



Symantec Mobile Management 7.1 Best Practices/Configuration Guide

TABLE OF CONTENTS

1 Introduction	1
2 Prerequisite check-list	2
2.1 Mobile Management Requirements	2
3 Recommended Architecture	5
3.1 Architecture Best-Practices and Components	5
3.2 Architecture Diagrams	8
3.3 Reverse Proxy Installation	10
4 Ports	20
4.1 Required network ports/connections	20
5 Certificate Requirements and Recommendations	21
5.1 Apple MDM/Certificates – overview and obtaining from Apple	21
5.2 Using an Identity certificate for device enrollment – POC only	21
5.3 Apple iOS MDM agent options – internal built vs. App store version	23
6 Configuring SMM for SSL Communication to support iOS 5 ...	24
6.1 Generating an SSL certificate request and SSL certificate	24
6.2 Installing your server certificates	25
6.3 Configuring IIS to use your SSL certificate	26
6.4 Configuring SSL communication in the SMM console	26
6.5 Creating the Credential payload for the root CA	27
7 How to check the prerequisite environment	30
7.1 Certificates (are responding as required)	30
7.2 Port Check (before SMM product installation)	33
8 Common Configuration Errors	34

1 Introduction

The purpose of this document is to give guidance on the best practices setup and configuration guidelines for Symantec Mobile Management 7.1, focusing on environment configuration guidelines such as prerequisites, required ports, recommended architecture, and certificate requirements. This document is intended to be a work in progress and will be updated as additional information is found and deemed appropriate.

2 Prerequisite check-list

- The customer has an Enterprise Apple Push Notification Service (APNS) certificate obtained via Apple Enterprise iOS Developer Membership and Agreement for Mobile Device Management - *see section 5.1 - Apple MDM/Certificates – overview and obtaining from Apple.*
- Required Ports Configured
- CA and Root Certificate
- SCEP server installed

2.1 Mobile Management Requirements

2.1.1 System Requirements

System Requirements and Prerequisites
<p>Mobile Management Server</p> <ul style="list-style-type: none"> • .NET Framework 3.5 • Windows Server 2008 R2 • Windows Server 2003 • SQL Server 2005 or 2008 • IIS 6.0 NET Framework 3.0 • Microsoft Message Queuing Service <p>Note: The Symantec Mobile Management (SMM) Site Server needs to be installed on a Windows Server 2008 R2 without SP1 currently. A fix will be made available as quickly as possible after the release of SMM 7.1 to allow the MMS site server to be installed onto a Windows Server 2008 R2 with SP1.</p>
<p>Symantec Management Platform Server:</p> <ul style="list-style-type: none"> • Windows Server 2008 R2 64bit • .Net Framework 3.0 • Windows Server 2008 R2 • SQL Server 2005 or 2008 • IIS 7.5 with Compatibility for IIS 6.0 Installed • .Net Framework 3.0 • Microsoft Message Queuing Service • Symantec Management Platform 7.1 SP1
<p>Console Software Prerequisite:</p> <ul style="list-style-type: none"> • Internet Explorer 7.1

<ul style="list-style-type: none"> • Java Runtime Environment – required for Remote Control
<p>Exchange (ActiveSync) Integration (not required for iOS native agent devices):</p> <ul style="list-style-type: none"> • Microsoft Exchange 2007 (SP1 or SP2) or Microsoft Exchange 2010 <ul style="list-style-type: none"> ○ Note: Exchange 2003 and Exchange 2007 RTM are not supported. ○ The minimum version is Exchange 2007 SP1 ○ • Microsoft Exchange Server 2007 Management Tools or Microsoft Server 2010 management Tools <ul style="list-style-type: none"> ○ Required Component – Exchange Management Shell • Microsoft Windows Management Framework <ul style="list-style-type: none"> ○ Required Component – Windows PowerShell Shell
<p>Microsoft Enterprise Certificate Authority</p>
<p>Microsoft Certificate Services</p> <ul style="list-style-type: none"> • Microsoft Certificate Authority • A Simple Certificate Enrollment Protocol (SCEP) Server needs to be available. The Microsoft Network Device Enrollment Service (NDES) and Certificate Enrollment Web Service (CEWS) services need to be installed onto a Windows 2008 server. <p>*Further information on this topic can be found at Microsoft SCEP Implementation Whitepaper</p> <ul style="list-style-type: none"> • The SCEP server should be separate (not installed onto) the CA server.
<p>Certificates</p> <ul style="list-style-type: none"> • Enterprise must provide an Apple Push Notification Service (APNS) certificate for use in push communications to the agent. Communication via APNS requires the use of an Apple APNS certificate to manage iOS devices. • The APNS certificate is available for customers who are members of the Apple Enterprise iOS Developer program. • Externally signed Root Certificate (e.g. VeriSign) available from the CA Server.
<p>Note: The Mobile Management Server Component also supports Windows Server 2003 32-bit for remote deployment of this piece in DMZ, etc. The SMP Server does not support this OS version any longer – only Windows 2008 R2 64 – bit (see architecture diagram)</p>

In addition to the native iOS agent, Symantec Mobile Management (SMM) 7.1 product can also utilize Microsoft Exchange ActiveSync to inventory and configure devices with policies without an agent. While this capability cannot manage Apple iOS devices as effectively as the native SMM 7.1 agent, it may be required in some environments and is the only way today to manage certain mobile operating systems (HP WebOS, Microsoft Windows Phone 7 and Android). Symantec Mobile Management ActiveSync support is enabled via integration with Microsoft Exchange 2007 or 2010. The Microsoft Exchange Server should be setup and connected with a Domain Controller system to ensure that email can be sent to and from user accounts (i.e. domain user names resolve properly).

2.1.2 Supported Device Operating Systems

Device Requirements
<p>iOS Agent requirements (New with MMS v7.1)</p> <ul style="list-style-type: none"> • Apple iPhone <ul style="list-style-type: none"> ○ Minimum IOS version: 4.1 ○ Models Supported: 3G, 3GS, 4 • Apple iPad <ul style="list-style-type: none"> ○ Minimum IOS version: 4.2 ○ Models Supported: All Models (Wifi and Wifi w/3G)
<p>Existing Device support requirements:</p> <ul style="list-style-type: none"> • Device Agents <ul style="list-style-type: none"> ○ Windows Mobile 2003, 5, 6.1, and 6.5 ○ Windows CE 4.2 to 6.0 ○ BlackBerry OS 4.3 – 5.0
<p>Agentless Management via Exchange ActiveSync:</p> <p>Apple iOS 2.x, 3.x and 4.x o Android 2.2 and higher</p> <ul style="list-style-type: none"> ○ Windows Mobile 6.1 and 6.5 ○ Palm WebOS 1.4.5 o Nokia (running Mail for Exchange v3.0.50) ○ Other devices compatible with Exchange ActiveSync will be reported on in the console, but are not verified and therefore currently not supported. Additional device OS types may be verified and supported after release of this Service Pack.

3 Recommended Architecture

Architecture configurations will vary based upon existing customer infrastructure available or level of integration desired. The following section provides information for configuration of components in approved installation scenarios and highlights best practices as it relates to the installation of Mobile Management 7.1.

3.1 Architecture Best-Practices and Components

For a production environment, it is strongly recommended to not install all components on a single box (e.g. SMM site server, SCEP server). With a single server approach it has consistently been found that the likelihood of a services conflict is much higher, and there is also a significantly increase in the difficulty of troubleshooting if issues arise during installation/configuration. For demonstration or POC purposes some services may be run in conjunction to minimize the number of servers required.

Microsoft Certificate Authority Server

This server is responsible for issuing digital certificates. A CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.

It is installed using a Server Roll service on a server residing within the private/internal network.

Simple Certificate Enrollment Protocol (SCEP) Server

This server is responsible for communicating certificate requests from devices running on the network, devices such as routers and switches, which cannot otherwise be authenticated on the network, to enroll certificates from a certification authority (CA). SCEP is a communications protocol and is used by installing the Microsoft Network Device Enrollment Service (NDES).

The Microsoft NDES service should be installed on a separate server from the CA and Mobile Management Server site servers in a production environment.

Note: The Microsoft Enterprise version of SCEP needs to be used/configured, and not the Standalone version.

*Further information on this topic can be found at [Microsoft SCEP Implementation Whitepaper](#)

Reverse Proxy Server

This is a server that is usually deployed in a network DMZ to protect HTTP servers on a corporate intranet by performing security functions that protect the internal servers from attacks by users on the Internet. The reverse proxy server protects internal HTTP servers by providing a single point of access to the internal network.

This server is only required in certain architecture configurations and will be installed in the DMZ. – see [Architecture Diagram 1](#)

Systems that are commonly used as a Reverse Proxy within the DMZ are a Microsoft IIS system, or an F5 device. F5 devices have a high-level of intelligence and are typically configured by a network team to support Reverse Proxy configuration required for Mobile Management Suite. See [section 3.3 for IIS Reverse Proxy configuration](#) for guidance.

Symantec Mobile Management Site Server

This server is responsible for housing the Symantec Mobile Management installation components which allow devices to communicate to the site servers and thus to the Symantec Management Platform server.

Depending upon desired architecture configuration, this server is installed in the DMZ or the internal network depending upon domain membership. It needs to be accessible to the mobile devices that are enrolling.

Symantec Management Platform Server

This server provides a set of services that IT-related products can leverage. Products plug into and take advantage of platform services, such as discovery, agent management, automation and reporting.

The Symantec Management Platform Server should not be installed into the DMZ, but rather into the private/internal network due to security considerations.

