iOS Mobile Device Solution with SAM 8.0

Version 1.0

December 2011
Contacting SafeNet

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact the SafeNet technical support team help-desk which is available 24 hours a day, seven days a week:

<table>
<thead>
<tr>
<th>Country/Region</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>+1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>+1-410-931-7520</td>
</tr>
</tbody>
</table>

For further assistance submit additional questions to the SafeNet technical support team at the following web page:

http://c3.safenet-inc.com/secure.asp

For assistance via email to SafeNet technical support send the request to the following address:

support@safenet-inc.com
# Table of Contents

**Introduction** ......................................................................................................................... 5

Solution Overview ....................................................................................................................... 6
Setting and Enrolling Operation Order ...................................................................................... 7
Certificate Storage Security on iOS Devices ................................................................................ 8

**MSCEP Configuration** .......................................................................................................... 9

Configuring Network Security on Windows Server 2003 .......................................................... 9
Configuring Network Security on Windows Server 2008/R2 ....................................................... 16

**CA Configuration** ................................................................................................................. 25

Enrolling an Enrolling Agent Certificate .................................................................................... 25
Prepare a Certificate Template for Client Authentication ......................................................... 27
Copy Local Trusted Root CA to the Mobile Device ................................................................. 31

**Setting Up a Profile** ............................................................................................................. 38

Creating an Exchange ActiveSync Profile .................................................................................. 40
Setting up the AnyConnect VPN Profile .................................................................................... 42
Exporting the iOS Profile ............................................................................................................. 46

**SAM Configuration** ............................................................................................................ 47

Configuration after Upgrading SAM ........................................................................................... 47
Configuring Roles for SAM Portals ............................................................................................ 50
Adding a Portal Connection ........................................................................................................ 54
Creating a Token Policy Object .................................................................................................. 56
Set a Connector for Microsoft CA ............................................................................................... 59
Defining TPO Rules ..................................................................................................................... 59
Mobile TPO Settings ................................................................................................................... 62
Importing a profile to the TPO ..................................................................................................... 65
Configure TPO Exchange ActiveSync Settings .......................................................................... 68
Configure TPO AnyConnect VPN Settings .................................................................................. 70

**Setting up the Server for Mobile Exchange ActiveSync** ..................................................... 72
Setup for Exchange 2003..................................................................................................................72
Setup for Exchange 2007 and above ..........................................................................................................73

Setting up Cisco ASA Device AnyConnect VPN Remote Access .........................................................81

Licensing requirements: ..........................................................................................................................81
Prerequisites for AnyConnect VPN........................................................................................................82
Documentation and Help ..........................................................................................................................83
Setting up the ASA with an AnyConnect SSL VPN ..................................................................................85
  Installing AnyConnect client on the device .........................................................................................85
  Configure Address Assignment .........................................................................................................87
  Create Address Pool ..........................................................................................................................87
  Creating an AnyConnect Connection Profile ...................................................................................88
  Enable AnyConnect SSL Access on the Outside Interface ...............................................................90
  Configure Group Policy Minimum Requirements ............................................................................91
  Install the CA Root Certificate ..........................................................................................................93
  Enrolling the ASA Device at the CA .................................................................................................95
  Setting Trustpoints ............................................................................................................................98
  Changing the ASA Management and VPN Ports (Optional) ..........................................................100
  Redirecting HTTPS Traffic to the SAM Portal Server ......................................................................102
  Allowing HTTPS Access to the SAM Portal Server ........................................................................105

Mobile Device Enrollment ......................................................................................................................107

  Enrolling a Device ...............................................................................................................................107
  Enrolling a Device with AnyConnect VPN Profile ............................................................................110
Chapter 1
Introduction

This guide provides information for enrolling an iOS mobile device to SafeNet Authentication Manager (SAM), using a dedicated SAM portal.

In this chapter:
- Solution Overview
- MSCEP Configuration
- CA Configuration
- SAM Configuration
- Configuring Roles for SAM Portals
- Setting up a profile
- Mobile Device Enrollment
- Profile Usage
Solution Overview

The solution for iOS mobile devices, includes mobile enrollment using a dedicated SafeNet Authentication Manager (SAM) portal and an Apple profile creation process.

An Apple profile is a file containing Apple specific settings, including certificates, VPN configuration, etc. When the file is installed on the mobile device, the settings are configured in the mobile device.

An Apple profile can be prepared using an external Apple utility called **iPhone Configuration Utility** which can be installed both on Windows OS and MAC OS.

The iOS Mobile solution requires the following prerequisites:

- Windows Server 2003 and above.
- SafeNet Authentication Manager (SAM) 8.0 SP2.
- SAM 8.0 SP2 Remote Portals.
- SafeNet Authentication Client (SAC) 8.0 or above.
- iPhone Configuration Utility (to create new Apple profiles).
Setting and Enrolling Operation Order

**MSCEP Settings**
1. Install and configure the MSCEP (server 2003) or Network Device Enrollment Service (server 2008 and up).
   a. Add a user to IIS_WPG group.
   b. Install the MSCEP (server 2003) or Network Device Enrollment Service (server 2008 and up).
   c. Set the anonymous access user in IIS for MSCEP site.

**CA Settings**
1. Enroll an enrolment agent certificate using a software base CSP.
2. Prepare a certificate template for client authentication.
3. Copy the root CA to the mobile device and make sure the root CA is trusted (only if working with the local root CA that is not trusted on the mobile device).
   a. Enroll a root CA certificate.
   b. Install the root CA to the trusted certification store.
   c. Using the iPhone Configuration Utility, copy the trusted root CA to the mobile device.

**Mobile Device Configuration Settings**
1. Create a new profile in the iPhone Configuration Utility (Only if there is no prepared mobileconfig file).
2. Export the profile to a mobileconfig file.

**SAM Settings**
1. Edit web.config of samwebapi site in IIS – Only if the SAM is upgraded from previous version.
2. Add op_web_service_api_access operation using the SAM Configuration Manager.
3. Add a portal connection.
4. Create a mobile device TPO.
5. Create and set a new request in the MSCA connector in the TPO.
6. Configure the Apple Mobile device Enrollment section in the TPO.
7. Import the mobileconfig file to the TPO.
8. Configure the profile settings in the TPO.
Certificate Storage Security on iOS Devices

The IOS certificates are stored in the keychain.
Their private keys can't be exported.

