Lab LC18: Implementing SMS 2003 SP2 Features

**Objectives**
After completing this lab, you will be able to:

- Identify an SMS 2003 SP2 site.
- Implement fully qualified host name lookups for management point and distribution points.
- Implement Active Directory Security Group Discovery and target an application to a discovered security group.
- Use the SMS 2003 Account Review Tool to identify configurations to provide a more secure SMS 2003 environment.

**Prerequisites**
Before working on this lab, one virtual computer should be running as a Microsoft Windows Server 2003 computer installed as an SMS 2003 SP2 primary site server (SP2 Server VPC). A second virtual computer is booted as a Windows XP Professional client installed as an Advanced Client in the SMS 2003 SP2 site (SP2 Windows XP VPC).

**Estimated time to complete this lab: 75 minutes**
Exercise 0
Preparing the Virtual Computer Clients for the Lab

In this exercise, you will update the collection membership of the All Systems collection. When you do, you will see the SMSClient computer appear twice in the membership list. This is due to Virtual PC 2004 virtualizing the SMBios serial number of the host computer, which SMS detects as being different than the original SMBios serial number. Because of this, SMS generates a new GUID for the client, which causes a new record to be generated.

Note Complete this procedure from the primary site server computer only.

فك To update the collection membership
1. Log on as administrator with a password of password.
2. On the Start menu, click SMS Administrator Console.
   The SMS Administrator Console window appears.
3. In the console tree, expand Site Database, expand Collections, and then click All Systems.
   The members of the All Systems collection appear in the details pane. Notice that the site server computer (SMSServer) and the Windows XP Professional client computer (SMSClient) appear as members.
4. On the Action menu, point to All Tasks, and then click Update Collection Membership.
   The All Systems message box appears prompting to update subcollection membership.
5. Click OK, and then on the Action menu, click Refresh.
   The collection membership is updated, and the current membership of the All Systems collection is displayed. Notice that the SMSServer computer is now displayed twice. Notice also that one of the instances is listed as being Obsolete and inactive. This is the old reference of the client.
6. In the details pane, click the topmost record for the SMSClient computer, which should be listed as an Obsolete client (scroll to the right in the details pane) and then on the Action menu, click Delete.
   A Confirm Delete message box appears prompting to delete the record.
7. Click Yes.
   The collection membership is updated, and the current membership of the All Systems collection is displayed. Notice that the SMSClient computer is now displayed only once.
8. Delete any other obsolete records from the All Systems collection.
9. Update the membership of the All Windows XP Systems collection.
   This collection will be used later in this lab for targeting of an advertisement.
   You have now prepared your images for the lab and may proceed to Exercise 1.
Exercise 1
Identifying an SMS 2003 SP2 Installation

In this exercise, you will verify that your site is an SMS 2003 SP2 site.

Note Complete this procedure from the primary site server computer only.

To identify an SMS 2003 SP2 site installation

1. If not already running, on the Start menu, click SMS Administrator Console.
   The SMS Administrator Console window appears.

2. In the console tree, click Site Database, and then on the Action menu, click About Systems Management Server.
   The About Systems Management Server dialog box appears displaying information about the local site.

3. What version of SMS is displayed?
   SMS 2.50 SP2 (4160)

4. Click OK.

5. In the console tree, expand Site Database, and then click Site Hierarchy.
   The local site information appears in the details pane.

6. What version of SMS is installed on the local site?
   2.50.4160.2000 which is SMS 2003 SP2.
Exercise 2
Implementing Fully Qualified Host Names for SMS 2003 SP2

In this exercise, you will implement the new SMS 2003 SP2 feature that allows SMS 2003 SP2 Advanced Clients to resolve the management point and distribution point through fully qualified host names instead of NetBIOS names. You will begin by extending the Active Directory schema for SMS 2003 SP2, which is a requirement to use this feature.

**Note** Complete this procedure from the primary site server computer only.

لزم To extend the Active Directory schema for SMS 2003 SP2

1. Run C:\SP2CD\SMSSetup\Bin\I386\Extadsch.exe.
   A command prompt window appears as you extend the Active Directory schema for use by SMS.
2. Open C:\Extadsch.log.
   Notepad displays the contents of the Extadsch.log file. This file is created by the Extadsch.exe utility and reports on the Active Directory schema extension process.
3. Was the schema extension process successful?
   Yes

4. Was any of the schema extension process already run prior to you running the utility?
   Yes, as indicated by the “already exists” entries on most of the attributes and classes the utility is trying to create.