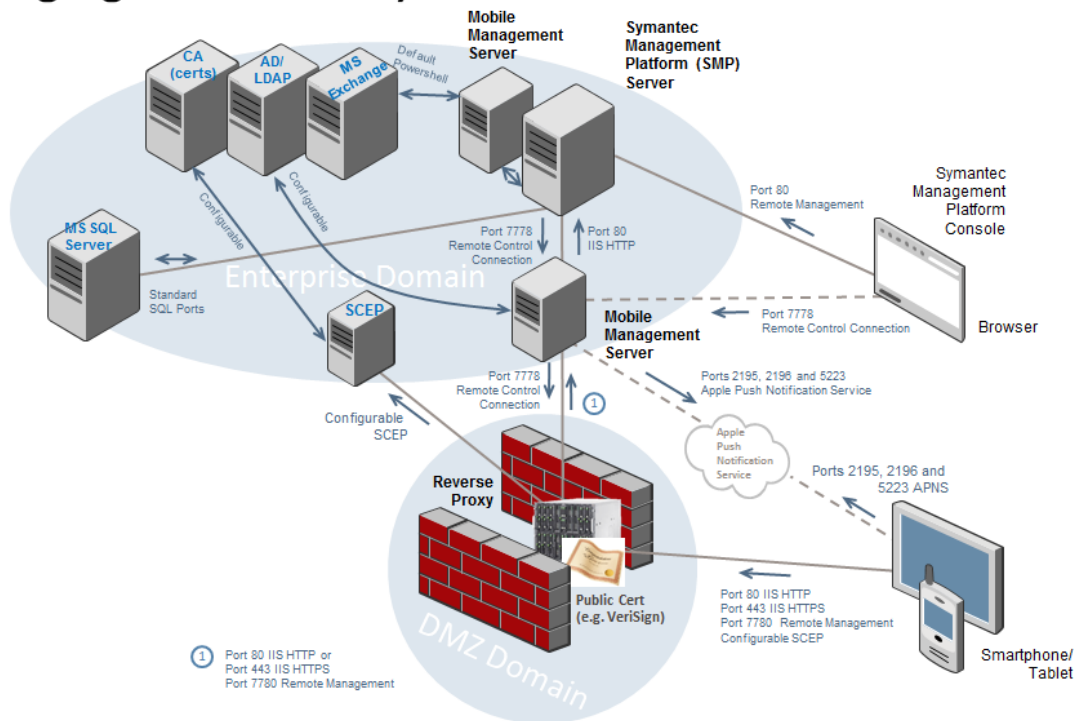
A single Microsoft domain is recommended for the main Mobile Management components and services (e.g. SMP, MMS site server, CA and SCEP)

It is not recommended that the MMS site server and SCEP server be put into a separate Microsoft Domain from the CA and SMP. It has been found this can cause naming resolution and certificate resolution issues. The SCEP and MMS site servers can be physically placed into the DMZ whilst still being a part of the single Microsoft Domain - see [Architecture Diagram 2](#)

If it is not desirable to have the SCEP or MMS site servers in the DMZ whilst part of a single Microsoft Domain, the alternative is to place a Reverse Proxy that is part of a separate Microsoft Domain in the DMZ, and have the SCEP and MMS site servers placed within the private (non DMZ) network. The CA, SMP, MMS site server and SCEP services remain in the same Microsoft Domain in the private network. The Reverse Proxy in this approach provides the certificate request and name resolution translations from the external mobile device in the external network to the private network containing the CA, SMP, MMS site server and SCEP components/services – see [Architecture Diagram 1](#)

3.2 Architecture Diagrams

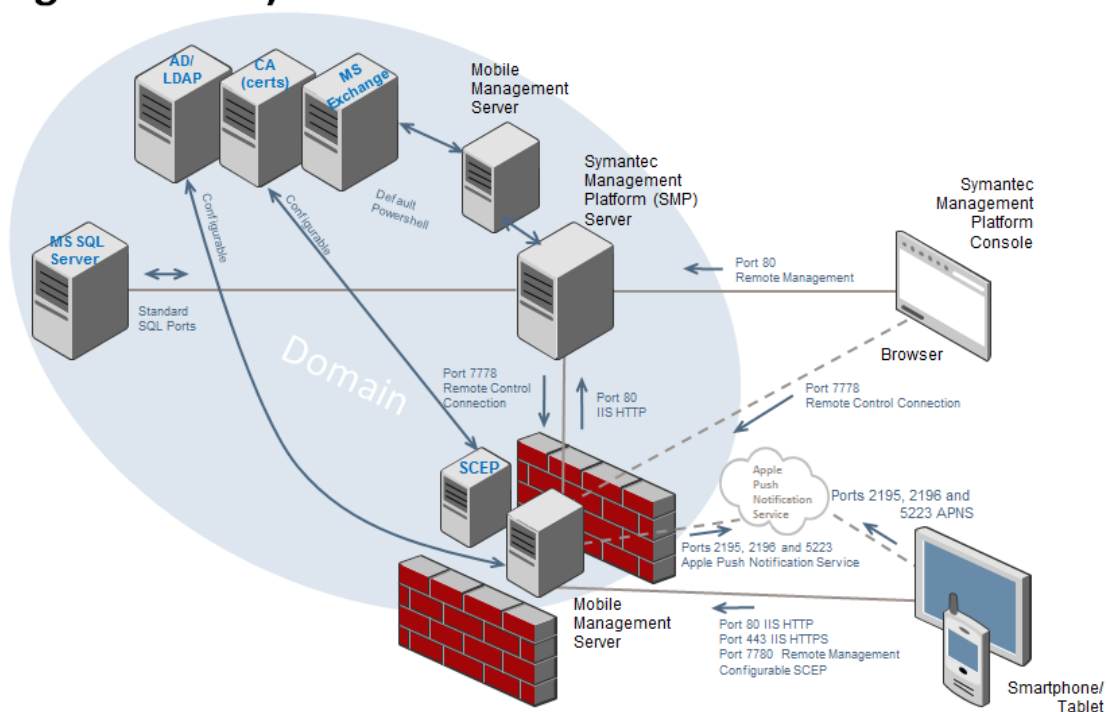
Mobile Management 7.1 Extended Architecture (segregated domains)



Mobile Management 7.1 Architecture

Architecture Diagram 1

Mobile Management 7.1 Extended Architecture (single domain)



Mobile Management 7.1 Architecture

Architecture Diagram 2

3.3 Reverse Proxy Installation

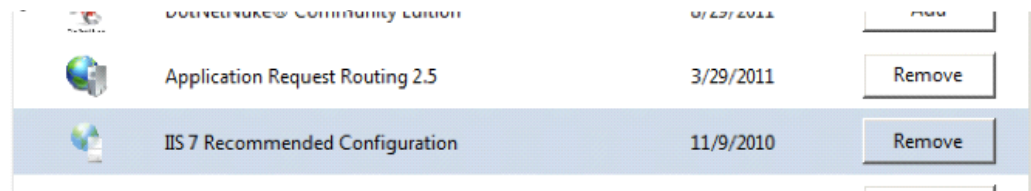
These steps are for installing and configuring the required components for a reverse proxy installation should it be required for the desired architecture configuration. These steps are documented using Windows 2008 R2 and assume this box is installed in the customer DMZ.

Basic IIS Application Request Routing (ARR) setup for a Mobile Management and SCEP server rule set (Reverse Proxy). For consistent results, using Web Platform Installer 3.0

<http://www.microsoft.com/web/downloads/platform.aspx>

Once the platform installer is open,

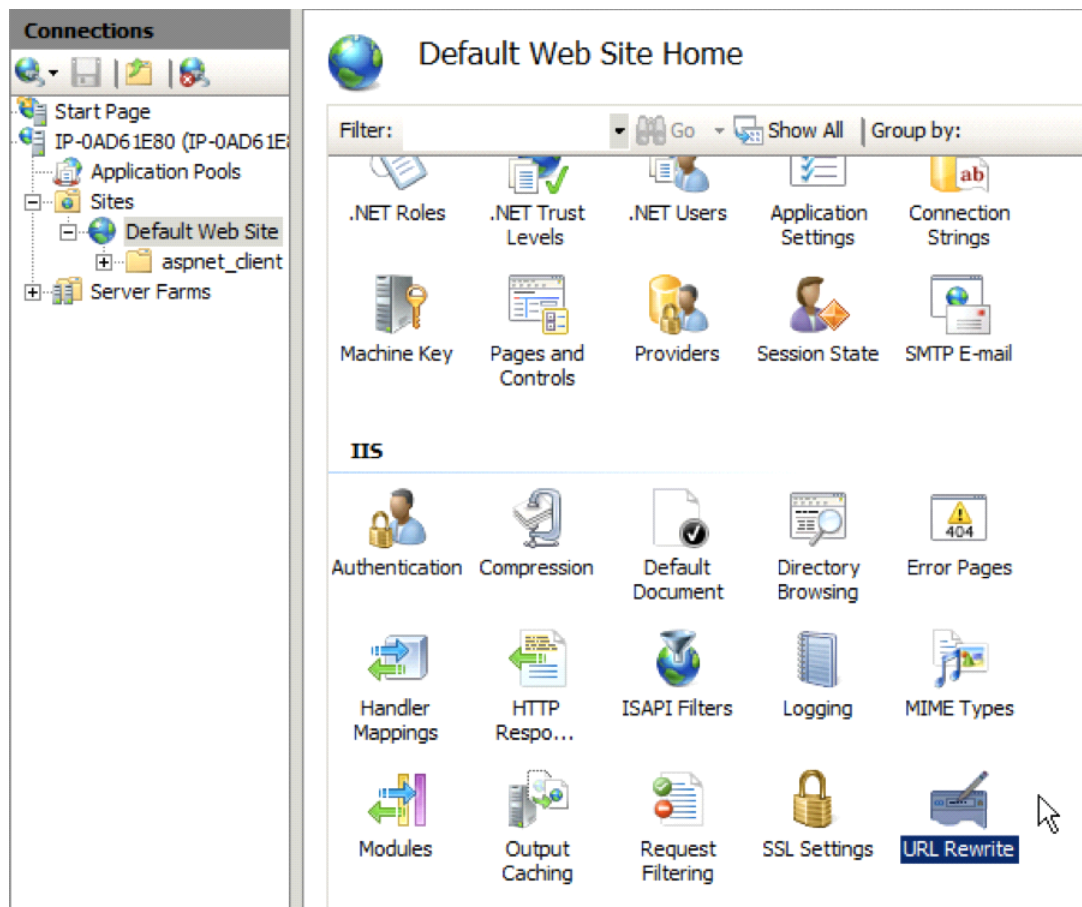
1. Select **Add** for Application Request Routing 2.5 and IIS 7 Recommended Configuration.
2. Install.




Once done installing you will need to go the default web site in Internet Information Services Manager.

3. Select **Default Web Site**
4. Under IIS section and select **URL Rewrite**.

NOTE: You may have to reset IIS and re-launch the Server Manager to see it.



