Microsoft System Center 2012 Configuration Manager RTM Endpoint Protection Document

Mar.25 2012

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

1. Deploy Environment Introduction：

This operations process including three servers.

1. DC：

   Role：ADDS + ADCS

   OS：Windows Server 2008 R2 Enterprise Edition with SP1

   IE : IE 9.0

   IP : 192.168.0.100/24

   DNS: 192.168.0.100

2. ConfigMgr2012：

   Role：SC2012 ConfigMgr RTM + SC2012 ConfigMgr Database

   OS：Windows Server 2008 R2 Enterprise Edition with SP1

   IE : IE 9.0

   IP : 192.168.0.101/24

   DNS : 192.168.0.100

3. Client：

   Role：Domain Member and SC2012 ConfigMgr RTM Client

   OS：Windows 7 Enterprise Edition with SP1 x64

   IE : IE 9.0

   IP : 192.168.0.200/24

   DNS : 192.168.0.100

2. Deploy Active Directory：

1) Logon to **DC** server , installing **ADDS** and **ADCS** . Domain name is **Contoso.msft** . Active Directory forest functional level is **Windows Server 2008 R2**.

This process is no longer described in this part.

3. Deploy and Configure SC2012 ConfigMgr RTM：

1) This process is no longer described in this part. You can reference《**System Center 2012 Configuration Manager RTM Deployment Document**》.

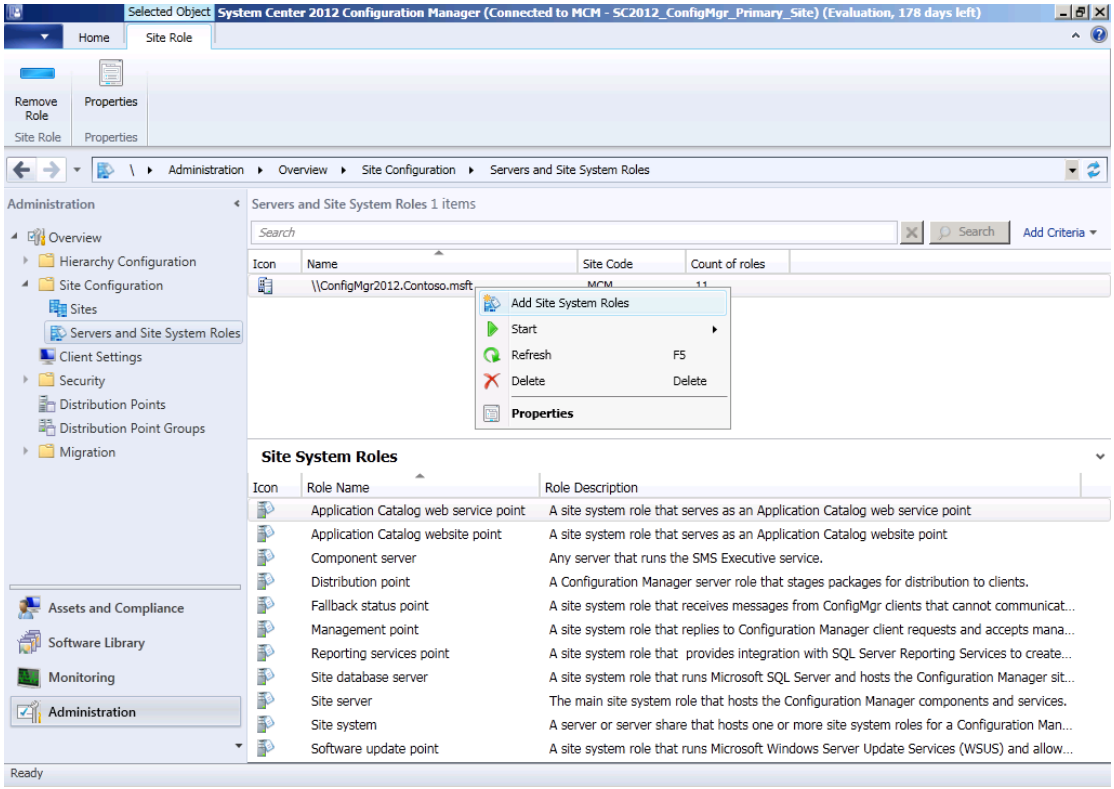
2) Default as you have already deployed and no any error.

3) SC2012 ConfigMgr RTM need to configuration , about this part , you can reference 《**System Center 2012 Configuration Manager RTM Configure Document**》

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

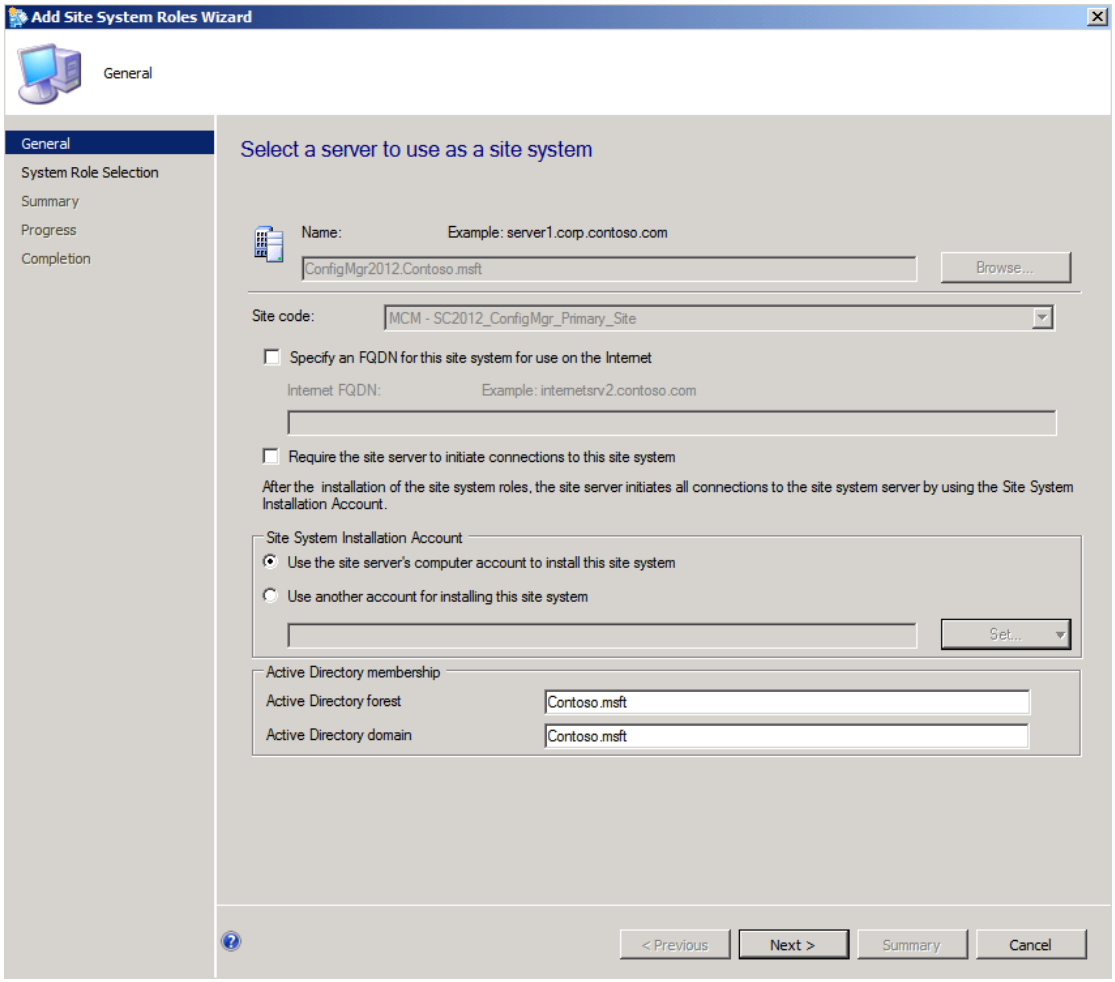
4. Enabling Endpoint Protection and Deploy Client :

