

Symantec™ PKI Client

Administrator's Guide

v2.10.1

Symantec™ PKI Client Administrator's Guide

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 [February 26, 2014](#)

Legal Notice

Copyright © 2011 - 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>

| | | |
|------------|--|----|
| Chapter 1 | Introduction | 1 |
| | About This Guide | 1 |
| Chapter 2 | Understanding PKI Client | 3 |
| | Hardware / Software Requirements | 3 |
| | Hardware Requirements | 3 |
| | Platform Requirements | 3 |
| | Security Device Requirements | 4 |
| | PKI Client Features | 5 |
| | Understanding the PKIClientAgent | 5 |
| Chapter 3 | Installing PKI Client | 7 |
| | Installing PKI Client on Windows | 7 |
| | Special Considerations for Security Devices | 7 |
| | Installing PKI Client as an End-User | 7 |
| | Installing PKI Client as an Administrator | 8 |
| | Uninstalling PKI Client on a PC | 10 |
| | Installing PKI Client on a Mac | 10 |
| | Uninstalling PKI Client on a Mac | 10 |
| Appendix A | Configuring Applications to use PKI Client | 11 |
| | SSL Client Authentication | 11 |
| | Prerequisites | 11 |
| | Setting Up SSL Client Authentication | 11 |
| | Enabling PKI Client-based Autoenrollment for Windows | 12 |
| | Additional Autoenrollment Tasks for Mac OS | 14 |
| | Enabling/Disabling Advanced PKI Client Features | 14 |
| Appendix B | Understanding Registry and Configuration File Settings..... | 19 |
| | Registry Settings for PKI Client Autoenrollment (Windows only) | 19 |
| | Registry Settings for the Symantec CSP for Windows | 20 |
| | Registry Settings for Smart Card Logon for Windows | 20 |
| | General PKI Client Registry Settings | 22 |
| | Symantec PKI Client Live Update Registry Settings | 25 |
| | Registry Settings for the Symantec CSP and KSP Dialog Boxes | 26 |
| | Registry Settings for Threading Library for Windows | 27 |
| | Configuration Settings for Mac | 27 |

Appendix C Troubleshooting PKI Client.....29

 Understanding Logging 29

 PKI Client Logging 29

 Post-processing Logging 29

 Installation Logging 30

 Troubleshooting Common Problems 30

 An end user’s smart card does not trigger the Windows login PIN dialog, or there is an error saying the appropriate drivers for the card are not installed. 30

 An end user's certificate shows up for smart card logon, but logon fails. 30

 Logging shows that an end user's smart card is not recognized. 30

 Even after configuring the policy setting to lock the workstation upon smart card removal, nothing happens when the smart card is removed. 31

 The end user's certificates are not propagated to the user certificate store when the card is inserted 31

 The end user has lost or locked out their PIN. How do they access their smart card? 31

 The smart card on a Mac locks up or cannot find certificates. 31

 Cannot export a certificate from the Windows certificate store or from a browser. ... 31

 PKI Client was installed on a Windows XP machine before the Microsoft Base Smart Card CSP. 31

 Users get an authentication error (401: Unauthorized) when PKI Client attempts to autoenroll them for certificates 32

 Users get an Error Code 193 when installing certificates 32

 Overriding default post-processing scripts 32

Index33

Introduction

Symantec PKI Client is software 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.

PKI Client is included with Managed PKI, and can be used to assist your end users with enrolling for and managing certificates issued by Managed PKI. Refer to the Managed PKI product and documentation for more information about Managed PKI and the Managed PKI certificate lifecycle.

This manual provides instructions for administrators who will install, configure, and troubleshoot Symantec PKI Client for end users.

About This Guide

The chapters of this guide are organized as follows:

- Chapter 2, "Understanding PKI Client" explains PKI Client features, user interface, and end-user hardware and software requirements.
- Chapter 3, "Installing PKI Client" explains how to install and uninstall PKI Client.
- Appendix A, "Configuring Applications to use PKI Client" explains PKI Client features that require administrative set-up, including smart card logon, Windows lock and unlock, and SSL client authentication.
- Appendix B, "Understanding Registry and Configuration File Settings" details the default Windows Registry settings used by PKI Client. This chapter also explains Registry settings that can be modified by administrators.
- Appendix C, "Troubleshooting PKI Client" explains how to log and resolve problems that may occur for end users of PKI Client.

Understanding PKI Client

This chapter explains the features, end-user hardware and software requirements, and describes the client process of Symantec PKI Client v2.10.1.

Review the PKI Client software and the PKI Client FAQs to learn more about PKI Client and how your users will use it. The PKI Client FAQs are available from the **Need Help?** link of PKI Client.

Hardware / Software Requirements

PKI Client is supported on both PC and Mac on the following platforms and software.

Hardware Requirements

- RAM: 512MB RAM
- Free space: 12MB (x86 machines) or 20MB (64-bit machines)

Platform Requirements

PKI Client is supported on all of these

Table 2-1 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 |

Table 2-1 PKI Client operating system/browser support (Continued)

| OS | Browser |
|-------------------------------|--|
| 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 |
| 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.

Security Device Requirements

PKI Client supports the following security devices using third-party Cryptographic Service Providers (CSPs). These CSPs may support other devices; however, Symantec has only qualified these devices with Managed PKI.

Note: Managed PKI provides limited support for Aladdin tokens initialized using third-party certificate management software, as long as the tokens already have certificates stored on them. If you remove these certificates, you will need to re-initialize the token with PKI Client to continue to use the token with Managed PKI.

Table 2-2 Supported security devices

| Security Device | CSP |
|----------------------|--|
| Gemalto SA .NET Dual | Microsoft Base Smart Card Cryptographic Service Provider |
| SafeNet 5100 | eToken Base Cryptographic Service Provider (Requires the SafeNet Authentication Client) |
| SafeNet iKey 4000 | |

Windows Smart Card Login Requirements

PKI Client supports the following for Windows smart card login:

- Standard users: One of the tokens listed in [Table 2-2](#), or an Aladdin eToken authentication device.

- Government users: CAC (Common Access Card) or PIV (Personal Identity Verification) smart card. USB PC/SC-compliant smart card reader appropriate for the smart card, and appropriate smart card reader drivers or support software from the manufacturer. (In many cases Windows update will install any required drivers.)

PKI Client Features

Symantec PKI Client offers the following features for both PC and Mac:

- Secure Email - Users can digitally sign, encrypt, and decrypt email in Outlook with a certificate stored on their computer or smart card. The settings are set so their certificate will only match their Outlook profile.
- Digital Signing of Documents - Using certificates stored on their smart card or computer, users can digitally sign documents.
- Client authentication - Users can securely access your company's Wi-Fi network and VPN, websites, or other services.
- SSL Web Authentication - Users can be authenticated to web sites using a certificate stored on their smart card or computer.
- Certificate Troubleshooting - Users can view advanced information about certificates stored on their computers or smart cards and view logs of operations performed with these certificates.
- 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.
- Importing a Certificate when Offline- Users can successfully import a certificate when offline, run immediate post processing scripts, and delay any remaining post processing scripts until later when back online.
- Administrator Credential Support for 3rd-party CSPs - For CI Plus administrator certificates, PKI Client supports SafeNet eToken, Microsoft Base Smart Card, and Symantec CSPs.

Symantec PKI Client offers the following features for Windows PC only:

- Secure Windows Login - Windows users can log on to their computers using a certificate stored on their smart cards, if that certificate is enabled for Windows Logon. See [“Windows Smart Card Login Requirements”](#) on page 4 for the smart cards supported by this feature.

Understanding the PKIClientAgent

PKI Client runs as a background process on both PC and Mac. It's called PKIClientAgent.exe on a PC and PKIClientAgent on Mac OSX. This process automatically runs when the end user logs in. When an end user inserts a smart card, PKI Client reads the certificates on the device and automatically places these certificates, making them available to the operating system and to third-party services and applications.

