

# *Microsoft*<sup>®</sup> Virtual Labs

## **Using System Center Mobile Device Manager 2008 Features**

**Microsoft**<sup>®</sup>

# Table of Contents

---

<b>Using System Center Mobile Device Manager 2008 Features .....</b>	<b>1</b>
Exercise 1: Using ISA Server to Publish the Mobile Device Manager Enrollment Web Service .....	2
Exercise 2: Creating Mobile Policies using the Group Policy Management Console Tool.....	4
Exercise 3: Installing and Using the Mobile Device Manager Self Service Portal.....	6
Exercise 4: Enrolling a Mobile Device.....	8
Exercise 5: Using the System Center Mobile Device Manager to Create a Pre-Enrollment .....	11
Exercise 6: Using Mobile Device Manager Software Distribution to Deploy an Application .....	12
Exercise 7: Using the System Center Mobile Device Manager Console to Wipe a Device .....	15

# Using System Center Mobile Device Manager 2008 Features

## Objectives

After completing this lab you will be able to:

- Understand how to deploy policies and software using System Center Mobile Device Manager
- Understand multiple methods of creating device enrollments, using either self-service or pre-enrollment, and actually enrolling devices
- Understand how mobile devices can be managed in a secure manner using a combination of policies, remote wipe, and centralized software deployment

## Scenario

Contoso is a fictitious 35-person manufacturing company based in the Midwestern United States that develops prototype manufacturing methods for medium and large companies. Contoso’s solutions enable its business customers to use fast prototyping and streamlined manufacturing procedures to bring products to market in a more efficient manner. To optimize inventory control, research methods and communication in its facilities, Contoso decided to issue Windows Mobile® 6.1 devices to everyone in the company. Due to security concerns, they wanted to ensure that the devices would be highly secure, protected in case of loss, and have the ability to receive software applications pushed out by IT personnel. To achieve these goals, Contoso decided to install, configure, and use Microsoft System Center Mobile Device Manager. With the devices being deployed only in company facilities, Contoso decided that there was not a present need for external connectivity or VPN gateway services. Even though VPN connectivity is not currently planned, Mobile Device Manager will be integrated with the company’s Microsoft Internet Acceleration and Security 2006 infrastructure for future expansion.




Now that the solution has been installed and configured, it is up to the IT personnel to enroll devices, create and assign policies, push software, and wipe devices that are lost or stolen.

*Note: In this set of labs, we are using a mobile device emulator to simulate a Windows Mobile® 6.1 device connecting to the corporate network over Wi-Fi. To gain this connectivity, we are using Microsoft ActiveSync® to tether the device inside a virtual machine. Some of the steps that are required to ensure connectivity of the device would not be needed in a real-world scenario.*

## Estimated Time to Complete This Lab

60-90 minutes


## Computers Used in this Lab

-  MDMCORE
-  AD01
-  MDMCLIENT
-  ISA01

# Exercise 1: Configuring ISA Server to Publish the Mobile Device Manager Enrollment Web Service Scenario

While the current deployment of Mobile Device Manager is aimed at internal connectivity only, a plan to expand to external connectivity is in the near future. Since we installed servers and services, it makes sense to modify the infrastructure to allow connectivity when we need it, instead of having one more step to do when time might be more critical. To this end, we're going to add a firewall rule to our ISA 2006 server that will allow mobile clients to enroll from outside the corporate network. The clients will not be able to receive policies and software with this change, but once the plan for external connectivity is implemented, external clients will be able to use the VPN client to connect to the network and receive policies and software.

**Note:** Due to the limitations of using a virtual environment (including using the mobile device emulator), it is not practical to actually host a client outside of the lab environment. This exercise will walk through the steps necessary to configure the features mentioned, but there will be no verification of functionality.


Tasks	Detailed Steps
<p>Complete the following task on:</p>  <b>ISA01</b> <p><b>1. Creating the Enrollment Web Service Publishing Rule</b></p>	<ol style="list-style-type: none"> <li>a. The <b>ISA01</b> machine has been pre-logged on using the Administrator account and a password of <b>pass@word1</b>.</li> <li>b. Launch <b>ISA Server Management</b> from <b>Start   Programs   Microsoft ISA Server</b>.</li> <li>c. Expand <b>ISA01</b>, select the <b>Monitoring</b> node, then select the <b>Firewall Policy</b> node, and then right-click the <b>Firewall Policy</b> node and click <b>New   Web Site Publishing Rule</b>.</li> <li>d. In the New Web Publishing Rule Wizard, type <b>MDM Enrollment Web Publishing Rule</b> in the <b>Web Publishing Rule Name</b> box and click <b>Next</b>.</li> <li>e. In the <b>Select Rule Action</b> page ensure that <b>Allow</b> is selected under <b>Action to take when rule conditions are met</b> and click <b>Next</b>.</li> <li>f. On the <b>Publishing Type</b> page, click <b>Publish a single Web site or load balancer</b> and click <b>Next</b>.</li> <li>g. On the <b>Server Connection Security</b> page ensure that the default of <b>Use SSL to connect to the published Web server or server farm</b> is selected and click <b>Next</b>.</li> <li>h. On the <b>Internal Publishing Details</b> page, type in <b>mobileenroll.contoso.net</b> in the <b>Internal site name</b> box.</li> <li>i. Select the <b>Use a computer name or IP address to connect to the published server</b> check box and type in the IP address of <b>192.168.0.2</b> in the <b>Computer name or IP Address</b> box and click <b>Next</b>.</li> <li>j. On the next page, <b>Internal Publishing Details</b>, leave the <b>Path (optional)</b> box blank and click <b>Next</b>.</li> <li>k. On the <b>Public Name Details</b> page type in <b>mobileenroll.contoso.net</b> in the <b>Public Name</b> box. Leave the <b>Path (Optional)</b> box blank and click <b>Next</b>.</li> <li>l. On the <b>Select Web Listener</b> page, click <b>New</b> to launch the New Web Listener Wizard.</li> <li>m. In the New Web Listener Wizard, type <b>SCMDM HTTPS Web Listener</b> in the <b>Web Listener Name</b> box and click <b>Next</b>.</li> <li>n. On the <b>Client Connection Security</b> page, leave the default value of <b>Require SSL secured connections with clients</b> and click <b>Next</b>.</li> </ol>

