Symantec[™] Managed PKI[®]

Integration Guide for MobileIron[®] Virtual SmartPhone Platform



Symantec[™] Managed PKI[®] Integration Guide for MobileIron[®] Virtual Smartphone Platform

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 November 13, 2013

Legal Notice

ii

Copyright © 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.

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 Certificates with the MobileIron Virtual Smartphone Platform	® 1
	Partner Information	1
	How the MobileIron VSP Works	2
	Integration Workflow	3
Chapter 2	Configuring MobileIron® VSP	7
	Adding the SCEP Profile for Configuration of MobileIron® VSP with Symantec Managed PKI	l 7
	Applying App Settings to Labels	. 10
	Adding a label	. 10
	Applying label to setting or configuration	. 10
	Applying label to a device	. 10
	Registering the Device	. 10
	Verifying the Certificate on VSP Admin Portal	. 12
	Verifying the Certificate on PKI Manager	. 12
	Connecting to Mobile Device	. 13
	Connecting an iOS device to MobileIron	. 13
	Connecting an Android device to MobileIron	. 14

iv Contents

Integrating Symantec Managed PKI Certificates with the MobileIron[®] Virtual Smartphone Platform

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 communications with company resources, such as VPNs and web sites.

This document is intended for customers who have chosen MobileIron as their preferred Mobile Device Management (MDM) vendor. It explains how to configure Managed PKI with the MobileIron Virtual Smartphone Platform (VSP) to issue end-entity certificates to mobile devices using Simple Certificate Enrollment Protocol (SCEP).

Partner Information

These procedures have been tested on the following platforms:

Table 1-1Partner Information

Partner Name	MobileIron [®]
Product Name	MobileIron® VSP
MobileIron® VSP version	5.7 and higher
Device (for certificate enrollment and installation)	iOS 7, Android 4.2

2 Integrating Symantec Managed PKI Certificates with the MobileIron® Virtual Smartphone Platform How the MobileIron VSP Works

How the MobileIron VSP Works

The following diagram describes how MobileIron VSP interacts with Symantec's Managed PKI to obtain a certificate for a device.



Figure 1-1 MobileIron VSP's interaction with Symantec Managed PKI

- **1** The mobile device initiates registration with MobileIron VSP using a MobileIron agent installed on the device.
- 2 MobileIron VSP authenticates the user and mobile device, interacts with MobileIron agent on the device, and gathers the device details.
- 3 MobileIron VSP requests Symantec Managed PKI to enroll for certificate.
- 4 Symantec Managed PKI accepts enrollment of the device and sends it to MobileIron VSP.
- 5 The MobileIron VSP sends the certificate to the mobile device.

Integration Workflow

The following diagram describes the general steps required to set up a Symantec Managed PKI account and integrate Managed PKI certificates with MobileIron VSP.



Figure 1-2 Managed PKI Integration Workflow

Task 1. Set up your Managed PKI 8.9 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 certificate profile

Managed PKI uses a certificate profile to define the certificates issued. Certificate issued by MDM profile enables Mobile Device Management (MDM) vendors to issue device certificates down 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 on to Managed PKI's PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.
- 2 On PKI Manager, click **Manage certificate profiles** or select **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.