Installing PKI Client

This chapter explains how to install and uninstall PKI Client for end users. There are three methods for installing PKI Client. Refer to the appropriate section for the type of installation you will perform:

- [“Installing PKI Client on Windows”](#) on page 7
- [“Quietly Installing PKI Client”](#) on page 8
- [“Installing PKI Client as an Administrator”](#) on page 8
- [“Installing PKI Client as an Administrator”](#) on page 8

Installing PKI Client on Windows

You can install PKI Client on a Windows machine in one of two ways:

[“Installing PKI Client as an End-User”](#) on page 7

[“Installing PKI Client as an Administrator”](#) on page 8

Special Considerations for Security Devices

If you will be using PKI Client with security devices, refer to the following special considerations before installing PKI Client:

- For SafeNet security devices, you must also install the SafeNet Authentication Client on the user's machine. Refer to the documentation provided with your SafeNet tokens for procedures.
- The Microsoft Base Smart Card Cryptographic Service Provider is not included with Windows XP. If your users will use this CSP on a Windows XP machine, you must install this CSP before installing PKI Client. Obtain this CSP from Microsoft (KB909520).

If PKI Client has already been installed on the Windows XP machine, refer to [“PKI Client was installed on a Windows XP machine before the Microsoft Base Smart Card CSP.”](#) on page 31.

Installing PKI Client as an End-User

- 1 On a Windows machine, extract the PKI Client installer to a location on your computer (C:\WINDOWS\Temp\Symantec-PKI-Client-2.10.1, for example).
- 2 Double-click the installer (Symantec-PKI-Client-2.10.1.exe).
- 3 In the installer, click **Next**.



Figure 3-1 PKI Client Installer

- 4 Click the **I accept the terms in the License Agreement** check box and click **Next**.
- 5 Click **Next** to confirm the destination folder.
- 6 Click **Install**.
- 7 Click **Finish**.

Quietly Installing PKI Client

You can install PKI Client quietly using the command line. Using this command you can install PKI Client without clicking through the installer. This method of installation is also useful for installing PKI Client remotely on end-user workstations or by group policy for domain users.

- 1 Open a Command Prompt (**Start** → **Run** → **Cmd**).
- 2 Run the installer command with the /q option. For example:

```
Symantec-PKI-Client-2.10.1.exe /qn
```

This will install PKI Client to the C:\Program Files\Symantec\PKI Client\ directory.

Installing PKI Client as an Administrator

Administrators can install PKI Client on users' machines using a Group Policy Object (GPO).

Extracting the MSI Files

Only MSI-specific installers will work with GPO installation. Multilingual installers cannot be installed using a GPO. To install PKI Client using a GPO push, you must extract the MSI-specific installer files from the PKI Client installer:

- 1 Open a Command Prompt (**Start** → **Run** → **Cmd**).
- 2 Run the installer command with the /ExtractCAB option. For example:

```
Symantec-PKI-Client-2.10.1.exe /ExtractCAB
```

This will extract the installation files to a `SupportFiles` directory in the same directory as the installer.

Setting up Group Policy Object (GPO) Installations on Windows

Set up a share, either on the server or somewhere that domain users or the domain machines can access. Add to the share the files you want to install.

Task 1. Create the GPO

- 1 Launch Group Policy Management:
 - For Windows Server 2008, go to **Administrative Tools** → **Group Policy Management**.
 - For Windows Server 2012, click Start and search for **Group Policy Management**.
- 2 Expand the options until you find your domain, and then expand below that.
- 3 Right-click **Group Policy Objects** and select **New**.
- 4 Enter a name, and do not select a **Source Starter GPO**.
- 5 Right-click the new GPO and select **Edit**.

Task 2. Assign the Package

To assign a package (this will install on all computers who are joined to the domain, once the group policy is updated on that machine):

- 1 Expand **Computer Configuration**, then **Policies**, then **Software Settings**, then select **Software Installation**.
- 2 Right-click and select **New** → **Package**.
- 3 Navigate to the share you created (or enter the full path in the File name space, making sure that the full path is actually what is selected, not a relative path). For example: \\IP/Servername\{Share}\{filename}
- 4 Select **Advanced** as the option for deploying the software on the next prompt.
- 5 In the Modifications tab, click **Add**, and navigate to the correct .mst file for the target system's locale and architecture (extracted as described in [“Extracting the MSI Files”](#) on page 8). Click **OK**.

The package should show up in the list of Software Installations.

Task 3. Link the GPO to your Domain

- 1 Back on the Group Policy Management screen, drag your new GPO onto your Domain.
- 2 At the prompt, select **Ok**.
- 3 Verify that your GPO is now right under the domain name, if you right-click that icon, you should see a checked Link option.

Importing a Certificate when Offline

You can enable your end users to successfully import a certificate when offline, run immediate post processing scripts, and delay any remaining post processing scripts until later when back online. In order to do this, push the roots of any certificates you are using so that end users do not receive any prompts. Otherwise, the end user may receive prompts, unaware of their origin.

Viewing Installation Logs

Complete the following procedures to view logs written by the installation:

- 1 Open a Command Prompt (**Start** → **Run** → **Cmd**).
- 2 Enter the following command:

```
Symantec-PKI-Client-2.10.1.exe /Log /Logfile bootstrap.log /ComponentArgs x86:"/l*vx  
msi_x32.log" /ComponentArgs x64:"/l*vx msi_x64.log"
```

Where:

- <installer.exe> is the location from where the installation script was run
- <x64/x86> is the version of the installer that was run. Use x64 for the 32-bit version. Use x86 for the 64-bit version.
- <dest_dir> is where the installation logs should be written.

Uninstalling PKI Client on a PC

To uninstall PKI Client from the Windows' Control Panel:

- 1 Open the Control Panel (**Start** → **Control Panel**).
- 2 In the Control Panel, click **Add or Remove Programs**.
- 3 Select **Symantec PKI Client** in the list of installed programs.
- 4 Click **Remove**.
- 5 Click **Yes** when prompted to confirm the removal of PKI Client.

Alternatively, you can uninstall PKI Client by re-running the PKI Client installer and selecting to uninstall the application.

Installing PKI Client on a Mac

You can install PKI Client quietly on a Mac using the Terminal. Using the Terminal, you install PKI Client without clicking through an installer. This method of installation is also useful for installing PKI Client remotely on end-user workstations or by group policy for domain users.

- 1 Open the Terminal (**Finder** → **Applications** → **Utilities** → **Terminal**).
- 2 Enter:

```
installer -pkg Symantec-PKI-Client-x64.2.10.1.pkg -target /
```

This will install PKI Client.

Configuration settings on Mac OSX are in the OSX flat file. On Mac PSX JSON formatting is used to encode all of the data.

Viewing Installation Logs

The OSX operating systems automatically writes all installation logs to /var/logs/install.log.

If you need to view logs for a specific PKI Client installation, you can manually run the installation by double-clicking the Symantec-PKI-Client-x64.2.10.1.pkg and performing the installation using the Mac Installer.

You will be able to view the installation logs by clicking **Window** → **Installer Log** from the Installer's menu bar during installation.

Uninstalling PKI Client on a Mac

To uninstall PKI Client from a Mac:

- 3 Go to (**Finder** → **Applications** → **Symantec Authentication** → **PKI Client Uninstaller**).
- 4 Follow the prompts to uninstall PKI Client.

Configuring Applications to use PKI Client

Some PKI Client features require additional set-up to work with your applications. You can either configure individual end-user workstations or configure group policies for domain users.

You can also write BAT (batch) executable files on a PC or SH files on a Mac to notify your applications of the certificate status and locations, and that the certificates are available for use. Refer to *Symantec™ PKI Client Writing Post-processing Scripts Guide* for more information.

SSL Client Authentication

You can verify the identity of end users and authenticate them to your organization's web site(s) using their smart card.

Prerequisites

In addition to requirements outlined in “[Hardware / Software Requirements](#)” on page 3, there are additional requirements for SSL Client Authentication:

- End users must be members of your organization's domain.
- End-user smart card certificates must be issued from or registered with Active Directory for your domain.
- End users must trust your web server's certificate, or the Certificate Authority that issued the web server's certificate, and have this certificate installed on their computer.

Setting Up SSL Client Authentication

You can require end users to authenticate with the certificate stored on their smart card.

Note: You can enable this feature using any web server that supports SSL Client Authentication.

- 1 On Windows Server, open **Internet Information Services (IIS) (Start → Run → inetmgr)**.
- 2 Right-click the web site in the left panel and select **Properties**.
- 3 Click the **Directory Security** tab.

- 4 In the Secure Communications Link section, click **Edit**.

