Symantec™ PKI Client Administrator's Guide

v2.15

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1

Introduction

This chapter includes the following topics:

About the Symantec PKI Client

Symantec PKI Client is software for digital signing, authentication, and data protection with desktop-based applications that use digital certificates which are stored on a smart card, security device, or end-user computer.

PKI Client is included with Managed PKI. It assists end users with enrolling for and managing certificates issued by Managed PKI.

See the Managed PKI product and documentation for more information about Managed PKI and the Managed PKI certificate lifecycle.

This documentation provides instructions for administrators who plan to install, configure, and troubleshoot Symantec PKI Client for end users.

Chapter 2

Understanding PKI Client

This chapter includes the following topics:

About the PKI Client

This documentation describes the features, end-user hardware and software requirements, and the client process of the Symantec PKI Client v2.15.

You need to review the PKI Client software and the PKI Client FAQs to learn more about PKI Client and how your users plans to use it. The PKI Client FAQs are available from the Need Help? link of PKI Client.

Hardware and Software Requirements

The PKI Client is supported on the following platforms and software.

Hardware Requirements

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

Platform Requirements

Table 2-1 lists all available platforms on which the PKI Client is supported.

Note: PKI Client does not support any IE browser running in Compatibility Mode.

Table 2-1 PKI Client Operating System and Browser Support

OS	Browser
Windows® 7 SP1 (64-bit)	IE 9 (32-bit), IE 10 (32-bit) and IE 11 Firefox 42 Chrome 46
Windows 8.1 (32-bit and 64-bit)	IE 11 Firefox 42 Chrome 46
Windows 10 (32-bit and 64-bit)	IE 11 Firefox 42 Chrome 46
Mac OS X® v10.9.5[a]	Safari 9.0 Firefox 42 Chrome 46
Mac OS X v10.10.5[b]	Safari 9.0 Firefox 42 Chrome 46
Mac OS X v10.11[b]	Safari 9.0 Firefox 42 Chrome 46

[a] Managed PKI does not support Government Edition CAC (Common Access Cards) and PIV (Personal Identify Verification) smart cards on the Mac 10.9.x operating system.

[b] Managed PKI does not support any hardware tokens on the Mac OS X10.10.x and 10.11 operating systems, including Government Edition CAC and PIV smart cards.

About 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.

Table 2-2 lists all supported security devices.

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 (Optionally requires the SafeNet Authentication Client)
SafeNet iKey 4000	eToken Base Cryptographic Service Provider (Requires the SafeNet Authentication Client)

About Windows Smart Card Login Requirements

The PKI Client supports the following for Windows smart card login:

- Standard users
  One of the tokens listed in the previous table 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.)

Additional Security Device Considerations

- 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 need to re-initialize the token with PKI Client to continue to use the token with Managed PKI.
- Users should only install the SafeNet Authentication Client if the certificates they will store on their security devices are issued from a certificate profile that requires it. Users should manage all other certificates using PKI Client.

If your users store multiple certificates on their security device issued by mixed certificate profiles (those that require SafeNet Authentication Client and those that do not), Symantec recommends that they initialize the security device using PKI Client, and do not allow the SafeNet Authentication Client to upgrade the security device format. Otherwise, PKI Client will not be able to manage the certificate, and renewals will fail.

About PKI Client Features

Symantec PKI Client offers the following features:

- 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 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.
- 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.

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

- Administrator Credential Support for 3rd-party CSPs
  For CI Plus administrator certificates, PKI Client supports SafeNet eToken, Microsoft Base Smart Card, and Symantec CSPs.
- 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.
- 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 "About Windows Smart Card Login Requirements" on page 8.

About the PKI Client Agent

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 user logs on. When an end user inserts a smart card, PKI Client reads the certificates on the device and automatically places these certificates to make them available to the operating system and to third-party services and applications.

The PKI Client Agent also handles other key features, such as autoenrollment, starting renewal, retrieving certificate policies, and ensuring that maintenance tasks are completed.

Chapter 3

Installing PKI Client

This chapter includes the following topics:

About Installing PKI Client

You can select the appropriate type of installation for the PKI Client that you plan to perform for end users:

- See “Installation Methods for PKI Client on Windows” on page 11.
- See “Installing PKI Client on a Mac” on page 16.

Installation Methods for PKI Client on Windows

You can install PKI Client on a machine that supports Microsoft Windows by one of the following methods:

- See “Installing PKI Client as an End-User” on page 12.
- See “Quietly Installing PKI Client” on page 13.

Special Considerations for Installation

This section lists some considerations that you and your end users need to be aware of when installing PKI Client:

- If your users will store certificates on FIPS-compliant SafeNet security devices, you must also install the SafeNet Authentication Client on the user's machine. See the documentation that is provided with SafeNet tokens for procedures.

- The first time you open the Google Chrome or Mozilla Firefox browser after installing PKI Client, you will be prompted to enable the PKI Client extension, Symantec Authentication Client Plugin Extension. If you do not enable this extension, you will need to manually enable this extension:
  - In the Chrome browser, navigate to the Settings → Extensions page and select **Enable** next to Symantec PKI Client Plugin Extension 0.1.
  - In the Firefox browser, click the **Firefox** button and click **Add-ons** to open the Add-on Manager. Select the **Extensions or Appearance or Plugins** panel, and click **Enable** next to Symantec Authentication Client Plugin Extension. You may need to restart the browser.

Installing PKI Client as an End-User

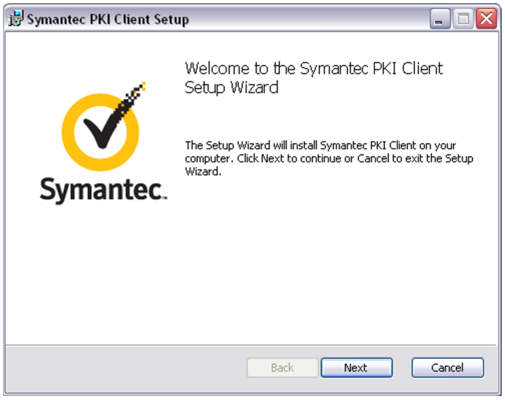
To install PKI Client as an end-user

1. On a machine that supports Microsoft Windows, extract the PKI Client installer to a location on your computer.

   For example:

   `C:\WINDOWS\Temp\Symantec-PKI-Client-2.15.x`

2. Double-click **Symantec-PKI-Client-2.15.x.exe**.
3. In the Symantec PKI Client Setup installer, click **Next**.



4. Click **I accept the terms in the License Agreement** and then 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 on the command line. If you use the command line, you can install PKI Client without clicking through the installer. You can also use this installation method if you install PKI Client remotely on an end-user's workstation or if you use a group policy for domain users.

To quietly install PKI Client

1. Open a Command Prompt (**Start > Run > Cmd**).
2. Run the installer command with the `/q` option.

   For example:

   ```
   Symantec-PKI-Client-2.15.x.exe /q
   ```

   This command installs PKI Client in the `C:\Program Files\Symantec\PKI Client\` directory.

Installing PKI Client as an Administrator

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

Extracting MSI Files

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

To extract MSI files

1. Open a Command Prompt (**Start > Run > Cmd**).
2. Run the installer command with the `/ExtractCAB` option.

   For example:

   ```
   Symantec-PKI-Client-2.15.x.exe /ExtractCAB
   ```

This command extracts the installation files to a `SupportFiles` directory in the same directory as the installer.

