Symantec™ Managed PKI® Enterprise Mobility Guide

Symantec™

Symantec™ Managed PKI® Enterprise Mobility Guide

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

Last updated November 21, 2013

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. VeriSign, VeriSign Trust, and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. Other names may be trademarks of their respective owners. The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. “Commercial Computer Software and Commercial Computer Software Documentation”, as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement. This document may describe features and/or functionality not present in your software or your service agreement. Contact your account representative to learn more about what is available with this Symantec® product.

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

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

Contents

Chapter 1 Configuring Symantec™ Managed PKI® for Mobile Devices 1
Supported Devices 2
Basic and Advanced Settings 2
Configuration Workflow 2

Chapter 2 Example End User Enrollment Flow 11
Enrollment Workflow on iOS 11
Enrollment Workflow on Android 14
Enabling External Controls on a VPN Client 14

Index 21

Chapter 1

Configuring Symantec™ Managed PKI® for Mobile Devices

The enterprise workplace has moved beyond the walls of your organization into a global, mobile environment. To maintain your 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.

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 describes how to configure Symantec™ Managed PKI Service to enable your end users to securely access your enterprise resources using their mobile devices.

Note: The solutions described in this document do not require the use of a separate Mobile Device Management (MDM) solution. If you are deploying an MDM solution in your enterprise, refer to your MDM documentation on how to integrate with the Managed PKI Service.

Using these procedures, you can configure your end users' iOS or Android mobile devices to use Managed PKI certificates for the following purposes:

- Wi-Fi access. The mobile device will use the certificate to authenticate the device to an organizations wireless network. Managed PKI supports the native Wi-Fi capability or iOS and Android devices.
- Virtual Private Network (VPN) access. The mobile device will use the certificate to authenticate the device to an organizations VPN, and secure communications over that network. Managed PKI supports Cisco IPSec and Juniper VPNs for iOS, and Cisco AnyConnect VPN Clients for Android.
- Microsoft® ActiveSync support. The mobile device will use the Managed PKI certificate to securely communicate with the enterprise ActiveSync server.

  For iOS mobile devices, you can also configure your ActiveSync solution for S/MIME. This installs the end user's current S/MIME certificate on the device, allowing the device to send signed and encrypted email.

Supported Devices

Symantec Managed PKI supports the following devices:

- iOS mobile devices: iPhone or iPad, running iOS 6 or 7.
- Android devices: The following Android mobile devices running Ice Cream Sandwich (ICS) 4.0:

Table 1-1 Supported Android devices

Samsung Devices	Motorola Devices	Sony Devices	Other Devices
Samsung Galaxy Nexus	Motorola Atrix 2 4G	Sony Tablet S	Asus EeePad TF300T
Samsung Galaxy Note 10.1 Tab	Motorola Droid 4	Sony Xperia Arc	Asus Nexus 7
Samsung Galaxy Note II	Motorola Droid Bionic	Sony Xperia Arc S	Asus EeePas TF101
Samsung Galaxy SIII Mini	Motorola Droid RAZR	Sony Xperia Neo L	Acer Iconia A100
Samsung Galaxy S Glide	Motorola Droid RAZR HD	Sony Xperia Ray	Acer Iconia A200
Samsung Galaxy S III	Motorola Droid RAZR M	Sony Xperia S	Acer Iconia A500
Samsung Galaxy S II Epic 4G Touch	Motorola XYBOARD		LG Nexus 4
Samsung Galaxy Tab 2 10.1	Motorola Xoom		LG Optimus G
Samsung Galaxy Tab 2 7.0	Motorola Xoom2 8.2		Archos 80 G9
Samsung Nexus 10			
Samsung Nexus S 4G			

Note: Additional Android mobile devices are constantly being qualified. Refer to the PKI Client download page on Google play™ for the most up-to-date list of supported devices.

For VPN access, the Android device must also have the Cisco AnyConnect® ICS+ VPN client (all supported models) or the Samsung AnyConnect® VPN client (Samsung devices only).

Basic and Advanced Settings

The default certificate profile settings allow you to configure the following for your Wi-Fi, VPN, or ActiveSync solutions:

- For Wi-Fi, you can set your SS ID
- For VPN, you can set your VPN Server name
- For ActiveSync, you can set your ActiveSync host name and, for iOS mobile devices, enable S/MIME

Typically, these are sufficient to allow your end users to access your organization's Wi-Fi network, VPNs, or ActiveSync server. However, if you will issue certificates to iOS devices, you can configure your certificate profile for more advanced options, for example, for more complex networks, for VPNs not supported by the basic settings, or for custom device policies. This requires that you upload a mobile.config file to your certificate profile, which carries the additional configuration settings (and optional root and intermediate CAs) that your end users' devices will need. This document describes both sets of procedures.

Configuration Workflow

Figure 1-1 describes the general tasks required to set up the Managed PKI account and configure the Managed PKI service to issue certificates to your end users. Refer to the resources listed for each task for specific information on performing these general tasks.

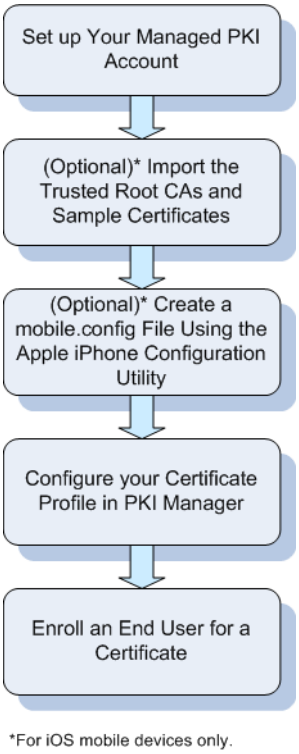

Figure 1-1 Managed PKI configuration work flow

Task 1. Set up your Managed PKI 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.

  Use your Managed PKI administrator ID to log into PKI Manager, configure your Managed PKI account, and upload your mobile.config file. Refer to PKI Manager and its online help for details on configuring Managed PKI.

Task 2. (Optional) Import trusted root CAs and sample certificates.