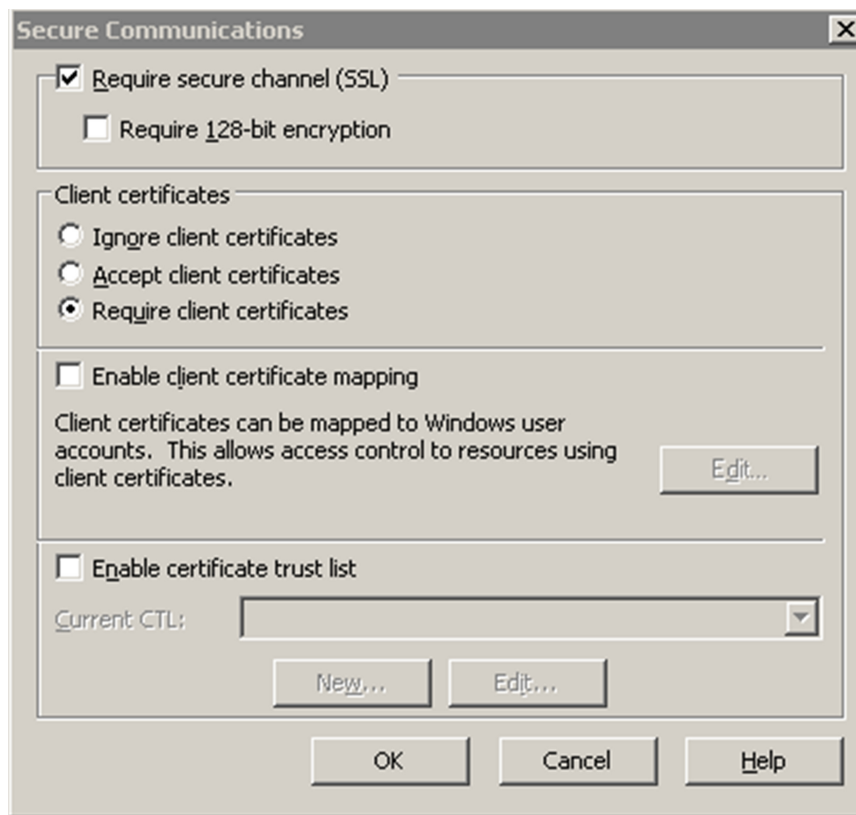


Figure A-1 Secure communications settings

- a Check the **Require secure channel (SSL)** check box.
 - b Select **Require client certificates**.
 - c Click **OK**.
- 5 In the Secure Communications section, click **Server Certificate**.
 - 6 Either import a server certificate or generate a new one if the issuing certificate authority is accessible. This certificate needs to be trusted by the end-user workstations.
 - 7 Click **OK**.

Enabling PKI Client-based Autoenrollment for Windows

You can configure Managed PKI to allow PKI Client to enroll users for certificates automatically. PKI Client will automatically enroll for any certificate profile (or profiles) configured for an end user, based on the user data contained in Active Directory. PKI Client autoenrollment is tightly integrated with PKI Enterprise Gateway, making autoenrollment nearly transparent to end users and administrators alike:

- Depending on how the certificate profile is configured, the enrollments will occur without end-user notification or intervention.
- Administrators will not need to provide an enrollment email, enrollment code, or enrollment link for certificate enrollment.

PKI Client also automates renewals, meaning that the entire certificate lifecycle experience is completely automatic for most users.

Autoenrollment Steps for Windows

Task 1. Install PKI Enterprise Gateway

Install PKI Enterprise Gateway as described in *Symantec™ PKI Enterprise Gateway Deployment Guide*, with the following specific configuration settings:

- **Active Directory** must be selected as the user store.
- End-user machines must be joined to the domain configured in PKI Enterprise Gateway.

Task 2. Configure your Managed PKI Certificate Profile

Create a certificate profile for PKI Client-based autoenrollment, with the following specific settings:

- Select **PKI Client** as the Enrollment method.
- Select **Active Directory** as the Authentication method, set the appropriate authorized user list and PKI Enterprise Gateway settings, and select the **PKI Client should automatically enroll for Windows users** checkbox.

Refer to PKI Manager and its associated help for details on creating certificate profiles.

Task 3. Provide the Managed PKI Root CA Certificate to the Domain (if Required)

If the Managed PKI root CA certificates are not pre-installed in the domain, download them from the *Manage CA* page of PKI Manager and use Microsoft Management Console (MMC) to push them out to the domain. Otherwise, the end user will be prompted to trust the root CA the first time PKI Client attempts to autoenroll for a certificate.

Refer to the Microsoft® documentation for procedures on installing and trusting a CA within a forest.

Task 4. Provide PKI Client to End Users

PKI Client-based autoenrollment requires PKI Client to be installed in your end user machines; end users will not be prompted to install it during autoenrollment. If PKI Client is not already installed on your end users' machines, provide it to them as described in Chapter 3 "Installing PKI Client."

Task 5. Provide the Group Policy Settings to End Users

- 1 On a machine with PKI Client installed, use a Group Policy Object (GPO) to push a computer policy to your end users. Enable **Managed PKI Auto-Enrollment Settings** and configure the policy settings with the following specific values (these values must match the settings you configured for your PKI Enterprise Gateway):
 - **Gateway URL** is the URL of your PKI Enterprise Gateway.
 - **RA Service Port** is the port on which the RA service listens.
 - **Authentication Service Port** is the port on which the Authentication service listens.
 - **RA Agent Port** is the port on which the RA Agent listens.
- 2 Push the group policy settings to your end user machines to initiate the automatic enrollment.

If an end user receives a certificate on one machine and then uses the same user account to log onto another machine in the same domain, the end user will receive an error stating that the certificate has already been enrolled, unless one of the following apply:

 - The certificate profile has been configured to allow multiple certificates. In this case, the end user will receive the certificate as expected.
 - The certificate is an S/MIME certificate. In this case, the end user will receive a copy of the existing, valid S/MIME certificate.

Refer to ["Enabling/Disabling Advanced PKI Client Features"](#) on page 14 for additional information on defining and pushing group policy settings to PKI Client on your end-user machines.

Additional Autoenrollment Tasks for Mac OS

Task 1. Prerequisites

For Mac OS, clients must be joined to a pre-existing / pre-configured OSX Server (Symantec has tested this on the OSX Mountain Lion Server). Profile Manager must already be set up (with profiles being pushed automatically). The clients must be joined to the Active Directory domain. Kerberos single-sign-on must already be on the domain and functioning properly.

Task 2. Set Mac OS X Server MobileConfig Profile

The AutoEnroll gatewayURL needs to be set in a Mac OS X Server mobileconfig profile.

- 1 Create a new profile for the appropriate user/device/group on the Mac OS X Server's Profile Manager (or edit an existing one).
- 2 PKI Client-based autoenrollment for Mac OS requires that you add a Custom Settings payload.
- 3 Set the Preference domain to com.symantec.pkiclient.autoenroll.
- 4 For Mac OS, add a String setting named gatewayURL with the value set exactly as it is set in the GPO on Windows.
- 5 Save the profile and let it be pushed to the appropriate user/device.

Note: Check the Active Tasks/Completed Tasks to see when the profile is pushed. This may take some time. Furthermore, after a profile has been successfully pushed, it may not take effect until the user logs off and restarts.

Enabling/Disabling Advanced PKI Client Features

This section describes how to enable advanced PKI Client features through a GPO. See [Table A-1](#) for more information about these features, as well as the feature-specific GPO settings you will need to configure.

Note: To enable these features for an individual end user, modify the appropriate registry entries on the user's machine. Refer to Appendix A, "Understanding Registry and Configuration File Settings," for the specific registry settings.

- 1 Launch Group Policy Management:
 - For Windows Server 2008, go to **Administrative Tools** → **Group Policy Management**.
 - For Windows Server 2012, click Start and search for **Group Policy Management**.
- 2 Select the feature to enable:
 - a Expand your domain and right-click **Group Policy Objects**.
 - b Select **New** and name the new group policy.
 - c Right-click the new group Policy and click **Edit**.
 - d Expand **Computer Configuration**, then **Policies**, then **Administrative Templates**, and then select **Symantec PKI Client**.
 - e Double-click the setting to be enabled, and then select **Enabled** in the top of the page to enable the feature and see the available options to set.

