Managed PKI® Getting Started with Android 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, read *Symantec™ Managed PKI® Enterprise Mobility 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 Android devices. This document assumes that you already have access to a Managed PKI or a Managed PKI TestDrive account.

Symantec continues to qualify new Android devices with the Managed PKI service. Refer to the PKI Client download page on Google play for the most up-to-date list of supported devices. For VPN Access, the mobile device must have the Cisco AnyConnect VPN client installed with External Controls enabled.

Configuring and Issuing Managed PKI Certificates

As the Managed PKI administrator, configure your Managed PKI account based on how your end users will use their certificates. These procedures describe the basic settings needed to configure your Managed PKI account to issue certificates to Android mobile device users for the following purposes:

- Microsoft® ActiveSync® integration
- Wi-Fi access
- VPN access
- Strong authentication for web access.

For more advanced configurations, refer to *Symantec™ Managed PKI® Enterprise Mobility Guide*.

Task 1. Create a certificate profile.

1 Create a certificate profile to fit your needs, with the following specific values:
   - Select the **Client Authentication** certificate profile template.
   - Select **Android** as the enrollment method.

   Note that you can create separate certificate profiles for each certificate purpose, or you can create a single certificate profile to support multiple certificate purposes.

2 Save the certificate profile, then, under *Provide device configuration settings*, configure the profile to issue certificates for your specific purpose or purposes:
   - For VPN access, select **Cisco AnyConnect settings** and enter a Connection name and a Server Host name or IP address.
   - For Microsoft® ActiveSync® integration, select **ActiveSync® settings**.
   - For Wi-Fi access, select **WiFi settings**, enter a Service Set ID, and select whether the network is hidden and whether mobile devices can join automatically.

   Strong authentication for web access is enabled by default.

Task 2. Upload end-user instructions.

You can upload additional instructions to the certificate profile describing how your end users should configure their device with settings specific to your mobile solution. Select the certificate profile in PKI Manager and, under *Provide certificate instructions*, select a file to upload. These instructions will be available to your end users after the certificate is installed.

If you are supporting ActiveSync this step is required; you must upload additional instructions describing how your end users should configure the ActiveSync client on their device.

Task 3. Configure your mobile solution.

Configure your mobile solution to meet your needs:

- Configure your Wi-Fi, VPN, or web server to accept PKI credentials according to the vendor's instructions.
- To configure an ActiveSync server, follow the procedures in *Symantec™ Managed PKI® Integration Guide for ActiveSync®*.

Task 4. Enroll end users for certificates.

In PKI Manager, create users and enroll them for certificates.

Managed PKI will send your end users an email that includes a certificate pick-up link. Since end users must pick up their certificates on their mobile devices, provide email addresses during enrollment that they can access using their mobile devices.

You must also provide the enrollment codes to the end users (for security reasons, send the enrollment codes separately from the enrollment link, and do not send the enrollment code by email).

Installing Managed PKI Certificates

Once you have enrolled your end users for certificates, Managed PKI sends them an email that contains a certificate pick-up link.

Follow these procedures to install a Managed PKI certificate on an Android mobile device:

1. Access the enrollment link in the email.
2. If not already installed, you are promoted to install PKI Client, Symantec's certificate management tool, from Google play.

   Once PKI Client is installed, close the browser window and access the enrollment link in the email again.
3. If prompted for an application, select **PKI Client**.
4. Enter the enrollment code and tap **Continue**. This step authenticates the end user to ensure the correct user is picking up the certificate.
5. The certificate extraction password and profile name are displayed. Make a note of the certificate extraction password. and tap **Install Certificate.**
6. You are prompted for the certificate extraction password and the certificate name. Enter the password you noted from Step 5, and tap **OK**. Do not change the certificate name.
7. Tap **OK** again. The certificate is installed on the mobile device.
8. If prompted for a password, 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.
9. If any additional configuration instructions were uploaded to the certificate profile, a link will appear on the success page. Tap this link to view and complete the instructions.

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

Copyright © 2012 - 2013 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.