If you are issuing certificates to iOS mobile devices and need to configure more advanced configurations than are provided by the basic settings, you will need to use the Apple® iPhone Configuration Utility to create a mobile.config file. This file will be pushed to the end user's mobile device during installation, and contains the configuration settings for your mobile solution, as well as the end user certificate to be installed. Refer to "(Optional) Create a mobile.config file using the Apple iPhone Configuration Utility." on page 4 for procedures on creating a mobile.config file.

Prior to create the mobile.config file, you must first make a sample end user certificate available to the iPhone Configuration Utility. Managed PKI will replace this sample certificate with the actual certificate issued to the end user (as a password-protected PKCS#12 file) when the mobile.config file is pushed to the end user's mobile device during certificate installation. If you have organization-specific root and intermediate CAs, you can also provide them to your end users' devices in the same manner.

Note: You can also use these procedures to provide the root and intermediate CAs for your Managed PKI certificates to your end users' devices. Obtain these from the *Manage CAs* link of PKI Manager.

When adding these certificate credentials (as PKCS#12 files and root CA and intermediate CA certificates) to the mobile configuration file, the iPhone Configuration Utility takes the credentials from the Microsoft Windows certificate store. Therefore, you will need to import these credentials into the Windows certificate store prior to adding them with the iPhone Configuration Utility, using the following steps:

1. Obtain the appropriate sample end-user certificate (as a PKCS#12 file):
   a. On the *Resources* page, click the **Managed PKI® enterprise mobility kit** link under *Symantec™ Managed PKI® Mobile Device Solution* to download a .zip file containing the sample certificates and this document. Save the file to a temporary location.
   b. Unzip the file. You will need to import one or both of the following files to your Windows certificate store:
      - For VPN and Wi-Fi mobile solutions, you will import SymantecManagedCertificate.pfx
      - For S/MIME mobile solutions, you will import SymantecManagedSMIMECertificate.pfx.
2. Import the sample end-user PKCS#12 file:
   a. On the machine where you will create the mobile.config file, browse to the sample PKCS#12 file, right-click on it, and choose **Install PFX**.
   b. Complete the Certificate Import Wizard by following the prompts. The password for the Managed PKI sample PKCS#12 file is **password**.
3. Import the trusted root CA:
   a. On the machine where you will create the mobile.config file, browse to the file containing the trusted root CA, right-click on it, and choose **Install Certificate**.
   b. Complete the Certificate Import Wizard by following the prompts. If you are importing the Managed PKI root CA certificate, the password is **password**.
4. Repeat step 3 for any intermediate CAs in this CA hierarchy. If you are importing the Managed PKI intermediate CA certificate, the password is **password**.

Task 3. (Optional) Create a mobile.config file using the Apple iPhone Configuration Utility.

By default, the basic settings available in a certificate profile are sufficient to allow end users' devices to access your organization's Wi-Fi network, VPN, or ActiveSync server. If you are issuing certificates to iOS devices and wish to provide more advanced settings, use the iPhone Configuration Utility to create a mobile.config file. This file includes advanced information for your end users' mobile devices on how to use the certificate you issue.

When the end user picks up his or her certificate, the mobile.config file will be sent as well. The file will contain:

- The end-user certificate and key pair as a password-protected PKCS#12 file, if provided. This enables SSL client authentication from the end user's device.
- Any root or intermediate CA certificates needed for SSL server authentication from the server to the end user's device, if provided.
- Client VPN or Wi-Fi configuration settings the device will need to securely access your organizations' protected resources.

Complete the following general steps to configure your mobile.config file. Refer to the help and documentation provided with this utility, as well as your own enterprise environment for details on the specific settings to configure.

1 Download and install the latest version of the iPhone Configuration Utility from Apple website.

2 Using the iPhone Configuration Utility, start a new mobile.config file:

   a Select **Start** → **Programs** → **iPhone Configuration Utility** → **iPhone Configuration Utility**.

   b Select **Configuration Profiles** and click **New**.

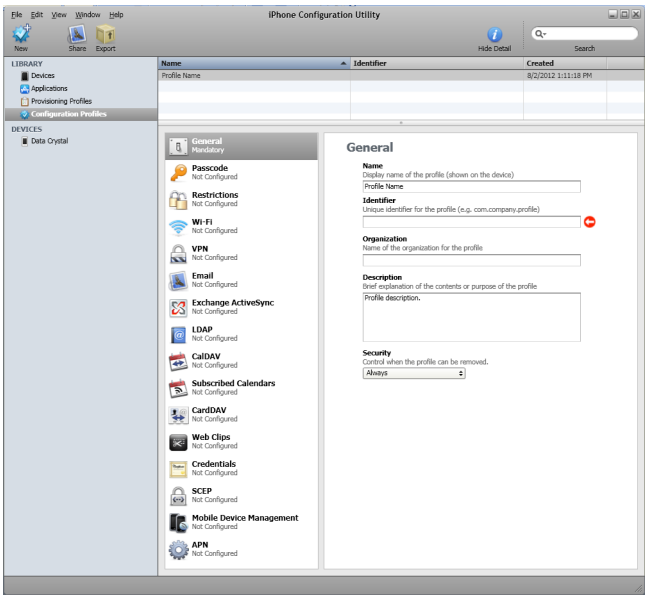

Figure 1-2 iPhone Configuration Utility

3 Configure the profile to meet your mobile solution. The settings you configure will vary based on your requirements.

   If you are providing organization-specific root and intermediate CAs (or the Symantec-provided root and intermediate CAs for your Managed PKI certificates) to your end users' devices, you must add the trusted root CAs and sample certificates:

   a Click **Credentials**, and then click **Configure**.

   b Browse to the sample end-user certificate you added in "(Optional) Import trusted root CAs and sample certificates." on page 3.

      As this is a sample certificate, enter any password when prompted and click **OK**. Managed PKI will replace this sample end user certificate and password with the end user's actual certificate and password (as a password-protected PKCS#12 file) during enrollment.

   c In the *Credentials* pane, click the plus icon in the top, right corner. and browse to the trusted root CA you added in "(Optional) Import trusted root CAs and sample certificates." on page 3.

   d Repeat Step c for any intermediate CAs you added in "(Optional) Import trusted root CAs and sample certificates." on page 3.

   e Configure your mobile solution (VPN, Wi-Fi, and so on) to use the sample end user certificate you imported in "(Optional) Import trusted root CAs and sample certificates." on page 3.

