of the issues addressed.