5. Was anything added to the schema extension process as a result of you running the SMS 2003 SP2 version of the schema extension utility?
   Yes, as indicated by the “Successfully updated class LDAP://cn=MS-SMS-Management-Point,CN=Schema,CN=Configuration” entry in the log file.

6. Verify that there are no errors listed in the log, and then close Notepad.
   Your site is now prepared for publishing of a fully qualified host name for the management point and distribution point.
In the following procedure, you will configure SMS to publish a fully qualified host name to Active Directory.

**Note** Complete this procedure from the primary site server computer only.

✔️ To publish a fully qualified host name for SMS

1. If not already started, start the **SMS Administrator Console**.
   The SMS Administrator Console window appears.

2. In the console tree, expand **Site Database**, expand **Site Hierarchy**, expand **MCM**, expand **Site Settings**, and then click **Site Systems**.
   The list of site systems for the local site appears. Notice that there is only one site system in the local SMS site, SMSServer.

3. In the details pane, click **SMSServer**, and then on the **Action** menu, click **Properties**.
   The **\SMSServer Site System Properties** dialog box appears displaying general information for the site system. Notice that you can specify a fully qualified host name on this tab.

4. Does SMS 2003 SP2 specify a fully qualified host name by default?
   No

5. Click **Specify a Fully Qualified Host Name**.
   Notice that the “Fully Qualified Host Name” field becomes available.

6. What is the default fully qualified host name?
   The **NetBIOS name of the site system, in this case, SMSSERVER.**

7. In the **Fully Qualified Host Name** box, type
   `smsserver.smsdomain.smsdemo.microsoft.com` and then click **OK**.
   The SMS Administrator Console window appears.

In the following procedure, you will verify that SMS published the fully qualified host name by viewing an SMS log file.

**Note** Complete this procedure from the primary site server computer only.

✔️ To verify the publishing of the fully qualified host name

1. Open `C:\SMS\Logs\Sitecomp.log`
   Notepad displays the contents of the Site Component Manager log file.
2. Search for `smsserver.smsdomain`.
   Notepad displays the first occurrence of the fully qualified host name (it actually publishes the full name). Notice that on lines around the highlighted text you will see entries for:
   - SMSServer is the default MP
   - Publishing SMSServer as a management in Active Directory
   - About to update MP object in AD MP (and lists the fully qualified host name)

   These are entries that indicate the publishing of the fully qualified host name into Active Directory.


In the following procedure, you will verify that SMS published the fully qualified host name at the SMS 2003 SP2 Advanced Client computer.

Note: Complete this procedure from either of the Advanced Client computers.

To verify the publishing of the fully qualified host name at the client:

1. Log on as **administrator** with a password of **password**.
2. In **Control Panel**, start **Administrative Tools**, and then start **Services**.
   The Services window appears.
3. Under **Name**, click **SMS Agent Host**.
   SMS Agent Host is the service for the Advanced Client.
4. On the **Action** menu, click **Restart**.
   Restarting the SMS Agent Host service will cause the SMS 2003 SP2 Advanced Client computer to search for the default management point using a fully qualified host name.
5. Open `C:\Windows\System32\Ccm\Logs\LocationServices.log`.
   Notepad displays the contents of the LocationServices log file.
   Notepad displays the first occurrence of the fully qualified host name. Notice that this is the result of the client searching for its default management point.
7. Close Notepad.

You have now verified that the SMS 2003 SP2 Advanced Client computer has discovered its default management point using the management point’s fully qualified host name. You will verify that the client will access a distribution point via fully qualified host name in the next exercise.
Exercise 3
Implementing Active Directory Security Group Discovery

In this exercise, you will implement the new SMS 2003 SP2 feature for discovery of security groups from Active Directory.

**Note** Complete this procedure from the primary site server computer only.

To discover Active Directory security groups

1. In the console tree, expand Site Database, expand Site Hierarchy, expand MCM, expand Site Settings, and then click Discovery Methods.

   The list of discovery methods for the local site appears. Notice that there is a new discovery method for SMS 2003 SP2, Active Directory Security Group Discovery.

2. In the details pane, click Active Directory Security Group Discovery, and then on the Action menu, click Properties.

   The Active Directory Security Group Discovery Properties dialog box appears.

3. Select Enable Active Directory Security Group Discovery, and then click New (the New button resembles a start burst icon).