To protect the keychain from known attacks, the following terms must be met:

- The mobile device must run IOS version 4.0 and above.
- The device must be protected with a passcode lock.
- The passcode must contain at least 6 alphanumeric characters.

For more details refer to:
Chapter 2
MSCEP Configuration

Configuring Network Security on Windows Server 2003

Configuring Simple Certificate Enrollment Protocol (SCEP) ensures a high security level for enrollment portal access from remote locations.

**To configure SCEP on Windows Server 2003:**

1. Ensure that the local computer’s IIS_WPG security group includes a Windows user account that can be used as the Service Account.
2. From the Microsoft website, download the *Simple Certificate Enrollment Protocol (SCEP) Add-on for Certificate Services*.

A confirmation dialog box opens.

4. Click **Yes**.

The *License Agreement* window opens.

5. Carefully read the license agreement, and then click **Yes** to accept it.
The Setup Wizard opens displaying the Welcome screen.

6. Click Next.

The Application Identity Options window opens.

7. Select Use a service account, and then click Next.

The Service Account Information window opens.
8. Complete the following fields:
   ♦ In the **Account Name** field, enter the Windows user account to be used for managing SCEP operations.
   
   **Note:** The account must already exist and must be a member of the local computer’s IIS_WPG security group.

   ♦ In the **Password** field, enter a password.
   ♦ In the **Confirm Password** field, enter the same value as in the **Password** field.

9. Click **Next**.

   The **Challenge Phrase Options** window opens.

10. Select **Require SCEP Challenge Phrase to Enroll**, and then click **Next**.

   **Note:** SCEP is also supported without challenge.

   If SCEP is already installed, a warning message opens.
11. Click **OK**.

   A confirmation dialog box opens.

12. Click **Yes**.

   The **SCEP RA Certificate Enrollment** window opens.

13. Complete the following fields:
   - Ensure that **Advanced Enrollment Options** is not selected.
   - Enter the relevant details in the **Name** and **Company** fields.

14. Click **Next**.

   The **Completing the Wizard** window opens.
15. Click **Finish**.

The SCEP installation begins.

On completion of the installation, the *Setup Successful* message opens. The message includes the partial URL for SCEP.

![SCEP Add On for Certificate Services Setup Wizard](image)

**Note:** The SCEP URL, together with the domain name extension must be entered in the Token Policy Object (TPO) Editor’s Apple Mobile Device Enrollment Settings.

16. Click **OK**.

17. From the *Windows* taskbar, click the **Start** button, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

The *Internet Information Services (IIS) Manager* opens.

![Internet Information Services (IIS) Manager](image)

18. In the left navigation pane, expand **Web Sites**, expand **Default Web Site**, and then expand **CertSrv**.

19. Right-click **mscep**, and then click **Properties**.

The *mscep Properties* window opens.

21. Under **Authentication and access control**, click **Edit**.

The Authentication Methods window opens.
22. In the **User name** and **Password** fields, enter the Service Account name and password designated in step 8 above.

23. Click **OK**.

24. Close the **IIS Manager**.
Configuring Network Security on Windows Server 2008/R2

Configure the Network Device Enrollment Service ensuring a high security level for portal access enrollment from remote locations.

To configure the Network Device Enrollment Service on Windows Server 2008/R2:

1. Ensure that the local computer’s IIS_IUSRS group includes a user for authorizing certificate requests.

2. From the Windows taskbar, click the **Start** button, point to **Administrative Tools**, and then click **Server Manager**.

   The **Server Manager** opens.

3. In the left navigation pane, select the **Roles** node.

   The **Roles** details are displayed in the right pane.

4. Under **Active Directory Certificate Services**, click the **Add Role Services** link.

   The Select Role Services window opens.
5. Select **Network Device Enrollment Service**, and then click **Next**.

The Specify User Account window opens.

6. In the right pane click **Select User**.

The Windows Security window opens.
7. Enter the account **User name** and **Password** to be used for managing SCEP operations, and then click **OK**.

**Note:** The account must already exist and must be a member of the local computer's IIS_IUSRS group.

The user account is displayed in the **Specify User Account** window.

8. Click **Next**.

The **Specify Registration Authority Information** window opens.
9. Leave the RA Name field contents as they appear, and if required enter the appropriate Optional Information.

10. Click Next.

The Configure Cryptography window opens.

11. No fields are to be changed in this window. Click Next.

The Confirm Installation Selections window opens.
12. Click **Install**.

The installation process begins.

When the installation is complete, **Results** is selected in the left pane and the installation results are displayed in the right pane.

13. Click **Close**.

The Network Device Enrollment Service is installed.

To allow more than five users to enroll at the same time, change the MSCEP **PasswordMax** registry key to the maximum number of users who may simultaneously run the enrollment process.
For more information, see the relevant Microsoft documentation

14. To set the correct Anonymous User account for SCEP access, from the
Windows taskbar, select Start, point to Administrative Tools, and then
click Internet Information Services (IIS) Manager.

The Internet Information Services (IIS) Manager opens.

15. In the left navigation pane expand Web Sites, expand Default Web Site,
expand CertSrv, and then select mscep.

The /CertSrv/mscep Home options are displayed in the center pane (Server
2008 and above).

Under IIS select Authentication.

The Authentication options are displayed in the center pane.
In the center pane select **Anonymous Authentication**. The **Anonymous Authentication** actions are displayed in the right pane.

16. In the right pane click **Edit**.

The *Edit Anonymous Authentication Credentials* window opens.

17. Click **Specify user**, and then click **Set**.

The *Set Credentials* window opens.

18. Enter the previously set **User name** and **Password** to manage SCEP operations.

19. Click **OK** until the *Edit Anonymous Authentication Credentials* window closes.

20. To set the correct **Request Filtering** settings, in the *IIS Manager* left pane, click **Sites**, expand **Default Web Site**, and then click **samios**.

21. Under **IIS** click **Request Filtering**.
Note: If the Request Filtering option is not displayed, use the Server Manager to install a Request Filtering role service.