Tasks	Detailed Steps
	<p><b>o.</b> On the <b>Web Listener IP Addresses</b> page, select <b>External</b> in the <b>Listen for incoming Web requests on these networks</b> list. Leave the check box selected for <b>ISA Server will compress content...</b> and click <b>Next</b>.</p> <p><b>p.</b> On the <b>Listener SSL Certificates</b> page click <b>Select Certificate</b> to display the list of available certificates. Select the <b>mobileenroll</b> SSL certificate, click <b>Select</b>, and then click <b>Next</b>.</p> <p><b>q.</b> On the <b>Authentication Settings</b> page, select <b>No Authentication</b> in the <b>Select how clients will provide credentials to ISA Server</b> list and click <b>Next</b>.</p> <p><b>r.</b> On the <b>Single Sign On Settings</b> page, click <b>Next</b>.</p> <p><b>s.</b> Click <b>Finish</b> on the <b>Completing the New Web Listener Wizard</b> page.</p> <p><b>t.</b> The <b>Select Web Listener</b> page should now have the Web listener that was created displayed in the list. Click <b>Next</b>.</p> <p><b>u.</b> On the <b>Authentication Delegation</b> page, select <b>No delegation, but client may authenticate directly</b> from the list and click <b>Next</b>.</p> <p><b>v.</b> On the <b>User Sets</b> page accept the default of <b>All Users</b> and click <b>Next</b>.</p> <p><b>w.</b> Click <b>Finish</b> on the <b>Completing the New Web Publishing Rule Wizard</b>.</p> <p><b>x.</b> To save changes and updated the ISA Server 2006 configuration click <b>Apply</b> in the main <b>Firewall Policy</b> page and click <b>OK</b>.</p> <p><i><b>Note:</b> Due to the limitations of using a virtual environment (including using the mobile device emulator), it is not practical to actually host a client outside of the lab environment. The steps in this exercise show the default configuration of a Web publishing rule in ISA Server 2006. For more information about publishing web sites using ISA 2006, please visit:</i></p> <p><a href="http://www.microsoft.com/technet/isa/2006/default.mspx">http://www.microsoft.com/technet/isa/2006/default.mspx</a></p>

## Exercise 2: Creating Mobile Policies using the Group Policy Management Console Tool

### Scenario

Once we have System Center Mobile Device Manager installed, the first step towards a secure mobile device is to develop a set of policies to push out to the enrolled devices. Using policies, we can work with many different aspects of mobile device security from password policies, to file encryption, to disabling applications. To apply these policies, we are going to log on to the AD01 machine, create and link a Group Policy object, and then edit it. Once we enroll a device, policies will automatically be enforced.

