Mobile Management for Configuration Manager 7.2

LAB GUIDE

Date published:
4 September 2012

Document Version:
1.0

Contents

SYMANTEC MOBILE MANAGEMENT FOR CONFIGURATION MANAGER 7.2: LAB GUIDE

The training virtual machine is configured as follows

- Windows 2008 Server R2 with SP1 installed
  - AD Domain Controller
    - The domain for the server is ***symmobile.net***. The name of the server is SCCM-Training1
  - DNS Server
  - IP Address 192.168.2.200
- MS SQL 2008 R2 with SP1 Installed
  - MSSqlServiceAccount is defined as the SQL Service account for SQL Services
  - MSSqlServiceAccount and Administrator are defined SQL Database administrators
- SCCM 2007 SP2
  - SCCM is running in ***Mixed Mode***
  - Site Code is ***SYM***
  - Site Name is ***Mobile***
  - Each server is also a SCCM Management with the default port 80
- Each of the VM's has the following installed
  - Notepad++
  - Adobe Acrobat
  - WinRAR
  - Google SDK
  - VeriSign SSL wildcard certificate is in the "Certificates" folder on the desktop. The password for the PFX is "P@ssw0rd1"
  - Apple APNS Certificate is located in the folder "Certificates" on the desktop. The password for the PFX is "P@ssw0rd1"
  - The Athena 7.2 installation bits are included on the desktop

By default, the VM is set to NAT which will work fine with the Android emulator. You will need to change the configuration to bridged with internet access on the VM in order to successfully enroll an iOS device. The preference would be a WIFI router connected to the Internet with the ports opened that allow Mobile Management to operate properly.

GETTING STARTED

1. Copy the VM to your desired location. The default password is Symc4now!
2. By default the VM is set to use 2 GB of RAM. Adjust to 4 GB if desired.
3. The username configured is "administrator" as the admin account in each VM
4. The password is "P@ssw0rd1" where 0=zero

PRE-REQUISITES

Google Cloud Management

To setup a GCM account, a Gmail account will be needed. To setup a Gmail account:

1. Access the following website: http://mail.google.com/mail/signup
2. Enter an account name that is easily identified, such as companyname-configman-mdm@gmail.com.

With a Gmail account, follow the steps below.

3. Access the following website. http://developer.android.com/guide/google/gcm/gs.html
4. On the website, follow step 1 and click the Google APIs console page to login to your Gmail account to setup the API's
5. Click "Create Project"
6. Scroll down to the "Google Cloud Messaging for Android" service and toggle the button to "ON"
7. Check the box to agree to terms and click "Accept"
8. Click "Create new Server key…"
9. When the new window opens, click "Create"
10. There are two details that need to be noted. The Project ID and the API key. The API key is listed in the server key details that were just created. The Project ID is in the URL similar to listed below

https://code.google.com/apis/console/#project:259691969641:access

If you do not want to create a GCM account, you can use the following:

- **Project ID:** 259691969641
- **API Key:** AIzaSyAjcmzGaKsvIY9E3FWfPpp-eg8aHG_OPH0

Accounts for Tunnel Server

Membership of the domain groups determine access to interactive Mobile Management Live Support Sessions from Mobile Management Device Explorer, and security groups for the Tunnel Server. After installation, members of groups will have Mobile Management Database read access. The Active Directory account of the Console user must be added to the groups.

The following is the preferred security group configuration that should be defined:

- Tier1 (Level 1 group for Tunnel Server)
- Tier2 (Level 2 group for Tunnel Server)
- Tier3 (Level 3 group for Tunnel Server)

The number determines access level - the higher the number, the more access. Three different security groups must be created for use and can use any name or site naming convention.

Install Symantec Mobile Management for Configuration Manager

The following is the proper order of installation in a Configuration Manager environment. For this lab, we will be focusing on the highlighted areas below which will be all installed on a single Central Server.