1) Logon to **ConfigMgr2012** server , on the **Start** menu , point to **All Programs** , point to **Microsoft System Center 2012** , point to **Configuration Manager** , and then click **Configuration Manager Console** . Click the **Administration** workspace , in the navigation pane , expand **Site Configuration** , and then click **Servers and Site System Roles** , right-click site server and click **Add Site System Roles** :

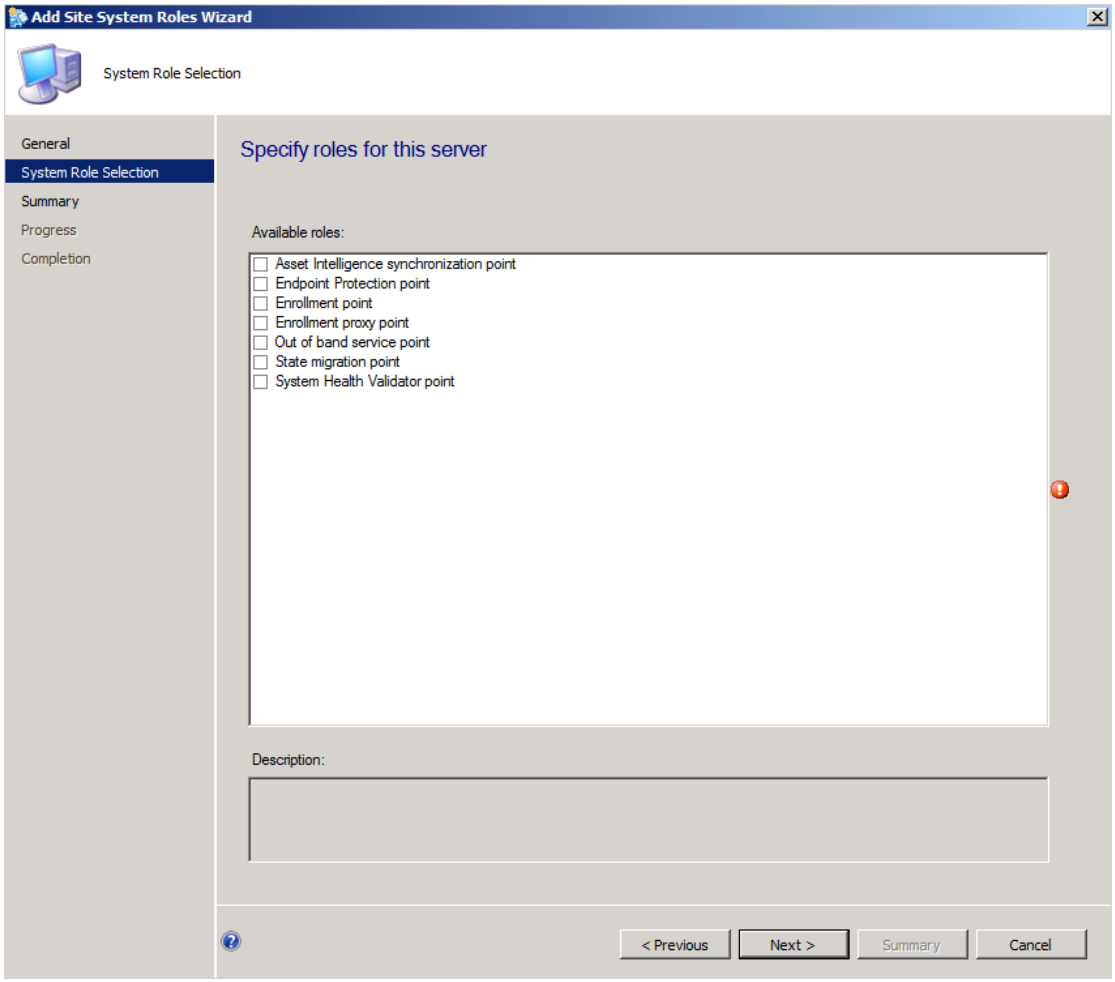


2) The **Add Site System Roles Wizard General** dialog box appears :

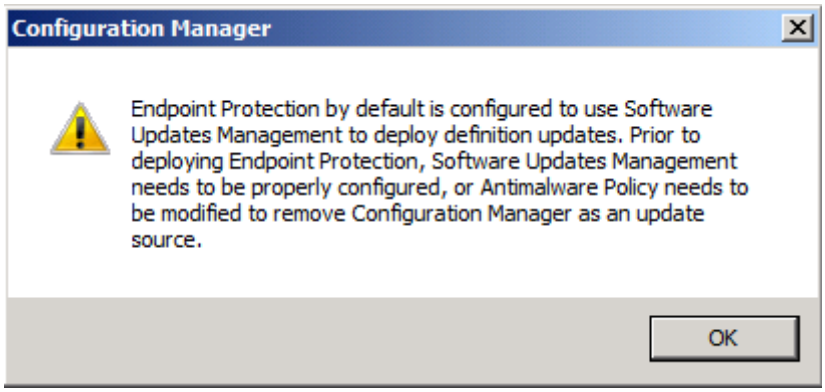
Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao



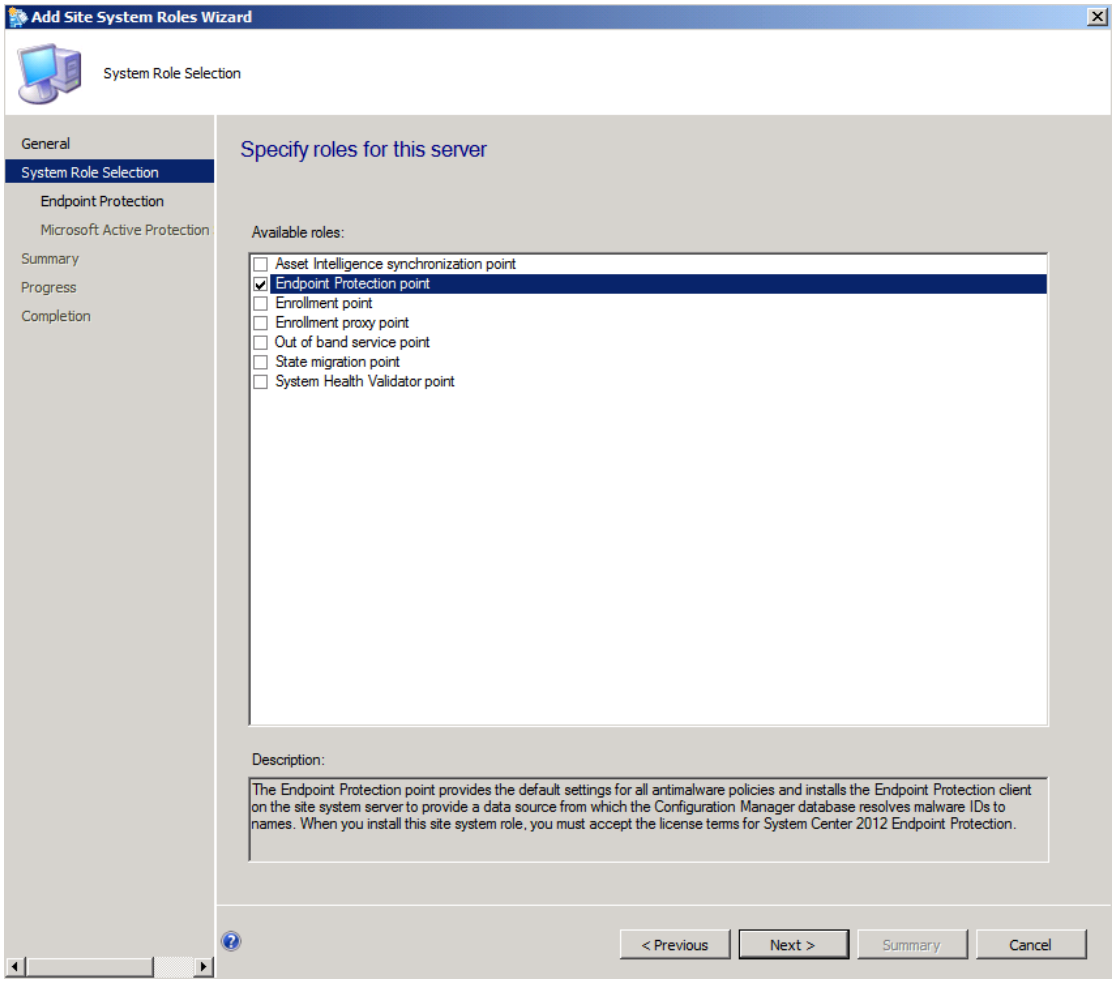
3) Click **Next** to accept the default configuration , the **System Role Selection** dialog box appears :



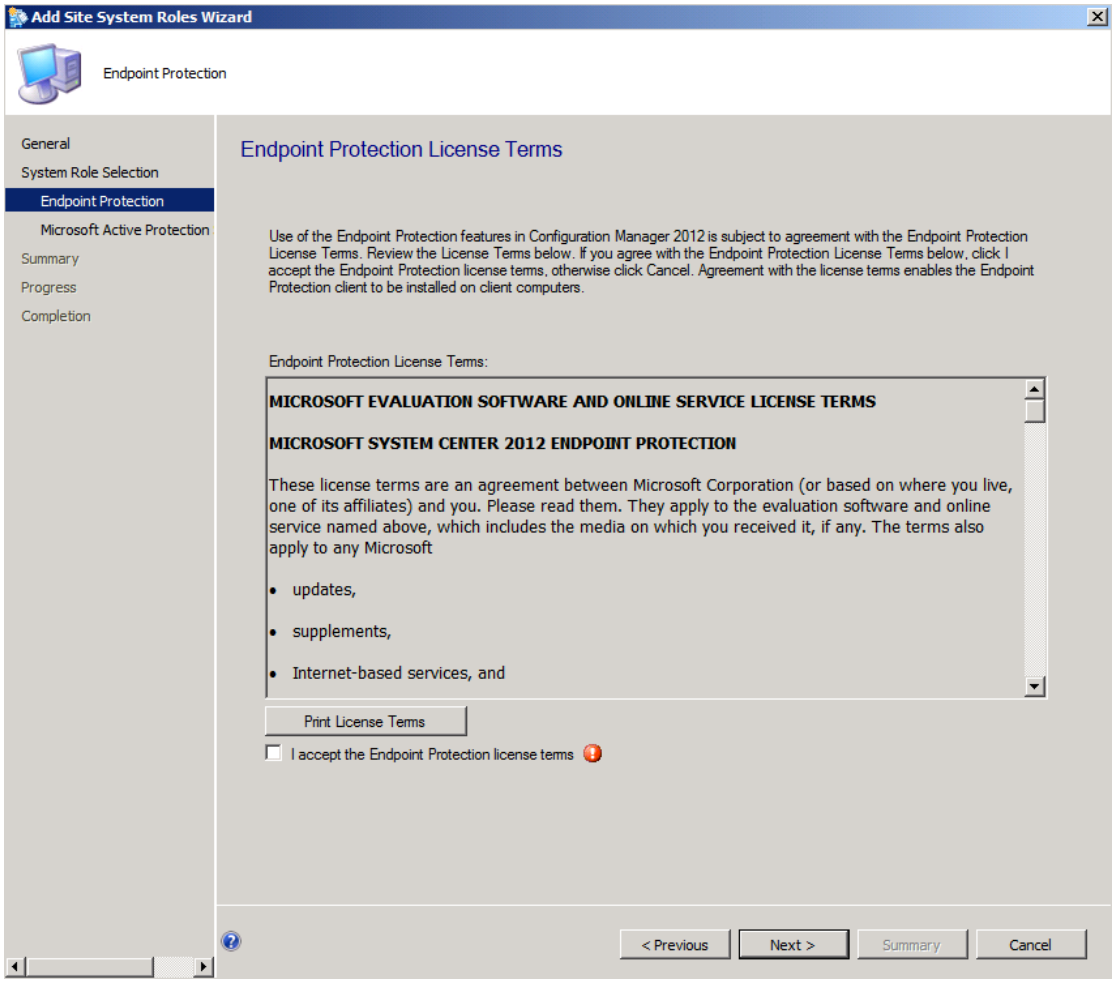
4) Under **Available roles** , select **Endpoint Protection point** , a **Configuration Manager** warning dialog box appears :