Tasks	Detailed Steps
<p><b>Complete the following task on:</b></p>  <b>AD01</b>	<ol style="list-style-type: none"> <li>a. Switch to <b>AD01</b> machine, this computer has been pre-logged on using the Administrator account and a password of <b>pass@word1</b>.</li> <li>b. Double-click the <b>Group Policy Management</b> icon on the desktop. We want to log on to this machine since it has the Policy Extensions and Group Policy Management Console installed.</li> <li>c. If it is not already visible, expand the forest, the contoso.net domain, and click <b>SCMDM2008 Managed Devices</b>.</li> <li>d. Right-click the <b>SCMDM2008 Managed Devices</b> organizational unit (OU) to expand the submenu, and then click <b>Create and Link a GPO Here...</b></li> <li>e. In the <b>New GPO</b> dialog box, type <b>Contoso Default Mobile Device Policy</b>. Click <b>OK</b>.</li> <li>f. Right-click the new policy and click <b>Edit</b>.</li> <li>g. In the <b>Group Policy Object Editor</b>, under the <b>Computer Configuration</b> node right-click <b>Administrative Templates</b> to expand the submenu and click <b>Add/Remove Templates</b>.</li> <li>h. In the <b>Add/Remove Templates</b> window, click <b>Add...</b></li> <li>i. Select the <b>mobile.adm</b> administrative template from <b>C:\windows\inf</b> and then click <b>Open</b>.</li> <li>j. The mobile administrative template will now be visible in the <b>Add/Remove Templates</b> window. Click <b>Close</b> to return to the Group Policy Object Editor.</li> <li>k. In the <b>Group Policy Object Editor</b>, under <b>Administrative Templates</b> for both <b>Computer Configuration</b> and <b>User Configuration</b>, a new folder named <b>Windows Mobile Settings</b> has been added. To make a <b>Computer Configuration</b> policy for wiping a device, expand the <b>Administrative Templates</b> folder, then expand the first <b>Windows Mobile Settings</b> folder, and select <b>Password Policies</b>. In the details pane, double-click <b>Wipe device after failed attempts</b>.</li> <li>l. By default, all device policies are set to <b>Not Configured</b>. Click <b>Enabled</b> and change <b>Wipe device after failed logins</b> to <b>3</b>. Click <b>OK</b>.</li> <li>m. Double-click the <b>Require password</b> policy setting and click <b>Enabled</b>, and then click <b>Next Setting</b>.</li> <li>n. In the <b>Password type</b> policy setting, click <b>Enabled</b> and then under the <b>Password complexity</b> list select <b>PIN</b>, then click <b>Next Setting</b>.</li> <li>o. In the <b>Password timeout</b> policy setting, click <b>Enabled</b> and then specify a timeout value of <b>15 minutes</b> and click <b>OK</b> to close the properties window.</li> </ol>



Tasks	Detailed Steps
	<ul style="list-style-type: none"><li data-bbox="508 195 987 226"><b>p.</b> Close the <b>Group Policy Object Editor</b>.</li><li data-bbox="508 243 1393 300"><b>q.</b> To verify that the Computer and User Device policies are in effect, expand <b>SCMDM2008 Managed Devices</b> in the <b>Group Policy Management</b> console.</li><li data-bbox="508 317 1369 373"><b>r.</b> Click the <b>Contoso Default Mobile Device Policy GPO</b> and click <b>OK</b> on the dialog box that appears, and then click the <b>Settings</b> tab in the details pane.</li><li data-bbox="508 390 1393 485"><b>s.</b> Click <b>show all</b> to see all policies. Both the <b>Computer Configuration</b> and the <b>User Configuration</b> policies should be enabled, although only the <b>Computer Configurations</b> heading has policies defined.</li></ul>

# Exercise 3: Installing and Using the Mobile Device Manager Self Service Portal Scenario

*At Contoso, there are a limited number of people available to fulfill IT requests. Because of the resource constraints, the decision was made to install the Self Service Portal from the Mobile Device Manager Resource Kit. This will allow end users to perform some tasks on their own devices. They will be able to create a pre-enrollment for a new device, and wipe devices that may be compromised. In this example, we want to walk through the installation of the Self Service Portal on the MDMCORE machine and then we will create a pre-enrollment.*

*More information about the Mobile Device Manager Resource Kit can be found at:*


<http://technet.microsoft.com/en-us/scmdm/cc304591.aspx>




Tasks	Detailed Steps
<p><b>Complete the following task on:</b></p>  <b>AD01</b> <p><b>1. Installing the Mobile Device Manager Self-Service Portal</b></p>	<ul style="list-style-type: none"> <li>a. From the desktop, click <b>Start   Administrative Tools   DNS</b>.</li> <li>b. Expand the <b>AD01</b> node, the <b>Forward Lookup Zones</b>, and then the <b>contoso.net</b> node.</li> <li>c. Right-click the <b>contoso.net</b> forward lookup zone, and click <b>New Alias (CNAME)</b>....</li> <li>d. In the <b>Alias</b> box type <b>mobileselfservice</b>.</li> <li>e. For the <b>Fully qualified domain name (FQDN) for target host</b> box, click <b>Browse...</b> and then double-click <b>AD01</b>, then <b>Forward Lookup...</b>, then <b>contoso.net</b>, and finally, click <b>MDMCORE</b> and click <b>OK</b>.</li> <li>f. Click <b>OK</b> when finished and close the <b>DNS Management Console</b>.</li> </ul>
<p><b>Complete the following tasks on:</b></p>  <b>MDMCORE</b> <p><b>2. Enrolling a Mobile Device Using the Self-Service Portal</b></p>	<ul style="list-style-type: none"> <li>a. The <b>MDMCORE</b> computer has been pre-logged in using the Administrator account and a password of <b>pass@word1</b>.</li> <li>b. Navigate to <b>C:\ssp\</b> and double-click the <b>selfserviceportal.msi</b>.</li> <li>c. On the <b>Welcome to the System Center Mobile Device Manager-Self Service Portal Setup Wizard</b> page, click <b>Next</b>.</li> <li>d. Read the <b>End User License Agreement</b>, click <b>I accept the License Terms for Microsoft Software</b>, and then click <b>Next</b>.</li> <li>e. On the <b>Installation Directory</b> page, accept the default installation path of <b>C:\Program Files\Microsoft System Center Mobile Device Manager Self Service Portal\</b> and then click <b>Next</b>.</li> <li>f. On the <b>Self Service Portal Location</b> page, enter the fully qualified domain name (FQDN) of <b>mobileselfservice.contoso.net</b> for the <b>Self Service Portal Server</b>, and then click <b>Next</b>.</li> <li>g. On the <b>Device Management Setup</b> page, enter port <b>442</b> (not 443) as the <b>Self Service Portal SSL port</b>. Leave the <b>Self Service Portal TCP port</b> set to <b>8442</b> and then click <b>Next</b>.</li> <li>h. On the <b>Server Certification Authority</b> page, type <b>ad01.contoso.net\CONTOSOCA</b> and click <b>Next</b>.</li> <li>i. On the <b>Ready to Install</b> page, click <b>Install</b>.</li> <li>j. Once the wizard is finished, click <b>Finish</b> to close the window.</li> </ul>