   The Browse for Active Directory dialog box appears allowing you to specify the use of a local domain, local forest, or custom query for the discovery. Notice the options available include recursive searches (enabled by default) and nested groups (not enabled by default).

4. Verify that Local domain is selected, and then click OK.

   The Select New Container dialog box appears allowing you to specify the container to use for discovery.

5. Select the local domain, and then click OK.

   The Active Directory Security Group Discovery Properties dialog box appears. Notice the distinguished name for the container to search. Also notice that a recursive search will be performed on that container, but that nested groups are excluded.

6. Click the Polling Schedule tab.

   The Active Directory Security Group Discovery Properties dialog box displays the default polling schedule for Active Directory Security Group Discovery. Notice that by default, this polling will occur daily.

7. Click Schedule.

   The Schedule dialog box appears.

8. Under Recurrence pattern, click None, and then click OK.

   The Active Directory Security Group Discovery Properties dialog box appears displaying the new schedule.

9. Click Run discovery as soon as possible and then click OK.

   The SMS Administrator Console window appears.
In the following procedure, you will verify the results of the Active Directory Security Group Discovery process.

Note You will need to wait for a moment for the discovery process to complete.

To verify Active Directory Security Group Discovery
1. In the console tree, click Collections. 
   The list of collections appears in the details pane.
2. Are there any new collections created for SMS 2003 SP2? 
   Yes, there is a default collection for All Active Directory Security Groups.
3. In the console tree, expand Collections, and then click All Active Directory Security Groups. 
   The member of the All Systems collection appears in the details pane. Notice that there are no members of the collection.
4. On the Action menu, point to All Tasks, and then click Update Collection Membership. 
   The All Active Directory Security Groups message box appears prompting to update subcollection membership.
5. Click OK. 
   The collection is updated. Notice the hourglass icon next to the All Active Directory Security Groups collection. This indicates the collection must be refreshed to display updated membership information.
6. On the Action menu, click Refresh. 
   The collection membership is updated, and the current membership of the All Active Directory Security Groups collection is displayed.
7. Are there any new members in the All Active Directory Security Groups collection? 
   Yes, 19 different AD security groups should have been discovered.
In the following procedure, you will create a new collection to be used for software distribution based on an Active Directory security group.

**Note** Complete this procedure from the primary site server computer only.

✔ **To create a new collection**

1. In the console tree, click **Collections**, and then on the **Action** menu, point to **New**.
   
   A new menu appears.

2. Click **Collection**.

   The **Collection Properties** dialog box appears.

3. In the **Name** box, type **Domain Users** and then click the **Membership Rules** tab.

   The **Collection Properties** dialog box appears displaying the membership rules for the collection. Notice that by default there are no membership rules for the collection.

4. Click **New Query Rule** (the **New Query Rule** button resembles a disk drive icon).

   The **Query Rule Properties** dialog box appears allowing you to configure the query to be used as the membership rule.

5. In the **Name** box, type **Domain Users**

6. In the **Resource class** box, click **User Group Reference**, and then click **Edit Query Statement**.

   The **Domain Users Query Statement Properties** dialog box appears allowing you to configure the query to be used as the membership rule.

7. Click the **Criteria** tab.

   The **Domain Users Query Statement Properties** dialog box appears allowing you to configure the query to be used as the membership rule. Notice that there are no query rules by default.

8. Click **New** (the **New** button resembles a start burst icon).

   The **Criterion Properties** dialog box appears allowing you to configure the query.

9. Click **Select**.

   The **Select Attribute** dialog box appears allowing you to select the attribute to query on.

10. In the **Attribute class** box, click **User Group Resource**.

11. In the **Attribute** box, click **Name**, and then click **OK**.

    The **Criterion Properties** dialog box appears allowing you to configure the query. Notice that it displays the attribute class and attribute selected.

12. Click **Values**.

    The **Values** dialog box appears displaying the discovered user group names.

13. Click **SMSDomain\Domain Users**, and then click **OK**.

    The **Criterion Properties** dialog box appears allowing you to configure the query. Notice that configured query is displayed.
14. Click OK.
   The Domain Users Query Statement Properties dialog box appears displaying the configured query statement.

15. Click OK.
   The Query Rule Properties dialog box appears.

16. Click OK.
   The Collection Properties dialog box appears. Notice that the Domain Users membership rule is listed.

17. Click OK.
   The Query Rule Properties dialog box appears.
   The list of collections appears. Notice the new collection appears.

