SCMDM 2008. Часть III. Установка ролей SCMDM.

Продолжая тему System Center Mobile Device Manager 2008, хочу рассказать о том, как именно происходит установка ролей SCMDM на серверы. Описываемые в этой части действия, предполагают, что читатель уже знает, что это за продукт и о его особенностях – если нет, то рекомендую предварительно прочитать первую статью из цикла. А если, планируется повторить все, о чем здесь пойдет речь, то дополнительно необходимо пройти шаги по подготовке к внедрению, описанные во второй части, т.к. без них ни одна роль MDM не может быть установлена.

Сразу хочу предупредить – все, о чем буду рассказывать, опять будет проецироваться на некую компанию «Компания», начавшую внедрять SCMDM еще в прошлой статье, и, поэтому, все имена серверов и экземпляров (instance) приведены в соответствие со схемой, продемонстрированной там же, и оговорками, приведенными по тексту.

При внедрении MDM существует правило, что роль Gateway Server устанавливается последней, но также есть неофициальная рекомендация, что роль Enrollment Server должна быть установлена первой, поэтому, не отклоняясь от рекомендаций, предлагаю следующий порядок установки:

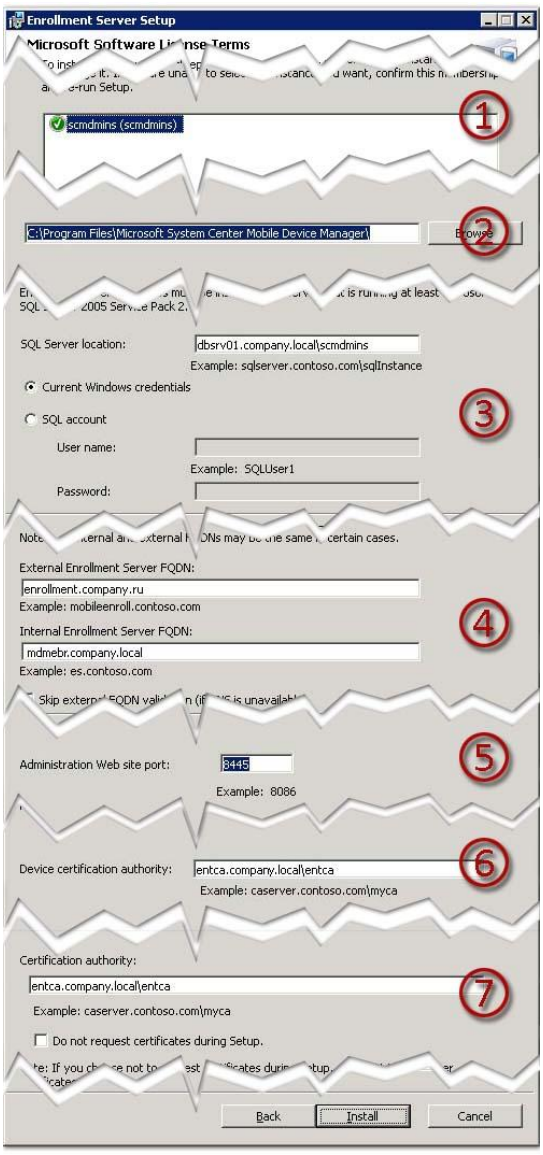
1. Установка Enrollment Server
2. Установка Device Management Server
3. Установка инструментов администратора MDM на его рабочую станцию
4. Установка Gateway Server

В общем, «Поехали!» (С)…

Установка MDM Enrollment Server.