Tasks	Detailed Steps
<p><b>3. Creating an Enrollment Request with the Self-Service Portal</b></p>	<ul style="list-style-type: none"> <li><b>a.</b> From the desktop, click <b>Start   Run</b> and type <b>https://mobileselfservice.contoso.net:442/pages/startenrollment.aspx</b> in the <b>Open:</b> box and press <b>Enter</b>.</li> <li><b>b.</b> At the logon prompt, type the domain name of <b>CONTOSOLizK</b> and password of <b>pass@word1</b>. Click <b>OK</b>.</li> <li><b>c.</b> Once logon is complete the <b>System Center Mobile Device Manager 2008 Self Service Portal</b> page appears.</li> <li><b>d.</b> Under the <b>New Enrollment</b> tab, type <b>MYDEVICE</b> for the device name and then click <b>Create Enrollment Request</b>.</li> <li><b>e.</b> On the <b>Pending Enrollment Details</b> page, review the steps needed to enroll the mobile device.</li> </ul> <p><i>Note: Be certain to copy down the <b>Enrollment PIN</b> (you can press <b>CTRL+C</b> and then paste the contents into <b>Notepad</b>) before closing the Web page.</i></p>

# Exercise 4: Enrolling a Mobile Device Scenario

Once a pre-enrollment has been created, it's time to actually enroll a device. For clients that are using a physical device, the process is fairly straight forward. To enroll the emulated device we are using in the lab, a few extra steps have to be taken to ensure that connectivity is established and the device gets all the necessary policies.


Tasks	Detailed Steps
<p>Complete the following tasks on:</p>  MDMCLIENT	<ol style="list-style-type: none"> <li>a. Switch to <b>MDMCLIENT</b> computer. The machine has been pre-logged in using the Administrator account and a password of <b>pass@word1</b>.</li> <li>b. Double-click the <b>Windows Mobile 6.1.4 Emulator</b> icon on the desktop.</li> <li>c. Once the device is loaded, double click on the <b>Device Emulator Manager</b> on the desktop and click <b>Refresh</b>.</li> <li>d. Under the <b>Others</b> node, right-click the GUID and click <b>Cradle</b>.</li> </ol> <p><i>Note: Due to limitations of the lab environment, it is necessary to use an emulator as our mobile device. Some of the steps necessary to run the emulator in a virtual environment are not required in real-world deployments. Using an ActiveSync® partnership to tether the device is only done to simulate a Wi-Fi connection of the device to the Contoso corporate network.</i></p> <p><i>Note: Microsoft ActiveSync® may bring up several prompts to initiate a partnership. Since we are only using this as a data connection, we can select <b>OK</b> and <b>Cancel</b> in the resulting windows.</i></p> <p><i>Note: The mobile emulator should now establish a Microsoft ActiveSync® session with the desktop host. If it does not, right-click the device in the <b>Device Emulator Manager</b>, click <b>Uncradle</b>, and try step <b>d</b> again.</i></p> <ol style="list-style-type: none"> <li>e. Switch back to the <b>WM 6.1.4 Professional -240x400</b> window, click <b>Start   Settings</b>, and click the <b>Connections</b> tab.</li> <li>f. In the <b>Connections</b> tab, click the <b>Domain Enroll</b> icon to begin the enrollment process.</li> <li>g. On the <b>Domain Enrollment</b> page, click <b>Enroll</b>.</li> <li>h. A notification will appear. Click <b>Next</b> to continue.</li> <li>i. Enter <b>lizk@contoso.net</b> in the <b>User Name</b> box and click <b>Next</b>.</li> <li>j. Enter the <b>Enrollment Password</b> generated during enrollment and click <b>Next</b>. You can find the password by switching to MDMCORE machine and</li> <li>k. A message will appear informing you that the device is enrolling.</li> <li>l. On the <b>Enroll</b> page, a message will appear stating that the device is being enrolled in the domain. Click <b>OK</b> to continue.(If you receive an error, check and ensure that the active sync has been setup for the emulator)</li> <li>m. The <b>Restart</b> message will appear asking you to restart the device. Click <b>Now</b> to begin a soft reboot of the device.</li> </ol> <p><i>Note: When the device reboots, if it does not connect, reset the ActiveSync Connection by right-clicking the device in the <b>Device Emulator Manager</b> and clicking <b>Uncradle</b>, and then right-clicking the device again and clicking <b>Cradle</b>.</i></p> <p><i>Note: Since we are emulating a mobile device, the length of time for the policies to be applied may be longer than in a real-world implementation. This being the case, the following tasks deal with exploring the Mobile Device Manager environment while</i></p>