The Request Filtering options are displayed in the center pane and the Alerts and Actions are displayed in the right pane.

22. In the right pane under Actions click Edit Feature Settings.

The Edit Request Filtering Settings window opens.

23. Change Maximum query string (Bytes) to 65536, and then click OK.
This chapter provides information for the CA configuration that must be performed to prepare the environment for the mobile device solution.

Enrolling an Enrolling Agent Certificate

This section is required only if the Enrollment Agent template is not in the CA certificate template list.

To enroll an enrolling agent certificate:
1. Open the CA application.
2. In the left navigation pane expand the CA <ca name>.
3. Right-click Certificate Template, point to New, and then click Certificate Template to Issue.

The Enable Certificate Templates window opens.
4. Select the **Enrollment agent** template, and then click **OK**.

5. Open Internet explorer and go to **http://localhost/certsrv**.

6. Enroll an enrollment agent certificate using a software base CSP.
Prepare a Certificate Template for Client Authentication

To prepare a certificate template for client authentication:

1. Open the CA application.

2. In the left navigation pane expand the CA <ca name>.

   Right-click **Certificate Template** and click **Manage**.

   A list with all the available templates appears.

3. In the right pane right-click on any template that had signing abilities (for example—Smartcard User), and then click **Duplicate Template**.
The *Properties of New Template* dialog box opens.

4. Select the *Request Handling* tab.

5. Select *Allow private key to be exported.*
6. Select the **Issuance Requirements** tab.

7. Select **This number of authorized signatures** and enter 1 in the text box.

8. Under **Application policy** select the **Certificate Request Agent** option.
9. Select the **Security** tab.

![Copy of Smartcard User Properties](image)

10. Select the required permissions for all relevant organizational groups and click **OK**.

11. Click **OK** again.

   The duplicated template is added to the list of templates.

12. Close the window and go back to the CA application.

13. Right click on certificate template node.

14. Select **New>Certificate Template to Issue**

   *Enable Certificate Template* window opens.

![Enable Certificate Templates](image)

15. Choose the duplicate template and click **OK**.

   The duplicated template is added to the Certificate Templates list.
Copy Local Trusted Root CA to the Mobile Device

This procedure is performed only when using a local root CA that is not trusted on the mobile device. This procedure installs the root CA as a trusted root CA. After this process, the certificate is transferred to the mobile device as a trusted certificate using iPhone Configuration Utility.

**Note:** This is only an example of how to make a root CA trusted in the mobile device, there may be other ways to perform the same task.

**To install a root CA from the server:**

1. Download the local root CA .cer file to the machine.
2. Install the local root CA to a Trusted Root CertificationAuthorities store.

**To copy local trusted root CA to the mobile device:**

1. Using a USB, connect the iOS mobile device to the machine.
2. Run the **iPhone Configuration Utility**.

The iPhone Configuration Utility window opens.

The device is displayed in the left pane under **Devices**.
3. On the left pane under **Utilities** select **Configuration Profiles**. In the right pane the **Configuration Profiles** details are displayed.

4. Click **New** in the Main Toolbar.

   ![Profile List](image)

   In the top right **Profile List** a new profile is added and the new profile configuration pane opens under the **Profile List** displaying configuration options in the left Profile pane.

5. In the left Profile pane click **General** and complete the compulsory details:
   - Name
   - Identifier—The identifier must be a unique name and must be in the format: `<unique name>.<full domain name>` (for example, if the domain name is vm2003.com, the unique name will be `something.vm2003.com`)
6. In the left Profile pane click **Credentials**.

   The **Configure Credentials** prompt is displayed in the right Profile pane.

7. In the right Profile pane click **Configure**.

   On Windows XP machines The **Personal Certificate Store** window opens.

   On Windows Vista and Windows 7 the following **Personal Certificate Store** opens.
8. Navigate and highlight the local root CA certificate and then click **OK**. The certificate details are displayed in the right pane.

9. In the left pane, under Devices select the iOS Apple device. The device details are displayed in the right pane.
10. In the right pane click the **Configuration Profiles** tab.

![Configuration Profiles Tab](image)

The newly created profile is displayed on the profiles list.

11. Click **Install** next to the new profile.

   The **Install Profile** window opens in the mobile device.

![Install Profile Window](image)

12. Click **Install** on the mobile device.

   A dialog box opens requesting installation confirmation.
13. Click **Install Now**.
   The certificate is installed. On completion a Profile Installed dialog box opens.

14. Click **Done**.
   The local root CA is now trusted and installed on the mobile device.

15. On the mobile device, in the left pane under **Settings** click **General** and then select the new Profile.
   The Profile details are displayed in the right pane.
16. The Profile is installed and the certificate is verified.
Chapter 4
Setting Up a Profile

When enrolling a mobile device, an Apple profile is installed on the mobile device. The profile is prepared in an Apple utility called Iphone Configuration Utility which can be downloaded from the Apple website for MAC and for Windows.

To create a profile:

1. Run iPhone Configuration Utility.
   
   The iPhone Configuration Utility window opens.

2. On the left pane, click Configuration Profiles.
   
   The right pane shows the list of profiles.
3. Click **New** in the upper left corner to create a new profile. A new profile appears in the right pane.

4. Enter the following details in the right pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the <strong>Name</strong> in the configuration file’s <strong>General payload</strong>.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Specifies the <strong>Identifier</strong> in the configuration file’s <strong>General payload</strong>.</td>
</tr>
<tr>
<td>Organization</td>
<td>Specifies the <strong>Organization</strong> in the configuration file’s <strong>General payload</strong>.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the <strong>Description</strong> in the configuration file’s <strong>General payload</strong>.</td>
</tr>
<tr>
<td>Security</td>
<td>Specifies the <strong>Security</strong> setting in the configuration file’s <strong>General payload</strong>.</td>
</tr>
</tbody>
</table>

For setting a profile with Exchange ActiveSync support or VPN support, please refer to **Setting up an Exchange ActiveSync Profile** (page 40) or **Setting up the AnyConnect VPN Profile** (page 42).
Creating an Exchange ActiveSync Profile

To create an exchange activesync profile:

1. In the iPhone Configuration Utility, after entering the General fields for a new profile, select Exchange ActiveSync on the left pane.