Роль Enrollment Server предназначена для первоначального подключения устройства к MDM для получения сертификата на устройство и базовых настроек. Для выполнения установки этой роли, администратор должен заранее спланировать следующее:

- Имя экземпляра MDM, для которого производится установка
- Имя сервера и экземпляра MS SQL Server, на котором будет размещаться рабочая база данных MDM
- Внешнее и внутренне имя Enrollment Server, по которым устройства будут обращаться к нему
- Порт, выделенный для управления Enrollment Server
- Имя сервера и экземпляра Certification Authority, который будет отвечать за выпуск сертификатов для подключаемых устройств и серверов MDM



Процесс установки происходит следующим образом:

После того, как администратор выбрал установку Enrollment Server, запускается стандартный помощник. После приветствия и принятия стандартного соглашения, администратору необходимо выбрать экземпляр MDM, для которого устанавливается данная роль (**1**). После этого необходимо указать путь для установки (**2**). Далее будет задан вопрос о том, какой SQL Server будет использоваться для хранения базы (**3**). Также на этом шаге указывается учетная запись, которая будет использоваться для подключения к SQL Server, поэтому лучше всего заранее создать отдельную сервисную учетную запись. На следующем шаге необходимо указать внешнее и внутреннее полное доменное имя (FQDN) Enrollment Server (**4**). В случае, если вы планируете установить несколько Enrollment Server, то вам необходимо указать имя, используемое балансировщиком. После того, как имена были указаны, помощник проверит их правильность. Если сервер не имеет подключения к сети Интернет, то лучше поставить галочку «**Skip external FQDN validation**», чтобы проверка внешнего имени не проводилась. Далее необходимо указать порт, по которому будет происходить управление Enrollment Server (**5**). Здесь можно указать любой порт, за исключением 443-го, т.к. он используется устройствами для подключения. На следующих двух шагах (**6**, **7**) нужно указать имя центра сертификации, который будет использоваться для выпуска сертификатов устройств и сертификата Enrollment Server. При этом можно указать, чтобы в момент установки сертификат сервера не запрашивался («**Do not request certificates during Setup**»), а выпустить и установить его позже вручную. Еще хочу обратить внимание, что выпустить необходимо два сертификата – для внутреннего имени и для внешнего. После этого нужно нажать кнопку «**Install**», дождаться окончания процесса и появится сообщение, что роль Enrollment Server успешно установлена.

Установка MDM Device Management Server.

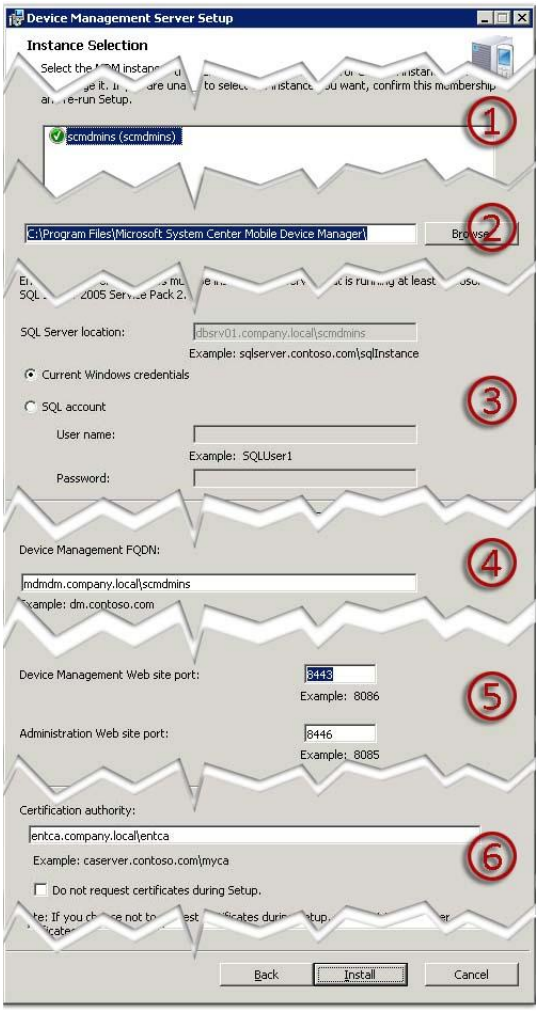
Роль Device Management предназначена для управления мобильными устройствами. Происходит это так – любые действия, которые должны быть совершены с устройством, переводятся в формат команд OMA DM (Open Mobile Alliance Device Management), после чего пересылаются с Device Management Server на устройство через Gateway Server. Именно на DM