18. In the console tree, click Domain Users, and then on the Action menu, click Refresh.
   The list of collection members appears in the details pane. Notice that the collection includes one member that being the Domain Users group from the domain and that the membership list does not display each individual member of the Domain Users group as would happen with other discovery methods.

In the following procedure, you will use the Distribute Software wizard to distribute a program to the new collection.

**Note**  Complete this procedure from the primary site server computer only.

To distribute the application

1. In the console tree, click the Domain Users collection, and then on the Action menu, point to All Tasks.
   A new menu appears.

2. Click Distribute Software.
   The Distribute Software to Collection Wizard dialog box appears.

3. Click Next.
   The Distribute Software to Collection Wizard Package dialog box appears providing options for package distribution.

4. Select Create a new package from a definition, and then click Next.
   The Distribute Software to Collection Wizard Package Definition dialog box appears allowing you to select the package definition file to use.

5. Click Browse.
   The Open dialog box appears.

6. Open C:\SMSTools\SMS Toolkit\SMS2003Toolkit2.msi.
   The Distribute Software to Collection Wizard Package Definition dialog box appears allowing you to select the package definition file to use. Notice that SMS 2003 Toolkit 2 has been added to the list.
7. Under **Package definition**, verify that **SMS 2003 Toolkit 2** is selected, and then click **Next**.

   The **Distribute Software to Collection Wizard Source Files** dialog box appears prompting for source file handling instructions.

8. Click **Always obtain files from a source directory**, and then click **Next**.

   The **Distribute Software to Collection Wizard Source Directory** dialog box appears allowing the designation of the source file directory.

9. Click **Local drive on site server**, and then click **Browse**.

   The **Browse for Folder** dialog box appears.

10. Click **C:\SMSTools\SMS Toolkit**, and then click **OK**.

    The **Distribute Software to Collection Wizard Source Directory** dialog box displays the designated source directory.

11. Click **Next**.

    The **Distribute Software to Collection Wizard Distribution Points** dialog box appears allowing the designation of distribution points to store the package files.

12. Under **Distribution Points**, select **SMSServer**, and then click **Next**.

    The **Distribute Software to Collection Wizard Select a Program to Advertise** dialog box appears allowing the configuration of advertisements.

13. Under **Programs**, click **Per-system unattended**, and then click **Next**.

    The **Distribute Software to Collection Wizard Advertisement Name** dialog box appears prompting for a name and comment for the advertisement.

14. Click **Next** to accept the default name.

    The **Distribute Software to Collection Wizard Advertise to Subcollections** dialog box appears prompting for advertising to subcollections.

15. Select **Advertise the program only to members of the specified collection**, and then click **Next**.

    The **Distribute Software to Collection Wizard Advertisement Schedule** dialog box appears prompting for a start and expiration time for the advertisement.

16. After **Advertise the program after**, verify that the current date and time is displayed.

17. Verify **No. This advertisement never expires** is selected, and then click **Next**.

    The **Distribute Software to Collection Wizard Assign Program** dialog box appears prompting for program assignments.

18. Verify that **No. Do no assign the program** is selected, and then click **Next**.

    The **Distribute Software to Collection Wizard** dialog box appears prompting to complete the wizard.

19. Click **Finish**.
In the following procedure, you will force the Advanced Client to check for new policies, which will include the advertisement to install the SMS 2003 Toolkit 2 in an unattended installation.

**Note** Complete this procedure from the Windows XP Advanced Client computer only.

❗️ **To run the advertised program on the client**

1. In **Control Panel**, start **Systems Management**.
   
The **Systems Management Properties** dialog box appears.

2. Click the **Actions** tab.
   

3. Click **User Policy Retrieval & Evaluation Cycle**, and then click **Initiate Action**.
   
The Advanced Client will request new policies, which will include the policy related to the advertised program. A **User Policy Retrieval & Evaluation Cycle** message box appears indicating the action was initiated, and may take several minutes to complete.

4. Click **OK**.
   
The **Systems Management Properties** dialog box appears.

5. Click **OK**.
   
   It will take two minutes for SMS to evaluate and implement the new policies. When that has completed, the **New Program Available** notification bubble appears in the System Tray.

6. In the System Tray, double-click the **New Program Available** icon.
   
The Run Advertised Program window appears. Notice the SMS 2003 Toolkit 2 program appears in the list.

