Symantec™ Managed PKI®

Integration Guide for Fiberlink® MaaS360® Mobile Device Management

Symantec

Symantec™ Managed PKI® Integration Guide for Fiberlink® MaaS360® Mobile Device Management

Last updated May 12, 2014

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/index.html

Contents

Chapter 1

Integrating Symantec Managed PKI® with Fiberlink's MaaS360® Mobile Device Management

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 devices they use, whether you provide their devices or they bring their own.

Symantec's Managed PKI digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from several to thousands of devices, providing an in-the-cloud solution for quick deployment and easy management. It also incorporates features from Symantec's other leading security products. Symantec's Managed PKI certificates can be used to authenticate users for secure communication with company resources, such as VPNs and Web sites.

This document is intended for customers who have chosen Fiberlink's MaaS360 as their preferred Mobile Device Management (MDM) tool. It explains how to configure Managed PKI with MaaS360 to issue end-entity certificates to mobile devices using Simple Certificate Enrollment Protocol (SCEP).

MaaS360 Mobile Device Management (MDM) provides a comprehensive set of capabilities to get devices configured for enterprise access and to make sure corporate data stored on these devices is secure. MaaS360 streamlines the configuration and device enrollment process by discovering new users and devices, and allowing your company's IT to launch a simple over-the-air enrollment process for the end user.

Partner Information

The procedures listed in this document have been tested against the following platforms:

Table 1-1 Partner information

Partner name	Fiberlink
Product name	MaaS360 MDM
Device used (for certificate enrollment and installation)	Android, iOS

How the MaaS360 MDM Works

The following diagram describes how Fiberlink's MaaS360 MDM interacts with Symantec's Managed PKI to obtain a certificate for a device.

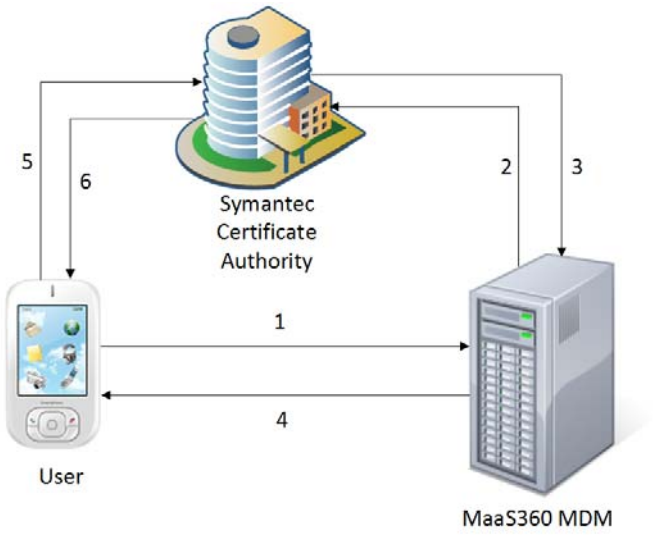

Figure 1-1 Interaction Between Fiberlink's MaaS360 MDM and Symantec's Managed PKI

1. The user initiates registration with the MaaS360 MDM from his or her mobile device.
2. MaaS360 authenticates the user and requests Symantec Managed PKI to enroll for a certificate.
3. Symantec Managed PKI accepts enrollment of the user and sends the SCEP URL to MaaS360.
4. MaaS360 forwards the SCEP URL to the requesting user.
5. The user accesses the SCEP URL to download and install the certificate from Managed PKI.
6. Symantec Managed PKI sends the certificate to the mobile device of the requesting user.

Integration Workflow

The following diagram describes the general steps required to set up a Symantec Managed PKI account and integrate the Managed PKI certificate with Fiberlink's MaaS360 MDM.

