

Microsoft®  
**System Center**  
**Mobile Device Manager 2008**

Этой статьей я начинаю цикл, посвященный платформе Mobile Device Manager (MDM) из семейства System Center. В него войдут статьи, посвященные вопросам установки, настройки и поддержки этого продукта. И в первой из них я хочу рассказать о том, что такое SCMDM, о его архитектуре и особенностях, а также немного затронуть вопросы лицензирования. Заранее хочу предупредить – все, о чем я буду рассказывать, относится к SCMDM 2008 с установленным SP1.

### Итак, что такое System Center Mobile Device Manager и для чего он нужен?

В нашей стране этот продукт, по ряду причин, является малоизвестным и его распространение происходит неспешно, но с течением времени все больше предприятий приходит к выводу, что мобильные устройства должны:

- поддерживать политики безопасности, традиционно относящиеся к рабочим станциям
- управляться централизованно
- обновляться независимо от их текущего местонахождения

и этот факт позволяет прогнозировать рост интереса к рассматриваемой платформе.

На мой взгляд, наиболее точно на вопрос о том, что такое MDM, отвечает определение, приведенное в документации по продукту: *основной задачей MDM является создание такой структуры, в которой устройства на базе Windows Mobile становятся неотъемлемой частью ИТ-инфраструктуры организации, полностью отвечающие ее требованиям по управлению и аутентификации. Платформа Windows Mobile является идеальной для подобного решения, а возможности MDM позволяют сделать ее более управляемой и безопасной.*

В данный момент на рынке присутствует достаточно много решений по управлению мобильными устройствами – например BlackBerry от RIM или Afaria от Sybase. Так что же позволяет выделить SCMDM из всего этого многообразия? На это есть несколько причин:

- При работе с корпоративной сетью **устройство использует т.н. Mobile VPN на базе IPSec**, что означает наличие безопасного канала для передачи данных между устройством и остальными узлами в сети предприятия. Так же **у мобильных пользователей появляется возможность работать с такими сервисами как OCS, Exchange Server, SharePoint, другими бизнес-приложениями без их публикации в сети Интернет.**
- **Управление устройствами при помощи стандартной консоли Group Policy Management.** При инициализации **устройства становятся частью корпоративного домена** и управление ими происходит при помощи стандартных групповых политик. Политики представлены в виде обычного шаблона ADM, импортируемого в стандартную консоль GPMC, и изначально содержащего более 125 параметров. При необходимости, **администратор может написать свой шаблон**, добавив в него нужные ему параметры.
- **Для распространения приложений на устройства MDM использует Windows Server Update Services (WSUS)**, что означает привычный и удобный для большинства администраторов интерфейс. Устройства могут быть сгруппированы либо вручную администратором, либо автоматически при помощи групповых политик (т.н. targeting).
- Т.к. **для хранения информации об устройствах MDM использует MS SQL Server**, то можно использовать стандартный инструмент для построения отчетов. Так, в SCMDM Resource Kit есть инструмент, под названием Reports, позволяющий создавать инвентаризационные отчеты.

Можно привести и еще больше причин, позволяющих сделать выбор в пользу SCMDM, но самые главные перечислены.

Как становится понятно из приведенного списка, ИТ-инфраструктура предприятия должна быть подготовлена к внедрению MDM и иметь определенные сервисы, которые являются для него обязательными, поэтому предлагаю рассмотреть архитектуру решения.

### Архитектура MDM и ее особенности

При рассмотрении архитектуры MDM первое, что хочется отметить, это использование открытых промышленных стандартов, таких как OMA DM, IPSec, IKEv2, MOBIKE, SCOMO, ведь именно они вместе с возможностями, которые предоставляет платформа Windows Server, позволяют создать мощное и легко масштабируемое решение.