7. Under **Program Name**, click **Microsoft Corporation SMS 2003 Toolkit 2**, and then click **Run**.
   
The Run Advertised Program window appears.

8. Click **Close**.
   
   This is a silent install, so no user interface will appear. To verify the installation, you can use advertisement status, or look to see if the new program group for the SMS 2003 Toolkit has been created on the client.

9. On the **Start** menu, point to **All Programs**.
   
   A new menu appears. Notice the menu created for SMS 2003 Toolkit 2. This indicates the unattended installation was successful using SMS software distribution targeted to a security group.
10. Open C:\Windows\System32\Ccm\Logs\LocationServices.log.
   Notepad displays the contents of the LocationServices log file.

11. Search for distribution point.
   Notepad displays the first occurrence of the search for a distribution point. Notice that following this entry is the result of the client searching for its distribution point to use for accessing the program source files. Notice that the request was resolved using the fully qualified host name of the distribution point.

   You have now verified that the SMS 2003 SP2 Advanced Client computer has resolved the distribution point using the computer’s fully qualified host name.
Exercise 4
Reviewing SMS Accounts with the Account Review Tool

In this exercise, you will use the SMS 2003 Account Review Tool to analyze your site to determine if there are any accounts implemented that are not required for your site.

**Note** Complete this exercise from the primary site server computer only.

**To install the SMS 2003 Account Review Tool**


   The **Choose Directory For Extracted Files** dialog box appears prompting for the folder to extract the SMS 2003 Account Review Tool files to. The preferred location to extract the Account Review Tool is the SMS\Bin\I386 folder.

2. In the **Choose Directory For Extracted Files** box, type C:\SMS\Bin\I386 and then click **OK**.

   Files are extracted. When complete, an **Extraction Complete** message box appears indicating the extraction process was successful.

3. Click **OK**.

In the following procedure, you will run the SMS 2003 Account Review Tool to identify accounts that are no longer required.

**To run the SMS 2003 Account Review Tool**

1. Start C:\SMS\Bin\I386\ART.exe.

   The SMS 2003 Account Review Tool window appears.

2. Click **Next**.

   The **SMS 2003 Account Review Tool Read the following Microsoft Software Licensing Terms** dialog box appears displaying the end user license agreement for the SMS 2003 Account Review Tool.

3. Read the license agreement, and then click **I accept the Terms of the Software License Agreement**.

4. Click **Next**.

   The SMS 2003 Account Review Tool runs. When complete, the **SMS 2003 Account Review Tool Account Review Wizard Completed with Warnings** dialog box appears indicating the tool ran, but identified warnings for the site.

5. Click **View Details**.

   An Internet Explorer window appears displaying the **SMS 2003 Account Review Tool report** information.
6. What warnings did the SMS 2003 Account Review Tool identify?

Use of the Advanced Client Network Access account (in use, may not be needed, and configured as a domain admin account), the Site Address account is used and needs to be a member of the Site to Site Connection group, the Client Push Installation Account is in use (may not be required, and has domain admin rights), use of the Client Connection Account (only needed for support of Legacy Clients), use of the Legacy Client Software Installation Account (only needed in some scenarios to support Legacy Clients), secure key exchange is not enabled, Advanced Client data signing is not enabled, Advanced Client data encryption is not enabled, and the SMS site is configured to use the default HTTP port.


The SMS 2003 Account Review Tool Account Review Tool Completed with Warnings dialog box appears.

8. Click Finish.

You have now identified a number of issues in the configuration of the SMS site. You will resolve these issues in the remainder of this lab, and then verify those that can be resolved are not reported as warnings any longer.

In the following procedure, you will resolve issues with SMS Legacy Client accounts that the SMS 2003 Account Review Tool identified as warnings.

To resolve SMS Legacy Client account issues

1. In the console tree of the SMS Administrator Console window, expand Site Database, expand Collections, and then click All Systems.

   The members of the All Systems collection appear in the details pane.

2. What client types are installed in the local SMS site?

   There are only two Advanced Clients, and no Legacy Clients.

As there are no Legacy Clients in the site, there is no requirement for any accounts that are only used by Legacy Clients.
3. In the console tree, expand Site Hierarchy, expand MCM, expand Site Settings, and then click Component Configuration.
   The list of configurable components appears in the details pane.