5. Double click to **open**.



URL Rewrite

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern
------	-------	-------	---------

Outbound rules that are applied to the headers or the content of an HTTP response:

Name	Input	Match	Pattern	Action Type
------	-------	-------	---------	-------------

Features View Content View

Actions

- [Add Rule\(s\)...](#)
- [Revert to Parent](#)
- Manage Server Variables**
 - [View Server Variables...](#)
- Manage Providers**
 - [View Rewrite Maps...](#)
 - [View Providers...](#)
- Inbound Rules**
 - [Import Rules...](#)
- Outbound Rules**
 - [View Preconditions...](#)
 - [View Custom Tags...](#)
- [Help](#)
- [Online Help](#)

6. Select **Add rule(s)**.

Add Rule(s)

Select a rule template:

Inbound rules

- Blank rule
- Request blocking

Inbound and Outbound Rules

- User-friendly URL
- Reverse Proxy**

Outbound rules

- Blank rule

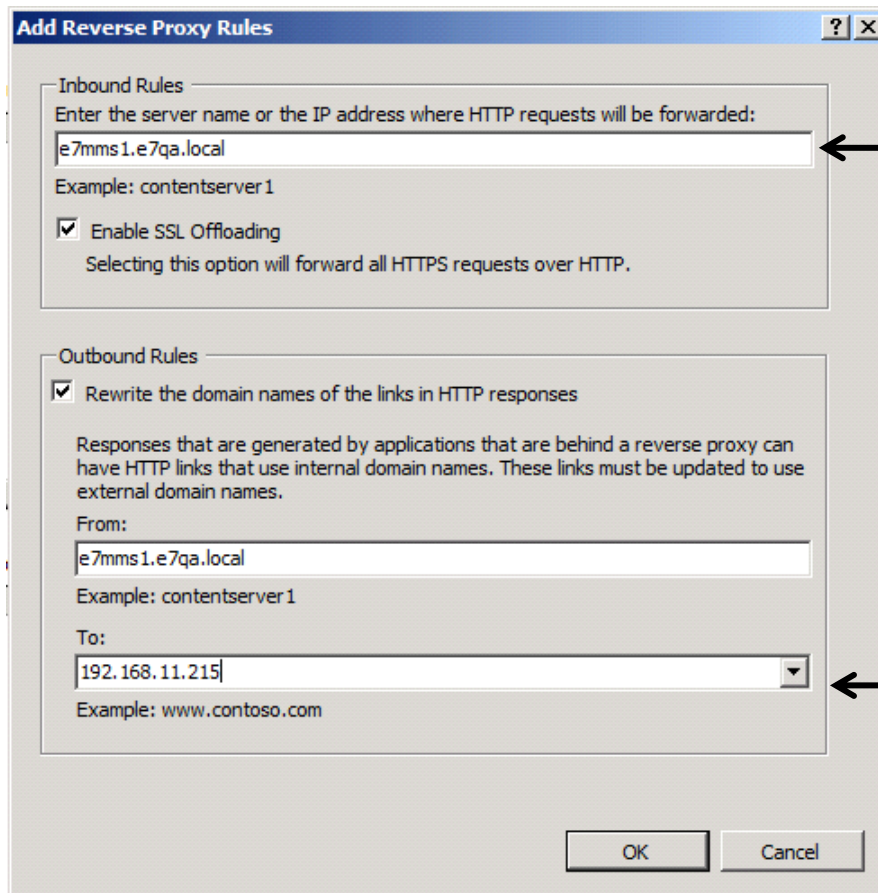
Search Engine Optimization (SEO)

- Enforce lowercase URLs
- Canonical domain name

Select this template to create a rule that will forward incoming HTTP requests to a back-end Web server.

OK Cancel

7. Select **“Reverse Proxy”**, and click **OK**



Add Reverse Proxy Rules

Inbound Rules

Enter the server name or the IP address where HTTP requests will be forwarded:

e7mms1.e7qa.local

Example: contentserver1

☒ Enable SSL Offloading

Selecting this option will forward all HTTPS requests over HTTP.

Outbound Rules

☒ Rewrite the domain names of the links in HTTP responses

Responses that are generated by applications that are behind a reverse proxy can have HTTP links that use internal domain names. These links must be updated to use external domain names.

From:

e7mms1.e7qa.local

Example: contentserver1

To:

192.168.11.215

Example: www.contoso.com

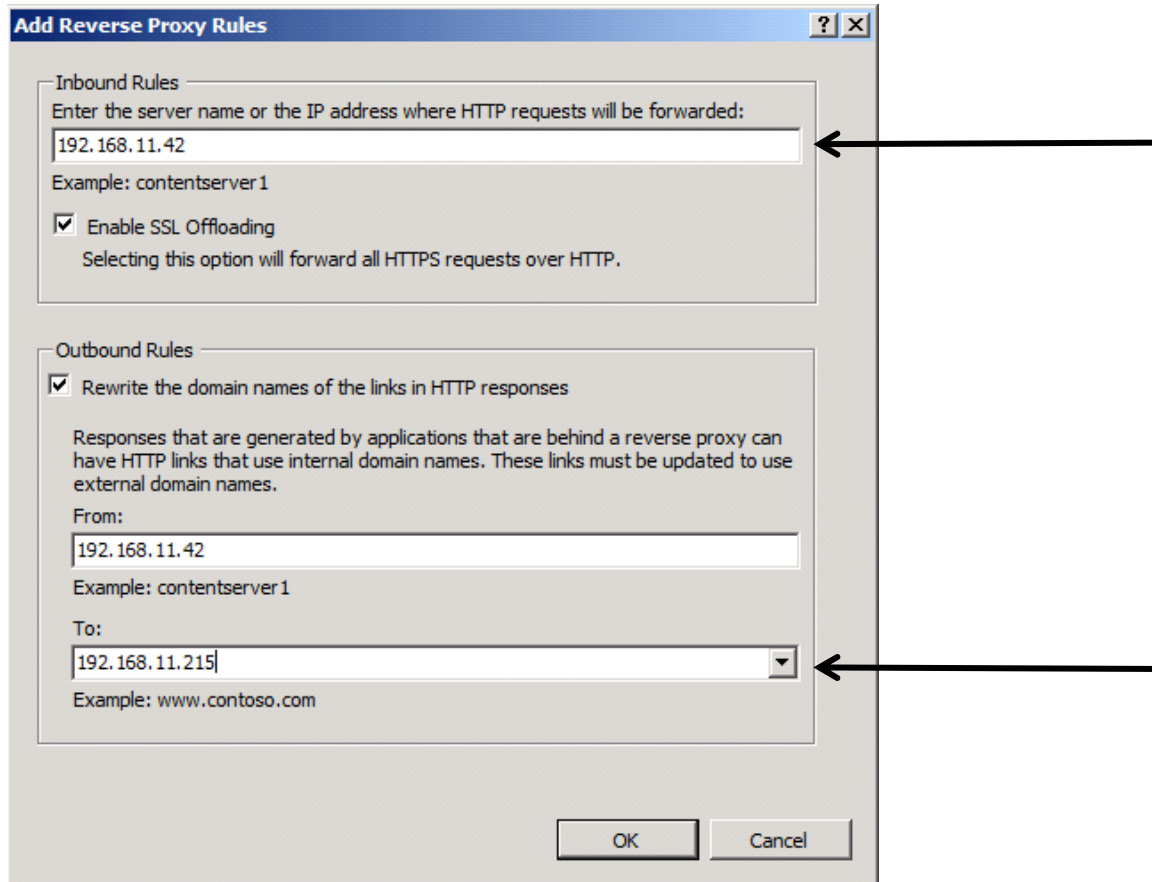
OK Cancel

The first inbound rule is for the SMM server.

8. **Enter** the SMM server FQDN or internal IP.

The outbound rule is also required.

9. In the To: field, **Enter** the reverse proxy server FQDN or IP.
10. Click **OK**

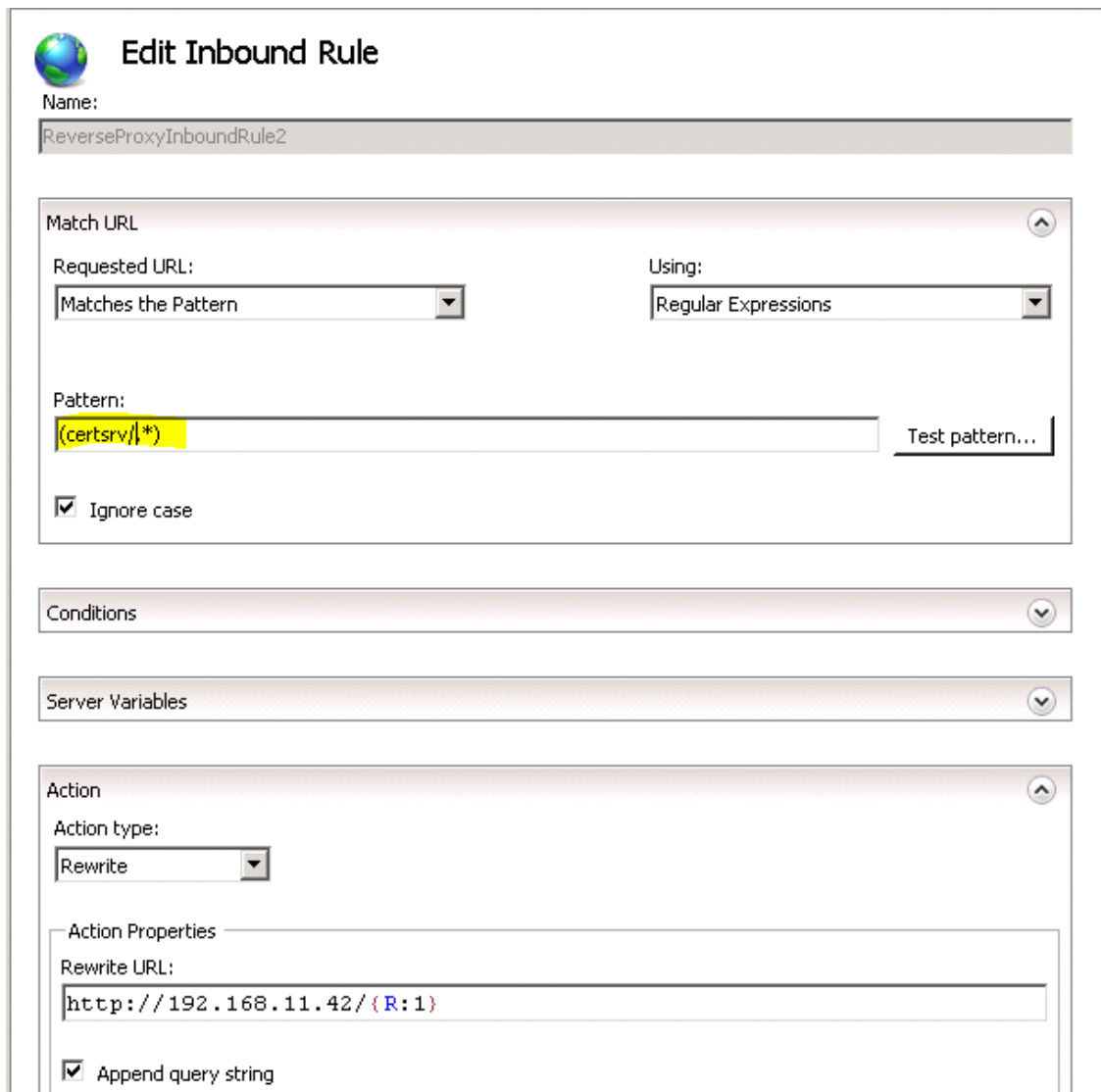


Create a second Inbound rule, this is for the SCEP server.