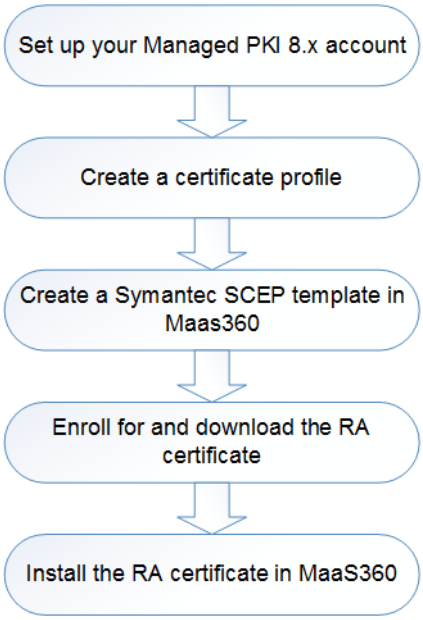

Figure 1-2 Managed PKI Integration Workflow

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. Create a Managed PKI certificate profile

Managed PKI uses a certificate profile to define the certificates issued. The certificate issued by the Client Authentication profile enables the MDM vendors to issue device certificates to mobile devices before pushing the encrypted profile to the user's mobile device.

Complete the following steps to create your Managed PKI MDM certificate profile:

1. Log into Symantec PKI Manager using your administrator certificate. You are prompted for your PKI Client PIN.
2. In PKI Manager, click **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.

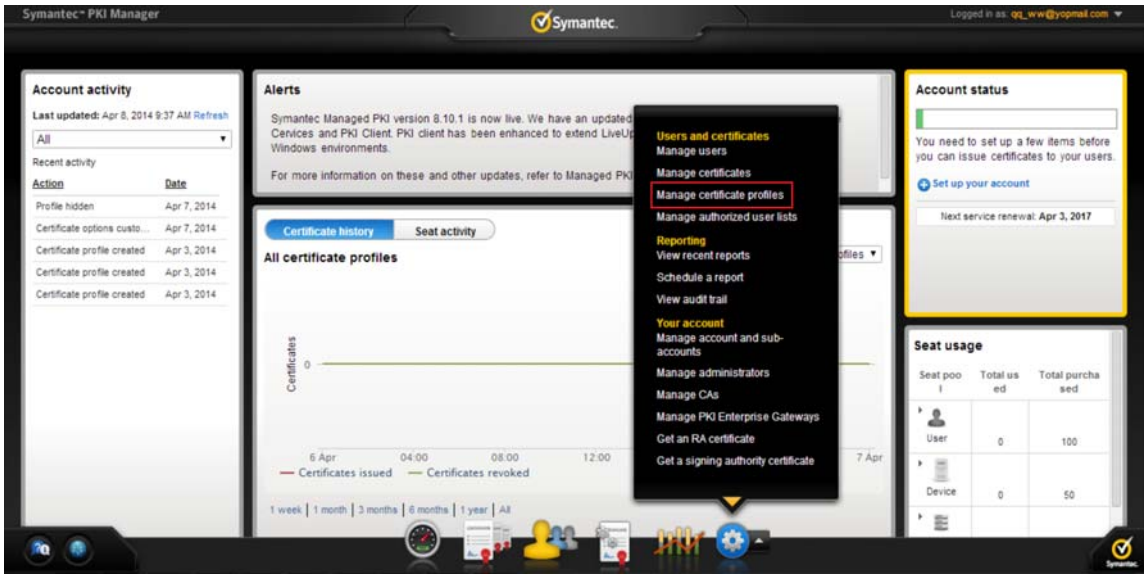

Figure 1-3 Manage Certificate Profiles Screen

3 Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page. The system displays the Create profile page.

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

5 Select **Client Authentication** as the certificate template and click **Continue**. The system displays the Customize certificate options page.

6 In the Customize certificate options, enter the Certificate profile name.

7 In the Primary certificate options section, select **SCEP** as the **Enrollment method**.

8 Click **Advanced options** and do the following:

   a Click **Add field** and select **Email address**. Email Address is now part of the Subject DN section.

   b In the **Certificate field** drop-down list, select **Email**.

   c In the **Source for the field's value** drop-down list, select **Scep Request**.

   d Set **Required?** to **Yes**.

   e Move **Email** to the top of the list using the up arrows in the Subject DN section.

   f Select **Common Name (CN)** and set **Required?** to **No**.

9 Click **Save** and then click **Continue**.

10 In the Customize user identification section, click **Edit** and verify that the **Seat ID** for the user is set to **Email**.