1. Internet-Facing Server
    a. Push Services
2. Central Server
    a. Console
    b. ISV Proxy (first time only)
    c. Services
    d. Reporting Services
    e. Feature Packs (optional)
    f. Replication Services
3. Primary Server
    a. Console
    b. Services
    c. Feature Packs (optional)
4. Secondary Server
    a. Console (optional)
    b. Services

Component Installation Notes:

For this lab, ensure that you use Fully Qualified Domain Name (FQDN) formats for the prompts.

1. Push Services Installation
    - The Push Services Installation consists of the APNS Web Service, GCM Service, and the Feedback Service
    - Push Services must be installed on a server that has access to the internet. Typically, this is a server not running Configuration Manager but for this lab it will all be installed on a single server
    - The iOS Feedbakc Service communicates with the Central server database and the APNS Web Service to obtain a list of iOS devices that are no longer communicating with the server
    - Google Cloud Messaging routes communication to Android devices
    - If the Feedback Service is located on a different server than the Push Services, then use the Fully Qualified Domain Name

2. Console Installation
    - Configuration Manager should be installed in Mixed mode, not Native mode
    - The installation shoulded be performed at the required rights level of an administrator for the Configuration Manager server

- If the console is being installed on a 64-bit OS, then the 64-bit version of Java must be installed
- The Console installation is typicallyed installed on every machine that has the Configuration Manager console installed
- Use the fully qualified domain name of the Central server during the installation
- The ISV proxy certificate must be added to the Configuration Manager console. This should be done on all Central and Primary servers in a site hierarchy
    i. From the Configuration Manager console expand Site Database > Site Management > yoursitename > Site Settings > Certificates
    ii. Right click on ISV Proxy and select Register or Renew ISV Proxy
    iii. On the certificate registration or renewal screen, select Register Certificate for ISV Proxy
    iv. Click Browse to locate the ISV Proxy certificate. By default this is placed in the C:\Program Files (x86)\Odyssey Software\Athena\SCCM folder
    v. Click Apply

3. Services Installation
    - Services installation is done on all Management Point servers to which devices are reporting
    - For multiple sites, installation should be done following the site hiearchy. Starting from the top and down
    - For the Tunnel Server component installation, enter the names of the three security groups we created. This must be in WINS name format i.e. symmobile\tier1
    - On the Device Agent Server Configuration screen, ensure that the server name for both Agent (iOS and Android) and iOS MDM (SSL) is entered as Fully Qualified Domain Name format

CONFIGURATION FOR LDAP AUTHENTICATION

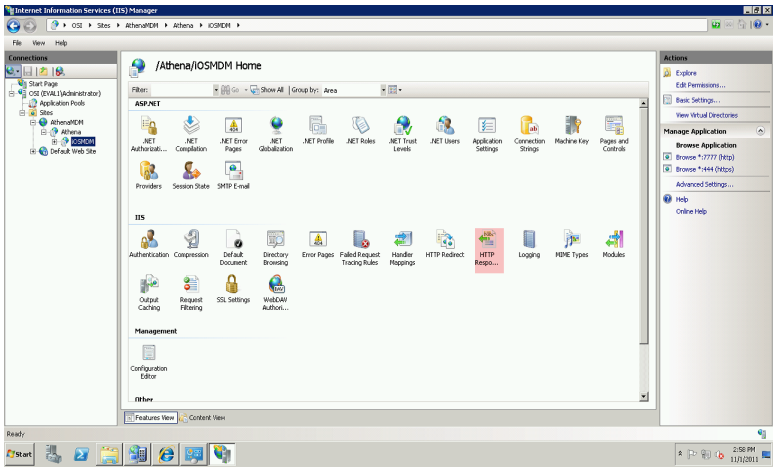
1. Open the C:\Program Files (x86)\Odyssey Software\Athena\SCCM\Web\Enrollment\Web.config file in an editor
2. Edit the following lines and set them to the appropriate values

```
<add key="SCCM-ActiveDirectoryServer" value ="SCCM-Train1" />
<add key="SCCM-DomainName" value="symmobile" />
<add key="SCCM-DomainExtension" value="net" />
<add key="SCCM-LDAPAuthenticationType" value="1" />
<add key="SCCM-LDAPUserContainer" value="{SeekUser}" />
<add key="SCCM-LDAPProtocol" value="LDAP" />
```

