Symantec™ Managed PKI®

Integration Guide for Cisco™ Identity Services Engine (ISE)

Symantec

Symantec™ Managed PKI® Integration Guide for Cisco™ Identity Services Engine (ISE)

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 January 28, 2015

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

https://www.symantec.com/contactsupport

Contents

Chapter 1

Integrating Symantec™ Managed PKI® with Cisco™ Identity Services Engine (ISE)

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, whether you provide the 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.

Cisco ISE helps organizations tie their network policies with the user identity. It also enables the organization's wireless network to easily integrate with various available authentication technologies.

This document explains the how to integrate Symantec™ Managed PKI® with Cisco™ Identity Services Engine (ISE) so as to enable Cisco ISE to issue valid certificates to end users and allow users to connect to the corporate network.

Note: This document contains references to *Cisco Identity Services User Guide, Release 1.2*. This user guide is maintained by Cisco and the reference topic names are prone to change.

Partner Information

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

Table 1-1 Partner Information

Partner name	Cisco
Product name	Identity Services Engine (ISE)
Version number	Release 1.2

About Setting Up Your Managed PKI 8.x Account

You must set up your Managed PKI account in order to start defining certificate profiles to begin issuing certificates. 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.

You must 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 must 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.

To configure Managed PKI, refer to Symantec PKI Manager and its online help and the Managed PKI documentation set.

Chapter 2

Configuring Cisco™ Identity Services Engine

Cisco ISE relies on Public Key Infrastructure (PKI) to provide secure communication with both endpoints and administrators, as well as between Cisco ISE nodes in a multi-node deployment.

This section discusses how to issue server and client certificates to establish trust and secure communication between an endpoint and the Cisco ISE node. Use the certificates to authenticate all HTTPS communication (Web server authentication) and the Extensible Authentication Protocol (EAP) communication (dial-up, VPN, and Wifi authentication).

The following are a summary of tasks you need to perform in order to enable Cisco ISE to issue valid certificates to end users and allow users to connect to the corporate network.

Task 1. Configure Cisco ISE for HTTPS

This section explains how to configure the Cisco ISE server for HTTPS so as to authenticate users connecting to the Cisco ISE portals. The following are the summary of procedures involved:

"Creating an HTTPS Server Certificate Profile in Managed PKI" on page 4

"Generating a CSR for the HTTPS Server Certificate in Cisco ISE" on page 5

"Enrolling for the HTTPS Server Certificate" on page 5

"Obtaining the HTTPS Server Certificate in Managed PKI" on page 5

"Installing the HTTPS Server Certificate in Cisco ISE" on page 5

Task 2. Configure Cisco ISE for EAP-TLS (WiFi)

This section discusses how to configure Cisco ISE for WiFi and also for mutual authentication between servers and clients. The following are the summary of procedures involved:

"Configuring the EAP-TLS server certificate profile in Managed PKI" on page 6

"Generating a CSR for the EAP-TLS server certificate in Cisco ISE" on page 6

"Enrolling for the EAP-TLS server certificate" on page 6

"Obtaining the EAP-TLS server certificate in Managed PKI" on page 7

"Installing the EAP-TLS server certificate in Cisco ISE" on page 7

Task 3. Configure the user to obtain the device certificate

This section explains how to obtain user device certificates.

You can configure MDMs to interact with Managed PKI to obtain the certificate. See "About configuring clients to obtain certificates using MDM" on page 7.

You can also configure Cisco ISE to issue the device certificate. See "About configuring clients to obtain certificates using Cisco ISE" on page 8.

Task 4. About Certificate Status

This section is an optional procedure and explains how to configure Cisco ISE to check for the certificate statuses. See "Revoking a Certificate" on page 9.

About Configuring Cisco ISE for HTTPS

Hypertext Transfer Protocol Secure (HTTPS) provides authentication to clients accessing the Web server hosting the Cisco ISE portals.

For details on how communication happens over HTTPS, refer to the section *HTTPS Communication Using the Cisco ISE Certificate* in *Cisco Identity Services Engine User Guide, Release 1.2*.

If you plan to use a trusted public certificate issued from the Symantec Public Root hierarchy, the Symantec root CA certificate will already be present in the browser that is used to access the Cisco ISE portal. To obtain the trusted public certificate, you need to request for one at http://www.symantec.com/en/uk/ssl-sem-page/.

Complete the following procedures to issue a certificate from the enterprise root CA maintained by Symantec. For validation purpose, you must also import the root CA certificate into Cisco ISE and also into the browsers accessing the Cisco ISE HTTPS portals.

Creating an HTTPS Server Certificate Profile in Managed PKI

You need to first create a certificate profile for users of your organization. This certificate must be signed by a Certificate Authority (CA).

