Symantec[™] Managed PKI[®]

Integration Guide for ActiveSync®



Symantec[™] Managed PKI[®] Integration Guide for ActiveSync[®]

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 March 28, 2013

Legal Notice

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.

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/contact/index.html#support4

Contents

Chapter 1	Integrating Managed PKI Certificates with Microsoft [®] ActiveSync [®]	1
	Pre-requisites	1
	Integration Overview	1
	Prepare for Certificate Mapping for ActiveSync	1
	Configure ActiveSync to Request Certificates	
	Configure ActiveSync to Map Certificates to Active Directory	
	Configure IIS and ActiveSync to Trust a Third Party CA	
	Map Certificates	
	Certificate Mapping Option 1 - Alternative Security Identities	
	Certificate Mapping Option 2 - UPN mapping	
	Test ActiveSync	
	Test Certificate Mapping	
	Test with an ActiveSync Emulator	
	Verifying if the CDP is Available	

iv Contents

Chapter

Integrating Managed PKI Certificates with Microsoft[®] ActiveSync[®]

Managed PKI certificates can be integrated with many common applications to enable secure communications and online access. This document describes how to integrate Managed PKI certificates with Microsoft® ActiveSync® to enable S/MIME (with or without userID and password authentication) using certificate mapping.

Pre-requisites

This integration has been qualified on the following platform:

- Microsoft Exchange ActiveSync[®] 14
- Windows[®] 2008 Server R2 64-bit Standard or Enterprise edition
- Microsoft Exchange[®] Server 2010
- Microsoft Internet Information Services[®] (IIS) 7.5

Integration Overview

Integrating Managed PKI certificates with ActiveSync consists of the following general steps:

- "Prepare for Certificate Mapping for ActiveSync" on page 1
- "Map Certificates" on page 5
- "Test ActiveSync" on page 7

Prepare for Certificate Mapping for ActiveSync

To prepare certificate mapping for ActiveSync, you configure ActiveSync and Exchange to enable certificate mapping for Active Directory (AD). Note the following special considerations:

- Your Exchange server and ActiveSync must be configured for userID and password.
- The Exchange server must be a member of a domain.
- The CDP for certificates issued by Managed PKI and which map to ActiveSync must be reachable without going through a proxy. If your client certificates are missing, the CDP is not available, or if the CRL cannot be accessed, certificate mapping will fail.
- To check if your CDP is not available, refer to the procedures in "Verifying if the CDP is Available" on page 9.

Note: If you are unable to reach the CRL without going through a proxy, you can set the web server to run as an administrator. Refer to the instructions at http://support.microsoft.com/kb/294305. However, running the web server as an administrator is not recommended.

Configure ActiveSync to Request Certificates

- 1 Open the Exchange Management console.
- $2 \quad Click \ on \ Server \ Configuration \rightarrow Client \ Access \rightarrow Exchange \ Active Sync \rightarrow Properties.$
- 3 Select the Authentication tab.

General	Authentication Remote File Servers	
To ena	the authentication method or methods that this virtual directory accepts ble authentication between the Exchange server and a mobile phone, Basic authentication or Client certificate authentication is required.	
⊠ Ba	sic authentication (password is sent in clear text)	
Client o	ertificate authentication:	
Ignore client certificates		
C Accept client certificates		
• <u>R</u> e	quire client certificates	
	configure SSL settings for this ActiveSync virtual directory, use the emet Information Services (IIS) snap-in.	



- To enable certificate and userID/password authentication, select Basic authentication (password is sent in clear text) and Require client certificates.
- To enable certificate authentication only, select Require client certificates.

Configure ActiveSync to Map Certificates to Active Directory

1 The ability to map certificates to Active Directory is typically not enabled by default. You must enable this manually. Refer to the Active Directory documentation or Microsoft for instructions. Make sure that the following Authentication options are enabled:





Figure 1-2 Top-level authentication method settings

- **b** At the Microsoft-Server-ActiveSync level:
 - Enable basic authentication for certificate and userID/password authentication.
 - Disable all authentication methods for certificate only authentication.





2 Using a POWERSHELL, run the following commands to enable mapping to occur at the ActiveSync level. This can be done manually or programmatically.