11. **Enter** the SCEP server FQDN or IP address into the Inbound rules.

The outbound rule is also required.

12. In the To: field, **Enter** the reverse proxy server FQDN or IP.
13. Click **OK**
14. **Open** the Inbound SCEP rule just created.
15. The rule pattern needs to be "(certsrv/.*)". Make sure to click **apply**.



The screenshot shows the 'Edit Inbound Rule' configuration window. At the top, there is a globe icon and the title 'Edit Inbound Rule'. Below the title, the 'Name' field is set to 'ReverseProxyInboundRule2'. The 'Match URL' section is expanded, showing 'Requested URL' set to 'Matches the Pattern' and 'Using' set to 'Regular Expressions'. The 'Pattern' field contains '(certsrv/|*)' and is highlighted in yellow. A 'Test pattern...' button is next to it. The 'Ignore case' checkbox is checked. Below the 'Match URL' section are 'Conditions' and 'Server Variables' sections, both collapsed. The 'Action' section is expanded, showing 'Action type' set to 'Rewrite'. The 'Action Properties' section is also expanded, showing 'Rewrite URL' set to 'http://192.168.11.42/{R:1}'. The 'Append query string' checkbox is checked.

Edit Inbound Rule

Name: ReverseProxyInboundRule2

Match URL

Requested URL: Matches the Pattern Using: Regular Expressions

Pattern: (certsrv/|*) Test pattern...

☒ Ignore case

Conditions

Server Variables

Action

Action type: Rewrite

Action Properties

Rewrite URL: http://192.168.11.42/{R:1}

☒ Append query string

16. In IIS Manager, **Open** the URL Rewrite menu and Reorder the inbound and outbound rules so that the SCEP rule is at the top of the list.

17. **Move** the outbound SCEP rule to the top of the outbound list as well.



URL Rewrite

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

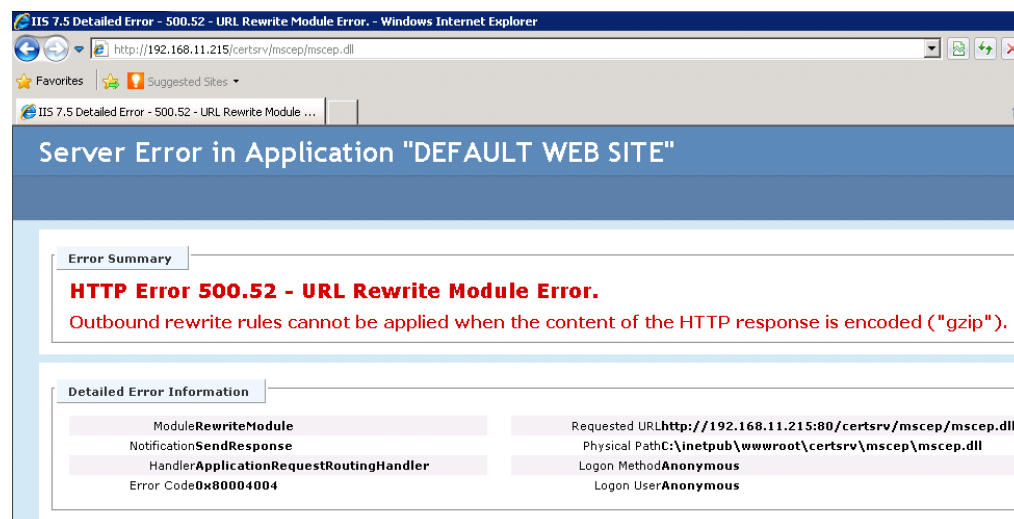
Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern	Action Type	Action URL	Stop Proce...	Entry Type
ReverseProxyInboundRule2	URL path after '/'	Matches	(certsrv/.*)	Rewrite	http://192.168.11.42/{R:1}	True	Local
ReverseProxyInboundRule1	URL path after '/'	Matches	(.*)	Rewrite	http://e7mms1.e7qa.local/{R:1}	True	Local

Outbound rules that are applied to the headers or the content of an HTTP response:

Name	Input	Match	Pattern	Action Type	Action Value	Stop Proce...	Entry T
ReverseProxyOutboundRule2	A, Form, Img	Matches	^http(s)?://192.168.11.42/(.*)	Rewrite	http{R:1}://192.168.11.215/{R:2}	False	Local
ReverseProxyOutboundRule1	A, Form, Img	Matches	^http(s)?://e7mms1.e7qa.local/(.*)	Rewrite	http{R:1}://192.168.11.215/{R:2}	False	Local

This error means that content returned is compressed and ARR is unable to modify the encoding variable. You need to manually add the **HTTP_ACCEPT_ENCODING** variable to the web.config file.



18. In the web.config file for the reverse proxy, you will need to manually add a variable specific to the SCEP URL.

19. Add bold variable as shown in web.config below:

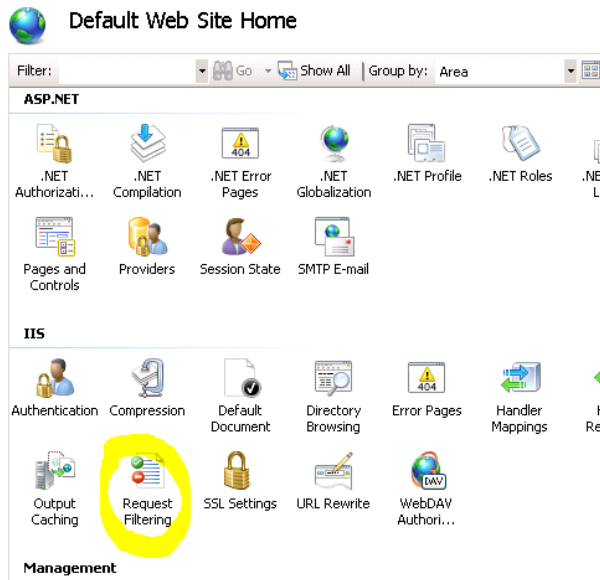
```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <rewrite>
      <outboundRules>
        <clear />
        <rule name="ReverseProxyOutboundRule2" preCondition="ResponseIsHtml1">
          <match filterByTags="A, Form, Img" pattern="^http(s)?://192.168.11.42/(.*)" />
          <conditions logicalGrouping="MatchAll" trackAllCaptures="true" />
          <action type="Rewrite" value="http{R:1}://192.168.11.215/{R:2}" />
        </rule>
      </outboundRules>
    </rewrite>
  </system.webServer>
</configuration>
```

```
<rule name="ReverseProxyOutboundRule1" preCondition="ResponselsHtml1">
  <match filterByTags="A, Form, Img" pattern="^http(s)?://e7mms1.e7qa.local/(.*)" />
  <conditions logicalGrouping="MatchAll" trackAllCaptures="true" />
  <action type="Rewrite" value="http{R:1}://192.168.11.215/{R:2}" />
</rule>
<preConditions>
  <preCondition name="ResponselsHtml1">
    <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" />
  </preCondition>
</preConditions>
</outboundRules>
<rules>
  <clear />
  <rule name="ReverseProxyInboundRule2" stopProcessing="true">
    <match url="(certsrv/.*)" />
    <conditions logicalGrouping="MatchAll" trackAllCaptures="false" />
    <action type="Rewrite" url="http://192.168.11.42/{R:1}" logRewrittenUrl="true" />
    <serverVariables>
      <set name="HTTP_ACCEPT_ENCODING" value="" />
    </serverVariables>
  </rule>
  <rule name="ReverseProxyInboundRule1" stopProcessing="true">
    <match url="(.*)" />
    <conditions logicalGrouping="MatchAll" trackAllCaptures="false" />
    <action type="Rewrite" url="http://e7mms1.e7qa.local/{R:1}" />
  </rule>
</rules>
</rewrite>
</system.webServer>
</configuration>
```

Note: You also need to add the server variable in IIS.

20. In IIS Manager, Open the URL Rewrite menu and click "View Server Variables..." on the right-side action pane.
21. Click **Add**
22. **Select** or type HTTP_ACCEPT_ENCODING
23. Click **OK**. The variable should be added as "Local".

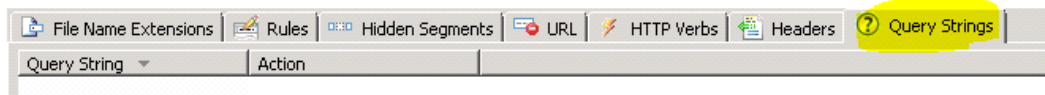
Request Filtering URL Size issue



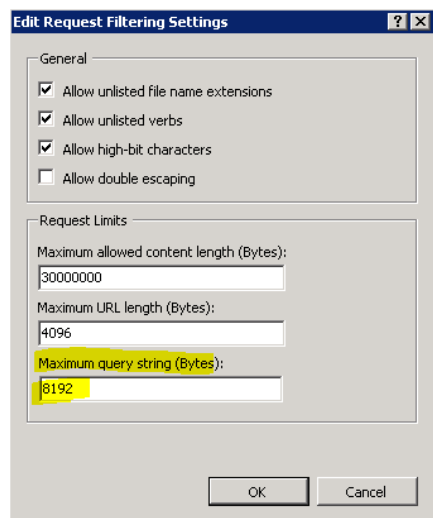
1. In IIS Manager, **Open** the “Request Filtering” menu.
2. **Select** the Query Strings tab.

Request Filtering

Use this feature to configure filtering rules.