4 Export the settings as a mobile.config file:

   a Click **File** → **Export**.

   b Set *Security* to **None**. As this is a template profile only, it should not be encrypted or signed. Managed PKI will deliver a signed, encrypted profile to the end user's device during enrollment.

c Click **Export** and save the file to a location that can be reached by the machine that you will use to access PKI Manager.

Task 4. Configure your certificate profile in PKI Manager.

Complete the following steps to configure Managed PKI to issue certificates to your end users' devices. Refer to PKI Manager and the online help for additional details on configuring Managed PKI for mobile certificate profiles.

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

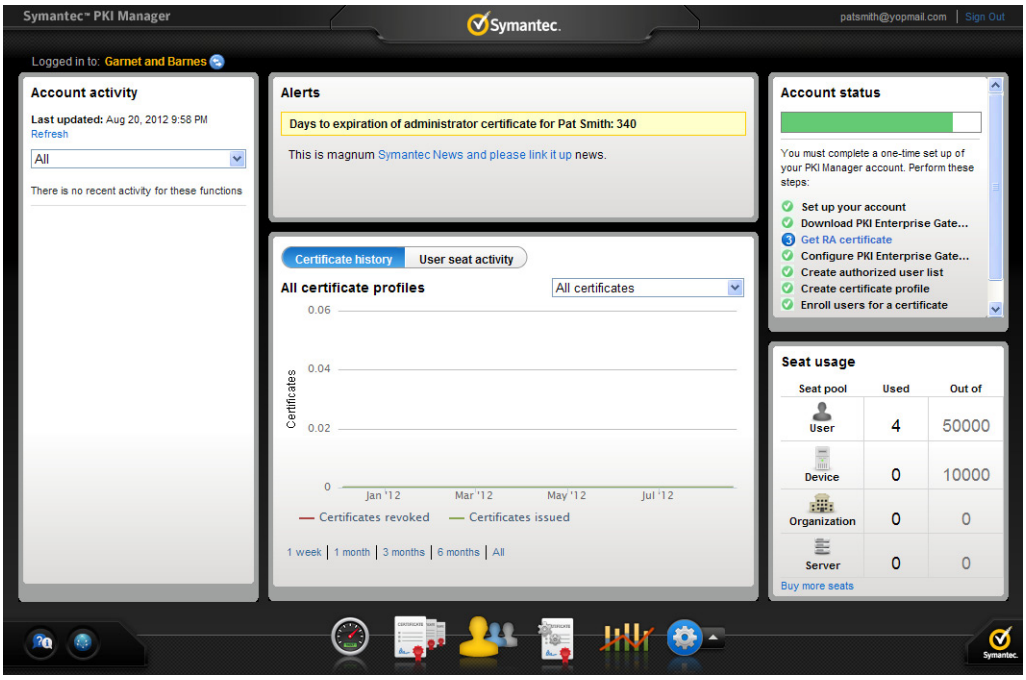

Figure 1-3 PKI Manager dashboard

2 Create a new certificate profile:

a Click **Manage certificate profiles** (or select **Manage certificate profiles** from the *Tasks* menu) on the bottom navigation bar.

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

c Complete the screens to create your certificate profile and click **Save**. Although the majority of the settings you will configure will vary based on your organizational needs, you should configure the certificate profile with the following:

- For Android mobile devices, select the **Secure Sign-in** certificate profile template for Android mobile devices. This template allows you to configure certificate profiles that issue VPN, ActiveSync, or Wi-Fi certificates.

  Due to an ActiveSync limitation, if configuring the profile for ActiveSync support, use only alphanumeric characters for the certificate profile name.

- For iOS mobile devices, select the **Secure-Sign-in** certificate profile template to configure certificate profiles that issue VPN or ActiveSync certificates. Select the **Wi-Fi** certificate profile template to configure certificate profiles that issue Wi-Fi certificates.

- Select **iOS** or **Android**, as appropriate, for the Enrollment method.

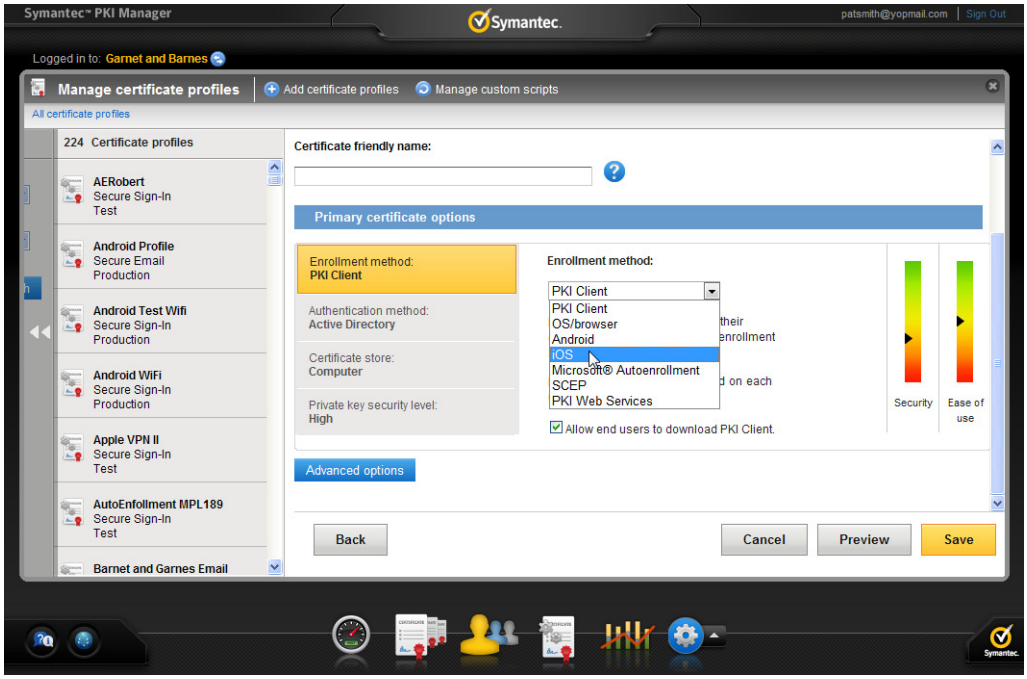

Figure 1-4 Selecting the Enrollment method

3 Configure your device profile settings. If not already selected, select the certificate profile in the *Certificate profiles* column.