3 Set the advanced feature required. Refer to [Table A-1](#) for specific GPO settings for each feature.

Table A-1 GPO settings

| Advanced Feature | Description | Setting |
|--|---|---|
| Configure LiveUpdate server host | Controls whether LiveUpdate is enabled or disabled, and sets the host to use for LiveUpdate connections. LiveUpdate is enabled by default. | <ul style="list-style-type: none"> Double-click LiveUpdate Service Configuration. Enter a value (in days) to elapse between update checks in the Scanning Interval (in days) field. The default is 1 day. Enter the host to use for LiveUpdate connections in the LiveUpdate Host field. If not configured, liveupdate.symantec.com is used by default. Click OK. |
| Configure PKI Client Agent Settings | Controls global PKI Client settings. <ul style="list-style-type: none"> Agent Scan Base Interval (seconds) defines how frequently the client will scan for updates to profiles for which to perform enrollments, renewals, or post-processing. The default is 14400 seconds (4 hours). Agent Scan Maximum Random Offset (seconds) is a random variable added to the base interval. Use this variable to stagger operations to avoid too many simultaneous requests. The default is 10800 seconds (3 hours). | <ul style="list-style-type: none"> Double-click PKI Client Agent Settings. Enter values for the following: Agent Scan Base Interval (seconds) Agent Scan Maximum Random Offset (seconds) Click OK. |
| Enable/Disable Outlook Profile Configuration | Controls whether certificates enumerated by the Symantec PKI Client are automatically registered with Outlook. This is disabled by default. | <ul style="list-style-type: none"> Double-click Control Outlook Profile Configuration. Select Enabled. Click Apply. |
| Control Outlook Profile Configuration | Controls whether Outlook sends the signing certificate with the email. If this setting is disabled, Outlook will send the signing certificate with the email. This is disabled by default. | <ul style="list-style-type: none"> Double-click Control Outlook Profile Configuration. Check Enable Outlook AutoConfiguration. Click OK. |
| Name Outlook Profile | Sets a friendly name for the Outlook profile. This is set to Symantec Corporation - Config by default. | <ul style="list-style-type: none"> Double-click Control Outlook Profile Configuration. Enter a friendly name for the Outlook profile in the Default Security Settings Name field. Click OK. |
| Match Email Address | Increases security by ensuring that the profile of a user matches the email in Active Directory. This is unchecked by default. | <ul style="list-style-type: none"> Double-click Control Outlook Profile Configuration. Check the box in front of the Match Email Address field. Click OK. |

Table A-1 GPO settings (Continued)

| Advanced Feature | Description | Setting |
|--|---|---|
| Set Encryption Algorithm | Allows you to set the algorithm Outlook will use to encrypt data and email. This is set to 3DES by default. | <ul style="list-style-type: none"> Double-click Control Outlook Profile Configuration. Select an algorithm for Outlook to use in the Default Encryption Algorithm field. Click OK. |
| Set Signing Algorithm | Allows you to set the algorithm Outlook will use to sign outgoing email. This is set to SHA1 by default. | <ul style="list-style-type: none"> Double-click Control Outlook Profile Configuration. Select an algorithm for Outlook to use in the Default Hash Algorithm field. Click OK. |
| Configure behavior when a device is removed | Controls whether smart card certificates are removed from the user's certificate store upon smart card removal. | <ul style="list-style-type: none"> Double-click Configure behavior on removal of device. Click OK. |
| Enable/Disable support for the software certificate store, such as virtual tokens (Control Software Certificate Store) | Controls whether the software certificate store (virtual tokens) are enabled and visible to users. This is enabled by default. | <ul style="list-style-type: none"> Double-click Control Software Certificate Support. Click OK. |
| Enable/Disable Diagnostics Mode Symantec connectivity check | Controls whether PKI Client will check for connectivity to the Symantec service when running in Diagnostics Mode. This is enabled by default. If disabled, PKI Client will not check for connectivity to Symantec services when running in Diagnostics Mode. Disable this setting if PKI Client will not have access to the Symantec service. | <ul style="list-style-type: none"> Double-click Configure Diagnostics Mode Symantec connectivity check. Click OK. |
| Enable/Disable Section 508 Compliance | Controls whether to enable 508 compliance. This disables all graphical elements except the Windows default coloring. | <ul style="list-style-type: none"> Double-click Configure Dialog. Click Enable Section 508 Compliance. Click OK. |
| Enable PIN Reset links in dialog boxes | Controls whether the Forgot Your PIN and Reset PIN links appear in dialog boxes. | <ul style="list-style-type: none"> Double-click Configure Dialog. Click Enable PIN Reset. Click OK. |
| Configure Authentication Credential Lifetime | Set how long login credentials based on a successful authentication will remain valid. Any authentication operation after the credential expires will require re-authentication. | <ul style="list-style-type: none"> Double-click Configure additional Console UI operations. Enter a value (in seconds) for how long the login credentials remain valid in the Authentication Credential Lifetime field. Click OK. |

Table A-1 GPO settings (Continued)

| Advanced Feature | Description | Setting |
|---|--|---|
| Managed PKI Auto-Enrollment Settings | <p>These settings are the same as what you enter into PKI Manager when setting up the PKI Enterprise Gateway for the first time (aside from the Agent Scan options).</p> <p>These settings can be viewed in the setup log file (usually C:\Users\Public\pgwSetup_log_*.txt).</p> | <ul style="list-style-type: none"> Double-click Managed PKI Auto-Enrollment Settings. Selecting Re-enroll deleted certificates determines if automatically-enrolled certificates deleted on the console are re-enrolled. Enter values for the following: Gateway URL RA Service Port Authentication Service Port RA Agent Port Click OK. |
| Microsoft Base Smart Card Crypto Support | <p>Enables PKI Client to import keys to security devices that support the Microsoft Base Smart Card Cryptographic Service Provider (CSP). Otherwise, keys cannot be imported to these security devices.</p> <p>Note: Wow6432Node entries affect 32-bit usage on 64-bit machines. The default determines whether the machine is natively 32-bit or 64-bit.</p> | <ul style="list-style-type: none"> Double-click Managed PKI Auto-Enrollment Settings. Select the following (you should either select all or select none): Enable Signature key import Enable Signature key import (Wow6432Node) Enable Exchange key import Enable Exchange key import (Wow6432Node) Click OK. |
| Control Key Usage Policy | <p>Enables PKI Client to manages policies related to key usage for certificates with a non-repudiation key usage extension.</p> <p>If selected, PKI Client will require a PIN for each operation that requires a key, and which is performed by a certificate with the non-repudiation key usage extension. If not selected, PKI Client will use the standard PIN authentication policy. This is the default.</p> | <ul style="list-style-type: none"> Double-click Managed PKI Auto-Enrollment Settings. Select Always authenticate non-repudiation certificates. Click OK. |
| Advanced PIV/CAC Smart Card Features | | |
| Enable Windows Logon/Unlock Computer | <p>Allow users to log into Windows or unlock their Windows-based computer using the certificate installed in their smart card.</p> <p>Requires that the smart card contains a certificate that is enabled for Windows Logon.</p> <p>Users must register their smart cards in PKI Client (by clicking Smart Card Settings, and clicking Register under Register for Windows logon). Users must have administrator rights to their computer to register smart cards.</p> | <ul style="list-style-type: none"> Double-click Configure additional Console UI operations. Select Activate Register-for-Logon Operation. Click OK. |

Table A-1 GPO settings (Continued)

| Advanced Feature | Description | Setting |
|---------------------------|--|---|
| Enable Device Unblock | <p>Enable users to unblock a PIV smart card that has been blocked due to too many failed PIN attempts by requesting a Personal Unblock Key (PUK) from their PKI Client administrator, and entering it into PKI Client.</p> <p>Your PKI Client administrators will need to provide the PUK using your existing smart card process and software.</p> | <ul style="list-style-type: none">■ Double-click Configure additional Console UI operations.■ Select Activate Device Unblock Operation.■ Click OK. |
| Enable PIV/CAC Preference | <p>Allow users to switch their smart cards between PIV and CAC modes by clicking Smart Card Settings, and then selecting PIV or CAC under Smart card mode.</p> | <ul style="list-style-type: none">■ Double-click Configure additional Console UI operations.■ Select Configure PIV/CAC Hybrid handling.■ Select which interface is the default (PIV or CAC).■ Click OK. |

Understanding Registry and Configuration File Settings

This chapter explains the Registry (Windows) and configuration file (Mac) settings that are created when PKI Client is first installed, what each setting does, and which settings can be modified by administrators of PKI Client.

If an end user is connected to a domain, PKI Client will not recognize any changes to the group policy that are made locally. 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.

Unless specified otherwise, the default values apply to all registry locations.