Как и большинство современных решений, MDM является многокомпонентным ПО. Его основными модулями, или, так будет правильно, ролями, являются:

- **MDM Device Management Server** – отвечает за управление устройствами, распространение ПО
- **MDM Enrollment Server** – отвечает за первичную инициализацию устройств
- **MDM Gateway Server** – шлюз, позволяющий обеспечить безопасное подключение к корпоративной сети

Помимо этого возможна установка т.н. **MDM Self Service Portal**, т.е. веб-портала, при помощи которого конечные пользователи могут самостоятельно выполнять некоторые из задач. Схематично архитектура MDM может быть представлена следующим образом:

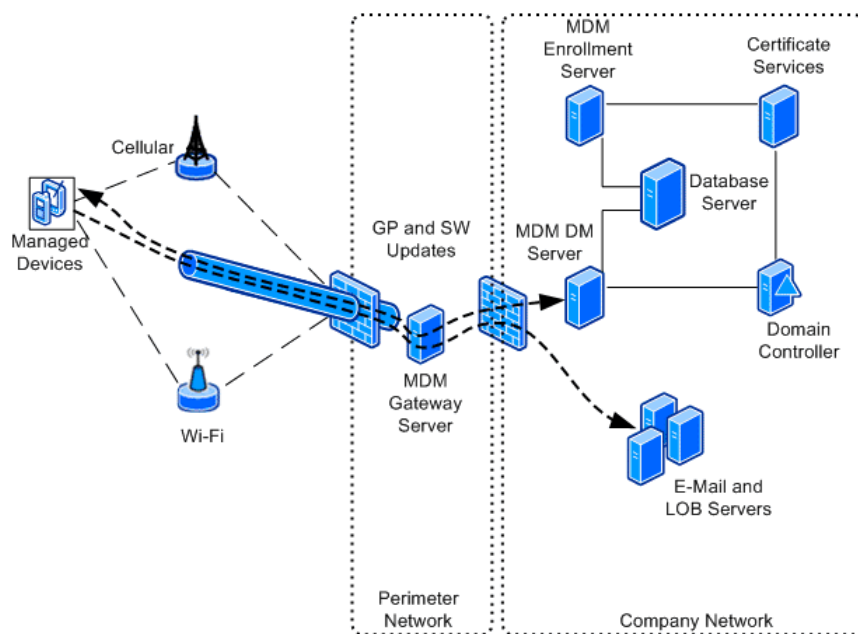


Рис. 1 Архитектура SC MDM 2008 (кликните для увеличения)

Как можно понять из рисунка, к главным особенностям архитектуры относятся:

- Обязательное наличие домена Active Directory
- Обязательное использование центра сертификации (CA)
- Обязательное использование MS SQL Server
- Обязательное использование службы WSUS

- Размещение сервера с ролью шлюза (MDM Gateway Server) в DMZ
- Размещение серверов с ролями MDM Enrollment Server и MDM DM Server во внутренней сети
- Возможность организации подключения устройства, как через сеть сотового оператора, так и при помощи точек доступа Wi-Fi

Но, кроме главных архитектурных особенностей, у MDM есть еще и, скажем так, побочные. И именно они зачастую являются главным сдерживающим фактором при принятии решения о внедрении продукта. Вообще, на мой взгляд, MDM является продуктом с очень большим количеством нюансов, а выражается это в следующем – очень часто при ответе на поставленный вопрос приходится употреблять частицу «но»... В общем, привожу список дополнительных особенностей:

- В качестве мобильной платформы для работы SCMDM может быть использована **только Windows Mobile и только версии 6.1 и выше** – это связано с тем, что только в этой версии появилась возможность ввода устройства в домен.
- Установка MDM может производиться **только на сервера под управлением Windows Server 2003 x64 с установленным SP2, Windows Server 2008 не поддерживается**. При этом MDM **поддерживает работу в лесах и доменах уровня 2003 Native и 2008 Native**. Также **поддерживается установка ролей, за исключением MDM Gateway Server, на виртуальные машины под управлением Hyper-V**. Центр сертификации при этом может находиться как под управлением Windows Server 2003, так и под управлением Windows Server 2008. И еще один момент, который обычно уточняют, – при установке MDM **расширение схемы Active Directory не производится**.
- При выборе платформы SQL Server необходимо учесть, что MDM работает с MS SQL Server 2005 с установленным Service Pack не ниже 2, и **не поддерживает работу с MS SQL Server 2008**. Редакции Express так же не поддерживаются.
- При установке MDM, **Windows Server Update Services должны быть установлены на тот же сервер, что и MDM DM Server**. Также не рекомендуется использовать службы WSUS в конфигурации downstream.
- **Совмещение роли MDM Gateway Server и любых других ролей невозможно**, поэтому минимальное количество серверов, отведенных под MDM, равняется двум (2).
- **MDM Gateway Server не поддерживает размещение позади NAT**.
- MDM поддерживает функцию **Enrollment autodiscovery**, аналогичную autodiscovery в Exchange Server. Она позволяет клиенту, при инициализации устройства, провести поиск MDM Enrollment Server по доменному суффиксу в UPN пользователя. Так вот, эта функция **работает на Windows Mobile версии не ниже 6.1.4**.
- При использовании политик безопасности Exchange ActiveSync и SCMDM, применяются либо те, либо другие. Настройка производится на MDM DM Server.