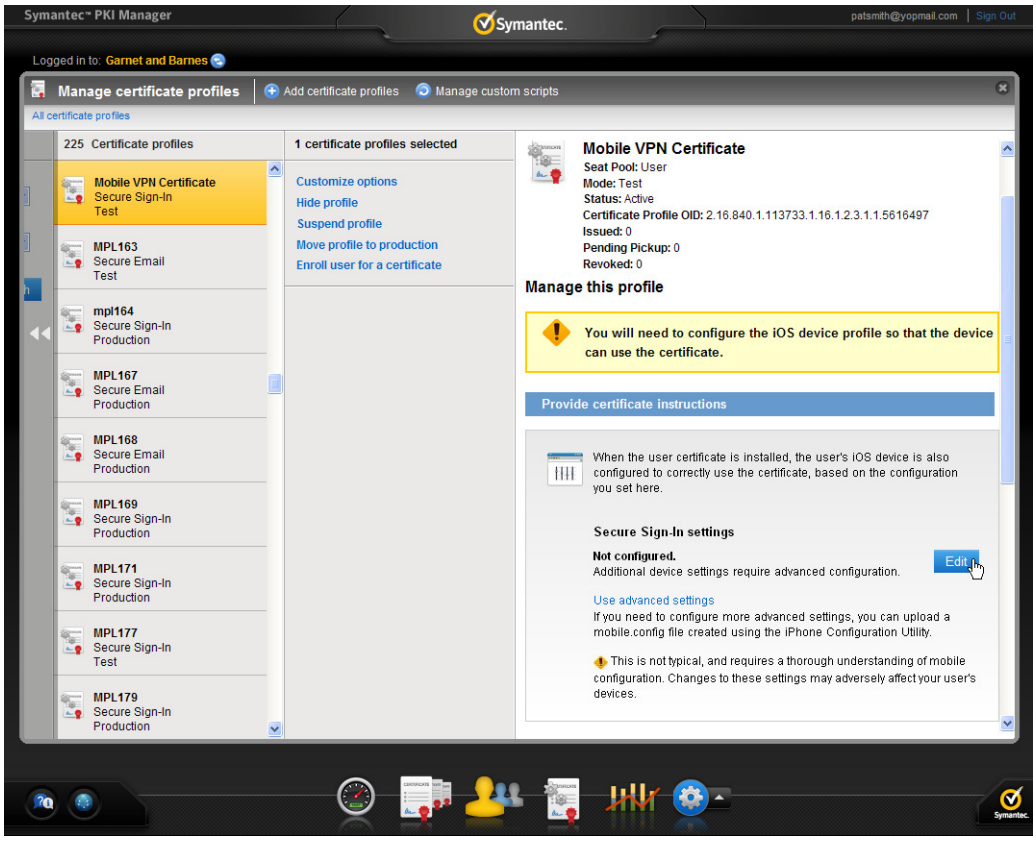

Figure 1-5 Configuring the device settings

- If using the basic settings, select **Edit**, and configure the profile as required for the type of solution you are issuing Managed PKI certificates (VPN, ActiveSync, or Wi-Fi). For Android devices you can enable multiple solutions for a single profile.
- If using a more advanced configuration (iOS mobile devices only), upload the mobile.config file you created in "(Optional) Create a mobile.config file using the Apple iPhone Configuration Utility." on page 4 into the new certificate profile.
  - Under *Provide device configuration settings*, click **Advanced settings**.
  - If enabling S/MIME, select **Enable S/MIME**, and select an S/MIME profile to associate with this profile.
  - **Click Choose**, click **Upload**, and browse to the mobile.config file. Click **Open**.

4 For Android mobile devices, you may upload additional instructions to display to your end users after the certificate is installed. Click **Edit** in the *Provide certificate instructions* section of the certificate profile details pane to browse to and upload the instructions file. The file can be in one of the following formats: PDF, DOC, DOCX, TXT, PPT, PPTX.

If you have configured the certificate profile for ActiveSync on Android devices, you must provide specific instructions on how the end user should configure the ActiveSync client on the device.

Task 5. (Optional) Configure your ActiveSync solution

If your end users' devices will use Managed PKI certificates to authenticate with your Microsoft Exchange Server, configure your ActiveSync solution to support these certificates. Refer to *Symantec™ Managed PKI®*

Integration Guide for ActiveSync® for procedures. This document is available from the *Resources* page of PKI Manager.

To enable the SMIME option for an iOS profile, the end user must already have enrolled for a key-escrowed S/MIME certificate on their desktop client machine using a PKI Client profile. If the user doesn't have an S/MIME certificate, the IOS profile will be installed on the end user's device, but no SMIME certificate will be installed.

Task 6. Enroll a user for a certificate.

Test the configuration by enrolling a user for a certificate. These procedures describe how to enroll for a single user (for test purposes); however, you can also enroll for multiple users at one time using the *Manage users* page and uploading a comma-separated value (CSV) file with your user data. Refer to PKI Manager and its associated online help for details on enrolling users in bulk.

When enrolling end users for certificates, provide an email address that they can access using their mobile devices.