1. Right Click the **Actions** menu
2. Select **Edit Feature Settings...**
3. Change the Maximum query string size to **8192**.
4. Click **OK** to save this setting



5. Restart IIS

4 Ports

4.1 Required network ports/connections

Connection	Port	Function
Agent -> Mobile Management Server	80 443	IIS HTTP for agent communication IIS HTTPS for agent communication (optional) Note: iOS 5 will require HTTPS communication (port 443)
Agent -> Mobile Management Server	7780	Remote Control (Windows Mobile and BlackBerry) Note: Windows Mobile and BlackBerry Remote Control will not operate correctly through a Reverse Proxy setup -- see Error! Reference source not found. and Architecture iagram .
Agent -> Apple Push Notification Service	5223	APNS Communications to Apple APNS servers
Mobile Management Server -> Apple Push Notification Service	2195 2196 5223	APNS Communications to agent via Apple APNS servers
SMP Server -> Mobile Management Server	7778	Remote Control Connection
Mobile Management Server -> SMP Server	80	IIS HTTP
Browser -> SMP Server	80	Console
Browser -> Mobile Management Server	7778	Remote Control Connection
SMP Server -> Microsoft SQL Server	Standard SQL Ports	Database

5 Certificate Requirements and Recommendations

5.1 Apple MDM/Certificates – overview and obtaining from Apple

Mobile Device Management Certificate allows the Symantec Mobile Management Server to push MDM commands through the Apple Push Notification Service to iOS devices in your environment.

Before installing Mobile Management Suite you must have an Apple Push Notification System (APNS) certificate for use in push communications to the mobile device agent. Communication via APNS requires the use of the Apple Push certificate created using the Apple iOS development tools.

In order to obtain an Apple Push Notification System (APNS) certificate you must be a member of the Apple iOS Developer Enterprise Program. This agreement allows you to create certificates that can be used for MDM services via the Apple Push Notification Service.

Note: You must contact Apple directly to join the Apple iOS Developer Enterprise Program.

For the Apple iOS Developer Enterprise Program membership you can sign up at the following:

<http://developer.apple.com/programs/ios/enterprise/>

5.1.1 Root Certificate Recommendations

If not previously installed, a Root Certificate needs to be placed into the Certificate Authority (CA).

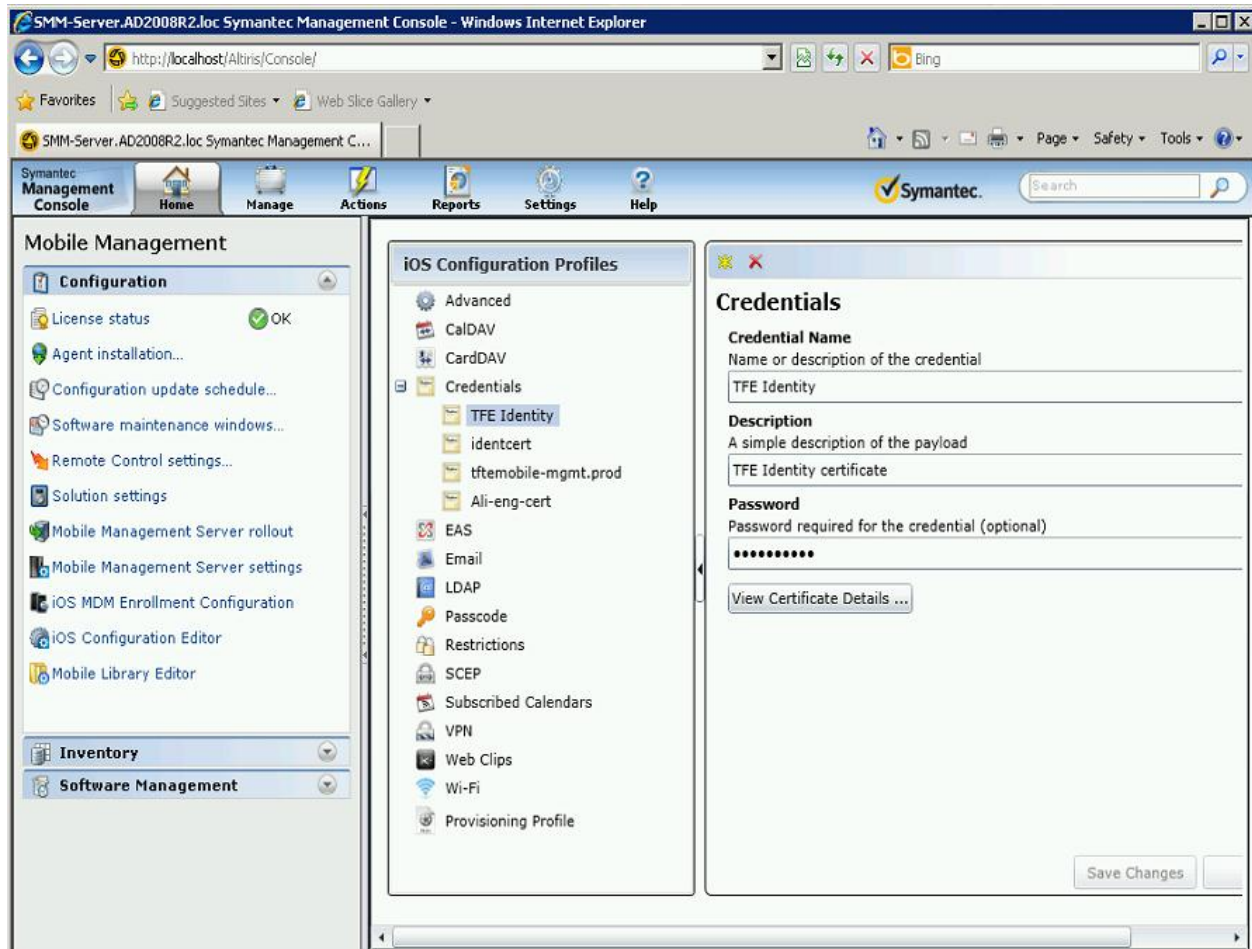
The Root Certificate must be obtained via a Commercial Authority (e.g. Verisign), or generated internally using your own Root Authority.

5.2 Using an Identity certificate for device enrollment – POC only

Production environments are recommended to use a CA infrastructure utilizing the SCEP protocol to facilitate the distribution of certificates for device enrollment and management. Detail around the configuration of this infrastructure can be found [Section 3 – Recommended Architecture](#). For POC only however there is another option that can be utilized that does not require the configuration of CA/SCEP infrastructure. An identity certificate can be configured and distributed to the device as part of the MDM enrollment process. This certificate will allow the device to properly enroll against the SMM infrastructure. It is recommended to be used for POC only, as the same identity certificate will be distributed to all enrolled devices. Though this will make the POC process easier to configure, using it in a production environment will remove the ability to individually revoke device certificates distributed through a CA/SCEP infrastructure. For POC use, you

can find an identity certificate posted on the [SymIQ EMM mobile site](#). The following is the process to install the identity certificate for use in the SMM console.

1. Download the Identity certificate and copy to the SMM server
2. In the SMM console, Open iOS Configuration Editor
3. Create a new credential profile browsing to the identity certificate file path location
4. Give this a credential name of your identity certificate with a description indicating that it is an identity certificate.
5. Input the certificate password



6. Click Save Changes
7. Open iOS MDM Enrollment Configuration
8. Under 'Cryptographic credential used for authentication' Select your identity certificate from the dropdown
9. Click Save changes

Note: You are instructing the mobile management server to use this credential for authentication when the device enrolls. In addition to the usual MDM payload, this credential containing the identity cert will be delivered to the device. Once the iOS

device has successfully enrolled, this certificate will be visible in device Settings > General > Profile > MDM Enrollment > More Details.

5.3 Apple iOS MDM agent options – internal built vs. App store version

There are two options for the agent on the Apple iOS devices.

There is a commercially available download of the Symantec agent available for download on the Apple app store. Users can search for Symantec Mobile Management and download it to the device. In many cases this agent will be adequate for deployment. As a best practice, it is recommended that you test with this version of the application after configuring your environment before using an internal built application.

Customers can also internally build/deliver/deploy a custom agent to their users mobile devices (the Apple App Store not is not required with this method). There are a couple of notable differences between these versions of the agent.

The internal built agent version of the Symantec Mobile Management Agent can be customized to incorporate customer specific logos for a personalized appearance. It can run in the background and perform actions regularly that cannot be done by an App obtained from the Apple App Store due to Apple restrictions (e.g. jailbreak detection, inventory collection, policy validation, etc.). The App from the public App store cannot typically run actively when placed in the background and will perform these types of functions less frequently.

The public App Store version of the SMM agent does not contain the 'App' tab. Applications created for use in the Mobile Library will appear in the 'Updates' tab with this version of the agent.

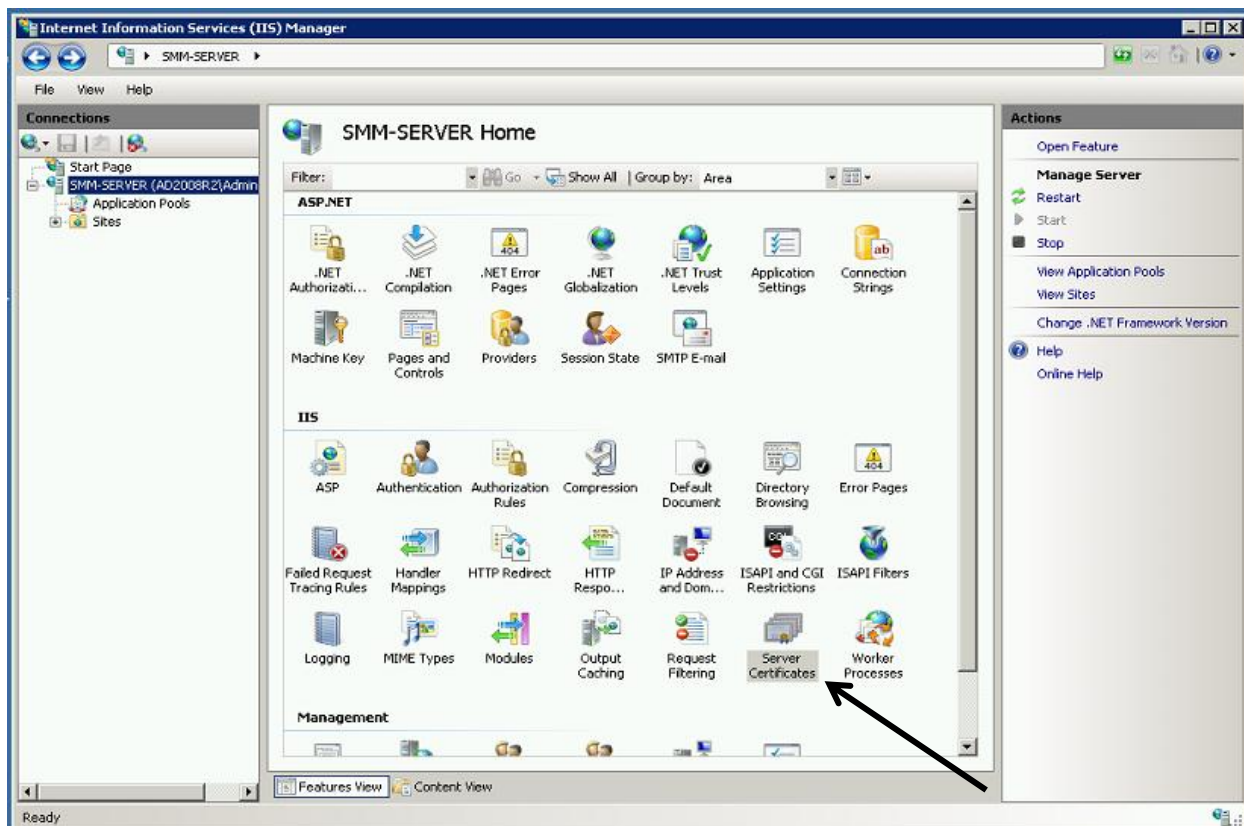
Further information for constructing an internal agent may be found in product documentation in the following location <http://www.symantec.com/docs/DOC3493>