Registry Settings for PKI Client Autoenrollment (Windows only)

The Symantec PKI Client Autoenrollment settings are found in Table B-2. The registry location is:

HKCU\Software\Policies\Symantec\PKI Client\4\AutoEnroll

Table B-1 Registry Settings for PKI Client Autoenrollment

| Registry Entry | Type | Default Value | Description |
|-------------------|-----------|---------------------|--|
| authServicePort | REG_DWORD | 9101 | Authentication Service port for PKI Enterprise Gateway |
| raAgentPort | REG_DWORD | 9102 | RA Agent port for PKI Enterprise Gateway |
| raServicePort | REG_DWORD | 9100 | RA Service port for PKI Enterprise Gateway |
| gatewayURL | REG_SZ | http://computername | Computer name for PKI Enterprise Gateway |
| scanBaseInterval | REG_DWORD | 4*60*60 seconds | Base time interval for which autoenrollment scans will occur, allowing companies to randomize client access to the Internet to avoid flooding the network at the same time |
| scanMaxRandOffset | REG_DWORD | 3*60*60 seconds | Variance from the base time interval for which autoenrollment scans will occur |
| reEnrollDeleted | REG_DWORD | 1 | Automatically re-enroll autoenroll certificates deleted on the console |

Registry Settings for the Symantec CSP for Windows

The Symantec Cryptographic Service Provider (CSP) (for Windows only) is used by applications like Outlook, Windows Logon, and Internet Explorer. The following table lists the Symantec CSP Registry locations:

Table B-2 Symantec CSP registry locations

| Environment | Registry Location |
|-----------------------------------|--|
| 32-bit machine | HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Symantec PKI Client CSP |
| 64-bit registry on 64-bit machine | HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Symantec PKI Client CSP |
| 32-bit registry on 64-bit machine | HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Symantec PKI Client CSP |

Table B-3 Symantec CSP registry entries

| Registry Entry | Type | Default Value | Description |
|----------------|--------|--|--|
| Image Path | STRING | 32-bit: C:\Program Files\Symantec\PKI Client\TBCSP.dll | The CSP dll to be used for the Symantec PKI Client CSP. Caution: Do not modify this entry. |
| PKCS11Module | STRING | 32-bit: C:\Program Files\Symantec\PKI Client\CSPPKCS11.dll | The CSP dll to be used for the Symantec PKI Client CSP. Caution: Do not modify this entry. |
| SigInFile | DWORD | 32-bit: 0 | A true or false value indicating whether or not the signature is contained within an associated file. Caution: Do not modify this entry. |
| Type | DWORD | 32-bit: 1 | The CSP Provider Type (PROV_RSA_FULL) Caution: Do not modify this entry. |

Registry Settings for Smart Card Logon for Windows

Windows keeps a database of smart-card-to-CSP associations called the Calais database. This database is populated with the appropriate entries for the supported smart cards. The following tables list the smart card registry locations and entries:

Note: PKI Client does not add registry entries for security devices supported by third-party CSPs.

Table B-4 Smart card logon registry locations

| Environment | Registry Location |
|-----------------------------------|---|
| 32-bit machine | HKLM\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\<Location> |
| 64-bit registry on 64-bit machine | HKLM\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\<Location> |
| 32-bit registry on 64-bit machine | HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards\<Location> |

Table B-5 Smart card logon registry entries

| Registry Entry | Type | Description | Default Value |
|----------------|--------|----------------------------------|---|
| <Location> | KEY | Registry location suffix for: | |
| | | Aladdin eToken | Aladdin |
| | | CAC OCS 5.2 | CAC OCS 5.2 |
| | | CAC OCS 5.5 | CAC OCS 5.5 |
| | | PIV 2 OCS v1.08 | PIV 2 OCS v1.08 |
| | | PIV 3 Gemalto TOP DL v2 | PIV 3 Gemalto TOP DL v2 |
| | | PIV 3 OCS Cold | PIV 3 OCS Cold |
| | | PIV 3 OCS Warm | PIV 3 OCS Warm |
| | | PIV-CAC Gemalto GX4 72K | PIV-CAC Gemalto GX4 72K |
| | | PIV-CACNG Gemalto GX4 144K | PIV-CACNG Gemalto GX4 144K |
| | | PIV-CACNG OCS 5.5 | PIV-CACNG OCS 5.5 |
| ATR | BINARY | The unique token identifier for: | |
| | | Aladdin eToken | 3b,d5,18,00,81,31,3a,7d,80,73,c8,21,10,30 |
| | | CAC OCS 5.2 | 3b,95,95,40,ff,ae,01,03,00,00 |
| | | CAC OCS 5.5 | 3b,db,96,00,80,1f,03,00,31,c0,64,77,e3,03,00,82,90,00,c1 |
| | | PIV 2 OCS v1.08 | 3b,db,96,00,81,b1,fe,45,1f,03,80,f9,a0,00,00,03,08,00,00,10,00,18 |
| | | PIV 3 Gemalto TOP DL v2 | 3b,7d,96,00,00,80,31,80,65,b0,83,11,11,e5,83,00,90,00 |
| | | PIV 3 OCS Cold | 3b,df,96,00,81,b1,fe,45,1f,83,80,73,cc,c1,cb,f9,a0,00,00,03,08,00,00,10,00,29 |
| | | PIV 3 OCS Warm | 3b,df,95,00,81,b1,fe,45,1f,83,80,73,cc,c1,cb,f9,a0,00,00,03,08,00,00,10,00,2a |
| | | PIV-CAC Gemalto GX4 72K | 3b,7d,96,00,00,80,31,80,65,b0,83,11,13,ac,83,00,90,00 |
| | | PIV-CACNG Gemalto GX4 144K | 3b,7d,96,00,00,80,31,80,65,b0,83,11,17,d6,83,00,90,00 |
| | | PIV-CACNG OCS 5.5 | 3b,db,96,00,80,1f,03,00,31,c0,64,b0,f3,10,00,07,90,00,80 |

Table B-5 Smart card logon registry entries (Continued)

| Registry Entry | Type | Description | Default Value |
|-----------------|--------|--|---|
| ATRMask | BINARY | Mask applied to the ATR during identification for: | |
| | | Aladdin eToken | ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff |
| | | CAC OCS 5.2 | ff,ff,ff,ff,ff,ff,ff,ff,ff |
| | | CAC OCS 5.5 | ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff |
| | | PIV 2 OCS v1.08 | ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff |
| | | PIV 3 Gemalto TOP DL v2 | ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff |
| | | PIV 3 OCS Cold | ff,ff |
| | | PIV 3 OCS Warm | ff,ff |
| | | PIV-CAC Gemalto GX4 72K | ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff |
| | | PIV-CACNG Gemalto GX4 144K | ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff |
| | | PIV-CACNG OCS 5.5 | ff,ff |
| Crypto Provider | STRING | The CSP that smart cards are associated with. | Symantec PKI Client CSP |

General PKI Client Registry Settings

The Symantec PKI Client configuration settings are located in the HKEY Local Machine (HKLM) and, unless indicated otherwise, in HKEY Current User (HKCU) keys:

Table B-6 Symantec® PKI Client registry locations

| Environment | Registry Location |
|-----------------------------------|---|
| 32-bit machine | <ul style="list-style-type: none"> HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\PKI Client\4 HKEY_CURRENT_USER\SOFTWARE\Symantec\PKI Client\4 |
| 64-bit registry on 64-bit machine | <ul style="list-style-type: none"> HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\PKI Client\4 HKEY_CURRENT_USER\SOFTWARE\Symantec\PKI Client\4 |
| 32-bit registry on 64-bit machine | HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\PKI Client\4 |

Table B-7 Symantec® PKI Client Registry Settings

| Registry Entry | Type | Default Value | Description |
|----------------|--------|--|--|
| CoreDirectory | STRING | 32-bit: C:\Program Files\Symantec\PKI Client | The location of the Symantec PKI Client executable and application files. Caution: Do not modify this entry. |
| | | 32-bit (on 64-bit): C:\Program Files (x86)\Symantec\PKI Client | |
| | | 64-bit: C:\Program Files\Symantec\PKI Client\ | |
| CoreList | STRING | (REG_MULTI_SZ) | The list of dll's to use with the machine-registered plug-in. Caution: Do not modify this entry. |