C:\Windows\SysWOW64\inetsrv\appcmd.exe unlock config /section:client CertificateMappingAuthentication

The command will return the following response:

Unlocked section "system.webServer/security/authentication/client CertificateMappingAuthentication" at configuration path "MACHINE/ WEBROOT/APPHOST".

C:\Windows\SysWOW64\inetsrv\appcmd.exe set config "Default Web Site/ Microsoft-Server-ActiveSync" -section:clientCertificateMapping Authentication /enabled:true

The command will return the following response:

Applied configuration changes to section "system.webServer/security/ authentication/clientCertificateMappingAuthentication" for "MACHINE/ WEBROOT/APPHOST/Default Web Site/Microsoft-Server-ActiveSync" at configuration commit path "MACHINE/WEBROOT/APPHOST/Default Web Site/ Microsoft-Server-ActiveSync"

3 Restart the World Wide Web Publishing Service. From the **Start** menu, click **Administrative Tools**→ Services → World Wide Web Publishing Service → Restart.

Configure IIS and ActiveSync to Trust a Third Party CA

Complete the following steps on the system that hosts Exchange and ActiveSync to establish a trust relationship with the IIS server.

- 1 Open the Microsoft Management Console (MMC).
- 2 Click File → Add/Remove Snap-in....
- 3 Select the Certificate snap-in for the Computer account on the local computer and click OK.

Console1 - [Console Root]	Add or Remove Snap-ins You can select snap-ins for this console from those available on your computer and o extensible snap-ins; you can configure which extensions are enabled. Available snap-ins: Selected snap-ins:
File Action View Favorites Window Help New Ctrl+N Open Ctrl+O Save Ctrl+S Save As Add/Remove Snap-in Ctrl+M Optons 1 C:\Windows\system32\dsa.msc 2 ServerManager.msc 3 Exchange Management Console.m 4 C:\Windows\\services.msc Exit	Snap-in Vendor Active Directory Do Morosoft Cor Active Directory Ste Morosoft Cor Active Scontrol Morosoft Cor Active Scontrol Morosoft Cor Active Scontrol Morosoft Cor Certificates Morosoft Cor Computer Management. Morosoft Cor Device Manager Morosoft Cor Device Manager Museus manage certificates for. Museus Exchance Server 2010 Museus account Description: Computer account Computer sconset Computer account

Figure 1-4 Selecting the Certificate snap-in for the Computer account on the local computer

- 4 Double-click Certificates (Local Computer).
- 5 Double-click Trusted Root Certificate Authorities.
- 6 Right-click on the Certificates folder under Trusted Root Certification Authorities and click All Tasks.
- 7 Select Import.

Console1 - [Console F	Root\Certificates (Loc	al Computer)\Truste
File Action View	Favorites Window H	Help
Þ 🔿 🖄 📅 🗎	a 🗟 🚺 🖬	
Console Root		Issued To 🔺
🖃 🔂 Certificates (Local C	Computer)	Class 3 Public
Ŧ 📄 Personal		Class 3 Public
🖃 📄 Trusted Root C	ertification Authorities	Copyright (c)
🚞 Certificates		
🕀 🧮 Enterprise Tru:	All Tasks	Import
🕀 🚞 Intermediate C	View	Microsoft Aut
🛨 📔 Trusted Publish		
🗉 🧮 Untrusted Cert	New Window from Her	
🛨 🧮 Third-Party Ro	New Taskpad View	Microsoft Cor
Trusted People	non rasipaa nonni	Microsoft Roo
🕀 🦳 Remote Deskto	Refresh	Microsoft Roo
🕀 🦳 Certificate Enri	Export List	Microsoft Tim
E Smart Card Tru		Microsoft Tim
Trusted Device.	Help	NO LIABILITY
E _ Husted Device		RootCA1

Figure 1-5 Importing the trusted CAs

8 Follow the prompts to install the trusted root CAs.

9 Repeat Step 1, "Open the Microsoft Management Console (MMC)." through Step 8, "Follow the prompts to install the trusted root CAs." for any intermediate CAs, except import them to the Intermediate Certification Authorities → Certificates branch rather than the Trusted Root Certification Authorities → Certificates branch.