Setting up Group Policy Object (GPO) Installations on Windows

You can set up a share either on the server or a location that domain users or the domain machines can access. Then you must add to the share the files that you want to install.

Creating the GPO

To create the GPO

1. Start the 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**.

Assigning a Package

You can assign a package that is installed on all computers which are joined to the domain as soon as the group policy is updated on that machine.

To assign a package

1. Expand **Computer Configuration**, then **Policies**, then **Software Settings** and then select **Software Installation**.
2. Right-click and select **New > Package**.
3. Navigate to theshare 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. On the Modifications tab, click **Add** and then navigate to the correct .mst file for the target system's locale and architecture

   See “Extracting MSI Files” on page 13.
6. Click **OK**.

   The package now appears in the list of software installations.

Linking the GPO to a Domain

To link the GPO to a domain

1. On the Group Policy Management screen, drag the new GPO to your Domain.
2. At the prompt, select **Ok**.
3. Verify that the GPO is under the domain name.

   If you right-click this icon, you can view the checked Link option.

Importing a Certificate when Offline

You can enable 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 that you use so that end users do not receive any prompts. Otherwise the end user may receive prompts, unaware of their origin.

Viewing Installation Logs

You need to complete the following procedures to view logs that have been generated during the installation.

To view installation logs

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

   ```
   Symantec-PKI-Client-2.15.x.exe /Log /Logfile bootstrap.log
   /ComponentArgs x86:"/l*vx
   msi_x32.log / "  /ComponentArgs x64:"/l*vx msi_x64.log"
   ```

   where:

   - <installer.exe> represents the location from where the installation script was run
   - <x64/x86> represents the version of the installer that was run.
     Be sure to apply x86 to the 32-bit version and x64 to the 64-bit version.
   - <dest_dir> represents the name of the folder in which the installation logs are saved.

Uninstalling PKI Client on a PC

To uninstall PKI Client on a PC

1. Open the Control Panel (**Start** → **Control Panel**).
2. In the Control Panel, click **Add** or **Remove Programs**.
3. In the list of installed programs, select **Symantec PKI Client**.
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 to uninstall the application.

Installing PKI Client on a Mac

You can install PKI Client quietly on a Mac using the Terminal. If you use the Terminal, you can 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.

To install PKI Client on a Mac:

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

   ```
   installer -pkg Symantec-PKI-Client-x64.2.15.x.pkg -target /
   ```

   The PKI Client is now installed.

   Configuration settings on Mac OSX are in the OSX flat file. On Mac OSX, 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.

To view installation logs

1. Double-click **Symantec-PKI-Client-x64.2.15.x.pkg**.
2. Perform the installation with the Mac Installer.
3. From the Installer's menu bar, click **Window > Installer Log** during the installation to view the installation logs.

Uninstalling PKI Client on a Mac

To uninstall PKI Client on a Mac

1. Go to **Finder > Applications > Symantec Authentication >PKI Client Uninstaller**.
2. Follow the prompts to uninstall PKI Client.

Appendix A

Configuring Applications to use PKI Client

This appendix includes the following topics:

About Configuring Applications for 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.

See *Symantec PKI Client Post-processing Scripts Guide* for more information.

About Certificate Client Authentication

You can verify the identity of end users and authenticate them to your organization's web site(s) using their PKI certificate. At a minimum, the server authenticating your end users must trust the end users' certificate hierarchy, and your end user clients must trust the server's certificate hierarchy.

The steps you follow to set up Certificate Client Authentication may vary depending upon your specific infrastructure. This guide provides an example showing how to set up Certificate Client Authentication on Internet Information Server in a Windows domain.

Prerequisites for SSL Client Authentication

In addition to the hardware and software requirements, you must meet the following additional requirements for Certificate Client Authentication:

See "Hardware and Software Requirements" on page 6.

- 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 Certificate Client Authentication

Set up Certificate Client Authentication to allow users to authenticate to your web pages using their certificates. for example, you can use this option to require end users to authenticate with the certificate stored on their smart card.

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

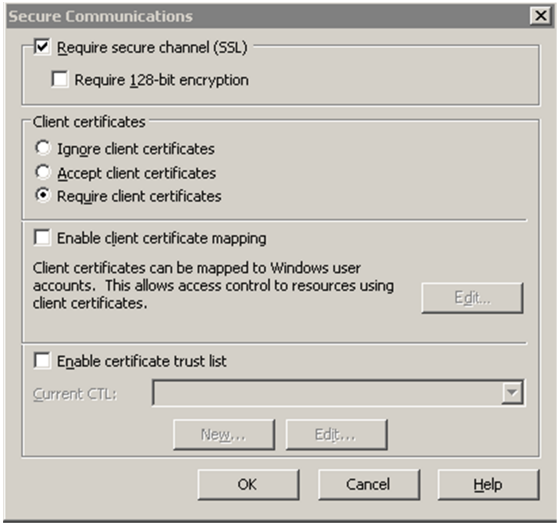
In addition to the hardware and software requirements, you must meet the following additional requirements for Certificate Client Authentication:

See "Hardware and Software Requirements" on page 6.

- End users must be members of your organization's domain
- End-user 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.

1. On the 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** to open the Secure Communications dialog box.



5. In the Secure Communications dialog box, do the following:
   - Check the **Require secure channel (SSL)** check box.
   - Select **Require client certificates**.
   - Click **OK**.
6. In the Secure Communications section, click **Server Certificate**.
7. 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.
8. 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 automatically enrolls any certificate profile or profiles that are configured for an end user. This process is based on the user data, which is included in Active Directory. PKI Client autoenrollment is integrated with PKI Enterprise Gateway to make autoenrollment nearly transparent to end users and administrators contingent upon the configuration of the certificate profile:

- The enrollments occur without end-user notification or intervention
- Administrators do not need to provide an enrollment email, enrollment code, or enrollment link for certificate enrollment

PKI Client also automates renewals. In other words, the entire certificate lifecycle experience is completely automatic for most users.

You must complete the following tasks to enable PKI Client-based autoenrollment for Windows:

- See "Installing PKI Enterprise Gateway" on page 21.
- See "Configuring a Managed PKI Certificate Profile" on page 21.
- See "Making the Managed PKI Root CA Certificate Available to the Domain" on page 22.
- See "Making PKI Client Available to End Users" on page 22.

Installing PKI Enterprise Gateway

See *Symantec™ PKI Enterprise Gateway Deployment Guide* for instructions on how to install PKI Enterprise Gateway.

To install PKI Enterprise Gateway:

1. Select **Active Directory** as the user store during the installation of the PKI Enterprise Gateway.
2. Join the end-user machines to the domain that is configured in PKI Enterprise Gateway.

Configuring a Managed PKI Certificate Profile

You need to create a certificate profile for PKI Client-based autoenrollment. However, you must specify certain settings during the configuration of the Managed PKI Certificate Profile.

To configure a Managed PKI Certificate Profile

1. Select **PKI Client** as the Enrollment method.
2. Select **Active Directory** as the Authentication method.
3. Set the appropriate authorized user list and PKI Enterprise Gateway settings.
4. Select **PKI Client should automatically enroll for Windows users**.

