iPad authentication with Symantec MPKI and Active Sync connections

Lab IC L23

Description	iPad authentication lab using Symantec's MPKI certificates for authentication through an Active Sync connection.
At the end of this lab, you should be able to	▪ Use Symantec Managed PKI Service to strongly authenticate users and secure the communication between their mobile device and a Microsoft Exchange server using the ActiveSync protocol ▪ In this lab, you will perform the following exercises o PKI Administrator - Enroll for Symantec Managed PKI Service Free Trial o PKI Administrator - Administer and configure the service to issue Client Authentication certificate and configuration payload that enable a mobile device to connect to Microsoft Exchange mailbox using ActiveSync o End User - Enroll and install the ActiveSync certificate/configuration o End User – Connect to your Exchange mailbox

Notes

- URLs needed for this lab
  - http://www.symantec.com/theme.jsp?themeid=free-trial – Symantec Managed PKI Service Free Trial
    Enroll for a free Test Drive account
  - http://mailinator.com/ - Mailinator – Free, disposable email.
    Use internet email service when enrolling for your free trial account to receive the email to pick-up your PKI Administrator certificate, and to receive the end-user enrollment email sent to the mobile device.

    If you have your own internet accessible email account, you are encouraged to use it instead.

    (If mailinator.com is not responding, you can also try http://www.yopmail.com)
  - https://testdrive-pki-manager.symauth.com/pki-manager/ - Symantec PKI Manager
    Access your MPKI account as PKI Administrator
- Microsoft Exchange ActiveSync Host
  `mail.ua.tso-cloud.com`

LAB AGENDA

Lab Exercise 1: PKI Administrator - Enroll for Symantec Managed PKI Service Free Trial

Quick, easy and free access to the Symantec Managed PKI Service online.

Lab Exercise 2: PKI Administrator - Configure your MPKI account for mobile device ActiveSync certificate use-case

Configure ActiveSync certificate profile for target device

- Select the Secure Sign-in certificate template
- Configure the Delivery Method (iOS) and Enrollment Method to include the enrollment code in the email
- Set the client ActiveSync configuration to use with the certificate.

Send ActiveSync certificate enrollment email to end-user

- Add the user to PKI Manager
- Enroll the user for the ActiveSync certificate profile for their device

Lab Exercise 3: End-user - Certificate enrollment, installation, configuration and usage

Device certificate enrollment, profile installation and configuration

Access your Exchange mailbox

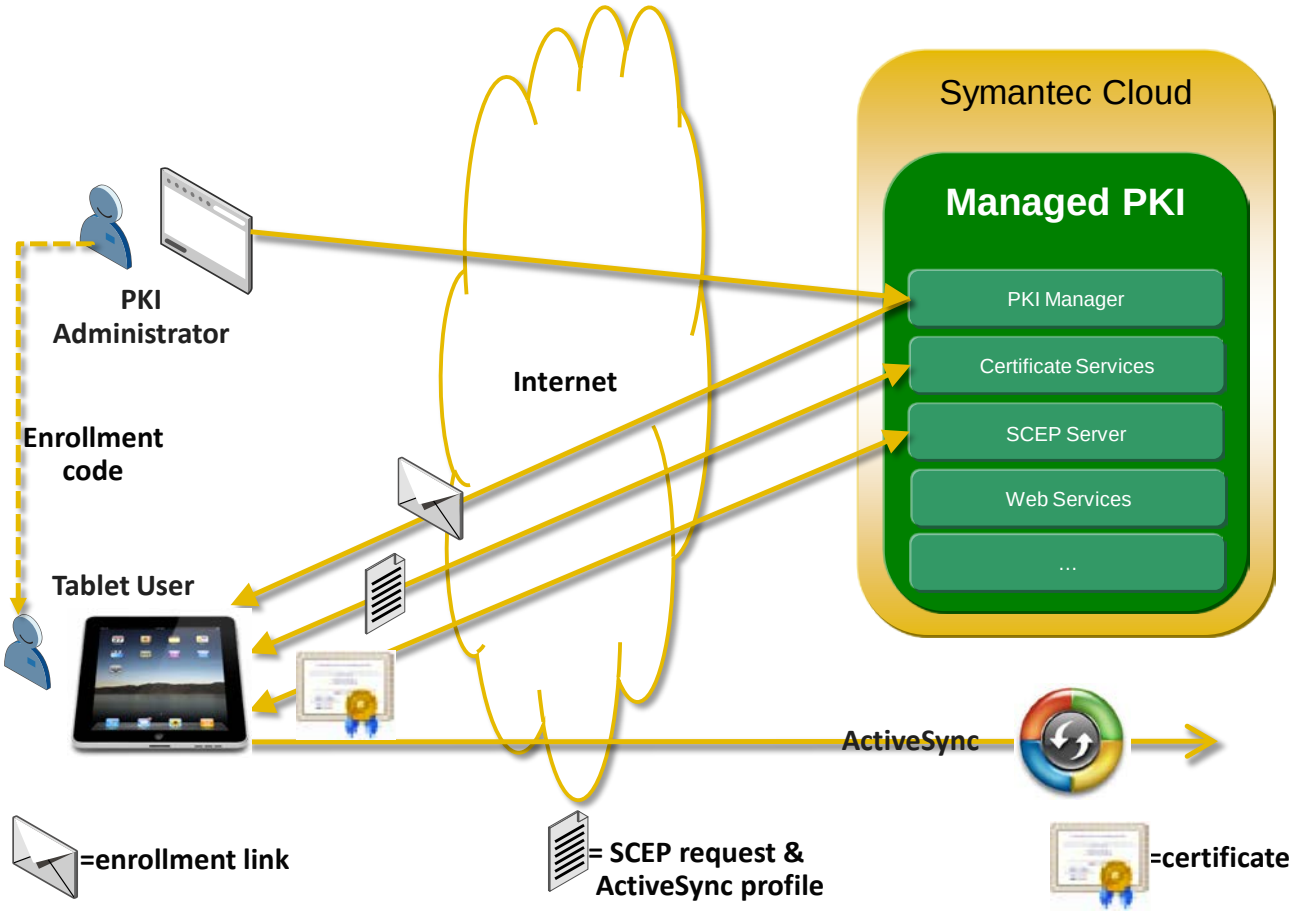
Discuss the Microsoft Exchange server side configuration