Server происходит интерпретация групповых политик и команд на распространение ПО. Для выполнения установки необходимы следующие сведения:

- Имя экземпляра MDM, для которого производится установка
- Имя сервера и экземпляра MS SQL Server, на котором будет размещаться рабочая база данных MDM
- Полное доменное имя Device Management Server во внутренней зоне DNS
- Порт, выделенный для работы мобильных устройств через Gateway Server
- Порт, выделенный для управления Enrollment Server
- Имя сервера и экземпляра Certification Authority, который будет отвечать за выпуск сертификатов для серверов MDM

Кроме этого, на сервере DM Server должен быть установлен WSUS версии не ниже 3.0 с Service Pack 1, который используется для распространения ПО на устройства.

Процесс установки происходит следующим образом:



Установка DM Server выполняется из общего меню установки SCMDM 2008. В целом она очень похожа на установку Enrollment Server – после запуска помощника появится приветствие, после которого необходимо принять лицензионное соглашение, выбрать для какого экземпляра MDM происходит установка (**1**), указать путь для установки программы (**2**), выбрать сервер с MS SQL, на котором размещается база данных MDM, соответствующий экземпляр и учетную запись, с которой будет осуществляться работа (**3**). На следующем шаге необходимо указать полное доменное имя (FQDN) для сервера (**4**). Далее нужно указать какие порты будут использоваться при работе DM Server – один для работы с устройствами (Device Management) и один для управления сервером (Administration) (**5**). После этого необходимо указать имя сервера и копии центра сертификации (Certification Authority), который будет использован для выпуска сертификата сервера (**6**). Так же, как и при установке Enrollment Server, можно указать, чтобы в момент установки сертификат сервера не запрашивался («**Do not request certificates during Setup**»), а выпустить и установить его позже вручную. После этого нужно нажать кнопку «**Install**» и дождаться окончания процесса установки.

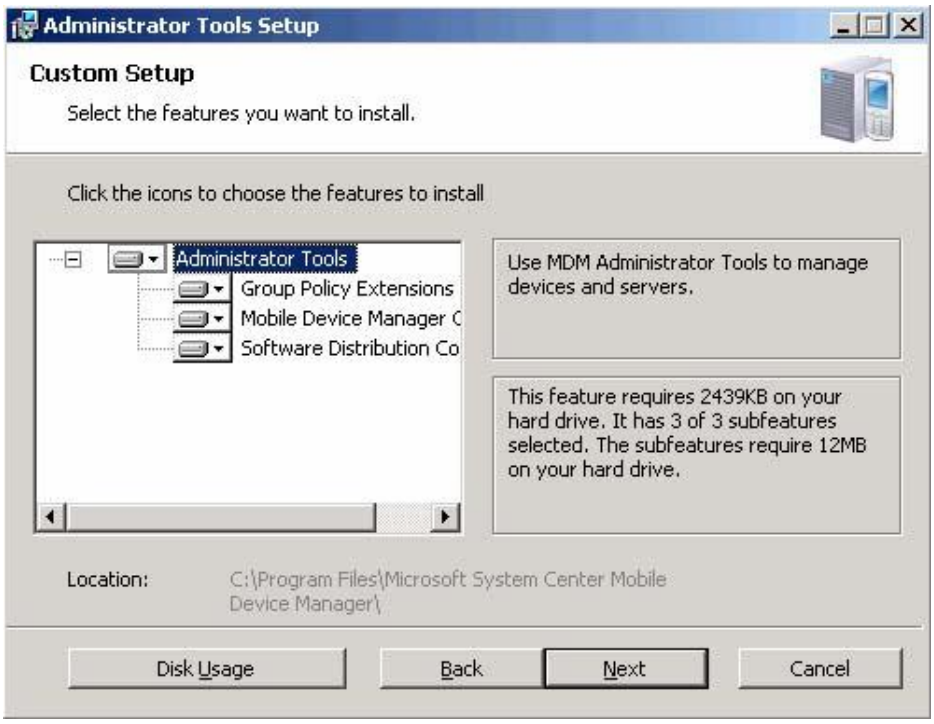
Установка инструментов администратора MDM