See the PKI Manager and its associated help for details on how to create certificate profiles.

Making the Managed PKI Root CA Certificate Available to the Domain

If the Managed PKI root CA certificates are not pre-installed in the domain, you need to download them.

To make the Managed PKI Root CA Certificate available to the domain

1. From the **Manage CA** page in the PKI Manager, download the Managed PKI Root CA certificate.
2. Use the Microsoft Management Console (MMC) to push the Managed PKI Root CA certificate to the domain.

   Otherwise the end user is prompted to trust the root CA the first time that the PKI Client attempts to autoenroll for a certificate.

See the Microsoft® documentation for procedures on how to install and trust a CA in a forest.

Making PKI Client Available to End Users

PKI Client-based autoenrollment requires PKI Client to be installed on your end users' machines. End users are not prompted to install PKI Client during autoenrollment. If the PKI Client is not already installed on your end users' machines, you must make the PKI Client available to them.

To make PKI Client available to end users, follow the instructions on how to install PKI Client.

See “About Installing PKI Client” on page 11.

Configuring Group Policy Settings for End Users

To configure group policy settings for end users

1. On a machine on which the PKI Client has been installed, select a Group Policy Object (GPO) to push a computer policy to end users.
2. Enable **Managed PKI Auto-Enrollment Settings** and configure the policy settings with the following specific values. All values except **Agent Scan Base Interval** and **Agent Scan Maximum Random Offset** must match the values you set in your PKI Enterprise Gateway.
   - **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.
   - **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.
   - **Gateway URL** represents the URL of your PKI Enterprise Gateway. **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.
   - **RA Service Port** represents 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
3. 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 into another machine in the same domain, the end user then receives an error message that the certificate has already been enrolled unless one of the following conditions applies:
   - The certificate profile has been configured to allow multiple certificates.
     In this case, the end user receives the certificate as expected.
   - The certificate is an S/MIME certificate.
     In this case, the end user receives a copy of an existing, valid S/MIME certificate.

Instructions on how to define and push group policy settings to PKI Client on your end-user machines are available.

See “Enabling or Disabling Advanced PKI Client Features” on page 25.

Additional Autoenrollment Tasks for Mac OS

You must complete the following tasks if your environment includes machines that support Mac OS:

- See "Additional Prerequisites for Mac OS" on page 24.
- See "Setting the Mac OS X Server Mobileconfig Profile" on page 24.

Additional Prerequisites for Mac OS

The following requirements must be met in a Mac OS environment:

- PKI Client must be joined to a pre-existing or pre-configured OSX Server Symantec has tested this on the OSX Mountain Lion Server.
- The 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

Setting the Mac OS X Server Mobileconfig Profile

You need to set the autoenrollment gateway URL in a Mac OS X Server mobileconfig profile.

To set the 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.

   PKI Client-based autoenrollment for Mac OS requires that you add a Custom Settings payload.

2. Set the **Preference** domain to `com.symantec.pkiclient.autoenroll`.
3. Add a String setting that is named gatewayURL with the value that is set in the GPO on Windows.
4. Save the profile and let it be pushed to the appropriate user/device.

Note: Check the **Active Tasks/Completed Tasks** to verify that the profile has been pushed. This may take some time. After a profile has been successfully pushed, it may not take effect until the user logs off and restarts.

Enabling or Disabling Advanced PKI Client Features

You can enable advanced PKI Client features through a GPO.

Table A-1 provides information about these features, as well as the feature-specific GPO settings that you need to configure.

Note: If you want to enable these features for an individual end user, you need to modify the appropriate registry entries on the user's machine.

See "About Registry and Configuration File Settings" on page 37.

To enable or disable advanced PKI Client features:

1. Start 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. To select the feature that you want to enable, do the following:
   - Expand your domain and right-click **Group Policy Objects**.
   - Select **New** and name the new group policy.
   - Right-click the new group Policy and click **Edit**.
   - Expand **Computer Configuration**, then **Policies**, then **Administrative Templates** to select **Symantec PKI Client**.
   - Double-click the setting that you want to enable and then select **Enabled** at the top of the page.
3. Set the advanced features.

   Table A-1 lists the GPO settings for each advanced 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.	■ 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. ■ **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).	■ 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. As Outlook registration is handled by post-processing, this setting is disabled by default.	■ Double-click **Control Outlook Profile Configuration**. ■ Select **Enabled**. ■ Click **Apply**.

Table A-1 GPO Settings *(continued)*

Advanced Feature	Description	Setting
Configure PKI Client Logging	Controls whether PKI Client writes logs, and configures log settings. PKI Client logging is enabled by default ■ **Cleanup Interval (in days)** sets how often PKI Client performs logging maintenance. The default (and the minimum) is 1 day. ■ **Compression Intervals (in days)** sets how old a log file must be before it is compressed. PKI Client compresses all logs older than this threshold. The default (and the minimum) is 2 days. ■ **Deletion Intervals (in days)** sets how old a log file must be before it is deleted. PKI Client deletes all logs older than this threshold. The default is 90 days. The minimum is 14 days. ■ **Minimum free disk space (in MB) to enable logging** sets the minimum amount of space that must be available before PKI Client starts logging. If the disk space drops below this threshold, PKI Client will not write log files.	■ Double-click **Configure PKI Client Logging**. ■ Select **Enabled**. ■ Enter values for the following: Cleanup Interval (in days) Compression Intervals (in days) ■ Deletion Intervals (in days) ■ Minimum free disk space (in MB) to enable logging ■ Click **OK**. The changes become effective within one minute after the GPO is applied.
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.	■ Double-click **Control Outlook Profile Configuration**. ■ Check **Enable Outlook AutoConfiguration**. ■ Click **OK**.

Table A-1 GPO Settings *(continued)*

Advanced Feature	Description	Setting
Name Outlook Profile	Sets a friendly name for the Outlook profile. This is set to **Symantec Corporation - Config** by default.	■ 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.	■ Double-click **Control Outlook Profile Configuration**. ■ Check the box in front of the **Match Email Address** field. ■ Click **OK**.
Set Encryption Algorithm	Allows you to set the algorithm Outlook will use to encrypt data and email. This is set to 3DES by default.	■ 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.	■ 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.	■ 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.	■ Double-click **Control Software Certificate Support**. ■ Click **OK**.

Table A-1 GPO Settings *(continued)*

Advanced Feature	Description	Setting
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.	■ 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.	■ 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.	■ 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.	■ 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	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). These settings can be viewed in the setup log file (usually C:\Users\Public\pgwSetup_log_*.txt).	■ 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	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. **Note:** Wow6432Node entries affect 32-bit usage on 64-bit machines. The default determines whether the machine is natively 32-bit or 64-bit.	■ 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	Enables PKI Client to manages policies related to key usage for certificates with a non-repudiation key usage extension. 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.	■ Double-click **Managed PKI Auto-Enrollment Settings**. ■ Select **Always authenticate non-repudiation certificates**. ■ Click **OK**.

Table A-1 GPO Settings *(continued)*

Advanced Feature	Description	Setting

Override PIN Policy	Configures settings for overriding the default PIN policy.
	