Trust the Issuing CA
Map certificate to domain user account

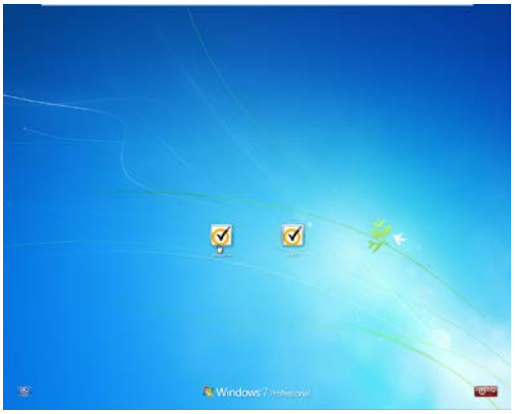
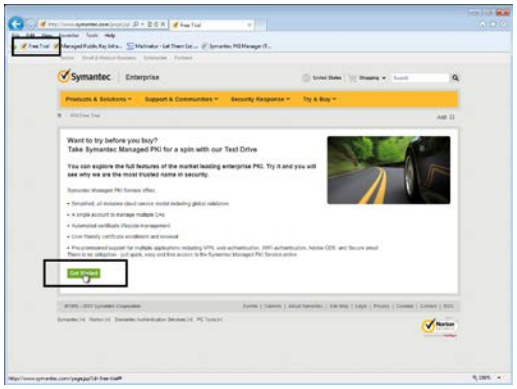
See **MPKI_ActiveSync.pdf** (Downloadable from **PKI Manager | Resources**.)

Appendix A – Removing the iOS Profile

LAB LAYOUT


Symantec Cloud
Managed PKI
PKI Manager
Certificate Services
SCEP Server
Web Services
...
PKI
Administrator
Internet
Enrollment
code
Tablet User
ActiveSync
=enrollment link
= SCEP request &
ActiveSync profile
=certificate

Lab Exercise 1: PKI Administrator - Enroll for Symantec Managed PKI Service Free Trial

1	***PKI Administrator - Register for Symantec Managed PKI Service Test Drive*** Login to Windows 7 User: **pkiadmin** Open a web browser and go to: http://www.symantec.com/theme.jsp?themeid=free-trial Click the link "**Get Started**".	 

Fill out the entire form.

Once you have submitted the registration form, you will be sent an email to pick-up your PKI Administrator certificate.