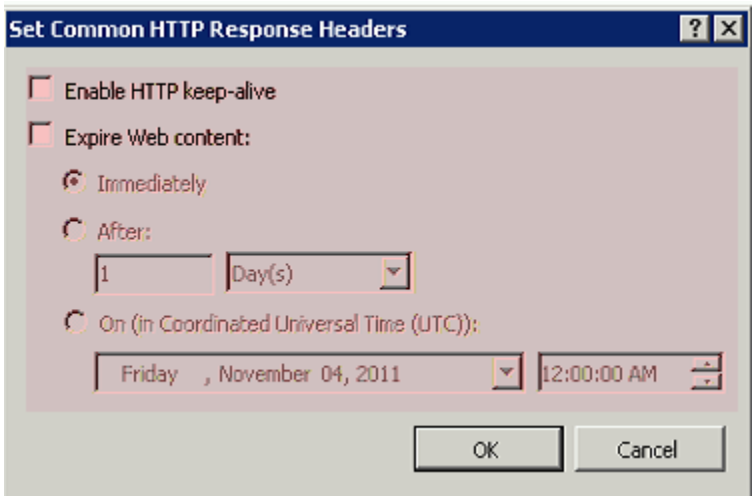
WINDOWS 2008 R2 SP1 IIS CHECK

1. Open IIS Admin
2. Open Sites
3. Expand the AthenaMDM site
4. Expand the Athena Website

5. Highlight iOSMDM site and select HTTP Response



6. Right click Powered by ASP.NET and select Remove
7. Click Set Common Headers
8. Uncheck all boxes including the Enable HTTP keep-alive

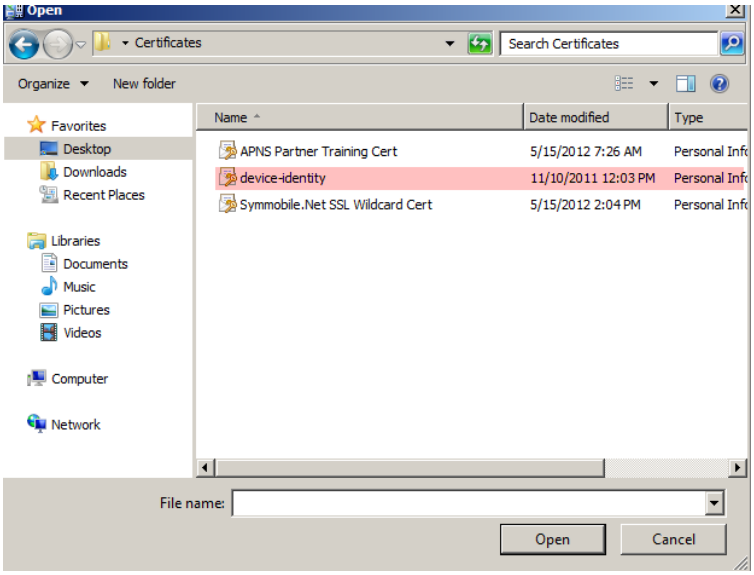


9. Click OK
10. Close IIS Admin

Device Identity Certificate

1. Open SCCM MMC
2. Select Computer Management
3. Select Mobile Device Management
4. Select Athena
5. Select Profiles
6. Select Configuration Editor

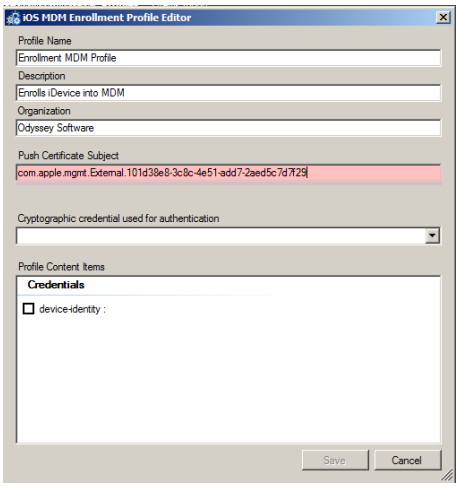
7. Select Credentials
8. Click the * to create a new profile
9. Click Select cert file
10. Browse to Desktop\Certificates
11. Select the device-identity certificate and click Open