Table B-7 Symantec® PKI Client Registry Settings (Continued)

| Registry Entry | Type | Default Value | Description |
|--|--------|---|--|
| ConsoleDirectory | STRING | 32-bit: C:\Program Files\Symantec\PKI Client\Console\ | The path to the user console applications. Caution: Do not modify this entry. |
| | | 32-bit (on 64-bit): C:\Program Files (x86)\Symantec\PKI Client\Console\ | This registry setting is not available in the HKCU keys. |
| | | 64-bit: C:\Program Files (x86)\Symantec\PKI Client\Console\ | |
| CSP | STRING | Symantec PKI Client CSP | The CSP that the Symantec PKI Client Utility associates with certificates. Caution: Do not modify this entry. This registry setting is not available in the HKCU keys. |
| DesktopVersion | STRING | Varies | The current installed version of the Symantec PKI Client. Caution: Do not modify this entry. This registry setting is not available in the HKCU keys. |
| ModuleDirectories | STRING | 32-bit: C:\Program Files\Symantec PKI Client\Modules | Location of additional Symantec modules (format is a semi-colon separated list of directories). Caution: Do not modify this entry. |
| | | 32-bit (on 64-bit): C:\Program Files (x86)\Symantec\PKI Client\Modules\ | |
| | | 64-bit: C:\Program Files\Symantec\PKI Client\Modules\ | |
| /Features/Outlook/EnableAutoConfiguration | DWORD | Not present (= 0) | This value controls whether certificates enumerated by the Symantec PKI Client are automatically registered with Outlook. 0 - disabled (default) 1 - enabled This registry setting is not available in the HKCU keys. |
| /Features/Outlook/DefaultProfileName | STRING | Symantec Corporation - Config | Specifies a friendly name for the Outlook profile. This registry setting is not available in the HKCU keys. |
| /Features/Outlook/DefaultEncryptionAlgorithm | STRING | 3DES | Specifies the algorithm used by Outlook when encrypting data and email. AES-256 AES-192 AES-128 3DES RC2-CBC-128 RC2-CBC-64 RC2-CBC-40 DES-CBC This registry setting is not available in the HKCU keys. |

Table B-7 Symantec® PKI Client Registry Settings (Continued)

| Registry Entry | Type | Default Value | Description |
|---|--------|---|---|
| /Features/Outlook/DefaultSignatureAlgorithm | STRING | SHA-1 | Specifies the algorithm used by Outlook when signing outgoing email. SHA-2-512 SHA-2-384 SHA-2-256 SHA-1 MD5 This registry setting is not available in the HKCU keys. |
| PKCS11SessionTimeout | DWORD | Not present (= 20000 - 2 seconds) | A timeout value (in milliseconds) for when the smart card transaction is released by PKCS#11. This registry setting is not available in the HKCU keys. |
| PinCachetimeout | DWORD | Not present (= 300000 - 5 minutes) | Timeout value (in milliseconds) for when the PIN code is cleared from the PIN cache. After the PIN is cleared any authentication operation will require re-authentication. The value is in milliseconds. This registry setting is not available in the HKCU keys. |
| PolicyURLS | STRING | Empty | A space-delimited list of URLs used to attempt to retrieve policies when no other URL has been passed in or found in an existing policy. This registry setting is not available in the HKCU keys. |
| StaticDSMCacheDir | STRING | 32-bit: C:\Program Files\Symantec PKI Client\DSM\ | Location of additional Symantec® modules (format is a semi-colon separated list of directories). Caution: Do not modify this entry. |
| | | 32-bit (on 64-bit): C:\Program Files (x86)\Symantec\PKI Client\DSM\ | |
| | | 64-bit: C:\Program Files\Symantec\PKI Client\DSM\ | |
| SoftwareTokenEnabled | DWORD | 1 | Controls whether the Software Certificate Store (virtual tokens) are enabled for users. 0 - disabled 1 - enabled |
| AllowTrayRegLogon | DWORD | 0 | Applies to PIV/CAC smart cards and Aladdin devices only: Controls whether users can use PKI Client to register their smart cards or devices for Windows Logon. 0 - disabled 1 - enabled (The user must have administrator privileges to his or her machine to use this feature). The tokens listed in this document are already registered for smart card logon and do not need to be re-registered using this registry setting. This registry setting is not available in the HKCU keys. |

Table B-7 Symantec® PKI Client Registry Settings (Continued)

| Registry Entry | Type | Default Value | Description |
|-----------------------------|-------|---------------|---|
| AllowTrayUnlock | DWORD | 0 | Applies to PIV smart cards only: Controls whether PIV users can use PKI Client to unlock devices that were locked due to too many failed PIN attempts. 0 - disabled 1 - enabled This registry setting is not available in the HKCU keys. |
| CacPreference | DWORD | 1 | Applies to PIV/CAC smart cards only: Controls in which mode users' smart cards function. If enabled but the user has not selected a preference, the system settings control the preference. 0 - smart cards function in PIV mode 1 - smart cards function in CAC mode This registry entry is only available in the HKCU keys if AllowUserCacPreference is enabled. In this case, this setting will override any system preferences set for these user activities. |
| AllowUserCacPreference | DWORD | 1 | Applies to PIV/CAC smart cards only: Controls whether users can switch their smart cards between PIV and CAC modes. 0 - disabled 1 - enabled This registry setting is not available in the HKCU keys. |
| TBTrayNoAutoUnregisterCerts | DWORD | 1 | Controls whether smart card certificates are removed from the user's certificate store upon smart card removal. 0 - disabled 1 - enabled This registry setting is not available in the HKCU keys. |

Symantec PKI Client Live Update Registry Settings

The Symantec PKI Client uses the Symantec Live Update feature to update the PKI Client in Windows. The following table lists the Symantec PKI Client Live Update registry locations.

If you are using GPO manage PKI Client deployment to end user machines, you will need to disable Live Update.

Table B-8 Symantec PKI Client Live Update Registry Locations

| Environment | Registry Location |
|-----------------------------------|--|
| 32-bit machine | HKLM\SOFTWARE\Symantec\PKI Client\4\Features\LiveUpdate\ |
| 64-bit machine | HKLM\SOFTWARE\Symantec\PKI Client\4\Features\LiveUpdate\ |
| 32-bit registry on 64-bit machine | HKLM\SOFTWARE\Wow6432Node\Symantec\PKI Client\4\Features\LiveUpdate\ |

Table B-9 Symantec PKI Client Live Update Registry Locations

| Registry Entry | Type | Default Value | Description |
|-----------------|--------|---|--|
| Directory | STRING | 32-bit (X86 Registry): C:\Program Files (x86)\Symantec\PKI Client\LUE\ | Directory where LUE components are installed. Caution: Do not modify this entry. |
| | | 32-bit (on 64-bit) (X86 Registry): C:\Program Files (x86)\Symantec\PKI Client\LUE\ | |
| Host | STRING | liveupdate.symauth.com | The host to use for liveupdate connections. Caution: Do not modify this entry. |
| Language | STRING | SymAllLanguages | The language registration to use with LiveUpdate. Caution: Do not modify this entry. |
| LastUpdated | STRING | 0 (= present time) | Time in ms GMT since the last update check was performed. Default = 0 Will get set to the current time if the value is zero. |
| Product | STRING | 32-bit (X86 Registry): Symantec PKI Client x86 | The product name in Live Update. Caution: Do not modify this entry. |
| | | 64 bit: Symantec PKI Client x64 | |
| ServiceDisabled | DWORD | 0x00 | Controls whether LiveUpdate is enabled or disabled. 0x00 - On 0x01 - Off (default) |
| UpdateInterval | STRING | 30 | The number of days to elapse between update checks. Default is 30. |
| Version | STRING | Varies | Current Live Update Version Identifier for the client. Caution: Do not modify this entry. |

Registry Settings for the Symantec CSP and KSP Dialog Boxes

The Symantec Cryptographic Service Provider (CSP) and the Key Storage Provider (KSP) dialog boxes appear only in Windows, and only when you use these applications to perform cryptographic functions through third-party applications. The following table lists the Symantec CSP and KSP dialog box Registry locations:

Table B-10 Symantec CSP and KSP registry locations

| Environment | Registry Location |
|-----------------------------------|---|
| 32-bit machine | HKLM\SOFTWARE\Symantec\PKI Client\4\Features\VIPER\ |
| 64-bit registry on 64-bit machine | HKLM\SOFTWARE\Symantec\PKI Client\4\Features\VIPER\ |
| 32-bit registry on 64-bit machine | HKLM\SOFTWARE\Wow6432Node\Symantec\PKI Client\4\Features\VIPER\ |

