Symantec™ Managed PKI®

Integration Guide for AirWatch® MDM Solution

Symantec™ Managed PKI® Integration Guide for AirWatch® MDM Solution

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

Last updated May 1, 2013

Legal Notice

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

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/contact/index.html#support4

Contents

Integrating Symantec Managed PKI Certificates with AirWatch MDM Solution

The enterprise workplace has moved beyond the walls of the organization into a global, mobile environment. To maintain productivity, your end users need to access company resources using a mobile platform. However, you need to be able to trust the end users accessing your systems, and the mobile device they use, no matter if you have provided their devices or if they are using their own mobile devices.

Symantec Managed PKI's digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from a few to thousands of devices, and its in- the-cloud solution provides quick deployment and easy management while also offering Symantec's industry leading security that is unmatched by in-house PKI solutions.

This document is intended for customers who have chosen AirWatch as their preferred MDM vendor. It provides information about configuring Managed PKI to issue end-entity certificates to mobile devices for client authentication, secure email (S/MIME), and MDM support using Web Services or Simple Certificate Enrollment Protocol (SCEP). For instructions on configuring your AirWatch MDM solution to provide these certificates to your users, refer to *AirWatch Integration with Symantec Managed PKI Guide*, available from AirWatch, or from Symantec's Knowledge Center at https://knowledge.verisign.com/support/mpki-support/index?page=content&id=SO22025&actp=search&viewlocale=en_US.

Partner Information

This integration is supported on Managed PKI 8.x with the following partner platforms.

Table 1-1 Partner Information

Partner Name	AirWatch®
Product Name	AirWatch® MDM solution 6.0 and higher
Device (for certificate enrollment and installation)	iOS, Android

Integration Architecture

The following diagram describes how AirWatch MDM solution integrates with Managed PKI.