The right pane changes accordingly.

2. Click Configure in the right pane.

The Exchange ActiveSync options appear.
3. Fill in the necessary fields (**Account name** and **Exchange ActiveSync Host** are mandatory).

**Note:** To enroll the same exchange configuration for all users (The same email, username and password), fill in the necessary fields. If those fields will remain empty, this configuration will be taken from the Active Directory, or by filling it in manually in the iOS mobile device.
Setting up the AnyConnect VPN Profile

To set up the AnyConnect VPN profile:

1. In the iPhone Configuration Utility, select VPN payload on the left pane. The right pane changes accordingly.

2. Fill in the relevant settings on the right pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the Name in the configuration file’s General payload.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Specifies the Identifier in the configuration file’s General payload.</td>
</tr>
<tr>
<td>Organization</td>
<td>Specifies the Organization in the configuration file’s General payload.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the Description in the configuration file’s General payload.</td>
</tr>
<tr>
<td>Security</td>
<td>Specifies the Security setting in the configuration file’s General payload.</td>
</tr>
</tbody>
</table>

3. Select the VPN payload, and then click Configure.
4. Enter the parameters in the right pane. Leave the Identity Authentication field blank.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Name</td>
<td>Specifies the <strong>Connection Name</strong> in the configuration file’s <strong>VPN</strong> payload.</td>
</tr>
<tr>
<td>Connection type</td>
<td>Specifies the <strong>connection type</strong> in the configuration file’s <strong>VPN</strong> payload.</td>
</tr>
<tr>
<td>Server</td>
<td>Specifies the <strong>server IP or hostname</strong> in the configuration file’s <strong>VPN</strong> payload.</td>
</tr>
<tr>
<td>User Authentication</td>
<td>Specifies the <strong>user authentication type</strong> in the configuration file’s <strong>VPN</strong> payload.</td>
</tr>
<tr>
<td>Identity certificate</td>
<td>Specifies the <strong>identity certificate</strong> setting in the configuration file’s <strong>VPN</strong> payload.</td>
</tr>
</tbody>
</table>
5. Click **Export**, to export the mobile configuration package.

**Note:** Make sure you select **Sign configuration profile** from the **Security** drop-down list.

The **Export Document To** window opens.

6. Browse to the location where you want the file saved. The file can also be copied manually.
Exporting the iOS Profile

In order to use the prepared profile with SAM, the profile should be exported from the iPhone Configuration Utility and imported to SAM.

To export the iOS profile:
1. Choose the profile on the upper pane.
2. Click on the Export icon at the top of the window.
   The Export Configuration Profile window appears.
4. Click Export.
   The Export Document to window appears.
5. Browse to the location you want to save to, and click Save.
This chapter provides SAM configuration information for enabling the iOS mobile device enrollment.

**Configuration after Upgrading SAM**

After SAM is upgraded from an earlier version, a code must be added to the `samwebapi` file. The file is not updated during the installation, because the service is running and cannot be updated automatically.

**To configure after SAM upgrade:**

1. Click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
   
   The Internet Information Services (IIS) Manager window opens.

2. In the left navigation pane click `<domain name>`, expand **Web Sites**, then expand **Default Web Site**.

3. Right-click `samwebapi` and click **Explore**.
The right pane displays the site files.

4. In the right pane, right click **web.config**, and open it with a text editor (e.g. notepad).
5. In Windows server 2003 and up, insert the following code after the <system.web> (As in the screenshot):

```xml
<httpHandlers>
  <add verb="*" path="*.asmx"
       type="AspCompatWebServiceHandler, AspCompatWebService, Version=2.0.1.0, Culture=neutral, PublicKeyToken=1d12ee7b52e0a2fa" />
</httpHandlers>
```

6. In Windows server 2008 and up, add the following code at the end of the file:

```xml
<system.webserver>
  <handlers>
    <add name="AspCompatWebServiceHandler" verb="*"
         path="*.asmx" preCondition="integratedMode"
         type="AspCompatWebServiceHandler, AspCompatWebService, Version=2.0.1.0, Culture=neutral, PublicKeyToken=1d12ee7b52e0a2fa" />
  </handlers>
</system.webserver>
```
Configuring Roles for SAM Portals

Before configuring or adding portal connections, an operation must be added to the Administrator role in SafeNet Authentication Manager - Authorization Manager.

To configure the Administrator Role:

1. Open the SAM Configuration Manager.

2. On the **Action** menu, point to **Authorization Manager**, and then select **Edit Roles**. The SafeNet Authentication Manager - Authorization Manager opens.

3. In the left navigation pane expand **Management Center**, expand **Definitions**, and then expand **Role Definitions**.

4. Right-click **Administrator** and select **Properties**.
The Administrator Definition Properties window opens.

5. Click the Definition tab.
6. Click **Add**.

   The *Add Definition* window opens.

![Administrator Definition Properties dialog box]

7. Click the **Operations** tab.

8. Click **op_web_service_api_access**.

![Add Definition dialog box]

9. Click **OK**.

   The *Administrator Definition Properties* dialog box opens.
10. Click **OK** to exit *SafeNet Authentication Manager - Authorization Manager*. 
Adding a Portal Connection

A connection must be added for the Mobile Device Enrollment portal.

To add a portal connection:

1. Click **Start>Programs>SafeNet>SafeNet Authentication Manager>Portals Configuration**.

   The SafeNet Authentication Manager - Portals Configuration window opens.

2. Click the **Connections** tab, and then click **Add**.

   The Connection Details window opens.
3. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Name</td>
<td>Enter a connection name.</td>
</tr>
<tr>
<td>SAM Server URL</td>
<td>Enter the SAM server URL in the following format: <a href="http://hostname">http://hostname</a></td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username used for logging on to SAM.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password used for logging on to SAM.</td>
</tr>
</tbody>
</table>
| Instance Name     | 1. Click Select. The Select SAM instance dialog box opens.  
|                   | 2. Click the SAM user store instance name for which the portal connection is added. |

4. Click OK.

The connection is added to the connections list in the SafeNet Authentication Manager - Portals Configuration window.
Creating a Token Policy Object

When using the mobile solution, a separate specific Token Policy Object (TPO) must be created.