	If enabled, you can set a more restrictive PIN policy in PKI Client than the default PIN policy on the device. The new PIN policy cannot be less restrictive than the device's default policy. For example, you cannot require alphanumeric characters if the device only supports numeric characters, or set a minimum or maximum character restriction that exceeds the minimum and maximum character restrictions set on the device.
	
	■ For Symantec CSP hardware tokens, the PIN cannot be less than 6 characters or more than 10 characters.
	■ For Symantec CSP software tokens, the PIN cannot be less than 6 characters or more than 24 characters.
	■ For third-party CSPs, the default PIN policy cannot be changed.
		■ Double-click **Override PIN Policy**.
		■ Select what characters can be used in PINs:
		  ■ Select Any Character to allow a mixture of numbers and letters.
		  ■ Select Alphabetic to allow letters only
		  ■ Select Numeric to allow numbers only.
		■ Select the minimum PIN length and maximum PIN length.
		■ Click **OK**.

Table A-2 Advanced PIV/CAC Smart Card Features

Advanced Feature	Description	Setting
Enable Windows Logon/Unlock Computer	Allow users to log into Windows or unlock their Windows-based computer using the certificate installed in their smart card. Requires that the smart card contains a certificate that is enabled for Windows Logon. 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.	■ Double-click **Configure additional Console UI operations**. ■ Select **Activate Register-for-Logon Operation**. ■ Click **OK**.
Enable Device Unblock	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. Your PKI Client administrators will need to provide the PUK using your existing smart card process and software.	■ Double-click **Configure additional Console UI operations**. ■ Select **Activate Device Unblock Operation**. ■ Click **OK**.
Enable PIV/CAC Preference	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.	■ Double-click **Configure additional Console UI operations**. ■ Select **Configure PIV/CAC Hybrid handling**. ■ Select which interface is the default (PIV or CAC). ■ Click **OK**.

Supporting the Chrome Browser in PKI Client on Windows and OSX

For Windows and OSX operating systems, PKI Client provides support for the Google Chrome browser through two components:

- A Chrome browser extension (Symantec Authentication Client Plugin Extension).
- Chrome Native Messenger. This component is installed along with PKI Client.

The first time that a user accesses the Certificate Lifecycle Services pages using the Chrome browser on Windows and OSX(typically when enrolling for certificates), the Certificate Lifecycle Services pages:

- Attempt to load the Chrome extension. The user needs to explicitly **Allow** the extension the first time the user launches Chrome after PKI Client is installed.
- Attempt to load PKI Client.

If any of these fail, the Certificate Lifecycle Services pages attempt to detect the point of failure and recover. If the process cannot recover, the user will see an error message. The most likely reasons that the process may fail are:

- The user has blacklisted the extension (by deleting the extension in Chrome). The user must reinstall PKI Client to trust the extension again. Alternatively, the enterprise can use a Chrome policy push the install the extension on the user's machine.
- The user has disabled the extension in Chrome. The user will be prompted to reinstall the Chrome extension and, potentially prompted to download and install the PKI Client. The user should install the extension, but can safely skip the PKI Client installation if it is already installed on their machine.
- Lost Internet connection. The user must retry the enrollment (the administrator may need to reissue the enrollment code).
- The enterprise has set a policy to not install PKI Client. In this case, the user will not be prompted to install PKI Client in the first place. The enterprise must change this policy. Alternatively, the enterprise can use a Chrome policy push the install the extension on the user's machine.

If the process cannot be recovered, you will need to do one of the following:

- See “Reinstalling PKI Client” on page 34.
- See “Manually Enabling the Chrome Extension” on page 34.
- See “Pushing the Chrome Extension to a User's Machine” on page 34.

See “About Troubleshooting the PKI Client” on page 54.

Reinstalling PKI Client

Have the user complete the following procedure to reinstall PKI Client. Only any missing components are reinstalled. Reinstalling PKI Client is usually required if the user has manually deleted the extension in Chrome.

1. Access the certificate enrollment link in your pick-up email.
2. Click **Install PKI Client** in the Certificate Lifecycle Services page.
3. You are prompted to manually install the Chrome extension. Follow the prompts to install and enable (Allow) the extension.
4. If prompted, download and install PKI Client.

Manually Enabling the Chrome Extension

Have the user complete the following procedure to manually enable the Chrome extension. This is usually required if the user has manually disabled the extension in Chrome.

1. In the Chrome browser, navigate to the **Settings** > **Extensions** page (or enter **chrome://extensions/** in the URL bar).
2. Select **Enable** next to Symantec Authentication Client Plugin Extension.

Pushing the Chrome Extension to a User's Machine

Use the Chrome ExtensionInstallForceList policy to push the Chrome extension to a user or group of users. This is usually required to install PKI Client for multiple users at one time, or if your policy is set to not allow PKI Client to be automatically installed.

If you use the Chrome ExtensionInstallForceList policy to install the Chrome extension on users' machines, the users will not be able to disable or delete the extension manually.

You will need the following for the ExtensionInstallForceList policy:

- 32-character extension ID for the Symantec Authentication Client Plugin Extension, as displayed in Developer Mode on the Chrome **Settings** > **Extensions** page (ahgdclgdhfeingghldkedleghekbfhef).
- The URL where the PKI Client crx file resides.

ExtensionInstallForceList Examples

- On Windows:

```
Software\Policies\Chromium\ExtensionInstallForcelist\1 = "ahgdcl
gdhfeingghldkedleghekbfhef;https://clients2.google.com/
service/update2/crx"
```

- On OSX:

```
<array>
<string>ahgdclgdhfeingghldkedleghekbfhef;https://clients2.google.
com/service/update2/crx"</string>
</array>
```

Installing Certificates on Android Devices

For the Android operating system, only PKI Client is required. If it is not already installed, the user is prompted to install PKI Client during certificate enrollment. Certificates are installed to the Android keychain. The certificate is then available to any application that consumes PKI certificates and that can access the keychain.

In Android 4.4 (Kit Kat) and later, the Android keychain is split into two key stores; one for Wi-Fi certificates and one for all other certificate uses (called **Wi-Fi** and **VPN and apps** , respectively). When a user enrolls for a certificate, PKI Client installs it in the correct key store. If the certificate is configured for use with both Wi-Fi and VPN, PKI Client installs the certificate in both key stores. In this scenario, advise the user to select the default settings when installing the certificate. If the user changes the Credential Use field from **VPN and apps** to **Wi-Fi**, the certificate will only be installed in the Wi-Fi key store and may not work for all certificate uses and with all applications.

Using PKI Client with an Authenticated Proxy

PKI Client allows users to access resources behind a proxy that uses Basic Authentication (that is, protected by a user name and password). However, your users must add the authentication credentials to PKI Client.

Before your users configure PKI Client, configure your proxy. If configured correctly, Internet Explorer should be able to access a website outside of your network without being asked for credentials.

Note: For Windows only: If you require an HTTPS connection through your proxy, you will need to allow revocation checking to use your proxy password (disabled by default). To allow this, you need to install the Microsoft Hotfix 915787 (http://support.microsoft.com/kb/915787) on your end users' machines.

Have your users complete the following steps to configure PKI Client to support an authenticated proxy:

1. In PKI Client, click **Advanced**.
2. Click **Proxy Authentication**.
3. Enter the proxy user name and password on the resulting Proxy credentials page.
4. Click **Submit**.