5) Click **OK** , will display select result :

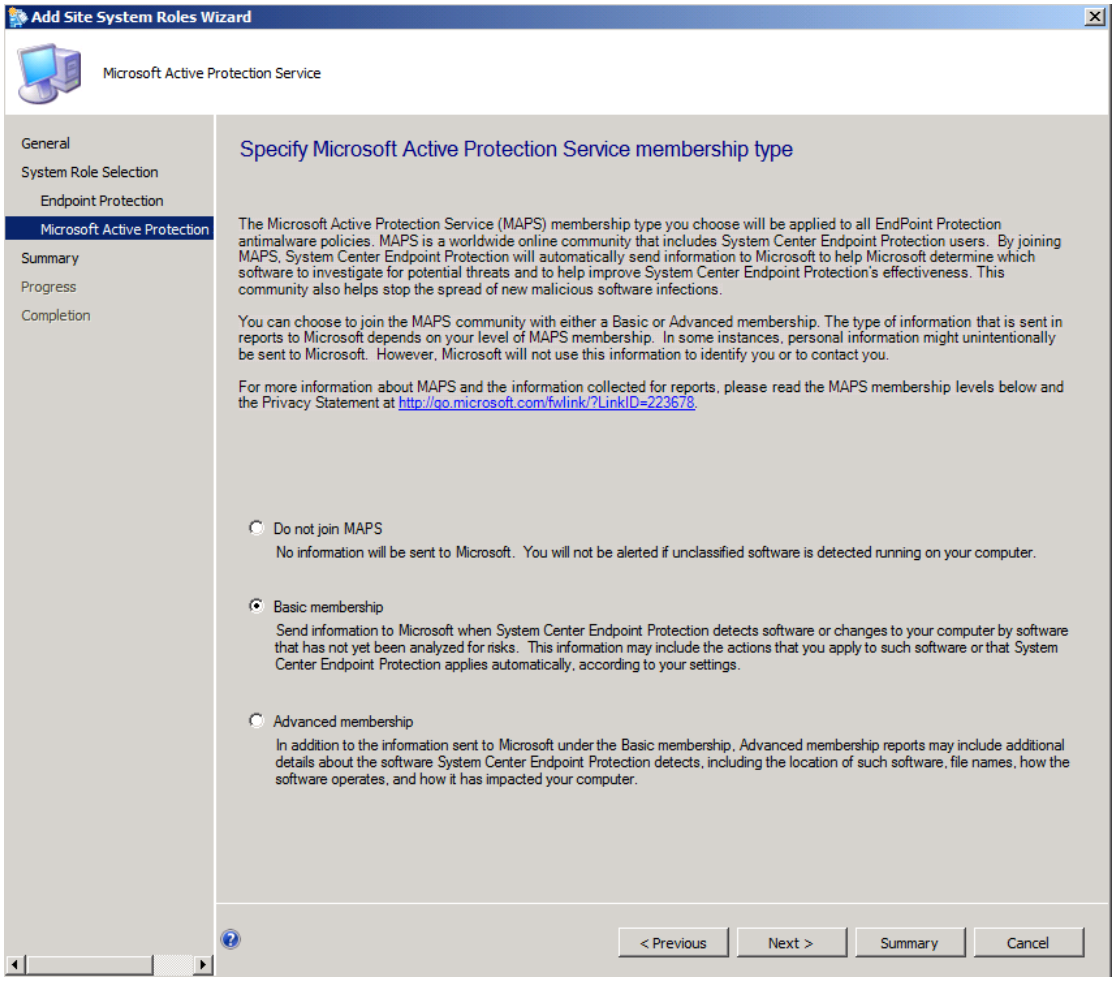


6) Click **Next** , the **Endpoint Protection** dialog box appears :

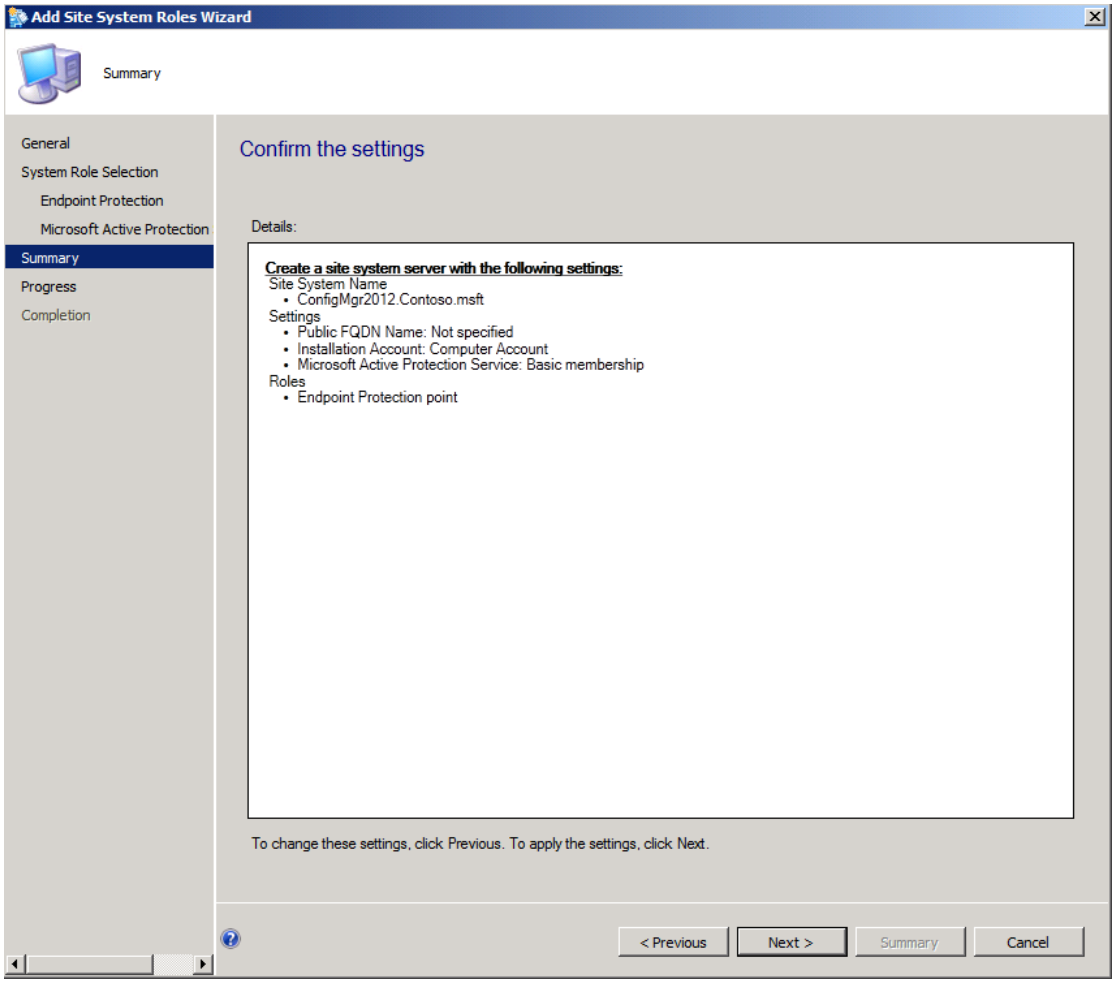


7) Select **I accept the Endpoint Protection license terms** , and click **Next** , the **Microsoft Active Protection Service** dialog box appears :