1 In PKI Manager, search for and select your mobile certificate profile.

2 In the *Manage this profile* page, click **Enroll user for a certificate**.

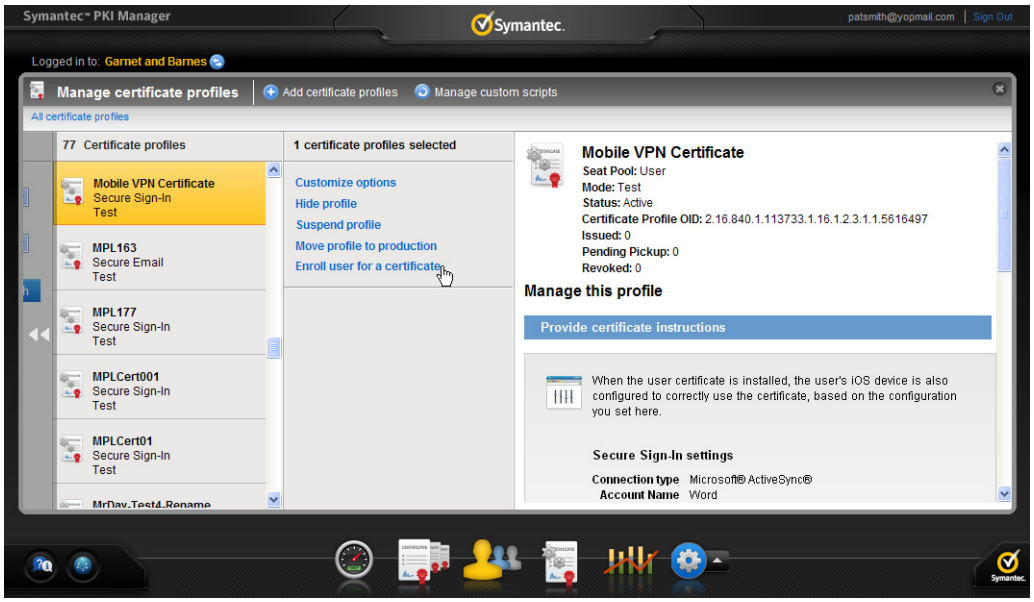

Figure 1-6 Enrolling a user for a certificate

3 Enter the **Seat ID** (typically the end user's email address), and define whether the system will generate an enrollment code for the user, and whether the system will send an enrollment email to the user. Then, click **Continue**.

   Symantec recommends that you have the system generate the enrollment code and send the enrollment email.

4 Enter the appropriate information for your end user and click **Continue**. lists the basic information required (not all information will be required for all users).

Table 1-2 Additional user information

User information	Description
First Name	The end user's first name.
Last Name	The end user's last name (surname)
Other Name (UPN)	The User Principal Name assigned to the user in your user store.

Table 1-2 Additional user information

User information	Description
Send enrollment email?	Select whether the system will send an enrollment email to the end user. If you do not have the system send an enrollment email to the end user,

5 If you had the system generate the enrollment code, the enrollment code appears in the enrollment successful dialog box. Make a note of the enrollment code.

6 The system sends an enrollment email to the end user, if you configured the certificate profile to do so. You must also send the enrollment code to the end user. Symantec recommends that you send the enrollment code separately from the enrollment link, and that you do not send the enrollment code by email.

Refer to Chapter 2, "Example End User Enrollment Flow," for sample end-user enrollment flows.

Chapter 2

Example End User Enrollment Flow

This chapter describes the enrollment flows the end user will experience when enrolling for and installing a certificate issued by Managed PKI.

Enrollment Workflow on iOS

Figure 2-1 describes the general steps your end user follows to pick up a Managed PKI certificate issued by your iOS certificate profile. This flow is performed on an Apple iPad running iOS 4, but the flow is essentially the same for iPhone users. The end user must be running iOS 4 or higher.

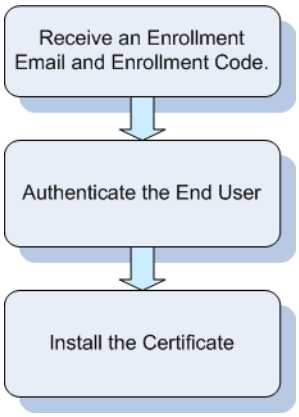

Figure 2-1 iOS enrollment work flow

Task 1. Receive an enrollment email and enrollment code.

If configured to do so, Managed PKI sends the end user an enrollment email that contains an enrollment link. Otherwise, you must provide the enrollment link to the end user.

You must also provide the enrollment code to the end user; however, for security reasons, you should send the enrollment code separately from the enrollment link, and not send the enrollment code by email.

Task 2. Authenticate the end user.

1 The end user accesses the enrollment link in the email (or provided by you), and, when prompted, enters his or her **User ID** (if required by the certificate profile) and enrollment code and taps **Continue**. This step authenticates the end user to ensure the correct user is picking up the certificate.

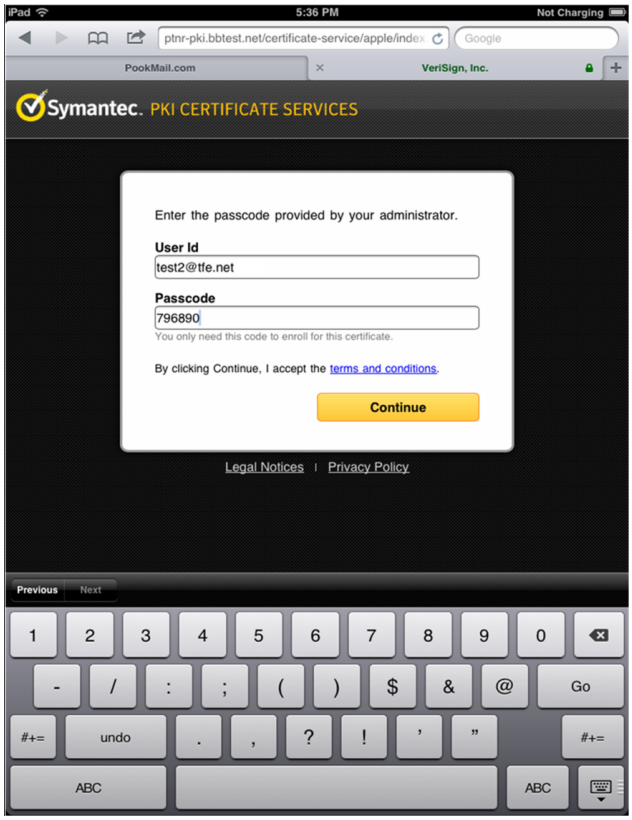

Figure 2-2 Enrollment page

2 The end user is authenticated and is authorized to install the certificate. The end user taps **Continue** to begin the certificate installation process.