11 Click **Save**. The system displays the confirmation page, which shows that the certificate profile is successfully created. The page also displays the **Certificate Profile OID**, **SCEP URL** and the **PKI Certificate Service Search URL**.

Note: Make a note of the **Certificate Profile OID**, **SCEP URL** and the **PKI Certificate Service Search URL** as these details are required when configuring the Symantec SCEP template in MaaS360. You can return to the confirmation screen by clicking the **Manage certificate profiles** option and then selecting the certificate profile you created.

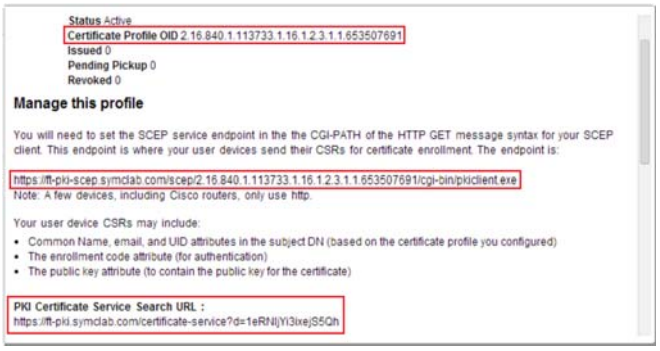

Figure 1-4 Confirmation Screen

Task 3. Create a Symantec SCEP template in MaaS360

Use the MaaS360 MDM Extender Configuration Tool to create a SCEP template. This template issues the SCEP request that devices can use to obtain the Managed PKI certificate.

Complete the following steps to create a new Symantec SCEP template:

1. Open the MaaS360 Cloud Extender Configuration Tool.
2. Check for Internet access and click **Next**.
3. Select the **Certificates Integration** check box and click **Next**.
4. On the Configure Certificate Templates screen, click **Add New Template**. The Template Configuration screen is displayed.
5. On the Template Configuration screen, enter the following details:
   - Template Name: Enter a unique template name.
   - Type: Select **Symantec SCEP (Symantec/VeriSign)**
   - URL: Enter the SCEP URL displayed while configuring the certificate profile in Symantec Managed PKI. See "Create a Managed PKI certificate profile" on page 3.
   - CA Name: Enter a unique certificate authority name.
   - Certificate Profile OID: Enter the Certificate Profile OID displayed while configuring the certificate profile in Symantec Managed PKI. See "Create a Managed PKI certificate profile" on page 3.
6. Select **Don't have a RA Certificate** to generate a Certificate Signing Request (CSR) for the RA certificate and enter a **Subject Name** and **Password** for the RA certificate.