Appendix B

Registry and Configuration File Settings

This appendix includes the following topics:

About Registry and Configuration File Settings

Registry (Windows) and configuration file (Mac) settings are created when you install the PKI Client for the first time. The following topics describe each setting and the settings that an administrator can modify.

If an end user is connected to a domain, PKI Client does 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 need to 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)

Table B-1 lists the Symantec PKI Client autoenrollment settings.

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 autoenrollment certificates deleted on the console

Registry Settings for the Symantec CSP for Windows

The Symantec Cryptographic Service Provider (CSP) for Windows is used by applications such as Microsoft Outlook, Windows Logon, and Internet Explorer.

Table B-2 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 lists the CSP registry entries.

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. **Warning:** 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. **Warning:** 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. **Warning:** Do not modify this entry.
Type	DWORD	32-bit: 1	The CSP Provider Type (PROV_RSA_FULL) **Warning:** Do not modify this entry.

Registry Settings for Smart Card Logon for Windows

Microsoft Windows keeps a database of smart-card-to-CSP associations that are called the Calais database. This database is populated with the appropriate entries for the supported smart cards.

Table B-4 lists the smart card logon registry locations and entries.

Note: PKI Client does not add registry entries for security devices that are 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 lists the Smart Card logon registry entries.

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

Table B-5 Smart Card Logon Registry Entries *(continued)*

Registry Entry	Type	Description	Default Value
		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
ATRMask	BINARY	Mask applied to the ATR during identification for:	
		Aladdin eToken	ff,ff,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,ff
		CAC OCS 5.5	ff,ff,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,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,ff,ff
		PIV 3 OCS Cold	ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff
		PIV 3 OCS Warm	ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,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,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,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 lists the Symantec PKI Client registry locations.:

Table B-6 Symantec® PKI Client Registry Locations

Environment	Registry Location
32-bit machine	▪ HKEY_LOCAL_MACHINE\SOFTWARE\ Symantec\PKI Client\4 ▪ HKEY_CURRENT_USER\SOFTWARE\ Symantec\PKI Client\4
64-bit registry on 64-bit machine	▪ 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 lists the Symantec PKI Client registry settings.

Table B-7 Symantec PKI Client Registry Settings

Registry Entry	Type	Default Value	Description
CoreDirectory	STRING	32-bit: `C:\Program Files\Symantec\PKI Client` 32-bit (on 64-bit): `C:\Program Files (x86)\Symantec\PKI Client` 64-bit: `C:\Program Files\Symantec\PKI Client\`	The location of the Symantec PKI Client executable and application files. **Warning:** Do not modify this entry.
CoreList	STRING	(REG_MULTI_SZ)	The list of dll's to use with the machine-registered plug-in. **Warning:** 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\` 32-bit (on 64-bit): `C:\Program Files (x86)\Symantec\PKI Client\ Console\` 64-bit: `C:\Program Files (x86)\ Symantec\PKI Client\ Console\`	The path to the user console applications. **Warning:** Do not modify this entry. This registry setting is not available in the HKCU keys.
CSP	STRING	Symantec PKI Client CSP	The CSP that the Symantec PKI Client Utility associates with certificates. **Warning:** 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. **Warning:** Do not modify this entry. 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
ModuleDirectories	STRING	32-bit: `C:\Program Files\Symantec PKI Client\Modules` 32-bit (on 64-bit): `C:\Program Files (x86)\Symantec\PKI Client\Modules\` 64-bit: `C:\Program Files\Symantec\PKI Client\Modules\`	Location of additional Symantec modules (format is a semi-colon separated list of directories). **Warning:** Do not modify this entry.
/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.

Table B-7 Symantec PKI Client Registry Settings *(continued)*

Registry Entry	Type	Default Value	Description
/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.
/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.

Table B-7 Symantec PKI Client Registry Settings *(continued)*

Registry Entry	Type	Default Value	Description
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\` 32-bit (on 64-bit): `C:\Program Files (x86)\Symantec\PKI Client\DSM\` 64-bit: `C:\Program Files\Symantec\PKI Client\DSM\`	Location of additional Symantec modules (format is a semi-colon separated list of directories). **Warning:** Do not modify this entry.
SoftwareTokenEnabled	DWORD	1	Controls whether the Software Certificate Store (virtual tokens) are enabled for users. 0 - disabled 1 - enabled

Table B-7 Symantec PKI Client Registry Settings *(continued)*

Registry Entry	Type	Default Value	Description
AllowTrayRegLogon	DWORD	0	**Note:** 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.
AllowTrayUnblock	DWORD	0	**Note:** 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.

Table B-7 Symantec PKI Client Registry Settings *(continued)*

Registry Entry	Type	Default Value	Description
CacPreference	DWORD	1	**Note:** 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	**Note:** 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.

Table B-7 Symantec PKI Client Registry Settings *(continued)*

Registry Entry	Type	Default Value	Description
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.

If you use GPO to manage PKI Client deployment to end user machines, you need to disable Live Update

Table B-8 lists the Symantec PKI Client Live Update registry locations.

Table B-8 Symantec PKI Client Live Update Registry Locations

Environment	Registry Location
32-bit machine	HKLM\SOFTWARE\Symantec\PKI Client\4\Features\LiveUpdate\
4-bit machine6	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 lists the PKI Client Live Update registry locations.

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\` 32-bit (on 64-bit) (X86 Registry): `C:\Program Files (x86)\Symantec\PKI Client\LUE\`	Directory where LUE components are installed. **Warning:** Do not modify this entry.
Host	STRING	liveupdate.symauth.com	The host to use for liveupdate connections. **Warning:** Do not modify this entry.
Language	STRING	SymAllLanguages	The language registration to use with LiveUpdate. **Warning:** 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` 64 bit: `Symantec PKI Client x64`	The product name in Live Update. **Warning:** Do not modify this entry.
ServiceDisabled	DWORD	0x00	Controls whether LiveUpdate is enabled or disabled. 0x00 - On 0x01 - Off (default)

Table B-9 Symantec PKI Client Live Update Registry Locations *(continued)*

Registry Entry	Type	Default Value	Description
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. **Warning:** 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.

Table B-10 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 lists the CSP and KSP registry entires.

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.

Table B-12 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 lists the Symantec Threading Library registry entries.

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. **Warning:** 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 configuration settings are found in a flat file:

Table B-14 lists the Mac configuration settings locations.

Table B-14 Mac Configuration Settings Locations

Setting	Configuration File
System-level settings	/etc/tblive-4/tblive.rat
User-level settings	/Users/{username]/.tblive-4/tblive.rat

Appendix C

Troubleshooting PKI Client

This appendix includes the following topics:

About Troubleshooting the PKI Client

There are a number of common end-user problems that may occur with Symantec PKI Client. Typically you need to gather information before you can resolve these issues.

About Logging

PKI Client logging is enabled by default. Logging writes to a set location and automatically cleans up logs according to a schedule. Any logs that are older than two weeks are automatically compressed. Logs are kept for the current and previous calendar year while others are deleted. PKI Client stops logging when disk space drops below 100MB.

Note that most of these settings can be configured for users' machines using a GPO.