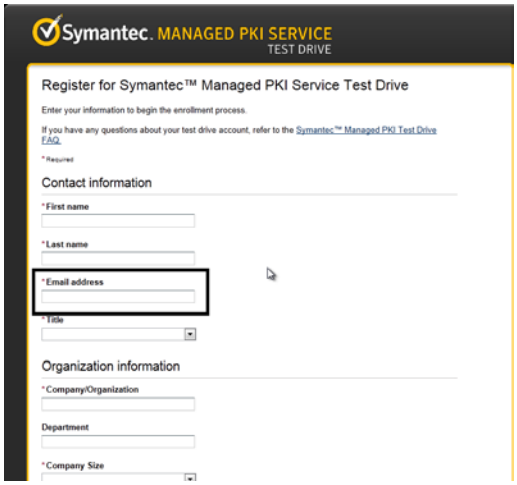
* *Choose an email address that you can retrieve email from the internet. It is recommended that you use your own internet accessible email account, if you have one.*

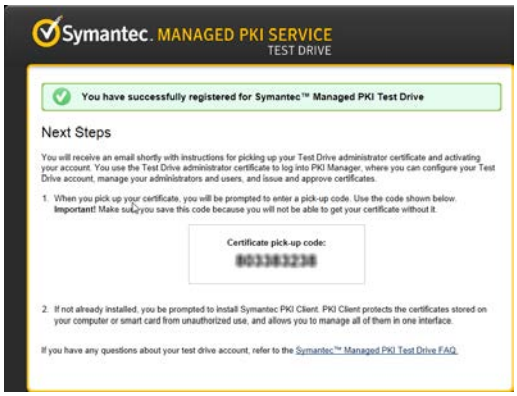
If you do not have you own email account, it is recommended that you use a free @mailinator.com email address.

If using mailinator.com, choose something unique for your administrator email address.

For example "VISION2013<yourFirstName><lastInitial>@mailinator.com"

I.e., "VISION2013LanceH@mailinator.com"

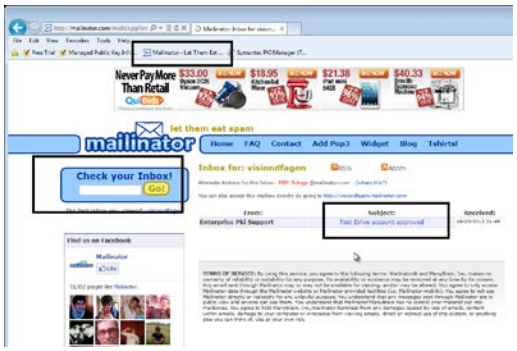




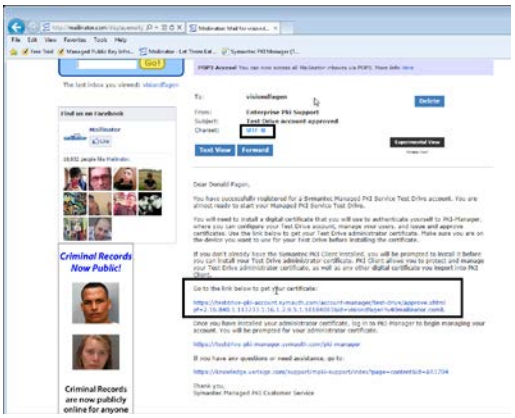
Retrieve your email to pick-up and install your PKI Administrator certificate

If using a mailinator.com email account, use your web browser to go to http://mailinator.com/ and login using the email address you chose in the previous step.

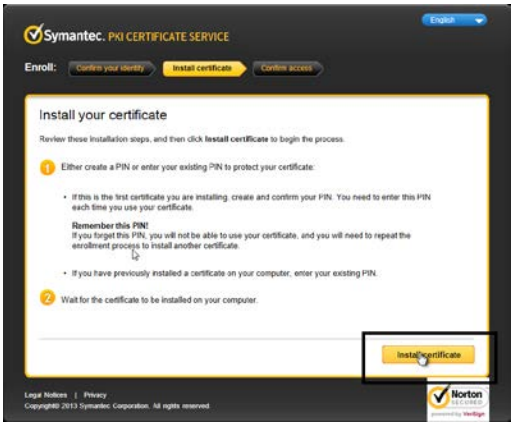
Open the email subject "Test Drive account approved".



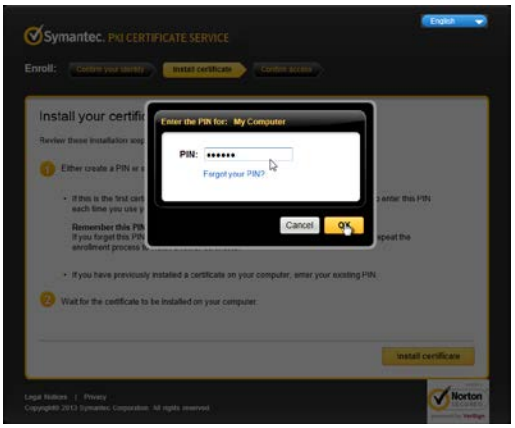
In the email body, click on the link labeled, "*Go to the link below to get your certificate:*"