Table B-11 Symantec CSP and KSP registry entries

| Registry Entry | Type | Default Value | Description |
|------------------|-------|-----------------|--|
| enableSection508 | DWORD | Not present (0) | Enables or disables Section 508 compliance. This removes all graphical elements except default Windows coloring. |
| enablePINReset | DWORD | Not present (1) | Controls whether the Forgot Your PIN and Reset PIN links appear in dialog boxes. |

Registry Settings for Threading Library for Windows

Symantec PKI Client uses threading settings in Windows to control the threading library. The following table lists the threading library Registry locations:

Table B-12 Symantec threading library registry locations

| Environment | Registry Location |
|-----------------------------------|---|
| 32-bit machine | HKLM\SOFTWARE\Symantec\PKI Client\4\Features\pthread\ |
| 64-bit registry on 64-bit machine | HKLM\SOFTWARE\Symantec\PKI Client\4\Features\pthread\ |
| 32-bit registry on 64-bit machine | HKLM\SOFTWARE\Wow6432Node\Symantec\PKI Client\4\Features\pthread\ |

Table B-13 Symantec threading library registry entries

| Registry Entry | Type | Default Value | Description |
|----------------|--------|---|---|
| LibraryPath | STRING | 32-bit: C:\Program Files\Symantec\PKI Client\LGPL\pthread.dll | The location of the threading library. Caution: Do not modify this entry. |
| | | 32-bit (on 64-bit): C:\Program Files (x86)\Symantec\PKI Client\LGPL\pthread.dll | |
| | | 64-bit: C:\Program Files\Symantec\PKI Client\LGPL\pthread.dll | |

Configuration Settings for Mac

On a Mac, the registry settings are found in a flat file:

Table B-14 Mac registry locations

| Setting | Registry File |
|-----------------------|--|
| System-level settings | /etc/tblive-4/tblive.rat |
| User-level settings | /Users/{username}/.tblive-4/tblive.rat |

Troubleshooting PKI Client

This chapter explains how to troubleshoot common end-user problems that may occur with Symantec PKI Client, and how to gather information to resolve such problems.

Understanding Logging

PKI Client logging is always enabled. Logging writes to a set location and automatically cleans up logs according to a schedule. Logs older than two weeks are compressed. Logs are kept for the current and prior calendar year, and others are deleted.

Click **Save** under Advanced Settings to create a .zip file that contains logs, debugging information, and other diagnostic data that the end user can send to an administrator to assist with troubleshooting issues.

There are two types of logging that are enabled by default for the Symantec PKI Client:

- PKI Client logging, which includes CSP, PKCS#11, client process, and KSP logging.
Refer to [“PKI Client Logging”](#) on page 29 for details about these logs.
- Post-processing logging. Refer to [“Post-processing Logging”](#) on page 29 for details about this log.

Additionally, you can write installation events to a log file during the installation process. Refer to [“Installation Logging”](#) on page 30 for details about this log.

For all logging, the user writing the logs must have permission to write logs files to the log file directory.

PKI Client Logging

PKI Client writes logs that contain information about CSP events (such as use of Windows Logon and Microsoft Outlook), as well as PKCS#11, client process, and KSP events.

Post-processing Logging

If you run a custom script to perform post-processing operations, PKI Client will capture any error thrown by this script. This log contains one line per error thrown, listing the following information:

- Date and time the error was thrown
- Complete path to the script that threw the error
- Name of the script that threw the error

On a PC, this error log is written to <user profile>/App Data/Local/PKI Client/4, and will only appear if the script throws an error. The user running the script must have appropriate permissions to write to this location.

On a Mac, this error log is written to /Users/{username}/.tblive-4/beretta.log, and will only appear if the script throws an error. The user running the script must have appropriate permissions to write to this location.

Refer to *Symantec™ PKI Client Writing Post-processing Scripts Guide* for more information about writing custom scripts.

Installation Logging

You can log installation events for installations run as an end user installation, or run as a GPO installation.

Logging when Installing as an End User

To log installation events if you are installing PKI Client as an end user (on a single end-user machine), run the PKI Client installer with the /Log and /Logfile options. For example:

```
Symantec-PKI-Client-2.10.1.exe /Log /Logfile bootstrap.log /ComponentArgs x86:''/1*vx  
msi_x32.log'' /ComponentArgs x64:''/1*vx msi_x64.log''
```

This installs the PKI Client and writes the installation log to the file MyLog.txt in the directory on the end user's machine where the command is run. It will also generate two log files, bootstrap.log and either msi_x32.log on 32-bit systems or msi_x64.log on 64-bit systems.

Logging and -Dumplog Function on a Mac

On a Mac, logging is always on and goes to /var/log/install.log. Also, on a Mac, there's a -dumplog function that puts the info on screen rather than just in the log file.

Logging when Installing with GPO

To log installation events if you are installing PKI Client as a GPO installation:

- 1 Go to **Administrative Tools** → **Active Directory Users and Computers**. Right-click on the name of your domain and click **Properties**.
- 2 Expand **Computer Configuration**, then **Administrative Templates**, and then **Windows Components**.
- 3 Select **Windows Installer**.
- 4 Double-click **Logging**, and then click **Enabled**. In the Logging box, enter the options you want to log. Enter `voicewarmupx-` for full logging.

The log file, Msi.log, appears in the Temp folder of the system volume.

Troubleshooting Common Problems

The following are common problems end users may encounter when installing and using PKI Client.

An end user's smart card does not trigger the Windows login PIN dialog, or there is an error saying the appropriate drivers for the card are not installed.

This scenario typically means the PIV/CAC smart card is not registered in the Windows Calais database. (This feature only applies to PIV/CAC smart cards.)

Make sure that the end user has a working reader plugged in, and that the certificates are showing up in PKI Client. If the smart card has a certificate that can be used for smart card log on, the user should click **Smart Card Settings**, and then select **Register** under **Register for Windows logon** in PKI Client.

An end user's certificate shows up for smart card logon, but logon fails.

Make sure the end user's workstation has been joined to the domain and that the user's workstation points the DNS to the domain controller. Also, look in the event log of the domain controller for any Kerberos errors indicating why the certificate was rejected.

Logging shows that an end user's smart card is not recognized.

Make sure the smart card and smart card reader are supported by PKI Client.

Even after configuring the policy setting to lock the workstation upon smart card removal, nothing happens when the smart card is removed.

Make sure the PIV/CAC smart card was used for Windows login. If the user logs in with username and password smart card removal will not have any effect.

If the end user is running Windows Vista or Windows 7, you need to make sure the Smart Card Removal Policy service is started. Otherwise the smart card removal policy setting will not work.

The end user's certificates are not propagated to the user certificate store when the card is inserted

Make sure the PKI Client process, PKIClientAgent, is running on the user's machine.

The end user has lost or locked out their PIN. How do they access their smart card?

- For non-PIV/CAC smart cards, once users lose or lock out their PIN, they must reset the PIN. It is important to note that resetting the PIN will delete all certificates stored on the smart card. If users must reset the PIN, you will need to assist them with recovering and/or replacing these certificates. If you issue certificates using Managed PKI, you can recover the user's keys or issue replacement certificates through PKI Manager.
- For PIV smart cards, if users lose or lock out their PIN, they must obtain a Personal Unlock Key (PUK) from their PKI Client administrator, and enter it in PKI Client.
- For CAC smart cards, if users lose or lock out their PIN, they must follow your existing process to unlock their devices.

The smart card on a Mac locks up or cannot find certificates.

Remove and re-insert the smart card and/or reader.

Cannot export a certificate from the Windows certificate store or from a browser.

By default, some certificates cannot be exported from the Windows certificate store or from a browser for security reasons. These include:

- Certificates stored on a security device. Certificates are stored on security devices, in part, to restrict the ability to export keys.
- Managed PKI administrator certificates. These certificates can be exported as a proprietary .glck file using PKI Client; however, they can only be imported to another instance of PKI Client. This enforces the requirements of the Certification Practices Statements (<http://www.verisign.com/repository/cps>) that apply to these types of certificates.

This is the expected behavior.

PKI Client was installed on a Windows XP machine before the Microsoft Base Smart Card CSP.

If a user on a Windows XP machine will use a security device that requires the Microsoft Base Smart Card CSP and PKI Client has already been installed on that machine, perform one of the following to correctly add the CSP and register PKI Client:

Uninstall PKI Client, install the Microsoft Base Smart Card CSP, and reinstall PKI Client.