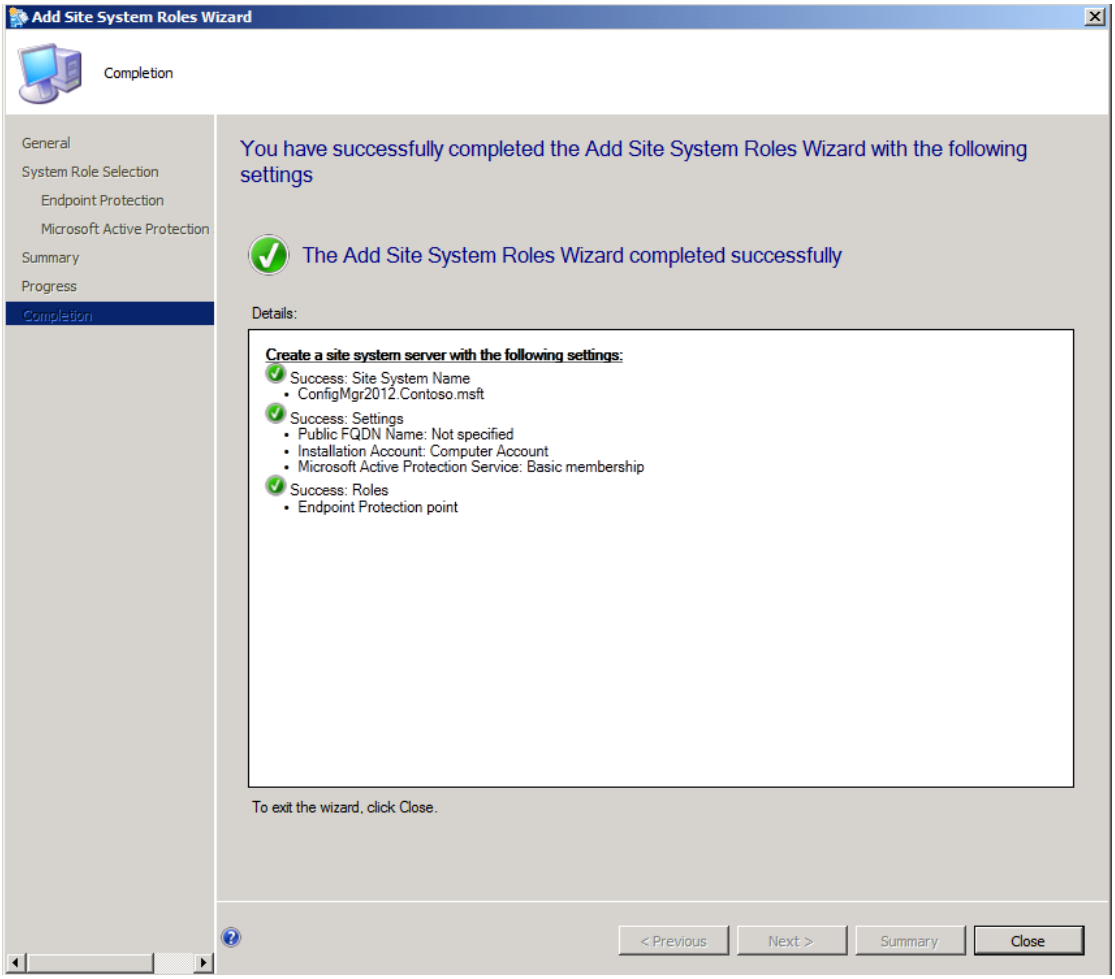
Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao



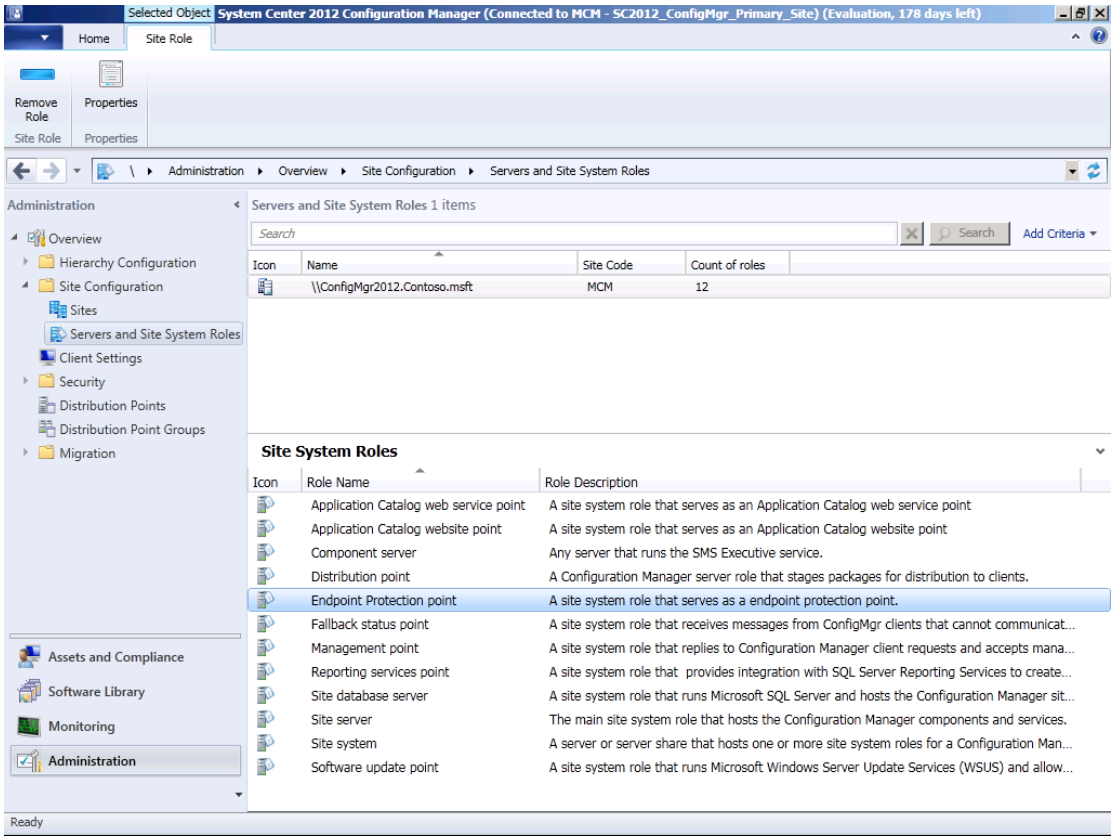
8) Select any item and click **Next** , the **Summary** dialog box appears :