Task 3. Install the certificate.

1 The end user is prompted to install the mobile profile and the certificate.

Note: If the Passcode Lock feature is not configured on the mobile device, the end user will be prompted to set this up.

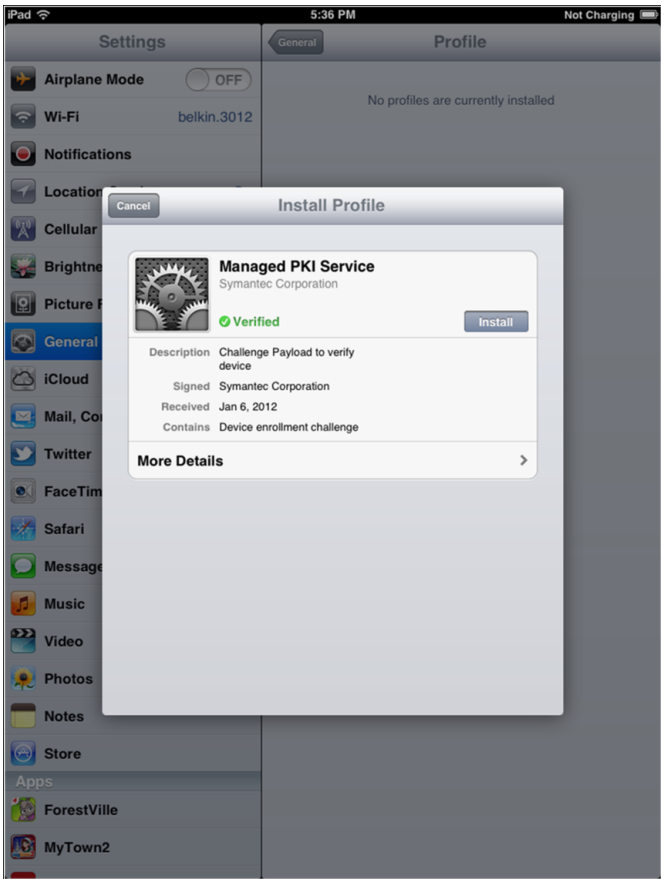

Figure 2-3 *Install Profile* screen

2 The end user taps **Install**, and then **Install Now** at the prompt. The key is generated and the certificate is installed on the end user's device.

3 If you have configured the mobile.config file to provide root and intermediate CAs (in "(Optional) Create a mobile.config file using the Apple iPhone Configuration Utility." on page 4), the end user is prompted to install them. The end user taps **Install**.

4 The end user may also be prompted to enter a PIN (for example, if the VPN server is configured to require a user PIN in addition to a certificate as authentication).

5 The certificate is now installed on the end user's device. The certificate can be viewed under **Settings** → **General** → **Profiles** → **More Details**.

Figure 2-4 *More Details* screen

Enrollment Workflow on Android

Figure 2-5 describes the general steps your end user follows to pick up a Managed PKI certificate issued by your mobile certificate profile using an Android device. This flow is performed on an mobile telephone running ICS 4.0, but the flow is essentially the same for Android tablet users. The end user must be running ICS 4.0.

Enabling External Controls on a VPN Client

If your profile is configured for VPN, the end user will need to install a Cisco VPN client. Managed PKI has been qualified with AnyConnect ICS+ on all supported mobile devices, and with Samsung AnyConnect on supported Samsung mobile devices. The end user will need to enable External Controls in the VPN client by selecting **Settings** → **AnyConnect** → **External Control** and choosing to either enable External Controls or to prompt the user when an application attempts to configure the client.

Symantec recommends choosing to have the client prompt the user, so that the user can control the configuration of the Cisco profile when PKI Client is installed. Refer to the Cisco VPN client instructions for additional details about External Controls.

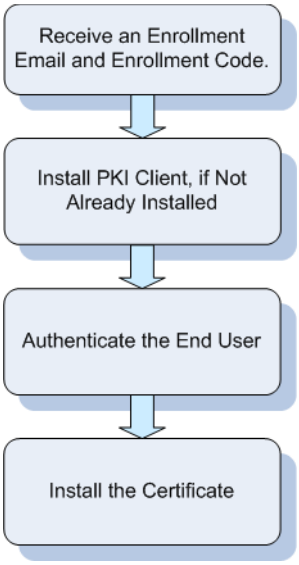

Figure 2-5 Android enrollment work flow

Task 1. Receive an enrollment email and enrollment code.

If configured to do so, Managed PKI sends the end user an enrollment email that contains an enrollment link. Otherwise, you must provide the enrollment link to the end user.

You must also provide the enrollment code to the end user; however, for security reasons, Symantec recommends that you send the enrollment code separately from the enrollment link, and not send the enrollment code by email.

Task 2. Install PKI Client, if not already installed

1 The end user accesses the enrollment link in the email (or provided by you). If not already installed, the end user is prompted to install PKI Client. PKI Client is Symantec's certificate management tool. It allows the end user to manage (obtain and view) certificates.

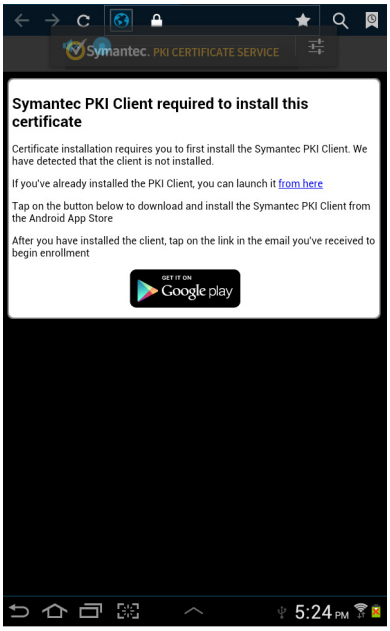

Figure 2-6 *Install PKI Client* prompt

2 The end user taps **Download from Google play**, and follows the prompts to install PKI Client.

3 Once installed, the end user must close the window and access the enrollment link in the email again to restart the enrollment process.