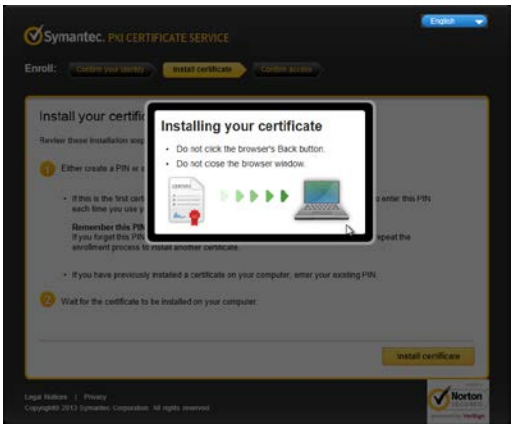
Wait for the page to load completely and click **Install Certificate**



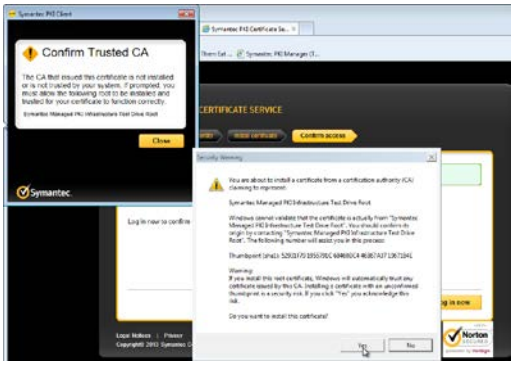
For this lab, the PIN has already been set. Enter the PIN: **123456**



Do not interrupt the browser while generating the key-pair and installing your certificate.



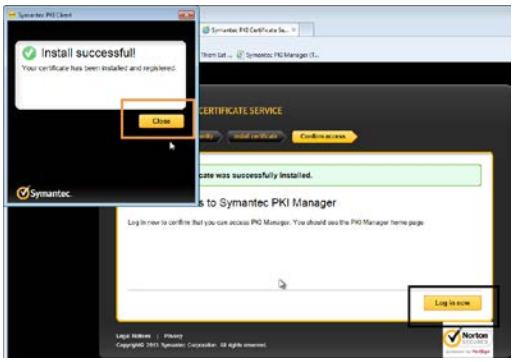
When prompted, install the *Symantec Managed PKI Infrastructure Test Drive Root CA*.



Close the *Symantec PKI Client* dialog.

On the certificate installation success page, click **Log in now**.

("Log in now" is the Symantec Test Drive PKI Manager URL:https://testdrive-pki-manager.symauth.com/pki-manager/)

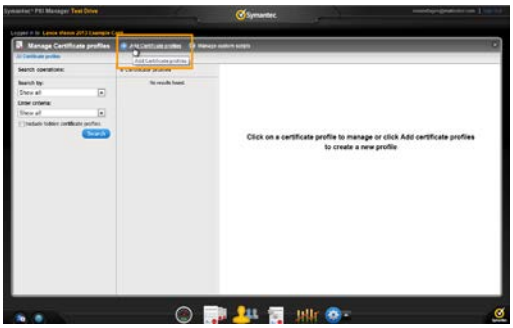


Welcome to the *PKI Manager* dashboard.

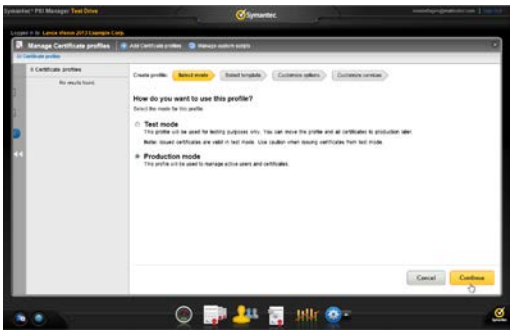
2 *PKI Administrator - Configure your MPKI account for mobile device ActiveSync certificate use-case*

Using your web browser, login to **PKI Manager** and click the **Tasks** icon for **Manage Certificate Profiles**.

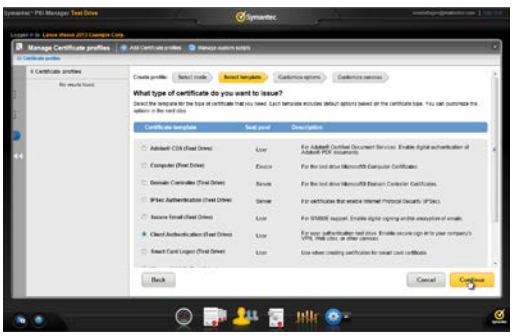
Click **Add certificate profiles**.