9) Click **Next** , the **Completion** dialog box appears indicating that the wizard completed successfully :

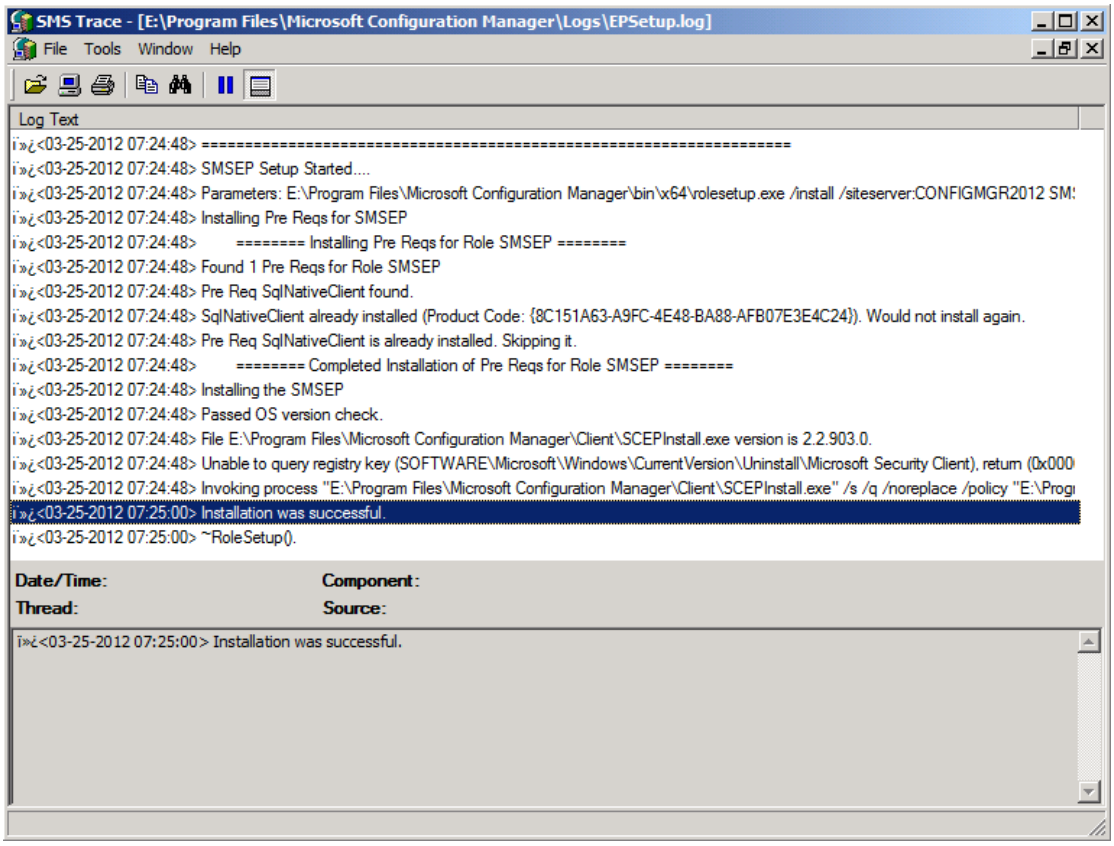


10) Click **Close** . You may need to refresh the list of **Site System Roles** on the site system to view the **Endpoint Protection point** site system role :

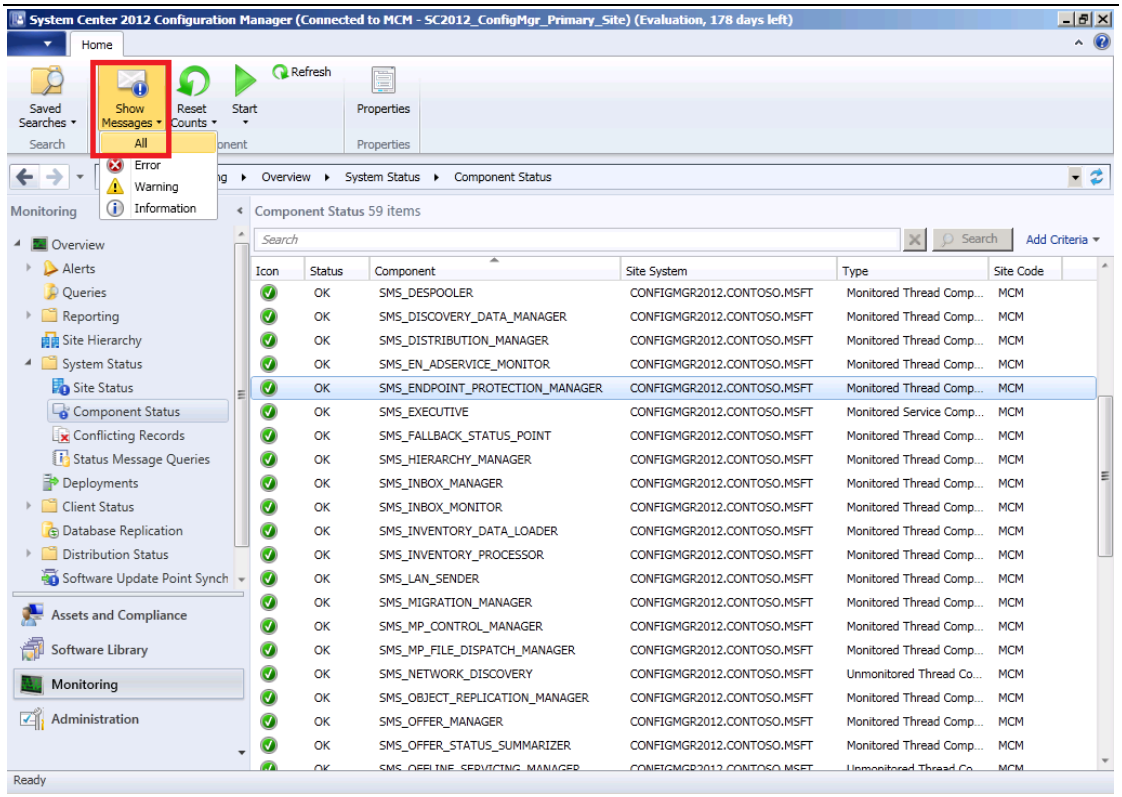


11) Open **EPSetup.log** , you can see the installation was successful :