6 Configuring SMM for SSL Communication to support iOS 5

6.1 Generating an SSL certificate request and SSL certificate

Enrolling iOS 5 devices requires the use of SSL communication between the mobile device and the SMM Site server. This configuration must be set up using a certificate issued by a trusted third party certificate authority, either an internal CA, or from a commercial CA such as Verisign. A certificate issued by a commercial third party, such as Verisign, is the recommended approach for a production environment to allow for easier setup and configuration of the trust infrastructure in your environment. You can also configure SSL communication using a certificate issued by your own internal CA. In that case you will also need to be sure that both the SMP server, as well as the SMM site server are configured with the trusted root certificate from that CA. That root certificate must also be distributed to the mobile device. Using a self-signed certificate from the SMM server alone is not supported. The following information walks through the request and configuration for instances where you are using an internal trusted third party CA. The portions shown binding the SSL cert will apply for either certificate type.

1. Open IIS
2. Highlight the SMM server
3. Double Click Server Certificates under IIS



5. Complete the Distinguished Name Properties field where the Common name used is the FQDN of the SMM server.
6. Click Next
7. Accept the default Cryptographic Service Provider Properties settings
8. Click next
9. Specify a file name for this request and browse to save file to the desktop or other storage area.
10. Click finish

Note: You will now have a text file created that contains an encoded certificate request string

11. Request an SSL certificate and Root certificate from an existing CA server

Note: This part of the process may vary slightly. If your customer has an existing CA authority server they will have a process to request the root CA and an SSL certificate similar to this. For a POC a certificate can also be requested from the following Symantec server.

<http://ali-eng-cert.altiris.com>

12. Upload or paste certificate request text from the file just created to the CA server
13. Download the DER encoded SSL certificate
14. Download the CA server root certificate by starting the certificate wizard from the CA server main page. Click the links to download the CA certificate

Note: The Root CA certificate is required when not using a certificate issued by a commercial certificate authority. The iOS device will not inherently trust your CA infrastructure and needs the root certificate to validate the SSL certificate communication.

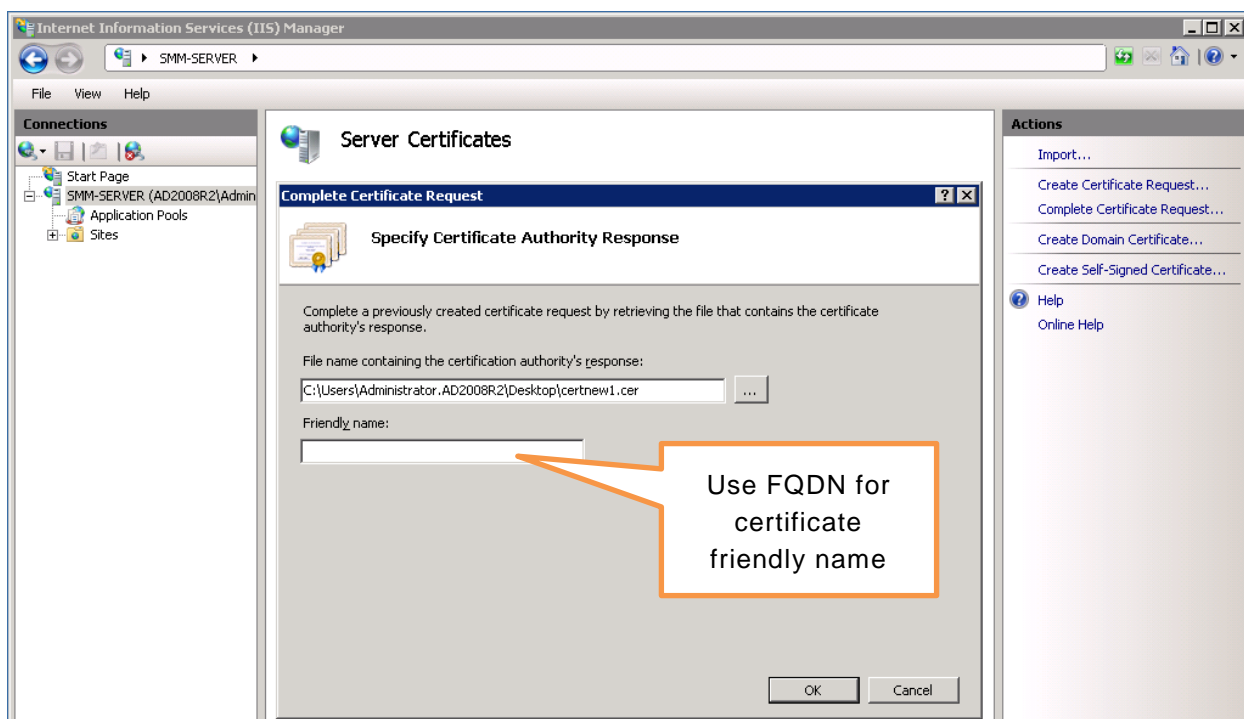
6.2 Installing your server certificates

1. Open an MMC certificates snap in connecting to the “Computer account”, local computer.
2. Import the CA root certificate to the Trusted Root Certification Authorities store.
3. Right click the SSL certificate
4. Select ‘Install Certificate’ to open the Certificate Import Wizard
5. Click Next
6. Accept the default to “Automatically select the certificate store.....”, Click Next
7. Click Finish

Note: Certificate should now be installed in the Personal Certificates store, you may need to refresh the view.

6.3 Configuring IIS to use your SSL certificate

1. Open IIS, browse to Server certificates as previous
2. Select complete certificate request on the right hand side
3. Browse to SSL certificate file location
4. Add certificate friendly name, use FQDN of your server for easy identification



5. Open the Default web site > Edit bindings
6. Edit https, port 443 and bind the new SSL cert to port 443 by selecting the Friendly name of your cert in the SSL certificate dropdown
7. Restart IIS

6.4 Configuring SSL communication in the SMM console

1. Open the SMP console, navigate to Mobile Management Configuration
2. Select Mobile Management Server settings in the left hand side
3. Under Site Server Settings, highlight the SMM site server, click the Edit pencil
4. Be sure that the Override server connection info is NOT selected

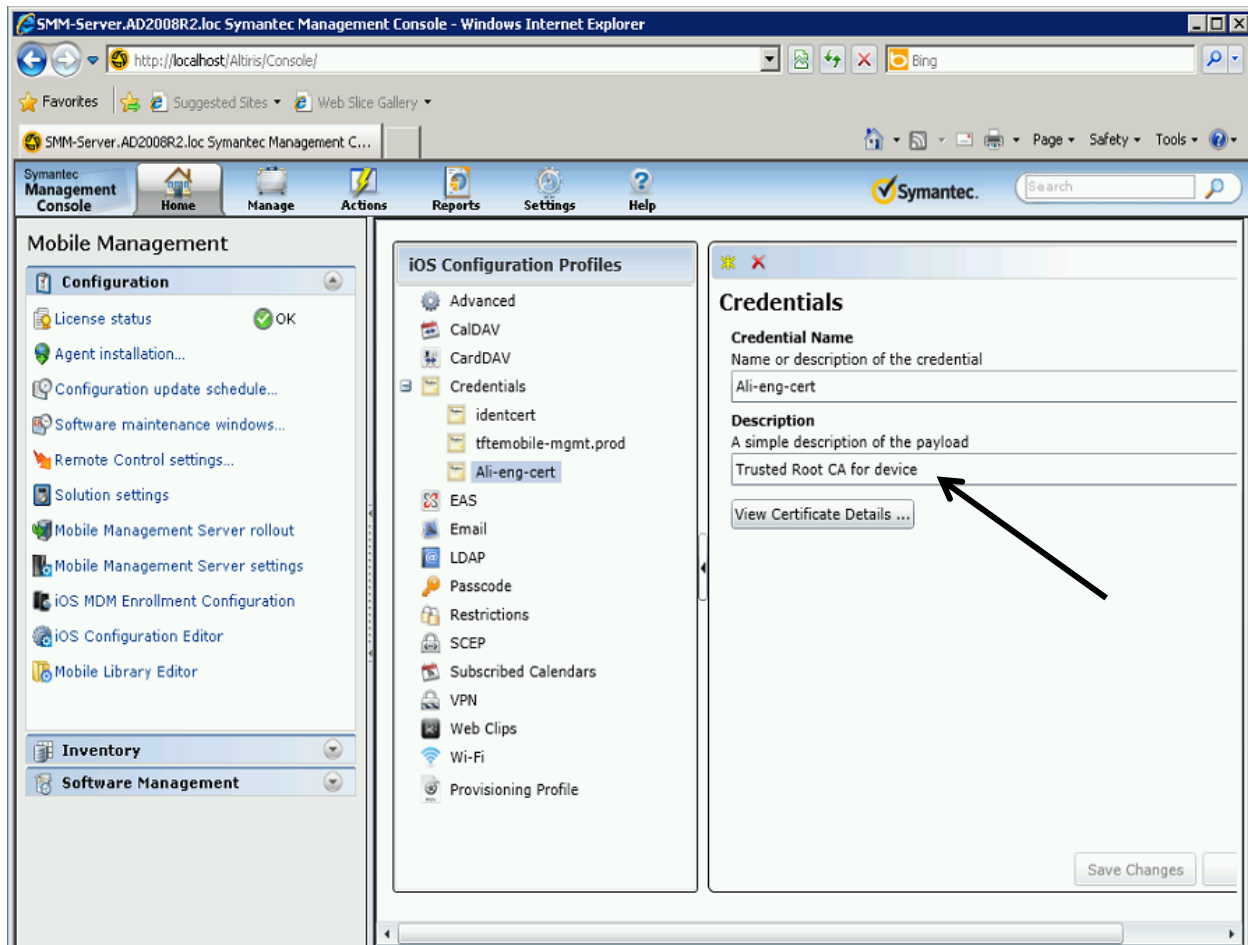
Note: This is the connection information for device communication with the SMM server. This will need to be using https and the FQDN of the server for use with iOS 5