4. In the details pane, click Software Distribution, and then on the Action menu, click Properties.
   The Software Distribution Properties dialog box appears. Notice that both a Legacy Client Software Installation Account and an Advanced Client Network Access Account are configured. As there are no Legacy Clients in the site, the Legacy Client Software Installation Account is not needed.

5. Under Legacy Client Software Installation Account, click Clear.
   A Confirm Account Delete message box appears prompting for confirmation to delete the account.

6. Click Yes.
   The Software Distribution Properties dialog box appears. Notice that now only an Advanced Client Network Access Account is configured for the site.

7. Click OK.
   The SMS Administrator Console window appears.

8. In the console tree, expand Connection Accounts, and then click Client.
   The list of SMS Client Connection accounts appear in the details pane. These accounts are only used by Legacy Clients and not Advanced Clients.

9. In the details pane, click SMSDomain\SMSClient, and then on the Action menu, click Delete.
   A Confirm Delete message box appears indicating it is not recommended to delete the last SMS Client Connection Account. However, as there are no Legacy Clients in the site, this account is no longer required.

10. Click Yes.
    The list of SMS Client Connection accounts appear in the details pane. Notice that there are no longer any accounts listed.

11. On the Start menu, point to Administrative Tools, and then click Active Directory Users and Computers.
    The Active Directory Users and Computers window appears.

12. In the console tree, expand smsdomain.smsdemo.microsoft.com, and then click Users.
    The Active Directory Users and Computers window displays the list of accounts in the domain. Notice the accounts that were used for the Legacy Client Software Installation Account (smsinstall) and the Client Connection Account (smsclient) are listed.

13. Delete both the SMSInstall and SMSClient accounts.
In the following procedure, you will resolve issues with other SMS accounts that the SMS 2003 Account Review Tool identified as warnings.

✔ **To resolve other SMS account issues**

1. In the details pane of the Active Directory Users and Computers window, click ACNA, and then on the Action menu, click Properties.

   The ACNA Properties dialog box appears.

2. Click the Member Of tab.

   The ACNA Properties dialog box displays the groups that ACNA is a member of. Notice that it is a member of Domain Admins, which is not a requirement.

3. Remove the Domain Admins membership for the Advanced Client Network Access Account, and then click OK.

   If you were sure you would not need this account, you could remove it from the SMS site configuration and the domain. You should only need it if you had Advanced Clients in non-trusted domains or in workgroup scenarios. For our lab, you will leave the account in the domain and SMS site to verify that the SMS 2003 Account Review Tool identifies it appropriately.

4. In the details pane, click SMS Push Installation Account, and then on the Action menu, click Properties.

   The SMS Push Installation Account Properties dialog box appears.

5. Click the Member Of tab.

   The SMS Push Installation Account Properties dialog box displays the groups that SMS Client Push Installation account is a member of. Notice that it is a member of Domain Admins, which is not a requirement.

6. Remove the Domain Admins membership for the SMS Client Push Installation Account, and then click OK.

   You would now need to ensure that the account was configured as a local admin on each computer that the SMS site server would need to push the SMS client installation to.

   If you were sure you would not need this account, you could remove it from the SMS site configuration and the domain. For our lab, you will leave the account in the domain and SMS site to verify that the SMS 2003 Account Review Tool identifies it appropriately.

7. In the details pane, click Remotesite, and then on the Action menu, click Properties.

   The Remotesite Properties dialog box appears.

8. Click the Member Of tab.

   The Remotesite Properties dialog box displays the groups that remotesite is a member of. Notice that it is a member of Administrators, which is not a requirement. In fact, if possible, you should not even use a user account for the site address account, but rather the computer account.
9. Delete the Remotesite account from the domain.
   You will now configure the site address to use the computer account of the
   site server instead of the remotesite account. To complete the configuration
   of this account, you’d need to add the local site server account (SMSServer)
   to the SMS_SiteToSiteConnection group of the remote SMS site (which
   there is not one for this lab).

10. Close the Active Directory Users and Computers window, and then return to
     the SMS Administrator Console.
     The SMS Administrator Console window appears.

11. In the console tree, click **Addresses**.
     The list of addresses configured in the site appears in the details pane.
     Notice the address to the remote site CHD. You can’t change the address to
     use the computer account when it is configured to use a user account, so you
     must delete and then recreate it.

12. In the details pane, click CHD, and then on the **Action** menu, click **Delete**.
     A **Confirm Delete** message box appears.