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.

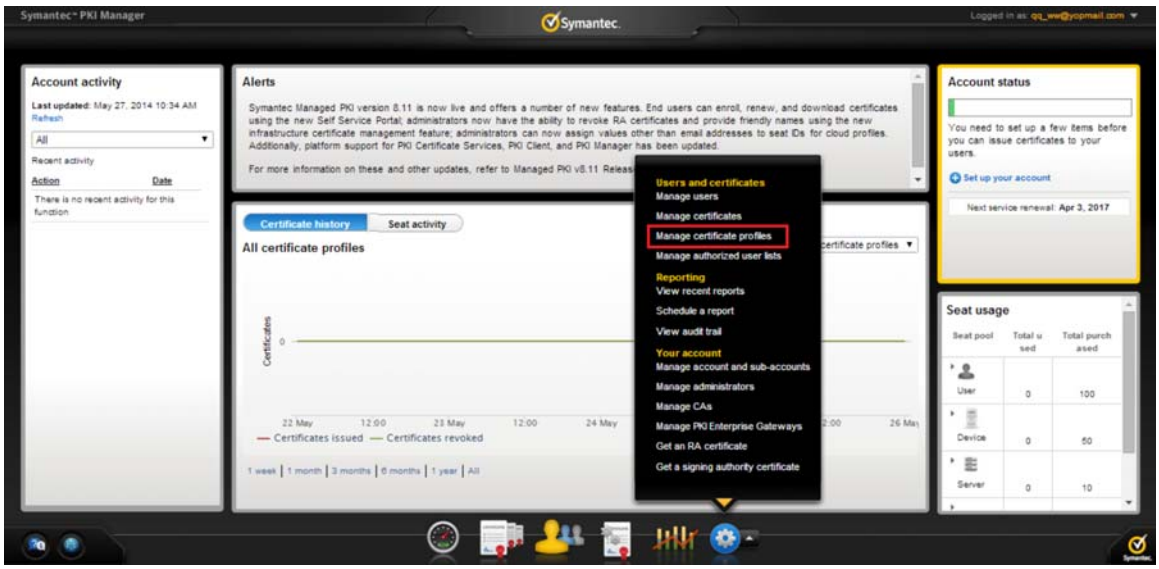

Figure 2-1 Manage Certificate Profiles

3 Click **Add Certificate profiles** at 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 **Private Server certificates** as the certificate template and click **Continue**. The system displays the Customize certificate options page.

6 In the **Customize certificate options** section, enter the certificate profile name.

7 In the **Primary certificate options** section, select **CSR** as the **Enrollment method**. The **Authentication method** is locked to **Manual approval**.

8 Click **Save**, and then click **Continue**. The system displays the confirmation page that shows that the certificate profile is successfully created. The page also displays the **PKI Certificate Services URL**.

Generating a CSR for the HTTPS Server Certificate in Cisco ISE

You need to generate a Certificate Signing Request (CSR) that needs to be uploaded into PKI Manager to enroll for the HTTPS server certificate. For more details on how to generate a CSR, refer to the section *Generating a Certificate Signing Request* in *Cisco Identity Services Engine User Guide, Release 1.2*.

Enrolling for the HTTPS Server Certificate

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

2 Click **Manage certificate profiles** and then select the certificate profile you created. See "Creating an HTTPS Server Certificate Profile in Managed PKI" on page 4.

3 Open a browser and enter the **PKI Certificate Services URL** that is displayed on the page.

4 Enter the details and paste the CSR in the **Paste your CSR** field. See "Generating a CSR for the HTTPS Server Certificate in Cisco ISE" on page 5.

5 Click **Continue** to submit the request for approval.

Obtaining the HTTPS Server Certificate in Managed PKI

To obtain the HTTPS server certificate, you need to log into PKI Manager and approve the certificate request.

1 Log into PKI Manager using your administrator certificate.

2 Click **Manage Users** or select **Managed Users** from the **Tasks** menu on the bottom navigation bar.

3 Select the pending request for the HTTPS server certificate.

4 Click **Manage this request**.

5 Select **Approved**, and click **Save**. The HTTPS certificate is signed, issued, and sent to the email address that you provided when you requested the certificate.

Installing the HTTPS Server Certificate in Cisco ISE

After you receive the signed HTTPS certificate, you must bind this certificate with its private key to install the server certificate in Cisco ISE. For more information on how to install the HTTPS server certificate, refer to the section *Binding a CA-Signed Certificate* in *Cisco Identity Services Engine User Guide, Release 1.2*.

About Configuring Cisco ISE for EAP-TLS (WiFi)

Extensible Authentication Protocol Transport Layer Security (EAP-TLS) provides mutual authentication to authenticate the client and server while securing the tunnel.