Map Certificates

There are two ways to map certificates with Microsoft. You can implement one or both of these methods.

Alternative Security Identities: This method is the most reliable method of mapping and works with any client authentication certificate. There is no need for specific fields in the certificate to be managed (no need to set UPN in SubjectAltName for example). Both One-to-One and Many-to-One mapping methods are available, which allows greater flexibility. Many-to-One also facilitates mapping many certificates to a single service account.

Symantec has qualified this method with all versions of ActiveSync.

 Universal Principal Name (UPN) Mapping: This method allows certificates that include a UPN field in their Subject Alternative Name to map to the Universal Principal Name for the user. If you do not have a UPN in your certificate that matches the corresponding user's Universal Principal Name, then you must use the Alternative Security Identities method for certificate mapping.

Symantec has qualified this method with ActiveSync 14 and 14.1.

Certificate Mapping Option 1 - Alternative Security Identities

- 1 Open the Active Directory Users and Computers snap-in. From the **Start** menu, click **Administrative Tools** → **Active Directory Users and Computers**.
- 2 Select View \rightarrow Advanced Features.
- 3 Navigate to your end user (under Users).
- 4 Right-click on the user's name and select Name Mappings.



Figure 1-6 Selecting Name Mappings for an end user

- 5 The Security Identity Mapping dialog box appears. Click **Add** and navigate to the certificate that you want to map to this user (the certificate should be in x509 format).
- 6 Select how you want the certificate to be mapped:

- To have this certificate map to one user, select the **Use Issuer for alternate security identity** and **Use Subject for alternate security identity** checkboxes. This is the default.
- To map additional certificates to this user, click **Add** and map another certificate, making sure that the **Use Issuer for alternate security identity** and **Use Subject for alternate security identity** checkboxes are selected for each certificate added.
- If you want all certificates from this issuer to map to this user, unselect the **Use Subject for alternative security identity** checkbox. You might use this when you want all certificates from a private root to map to a single service account.

Attribute	Information	
	E=testUser@cademo1.com	
	CN=test user	
	CN=Users	
	DC=cademo1	
Subject	DC=com	
	CN-RootCA1	
<u> </u>		
Identity Ma	pping	
🗹 Usels	suer for alternate security identity	
Use St	ubject for alternate security identity	

Figure 1-7

Mapping a single certificate to a single user

Certificate Mapping Option 2 - UPN mapping

Configure your domain to recognize your Certificate Authority as being authorized to issue certificates that include the UPN value:

- 1 Obtain a copy of your root CA certificate (.cer) and copy it to your domain controller (this is typically not the same machine that hosts Exchange and ActiveSync).
- **2** Issue the following command when logged in as Domain Administrator on the Primary Domain Controller:

certutil -dspublish -f YourRoot.cer NTAuthCA

Where YourRoot.cer is the filename of the root CA that you want to authorize to use the UPN mapping.

It may take some time for this change to replicate across all systems on the domain.

• You can verify if an individual system has recognized this update by examining the following registry location:

 $HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates\NTAuth\Certificates$

Double-click on the certificates under this branch and look for one that includes the subject DN of YourRoot.cer.

• You can immediately force the update on any system in the domain by running the gupdate /force command on that system.

			Certifi	cate	
			Gene	ral Details Certification Pat	h
			Sho	w: <al></al>	
			Fie	aq	Value
test user Properties		<u>? ×</u>		SMIME Capabilities Subject Key Identifier Certificate Template Name	[1]SMIME Capability: Object I cc 09 3c 6d dd 1a 1c ca 40 50 User
Dial-in	Environment	Sessions		Authority Key Identifier	KeyID=a2 09 6f ab ac 77 ec 0
Remote control	Remote Desk	top Services Profile	l l l	CRL Distribution Points	[1]CRL Distribution Point: Distr
Personal Virtual De	sktop COM+	UNIX Attributes		Authority Information Access	[1]Authority Info Access: Acc
General Address Ac		Organization Member Of		Enhanced Key Usage	Encrypting File System (1.3.6
			3	Subject Alternative Name	Other Name:Principal Name=.
User logon name:					`
testUser	@cademo1.co	m 🔹		ier Name: Principal Name=testUser@cade	emo1.com
the state of the s					
User logon name (pre-					
CADEMO1\	testUser		ſ		
Logon Hours	Log On To				

Figure 1-8 Verifying if the root CA has been recognized by a user's system

Test ActiveSync

Testing your configuration requires two steps:

- "Test Certificate Mapping" on page 7
- "Test with an ActiveSync Emulator" on page 8

Test Certificate Mapping

Complete the following steps to test if the certificate mapping is configured correctly.