Account activity	Alerts	Account status		
Last updated: Oct 17, 2013 6 09 AM Refresh All Part And P	Symanteo Managed PKI is pleased to announce that version 8.9 is now LIVE. This version includes significant advances in a number of key seas; administrators now have the ability to delete certificate profiles and revole multiple certificates at one time. Web services have been enhanced, and third-party integration all website in the dole of comband through the PKI Manager Revolute apple. Additionally, Manager PKI 38 analise arguitations to perform a valiable for dominant Organizational certificate and Secure Email Gateway certificates (contact your Symantic nepresentative if you with to take advantage of these new certificate templates). For more information on the these and other security updates available in this release, refer to Managed PKI v3.9 Release notes available on the Resources page.	You need to set up you can issue certi users. Set up your accourt Next service rene	a few ite ficates to nt wai: Oct 17,	ms before your 2016
	There is no data to display for this account.			
		Seat usage Seat pool	Total used	Total
	Users and certificates Manage users Manage perificates	Seat usage Seat pool	Total used 0	Total purchased 1000
	Users and certificates Manage users Manage certificates Manage certificates	Seat usage Seat pool	Total used 0	Total purchased 1000
	Users and certificates Manage certificates Manage certificates Manage certificates Manage services profiles Manage certificates Properting	Seat usage Seat pool User Device	Total used	Total purchased 1000 100
	Users and certificates Manage users Manage certificates Manage certificates Manage school perfise Manage school perfise Vere resert, sports School de a coro r	Seat usage Seat pool User Device Sarver Sarver	Total used 0 0	Total purchased 1000 100 100
	Users and certificates Manage users Manage certificates Manage certificates Manage suthorized user lists Responsion Visan societ ruports Solicable a ruport Visan societ ruports	Seat usage Seat pool User Device Server Server Organization	Total used 0 0 0	Total purchased 1000 100 100 100
	Users and certificates Manage users Manage certificates Manage certificates Manage schiftschaft perfiles Manage schiftschaft perfiles Weier societ into Schichule a report View societ rasi Schichule a report View societ trait Schichule a report View societ trait	Seat usage Set pool User Device Server Server Server Loboe CDS Organization	Total used 0 0 0 0	Total purchased 1000 100 100 100 100
	Users and certificates Manage users Manage certificates Manage certificates profiles Manage and the state fists Reporting Var refect sports Solid-bide report Var refect sports Solid-bide report Var refect sports Solid-bide report Var and rail Var and and Manage account and solid- abcounts Manage account and solid- abcounts	Seat usage Set pool User Device Server Server Cryanization Cryanization Cryanization	Total used 0 0 0 0	Total purchased 1000 100 100 100 100
	Users and certificates Manage users Manage certificates Manage certificates Manage schortzed user fists Reporting Visue monit reports Solidable argorit Visue audit trail Your account Manage Schortzet and Aud- abcounts Manage Phil Enterprise Subserves	Seat usage Set pool User Divice Server Server Criganization Criganization Criganization Secure Enail Gateway Boy more seas	Total used 0 0 0 0 0	Total purchased 1000 100 100 100 100 100
	Users and certificates Manage certificates Manage certificates Manage certificates Manage authorized user lists Reporting Verse receit reports Solidable argort Verse audit stal Your secont Manage PAR discount et auto- accounts Manage CAs Manage CAs	Seat usage Seat pool User Device Server Graenization Adobet CDS Organization Market Server Se	Total used 0 0 0 0	Total purchased 1000 100 100 100 100

Figure 1-3Manage Certificate Profile

- **3** Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page. The Create profile page appears.
- 4 Select whether these certificates will be issued in Test mode or Production Mode, and click **Continue**. The Create profile page appears.
- 5 Select **MDM (Web Service Client)** as the certificate template and click **Continue**. The Customize certificate options page appears.
- 6 In the Customize certificate options, enter a certificate profile name.

Symantec * PKI Manager		⊘ Symantec	Logged in as: mawit@yopmail.com
Manage Certificate profiles X Contract portal Search operations: Search by: Show all Enter criteria: Show all Include hidden certificate profiles Search	Add Certificate profiles Add Certificate profiles Certificate profiles No results found.	Create profile: Select mode Select templare Costomize options Customize services Customize certificate options Review and change the template options for this profile. Certificate hierdry name: Mobile from MOM	3
		Envolment mathod: PPI Nueb Services Authonication method: Crd party application Not applicable Private bary security level Not applicable Private bary security level Not applicable	
		Back Cancel Preview Save	
Pa (0)		© ⊒ <u>₩</u> 2 ₩ 2	

Figure 1-4 MDM (Web Service Client) Certificate options

7 The Primary certificate options are selected appropriately.

Click Advanced options to view certificate options and define any additional attributes you may need.

8 Click Save.

On the confirmation page, you can view the attribute used for the seat ID, a mandatory attribute that authenticates the user for third-party configurations or during enrollment process. This is typically the user's email address.

You can also customize the profile further, such as adding custom scripts, and customizing languages or email notifications on this page.

6 Integrating Symantec Managed PKI Certificates with the MobileIron® Virtual Smartphone Platform Integration Workflow



Configuring MobileIron® VSP

This chapter discusses how to configure MobileIron VSP with Symantec Managed PKI.