After installing the Microsoft Base CSP, manually edit the following registry entries on the user's computer. Set these to **1**.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Base Smart Card Crypto Provider\AllowPrivateExchangeKeyImport
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Base Smart Card Crypto Provider\AllowPrivateSignatureKeyImport

Users get an authentication error (401: Unauthorized) when PKI Client attempts to autoenroll them for certificates

This occurs if the fully-qualified Domain Name (FQDN) for your PKI Enterprise Gateway machine is not trusted by the end user's computer. Use a GPO push to add the FQDN to the **Internet Settings** → **Intranet Security Zone** (or have the user manually add the FQDN). Alternatively, use the Netbios name of the machine hosting the PKI Enterprise Gateway for the Gateway URL when configuring the PKI Enterprise Gateway.

Users get an Error Code 193 when installing certificates

This occurs when running post-processing scripts. These scripts depend upon the base Windows utilities, such as find.exe, being in the PATH. If third-party applications install their versions of these utilities in the PATH before the Windows version, post-processing errors will occur.

Overriding default post-processing scripts

By default, PKI Client runs pre-defined scripts each time a user enrolls for or renews a certificate:

- InstallCA.signed.bat. This script installs the certificate chain in the system certificate store. If a root CA is new to users' computers, the users may see a system prompt notifying them of this.
- RegisterFirefox.signed.bat. This script installs the certificate and its chain into Firefox, and if necessary, registers the PKCS11 module. If Firefox is running on users' computers when this script is run, they may see a system prompt notifying them that Firefox needs to be restarted.

You can override this behavior by creating and uploading custom scripts with the same name and attaching them to the appropriate certificate profiles. The next time post-processing is invoked for those profile, the modified scripts will be downloaded and stored for future use.

Numerics

- 32-bit machine
 - CSP and KSP dialog box registry location for 26
 - CSP registry location for 20, 27
 - Live Update registry location for 25
 - PKI Client registry locations 22
 - smart card logon registry location 20
 - threading library registry location for 27
- 32-bit registry on 64-bit machine
 - CSP and KSP dialog box registry location for 26
 - CSP registry location for 20
 - PKI Client registry location for 22, 25
 - smart card logon registry location for 20
 - threading library registry location for 27
- 64-bit registry on 64-bit machine
 - CSP and KSP dialog box registry location for 26
 - CSP registry location for 20
 - PKI Client registry location for 22, 25
 - smart card logon registry location for 20
 - threading library registry location for 27

A

- administrators installing PKI Client 8
- advanced features
 - CAC smart card 17
 - PIV smart card 17
- advanced PKI Client features 14-18
- application configuration 11-18
- assigning a GPO package
 - Windows 2008 9
 - Windows 2012 9

B

- BAT files, writing 11

C

- CA, trusted 11
- CAC smart card 5
 - advanced features 17
 - computer lock and unlock with 5
 - secure windows login with 5
- Calais database 20
- certificate troubleshooting 5
- client authentication 5
- Common Access Card
 - see* CAC smart card
- common problems 30
- computer lock and unlock 5
- configuration settings for PKI Client 22
- configuring

- applications to use PKI Client 11-18
- SSL client authentication 11-12
- creating the GPO
 - Windows 2008 9
 - Windows 2012 9
- Cryptographic Service Provider
 - see* CSP
- CSP 4, 7, 31
 - enabling logging for 29
 - logging 29
 - registry entries 20
 - registry locations 20
- CSP dialog box
 - registry entries 27
 - registry locations 26

D

- digital signing of documents 5
- disable Live Update for 25

E

- enabling CSP logging 29
- enabling logging for PKCS#11 29
- end users installing PKI Client 7
- end-user requirements 3
- eToken Base Cryptographic Service Provider 4

F

- features
 - advanced PKI Client 14-18
 - CAC smart card advanced 17
 - PIV smart card advanced 17
 - PKI Client 5

G

- government end-user requirements 5
- GPO 25
 - assigning a package on Windows 2008 9
 - assigning a package on Windows 2012 9
 - creating on Windows 2008 9
 - creating on Windows 2012 9
 - enabling and disabling advanced features through 14-18
 - installation logging 30
 - installing PKI Client using a 8
 - instructions for Windows 2008 9
 - instructions for Windows 2012 9
 - linking to a domain on Windows 2008 9
 - linking to a domain on Windows 2012 9
 - setting up a share on a server 9

group policy 9, 11, 19
 Group Policy Object
 see GPO

H

hardware requirements 3

I

installation event logging 29
 installer 7
 MSI 8
 multilingual 8
 installing PKI Client 7-9
 administrators 8
 end users 7
 quietly 8, 10
 using GPO for 8

K

Key Storage Provider
 see KSP
 KSP 26
 KSP dialog box
 registry entries 27
 registry locations 26

L

license agreement 8
 linking a GPO to a domain 9
 Live Update registry settings 25
 logging
 CSP 29
 installation event 29
 PKCS#11 29
 post-processing 29, 30

M

Microsoft Base Smart Card Cryptographic Service Provider 4,
 7, 31
 multilingual installers 8

P

Personal Identity Verification
 see PIV smart card 5
 PIV smart card 5
 advanced features 17
 computer lock and unlock with 5
 secure windows login with 5
 PKCS#11
 enabling logging for 29
 logging 29
 PKI Client
 administrators installing 8
 advanced features 14-18

configuration settings 22
 configuring applications to use 11-18
 end users installing 7
 end users installing quietly 8, 10
 features of 5
 installer 7
 installing and uninstalling 7-10
 process 5
 registry locations 22
 registry settings 19-27
 troubleshooting 29
 using GPO to install 8
 post-processing logging 29, 30
 pre-requisites
 SSL client authentication 11
 problems 30
 process 5

Q

quiet installation of PKI Client 8, 10

R

registry entries
 CSP 20
 CSP dialog box 27
 KSP dialog box 27
 smart card logon 21-22
 threading library 27
 registry locations
 32-bit machine 20, 27
 32-bit machine CSP and KSP dialog box 26
 CSP 20
 CSP 32-bit registry on 64-bit machine 20
 CSP 64-bit registry on 64-bit machine 20
 CSP and KSP dialog box 32-bit registry on 64-bit
 machine 26
 CSP and KSP dialog box 64-bit registry on 64-bit
 machine 26
 CSP dialog box 26
 KSP dialog box 26
 Live Update 32-bit machine 25
 PKI Client 22
 PKI Client 32-bit machine 22
 PKI Client 32-bit registry on 64-bit machine 22, 25
 PKI Client 64-bit registry on 64-bit machine 22, 25
 smart card logon 20
 smart card logon 32-bit machine 20
 smart card logon 32-bit registry on 64-bit machine 20
 smart card logon 64-bit registry on 64-bit machine 20
 threading library 27
 threading library 32-bit machine 27
 threading library 32-bit registry on 64-bit machine 27
 threading library 64-bit registry on 64-bit machine 27
 registry settings 19-27
 Live Update 25
 requirements 3
 SSL client authentication 11

S

- SafeNet Authentication Client 7
- Section 508 compliance 27
- secure email 5
- secure Windows login 5
- security device
 - requirements for 4
- server share 9
- setting up a share on a server for GPO 9
- share 9
- smart card
 - readers for 5
 - Windows login requirements 4
- smart card logon
 - registry entries 21-22
 - registry locations 20
- software requirements 3
- SSL client authentication
 - configuring 11-12
 - requirements for 11
- SSL web authentication 5
- Symantec CSP
 - see* CSP
- Symantec PKI Client
 - see* PKI Client
- Symantec-PKI-Client msi installer file 7

T

- threading library 27
 - registry entries 27
 - registry locations 27

- troubleshooting
 - certificates 5
 - common problems 30
 - PKI Client 29

U

- uninstalling PKI Client 10

V

- VPN 5

W

- web server certificate 11
- Wi-Fi 5
- Windows 2008
 - assigning a GPO package 9
 - creating the GPO 9
 - installing with GPO on 9
 - linking a GPO to a domain 9
- Windows 2012
 - assigning a GPO package 9
 - creating the GPO 9
 - installing with GPO on 9
 - linking a GPO to a domain 9
- Windows process 5
- Windows registry settings
 - see* registry settings
- Windows XP 7, 31
- writing BAT files 11