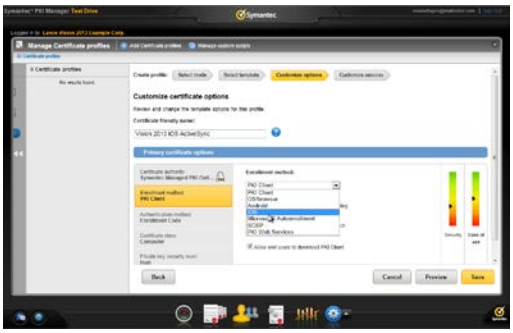
Select **Production Mode** and click **Continue**.



Choose the **Certificate template**, **Client Authentication (Test Drive)** and click **Continue**.



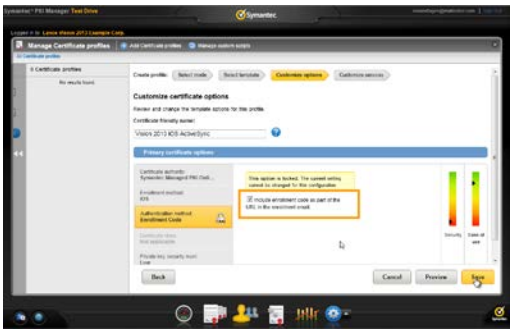
Enter a **Certificate friendly name**, "*iOSActiveSync*",
and change the **Enrollment Method** to **iOS**.



Click **Continue** to change the enrollment method.

Select "Authentication method:" **Enrollment Code**,
then check the box: "*Include enrollment code as part of the URL in the enrollment email.*"

And **Save**.



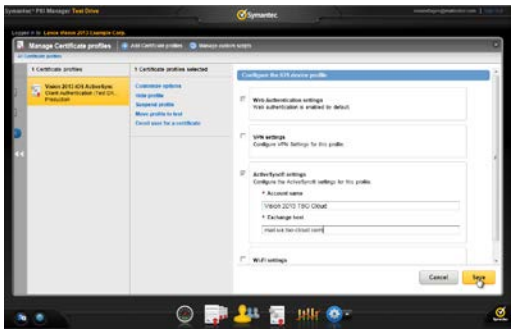
Click **Continue** to save this certificate profile.

Click **Edit**, to set the device configuration.

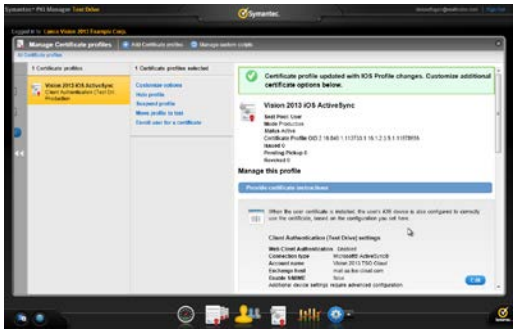
Configure the **ActiveSync settings**, and click **Save**.

Account Name: `Vision 2013 IC L23`

Exchange host: `mail.ua.tso-cloud.com`



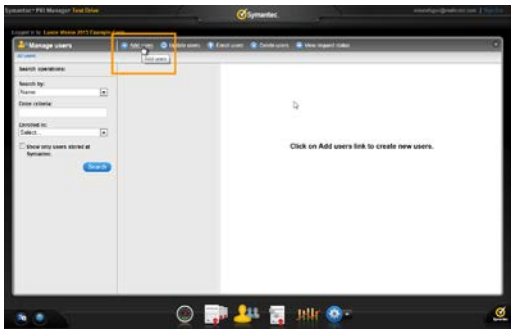
Certificate profile configuration is complete.



Add the user to PKI Manager

Click the **Tasks** icon for **Manage users**.

Click **Add users**.



Select the radio button for **Add: A single user**

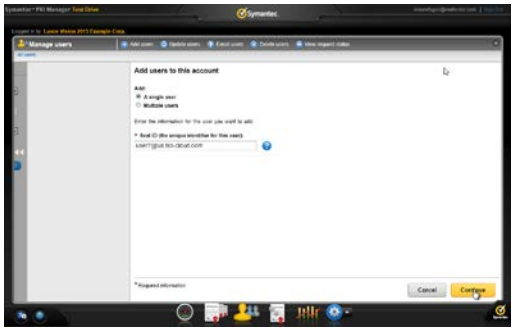
And enter the **Seat ID**.

For this lab we will set the user's Seat ID as their Windows domain Universal Principal Name (UPN).

This UPN value will also be included in the certificate SubjectAltName and is used by ActiveSync to map the domain user's mailbox.

