Symantec™ Managed PKI®

Integration Guide for Microsoft Office 365

Symantec

Symantec™ Managed PKI® Integration Guide for Microsoft Office 365

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 June 9, 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 S/MIME Certificate with Microsoft Office 365

The enterprise workplace has moved beyond the walls of the organization into a global environment. To maintain productivity, your end users need to access company resources on the go. However, you need to be able to trust the end users accessing your systems.

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.

Microsoft Office 365 is a cloud hosted platform that offers access to various services and software built around the Microsoft Office platform. The environment provides office productivity solutions including e-mail, document creation and management, and messaging services to the enterprises. While the document and office productivity solutions can be provided by a hosted service, the enterprise user accounts may still be maintained in the organization's Active Directory.

The Office 365 service consists of a number of products and services. All of Office 365's components can be managed and configured through an online portal; users can be added manually, imported from a CSV file, or Office 365 can be set up for single sign-on with a local Active Directory using Active Directory Federation Services (AD FS)

This document discusses how to configure Microsoft Outlook 2010/2013 to use the S/MIME certificate with a Microsoft Office 365 account.

To configure Microsoft Office 365 for Single Sign On (SSO) with AD FS, refer to the *Symantec™ Managed PKI® Integrating Client Authentication Certificates for Web SSO through AD FS* guide for details.

Important! In order to configure Microsoft Outlook 2010/2013 to digitally sign and encrypt email messages, you must integrate the Managed PKI S/MIME certificate into Outlook. Once you have configured Office 365 as described in this guide, you must complete the steps in *Symantec Managed PKI Integration Guide for S/MIME* to integrate the S/MIME certificates into Outlook.

Partner Information

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

Table 1-1 Partner information

Partner name	Microsoft
Product name	Office 365
Outlook version	Outlook 2010/2013

Integration Workflow

The following diagram describes the general steps required to set up a Symantec Managed PKI account and integrate Managed PKI S/MIME certificate with Office 365.

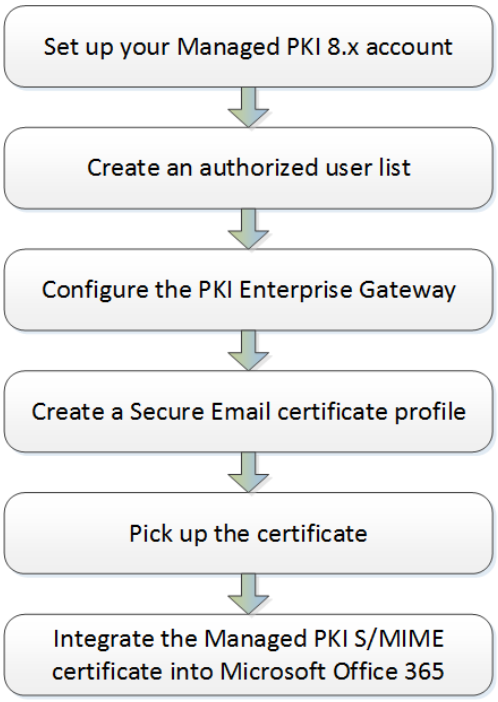

Figure 1-1 Integration Workflow

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 must 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 an authorized user list

An authorized user list identifies all employees who are eligible to get a certificate.You can create an authorized user list by identifying the Active Directory or LDAP groups that include the eligible users.

Complete the following steps to create an authorized user list:

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

2 On the PKI Manager dashboard, click **Manage authorized user lists** from the Tasks menu on the bottom navigation bar.

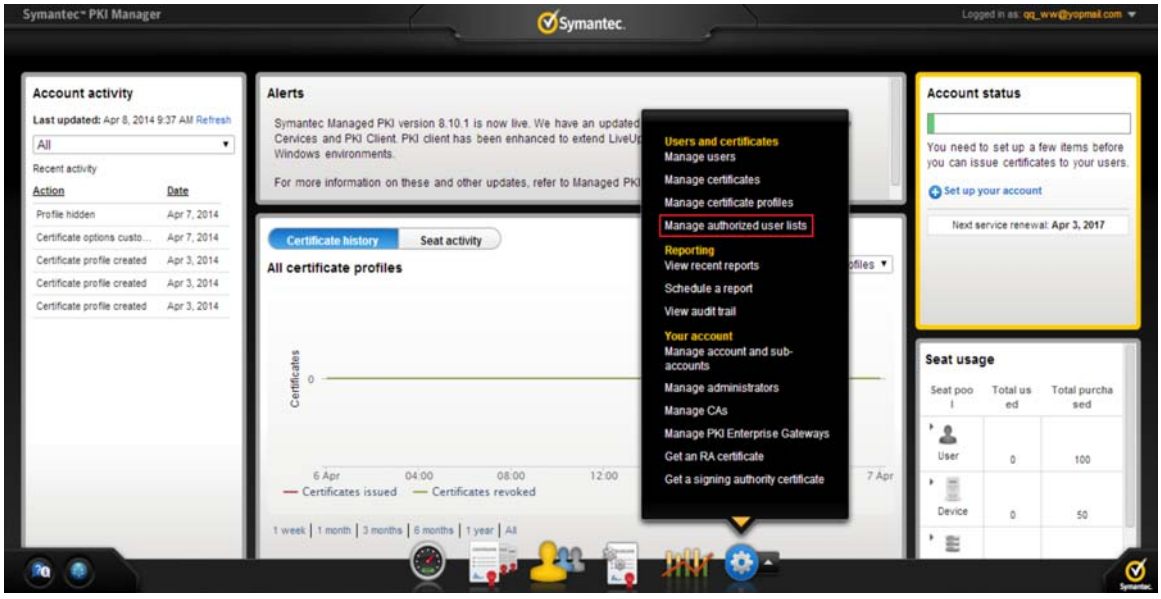

Figure 1-2 Manage Authorized User Lists

3 Click **Add authorized user lists** from the top of the resulting Manage authorized user lists page.

4 Enter the user list information in Table 1-2.

Table 1-2 User List Information

Field	Description
User list friendly name	Enter a unique name to identify this user list.
User list directory type	Select Active Directory as the user store.
Set as default for new profiles	Identify if this profile will be used for all new certificate profiles by default.
Directory groups	Enter the directory group based on the directory type selected.

5 Click **Save**.

Task 3. Configure the PKI Enterprise Gateway

Specify your PKI Enterprise Gateway settings so that you can issue certificates using your company's current employee and partner information from your Active Directory.

Complete the following steps to configure the PKI Enterprise Gateway:

1. On the PKI Manager dashboard, click **Manage PKI Enterprise Gateways** from the Tasks menu on the bottom navigation bar.
2. On the Manage PKI Enterprise Gateways page, click **Add PKI Enterprise Gateways**.
3. Enter a unique name and description for the PKI Enterprise Gateway.
4. Select **Active Directory** as the **Gateway directory type**.
5. Select **Single server** as the PKI Enterprise Gateway deployment type and enter the following PKI Enterprise Gateway component values:
   - URL where the PKI Enterprise Gateway is installed.
   - Authentication Service port number. The default value is 9101.
   - RA Agent port number. The default value is 9102.
   - RA Service port number. The default value is 9100.