Tasks	Detailed Steps
	<i>waiting for the device to receive policies.</i>
<p><b>Complete the following task on:</b></p>  <b>MDMCORE</b> <p><b>2. Validating Enrollment to Mobile Device Manager</b></p>	<ol style="list-style-type: none"> <li>a. Switch to the <b>MDMCORE</b> computer.</li> <li>b. Double-click the <b>Mobile Device Manager Console</b> icon on the desktop. In the navigation pane, expand the <b>Device Management</b> node.</li> <li>c. Select <b>All Managed Devices</b>.</li> <li>d. Click the <b>MYDEVICE</b> device. Click the <b>Device Status</b> tab in the lower half of the console's center pane.</li> <li>e. View the device's details in the <b>Device Status</b> tab.</li> </ol>
<p><b>Complete the following task on:</b></p>  <b>AD01</b> <p><b>3. Verifying the Device in Active Directory</b></p>	<ol style="list-style-type: none"> <li>a. Log on to <b>AD01</b> using the Administrator account and a password of <b>pass@word1</b>.</li> <li>b. Double-click the <b>Active Directory Users and Computers</b> icon on the desktop.</li> <li>c. Under the <b>contoso.net</b> node, click the <b>SCMDM2008 Managed Devices</b> node.</li> <li>d. Double-click the computer account named <b>MYDEVICE</b>.</li> <li>e. In the <b>MYDEVICE Properties</b> window, click the <b>Operating System</b> tab.</li> <li>f. Verify that the <b>Name</b> field says <b>Windows Mobile Device</b>.</li> <li>g. Click <b>OK</b> to close the properties window, and close the MMC window.</li> <li>h. Click <b>No</b> on the message asking if you want to save the console settings.</li> </ol>
<p><b>Complete the following tasks on:</b></p>  <b>MDMCLIENT</b> <p><b>4. Enrolling a Windows Mobile 6.1 Device</b></p>	<ol style="list-style-type: none"> <li>a. Switch to the <b>MDMCLIENT</b> virtual machine.</li> <li>b. In the <b>WM 6.1.4 Professional -240x400</b> window, select <b>OK</b> from the resulting <b>Update Required</b> dialog. Enter <b>4123</b> in the <b>Password</b> field, enter <b>4123</b> in the <b>Confirm</b> field, and select <b>OK</b>.</li> <li>c. The <b>Restart</b> message will appear asking you to restart the device. Click <b>Now</b> to begin a soft reboot of the device.</li> </ol> <p><i>Note: It may take several minutes for the device to receive all of the software and policies from the Mobile Device Manager server, due to the emulated environment.</i></p> <p><i>Note: If the device takes longer than the allotted time to perform a synchronization with the Mobile Device Manager server, we can initiate a connection using the <b>MDM ConnectNow</b> tool. The steps for using this tool are contained in the next task.</i></p>
<p><b>5. Using the MDM ConnectNow Tool to Force Synchronization</b></p>	<p><i>Note: The <b>MDM ConnectNow</b> tool is a client application from the <b>Mobile Device Manager Resource Kit</b>. More information on this tool can be found on <a href="#">Microsoft Technet</a>.</i></p> <ol style="list-style-type: none"> <li>a. On the mobile device emulator, enter the <b>PIN (4123)</b>, and click <b>Unlock</b>.</li> <li>b. Reset the ActiveSync Connection by right-clicking the device in the <b>Device Emulator Manager</b> and clicking <b>Uncradle</b>, and then right-clicking the device again and clicking <b>Cradle</b>.</li> </ol> <p><i>Note: Click <b>OK</b> or <b>Cancel</b> on any warnings that may come up from ActiveSync, warning about a new partnership.</i></p> <ol style="list-style-type: none"> <li>c. On the mobile device emulator, enter the <b>PIN (4123)</b>, and click <b>Unlock</b>.</li> <li>d. Once the device is unlocked, click <b>Start</b> and click <b>Programs</b>.</li> <li>e. In <b>Programs</b>, click the icon for the <b>MDM ConnectNow</b> program.</li> <li>f. In the <b>MDM ConnectNow</b> program, click <b>Connect Now</b> to initiate a connection</li> </ol>

Tasks	Detailed Steps
	<p>with the Mobile Device Manager.</p> <p><b>g.</b> Wait for the <b>Last Connection Status</b> to display <b>Success</b> and then close the <b>MDM ConnectNow</b> application.</p> <p><i><b>Note:</b> It may take several minutes for the tool to display progress. If the mobile device does not display progress for a long time, it can be soft-reset by going to the <b>File</b> menu of the emulator window, selecting the <b>Reset</b> submenu and clicking <b>Soft</b>. Once this is done, reset the ActiveSync Connection by right-clicking the device in the <b>Device Emulator Manager</b> and clicking <b>Uncradle</b>, and then right-clicking the device again and clicking <b>Cradle</b>.</i></p> <p><i><b>Note:</b> You may need to run the tool more than once for the policies to take effect.</i></p>