5. Click Save changes
6. Open Services and Restart the Symantec Mobile Management Service Agent if changes have been made

6.5 Creating the Credential payload for the root CA

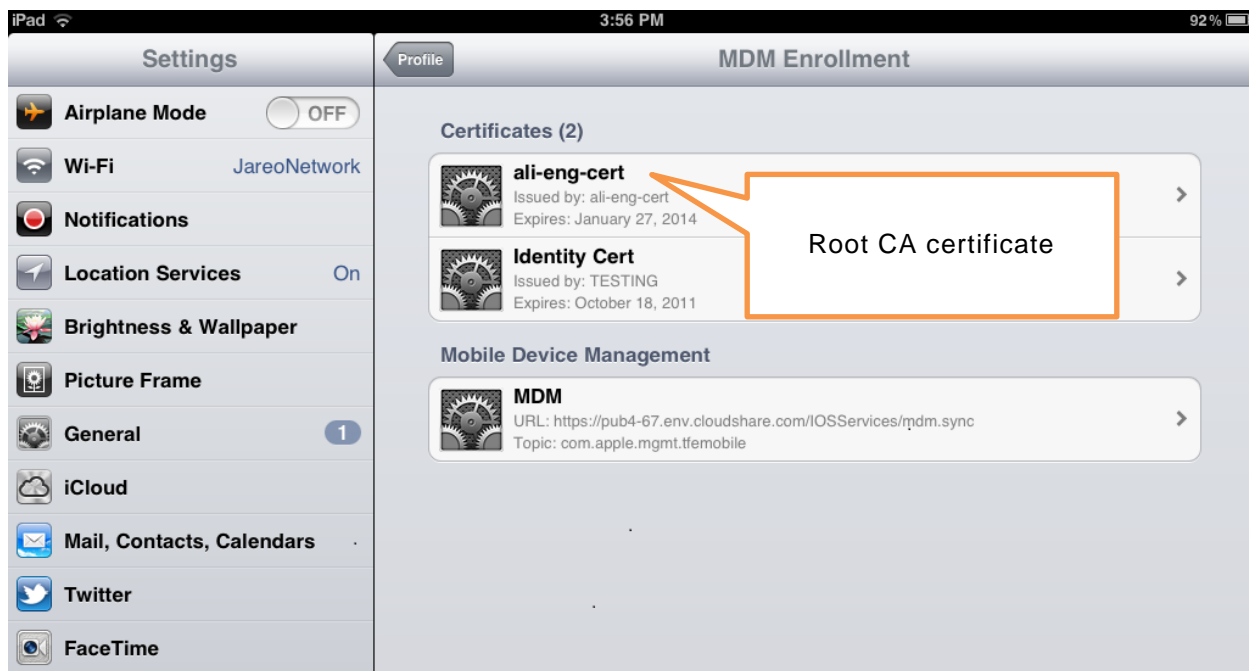
If you are using a self-signed SSL certificate you must also configure a payload which will deliver your server's root CA to the device. The iOS device will not inherently trust your CA. This step is not required when using a commercial trusted third party root certificate such as one from Verisign. The iOS device will already trust this authority. This process is completed by establishing a credential payload that is distributed to the device upon enrollment. You can create this payload as follows:

10. In the SMM console, Open iOS Configuration Editor
11. Create a new credential profile browsing to the root certificate file path location
12. Give this a credential name of your root certificate with a description indicating that it is a trusted root certificate.



13. Click Save Changes
14. Open iOS MDM Enrollment Configuration
15. Under 'Additional Configuration Profiles to include' Click the yellow asterisk to add a new configuration profile
16. Select the new credential payload you have just created.

Note: You are instructing the mobile management server to include this credential when the device enrolls. In addition to the usual MDM payload, this credential containing the root CA will be delivered to the device. Once the iOS device has successfully enrolled, this certificate will be visible in device Settings > General > Profile > MDM Enrollment > More Details.



17. Save Changes

7 How to check the prerequisite environment

7.1 Certificates (are responding as required)

SSL Communication

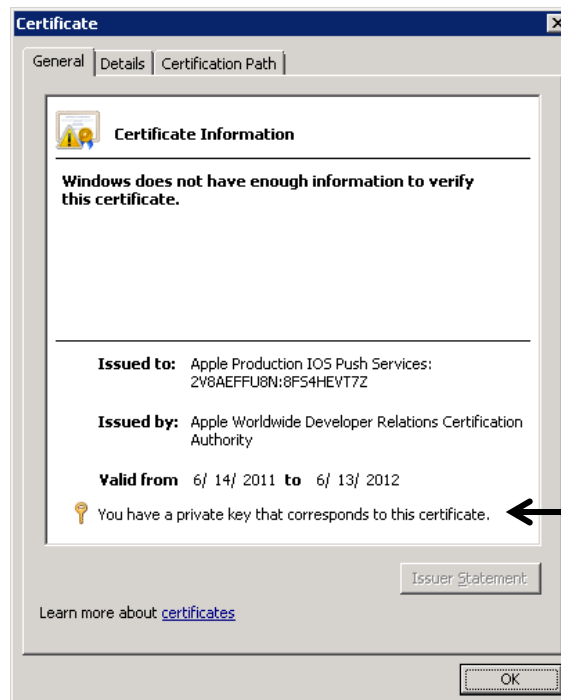
- Go to the default web page using HTTPS and the FQDN

Mobile Device Communication

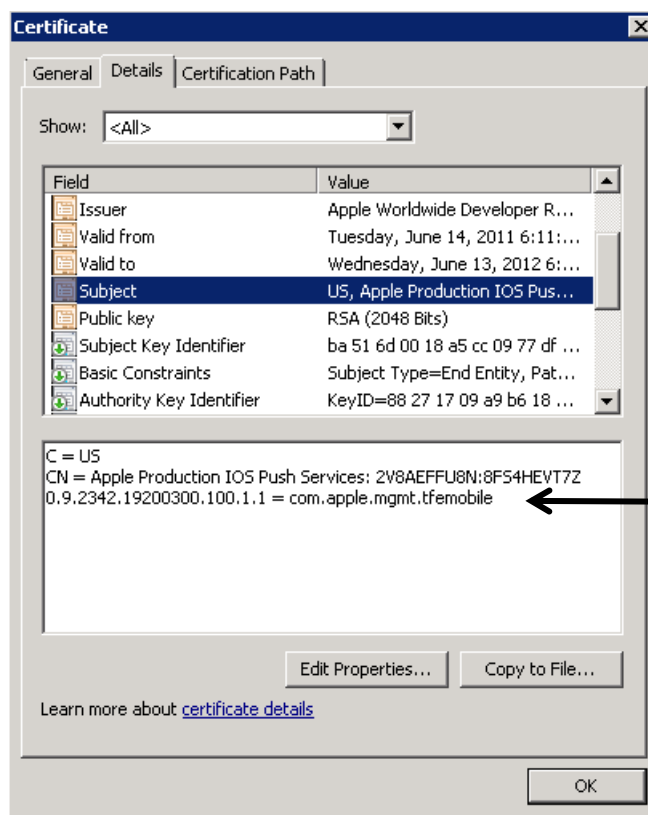
- Via Safari connect to the default webpage using HTTPS and the FQDN. If a non-VeriSign or non-Apple trusted certificate is being used then this will give an error message. Apple will not trust a self-signed certificate.

APNS certificate

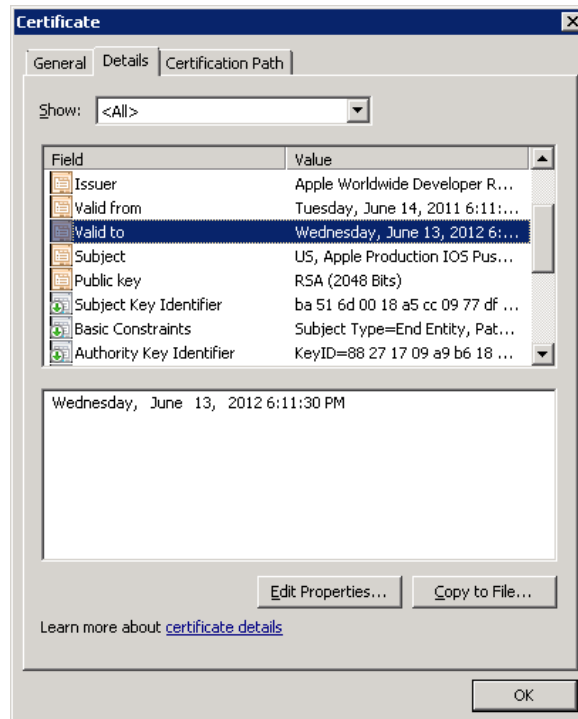
- Ensure the private key is part of the certificate. In Windows after the certificate is installed into the SMM server look for a 'Key' in the right top part of the certificate icon and a message that says that you have a private key that corresponds to this certificate