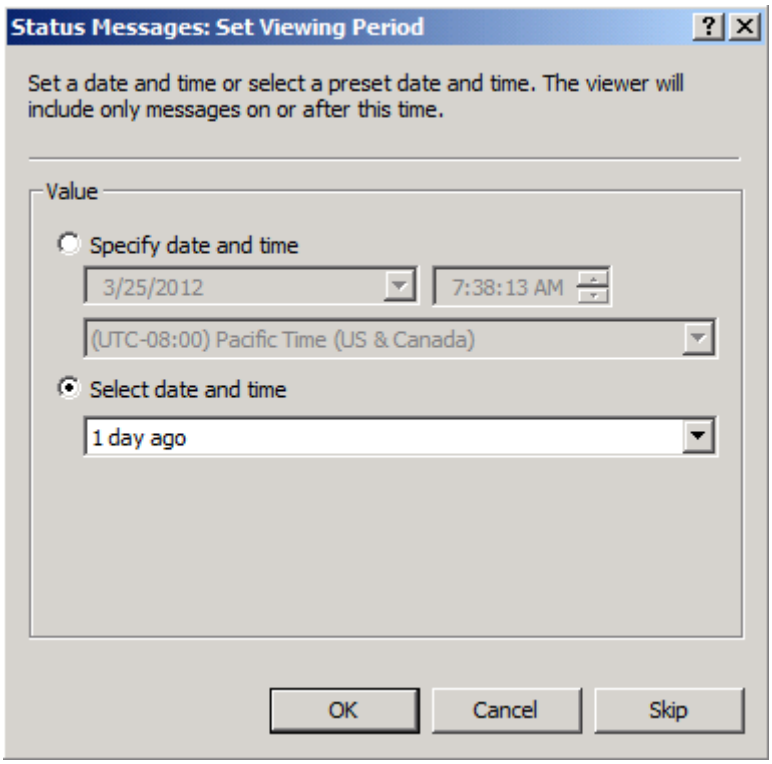
Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao



12) Click the **Monitoring** workspace , in the navigation pane , expand **System Status** , and then click **Component Status** , click **SMS_ENDPOINT_PROTECTION_MANAGER** , and the on the **Ribbon** , click **Show Messages** , click **All** :

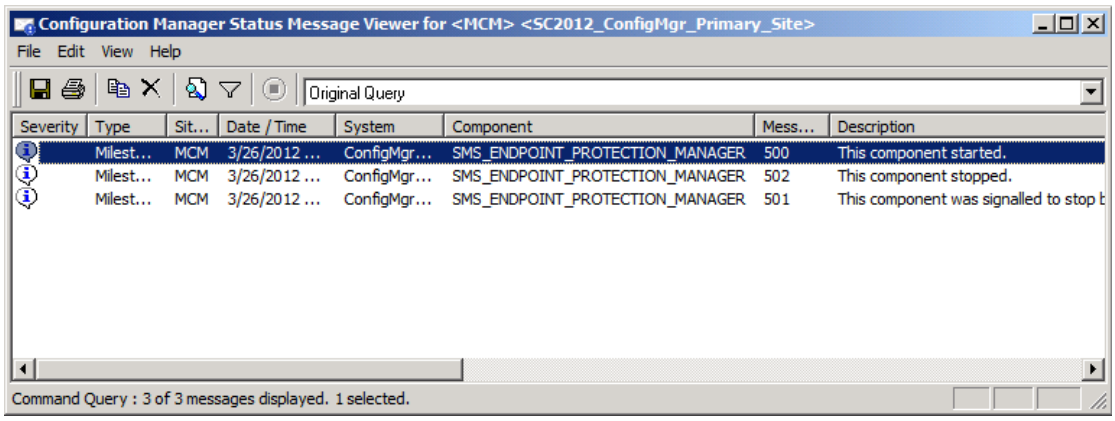


13) The **Status Messages : Set Viewing Period** dialog box appears prompting for the age of status messages to display :

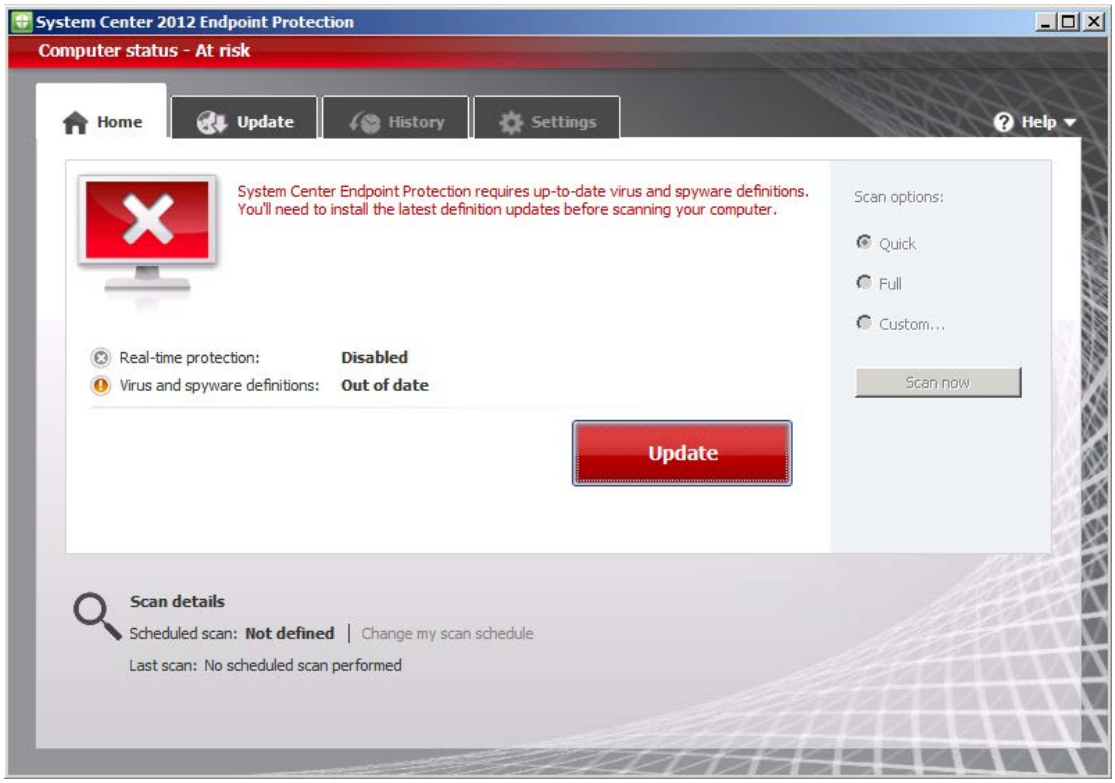


Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

14) Click **OK** to view messages for the past 24 hours . Notice a message with an ID of **500** , this message indicates that the component was started . This is an indication that the Endpoint Protection point has been installed successfully :