Установка инструментов администратора выполняется на его рабочей станции, либо на станции, с которой будет осуществляться управление. Для успешной установки на станции должны уже быть установлены:

- .Net версии не ниже 2.0 с SP1
- MMC версии 3.0
- Консоль управления WSUS 3.0 SP1
- PowerShell 1.0
- Консоль GPMC

Инструментарий включает в себя следующие компоненты:

- **Group Policy Extensions** – представляют из себя дополнительные шаблоны ADM, предоставляющие расширения для управления мобильными устройствами.
- **Mobile Device Manager Console** – основная консоль для работы с SCMDM
- **Software Distribution Console** – консоль по управлению распространением ПО



Подробно описывать установку инструментария не буду, т.к. никаких сложностей она не представляет. Скажу лишь, что компоненты могут быть разнесены по различным станциям и серверам, в том числе возможна установка и на сервера MDM, за исключением Group Policy

Extensions – т.к. консоль GPMC установку на Windows XP x64 / Server 2003 x64 не поддерживает.

Установка MDM Gateway Server.

Роль Gateway Server является шлюзом для устройств, подключающихся к внутренней сети предприятия. После выполнения инициализации устройства, оно получает от Enrollment Server данные, необходимые для полноценного подключения. Среди этих данных находится, в том числе, и информация о Gateway Server.

Схема работы устройства с сетью выглядит следующим образом:

- Устройство, используя имеющуюся информацию о Gateway Server, производит подключение к нему с использованием Mobile VPN.
- После подключения, устройству выделяется адрес из имеющегося в распоряжении Gateway Server пула частных адресов. Этот пул создается после установки Gateway Server, во время его настройки. Диапазон используемых адресов не должен совпадать с теми, которые имеются во внутренней сети.
- При обращении к любому серверу, находящемуся во внутренней сети, устройство использует Gateway Server в качестве шлюза по умолчанию. При необходимости можно настроить пересылку трафика на другой шлюз.

Установку Gateway Server условно можно разделить на два этапа – подготовительный и, собственно, сама установка.

На подготовительном этапе выполняются следующие действия:

Необходимо выпустить сертификат для сервера. Это можно сделать двумя способами – либо используя Web-консоль центра сертификации, либо создав файл с запросом на выпуск сертификата, выпустив его на введенном в домен сервере и установив на шлюз (эти действия выполняются при помощи утилиты ***certreq.exe***). Рассмотрим оба способа:

1. Для выпуска сертификата через Web-консоль, необходимо в IE зайти на страницу **https://<FQDN центра сертификации>/certsrv** (в случае с «Компанией» это https://entca.company.local/certsrv), перейти по ссылке «**Request a certificate**», выбрать «**advanced certificate request**» и «**Create and submit a request to this CA**». В открывшейся форме необходимо выбрать шаблон «**SCMDMWebServer (<имя экземпляра MDM>)**» («**SCMDMWebServer (scmdmins)**» в случае с «Компанией»), указать полное внутреннее доменное имя (FQDN) Gateway Server в поле «**Name**», отметить пункт «**Store certificate in the local computer certificate store**» и нажать кнопку «**Submit**». После чего на открывшейся странице нажать «**Install this certificate**». На все задаваемые вопросы предлагаю соглашаться, т.к. в противном случае выпуск и установка сертификата не произойдут.
   Хочу предупредить – для того, чтобы этот способ выпуска был доступен, необходимо, чтобы была установлена Web-консоль на сервере центра сертификации (при установке Certification Authority она является опциональной).