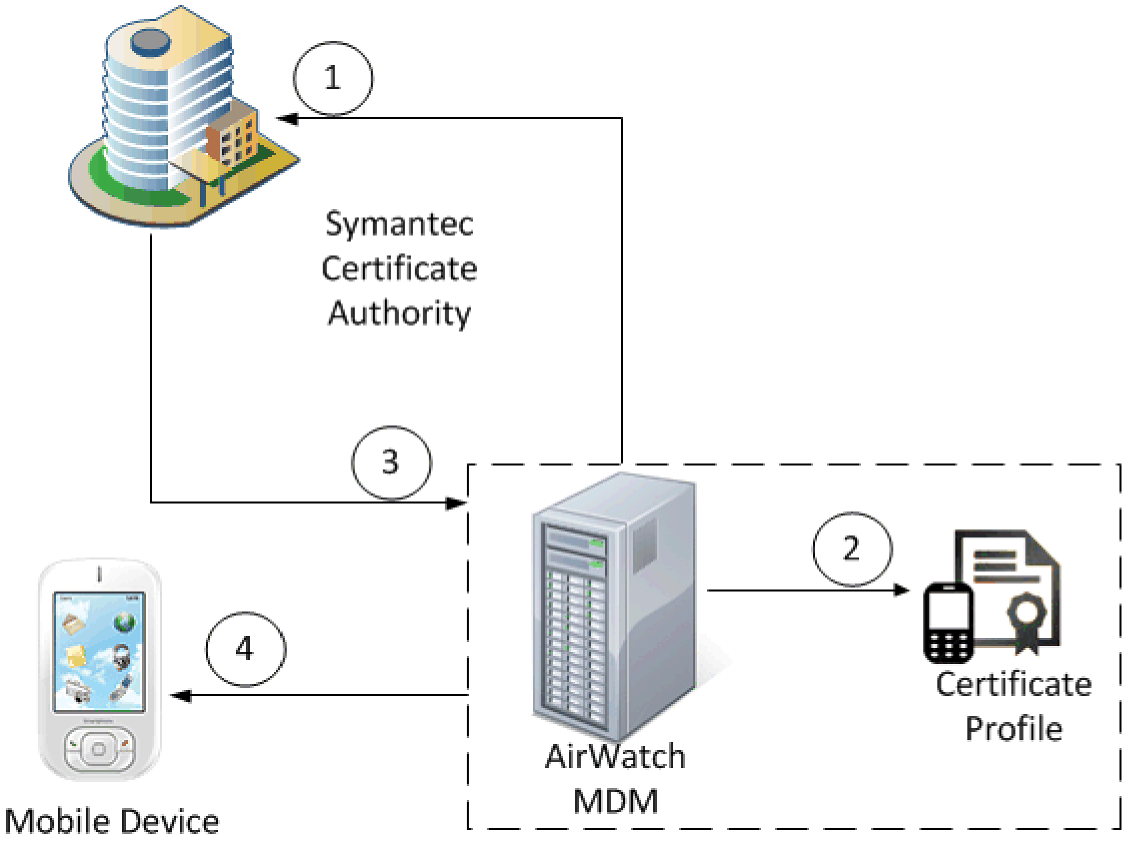


Figure 1-1 AirWatch MDM interaction with Managed PKI

1. AirWatch MDM communicates with Symantec Certificate Authority to generate an Registration Authority (RA) certificate.
2. Create a Certificate Template corresponding to the profile created in Managed PKI 8.x.
3. Get a certificate from Symantec Certificate Authority using PKI or SCEP for configuring Active Sync, VPN, or Wi-Fi payload.
4. AirWatch MDM will deploy the certificate profile to the mobile device.

Prerequisites

These procedures assume you have access to a Managed PKI 8.x account and AirWatch MDM solution 6.0.

Integration Workflow

The following diagram describes the general steps required to set up the Managed PKI account and integrate Managed PKI certificates with AirWatch MDM.

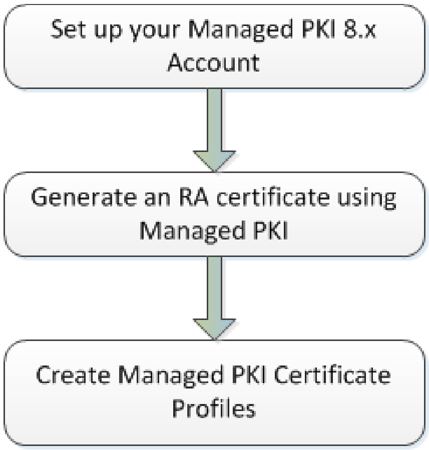

Set up your Managed PKI 8.x Account
Generate an RA certificate using Managed PKI
Create Managed PKI Certificate Profiles

Figure 1-2 Managed PKI and AirWatch integration workflow

Task 1. Set up your Managed PKI 8.x account

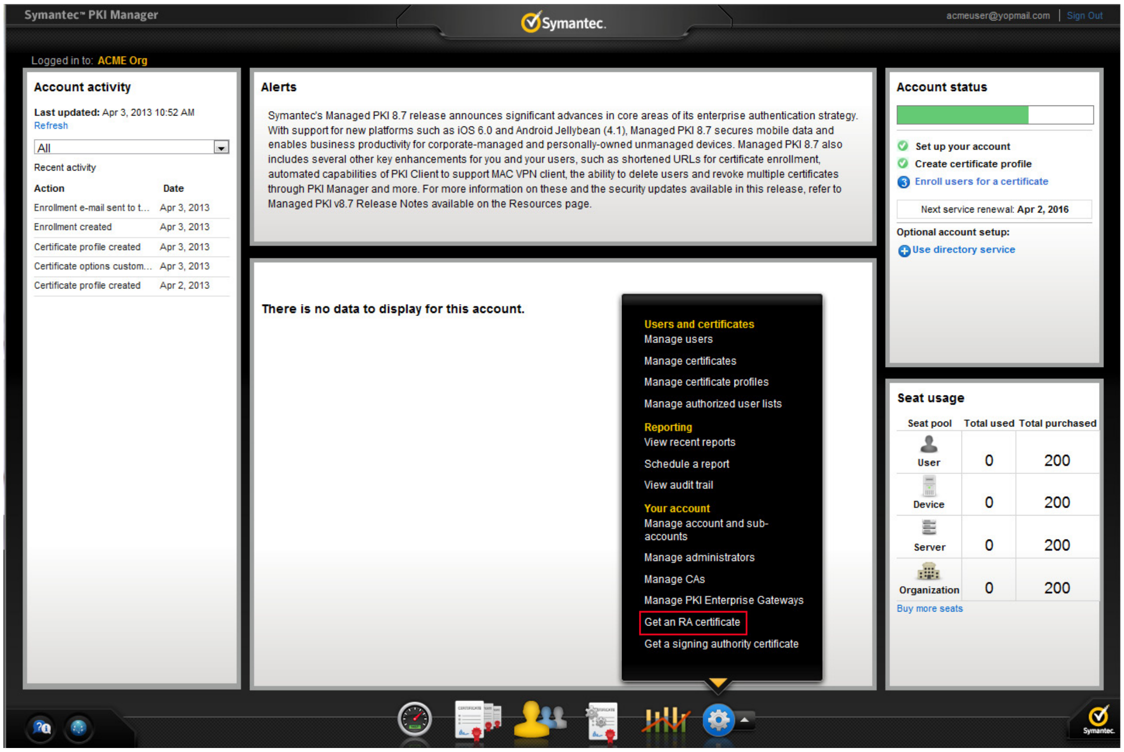
Contact your Symantec Sales representative to set up your Managed PKI account. Your representative will provide you with the necessary information to begin defining your account and certificate profile.