To create a TPO:

1. Open **Active Directory Users and Computers**.

2. Right click the domain name and click **Properties**.

   The *<domain name> TPO Properties* dialog box opens.

3. Click the **Token Policy** tab.

4. Click **Open**.
The Token Policy Object window opens.

5. Click **New**.

   The Token Type dialog box opens.

6. Click **Mobile Device**, and then click **OK**.

   The new added token policy is displayed in the Token Policy Object window.
Set a Connector for Microsoft CA

The Connector for Microsoft CA (MSCA) enables the user to generate certificates using the Microsoft Certificate Authority (CA) services.

Defining TPO Rules

Use the Connector Policy Object Editor to set the SAM connector policies.

To define TPO rules:

1. Open the TPO Editor.
2. In the left pane, click Connector Settings.
   The list of installed SafeNet Authentication Manager connectors opens in the right pane.

3. In the right pane, right-click Connector for Microsoft CA, and select Properties.
   The Connector for Microsoft CA Properties window opens.
4. Select **Define this policy setting**, select **Enabled**, and click **Definitions**. The Connector Policy Object Editor opens.

5. By default, there is no limit to the number of certificates that can be enrolled to a token. To limit the number of certificates on a token do the following:
   a. In the right pane, right-click **Maximum number of certificates on token**, and select **Properties**.
   b. Select **Define this policy setting**.
   c. Enter the maximum number of certificates that can be enrolled on the token, and click **OK**.

6. Right-click **Microsoft CA Connector**, and select **Create new request**. The Create New Request window opens.
7. For each request, enter the fields as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Name</td>
<td>May be any name. If a request with the same request name exists in a different TPO definition, the new parameters are merged with that request's parameters during token enrollment. If the request name does not exist in a TPO relevant to the enrolled user, the request is added. Default: New Request, followed by the next sequential number.</td>
</tr>
<tr>
<td>Name</td>
<td>CA from the list of CAs installed in the AD tree. Default: the first CA in the drop-down list.</td>
</tr>
<tr>
<td>Type</td>
<td>Depends on Active Directory being present. <strong>Standalone</strong>: permits the generation of certificates for anyone. <strong>Enterprise</strong>: permits the generation of certificates for authenticated users only. No default.</td>
</tr>
<tr>
<td>Certificate Usage</td>
<td>Filter used to narrow the selection in the Templates drop-down list. Type of templates to be enrolled: <strong>Smartcard Logon</strong>, <strong>Encryption</strong>, <strong>Signature</strong>, <strong>VPN</strong>, <strong>Other</strong>. No default.</td>
</tr>
<tr>
<td>Templates</td>
<td>A certificate template from one or both of the template lists appropriate for the Certificate Usage selected: <strong>Administrator-generated certificate template</strong>: used when enrollment is performed by the administrator. <strong>User-generated certificate template</strong>: used during self-service enrollment. No default. In this solution, only the <strong>Administrator-generated certificate template</strong> should be chosen.</td>
</tr>
</tbody>
</table>

**Note**: Once a request is created, these fields cannot be modified. If a change is required in the fields, the request must be deleted and a new request created.

Click **OK** repeatedly to close the Connector Properties window. The updated connector settings are applied.
Mobile TPO Settings

This section describes only the required settings to configure for mobile device enrollment.

To configure mobile device TPO settings:

1. Open **Active Directory Users and Computers**.

2. Right click the domain name and click **Properties**.

   The <domain name> TPO Properties dialog box opens.

3. Click the **Token Policy** tab.

4. Click **Open**.
The **Token Policy Object** window opens.

5. Select the created Mobile Device policy and select **Edit**.

The **Token Policy Object Editor** opens.

6. On the left pane, click **Apple Mobile Device Enrollment**.
   
   The **Apple Mobile Device Enrollment** details are displayed in the right pane.
7. In the right pane configure the device enrollment as follows:

- **Signing certificate**—Defines the local computer store certificate to use for signing enrollment data sent to mobile devices. Here is where every certificate with signing abilities can be selected.

- **SCEP URL**—Defines the full server name, including the domain name extension, for the Simple Certificate Enrollment Protocol (SCEP) service that enrolls network devices in the format:

  `http://<SCEP server netbios name>.<domain name>/certsrv/mscep`

  (The same link provided at the end of the SCEP installation.)

- **CA name**—Defines the Certificate Authority name on the SCEP service server.
Importing a profile to the TPO

To import a mobile device configuration file configured by the iPhone Configuration Utility:

1. Open **Active Directory Users and Computers**.

   ![Active Directory Users and Computers](image1)

2. Right click the domain name and click **Properties**.

   The `<domain name> TPO Properties` dialog box opens.

   ![Properties](image2)

3. Click the **Token Policy** tab.
4. Click **Open**.

The *Token Policy Object* window opens.

![Token Policy Object Window](image)

5. Select the created Mobile Device policy and select **Edit**.

The *Token Policy Object Editor* opens.

![Token Policy Object Editor](image)

6. Select the **Apple mobile device** Enrollment node.

The *Apple Mobile Device Enrollment* details are displayed in the right pane.

7. Right-click **Apple Mobile Device Enrollment settings** and then click **Import a configuration file**.
The Import window opens.

8. Click Browse, navigate the required folder and then select the configuration file.

9. The profile is added to the TPO and its details are displayed in the right pane.

Note: Only one Apple mobile device configuration is supported per TPO. Any previously imported mobile device configuration file is deleted.
Configure TPO Exchange ActiveSync Settings

1. Click **Exchange ActiveSync Settings** in the left pane.

   The settings appear on the right pane.

2. Set the **User**, **Email address** and **Password** settings Enable/Disable.
   - **Enable** - the value will be taken from the Active Directory during enrollment
   - **Disable** – During enrollment, if the value is defined in the mobileconfig file, the defined value will be applied to all users. If no value is defined in the mobileconfig file, users will be prompted to enter a value.

3. In the right pane, double-click on the **Authentication Credential Name**.

   The **Authentication Credential Name Properties** window appears.