## Exercise 5: Using the System Center Mobile Device Manager Console to Create a Pre-Enrollment Scenario

*In some cases, IT personnel will need to use the Mobile Device Manager Console to create pre-enrollments and then enroll devices in the environment. To do this, we will first log on to the MDMCORE machine and create the pre-enrollment. Since we already enrolled our emulated device, this exercise is for education only; given to present you with an alternate method of creating enrollments for devices.*


Tasks	Detailed Steps
<p><b>Complete the following task on:</b></p> <p> <b>MDMCORE</b></p> <p><b>1. Creating an Enrollment Request</b></p>	<ol style="list-style-type: none"> <li><b>a.</b> Log on to <b>MDMCORE</b> using the Administrator account and a password of <b>pass@word1</b>.</li> <li><b>b.</b> On <b>MDMCORE</b>, double-click the <b>Mobile Device Manager Console</b> icon on the desktop, if it is not already open.</li> <li><b>c.</b> In the MDM Console, click <b>Pending Enrollments</b>. In the <b>Actions</b> pane, click <b>Create Pre-Enrollment</b>.</li> <li><b>d.</b> On the first page of the Pre-Enrollment Wizard, click <b>Next</b>.</li> <li><b>e.</b> On the <b>Name Device</b> page, enter <b>LIZK01</b> in the <b>Device Name</b> box and then click <b>Browse</b> to locate the <b>SCMDM2008 Managed Devices</b> organizational unit for the mobile device.</li> <li><b>f.</b> Upon selection, click <b>OK</b> to return to the Device Name page and click <b>Next</b> to continue.</li> <li><b>g.</b> On the <b>Select User</b> page, click <b>Browse</b> and another dialog box will appear. Select <b>Liz Keyser</b> as the Microsoft Active Directory® user account to be used in the mobile device enrollment process and click <b>OK</b>.</li> <li><b>h.</b> On the <b>Select User</b> page, click <b>Next</b>.</li> <li><b>i.</b> On the <b>Create Pre-Enrollment</b> page, click <b>Create</b>.</li> <li><b>j.</b> The <b>Completion</b> page will list all required information to begin the enrollment process, which is detailed in the next section. This includes the <b>Enrollment ID (e-mail address)</b> and <b>Enrollment Password</b>.</li> <li><b>k.</b> Click <b>Finish</b> to end the enrollment request process.</li> <li><b>l.</b> To verify the pending enrollment, check to see that there is an object in the <b>Pending Enrollments</b> pane on the console.</li> </ol>


## Exercise 6: Using Mobile Device Manager Software Distribution to Deploy an Application Scenario

One of the advantages of centrally managing mobile devices is that it is quite easy to sign, package, and deploy mobile applications to any device in the organization. Using the Mobile Device Manager Software Distributor, we can take application packages that we create and assign them to devices and have those applications installed automatically.

To comply with time requirements in the lab, we completed the following steps that have to be performed in the organization, prior to deploying signed packages.. More information about the steps required can be found in the System Center Mobile Device Manager documentation and also at <http://technet.microsoft.com/en-us/scmdm/default.aspx>. The steps we performed are:

- Install CA certificates on the Mobile Device Manager 2008 server that will be publishing software.
- Import the CA certificates to the mobile device store and install them (can be deployed through Group Policy).
- Create a Code Signing template on the CA.
- Request and install the code signing certificate from the CA Web site on the software publishing computer.
- Copy the code signing certificate from the Personal to the Trusted Publishers Certificate store.
- Export the certificate from the Personal store as a PFX.

Tasks	Detailed Steps
<p><b>Complete the following tasks on:</b></p>  <b>MDMCORE</b> <p><b>1. Signing Cabinet Files for Distribution</b></p>	<p><b>a.</b> From the desktop, navigate to <b>C:\signfolder</b> to verify that the <b>signcert.pfx</b> certificate is there.</p> <p><b>b.</b> Open a command prompt by clicking <b>Start   Run</b> and then type <b>cmd</b> in the <b>Open:</b> box, and press <b>ENTER</b>.</p> <p><b>c.</b> At the command prompt, type <b>cd c:\signfolder</b> to change into the signfolder directory.</p> <p><b>d.</b> In the <b>signfolder</b> directory type the following command and then press <b>ENTER</b>:</p> <pre>cabsigntool.exe c:\signfolder\MDMManagedDeviceStatusViewer.cab c:\signfolder\MDMManagedDeviceStatusViewer_SIGNED.cab -f c:\signfolder\signcert.pfx -p "pass@word1"</pre> <p><b>e.</b> The <b>cabsigntool</b> should display <b>Done</b> when it is done signing the cab's contents.</p> <p><b>f.</b> Close the command prompt window.</p>
<p><b>2. Creating a Device Group</b></p>	<p><b>a.</b> From the desktop, double-click the <b>Mobile Device Manager Software Distribution</b> icon to open the software distribution console.</p> <p><b>b.</b> Expand the <b>Software Distribution   MDMCORE   Devices</b> nodes. Right-click <b>All Devices</b> and click <b>Options</b>.</p> <p><b>c.</b> On the <b>General</b> tab click <b>Use the Mobile Device Manager Software Distribution console to assign each device to a group or groups. Devices will be placed in the Unassigned Devices group for you to reassign.</b> Click <b>OK</b> to close the prompt.</p> <p><b>d.</b> Next, right-click <b>All Devices</b> and click <b>Add Device Group....</b></p> <p><b>e.</b> In the <b>Add Device Group</b> dialog box, type <b>Software Distribution Test Group</b> as the name for the group and click <b>Add</b>. Upon completion, expand the <b>All Devices</b> node and observe that the group has been added.</p>