В общем-то, все... Конечно, есть и другие нюансы, но они не оказывают настолько глобального влияния на создаваемую структуру. Про приведенный список могу сказать, что, на мой взгляд, большая часть особенностей является т.н. «детскими болезнями», т.е. продукт еще достаточно молод[1], но внимание, уделяемое Microsoft этому направлению достаточно велико, что позволяет оптимистично смотреть на его будущее. С другой стороны, часть из озвученных ограничений может пойти во благо – например, стать стимулом для написания регламента по используемым в компании моделям устройств, за актуальностью которого должен следить администратор системы.

И последнее, о чем хотел бы рассказать, из относящегося к архитектуре – это о масштабируемости и отказоустойчивости решения. Тут все просто – при работе SCMDM поддерживает концепцию экземпляров (instance) и означает это следующее:

- В лесу Active Directory может быть до 100 экземпляров SCMDM
- Каждый экземпляр может содержать не более 16 MDM Gateway Server, при этом каждый поддерживает до 15 000 устройств
- Каждый экземпляр может содержать не более 4 MDM DM Server, при этом каждый поддерживает до 15 000 устройств[2]
- Каждый экземпляр может содержать не более 4 MDM Enrollment Server, при этом каждый поддерживает до 25 параллельных инициализаций устройств[2]
- Каждый экземпляр MDM поддерживает до 60 000 пользователей.

Отказоустойчивость MDM Gateway Server обеспечивается средствами DNS, а MDM DM Server и MDM Enrollment Server установкой перед ними аппаратных либо программных балансировщиков нагрузки. Отказоустойчивость остальных служб обеспечивается стандартными для этих служб средствами.

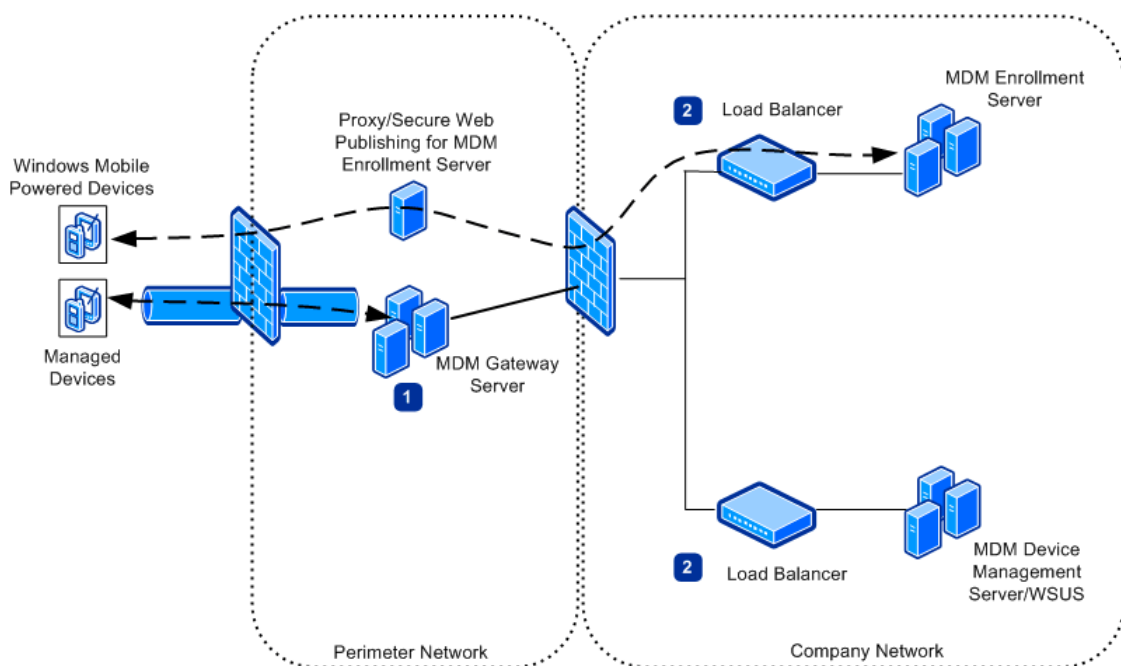


Рис. 2 Обеспечение отказоустойчивости SCMDM (кликните для увеличения)