2. Для выпуска сертификата при помощи утилиты ***certreq.exe*** необходимо создать тестовый файл со следующим содержанием:

   [NewRequest]
   Subject = "CN=<полное доменное имя Gateway Server>"
   MachineKeySet = True
   KeySpec = 1

   В качестве доменного имени указывается имя, для которого создана запись типа A во внутренней зоне на сервере DNS (на примере «Компании» эта стока будет выглядеть так – **Subject = "CN=mdmgw.company.local"**). Microsoft настоятельно рекомендуется набрать все руками в Notepad без копи-паста, чтобы избежать проблем с используемыми кодировками и служебными символами. После того, как текст был набран, необходимо сохранить его в файл с расширением .inf (например, **GatewayCertReq.inf**). Далее в командной строке нужно выполнить:

   certreq –new GatewayCertReq.inf GatewayCertReq.txt

   В результате будет создан файл **GatewayCertReq.txt**, содержащий запрос на выпуск сертификата. Этот файл необходимо перенести на сервер, входящий в домен, и на нем выполнить команду:

   certreq –submit –attrib «CertificateTemplate:SCMDMWebServer (<имя экземпляра MDM>)» GatewayCertReq.txt GatewayCertReq.cer

   При выполнении этой команды может появиться окно, в котором необходимо указать используемый для выпуска центр сертификации. По завершении, в том же каталоге будет создан файл сертификата GatewayCertReq.cer, который необходимо перенести на Gateway Server и выполнить его импорт в хранилище сертификатов командой:

   certreq –accept GatewayCertReq.cer

Хочу обратить внимание, что выпускаемый сертификат является сертификатом машины, и поэтому, если будете выполнять проверку, его нужно искать в local computer.

После того, как был выпущен сертификат для Gateway Server, необходимо выполнить импорт корневого сертификата. Это так же можно проделать двумя способами:

1. С Gateway Server через Web-консоль зайти на страницу центра сертификации, перейти по ссылке «**Download a CA certificate, certificate chain or CRL**» и выбрать «**Download CA certificate**». Сертификат необходимо сохранить локально, но не устанавливать, т.к. иначе он попадет не в то хранилище. После сохранения, необходимо открыть консоль MMC «**Certificates**» для «**Local computer**», развернуть ветку «**Trusted Root Certification Authorities**», вызвать контекстное меню на пункте «**Certificates**» и выполнить «**All Tasks**» -> «**Import**». Далее необходимо указать путь до файла с сертификатом, в

качестве места хранения выбрать «**Place all certificates in the following store**» -> «**Trusted Root Certification Authorities**», и нажать кнопку «**Finish**».
При использовании этого метода действует то же ограничение, что и при выпуске сертификата Gateway Server через Web-консоль.

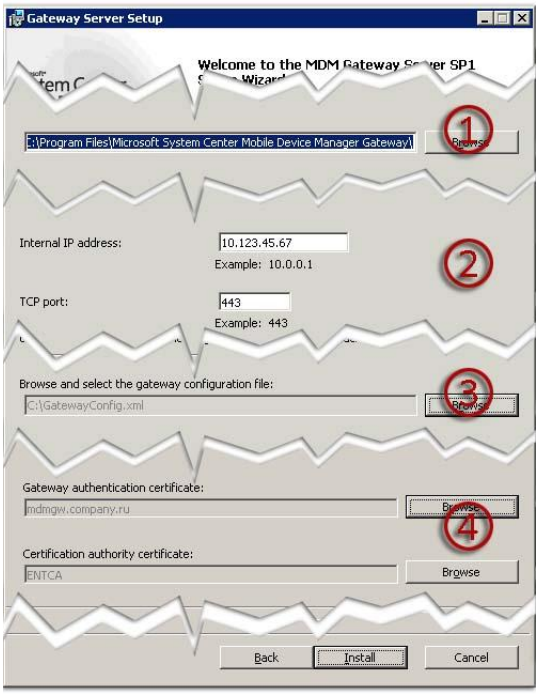
2. Зайти на сервер центра сертификации, открыть консоль MMC «**Certification Authority**», вызвать контекстное меню на имени центра и выбрать «**Properties**». Далее необходимо перейти на вкладку «**General**», выбрать корневой сертификат для просмотра («**View Certificate**»), и на вкладке «**Details**» выбрать «**Copy to File**» - запуститься помощник экспорта сертификатов. При прохождении шагов необходимо выбрать формат «**DER encoded binary X.509(.CER)**» для файла сертификата, указать его имя и путь, по которому он будет сохранен. После сохранения, файл сертификата нужно перенести на Gateway Server и выполнить его импорт аналогично импорту в предыдущем варианте.