13. Click **Yes**.
     The list of addresses configured in the site appears in the details pane.
     Notice that there are no addresses configured for the site. You will now
     create a new address for CHD, and configure it to use the computer account.

14. On the **Action** menu, point to **New**, and then click **Standard Sender
     Address**.
     The **Standard Sender Address Properties** dialog box appears.

15. In the **Destination site code** box, type CHD

16. In the **Site server name** box, type SMSAdd
     Notice the message that states if no user account is configured, the site
     server computer account will be used.

17. Click **OK** to use the site server computer account.
     The list of addresses configured in the site appears in the details pane.
     Notice that new address for CHD appears.

In the following procedure, you will the resolve issues identified by the SMS
2003 Account Review Tool in terms of site configuration.

⚠️ **To resolve SMS configuration issues**

1. In the console tree, click **MCM**, and then on the **Action** menu, click
   **Properties**.
   The **MCM – SMS 2003 Primary Site Site Properties** dialog box appears.

2. Click the **Advanced** tab.
   The **MCM – SMS 2003 Primary Site Site Properties** dialog box appears
   displaying advanced properties for the site.

3. Under **Site connection**, click **Require secure key exchange between sites**.
   This should resolve one issue identified by the SMS 2003 Account Review
   Tool.
4. Under **Inventory protection**, click **Sign data before sending to Management Point**.

   A **MCM – SMS 2003 SP1 Primary Site Site** dialog box appears indicating this change affects the Advanced Clients at the local site, as well as any child secondary site.

5. Click **Yes**.

   This should resolve another issue identified by the SMS 2003 Account Review Tool.

   The **MCM – SMS 2003 Primary Site Site Properties** dialog box appears displaying advanced properties for the site.

6. Under **Inventory protection**, click **Encrypt data before sending to Management Point**, and then click the **Ports** tab.

   The **MCM – SMS 2003 Primary Site Site Properties** dialog box appears displaying the port properties for the site.

7. What is the default port value?

   **Port 80**

8. Click **New** (the **New** button resembles a star burst icon).

   The **Port Detail** dialog box appears allowing the configuration of a new port.

9. In the **Description** box, type **Port 1337** and then in the **Port number** box, type **1337**

10. Click **Default client port**, and then click **OK**.

    A **Set Default Client Port** message box appears to configure the new port as the default client port.

11. Click **Yes**.

    The **MCM – SMS 2003 Primary Site Site Properties** dialog box appears displaying the port properties for the site. Notice that both the default port of 80 and the new port of 1337 are listed. It is important to retain the default port number until all clients in the site (and potentially hierarchy) are configured with the new port before removing the original port.

    If you were to fully complete this process, you would need to configure each Advanced Client in the local site, as well as those at any direct child secondary sites, to use the same port. You will not do so in this lab for time considerations.

12. Click **OK**.

    This should resolve another issue identified by the SMS 2003 Account Review Tool.

    The SMS Administrator Console appears.
In the following procedure, you will run the SMS 2003 Account Review Tool to verify that some of the issues identified earlier are no longer issues.

**Note** Wait a moment before beginning this procedure to allow the previous configurations to be implemented at the site.

🔗 **To run the SMS 2003 Account Review Tool**

1. Start `C:\SMS\Bin\I386\ART.exe`.
   
   The SMS 2003 Account Review Tool window appears.

2. Click **Next**.

   The SMS 2003 Account Review Tool runs. When complete, the **SMS 2003 Account Review Tool Account Review Wizard Completed with Warnings** dialog box appears indicating the tool ran, but identified warnings for the site.

3. Click **View Details**.

   An Internet Explorer window appears displaying the **SMS 2003 Account Review Tool report** information.

4. What warnings did the SMS 2003 Account Review Tool identify?

   **Use of the Advanced Client Network Access account** (in use and may not be needed, but no longer a warning about being configured as a domain admin account), and the **Client Push Installation Account is in use** (may not be required however no longer a warning about having domain admin rights).

5. Close the **SMS 2003 Account Review Tool report**.

   The **SMS 2003 Account Review Tool Account Review Tool Completed with Warnings** dialog box appears.

6. Click **Finish**.

   You have now resolved a number of issues in the configuration of the SMS site and verified that they are no longer reported as warnings any longer.

   Complete procedures for implementing Advanced Client signing and data encryption, and configuration of a new HTTP port are available in the lab “Implementing New SMS 2003 SP1 Features”.