Так, с архитектурой вроде все. Следующий вопрос, который обычно возникает – «**А как это все работает?**». Если упрощенно описать работу MDM, то схема будет выглядеть следующим образом:

- Пользователь получает мобильное устройство и извещает об этом администратора.
- Администратор выполняет т.н. пре-инициализацию (pre-enrollment), в ходе которой в Active Directory создается запись для устройства, сопоставляется с учетной записью пользователя, генерируется пароль для инициализации (enrollment). Данная операция может быть делегирована пользователю через MDM Self Service Portal. При выполнении данной операции пользователь либо администратор получает всю информацию, необходимую для инициализации устройства, на экран. При необходимости эта информация может быть продублирована на почтовый ящик пользователя.
- Пользователь выполняет инициализацию устройства, в ходе которой устройство подключается к MDM Enrollment Server и получает первичные настройки. Для проведения данной операции от пользователя требуется знать имя либо адрес Enrollment Server, UPN своей учетной записи, пароль для инициализации (который был сгенерирован на 2-м шаге). Если внешний DNS содержит необходимую для Enrollment autodiscovery запись и

устройство пользователя работает на платформе Windows Mobile 6.1.4, то от пользователя не требуется указывать имя либо адрес Enrollment Server.

- Получив первичные настройки, в том числе информацию о MDM Gateway Server, устройство предлагает выполнить перезагрузку, после чего подключается к шлюзу с использованием Mobile VPN. В случае успешного подключения устройство получает все определенные политиками настройки и производит установку назначенного ПО. Интервал последующих подключений определяется настройками на MDM DM Server.
- В случае необходимости выполнить блокировку либо его очистку, это может сделать как администратор из консоли управления MDM DM Server, так и пользователь при помощи Self Service Portal.

В целом данная схема стабильна и неизменна. Более подробно некоторые моменты будут описаны в статьях, посвященных установке MDM и распространению ПО на устройства.

И последнее, о чем я хотел бы рассказать – это **лицензирование и ценовая политика**.

SCMDM 2008 предлагается приобретать в рамках Microsoft Volume Licensing и Volume Licensing. Программа лицензирования является стандартной и предполагает приобретение серверных и клиентских (либо пользовательские, либо на устройство) лицензий. Цены, приведенные на сайте Microsoft, справедливы для США и могут несколько отличаться от имеющихся у нас. Из особенностей – можно приобрести серверную лицензию SCMDM вместе с лицензией на SQL Server 2005, но при этом SQL Server можно использовать только для нужд SCMDM.

Предлагаемая лицензия	Цена
<b>System Center Mobile Device Manager 2008</b>	
MDM 2008 Server License	\$2149
MDM 2008 User Client Access License (CAL)	\$57
MDM 2008 Device Client Access License (CAL)	\$57
<b>System Center Mobile Device Manager 2008 with SQL Server 2005 Technology</b>	
MDM 2008 with SQL Server License	\$3041
MDM 2008 with SQL User Client Access License (CAL)	\$57
MDM 2008 with SQL Device Client Access License (CAL)	\$57

На этом я хотел бы завершить вводную часть, посвященную SCMDM 2008, и пожелать всем приятного знакомства с этим интересным продуктом. Тем, кому стало интересно и кто захочет сам посмотреть на MDM, развернув его на стенде в своей компании, могу дать ценный совет – при работе со встроенной справкой, страницей SCMDM на TechNet и продуктовыми гайдами – проверяйте всю информацию между этими источниками. Как показала практика – встроенная справка в SCMDM 2008 SP1 практически не обновилась со времен SCMDM RTM, а изменений там очень много, на странице SCMDM на TechNet ситуация несколько лучше, но все равно не вся информация достоверна. Наиболее доверенным источником для меня стали руководства по продукту, которые можно скачать с TechNet вместе с пробной версией продукта.

[1] SCMDM 2008 RTM стал первой версией продукта и вышел в феврале 2008 года, а SP1 появился в декабре того же года.

[2] В некоторых документах приводятся другая цифра – до 6 MDM DM Server и до 2 MDM Enrollment Server. Проверить на практике точность еще не довелось, но если что, имейте ввиду.

**Алексей Ватутин**