Task 3. Authenticate the end user.

1 The end user accesses the enrollment link in the email (or provided by you). The end user is prompted to open PKI Client or use the Internet browser to continue. The end user should select **PKI Client**.

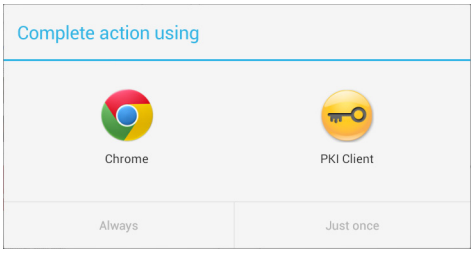

Figure 2-7 Enrollment page

2 The end user enters his or her **Enrollment code** (if required by the certificate profile) and taps **Continue**. This step authenticates the end user to ensure the correct user is picking up the certificate.

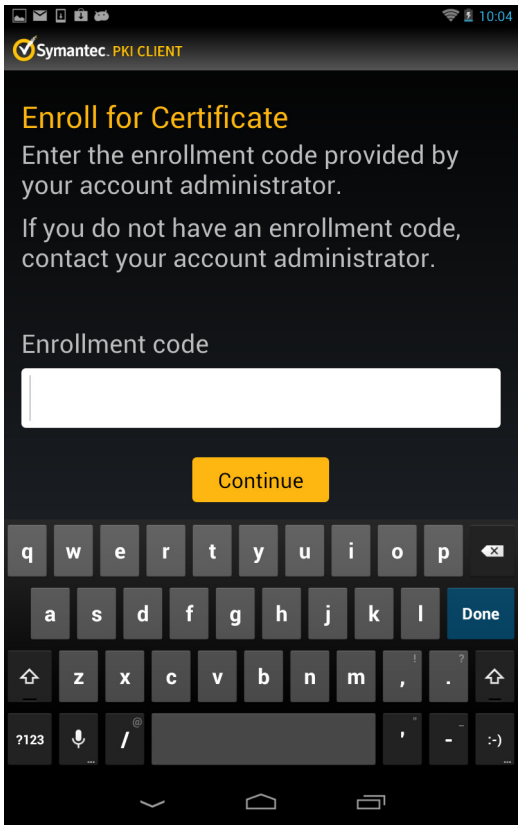

Figure 2-8 *Enroll for Certificate* page

Task 4. Install the certificate.

1 The end user is prompted to extract and install the certificate. The prompt displays the certificate extraction password and certificate profile name.

The end user taps **Install certificate**.

Note: If the mobile device is not configured for screen or swipe lock, the end user will be prompted to set this up.

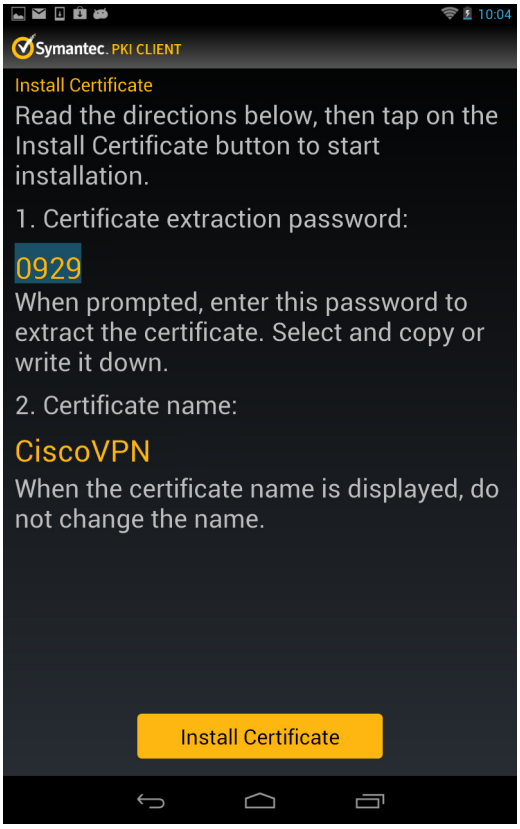

Figure 2-9 *Install Certificate* screen

a The end user is prompted for the certificate extraction password. The end user should enter the password provided on the previous screen.

b The end user is prompted for the certificate name. The end user should retain the default certificate name.

2 If your profile is configured for Cisco AnyConnect VPN access, the end user is prompted to enter a password for certificate import. The end user should enter the certificate extraction password provided on the previous screen again.

3 The certificate is now installed on the end user's device, and can be viewed under **PKI Client**→ **View certificates**.

If the administrator has uploaded post-installation instructions to PKI Manager, a link will display on the success page. Selecting the link will open the instructions file in the appropriate app on the device.

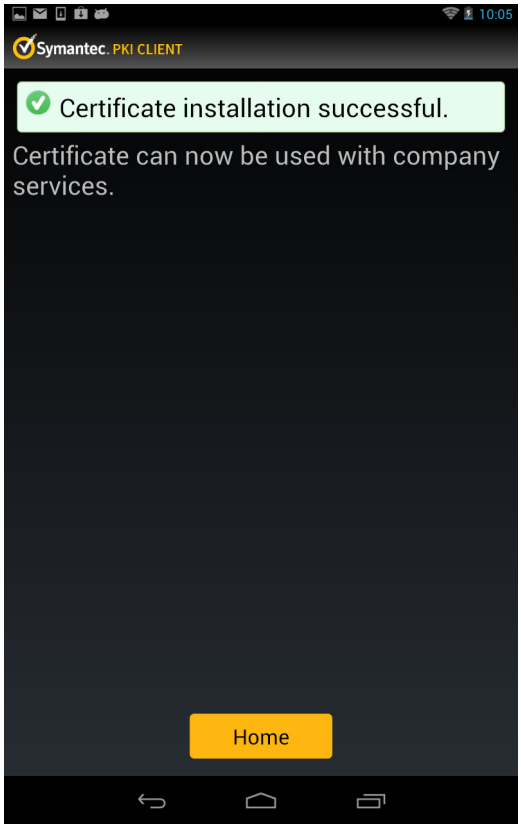

Figure 2-10 *Certificate installation successful* screen

Index

A

ActiveSync support 1
- advanced configuration for 4
- basic settings for 8
- certificate profile template for Android 6
- certificate profile template for iOS 6
- configuring 8
- enabling S/MIME for 2
- S/MIME 1
- set ActiveSync host name for 2

adding to mobile.config file 5
additional instructions for end users 8, 18
administrator ID 3
advanced configuration 3, 4
advanced configuration for iOS 4, 8
Android
- configuring multiple profiles for 8
- installing the certificate on 17
- installing VPN Client on 14
- uploading additional instructions for 8