Tasks	Detailed Steps
<p><b>3. Move a device to the Software Distribution Test Group</b></p>	<ul style="list-style-type: none"> <li>a. Click the <b>Unassigned Devices</b> node and select <b>Any</b> in the <b>Status</b> list, and then click <b>Refresh</b>.</li> <li>b. In the details pane, right-click the device <b>MYDEVICE</b> and click <b>Change Membership...</b></li> <li>c. In the <b>Set Device Group Membership</b> dialog box, select the <b>Software Distribution Test Group</b> check box, and then click <b>OK</b>.</li> </ul>
<p><b>4. Creating the Software Package</b></p>	<ul style="list-style-type: none"> <li>a. In the <b>Software Distribution Console</b>, expand the <b>Software Distribution   MDMCORE   Packages</b> nodes. Right-click <b>Software Packages</b> and click <b>Create</b>.</li> <li>b. On the <b>Introduction</b> page, click <b>Next</b>.</li> <li>c. On the <b>Software Package</b> page, click <b>Browse</b> and navigate to the signed <b>MDMManagedDeviceStatusViewer_SIGNED.cab</b> file in <b>C:\signfolder</b>. Select the file and click <b>Open</b>. Under <b>Package title</b>, type <b>Contoso Field App</b> as the name for your software package and enter a description in <b>Package description</b>. Click <b>Next</b> to continue.</li> <li>d. On the <b>Target Devices</b> page, click <b>All</b>. Click <b>Next</b>.</li> <li>e. On the <b>Permit Uninstall</b> page, click <b>Yes</b> under <b>Should users be allowed to uninstall this package?</b> Click <b>Next</b>.</li> <li>f. On the <b>Device Languages</b> page, click <b>All languages</b>. Click <b>Next</b>.</li> <li>g. Under <b>Software Dependencies</b> click <b>No software dependencies</b> and click <b>Next</b>.</li> <li>h. Under <b>Registry Dependencies</b> click <b>No registry dependencies</b> and click <b>Next</b>.</li> <li>i. On the <b>Create Installation Package</b> page, click <b>Create</b>.</li> <li>j. On the <b>Completion</b> page, Click <b>Finish</b>.</li> </ul>
<p><b>5. Approving the Software Package</b></p>	<ul style="list-style-type: none"> <li>a. In the <b>Software Distribution Console</b>, click <b>Software Packages</b>.</li> <li>b. In the details pane, right-click <b>Contoso Field App</b> and click <b>Approve...</b></li> <li>c. On the <b>Approve Packages</b> page, click the <b>Software Distribution Test Group</b>. Click the list next to the group and select <b>Approved for Install</b>. Click <b>OK</b>.</li> <li>d. When the progress bar finishes on the <b>Approval Progress</b> page, click <b>Close</b> to finish the approval process.</li> </ul>
<p><b>6. Synchronizing Active Directory and Mobile Device Manager</b></p>	<ul style="list-style-type: none"> <li>a. Double-click the <b>Mobile Device Manager Shell</b> icon to open a PowerShell command prompt.</li> <li>b. Run the PowerShell cmdlet by typing <b>Update-MobilePolicyCalculation EXCAL01</b> and pressing ENTER.</li> </ul> <p><i>Note: This cmdlet forces a recalculation of the Resultant Set of Policies (RSOP) by contacting Active Directory, reading the policies to be applied to the device and user. Once this is calculated, the server caches the policy set and delivers it during the next device management session.</i></p>
<p><b>Complete the following task on:</b></p> <p> <b>MDMCLIENT</b></p> <p><b>7. Using the MDM ConnectNow Tool</b></p>	<p><i>Note: The <b>MDM ConnectNow</b> tool is a client application from the <b>Mobile Device Manager Resource Kit</b>. More information on this tool can be found on Microsoft Technet.</i></p> <ul style="list-style-type: none"> <li>a. Switch to the <b>MDMCLIENT</b> virtual machine.</li> <li>b. On the mobile device emulator, enter the <b>PIN (4123)</b>, and click <b>Unlock</b>.</li> </ul>