For details on how communication happens over EAP-TLS using the Cisco ISE certificate, refer to the section *EAP Communication Using the Cisco ISE Certificate* in *Cisco Identity Services Engine User Guide, Release 1.2*.

This section describes the following:

- "About Configuring the EAP-TLS Server Certificate" on page 6
- "About Configuring the User to Obtain the Device Certificate" on page 7

About Configuring the EAP-TLS Server Certificate

If you plan to use a trusted public certificate issued from the Symantec Public Root hierarchy, the Symantec root CA certificate will already be present in the browser that is used to access the Cisco ISE portal. To obtain the trusted public certificate, you need to request for one at http://www.symantec.com/en/uk/ssl-sem-page/.

Complete the following procedures to issue a certificate from the enterprise root CA maintained by Symantec. For validation purpose, you must also import the root CA certificate into Cisco ISE.

The EAP-TLS server certificate must also be present in the user's devices connecting to the EAP-TLS server. For more information on how to provision the server certificates for the user devices, refer to your Mobile Device Management documentation or the Cisco ISE documentation.

Configuring the EAP-TLS server certificate profile in Managed PKI

You need to first create a certificate profile for users of your organization. This certificate must be signed by a Certificate Authority (CA).

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.
3. Click **Add Certificate profiles** at 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 **Private Server certificates** as the certificate template and click **Continue**. The system displays the Customize certificate options page.
6. In the **Customize certificate options** section, enter the certificate profile name.
7. In the **Primary certificate options** section, select **CSR** as the **Enrollment method**. The **Authentication method** is locked to **Manual approval**.
8. Click **Save** and then click **Continue**. The system displays the confirmation page, which shows that the certificate profile is successfully created. The page also displays the **PKI Certificate Services URL**.

Generating a CSR for the EAP-TLS server certificate in Cisco ISE

You need to generate a CSR that needs to be uploaded into PKI Manager to enroll for the EAP-TLS server certificate. For more information on how to generate a CSR, refer to the section *Generating a Certificate Signing Request* in *Cisco Identity Services Engine User Guide, Release 1.2*.

Enrolling for the EAP-TLS server certificate

1. Log into Symantec PKI Manager using your administrator certificate. You are prompted for your PKI Client PIN.
1. Click **Manage certificate profiles** and then select the certificate profile you created. See "Configuring the EAP-TLS server certificate profile in Managed PKI" on page 6.
2. Open a browser and enter the **PKI Certificate Services URL** that is displayed on the page.
3. Enter the details and paste the CSR in the **Paste your CSR** field. See "Generating a CSR for the EAP-TLS server certificate in Cisco ISE" on page 6.
4. Click **Continue**. The request is submitted for approval.

Obtaining the EAP-TLS server certificate in Managed PKI

You need to log into PKI Manager using your administrator credentials and approve the pending certificates.

1. Log into PKI Manager using your administrator certificate.
2. Click **Manage Users** or select **Managed Users** from the Tasks menu on the bottom navigation bar.
3. Select the pending approval request for the server certificate.
4. Click **Manage this request**.
5. Select **Approved** and click **Save**. The certificate is issued and sent to the registered email ID.

Installing the EAP-TLS server certificate in Cisco ISE

After you receive the signed EAP-TLS server certificate, you must bind this certificate with its private key to install the server certificate in Cisco ISE. For more information on how to install the EAP-TLS server certificate, refer to the section *Binding a CA-Signed Certificate* in *Cisco Identity Services Engine User Guide, Release 1.2*.

About Configuring the User to Obtain the Device Certificate

You need to configure the mobile devices of your users who want to access your company's network to obtain the device certificate. The device certificate authorizes that the user is a valid user with access permissions. You can configure the user's device to obtain the certificate in the following two ways:

- Configure the user's device to obtain the device certificate using an MDM. See "About configuring clients to obtain certificates using MDM" on page 7.
- Configure the user's device to obtain the device certificate using Cisco ISE. See "About configuring clients to obtain certificates using Cisco ISE" on page 8.

About configuring clients to obtain certificates using MDM

Cisco ISE may use MDMs as a policy server to control the use of some applications on a mobile device.

Cisco ISE supports the following MDM vendors:

- Airwatch, Inc.
- MobileIron, Inc.
- Citrix XenMobile
- Fiberlink MaaS

For more information on how to configure the MDM with Symantec Managed PKI, click on the Symantec PKI **Resources** icon in the lower left corner of Symantec PKI Manager and select the appropriate Integration Guide.

For more information on how to configure the MDMs in Cisco ISE, refer to the section *Setting Up MDM Servers With Cisco ISE* in *Cisco Identity Services Engine User Guide, Release 1.2*.