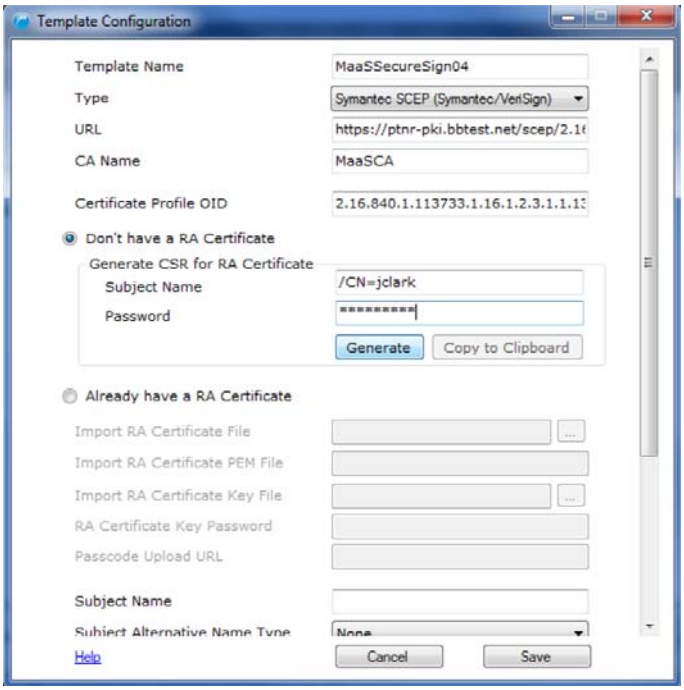

Figure 1-5 Template Configuration Screen - Generate CSR for RA Certificate

7 Click **Generate**. The system generates the CSR that you can use to obtain your RA certificate from Symantec.

8 Click **Copy to Clipboard** to copy the CSR to your clipboard.

Task 4. Enroll for and download the RA certificate

1 Log into Symantec PKI Manager using your administrator certificate. You are prompted for your PKI Client PIN.

2 On the PKI Manager page, click **Get an RA certificate** from the Tasks menu on the bottom navigation bar.

3 In the **Paste your CSR** field, paste the CSR that you previously copied to the clipboard

4 Click **Continue** to generate your RA certificate. See "Create a Symantec SCEP template in MaaS360" on page 5.

5 Download and save the resulting RA certificate to a location accessible by MaaS360.

Task 5. Install the RA certificate in MaaS360

1 On the Template Configuration screen in MaaS360, select **Already have a RA certificate**.

2 Click the button next to the **Import RA Certificate File** field and navigate to the location where you downloaded and saved the RA certificate. The system populates the **Import RA Certificate PEM File**, **Import RA Certificate Key File**, and **RA Certificate Key Password** fields.

3 Enter the remaining details:

- Passcode Upload URL: Enter **https://pki-ws.symauth.com/pki-ws/**.
- Subject Name: Enter the Subject name in the following format: **/CN=%uname%/ emailAddress=%email%/O=Fiberlink Communications/**
- Subject Alternative Name Type: Select **Email**.

- Key Type: Select the appropriate option.
- Key Size: Select the appropriate option. Only 2048 and above is supported.
- Key Usage: Select the appropriate option.
- CA Signature Algorithm: Select the appropriate option.
- CA Encryption Algorithm: Select the appropriate option.
- Certificate Storage Path: Click the button next to this field and navigate to the location where the downloaded device certificates will be stored. Typically this value is: C:\ProgramData\MaaS360\MaaS360 Visibility Service\Certs.
- Certificate Password: Enter the password for the certificate store where the device certificates will be placed.

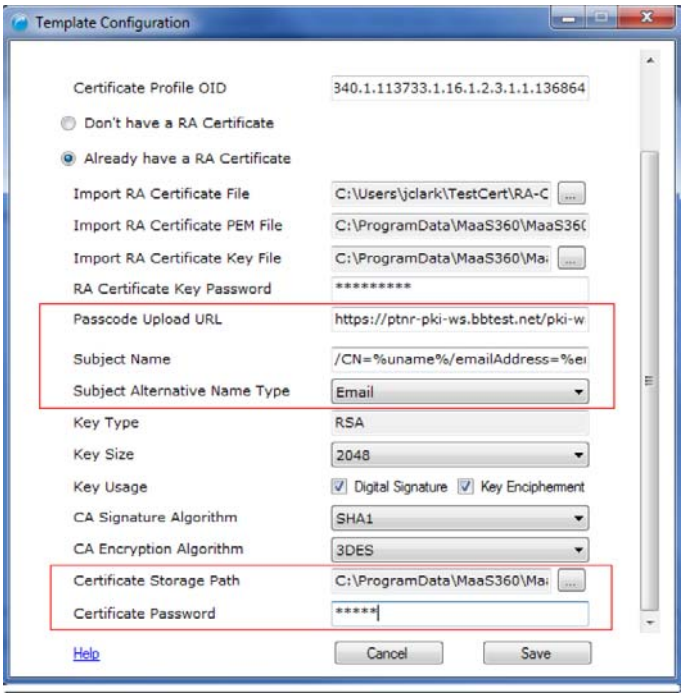

Figure 1-6 Template Configuration Screen - Create Certificate Template in MaaS360

4 Click **Save** to the save the certificate template. The new certificate template should now appear in the list of certificate templates on the Configure Certificate Templates screen.

5 Click **Next** on the Configure Certificate Templates screen.

6 Click **Finish** to close the MaaS360 Cloud Extender Configuration Tool.