Tasks	Detailed Steps
<p><b>to Force Synchronization</b></p>	<p><b>c.</b> Reset the ActiveSync Connection by right-clicking the device in the <b>Device Emulator Manager</b> and clicking <b>Uncradle</b>, and then right-clicking the device again and clicking <b>Cradle</b>.</p> <p><i>Note: Click <b>OK</b> or <b>Cancel</b> on any warnings that may come up from ActiveSync, warning about a new partnership.</i></p> <p><b>d.</b> On the mobile device emulator, enter the <b>PIN (4123)</b>, and click <b>Unlock</b>.</p> <p><b>e.</b> In <b>Programs</b>, click the icon for the <b>MDM ConnectNow</b> program.</p> <p><b>f.</b> In the <b>MDM ConnectNow</b> program, click <b>Connect Now</b> to initiate a connection with the Mobile Device Manager.</p> <p><b>g.</b> Wait for the <b>Last Connection Status</b> to display <b>Success</b> and then close the <b>MDM ConnectNow</b> application.</p> <p><i>Note: It may take several minutes for the tool to display progress. If the mobile device does not display progress for a long time, it can be soft-reset by going to the <b>File</b> menu of the emulator window, selecting the <b>Reset</b> submenu and clicking <b>Soft</b>. Once this is done, reset the ActiveSync Connection by right-clicking the device in the <b>Device Emulator Manager</b> and clicking <b>Uncradle</b>, and then right-clicking the device again and clicking <b>Cradle</b>.</i></p> <p><i>Note: You may need to run the tool more than once for the policies to take effect.</i></p> <p><b>h.</b> To track the progress of the application that is being pushed out to the device, click <b>Start   Settings</b> and then click on the <b>System</b> tab.</p> <p><b>i.</b> On the <b>System</b> tab, click <b>Managed Programs</b>.</p> <p><b>j.</b> In the <b>Managed Programs</b> application, you can view the progress by clicking <b>Downloading now...</b> or viewing the <b>Installation History</b>.</p> <p><i>Note: You may need to run the <b>MDM ConnectNow</b> tool more than once for the software to be deployed.</i></p>

# Exercise 7: Using the System Center Mobile Device Manager Console to Wipe a Device

## Scenario

One of the advantages of centrally managing devices is the ability to control what data they have on them at any given time. In the event of a lost or stolen device, we can use the Mobile Device Manager Console to issue the command to wipe the device. If the device is connected to the corporate network (or through the VPN in the case of an external device), at the next device management session, the device will be hard-booted, wiping any and all data. This coupled with a PIN and encryption means that even if the device is taken off-site and away from the network, strong security protects the data. In this exercise, we don't want to wait for the next device management session, so we initiate a session using the MDM ConnectNow tool.

Tasks	Detailed Steps
<p><b>Complete the following task on:</b></p> <p> <b>MDMCORE</b></p> <p><b>1. Performing Device Wipes Using the Mobile Device Manager Administration Console</b></p>	<ol style="list-style-type: none"> <li>a. Switch to the <b>MDMCORE</b> computer</li> <li>b. Double-click the <b>Mobile Device Manager Console</b> icon on the desktop, if it is not already open. In the navigation pane, expand the <b>Device Management</b> node.</li> <li>c. Select <b>All Managed Devices</b>. If the <b>Mobile Device Manager Console</b> was already open, select <b>All Managed Devices</b> and click the <b>Refresh</b> button.</li> <li>d. In the center pane, right-click the <b>MYDEVICE</b> device and then click <b>Wipe Now</b>.</li> <li>e. In the confirmation dialog box, click <b>Yes</b> to confirm that you want to wipe the device.</li> <li>f. Switch back to the <b>MDMCLIENT</b> virtual machine.</li> <li>g. On the mobile device emulator, unlock the device by entering the <b>PIN</b>, if locked, and then click <b>Start</b> and click <b>Programs</b>.</li> <li>h. In <b>Programs</b>, click the icon for the <b>MDM ConnectNow</b> program.</li> <li>i. In the <b>MDM ConnectNow</b> program, click <b>Connect Now</b> to initiate a connection with the <b>Mobile Device Manager</b>.</li> </ol> <p><i>Note: It may take several minutes for the tool to display progress. If the mobile device does not display progress for a long time, it can be soft-reset by going to the <b>File</b> menu of the emulator window, selecting the <b>Reset</b> submenu and clicking <b>Soft</b>. Once this is done, reset the <b>ActiveSync Connection</b> by right-clicking the device in the <b>Device Emulator Manager</b> and clicking <b>Uncradle</b>, and then right-clicking the device and clicking <b>Cradle</b>.</i></p> <p><i>Note: To view a list of recent device wipes, select <b>Recent Wipes</b> in the navigation pane in the <b>Mobile Device Manager Console</b> on the <b>MDMCORE</b> virtual machine. A list of managed devices and their wipe status will be displayed in the center pane.</i></p> <ol style="list-style-type: none"> <li>j. Once the <b>Last Connection Status</b> has changed to <b>Success</b>, the device will perform a hard reset, wiping all data.</li> <li>k. After the device has been reset, close the emulator by selecting <b>File   Exit</b> from the menu bar. In the <b>Device Emulator</b> prompt, select <b>No</b> to not save the emulator state before exiting.</li> </ol>