- You will need to complete and return the following documents. As needed, your Symantec representative will assist you with obtaining and completing these forms.
  - Master Service Agreement
  - Issuing Authority Naming Application (also known as the CA Naming Document)
  - Symantec Services Order Form
  - Purchase Order, credit card, or reference number
- You will need to obtain your initial Managed PKI administrator ID, which is your credential to access your Managed PKI account. Your Symantec representative will assist you with obtaining your Managed PKI administrator ID. You will use your Managed PKI administrator ID to log into PKI Manager, configure your Managed PKI account, and obtain your RA certificate. For more information on configuring Managed PKI, refer to PKI Manager and its online help.

Task 2. Generate an RA certificate using Managed PKI

For AirWatch MDM to communicate with Managed PKI, you must generate an RA certificate.

1. Generate a Certificate Signing Request (CSR) on any local machine. Instructions to generate a CSR vary between operating systems.
   - For generating a CSR on Windows, refer to http://support.microsoft.com/kb/295281
   - For generating a CSR on Linux, refer to http://www.trustis.com/pki/fpsia/guide/ssl-server/csr/apache_redhat.htm
   - For generating a CSR on Mac, refer to http://support.apple.com/kb/HT3976
2. After you generate a CSR, store the CSR on the local machine.
3. Log into Managed PKI's PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.
4. On PKI Manager, click the **Tasks** menu on the bottom navigation bar and select **Get an RA certificate** in the expanded menu.



Account activity

Last updated: Apr 3, 2013 10:52 AM
Refresh

All

Recent activity

Action	Date
Enrollment e-mail sent to t...	Apr 3, 2013
Enrollment created	Apr 3, 2013
Certificate profile created	Apr 3, 2013
Certificate options custom...	Apr 3, 2013
Certificate profile created	Apr 2, 2013

Alerts

Symantec's Managed PKI 8.7 release announces significant advances in core areas of its enterprise authentication strategy. With support for new platforms such as iOS 6.0 and Android Jellybean (4.1), Managed PKI 8.7 secures mobile data and enables business productivity for corporate-managed and personally-owned unmanaged devices. Managed PKI 8.7 also includes several other key enhancements for you and your users, such as shortened URLs for certificate enrollment, automated capabilities of PKI Client to support MAC VPN client, the ability to delete users and revoke multiple certificates through PKI Manager and more. For more information on these and the security updates available in this release, refer to Managed PKI v8.7 Release Notes available on the Resources page.

There is no data to display for this account.

Account status

✓ Set up your account
✓ Create certificate profile
3 Enroll users for a certificate