- 1 Select a user that has an Exchange mailbox for which certificate mapping has been configured.
- 2 Use the private key for the user's certificate to install the certificate into Internet Explorer.
- **3** Using Internet Explorer, navigate to https://<ExchangeServer>/Microsoft-Server-ActiveSync (for example, https://exch1.cademo1.com/Microsoft-Server-ActiveSync.)

You are prompted to select or confirm a certificate. This should be the user certificate added in previous step. (If not, verify that you set the correct root and intermediate CAs as trusted in "Configure IIS and ActiveSync to Trust a Third Party CA" on page 4.

4 Select the certificate. You may see an error page with a message similar to the following:

HTTP Error 505.0 - Http Version Not Supported

This page cannot be displayed because the HTTP version is not supported.

- 8 | Integrating Managed PKI Certificates with Microsoft® ActiveSync® Test ActiveSync
 - You can safely ignore this error.



Figure 1-9 Verifying the Logon User

- 5 Verify that the Logon User matches the expected user in the certificate mapping (see Figure 1-7). If the Logon User is Anonymous or To be determined, verify that you have configured your certificate mapping correctly in "Map Certificates" on page 5. Also:
 - Make sure you issue the appcmd.exe commands as described in "Configure ActiveSync to Map Certificates to Active Directory" on page 2.
 - Make sure you can reach the CRL that is published in the CDP without having to go through a proxy.

Test with an ActiveSync Emulator

Using an ActiveSync emulator, test that the configuration works end-to-end. This example test uses the Exchange ActiveSync MD (EAS MD) available at http://mobilitydojo.net/downloads.

- 1 Select Trust all Certificates.
- 2 Enter the userID in the Username field, but leave the Password field blank.
- 3 Select Use Client Certificate (Specify Path) and enter the path to the certificate file.
 - If you enter the path to a .cer file (where the private key is installed already in CAPI), leave the **Certificate password (if applicable)** field blank.
 - If you enter the path to a .pfx file, enter the password for the file in the **Certificate password (if applicable)** field.

4 Click **Basic Connectivity Test** or **Full Sync Test**, as appropriate. You will be prompted to select which MS-APProtocol Version you want to test if you run the Full Sync Test. All tests should pass.

ain	Device Information Certificate	nfo Information Rights Management Base64 Utility Autodiscover About
~	nnection Parameters	
Use	mame: testUser	Device Id: Provisionable
Pas	isword:	Device Type
Don	main: cademo1.com	User Agent: Support security policies
Sen	ver Address:	Output
excl	h1.cademo1.com	
Only	y FQDN - don't include http(s)://	Clear Output Rinary XML Word Wrap (Binary XML) Base64
	Use SSI	
	Use Client Certificate (Specify Path)	Testing HTTP GET:
_		Response: The remote server returned an error: (505) Http Version Not Supported. Explanation:
· · · · ·	Users\Public\testUser.cer	This is consist, behaviour, and means your Exchange server is responding!
Cert	tificate password (f applicable):	Status: PASS
		Testing HTTP OPTIONS:
		Alow OPTIONS, POST
MS	ASProtocolVersion	MS-Server-ActiveSync:14.1
	.1 (Exchange 2010 SP1)	MS-ASProtocolVersions:2.0,2.1,2.5,12.0,12.1,14.0,14.1 MS-
	.0 (Exchange 2010)	ASProtocolCommands:Sync,SendMail,SmartForward,SmartReply,GetAttachment,GetHierarchy,Cr
	.1 (Exchange 2007 SP1) .0 (Exchange 2007 RTM)	eateCollection,DeleteCollection,MoveCollection,FolderSync,FolderCreate,FolderDelete,FolderUpd
12	.0 (Exchange 2007 RTM)	ate.MoveItems,GetItemEstimate.MeetingResponse,Search,Settings,Ping.ItemOperations,Provision ResolveRecipients.ValidateCert
		Public:OPTIONS.POST
Act	ione	Content-Length:0
1		Cache-Control private Date:Thu, 17 Nov 2011 04:34:17 GMT
	Basic Connectivity Test	Server:Microsoft-IIS/7.5
Ē	Full Sync Test	X-AspNet-Version:2.0.50727
_	Full Sync Test	X-Powered-By:ASP.NET
	Remote Wipe (Emulated)	Status: PASS