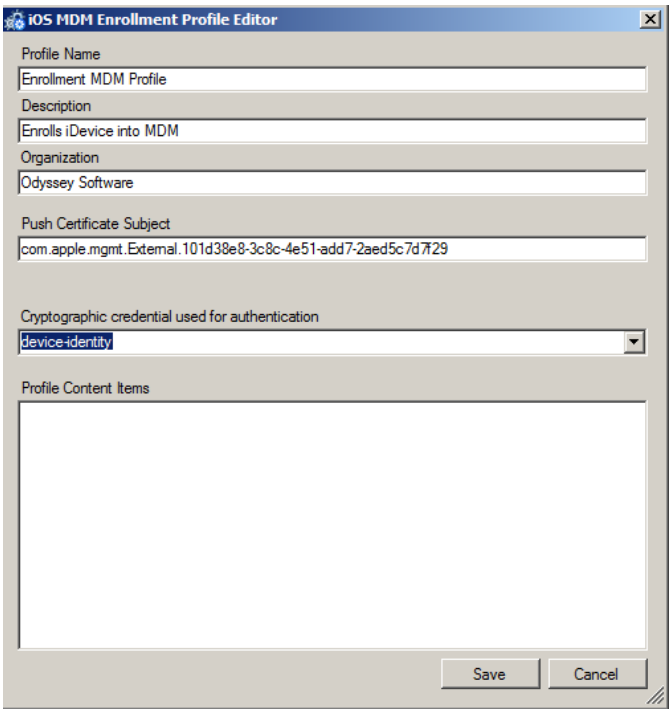
12. Enter “athena” without the “ “ as the password
13. Click Save Changes
14. Close the Config Editor

Modifying the Enrollment MDM Profile

1. In the SCCM MMC go to Computer Management\Mobile Device Manager\Athena\Profile
2. Right click the Enrollment MDM Profile and select edit
3. Change the Push Certificate Subject to match the subject of the installed APNS cert on the training VM



4. Click the down arrow on Cryptographic credential used for authentication and select device-identity.



5. Click Save

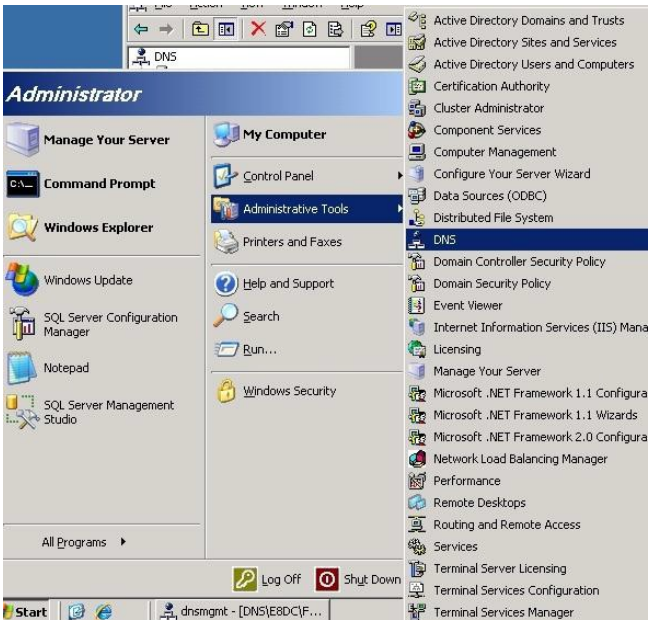
Enterprise Mobile Library Content

1. Content has been put on the Desktop to populate the Enterprise Mobile Library
2. In the SCCM MMC go to Computer Management\Mobile Device Manager\Athena\Mobile Library
3. Create a new feed called Training