Adding the SCEP Profile for Configuration of MobileIron[®] VSP with Symantec Managed PKI

You must add a SCEP profile within the MobileIron VSP's Admin Portal to configure MobileIron VSP with Symantec Managed PKI service.

- 1 In MobileIron VSP's Admin Portal, enter your login credentials and click Sign In.
- 2 To create new users:
 - a Select USERS & DEVICES and click USERS. The Users Details page is displayed.
 - b Click Add Local User.
 - **c** Enter the user's user ID, first name, last name, password, and email address to identify the user being added.

						abels Users Retired Devices	
		r Delete User	Link to LDAP User To: Aut	thorized Users 💌		by Name 🔎 Resync with LDAP Force Password Change	
dit	Name	User ID	Email	Creation Date	Source	Roles	
2	admin	admin	address@domain.com	2011-02-08 8:2	Local	Admin Locate, Admin Wipe, Apps / File Catalogs, Event Center, Mobile Activity Intelligence, MyPhone@Wo	
2	Leo Markensteijn	leom	leotest1@mobileiron.com	2013-10-08 5:4	Local	API, Admin Locate, Admin Wipe, Apps / File Catalogs, Enterprise Connector Access, Event Center, Policie	
2	mitest	mitest	mitest@mobileiron.com	2013-10-09 7:4	Local	User Portal	
2	mpei	mpei	mpei@yahoo.com	Add New User			
2	srikanth v	srikv	srikanth_v@symantec.com		Iser ID:	ogs, Enterprise Connector Access, Event Center, Policie	
				First	Name:		
				Last	Name:		
				Display	Name:		
				Pas	sword:		
				Confirm Pa	sword:		
					Email:		
				Save			

Figure 2-1 Add User

d Click Save.

e Device is registered for users and registration details will be sent to email addresses provided.

From: notifications@mobileiron.net[mailto:notifications@mobileiron.net] Sent: Thursday, October 17, 2013 02:49 PM To: Srikanth V. Subject: verisigndev device registration instructions for test user (6687689876)
verisigndev is using MobileIron's Virtual Smartphone Platform to enable access to corporate resources.
To allow you to easily register your device with this system, we have sent a registration text message to 6687689876.
From your device:
1) Open the text message.
2) Click the link.
3) Tap 'Get App'.
4) Download the MobileIron Mobile@Work application from the Google Play Store.
5) Launch the MobileIron app from your device's home screen and fill in the following information:
 Server Address: m.mobileiron.net:43761 User Name: stikv Password: your password
6) Update your device's configuration, in accordance with IT policy, by following the configuration prompts.
If you encounter any difficulty registering your device, please contact your IT administrator for assistance.
NOTE: If you do not receive the text message, or are not able to follow the link, please go directly to https://m.mobileiron.net/verisigndev/c/d/android.html via your device's web browser and them begin at step 3

Figure 2-2 Instructions for Device Registration

- **3** To add new configurations:
 - a Select **POLICIES & CONFIGS** and click **Configurations**. The Configurations page is displayed.
 - b Click Add New and from the sub-menu, select SCEP. The New SCEP settings page appears.

		hboard Confi	gurations Policies							
lete More Actions •	Add New • Label	s: All-Smartphones	V Search	n by User 🔎						
Name 🔺	Setting Type	Bundle/Package ID	Desc # Phones Lab	els	WatchList	App Setting Details				
System - Multi-User Secur	WEBCLIP		Auto 0		0 C			_		
System - IOS Enrollment C	CERTIFICATE New	SCEP Setting						\bowtie		
System - iOS Enrollment S	SCEP						Save	Cancel		
System - IOS Enterprise A	WEBCLIP									
System - IOS Enterprise A	SCEP	Name:						- n		
System - iOS MDM	MDM	Description:								
System - IOS MDM CA Cert	CERTIFICATE									
NEWSCEP	SCEP	Enable Proxy:	V							
	SCEP		Cache locally generated	keys on the VSP 🟮				E .		
	APPENROLLM		O User Certificate	Device Certificate				3	w details	
System - Windows Phone	SCEP	Setting Type:	Symanter Web Services N	Jananed PKT						
			Synancee treb Sernees I	andges the						
		Server:	pki-ws.symauth.com							
		Certificate:	Upload Certificate							
		Mo	bile Profiles: Please select	profile			~			
	Sau	Cancal								
	oav	Cancel								



c Enter the field values listed in Table 2-1 to add a SCEP profile.

