

Managed PKI™ v8.10.1 Release Notes

Managed PKI™ v8.10.1 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 [March 3, 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. VeriSign, VeriSign Trust, and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. 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 v8.10.1	1
Updated Component Support	1
Updated Platform Support	1
PKI Manager Updates	5
PKI Client Updates	6
PKI Certificate Services Updates	6
TC TrustCenter Migration Support	6
Issues Addressed and Known Issues and Workarounds	6

Managed PKI v8.10.1 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI v8.10.1 release. Managed PKI v8.10.1 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 installed at your enterprise location, as described in these release notes.

What's New in Managed PKI v8.10.1

This release of Managed PKI provides the following updates:

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

Updated Component Support

Table 1-1 lists the optional components supported by Managed PKI v8.10.1. All components are available from the *Resources* page of PKI Manager.

Table 1-1 Supported components

Component	Version Supported
PKI Client	v2.10.1 ^a
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.10
PKI Web Services	v1.10

a. Previous versions of PKI Client will work with Managed PKI v8.10.1; however, you must be running v2.10.1 or higher to benefit from the features described in these release notes.

Updated Platform Support

Managed PKI v8.10.1 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.

Important! Managed PKI will no longer support Windows XP and Mac OSX 10.7 after this release. Additionally, Internet Explorer 8 will no longer be supported after this release.

PKI Manager

PKI Manager is a web portal hosted in Symantec’s data centers that allows 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® XP SP3 (32-bit)	IE 8 (32-bit) Firefox 24, 25
Windows 7 Enterprise edition SP1 (32-bit)	IE 9 (32-bit), IE 8 (32-bit) Firefox 24, 25
Windows 7 Enterprise edition SP1 (64-bit)	IE 9 (32-bit and 64-bit), IE 8(32-bit and 64-bit) Firefox 24, 25

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 XP SP3 (32-bit)	IE 8 (32-bit) Firefox 24, 25 Chrome 30 ^a
Windows 7 Enterprise edition SP1 (32-bit)	IE 11 ^b , IE 10 (32-bit), IE 9 (32-bit), IE 8 (32-bit) Firefox 24, 25 Chrome 30 ^a
Windows 7 Enterprise edition SP1 (64-bit)	IE 11 ^b , IE 10 (32-bit and 64-bit), IE 9 (32-bit and 64-bit), IE 8 (32-bit and 64-bit) Firefox 24, 25 Chrome 30 ^a
Windows® 8 (32-bit)	IE 10 (32-bit) Firefox 24, 25 Chrome 30
Windows® 8 (64-bit)	IE 10 (32-bit and 64-bit) Firefox 24, 25 Chrome 30
Windows® 8.1 (32-bit)	IE 11 ^b Firefox 24, 25 Chrome 30
Windows® 8.1 (64-bit)	IE 11 ^b Firefox 24, 25 Chrome 30
Mac OS X v10.7	Safari 5.1 Firefox 24, 25

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

OS	Browser
Mac OS X v10.8	Safari 6 Firefox 24, 25
Mac OS X v10.9.1	Safari 7.1 Firefox 24, 25

a. The Chrome browser is supported for certificate lifecycle operations using PKI Client only.

b. 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 XP SP3 (32-bit)	IE 8 (32-bit) Firefox 24, 25 Chrome 30
Windows Vista SP 2 (32-bit) ^a	IE 9 (32-bit), IE 8 (32-bit) Firefox 24, 25 Chrome 30
Windows Vista SP 2 (64-bit) ^a	IE 9 (32-bit and 64-bit), IE 8(32-bit and 64-bit) Firefox 24, 25 Chrome 30
Windows 7 Enterprise edition SP1 (32-bit)	IE 11, IE 10 (32-bit), IE 9 (32-bit), IE 8 (32-bit) Firefox 24, 25 Chrome 30
Windows 7 Enterprise edition SP1 (64-bit)	IE 11, IE 10 (32-bit and 64-bit), IE 9(32-bit and 64-bit), IE 8 (32-bit and 64-bit) Firefox 24, 25 Chrome 30
Windows® 8 (32-bit)	IE 10 (32-bit) Firefox 24, 25 Chrome 30
Windows® 8 (64-bit)	IE 10 (32-bit and 64-bit) Firefox 24, 25 Chrome 30
Windows® 8.1 (32-bit)	IE 11 Firefox 24, 25 Chrome 30
Windows® 8.1 (64-bit)	IE 11 Firefox 24, 25 Chrome 30

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

OS	Browser
Mac OS X v10.7 ^b	Safari 5.1.5 Firefox 24, 25
Mac OS X v10.8 ^b	Safari 6 Firefox 24, 25
Mac OS X v10.9.1 ^b	Safari 7.1 Firefox 24, 25

a.Windows Vista users who use hardware tokens must install the manufacturer drivers and should not rely on Windows drivers.
b.Managed PKI does not support Government Edition CAC (Common Access Cards) and PIV (Personal Identity 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)

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 Manager Updates

This release of Managed PKI adds two new custom certificate profile templates. Contact your Symantec representative to take advantage of these new custom certificate profile template.

- **Federal Agency Smart Credential Number (FASC-N).** This custom certificate profile template enables an organization to issue FASC-N-compliant user certificates.
- **Wi-Fi Alliance.** This custom certificate profile template enables an organization to issue Wi-Fi Alliance-compliant server certificates.

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 2.10.1. 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.

New Platform Support

PKI Client has been enhanced to support the following new platforms:

- Mac OSX 10.9.1
- Windows 8.1
- IE 11 on Windows 7

Support for LiveUpdate through Proxy Servers

With this release of Managed PKI, PKI Client has been enhanced to extend LiveUpdate support through proxy servers to 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.

PKI Certificate Services Updates

PKI Certificate Services has been enhanced to support the following new platforms:

- Mac OSX 10.9.1
- Windows 8.1
- IE 11 on Windows 7

TC TrustCenter Migration Support

This release provides TC TrustCenter customers with tools for migrating their PKI certificates from the TC Enterprise ID application into Managed PKI:

- A command line tool to migrate recoverable certificates from the TrustCenter Enterprise ID application into Managed PKI.
- A Web Service API that can be used to search your Managed PKI account for certificates migrated from the TrustCenter Enterprise ID application and for certificates originally issued by Managed PKI.

Contact your Symantec representative for more information about these migration tools.

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 v8.10.1** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in Managed PKI v8.10.1** as the Knowledge Center Search text to obtain a list of the issued addressed.