   This setting sets the certificate that will be enrolled in order to use the Exchange account on the mobile device.

4. Check the option **Define this policy setting**.
5. In the **Profile Name** field, enter the name of the MSCA connector request that will be used during the enrollment.

   **Note:** The request name must be case sensitive.

6. Click **OK**. The Token Policy Object Editor window opens.

7. Click **OK** again.
Configure TPO AnyConnect VPN Settings

To configure TPO AnyConnect VPN settings:

1. Import the profile generated under **Setting up the AnyConnect VPN profile** as shown in the **importing a profile** chapter above.

2. Select apple mobile device configuration and fill in the **Signing certificate**, **SCEP url** and **CA NAME**.

**Note:** Make sure you use the SCEP server FQDN.

3. In the left pane, click on **VPN Settings**, The settings appear in the right pane.  
   Double click the **CA name** in the right pane.  
This parameter sets the certificate that will be enrolled in order to use the AnyConnect VPN on the mobile device.

4. Check the option **Define this policy setting.**

5. In the **Profile Name** filed, enter the name of the MSCA connector request that will be used during the enrollment.

**Note:** The request name must be case sensitive.

6. Click **OK.**
   The *Token Policy Object Editor* window appears.

7. Click **OK** again.
Chapter 6
Setting up the Server for Mobile Exchange ActiveSync

An exchange profile can be used when working with Exchange 2003 and above

Setup for Exchange 2003

To set up exchange 2003:

1. Run All Programs>Microsoft Exchange>System Manager.

   The Exchange System Manager window opens.

2. Right-click on Global Settings>Mobile Services.
3. Choose **Properties**.

The *Mobile Properties Services* window opens.

4. Check **Enable Outlook Mobile Access** and **Enable unsupported devices**.

5. Click **OK**.

**Setup for Exchange 2007 and above**

In order to set the IIS to work with the iOS mobile device with exchange, few changed should be made through the IIS. To make these changes, an *administrator pack* of the IIS should be installed. This pack can be downloaded from:

[http://www.iis.net/download/administrationpack](http://www.iis.net/download/administrationpack)

**Setting up the Server**

To **set up the server**:

1. Open Server Manager.

    The *Server Manager* window opens.
2. Click on the Roles node. The Roles node expands.

3. Click on Web Server (IIS) node. The right pane changes and the Web Server details appear.
4. Click the link **Add Role Services** in the right pane.

   The *Add Role Services* window opens.

5. Under **Web Server>Security** check the following:
   - Client Certificate Mapping Authentication
   - IIS Client Certificate Mapping Authentication
   - Basic Authentication.
6. Click **Next**.

   Confirmation details appear.

   ![Add Role Services](image1.png)

7. Click **Install**.

   After the installation progress, the result details appear.

   ![Add Role Services](image2.png)

8. Click **Close** to close the wizard.

9. Click **Start**>**Programs**>**Administrative Tools**>**Internet Information Services (IIS) Manager**.
10. Click on the main IIS host in the left pane.

The right pane displays the option for the main IIS host.

11. In the right pane, open Authentication.

12. Right-click on Active Directory Client Certificate Authentication and enable it.
13. Under **Sites**, Click on **Microsoft-Server-ActiveSync** site.

The right pane changed according to the chosen site.

14. In the right pane, Under **IIS**, run **Authentication**.

In the right pane the **Authentication** options appear.

15. In the right pane, click on **Basic Authentication** and select **Enable**.

16. In the left pane, under **Sites**, click on **Microsoft-Server-ActiveSync** site again.
17. In the right pane, under **Management**, run **Configuration Editor**.

   The right pane shows the Configuration Manager.

18. On the top toolbar, in the **Section** field, open the dropdown menu.


   The right pane displays the properties.

20. Set the properties as follows:
- **enabled** – True
- **manyToOneCertificateMappingEnabled** – False
- **oneToOneCertificateMappingEnabled** – False

21. In the right pane, click **Apply**.

22. Close the Web Server (IIS) Manager.
Chapter 7
Setting up Cisco ASA Device
AnyConnect VPN Remote Access

Licensing requirements:

The ASA requires an AnyConnect Mobile license (L-ASA-AC-M-55XX=), as well as either an AnyConnect Essentials (L-ASA-AC-E-55XX=) or AnyConnect Premium Clientless SSL VPN Edition (L-ASA-AC-SSL-YYYY=) license, where XX is the last two digits of your ASA model number and YYYY is the number of simultaneous users.

For further information regarding licensing see:


For further reference please contact Cisco licensing support. Refer to Cisco licensing site for access suiting your area.

https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet

An AnyConnect profile can be used when working with Cisco’s Adaptive Security Appliance (ASA) devices.

Firmware version and ASDM version

Please note that although AnyConnect for iOS requires a Cisco ASA running software image 8.0(3).1 or later Safenet recommends image version 8.4(2) and above as well as ASDM 6.4 and above
Prerequisites for AnyConnect VPN

Some instructions require CLI access and others can be performed using ASDM. For further information refer to Cisco’s documentation regarding Connecting to ASDM for the First Time in the following document:


Setting up Cisco AnyConnect VPN requires that you have configured the ASA. You can achieve this minimal configuration by running the Startup Wizard using the ASDM. To run the Startup Wizard, follow the following procedure:

1. In the menu bar, click Wizards.
2. Select Startup Wizard... from the menu.
3. Follow the instructions of the guide.
Documentation and Help

Throughout the document an outline for the procedure is explained. Please refer to the following documents or any superseding documents from Cisco support:

Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0

Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4

You can also use the ASDM built in support ASDM Assistant

1. Press the Configuration button on the top of the ASDM, the contents of the window changes.

2. In the left panel of the ASDM select Remote access VPN

![ASDM Configuration Screen]

3. In the right panel select SSL or IPsec (IKEv2) VPN remote access (using Cisco AnyConnect client) the contents of the left widow will change to the ASDM assistant guiding you for the required procedure to create the AnyConnect VPN.
Setting up the ASA with an AnyConnect SSL VPN

**Note:** This is only an example of installing the AnyConnect app to the mobile device; there may be other ways to perform the same task.