Use one of the domain users 1 thru 10 that are available in the lab domain:

user1@ua.tso-cloud.com, user2@ua.tso-cloud.com, user3@ua.tso-cloud.com, user4@ua.tso-cloud.com, user5@ua.tso-cloud.com, user6@ua.tso-cloud.com, user7@ua.tso-cloud.com, user8@ua.tso-cloud.com, user9@ua.tso-cloud.com, user10@ua.tso-cloud.com



Click **Continue**.

Enter the user's **First Name**, **Last Name**, **Email***,
(Do *not* the checkbox for "*I want to enroll the user for a certificate*", as this will be performed in the next step.)

and click **Continue**.

*The email should be sent to an address where it can be read from the end-user device using the web browser and internet email.

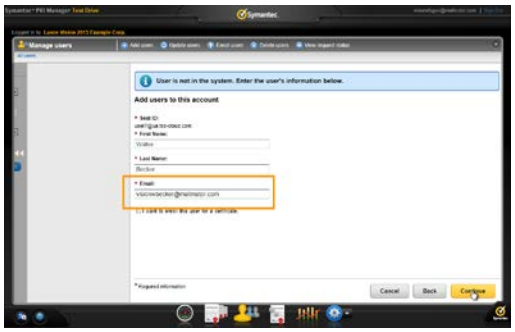
You can use your own internet accessible email account.

If you do not have your own email account, you can use a mailinator.com(free, disposable email) address.

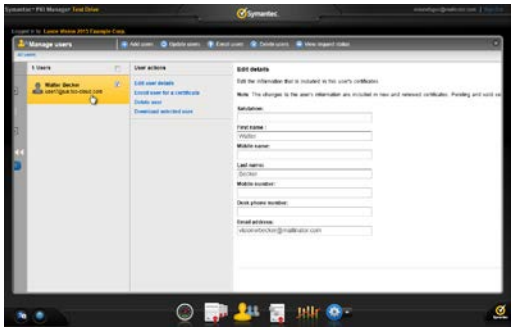
Choose your own unique email address, so that you can find your enrollment email.

E.g.,
"VISION2013USER<yourFirstName><lastInitial>@mailinator.com"

I.e., "VISION2013USERLanceH@mailinator.com"

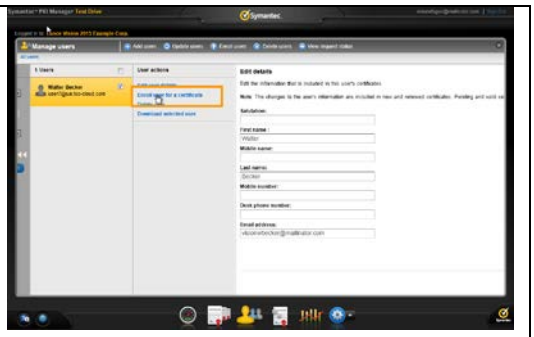


Add user is complete.

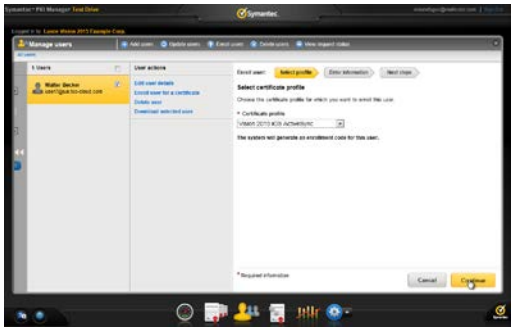


Enroll the user for the ActiveSync certificate profile for their device

Click **Enroll user for a certificate**.



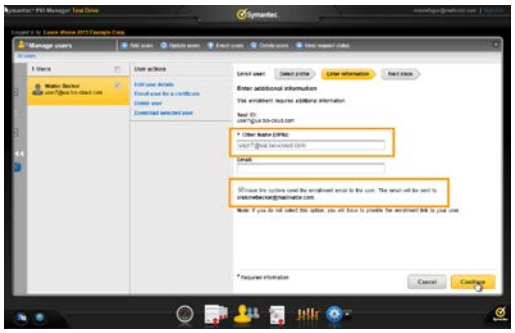
Select the appropriate **Certificate profile** for the end-user's device, "**iOSActiveSync**" and click **Continue**.



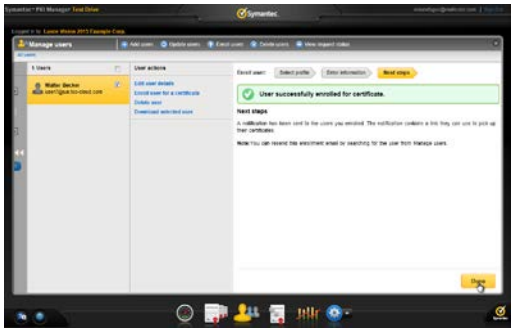
Set "**Other Name (UPN):**" value to the same domain user that you chose for the Seat ID and leave Email blank.