После того, как сертификаты доставлены на Gateway Server и экспортированы в соответствующие хранилища, необходимо создать конфигурационный файл для Gateway Server. Для этого необходимо на любой из введенных в домен машин MDM (Enrollment Server, DM Server, станция администратора MDM) в консоли PowerShell выполнить команду:

Export-MDMGatewayConfig

В результате будет создан файл **GatewayConfig.xml**, который необходимо доставить на Gateway Server. На этом подготовительная стадия заканчивается, можно переходить к установке роли.

Сама установка Gateway Server после Enrollment и DM Server выглядит достаточно стандартной – запускается из общего меню, далее следуют приветствие и лицензионное соглашение, а так же предложение указать путь для установки (**1**). После этого следует шаг, на котором необходимо указать внутренний IP-адрес Gateway Server и порт, по которому будет происходить общение с DM Server (**2**). Далее необходимо указать путь к файлу с конфигурацией, созданному на подготовительном этапе (**3**). На следующем шаге выбираются сертификаты для самого сервера и корневой сертификат, которые так же были созданы и экспортированы на этапе подготовки (**4**). После этого необходимо нажать кнопку «**Install**» и дождаться окончания процесса установки.

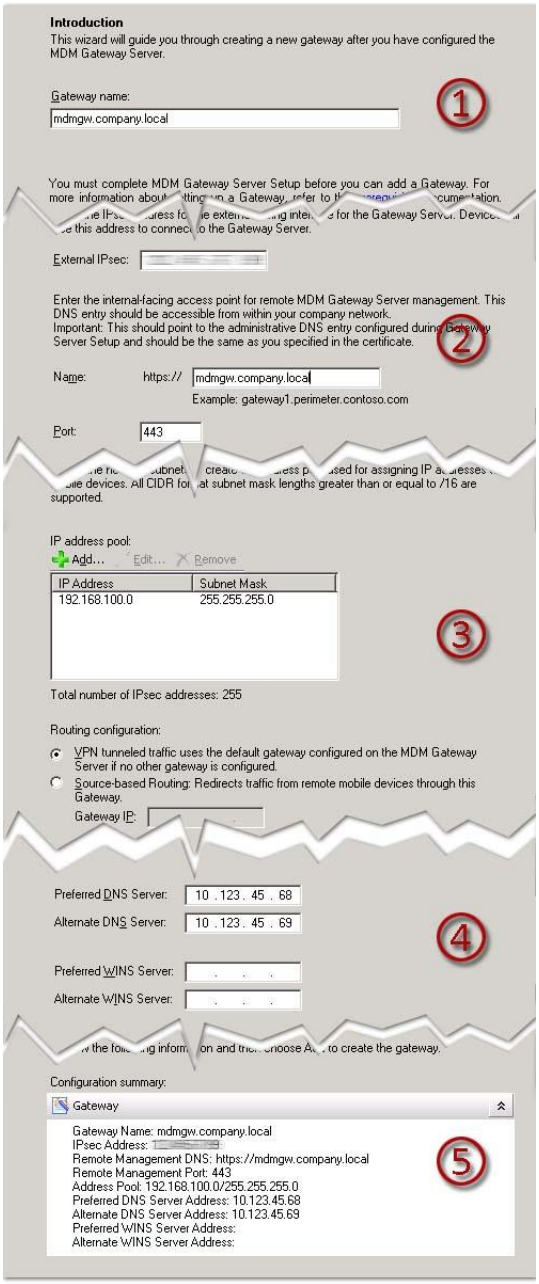


Далее, необходимо известить MDM о том, что появился Gateway Server. Делается это следующей командой с любой доменной машины MDM в консоли PowerShell:

Set-EnrollmentConfig –GatewayURI <ссылка на внешний интерфейс MDM>

В качестве ссылки может быть использован как IP-адрес, так и внешнее FQDN имя Gateway Server. Но Microsoft не рекомендует использовать IP-адрес в том случае, если установлен только один Gateway – если произойдет его смена, то будет необходима очистка уже используемых устройств и их новая инициализации.