After you have completed the initial setup, you can begin configuring the ASA device with an AnyConnect VPN.

**Installing AnyConnect client on the device**

Although the first step in the ASDM assistant is uploading the client packages, Cisco does not provide an AnyConnect app for iOS devices but recommends downloading them from the app store.

**To install AnyConnect client on the device:**

1. Open the app store, and type *Cisco AnyConnect* in the **search** field.

2. Depending on your device, select the **iPad** or **iPhone/iPod** version.
3. Press **Install**, and authorize with your password (if applicable).

The icon will appear on your device after the installation completes.
Configure Address Assignment

In the following section you will configure address assignment policy.

**Note:** This is only an example of using ASA based DHCP pool in the AnyConnect configuration. There are other ways to provide for client addresses. Consult Cisco's documentation for further guidance.

**To configure address assignment:**

1. To configure address assignment, Press the **Configuration** button on the top of the ASDM, the contents of the window changes.
2. In the left panel of the ASDM, select **Remote access VPN**.
3. In the left pane, expand **Address assignment** then select **Assignment policy**. The following widow appears on the right pane:

![Configuration window with address assignment settings](image)

4. Uncheck **Use Authentication Server** and **Use DHCP**.

Create Address Pool

In the section below you will create an address pool.

**To create an address pool:**

1. To Create an address pool, click **Configuration** on the top of the ASDM, the contents of the window changes.
2. In the left panel of the ASDM select **Remote access VPN**.
3. In the left pane, expand **Address assignment** and select **Address pools**.

The following window appears in the right pane:

![Address assignment window](image)

4. Click **Add**, the **edit IP pool** window opens.

![Edit IP Pool window](image)

5. Enter the **Starting IP Address** and the **Ending IP Address**, and select the relevant **Subnet Mask** from the drop-down list box.

6. Click **OK**.

**Creating an AnyConnect Connection Profile**

AnyConnect connection profile defines the VPN type and its settings.

**To create an AnyConnect connection profile:**

1. Click **Configuration** at the top of the ASDM. The contents of the window changes.

2. In the left panel of the ASDM select **Remote access VPN**.

3. In the left pane, select **AnyConnect connection profiles**.
The following window appears in the right pane:

4. **Under Connection Profiles**, click **Add**. The *Edit AnyConnect Connection Profile* window opens.

5. **Complete the fields as follows:**
   - Ensure that the **Enable SSL VPN client protocol** checkbox is selected.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a connection profile name.</td>
</tr>
<tr>
<td>Alias</td>
<td>Is a simple name for the users to see.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select the <strong>Certificate</strong> radio button.</td>
</tr>
<tr>
<td>Client Address Pools:</td>
<td>Type the pool you created or click <strong>Select</strong> to browse for it.</td>
</tr>
<tr>
<td>Default Group Policy</td>
<td>Leave the suggested policy as is. You can always edit it later on.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>The internal DNS server’s address.</td>
</tr>
<tr>
<td>WINS Server</td>
<td>The internal WINS server’s address (if required).</td>
</tr>
</tbody>
</table>

**Enable AnyConnect SSL Access on the Outside Interface**

**To enable AnyConnect access on outside interface:**

1. Click **Configuration** at the top of the ASDM, the contents of the window changes.
2. In the left panel of the ASDM, select **Remote access VPN**.
3. In the left pane, select **AnyConnect connection profiles**.
   The following widow appears on the right pane:

   ![AnyConnect Connection Profiles](image)

4. On the **outside** interface make sure that the **SSL access** and **Enable DTLS** checkboxes are selected.
Note: Although Datagram Transport Layer Security (DTLS) is not required, using DTLS reduces latency and bandwidth problems associated with SSL connections and improves the performance of real-time applications that are sensitive to packet delays. By default, DTLS is enabled when SSL VPN access is enabled on an interface. Consult Cisco's documentation for further guidance.

Configure Group Policy Minimum Requirements

To configure group policy minimum requirements:

1. Click Configuration at the top of the ASDM, the contents of the window changes.
2. In the left panel of the ASDM select Remote access VPN.
3. In the left pane Select Group policies.
   The following widow appears on the right pane.

4. Click the policy created when you created the connection profile, or Add to create a new policy. The edit internal group policy window opens.
5. Click More Options to expand the options part.
6. Make sure the **SSL VPN client** checkbox is selected.

7. In the left pane, click **Servers**. The contents in the right pane change.

Make sure that the **DNS** and **WINS Server** details are entered and the **Inherit** checkboxes are not selected. If they are selected, then uncheck them and enter the relevant details.
Install the CA Root Certificate

*Note:* This is only an example of installing the CA certificate; there may be other ways to perform the same task.

To install the CA root certificate:

1. Click **Configuration** at the top of the ASDM, the contents of the window changes.
2. In the left panel of the ASDM, select **Remote Access VPN**.
3. In the left pane, expand **Certificate Management** then click **CA Certificates**.

The following widow appears in the right pane:
4. Click **Add** to add a new certificate the **Install Certificate** widow opens.

![Install Certificate Window](image)

5. Select the **Use SCEP** radio button and fill in the **SCEP** server address, using the format: `ip.address /certsrv/mscep/mscep.dll`

6. Click **Install Certificate**.

![Install Certificate Progress](image)

A confirmation message appears when the installation completes.

![Certificate Installed Successfully](image)
Enrolling the ASA Device at the CA.

Note: This is only an example of enrollment; there may be other ways to perform the same task.

To enroll the ASA device at the CA:

1. Click Configuration at the top of the ASDM, the contents of the window changes.
2. In the left panel of the ASDM, select Remote access VPN.
3. In the left pane, expand Certificate Management, and click Identity Certificates. The following widow appears on the right pane:

4. Click Add to add a trustpoint. The Add Identity Certificate window opens.
5. Check the **Add a new identity certificate** radio button then click **Advanced**. The **Advanced Options** window opens.