Next service renewal: **Apr 2, 2016**

Optional account setup:
Use directory service

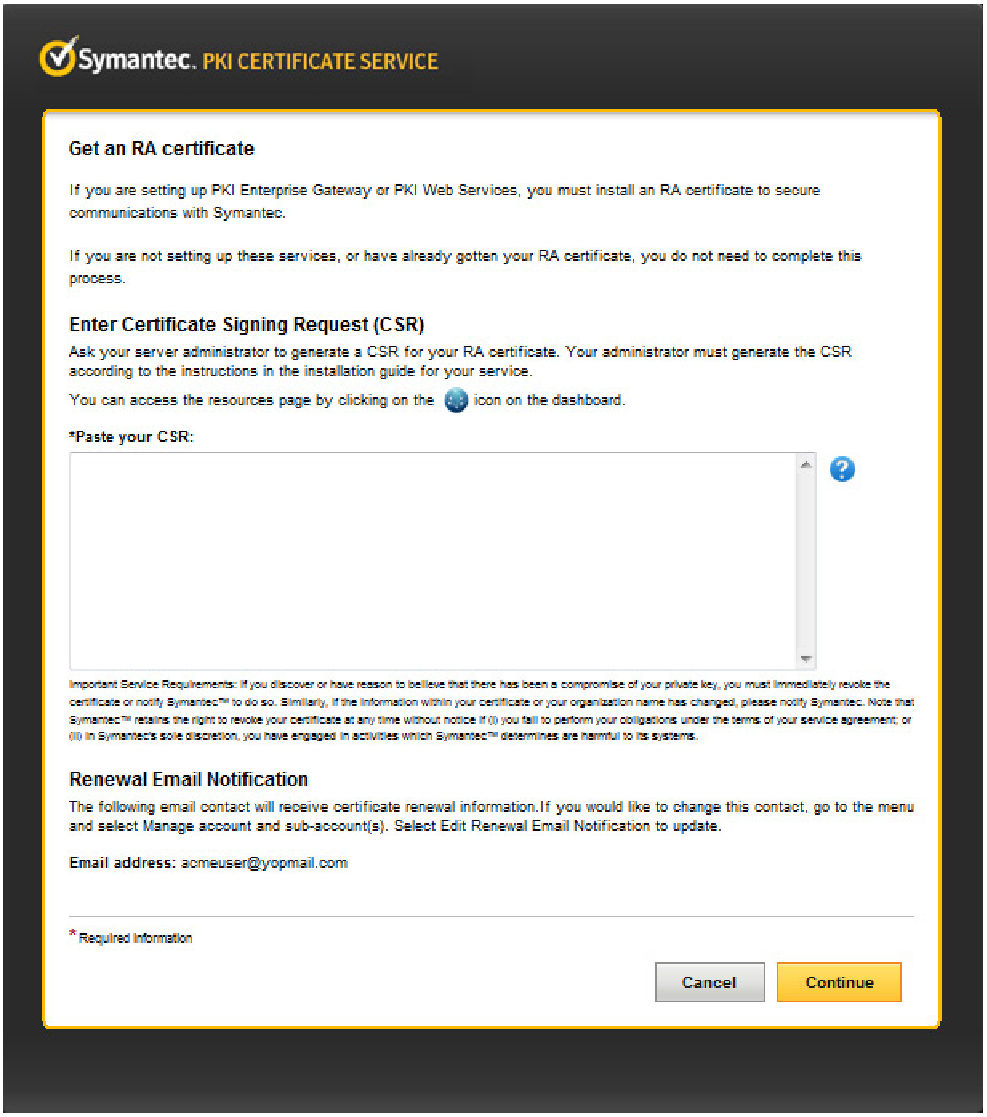
Seat usage

Seat pool	Total used	Total purchased
User	0	200
Device	0	200
Server	0	200
Organization	0	200

Buy more seats

Figure 1-3 Get an RA certificate

5 Paste the CSR that you generated in Step 1 in the **Enter Certificate Signing Request (CSR)** text box.



Get an RA certificate

If you are setting up PKI Enterprise Gateway or PKI Web Services, you must install an RA certificate to secure communications with Symantec.

If you are not setting up these services, or have already gotten your RA certificate, you do not need to complete this process.

Enter Certificate Signing Request (CSR)

Ask your server administrator to generate a CSR for your RA certificate. Your administrator must generate the CSR according to the instructions in the installation guide for your service.

You can access the resources page by clicking on the icon on the dashboard.

*Paste your CSR:

Important Service Requirements: If you discover or have reason to believe that there has been a compromise of your private key, you must immediately revoke the certificate or notify Symantec™ to do so. Similarly, if the information within your certificate or your organization name has changed, please notify Symantec. Note that Symantec™ retains the right to revoke your certificate at any time without notice if (i) you fail to perform your obligations under the terms of your service agreement; or (ii) in Symantec's sole discretion, you have engaged in activities which Symantec™ determines are harmful to its systems.