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

The following types of logging are enabled by default for the Symantec PKI Client:

- PKI Client logging, which includes CSP, PKCS#11, client process, and KSP logging.
  See "PKI Client Logging" on page 55.
- Post-processing logging.
  See "Post-processing Logging" on page 55.

Additionally, you can write installation events to a log file during the installation process.

See "Installation Logging" on page 56.

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

PKI Client Logging

PKI Client writes logs that include 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 captures any errors that occur as a result of running a script. The log include one line per error that has occurred.

The following information appears in the log:

- Date and time that the error occurred
- Complete path to the script that caused the error to occur
- Name of the script that caused the error to occur

On a PC, this error log is written to <user profile>`/App Data/Local/PKI Client/4`. It only appears if the script causes an error to occur. The user who runs 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`. It only appears if the script caused an error to occur. The user who runs the script must have appropriate permissions to write to this location.

See *Symantec PKI Client Writing Post-processing Scripts Guide* for more information on how to write custom scripts.

Installation Logging

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

Logging Events During an End User Installation

If you want to log installation events during an installation of a PKI Client as an end user on a single end-user machine, you must install the PKI Client with the **/Log** and **/Logfile** options.

For example:

```
Symantec-PKI-Client-2.15.x.exe /Log /Logfile bootstrap.log
/ComponentArgs x86:"/l*vx msi_x32.log" /ComponentArgs x64:"/l*vx
msi_x64.log"
```

This command 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 also generates 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 displays the information rather than just in the log file.

Logging Events During a GPO User Installation

To log installation events during a GPO installation of PKI Client

1. Go to **Administrative Tools > Active Directory Users and Computers** to right-click the name of your domain and then 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**.
5. In the Logging box, enter the options that you want to log.
6. Enter **voicewarmupx-** for full logging.

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

Server Access Requirements

PKI Client requires access to the following external servers. If you experience errors or connectivity issues with certificate lifecycle operations, verify that PKI Client has access to these servers (for example, that firewalls do not restrict this access).

Table C-1 Server access requirements

Server Access	Symantec URL
PKI Client LiveUpdate server This is the server that provides updates to PKI Client through the LiveUpdate feature. Access to these servers is required if LiveUpdate is enabled.	http://liveupdate.symantec.com
PKI Certificate Services server This server hosts the set of pages that an end user accesses to enroll for certificates. This server also hosts the file download service which is required for default post-processing.	https://pki.symauth.com/certificate-service
PKI Certificate Services CRL server This server hosts the CRL-based certificate status checking site configured for the PKI Certificate Services site. Access to this server is required if CRL services are configured.	http://sr.symcb.com/sr.crl
PKI Certificate Services OCSP server This server hosts the OCSP-based certificate status checking site configured for the PKI Certificate Services site. Access to this server is required if OCSP services are configured.	http://sr.symcd.com
RA server This is the Registration Authority server.	https://pki-ra.symauth.com
RA server CRL server This server hosts the CRL-based certificate status checking site configured for the RA server.	http://sr.symcb.com/sr.crl

Table C-1 Server access requirements *(continued)*

Server Access	Symantec URL
RA server OCSP server This server hosts the OCSP-based certificate status checking site configured for the RA server.	http://sr.symcd.com
Policy signing certificate CRL and OCSP servers This server hosts the certificate status checking sites configured for the policy signing certificate site.	http://pki-ocsp.symauth.com http://pki-crl.symauth.com
End-user certificate CRL and OCSP servers This server hosts the certificate status checking sites configured for the end-user certificates you issue.	http://pki-ocsp.symauth.com http://pki-crl.symauth.com

Troubleshooting Common Problems

Table C-2 lists common problems that end users may experience when they install and use PKI Client, as well as their solutions, if applicable.