About configuring clients to obtain certificates using Cisco ISE

Cisco ISE manages the registered mobile device users that access the Cisco network. This section describes how Cisco ISE manages its user's devices to deploy the device certificate.

The following diagram describes how Cisco ISE interacts with Symantec's Managed PKI to obtain a device certificate:

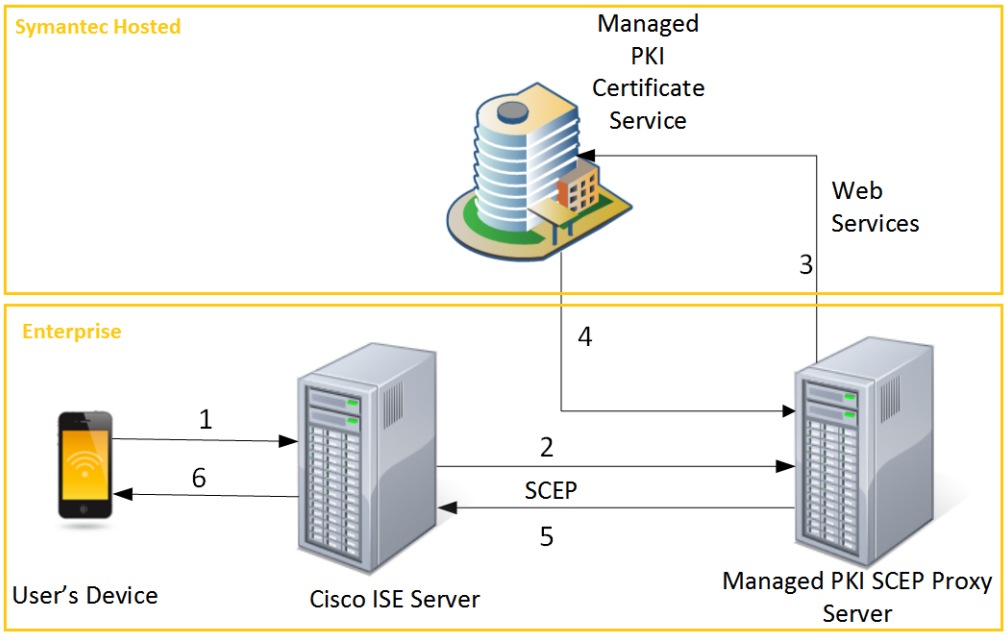

Figure 2-2 Interaction Between Cisco ISE and Symantec's Managed PKI

1 A registered mobile device requests for a device certificate.

> **Note:** For more information on how to register your mobile device, refer to the section *Supporting Personal Devices* in *Cisco Identity Services Engine User Guide, Release 1.2*.

2 The Cisco ISE server sends the SCEP request to the Managed PKI SCEP Proxy server.

3 After receiving the SCEP request, the Managed PKI SCEP Proxy server sends a Web Services request to Managed PKI for certificate enrollment.

4 Managed PKI sends the certificate to the Managed PKI SCEP Proxy server.

5 After the Managed PKI SCEP Proxy server receives the Web Services response, it sends the certificate to the ISE server.

6 The ISE server forwards the certificate to the user's device.

For more information on how to configure the Managed PKI SCEP Proxy server, refer to the *Symantec Managed PKI SCEP Integration Guide*.

For more information on how to configure SCEP in Cisco ISE, refer to the section *Simple Certificate Enrollment Protocol Profiles* in *Cisco Identity Services Engine User Guide, Release 1.2*.

About Certificate Status

Every certificate has an expiry date that determines the certificate validity. You can configure the method to check for a certificate status per CA. The two methods by which you can check the status of a certificate are:

- Online Certificate Status Protocol (OCSP): The OCSP servers are updates in real time. Cisco ISE primarily performs certificate validation using the OCSP servers via HTTP.
- Certificate Revocation List (CRL): CRL is updated once in a fixed period of time. Cisco ISE switches to checking the CRL in case of failure of the primary and secondary OCSP servers.

For more information on how Cisco ISE checks for the certificate status, refer to the section *OSCP Services* in *Cisco Identity Services User Guide, Release 1.2*.

Revoking a Certificate

You may need to revoke a certificate for the following reasons:

- The user's original certificate is lost or stolen.
- The user leaves your company.
- The user no longer needs the certificate.
- User information in the original certificate is no longer valid.

A revoked certificate is permanently deactivated and no longer valid. A revoked certificate can no longer be used to access the services that the certificate is intended for.

Complete the following steps to revoke a certificate:

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** from the Tasks menu on the bottom navigation bar. The Manage certificates page displays the list of certificates with their statuses.
3. Click on a certificate and then click **Revoke certificate**.
4. Select a reason to revoke the certificate and click **Revoke certificate**.