Table 2-1Manage SCEP Settings

Field	Value
Name	Enter a name (for example, Symantec Managed PKI)

Table 2-1Manage SCEP Settings

Field	Value
Description	Enter a description.
Enable Proxy	 Select Enable Proxy and then select an option based on your business requirement: Cache locally generated keys on the VSP - Specifies if VSP stores the private key sent to each device. If you remove the cache requirements after device is provisioned, you must re-provision the certificates for all the impacted devices. User Certificate - Specifies that certificate issued to multiple devices is assigned to a single user. Device Certificate - Specifies that the certificate is bound to the given device.
Setting Type	Select Symantec Web Services Managed PKI.
Server	Enter the server address for the Symantec Web Services Managed PKI (received from Symantec). The default is set to pki-ws.symauth.com. Note: Only the host name of the Symantec CA server should be provided. Do not add https:// before the server name, and do not add path information after the
Certificate	server name. Click Upload Certificate to navigate and select the RA certificate you received from Symantec. This is usually a .p12 file. Enter the password for the certificate when prompted.
Mobile Profiles	Select the MDM (Web Services Client) profile to use for this setting. Only the object ID (OID) for the profile is listed. The OID is a series of numbers. Before selecting the profile, you may want to verify with the Symantec Web Services PKI manager for the correct OID.
Required Fields	The Required Fields and Optional Fields for the certificate are displayed based on how the MDM (Web Service Client) profile was set up in the Symantec PKI Manager. The SeatID value in the SCEP settings must map to the value you created for the SeatID in the Symantec PKI Manager.
Optional Fields	Symantec does not require optional fields, but they are still used if available. Therefore, you must still specify the appropriate variable for each optional field. For example, the phone number might be an optional field because the tablets in your organization do not have phone numbers. However, the Symantec Web Services server might still use this information to request a certificate from the PKI server if it is present.
Issue Test Certificate	Select this option to issue a test certificate to verify the SCEP settings. Some certificate authorities charge for each certificate. To avoid incurring additional charges, clear this check box after initial testing.

4 Click Save.

A new SCEP setting is created and listed in the App Settings page. The SCEP profile that is created with the name identified (for example, Symantec Web Services Managed PKI) can be accessed in network settings such as Exchange, Wi-Fi, or VPN profiles where certificate authentication is required.

Applying App Settings to Labels

After you create SCEP settings, you need to apply label to tag the phones that is associated with a group.

Adding a label

To apply a label to the app settings:

- 1 On the MobileIron VSP Admin portal, select USERS & DEVICES and click Labels.
- 2 Click Add New to create a label.
- **3** Enter a name and description for the label.
- 4 Click Save.

Applying label to setting or configuration

To apply a created label to a setting or a configuration:

- 1 On the MobileIron VSP Admin portal, select **POLICIES & CONFIGS** and select the label that you created.
- 2 Click More Actions > Apply to Label.
- **3** Select the name of the label you want to associate with the configuration. For example, Android, iOS, Employee-Owned, Company-Owned, and so on.
- 4 Click Apply. A message is displayed to confirm that the labels are applied to the configuration.

Applying label to a device

To apply a created label to a device:

- 1 On the MobileIron VSP Admin portal, select USERS & DEVICES and click Devices.
- 2 Select the device you want to associate with the configuration.
- 3 Click Actions. From the sub-menu, select Apply to Label.
- 4 Select the name of the label you want to associate with the device.
- 5 Click Apply. A message is displayed to confirm that the labels are applied to the device.

Registering the Device

To register the device on the MobileIron VSP Admin portal:

- 1 Select USERS & DEVICES and click Devices.
- 2 Click Add. From the sub-menu, select Single Device or Multiple Devices.
 - a Enroll for a single device by entering device details.