Table C-2 Common problems and solutions for PKI Client

Problem	Solution
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 indicates that 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 that is plugged in and certificates that appear 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.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
An end user's certificate shows up for smart card logon, but logon fails.	Make sure that the end user's workstation has been joined to the domain and that the user's workstation points the DNS to a domain controller. Also, you need to search in the event log of the domain controller for any Kerberos errors that indicate why the certificate has been 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 that the PIV/CAC smart card was used for Windows logon. If the user logs in with username and password, smart card removal does not have any effect. If the end user runs Windows Vista or Windows 7, you need to make sure that the Smart Card Removal Policy service is started. Otherwise the smart card removal policy setting does not work.
The end user's certificates are not propagated to the user certificate store when the card is inserted.	Make sure that the PKI Client process, PKIClientAgent, runs 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 or replacing these certificates. If you issue certificates through 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.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
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 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. It enforces the requirements of the Certification Practices Statements that apply to these types of certificates, as shown at the following location: https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf It is the expected behavior.
Users get an Unexpected Error when PKI Client attempts to enroll for certificates on smart cards using 3rd-party CSPs.	This issue typically occurs if the user's smart card or token uses a 3rd-party cryptographic service provider (CSP) and the token or smart card is full. The 3rd-party CSP prevents PKI Client from deleting certificates from the token or smartcard during enrollment, even if the **Make space for certificates** option is enabled for the certificate profile in PKI Manager. The user must manually delete one or more certificates using PKI Client.
Users get an authentication error (401: Unauthorized) when PKI Client attempts to autoenroll for certificates.	This issue occurs if the fully-qualified Domain Name (FQDN) for your PKI Enterprise Gateway machine is not trusted by the end user's computer. Then you must use a GPO push to add the FQDN to the **Internet Settings > Intranet Security Zone** (or have the user add the FQDN). Alternatively, you can use the Netbios name of the machine that hosts the PKI Enterprise Gateway for the Gateway URL when you configure the PKI Enterprise Gateway.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
Users get an Error Code 193 when installing certificates.	This issue occurs when you run post-processing scripts. These scripts depend on 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 occur.
Overriding default post-processing scripts	By default, PKI Client runs pre-defined scripts each time that a user enrolls for 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 be able to view a system prompt that notifies them about this issue. ■ RegisterFirefox.signed.bat This script installs the certificate and its chain into Firefox, and if necessary, registers the PKCS11 module. If Firefox runs on users' computers when this script is run, they may be able to view a system prompt that notifies 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 when post-processing is invoked for those profile, the modified scripts are then downloaded and stored for future use.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
PKI Client is not available in Chrome or Firefox	If a user installs PKI Client in Chrome or Firefox and does not enable the Symantec Authentication Client Plugin Extension when prompted, PKI Client will not be available to manage certificates. This issue also occurs if a user installs Firefox after installing PKI Client. In these situations, the user must manually enable the extension in the browser: ■ In the Chrome browser, navigate to the Settings > Extensions page and select **Enable** next to Symantec Authentication Client Plugin Extension. ■ In the Firefox browser, click the **Firefox** button and click **Add-ons** to open the Add-on Manager. Select the **Extensions or Appearance or Plugins** panel, and click **Enable** next to Symantec Authentication Client Plugin Extension. You may need to restart the browser.
When using the Microsoft Base Smart Card Crypto Provider to perform intensive operations such as decrypting a vToken, the operation can briefly use close to 100% of the computer's CPU resources.	This is a known issue with the Microsoft Base Smart Card Crypto Provider. However, the operation will release the CPU resources after a few moments.
For some new enrollments using PKI Client with middleware clients (such as some instances using SafeNet tokens) the token fails to initialize.	This is likely because of an incorrect PIN. Users of SafeNet tokens or other middleware need to reference their vendor's user documentation for proper procedures and PIN information to ensure successful initialization. Symantec does not document the processes for third-party tools.
If a user inserts an Aladdin token with an Adobe signing certificate on it and does not have Adobe running, they will not be prompted to restart Adobe.	This occurs because post-processing only runs once per certificate. Ensure Adobe is running before a smart card is inserted with an Adobe signing certificate on it for the first time, or restart Adobe manually after adding an Adobe signing certificate.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
If you change your password when using a vToken, and then use that token to access a different network using the new password, the vToken appears corrupted.	There is no workaround to this issue.
When using Chrome to enroll for certificates on third-party tokens, the user may receive inconsistent PIN prompts. When enrolling to a third-party token, after selecting **Install certificate** on the final page of the enrollment flow, Chrome will minimize itself, and a prompt will ask for the token's PIN. After entering the PIN and confirming the prompt, Chrome does not show itself again; it remains docked.	This is a limitation of the Chrome browser. To see the results of the enrollment, the user must expand the Chrome window manually.
PKI Client does not add intermediate and root CAs as part of the post-processing for third-party CSPs by default.	This is as designed. You must manually use the certutil tool to add intermediate and root CAs as part of the post-processing for third-party CSPs.
PKI Client has intermittent issues with reading eTokens in Mac OS X when you insert a token and it kicks off as a background process.	To avoid this issue, do not remove or insert tokens while other processes are taking place. If you encounter issues, try again.
PKI Client may displays theerror message: "This webpage wants to run the 'Control name is not available'... add-ons" on the enrollment and renewal pages. This warning sometimes appears on the certificate profiles and enrollment methods on Win8/IE10 and Win7/IE9, but may appear on all the certificate profiles.	There is no workaround for this issue.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
When trying to import a certificate intended for a third-party CSP token to the vToken, you are prompted that this certificate needs to be imported to a CSP token; however, it displays the icon for a SafeNet token.	There is no workaround for this issue. However, functionality is not impaired.
In PKI Client, a modal dialog sometimes appears that warns about the use of dangerous add-ons; however, the enrollment was already done at this point.	There is no workaround for this issue. You can safely ignore this message.
In Windows 7, if you reset the file association for a downloaded batch of certificates, it does not change the icon back as it should.	There is no workaround for this issue. However, functionality is not impaired; the file will be processed correctly when double-clicked.
PKI Client's batch scripts depend on the base Windows utilities, like find.exe, being in the PATH – so if you have, for instance, Cygwin or MinGW/MSYS installed and their find.exe is in the path before the Windows version, you may receive errors in post-processing. Additionally, PKI Client may throw the error 193 when trying to register with Firefox.	Make sure the base Windows utilities are in the PATH before any third-party applications.
When a user deletes an auto-enrolled certificate, PKI Client does not prompt the user to re-enroll for the certificate. It also does not inform the user that deleting a certificate from the PKI Client does not revoke it--that it should be revoked as well as deleted.	You must educate your users to revoke certificates after deleting them. Additionally, you must educate your users to re-enroll for a deleted certificate if a replacement certificate is necessary.
If an end user attempts to access an enrollment link for an Android-based certificate on a non-Android device on which PKI Client is not installed, the enrollment page will prompt to install PKI Client, rather than present an error message.	There is no workaround for this issue; however, correct error messages will appear if an end user attempts to continue with PKI Client installation and certificate enrollment.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
If a user running Windows 8.1 (64-bit) attempts to install an earlier version of PKI Client, the user will be prompted to uninstall the current version, and may then receive the error, "This action is only valid for products that are currently installed."	There is no workaround for this issue.
Users manually upgrading PKI Client will see a "Files in Use" dialog box. Clicking Retry will not continue the upgrade. The user must click Ignore to continue the upgrade. This will require that the user restart the computer after the upgrade is complete.	The user must click **Ignore** and restart the computer after the upgrade is complete. Alternatively, the administrator can push the upgrade to the user's computer.
Some of the custom script templates available in PKI Manager have incorrect line breaks, which might adversely affect PKI Client post-processing.	Ensure that you correctly format the custom scripts you upload to PKI Manager. Detailed instructions are available in *Symantec™ PKI Client Writing Post-processing Scripts Guide*, available in the **Resources** page of PKI Manager.
If users set their browsers to block the PKI Client renewal plug-in, PKI Client will fail any operation that uses the plug-in.	This is by design. Notify users to enable PKI Client and its plug-ins in their browsers.
In rare circumstances, PKI Client may hang if certificate enrollment is performed on a new machine and with an Aladdin token that already contains certificates.	There is no workaround for this issue; however, this is a rare occurrence.
The Chrome browser has deprecated NPAPI plug-ins, breaking backwards compatibility with PKI Client. Versions of PKI Client prior to v2.11 will not work with the Chrome browser.	There is no workaround for this issue. Users should update to the latest PKI Client v2.11 or use another supported browser.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
During certificate enrollment using Chrome, if the user has PKI Client installed but not the PKI Client extension for Chrome, and the user clicks Download before the page has completely loaded, the user is prompted to install PKI Client.	Users need to manually install the PKI Client extension for Chrome from the following link: https://chrome.google.com/webstore/detail/ahgdclgdhfeingghldkedleghekbfhef Once the user has added the extension, a confirmation message is displayed on the browser.
PKI Client shows two views of the same physical token: eToken Pro (displayed by PKI Client) and Security Device (displayed by the SafeNet Authentication Client). If a user resets the token using the eToken Pro view, the token will be reset, including the FIPS State. The token will no longer be FIPS 140-2 compliant, and should no longer be used for enrollments that require the 3rd party CSP with FIPS compliance.	This is by design. Always have the user reset the token using the FIPS initialization option of the SafeNet Authentication Client.
Users running PKI Client may experience stability issues on OSX 10.10. Additionally, OSX 10.10 will not recognize smart cards in PKI Client. As a result, any application (such as Mail or Outlook) that depends on PKI Client to access or store certificates on smart cards will not work.	PKI Client does not support OSX 10.10. Users should continue to use a supported platform. Refer to *PKI Client Administrator's Guide* or the latest Managed PKI Release Notes for a list of the currently supported platform and browsers. Both are available from the **Resources** page in PKI Manager.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
If a user's smart card or token is full and you have enabled the Make space for certificates option for a certificate profile using PKI Client, then PKI Client will delete the oldest certificate issued by the certificate profile to make room for a new certificate enrollment. However, if the smart card or token uses a 3rd-party cryptographic service provider (CSP), PKI Client will be unable to delete any existing certificates, and the enrollment will fail with an "Unexpected Error".	This is a limitation of the 3rd-party CSP. Have the user verify that the smart card or token is full. If so, the user must manually delete one or more certificates using PKI Client.
ActivIdentity has removed their CSP from their clients starting with version 7.0.2. Versions of this client starting with 7.0.2 use the Microsoft Base CSP, instead. If a user updates their ActivIdentity client to 7.0.2 or newer, the ActivIdentity CSP will no longer be installed. As a result, there is no guarantee that certificates will continue to work. Also, users cannot renew existing certificates, as the renewal process requires the missing CSP.	Users can continue to use ActivIdentity client version 6.2 without any issues. Administrators for users that upgrade their ActivIdentity client to 7.0.2 must create a new profile in PKI Manager that specifies the Microsoft Base Smart Card Provider as the CSP. The user will need to re-enroll for their ActivIdentity certificates with the new profile.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
If a user tries to authenticate to a Radius-authenticated Wi-Fi network (WPA-2 Enterprise) with a Client Authentication certificate issued by Managed PKI, the connection will fail if the user does not trust the Radius server's certificate. The Authentication Certificate authenticates the user to the radius server, but the user's computer or device must also trust the server certificate in order to authenticate the server to the user's computer.	Use one of the following methods to make sure that the Radius server certificate is trusted on the user's machine: ■ Use a certificate on your server machine that chains up to a public root (this assumes that your users' machines have the public root installed). ■ Push the server certificate out to the users' machines or devices by another means (for example, if the certificate is a domain root, you can send it to domain-joined machines using a group policy r provide it to the user to manually install). ■ Use a post-processing script to install the root certificate through PKI Client. The user will be prompted to trust the certificate. ■ On Windows, set the Wi-Fi profile to allow prompting for new servers (not recommended, as Windows does not check the validity of the root certificates).
If users have installed the PKI Client extension in Firefox but have disabled it, they will be repeatedly prompted to install the extension during certificate enrollment on that browser. If the extension is disabled, the enrollment process will not see the extension, and cannot enable the extension or install over it.	Users will need to manually enable the extension to continue the enrollment on the Firefox browser: 1 Enter about:addons in the URL bar. 2 Click **Extensions** in the left pane. 3 Click **Enable** next to **Symantec Authentication Client Plugin Extension**.
If the administrator has set the certificate profile to prohibit downloading PKI Client but the user already has PKI Client installed without the Firefox extension, the user will not be able to download the extension on a Firefox browser. As a result, the user will not be able to obtain the certificate.	Do one of the following to correct this issue: ■ Set the certificate profile to allow PKI Client to be downloaded. ■ Have the user manually install the extension by accessing the following link in Firefox: https://browser-extension.symclab.com/auth-client/firefox/symantec-auth-client-extension.xpi ■ Have the user obtain the certificate on another supported browser.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
Because of changes in the Mozilla Firefox browser, you might experience issues logging into a website using the latest version of PKI Client. This typically occurs if you have upgraded to the latest version of PKI Client and: ■ This is the first time that you have used PKI Client on the Firefox browser to log into a website; or, ■ You have not previously enrolled for a certificate on the Firefox browser with this version of PKI Client.	You will need to manually install the Firefox extension for PKI Client: 1 From your Firefox browser, click this link: https://browser-extension.symclab.com/auth-client/firefox/symantec-auth-client-extension.xpi 2 Follow the prompts to install the extension. 3 You can verify the extension was installed: ■ Enter about:addons in the URL bar. ■ Click **Extensions** in the left pane. You should see **Symantec Authentication Client Plugin Extension** in the list of extensions. If the extension is disabled, click **Enable** next to it.
With users running PKI Client with Managed PKI 8.12 or earlier, if a post-processing script error occurs, PKI Client will roll back the enrollment. However, Managed PKI will not know that the enrollment was rolled back, and expects that the certificate was issued. With users running PKI Client with Managed PKI 8.13 or later, if a post-processing script error occurs, PKI Client reports the failure to the user, but does not roll back the enrollment.	With users running PKI Client with Managed PKI 8.12 or earlier, correct the post-processing error. Then, have the user enroll for a new certificate. With users running PKI Client with Managed PKI 8.13 or later, correct the post-processing error. Then, have the user re-run the post-processing script by enabling Diagnostics Mode in the PKI Client Console, and clicking Re-run certificate configuration for the certificate.
Due to recent changes made to the Safari browser, users are being asked to trust any plug-ins they use. As a result, users will be prompted to trust the Symantec PKI Client plug-in when performing cryptographic operations such as enrolling for certificates.	Symantec recommends that users trust Symantec plug-ins when prompted. Otherwise, users will continue to be prompted any time they use these plug-ins.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
If an end user is connected to a domain and uses PKI Client to import a certificate or enroll or renew a certificate through the Symantec user store, and the certificate profile is configured to publish to the Active Directory, the certificate will be added for the user connected to the domain, regardless if the certificate is valid for the user. Refer to ID number artf108210 if you call Customer Service about this issue.	Ensure that the certificate being acted upon belongs to the user logged into the domain.
If an end user manually uninstalls PKI Client while other users are logged in the background, the PKI Client process will only stop for the user performing the uninstall.	Log off all users before attempting to uninstall PKI Client.
If an end user manually clicks the link to run LiveUpdate multiple times, multiple LiveUpdate instances open.	There is no workaround for this issue; however LiveUpdate will continue to update correctly. Have the end user close any extra LiveUpdate instances.
If end users with three or more certificate stores in PKI Client (including My Computer, vtokens, or physical tokens/smart cards) attempt to perform a certificate operation on Firefox, they may be prompted for a PIN for one certificate store, when actually using a different certificate store.	This is a known issue with Mozilla Firefox. There is no workaround for this issue.
If an end user has an Aladdin token that is full, and space cannot be made during PKI Client-based autoenrollment, the enrollment will fail with the error code F011.	Have the end user delete unnecessary certificates from the token using PKI Client and let PKI Client retry the operation.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution

If an end-user machine adds a server-side certificate for the endpoint to its private certificate information store and the certificate is not yet trusted by that store, the CheckPoint post-processing will try to query the user on the console if they want to trust the certificate.
 	
However, the PKI Client console is not displayed to the end user in this instance, so the end user cannot trust the certificate.
	There are two solutions for this issue:
	
	■ Configure the post-processing script to trust the CA certificate when the script is run:
	  ■ Download the CheckPoint VPN Configuration post-processing script template from PKI Manager and make any changes to the template required for your environment.
	  ■ In the template, change the line: `"%InstallPath%\trac.exe" create -s "%SiteName%" -a "certificate"` to `ECHO Y | "%InstallPath%\trac.exe" create -s "%SiteName%" -a "certificate"`
	  ■ Upload the revised post-processing script to the certificate profile.
	■ Configure the post-processing script to display a command prompt to the end user and have the end user explicitly set the CA certificate as trusted:
	  ■ Download the CheckPoint VPN Configuration post-processing script template from PKI Manager and make any changes to the template required for your environment.
	  ■ In the template, change the line: `"%InstallPath%\trac.exe" create -s "%SiteName%" -a "certificate"` to `start /wait "%InstallPath%\trac.exe" create -s "%SiteName%" -a "certificate"`
	  ■ Upload the revised post-processing script to the certificate profile.

Table C-2 Common problems and solutions for PKI Client *(continued)*

Problem	Solution
Users will see issues if they attempt to integrate certificates in the keychain with applications that do not support certificates in the keychain. For example, the version of the email client provided on some Android devices does not support the use of certificates in the keychain. As a result, when trying to set up ActiveSync, users with these clients are prompted to choose a PKCS#12 file from the device, rather than choosing a certificate from the keychain.	Use an application that supports certificates in the keychain. For example, download and install the most recent version of the Android email client.

Index

Q

R

S

T

U

V

W