Renewal Email Notification

The following email contact will receive certificate renewal information.If you would like to change this contact, go to the menu and select Manage account and sub-account(s). Select Edit Renewal Email Notification to update.

Email address: acmeuser@yopmail.com

* Required Information

Figure 1-4 Paste your CSR

6 Click **Continue** to generate a `.cer` file.

7 Follow the instructions to generate the RA certificate and export the certificate as a `.pfx` file.

8 The `.pfx` file is the RA certificate that the AirWatch MDM will use to communicate with Managed PKI 8.x. For more information on installing the RA in your AirWatch MDM solution, refer to *AirWatch Integration with Symantec Managed PKI Guide*, available from AirWatch, or from Symantec's Knowledge Center at https://knowledge.verisign.com/support/mpki-support/index?page=content&id=SO22025&actp=search&viewlocale=en_US.

Create Managed PKI Certificate Profiles

You create certificate profiles in Managed PKI's PKI Manager. The certificate profile defines the type of certificate that will be issued to an end user. The certificate issued can be used on any supported mobile device. Managed PKI 8.x has been tested for the following certificate types:

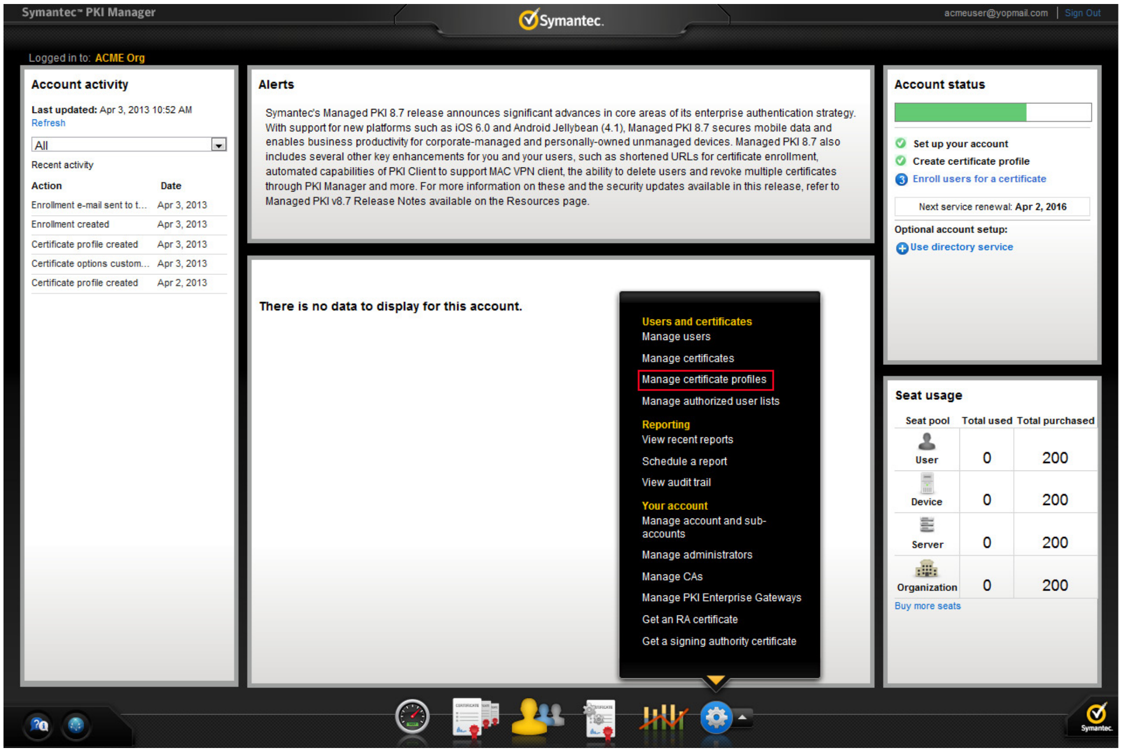
- Client authentication - Issues certificates that can be used to authenticate users to and secure communications with company resources such as VPNs and web sites.
- Secure email (S/MIME) - Issues certificates that can be used for digital signing and/or authentication of emails through S/MIME. By default, Key escrow option is supported for Secure email profile. This option automatically back up the certificate's private key when the certificate is generated and issued. AirWatch MDM solution also supports key recovery requests.
- MDM - Issues certificates to mobile devices that can be used to authenticate users to and secure communications with company resources such as VPNs and web sites.