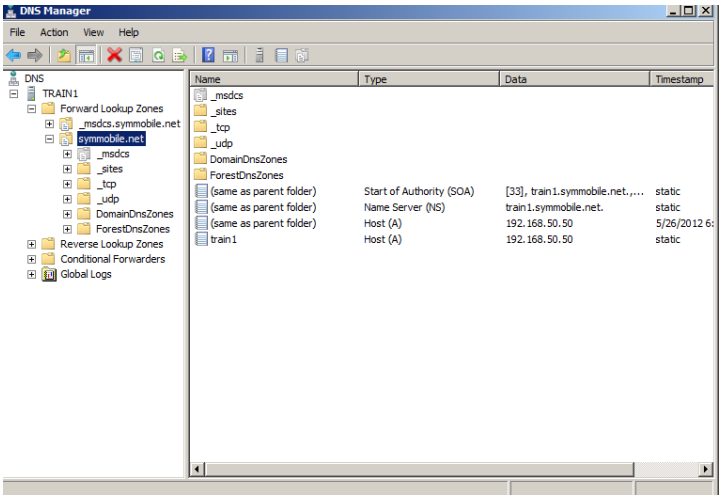
4. Click Items
5. Add these items to the Enterprise Mobile Library
    a. Athena Agent Guide – PDF
    b. Lake Video – Video
    c. Good Reader
        i. Apple App Store URL - http://itunes.apple.com/us/app/goodreader-for-ipad/id363448914?mt=8
6. Assign Enterprise Mobile Library Feed to the All Apple Mobile Devices Collection.

CREATING MDM DNS TXT ENTRIES

1. Log in to the Domain Controller.
2. Access **Start > Administrative Tools > DNS** to run the DNS utility



3. From the DNS Window, navigate to the domain folder.



4. Right-click the domain folder and select **Other New Records**
5. On the Resource Record Type dialog, select *Text (TXT)* from the list.
6. Click **Create Record**.
7. Leave the **Record name** field blank.
8. Enter the following entry in the **Text** field for either iOS (following) or Android (page xviii of this appendix).

For iOS:

OSIAGENTREGURL=http://*<site server IP address or FQDN servername>*/Athena/Enrollment/AthenaIosEnroll.aspx

Note: The best practice is to use the Fully Qualified Domain Name (FQDN) of the server and use SSL (https) for enrollment.

Example:

https://sccm-train1.symmobile.net/Athena/Enrollment/AthenaIosEnroll.aspx

For Android:

android-mdm-enroll=http://*<site server IP address or FQDN servername>*/Athena/Enrollment/AthenaAndroidEnroll.aspx

Note: The best practice is to use the Fully Qualified Domain Name (FQDN) of the server and use SSL (https) for enrollment.

Example:

https://sccm-train1.symmobile.net/Athena/Enrollment/AthenaAndroidEnroll.aspx

9. Close DNS Manager

UPDATE QUERY FOR ALL WINDOWS MOBILE DEVICES

By default, SCCM will put all mobile devices in the same Windows Mobile collection, regardless if they are Windows Mobile or not. To correct this, the query used to determine membership must be changed.

1. Browse to Site Database > Computer Management > Collections
2. Right-click “All Windows Mobile Devices” and select “Properties”
3. Click the “Membership Rules” tab
4. Double click the “All Windows Mobile Devices” membership rule
5. Click “Edit Query Statement”
6. Click the “Criteria” tab
7. Replace the current text with the following

```
select SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,
SMS_R_SYSTEM.Name,SMS_R_SYSTEM.SMSUniqueIdentifier,
SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from SMS_R_System where
SMS_R_System.ResourceType = 5 and SMS_R_System.ClientType = 3 and
SMS_R_System.OperatingSystemNameandVersion like "Windows%"
```

CONCLUSION

Hopefully this document has provided insight on the Symantec Mobile Management for Configuration Manager setup. Thank you for your time.

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical

This document may include information about pre-release software. Any unreleased update to the product or other planned modification is subject to ongoing evaluation by Symantec and therefore subject to change. This information is provided without warranty of any kind, express or implied. Customers who purchase Symantec products should make their purchase decision based upon features that are currently available.

Symantec reserves the right to make changes without prior notice.

About Symantec

Symantec is a global leader in providing security; storage and systems solutions to help businesses and consumers secure and manage their information. Headquartered in Mountain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S. call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com