Figure 1-10 Testing with the Exchange ActiveSync MD emulator

Verifying if the CDP is Available

Complete the following steps to verify if the CDP is available:

- 10 Integrating Managed PKI Certificates with Microsoft® ActiveSync® Verifying if the CDP is Available
 - 1 Enroll for and pick up a sample client certificate. The CRL Distribution Points will be listed in the certificate. Open the certificate to view the details.

Certificate	? 🛛			
General Details Certification Pa	th			
Show: <all></all>	~			
Field	Value 🔨			
🖻 Valid from	Monday, November 21, 2011			
Valid to	Wednesday, November 21, 20 🔤			
Subject	alantest0102.verisign.net			
Public key	RSA (2048 Bits)			
Subject Alternative Name	DNS Name=alantest0102.veri			
Basic Constraints	Subject Type=End Entity, Pat			
CRL Distribution Points	[1]CRL Distribution Point: Distr			
Subject Key Identifier	b2 69 48 39 95 a2 cd 1f 89 99 💌			
[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://pilotonsitecrl.verisign.com/VeriSignIncSCEPTesting1/LatestCR L.crl				
[Edit Properties Copy to File			
	ОК			



- 2 Select CRL Distribution Points.
- **3** Copy and paste the URL into a browser.

If you are prompted to download the CRL, you have successfully reached the CDP from your browser.

Index

Α

ActiveSync testing 7-9 testing with an emulator 8 Alternative Security Identities mapping certificates by 5 appcmd.exe 3, 8 Authentication options 2

В

Basic Connectivity Test 9

С

CDP 1.8 certificate configure ActiveSync to map Active Directory to 2 configure ActiveSync to request 2 configure ActiveSync to trust third-party CAs 4 configure IIS to trust third-party CAs 4 map additional to one user 6 map all to one user 6 map one to one user 6 mapping 5 root CA 6 testing mapping 7 using Alternative Security Identities to map 5 using UPN to map 6 certificate authentication 2 certificate mapping preparing for 1 configure ActiveSync to map certificates to Active Directory 2 configure ActiveSync to request certificates 2 configure ActiveSync to trust third-party CAs 4 configure IIS to trust third-party CAs 4 console Exchange Management 2 CRL 1,8

D

domain controller 6

Ε

EAS MD see Exchange ActiveSync MD emulator testing 8 Exchange ActiveSync MD 8 Exchange mailbox 7 Exchange Management console 2

F

Full Sync Test 9

G

gupdate 7

Η

hardware requirements 1

I

intermediate CAs 5

Μ

mailbox 7 map additional certificates to a user 6 map all certificates to a user 6 map one certificate to a user 6 mapping certificates 5 test certificate 7 MD 8 Microsoft Management Console 4 MMC see Microsoft Management Console MS-APProtocol 9

Ρ

platform requirements 1 preparing for certificate mapping 1 pre-requisites 1 private key 7 proxy 2

R

requirements 1 root CA 6

S

software requirements 1 special considerations 1

Т

test ActiveSync 7-9 ActiveSync emulator 8 certificate mapping 7 third-party CAs configuring ActiveSync to trust 4 configuring IIS to trust 4 intermediate 5 trusting intermediate CAs 5

U

Universal Principal Name

see UPN UPN mapping certificates by 6 userID/password authentication 2

W

World Wide Web Publishing Service 4