Android Enrollment method 6
Android supported devices 2
AnyConnect VPN 1, 18
AnyConnect VPN Client 2, 14
Apple iPhone Configuration Utility
- creating a mobile.config file with 4
- downloading 5

Apple® iPhone Configuration Utility 3
authenticating the end user 12, 16

B

basic settings 4, 8

C

CA Naming Document 3
certificate
- viewing on Android 18
- viewing on iOS 14

certificate extraction password 18
Certificate Import Wizard 4
certificate name. 18
certificate profile 9
- configuring 6
- creating 6
- defining 6

certificate profile template for Android 6
certificate profile template for iOS
- Secure Sign-in 6
- Wi-Fi 6

certificates, enrolling for 9
Cisco AnyConnect VPN 1, 18
Cisco IPSec 1
Cisco VPN Client
- installing on Android 14

client authentication 4
comma-separated value
- see CSV

configuration workflow 2
configure the certificate profile 6
configuring ActiveSync support 8
creating a certificate profile 6
credential 3
credit card 3
CSV file 9
custom device policies 2

D

device policies 2
device profile settings 8
documents
- CA Naming Document 3
- Issuing Authority Naming Application 3
- Master Service Agreement 3
- purchase order, credit card, or reference number 3
- Symantec Services Order Form 3

downloading the Apple iPhone Configuration Utility 5

E

email address 9
email, signed and encrypted 1
enabling External Controls on Android 14
encrypted email 1
end user
- authenticating 12, 16
- email address 9
- enrolling in bulk 9
- enrollment flows 11-19
- enrollment information for the 9

uploading instructions for 8
viewing instructions for 18
end user certificate
enrolling for 9
in mobile.config file 4
enroll end users in bulk 9
enrolling for end user certificate 9
Enrollment code
Android 17
see also Seat ID 17
enrollment code 10
generating 9
receiving iOS 11, 15
sending 10
enrollment email 10, 16
configuring 9
receiving Android 15
receiving iOS 11
enrollment flow 11, 19
enrollment flows
Android 14-19
iOS 11-14
enrollment link 11
Enrollment method 6
example enrollment flows 11-19
External Control, enabling 14

G

Google play 16

I

installing the certificate
Android 17
iOS 12
instructions for end users
uploading 8
viewing 18
intermediate CA 3, 5
in mobile.config file 4
password 4
intermediate CA installing 13
iOS
advanced configuration 3
advanced configurations for 4, 8
configuring S/MIME for 8
enabling S/MIME for 2
Enrollment method 6
installing the certificate on 12
installing the mobile.config file 13
IPSec 1
S/MIME 1
supported devices 2
iOS devices
intermediate CA 3
sample certificates 3
trusted root CA 3
iPhone Configuration Utility 3
creating a mobile.config file with 4
downloading 5
IPSec for iOS 1

J

Juniper VPN 1

K

key pair 13
key pair in mobile.config file 4

L

login 3

M

Managed PKI
administrator ID 3
configuring 3
configuring, SCEP certificate profiles 6
root and intermediate CAs 4
setting up the Managed PKI account 3
Managed PKI Service 1
Master Service Agreement 3
MDM solution 1
Microsoft® ActiveSync support 1
mobile.config file 2, 3
adding CAs and sample certificate 5
creating 4
exporting 5
installing 13
uploading the 8
multiple profiles for Android 8

O

online help 6

P

Passcode Lock 12
password for certificate import 18
password for PKCS#12 file 4
password-protected PKCS#12
adding to mobile.config file 5
password-protected PKCS#12 file
in mobile.config file 4
PIN

PKI Client 6
user authentication to VPN 13
PKCS#12 file
in mobile.config file 4
password 4
PKCS#12 files 4
PKI Client 15
downloading 16
using to install a certificate on Android 16
PKI Client PIN 6
PKI Manager 3, 4
configure the certificate profile in 6
enrolling users in 9
logging into 6
login 3
online help 6
policies 2
purchase order 3

R

reference number 3
required documents 3
root CA 3
adding to mobile.config file 5
in mobile.config file 4
installing 13

S

S/MIME
ActiveSync 1
configuring iOS for 8
iOS 1, 2
sample certificate 3
screen or swipe lock 17
Seat ID 9
Secure Sign-in
certificate profile template for Android 6
certificate profile template for iOS 6
setting up the Managed PKI account 3
signed email 1
SSL client authentication 4
supported devices 2
Symantec Services Order Form 3

T

testing your mobile solution 9
trusted root CA 3
adding to mobile.config file 5
importing the 4
in mobile.config file 4
installing 13

U

uploading instructions for end users 8
uploading the mobile.config file 8
UPN 9
User ID
iOS 12
see also Seat ID 12
user PIN 13
User Principal Name
see UPN

V

viewing instructions for end users 18
viewing the certificate on Android 18
viewing the certificate on iOS 14
Virtual Private Network
see VPN
VPN
Android 1, 18
certificate profile template for iOS 6
iOS 1
PIN 13
VPN access
about 1
advanced configuration for 4
basic settings for 8
certificate profile template for Android 6
client settings for 4
set VPN Server name for 2
VPN Client for 2
VPN Client 2
installing on Android 14

W

Wi-Fi
certificate profile template for iOS 6
Wi-Fi access
about 1
advanced configuration for 4
basic settings for 8
certificate profile template for Android 6
certificate profile template for iOS 6
configuration settings 4
set SS ID for 2