Symantec recommends to use a single certificate profile with multiple payloads to reduce certificates exposed.

Complete the following steps to create your Managed PKI certificate profiles:

1 Log into PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.

2 In PKI Manager, click **Manage certificate profiles** or select **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.



Symantec™ PKI Manager

acmeuser@yopmail.com | Sign Out

Logged in to: ACME Org

Account activity

Last updated: Apr 3, 2013 10:52 AM
Refresh

All

Recent activity

Action	Date
Enrollment e-mail sent to t...	Apr 3, 2013
Enrollment created	Apr 3, 2013
Certificate profile created	Apr 3, 2013
Certificate options custom...	Apr 3, 2013
Certificate profile created	Apr 2, 2013

Alerts

Symantec's Managed PKI 8.7 release announces significant advances in core areas of its enterprise authentication strategy. With support for new platforms such as iOS 6.0 and Android Jellybean (4.1), Managed PKI 8.7 secures mobile data and enables business productivity for corporate-managed and personally-owned unmanaged devices. Managed PKI 8.7 also includes several other key enhancements for you and your users, such as shortened URLs for certificate enrollment, automated capabilities of PKI Client to support MAC VPN client, the ability to delete users and revoke multiple certificates through PKI Manager and more. For more information on these and the security updates available in this release, refer to Managed PKI v8.7 Release Notes available on the Resources page.

There is no data to display for this account.

Account status

Set up your account
Create certificate profile
Enroll users for a certificate

Next service renewal: **Apr 2, 2016**

Optional account setup:
Use directory service

Seat usage

Seat pool	Total used	Total purchased
User	0	200
Device	0	200
Server	0	200
Organization	0	200

Buy more seats

Figure 1-5 Manage Certificate Profile

3 Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page.

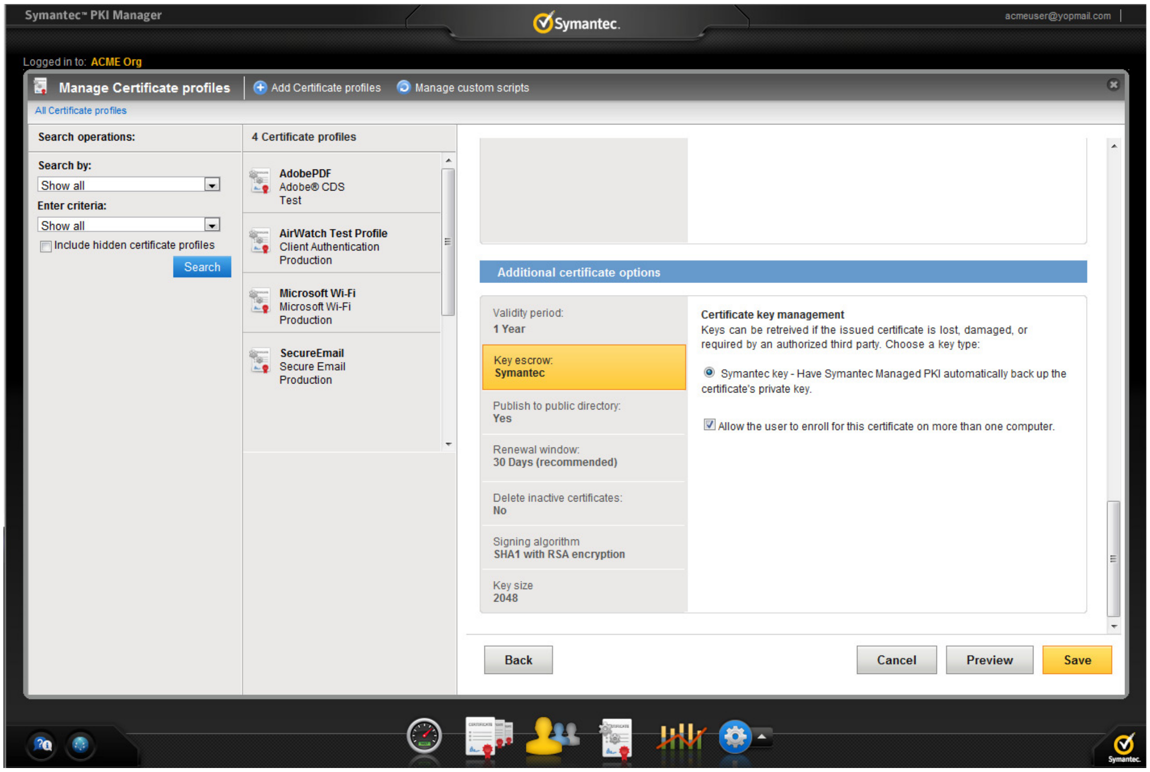
4 Select whether these certificates will be issued in Test mode or Production mode, and click **Continue.**