Check the box "*Have the system send the enrollment email to the user. The email will be sent to **…***"

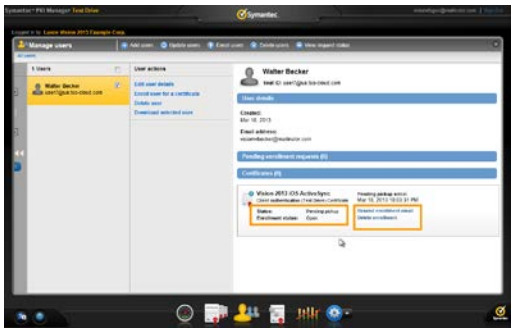
And click **Continue**.



Click **Done**.

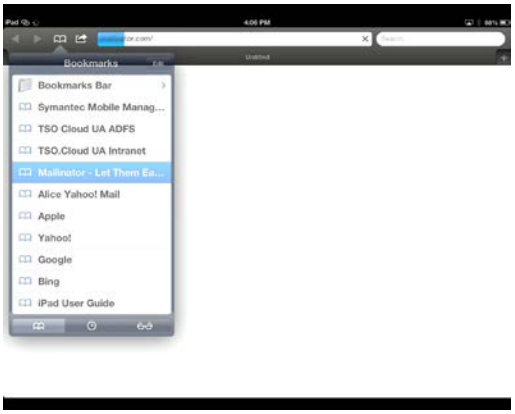


The enrollment request email is now sent and is pending pickup.



3 *End-user - Certificate enrollment, installation, configuration and usage*

On the iOS device, use the web browser to retrieve the email from your account.



If you are using mailinator, go to **mailinator.com** website.

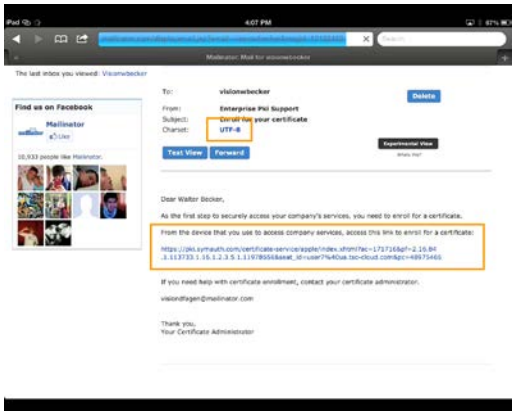
Enter the username portion of your email address in **Check your Inbox!** and click **Go!**

E.g., “VISION2013USERLanceH”

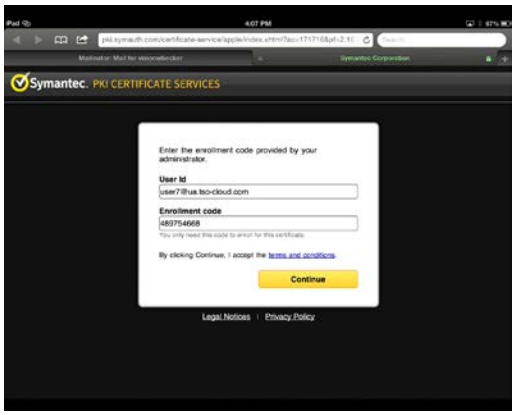
Open the email subject “**Enroll for your certificate**”.

In the email body, click the link to the start the **certificate enrollment**.

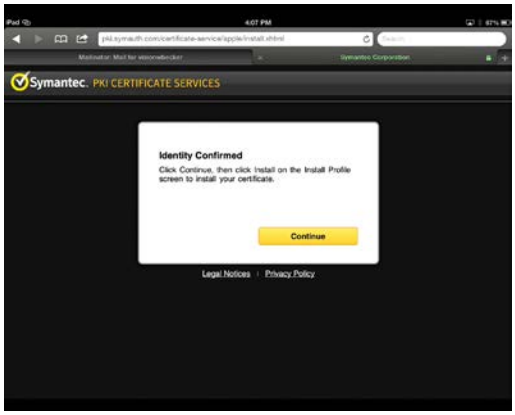
(Note: For mailinator.com, clicking Charset: **UTF-8** will convert the URL to a clickable hyperlink.)



Click to **Continue** the certificate enrollment process.