Далее необходимо выполнить первоначальную настройку Gateway Server. Выполняется она с рабочей станции администратора MDM при помощи консоли **Mobile Device Manager Console**.



После открытия консоли, необходимо выбрать в ее левой части «**Gateway Management**», а в меню «**Action**» действие «**Add MDM Gateway Wizard**». Запуститься помощник настройки шлюза, в ходе выполнения которого необходимо указать имя сервера, под котором он будет отображаться в консоли (**1**). Далее нужно ввести IP-адрес внешнего сетевого интерфейса, полное внутреннее доменное имя сервера и порт, по которому будет происходить общение с DM Server (**2**). Порт должен быть тем же, что был указан при установке роли Gateway Server на шаге 2. После этого необходимо создать пул адресов, из которого будет происходить выдача адресов подключаемым устройствам (**3**). Этот пул не должен пересекаться с имеющимися на предприятии подсетями. Также на этом шаге необходимо указать, будет ли Gateway являться конечным шлюзом для устройств, либо будет настроена пересылка получаемого IPSec-трафика на другой шлюз. Далее настраиваются адреса DNS и WINS серверов, которые будут использоваться устройствами в процессе разрешения имен (**4**). Наконец, будет выведена сводная информация по настройкам Gateway Server (**5**) и предложено закончить конфигурирование.

И последнее, что необходимо выполнить при настройке Gateway Server, это указать маршруты к подсети, которая используется устройствами – об этом я писал в предыдущей статье, предлагая выполнять это заранее, еще на стадии подготовки сетевого оборудования. На оборудовании тех сегментов, в которых размещены сервисы, используемые мобильными устройствами, необходимо указать маршрут до подсети мобильных устройств с использованием Gateway Server в качестве шлюза – в случае с

«Компанией» нужно прописать маршрут к подсети 192.168.100.0/24 через шлюз 10.123.45.67. Если это действие не будет выполнено, то сервисы не будут доступны устройствам.

На этом установка ролей SCMDM окончена – «Компания» может начинать опытную эксплуатацию.

Напоследок

Ну и напоследок несколько советов тем, что все-таки попробует внедрить SCMDM самостоятельно. Обычно такие советы дают где-то в самом начале, но мне это кажется не всегда разумным, т.к. люди должны сначала представить, что их ожидает, а уже потом выслушивать наставления…

После того, как все роли установлены, можно и нужно воспользоваться таким инструментом, входящим в состав Resource Kit Tools, как Best Practice Analyzer (BPA). Этот инструмент позволяет проверить правильность выполненной установки и может дать советы по исправлению недочетов, если таковые присутствуют. Однако, его можно использовать и на стадии подготовки к внедрению – в этом случае он поможет проверить готовность инфраструктуры и соответствие подготовленных серверов требованиям SCMDM.

При устойчивой проблеме с подключениями устройств, первое, что рекомендую проверить, это правильность сертификатов на серверах MDM через консоль IIS. Личный опыт показывает, что более половины случаев связаны именно с ними.

Еще раз советую обратить внимание, на то, что документация по продукту страдает несостыковками. Так, файлы помощи, которые идут вместе с продуктом, общий файл помощи, доступный на TechNet и библиотека TechNet иногда предоставляют различные сведения по одному и тому же вопросу. Связано это с тем, что не вся документация стала версии SP1 вместе с SCMDM. Наиболее точным источником информации я считаю библиотеку TechNet.

Не стесняйтесь задавать вопросы. Делать это можно по разному – можно спросить у команды поддержки SCMDM письмом (русский язык не поддерживается), можно задать вопрос на форуме TechNet… Можно попробовать озадачить меня – результат не гарантирован, но помочь всегда попробую.

В общем, удачи во внедрении!

Алексей Ватутин