User:		
	This device has no phone nur	nbei
Device Platform:	Select Platform	~
Country:	United States	~
Mobile:	1 Prefix and Number Country Code	
Operator:	Select Operator	~
Device Owner:	🖲 Company 🔘 Employee	
Device Language:	English 👻	
Email User:		



b Enroll for multiple devices at one time by uploading a comma-separated value (csv) file with your user data.

Ac	ldir	ng Multiple De	vices										×
	Mul	tiple Devices File:	AddMultipl	eDevicesFile	Browse	nport File	Sample	e CSV File	Ap	ply			
		User	Status	Password	Country C	Mobile Num	Oper	Platform	Owner	Source	First Name	Last Name	

Figure 2-5 Add Multiple devices

- 3 Click **Register**. You will receive the registration steps in mobile or email.
- **4** Follow the instructions that you received in the text message or email to complete the device registration.

On successful device registration, the certificate is issued to the device.

Verifying the Certificate on VSP Admin Portal

To verify the certificate on the MobileIron VSP Admin portal:

1 Select LOGS & EVENTS and click Certificate Logs. All the registered devices will be displayed.

			ι	JSERS & DEVI	CES APPS POLI	CIES & CONFIGS	SETTINGS	LOGS & EVENTS	
			Ν	IDM Logs	Certificate Logs	All Logs Event Se	ettings	Events	
R	move Revoke	Sear	ch by User/Set	ting Nam 🔎	Expiration Date Range:	То		Search	
	Last Name 🔻	Fi	User	Phone Num	Email	Setting Name	Cert Type	Expiration Date	Content
	v	sri	srikv	PDA	address_v@symantec.com	System - iOS Enterpri		2014-10-09 9:56:08 PM	View
	Pei	Ming	mpei	6508105037	mpei@yahoo.com	System - iOS Enterpri		2014-09-05 2:08:57 PM	View
	admin	ad	admin	PDA 2	address@domain.com	System - iOS Enterpri		2014-10-10 1:42:09	View
			misys_ano		anonymous@mobileiron.com	Enrollment SCEP templ	User Certif	2043-10-07 11:18:3	View

Figure 2-6 Verifying the Certificate on MobileIron VSP Admin Portal

2 Select the device for which you need to view certificate information and click View.

Verifying the Certificate on PKI Manager

To verify the certificate on PKI Manager:

- 1 On PKI Manager, click **Manage certificates** or select **Manage certificates** from the Tasks menu on the bottom navigation bar. The Manage certificates page displays the status of the issued certificates.
- 2 Select a certificate to view the details of the certificate.

Configuring MobileIron® VSP Connecting to Mobile Device

Connecting to Mobile Device

The following are the scenarios through which an end user can connect their devices to the MobileIron VSP to securely access company resources.

Connecting an iOS device to MobileIron

- 1 Download the **Mobile@Work** application from App StoreSM.
- 2 Tap MobileIron.
- 3 Enter the user name and tap Next.
- 4 Enter the server details that you received in the email and tap Next.
- 5 Enter the password and tap **Register**.

		Mobile@Work	l l l l l l l l l l l l l l l l l l l
		MODICEMOIN	
User Name	rikv		
Server	m.mobileiron.net:43761		
Password	•••••		
		POWERED BY	
		MobileIron	

Figure 2-7 Credentials Screen

6 A confirmation page is displayed.



Figure 2-8iOS Confirmation Screen

Connecting an Android device to MobileIron

- 1 Download the **Mobile@Work** application from the Google PlayTM.
- 2 Tap MobileIron.
- 3 Enter the server details that you received in the email and tap Next.
- 4 Enter the user name and tap Next.
- 5 Enter the password and tap **Register**.
- 6 Tap **CONFIGURE** to configure the certificate. The Certificate Setup page is displayed.

Google Play Apps	
In-house Apps	
Configuration Update	
Your Mobile@Work admin has provided an update for your device. Follow the setup instructions that appear.	
Certificate	
CONFIGURE	

Figure 2-9 Android Configuration

7 Click Next. Press and hold in the password field and tap Paste to extract the certificate.

4ae_add9_37c6944427fa
4ae_add9_37c6944427fa es.
4ae_add9_37c6944427fa ^{es.}



8 Click OK.

16 Configuring MobileIron® VSP Connecting to Mobile Device