6. Enter the ASA device in the FQDN field, then select the **Enrollment Mode** tab.

7. Press the **Request Certificate from a CA** radio button and enter the MSCEP url using the format:
   
   `ip.address/certsrv/mscep/mscep.dll`

8. Go to the MSCEP server, and browse to :

   `http://localhost/certsrv/mscep/mscep.dll`

9. Copy the enrollment challenge password.
10. In the **advanced options** window, select the **SCEP Challenge Password** tab and paste the password.

![Advanced Options](image)

**Note:** When copying the password, an extra space may also be copied at the end, paste the password in a visible field to check that it is not present.

11. Click **OK** to get back to the main window and click **Add Certificate**.
A confirmation message appears when the enrollment completes.

Setting Trustpoints

To set up trustpoints:

1. Click **Configuration** at the top of the ASDM, the contents of the window changes.
2. In the left panel of the ASDM, select **Remote access VPN**.
3. In the left pane, expand **Advanced**, and then click **SSL Setting**. The following window appears in the right pane.
4. Double-click the inside interface. The select SSL certificate window opens.

5. Select the certificate you enrolled from the previous section (*Enrolling the ASA device at the CA*).

6. Repeat the same procedure for the external interface using the same certificate.
Changing the ASA Management and VPN Ports (Optional)

**Note:** This is only an example of using ASA based device using one IP address in the AnyConnect configuration. There are other ways to provide for an appropriate solution.

To change the ASA management and VPN ports:

1. Click **Configuration** at the top of the ASDM, the contents of the window changes.
2. In the left panel of the ASDM, select **Device Management**.
3. In the left pane, select expand **Management Access**, and click **ASDM/HTTPS/Telnet/SSH**. The following widow appears in the right pane:

4. Under port number select a port that is different to 443 (e.g. 8443).
5. To Change the ASA VPN port, click **Configuration** at the top of the ASDM, the contents of the window changes.
6. In the left panel of the ASDM, select **Remote Access VPN**.
7. In the left pane, select **AnyConnect Connection Profiles**. The following widow appears on the right pane:
8. In the right pane click **Port Settings**. The Configure Port Settings window opens.

9. Change the port number to something that is different to 443, e.g. 5443.

10. Click **OK**.
Redirecting HTTPS Traffic to the SAM Portal Server

To redirect HTTPS traffic to the DMZ portal server:

1. Click **Configuration** at the top of the ASDM, the contents of the window changes.

2. In the left panel of the ASDM select **Firewall**, and then **NAT Rules**, the contents of the window changes.

3. Click **Add** to create a new rule.

4. Under **Match Criteria: Original Packet**, select **outside** in the **Destination Address** field and **any** in the **Source Address** field.
5. Under **Match Criteria: Original Packet**, type **Https** in the **Service** field, or click ![image] to browse for the service. The *Browse Original Service* window opens.

6. Select the **https** service and click **OK**.

![image]

7. Under **Action: Translated Packet**, in the **Destination Address** field, click ![image]. The *Browse Translated Destination Address* window opens.
8. Click Add then select Network Object. The Add Network Object window opens.

9. In the Name field, enter the name of the SAM portal server and its IP Address, then click OK.

10. Enter the name of the newly created object under Translated Destination address, then click OK.

11. In the Edit NAT Rule window click OK again.
Allowing HTTPS Access to the SAM Portal Server

To allow https access to your SAM portal server:

1. Click **Configuration** at the top of the ASDM, the contents of the window changes.

2. In the left panel of the ASDM, select **Firewall** then **Access Rules**, the contents of the window changes.

3. Click **Add** to add, and then select **Add Access Rule** to create a new access rule, the **Add Access Rule** window opens.
4. In the **Destination** field, select the server object created under *Redirecting HTTPS traffic to the SAM Portal Server*.

5. In the **Service** field, enter Https.

6. Click **OK**.
Chapter 8
Mobile Device Enrollment

The iOS mobile device enrollment is performed using a SAM portal (SAMiOS portal). During the enrollment the mobile device is assigned to a user, and the configured profile in the TPO is installed on the device.

Enrolling a Device

To enroll a device:
1. On the mobile device, open the Safari browser.
2. Enter the SAMiOS path <server name.domain name>/samios
   The SAMiOS portal opens.
3. Enter the Username and Password, and then click Submit.
   The Mobile Device Enrollment Page opens.
4. Click **Start**.

   The **Install Profile** window opens.

5. Click **Install**.

   A confirmation dialog box opens.
6. **Click Install Now.**

   The profile installation begins.

   On installation completion a confirmation dialog box opens.

   ![Profile Installed](image)

   The profile is displayed in the mobile device’s installed profiles list.
Enrolling a Device with AnyConnect VPN Profile

To enroll a device:

1. On the mobile device, open the Safari browser.

2. Enter the SAMiOS path `<server name.domain name>/samios`
   The SAMiOS portal opens.

3. Enter the Username and Password, and then click Submit.
   The Mobile Device Enrollment Page opens.

4. Click Start.
   The Install Profile window opens.
5. Click **Install**.

A confirmation dialog box opens.

6. Click **Install Now**.
The profile installation begins.
During the installation the following stages appear (some stages might be longer than others):

- **Installing Profile**
  - **Profile Service**
    - **SafeNet**
    - **Verified**
  - **Profile Service**
    - **SafeNet**
    - **Description**
      - Enter device into the SafeNet encrypted profile service
    - **Signed** 2003s.vm2003.com
    - **Received 2011-09-08**
    - **Contains Device enrollment challenge**
  - **More Details**

- **Generating Key**
  - **Profile Service**
    - **SafeNet**
    - **Verified**
  - **Profile Service**
    - **SafeNet**
    - **Description**
      - Enter device into the SafeNet encrypted profile service
    - **Signed 2003s.vm2003.com**
    - **Received 2011-09-08**
    - **Contains Device enrollment challenge**
  - **More Details**

- **Enrolling Certificate**
  - **Profile Service**
    - **SafeNet**
    - **Verified**
  - **Profile Service**
    - **SafeNet**
    - **Description**
      - Enter device into the SafeNet encrypted profile service
    - **Signed 2003s.vm2003.com**
    - **Received 2011-09-08**
    - **Contains Device enrollment challenge**
  - **More Details**
When installation completes, a confirmation dialog box opens.

The profile is displayed in the mobile device's installed profiles list.