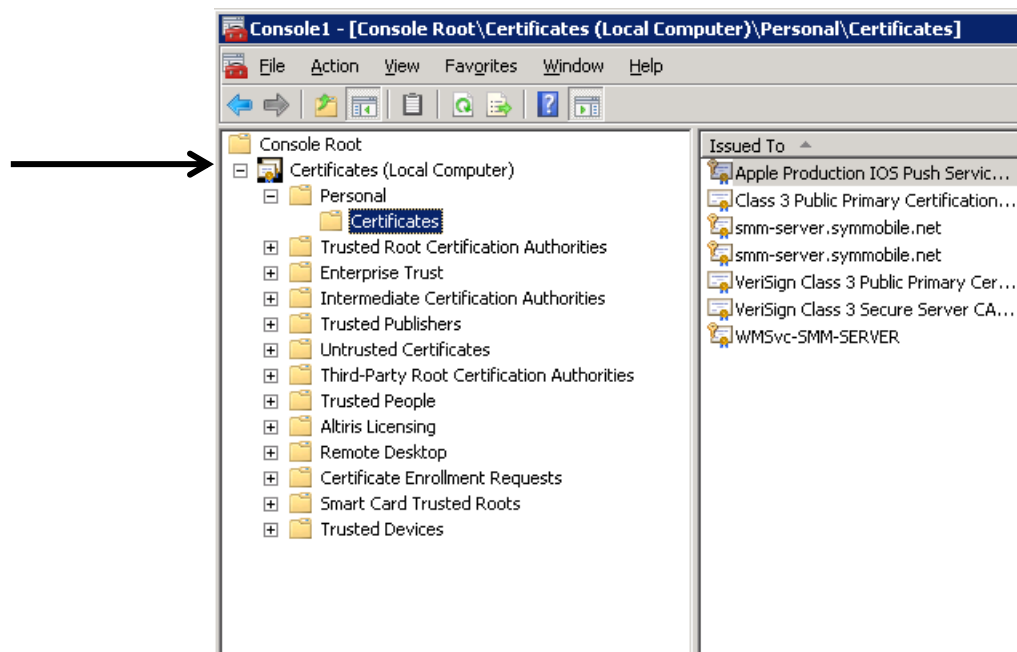
- In the subject part of the certificate the CN= will contain com.apple.mgmt – anything after this is specified by the customer when the APNS certificate is created. If the com.apple.mgmt is not specified correctly then MDM management will fail.



- Check the expiration date of the APNS certificate (note that developer certificates only last for three months).



- Ensure the certificate has been added to the Local Computer Account section of the Microsoft Management Console (MMC) Certificate snap-in and not the User Account section.



7.2 Port Check (before SMM product installation)

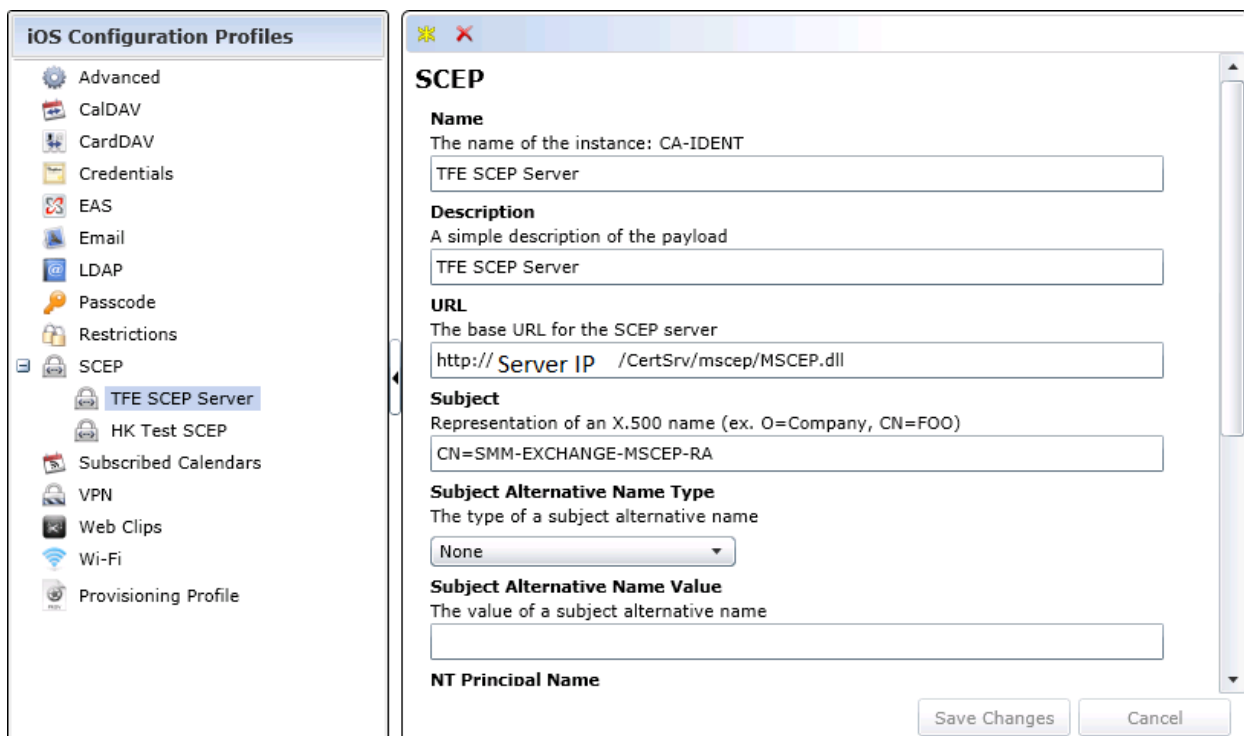
Check the following ports are responding before the SMM product installation.

- Port 2195, 2196 (from the SMM site server). Use telnet to test these ports outbound to the following:
 - telnet gateway.sandbox.push.apple.com 2195
 - telnet gateway.sandbox.push.apple.com 2196
- Ensure that the customer is 100% cellular, or if not, that port 5223 (from the Mobile Device) is enabled for outbound communication from the WiFi network. Port 5223 requires a continuous connection.

8 Common Configuration Errors

The following are areas are commonly found configuration mistakes:

- The Standalone version of SCEP is being used in conjunction with the CA on a single server. The CA and SCEP services should be on their own servers.
- The SCEP server in the DMZ has been installed into a separate Microsoft Domain than the CA, SMP and SMM site server, thus causing certificate request and name resolution issues – [See section 3 – Recommended Architecture](#)
- All Mobile Management Suite product components (SMP, SMM Site Server, CA and SCEP service) have been installed onto a single server, rather than separate servers - [See section 3 Recommended Architecture](#)
- When creating the SCEP payload that goes down to the mobile device required fields are left blank, or are not correctly completed.



iOS Configuration Profiles

- Advanced
- CalDAV
- CardDAV
- Credentials
- EAS
- Email
- LDAP
- Passcode
- Restrictions
- SCEP**
 - TFE SCEP Server**
 - HK Test SCEP
- Subscribed Calendars
- VPN
- Web Clips
- Wi-Fi
- Provisioning Profile

SCEP

Name
The name of the instance: CA-IDENT
TFE SCEP Server

Description
A simple description of the payload
TFE SCEP Server

URL
The base URL for the SCEP server
http://Server IP /CertSrv/mscep/MSCEP.dll

Subject
Representation of an X.500 name (ex. O=Company, CN=FOO)
CN=SMM-EXCHANGE-MSCEP-RA

Subject Alternative Name Type
The type of a subject alternative name
None

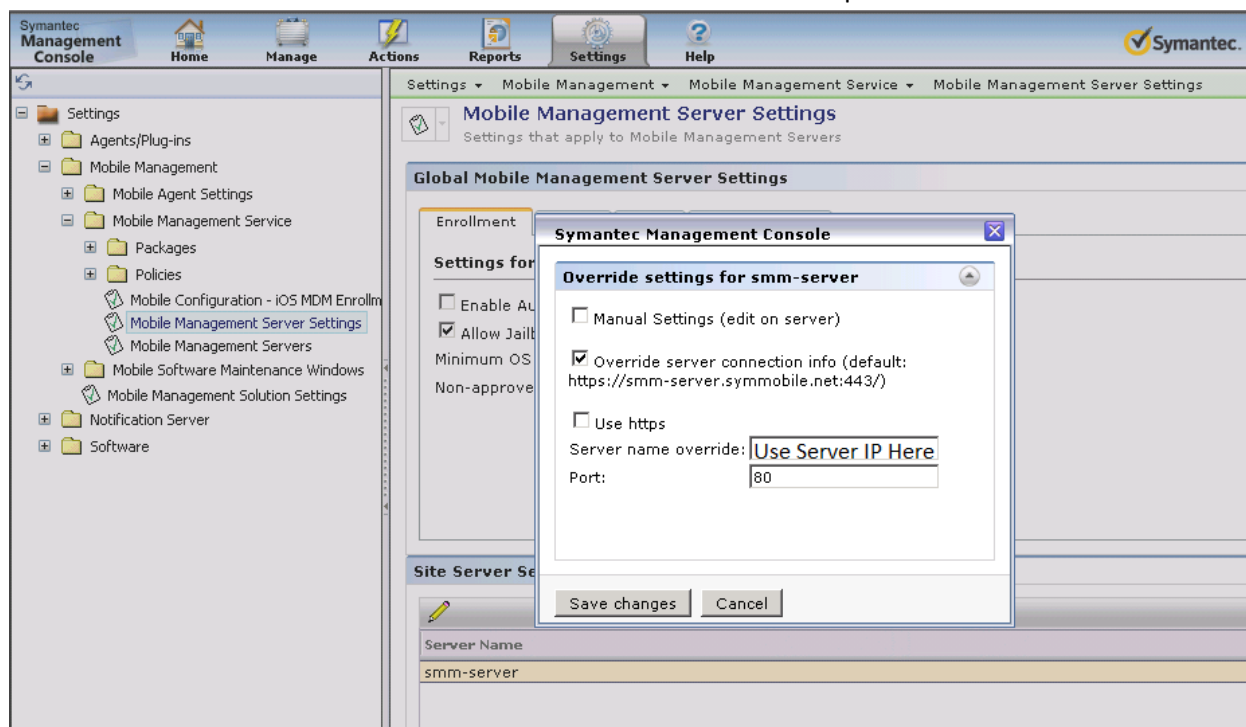
Subject Alternative Name Value
The value of a subject alternative name

NT Principal Name

Save Changes Cancel

- Under the Mobile Management Server Settings APNS configuration tab on the SMP server, the 'Use Development APNS' has not been ticked on if the APNS certificate is a development certificate (rather than a production certificate). And vice versa if a production certificate is being used instead of a development certificate.

- Under the Mobile Configuration – iOS MDM Enrollment configuration page on the SMP server, the 'Use Development APNS Server' has not been ticked on if the APNS certificate is a development certificate (rather than a production certificate). And vice versa if a production certificate is being used instead of a development certificate.
- Under the Mobile Management Server Settings configuration page on the SMP server, the 'Override server connection info' is not ticked on and completed



The device will not be able to login without this. If this is occurring you will typically see the following error dialog:

