Managed PKI® Getting Started with iOS Mobile Devices

What to Read

- For an overview of Managed PKI and all of its options, read *Symantec™ Managed PKI® Overview*.
- For detailed procedures on configuring Managed PKI certificates for mobile devices, including advanced configurations for iOS devices, read *Symantec™ Managed PKI® Mobile Device Integration Guide*.
- For procedures on configuring Managed PKI certificates for email signing and encryption, refer to *Symantec™ Managed PKI® Integration Guide for ActiveSync®*
- For detailed usage of PKI Manager, refer to the PKI Manager and its associated online help.

This document describes the general steps you follow to issue and install Managed PKI certificates on iOS devices. This document assumes that you already have access to a Managed PKI or a Managed PKI TestDrive account.

The Managed PKI service supports devices running iOS 4 or higher.

Configuring and Issuing Managed PKI Certificates

As the Managed PKI administrator, configure your Managed PKI account based on your mobile solution. These procedures describe how to use the basic settings for Microsoft® ActiveSync® integration, to enable Wi-Fi and VPN access, and to enable strong authentication for web access. For more advanced configurations, refer to *Integrating Symantec™ Managed PKI with your Mobile Device Solution*.

Enable ActiveSync Integration

To enable the SMIME option for an iOS profile, your end users must have already enrolled for a key-escrowed S/MIME certificate on their desktop client machine using a PKI Client profile.

1. Create a certificate profile to fit your needs, with the following specific values:
   - Select the **Secure Sign-in** certificate profile template.
   - Select **iOS** as the enrollment method.
2. Save the certificate profile, then configure the profile for ActiveSync (under *Basic settings*).
3. Configure your ActiveSync server following the procedures in *Symantec™ Managed PKI® Integration Guide for ActiveSync®*.
4. Create users and enroll them for certificates. During enrollment, provide email addresses for your end users that they can access using their mobile devices.

Enable Wi-Fi Access

1. Create a certificate profile to fit your needs, with the following specific values:
   - Select the **Wi-Fi** certificate profile template.
   - Select **iOS** as the enrollment method.
2. Save the certificate profile, then configure the profile for Wi-Fi (under *Basic settings*).
3. Configure your Wi-Fi server to accept PKI credentials, according to the vendor's instructions.
4. Create users and enroll them for certificates. During enrollment, provide email addresses for your end users that they can access using their mobile devices.

Enable VPN Access

1. Create a certificate profile to fit your needs, with the following specific values:
   - Select the **Secure Sign-in** certificate profile template.
   - Select **iOS** as the enrollment method.
2. Save the certificate profile, then configure the profile for VPN (under *Basic settings*).
3. Configure your VPN server to accept PKI credentials, according to the vendor's instructions.
4. Create users and enroll them for certificates. During enrollment, provide email addresses for your end users that they can access using their mobile devices.

Enable Client Authentication for Web Access

1. Create a certificate profile to fit your needs, with the following specific values:
   - Select the **Secure Sign-in** certificate profile template.
   - Select **iOS** as the enrollment method.
2. Configure your web server to accept PKI credentials, according to the vendor's instructions.
3. Create users and enroll them for certificates. During enrollment, provide email addresses for your end users that they can access using their mobile devices.

Installing Managed PKI Certificates

Once you have enrolled your end users for certificates, Managed PKI sends them an enrollment email that contains an enrollment link. You must also provide the enrollment code to the end user (for security reasons, send the enrollment code separately from the enrollment link, and do not send the enrollment code by email).

Follow these procedures to install a Managed PKI certificate on an iOS mobile device.

1. Access the enrollment link in the email.
2. Enter the User ID and enrollment code and tap **Continue**. This step authenticates the end user to ensure the correct user is picking up the certificate.
3. Click **Continue** to begin the certificate installation process.
4. Click **Install**, and then **Install Now** at the prompt. The key is generated and the certificate is installed on the mobile device.
5. If prompted for a PIN, enter it and tap **Continue**. This may be required if the VPN server is configured to request a user PIN in addition to a certificate as authentication.

You can now use the mobile device to securely access your organization's online services.