5 Configure the remainder of the certificate profile based on the profile type and your certificate needs. Refer to Table 1-2 for some guidelines.

Table 1-2 Certificate profile options

Certificate Profile Template Type	Option	Value
Client authentication	Certificate template	Client authentication
	Enrollment method	■ Select **PKI Web Services** if you will develop your own certificate management application to replace the PKI Certificate Services for your users. ■ Select **SCEP** if your user will enroll for certificates using SCEP.
	Authentication method	■ For the PKI Web Services Enrollment method, the Authentication method is **3rd party application.** ■ For the SCEP Enrollment method, the Authentication method is **Enrollment code.**
Secure email (S/MIME)	Certificate template	Secure email
	Enrollment method	■ Select **OS/browser** if your user will enroll for certificates using browser. ■ Select **PKI Client** if your user will enroll for certificates using PKI Client. ■ Select **PKI Web Services** if your user will enroll for certificates using third party applications.
	Authentication method	■ For the PKI Web Services Enrollment method, the Authentication method is **3rd party application.** ■ For the PKI Client or OS/browser Enrollment method, the Authentication method is **Active Directory.**
MDM	Certificate template	MDM
	Enrollment method	SCEP
	Authentication method	Enrollment Code

6 Click **Advanced options** to view certificate options and define any additional attributes you may need. The Key escrow option for Secure email profile is available on the Additional certificate options.



Additional certificate options

Validity period:
1 Year

Key escrow:
Symantec

Publish to public directory:
Yes

Renewal window:
30 Days (recommended)

Delete inactive certificates:
No

Signing algorithm
SHA1 with RSA encryption

Key size
2048

Certificate key management
Keys can be retreived if the issued certificate is lost, damaged, or required by an authorized third party. Choose a key type:

● Symantec key - Have Symantec Managed PKI automatically back up the certificate's private key.

☑ Allow the user to enroll for this certificate on more than one computer.

Figure 1-6 Key escrow for Secure email profile

7 Click **Save**.

On the confirmation page, you can view the attribute used for the Seat ID, which is a mandatory attribute in your AirWatch configuration. You can also customize the profile further, such as adding custom scripts, and customizing languages or email notifications on this page.

Device Identity Certificate for iOS devices

There are several ways to provision an iOS device setting. You require a client authentication certificate to securely encrypt these settings, and a device certificate to decrypt these settings. The MDM products use device identity certificates to encrypt and decrypt these settings.

For the delivery of the actual profiles (such as Client Authentication and S/MIME) to the user's intended device, the MDM profile sends a profile that is customized for a particular device. In some environments, it is important to make sure that corporate settings and policies are protected securely. To provide this protection, iOS allows you to encrypt profiles so that they can be read only by a single intended device. An encrypted profile is similar to a normal configuration profile except that the configuration profile payload is encrypted with the public key associated with the device's X.509 identity.

Before enrolling for a device certificate, make sure to create a profile of the type MDM. For more information on MDM certificate, See Table 1-2, "Certificate profile options," on page 7.

Configuring AirWatch MDM for Managed PKI 8.x

Complete the following steps to integrate AirWatch MDM solution with Managed PKI 8.x.

- Integrate AirWatch with Managed PKI Certificate Authority.
- Configure a certificate template that AirWatch will deploy.
- Deploy certificate profiles from AirWatch to your user's devices.

For more information on completing these steps, refer to *AirWatch Integration with Symantec Managed PKI Guide*, available from AirWatch, or from Symantec's Knowledge Center at https://knowledge.verisign.com/support/mpki-support/index?page=content&id=SO22025&actp=search&viewlocale=en_US.