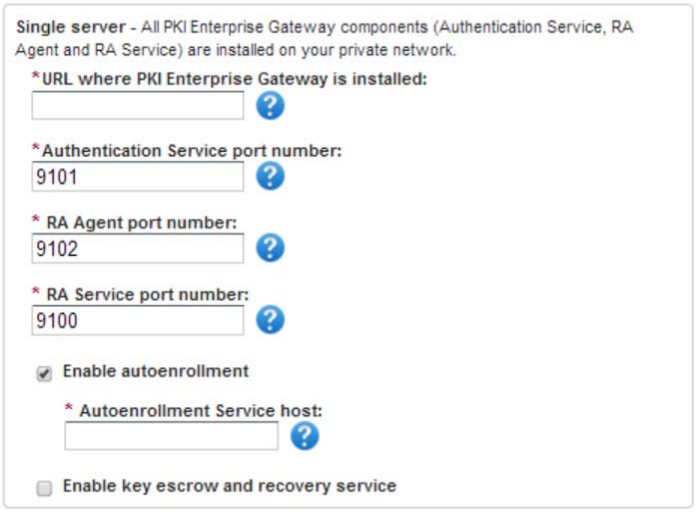

Figure 1-3 Enterprise Gateway Components

6. Select the **Enable autoenrollment** check box and enter the host name for the Autoenrollment server. The host name must be a fully qualified domain name.
7. Click **Submit** to create the new PKI Enterprise Gateway.

Task 4. Create a Secure Email certificate profile

Managed PKI uses a certificate profile to define the certificates issued. Certificates issued by the Secure Email profile support the S/MIME protocol. This certificate can be used for digital signing and/or authentication of emails through S/MIME.

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

1. On the PKI Manager dashboard, click **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.
2. Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page. The system displays the Create profile page.

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

4 Select **Secure Email** as the certificate template and click **Continue**.

5 In the Customize certificate options, enter a certificate profile name.

6 In the Primary certificate options section, select the following:

- Enrollment method: PKI Client
- Authentication method: Active Directory
- Certificate store: Computer
- Private key security level: Set an appropriate value

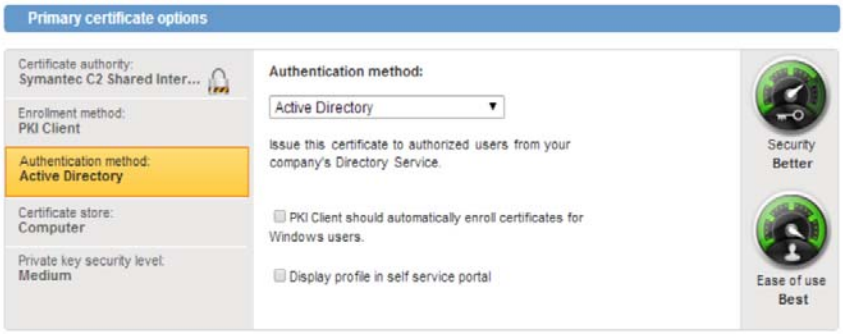

Figure 1-4 Primary Certificate Options

7 Click **Advanced options**. The system displays the Subject DN section.

8 Set the **Common Name (CN)** attributes as follows:

- Source for field's value: Active Directory attribute
- Attribute: mail

9 Set the **Organizational unit (OU)** attributes as follows:

- Source for field's value: Active Directory attribute
- Attribute: mail

10 In the SubjectAltName section, select the following:

- Source for field's value: Active Directory attribute
- Attribute: mail

11 Click **Save**.

Task 5. Pick up the certificate

Complete the following steps to download the S/MIME certificate:

1 Login to the system where you have installed Microsoft Outlook.

2 Click the enrollment link in the email.

3 Enter your Active Directory credentials.

4 Download and install the S/MIME certificate.
The certificate is installed on your machine.

Task 6. Integrate the Managed PKI S/MIME certificate into Microsoft Office 365

Complete the following steps to integrate the Managed PKI S/MIME certificate into Office 365:

1. You need to first set up Office 365. For this, make sure you meet the following prerequisites:
   - You must have administrative rights on the Office 365 portal.
   - You must register for appropriate services on the Office 365 portal.
   - You must have created users in your enterprise Active Directory. These users will be mapped to the Office 365 users.
   - You must install Outlook 2010/2013
2. Create user accounts in Microsoft Outlook 2010/2013.
3. Synchronize the Office 365 user account with Outlook by logging into the Office 365 portal using the enterprise user's Active Directory credentials.
4. Configure Microsoft Outlook 2010/2013 to digitally sign and encrypt the email messages using the MPKI S/MIME certificate. For information on configuring Microsoft Outlook with the S/MIME certificate, see *Symantec Managed PKI Integration Guide for S/MIME*.