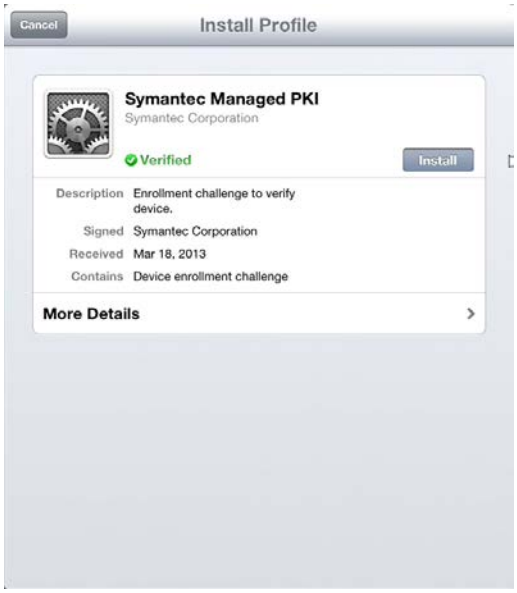


Click **Continue** to install the profile and certificate.



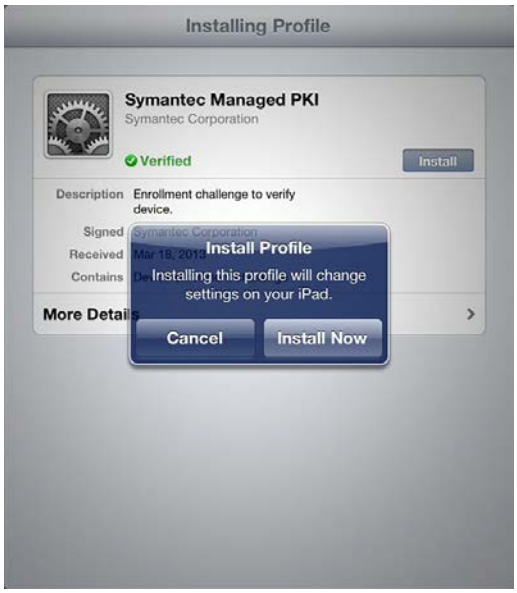
You are prompted to install the Symantec Mangaged PKI profile.

Click **Install**.



At the verification pop-up, click **Install Now**.

(If your device is PIN protected you will need to grant access by entering your device PIN.)

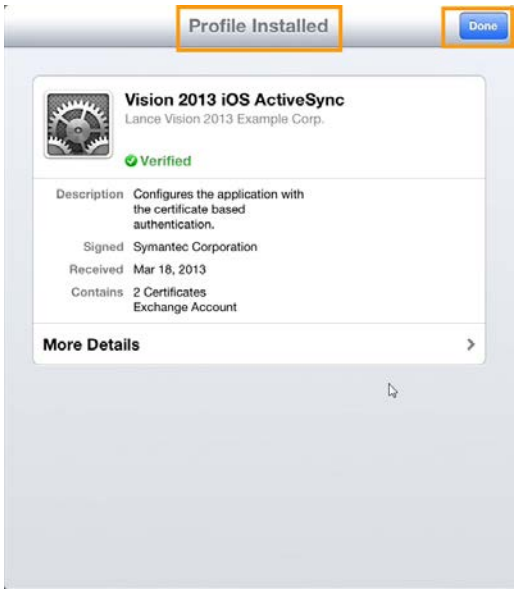


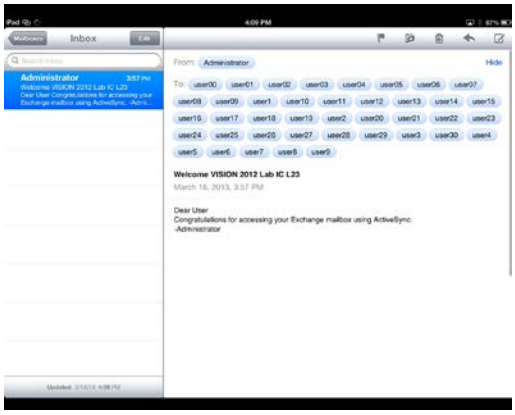
If prompted to install and trust the "**Symantec Managed PKI Online Test Drive Root**" certificate,
click **Install Now**.

Wait for "*Installing Profile*", "*Generating Key*", "*Enrolling Certificate*".

"*Profile Installed*"

Click **Done**.



	Access the Exchange mailbox Click **Mail**.	 

	Discuss the Microsoft Exchange server side configuration **Trust the Issuing CA** **Map certificate to domain user account**	See **MPKI_ActiveSync.pdf** (Downloadable from **PKI Manager | Resources**.)

Appendix

A *Removing the iOS Profile*

Open **Settings** → **General** → **Profiles**

Select the profile you wish to remove, "**Vision 2013 iOS ActiveSync**".

Click **Remove**.

At the verification pop-up, click **Remove**.

(If your device is PIN protected you will need to grant access by entering your device PIN.)