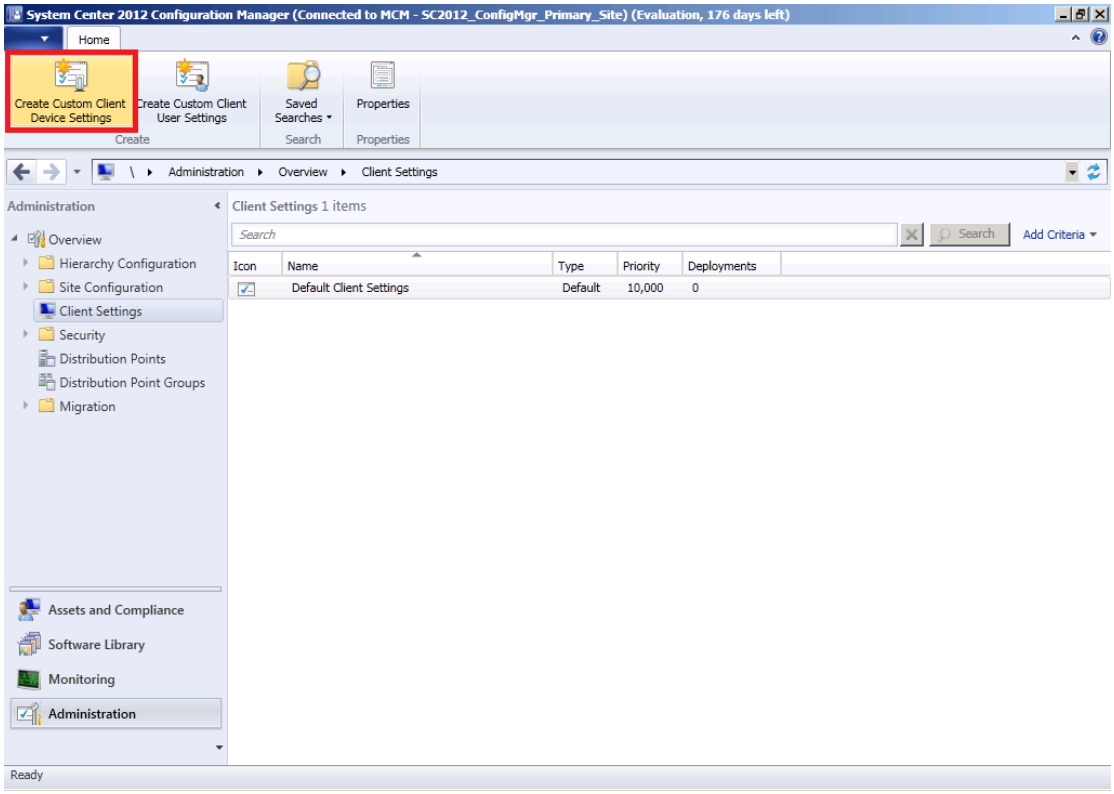


15) On the **Start menu** , click **System Center 2012 Endpoint Protection** , the **System Center 2012 Endpoint Protection** window appears , the status is **Computer status – At risk** :

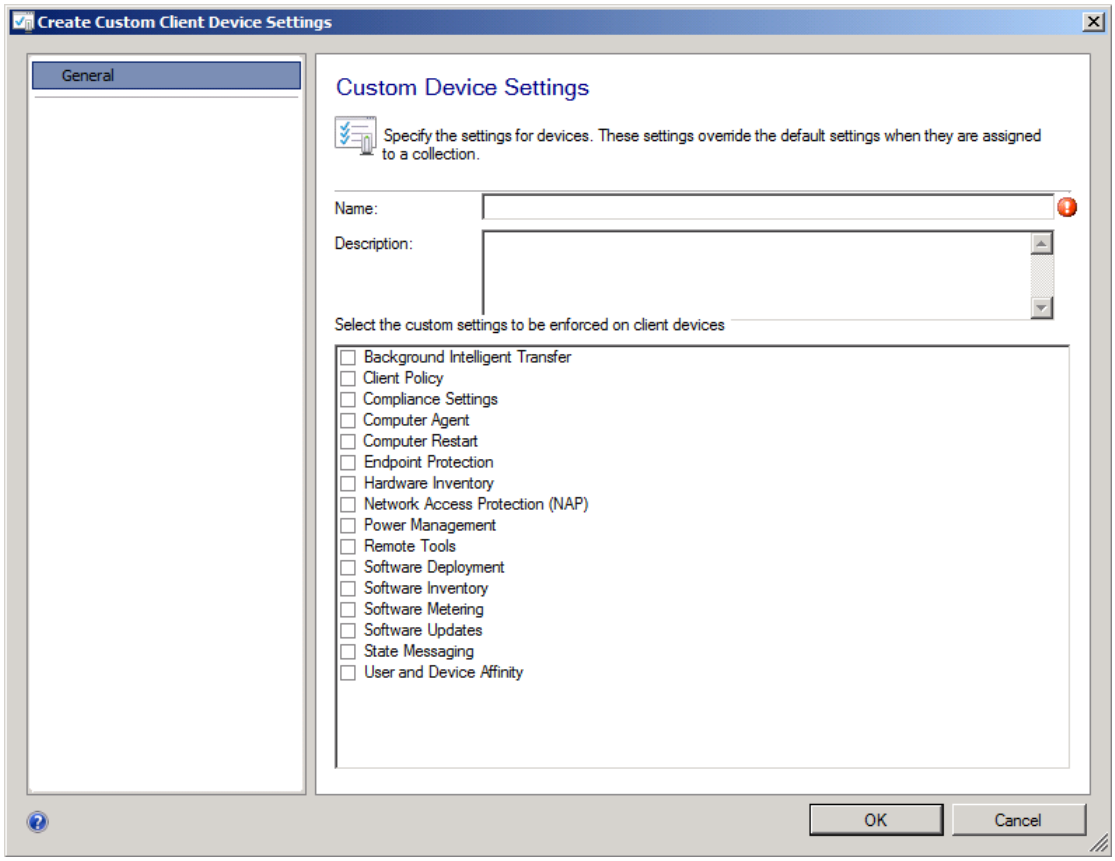


Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

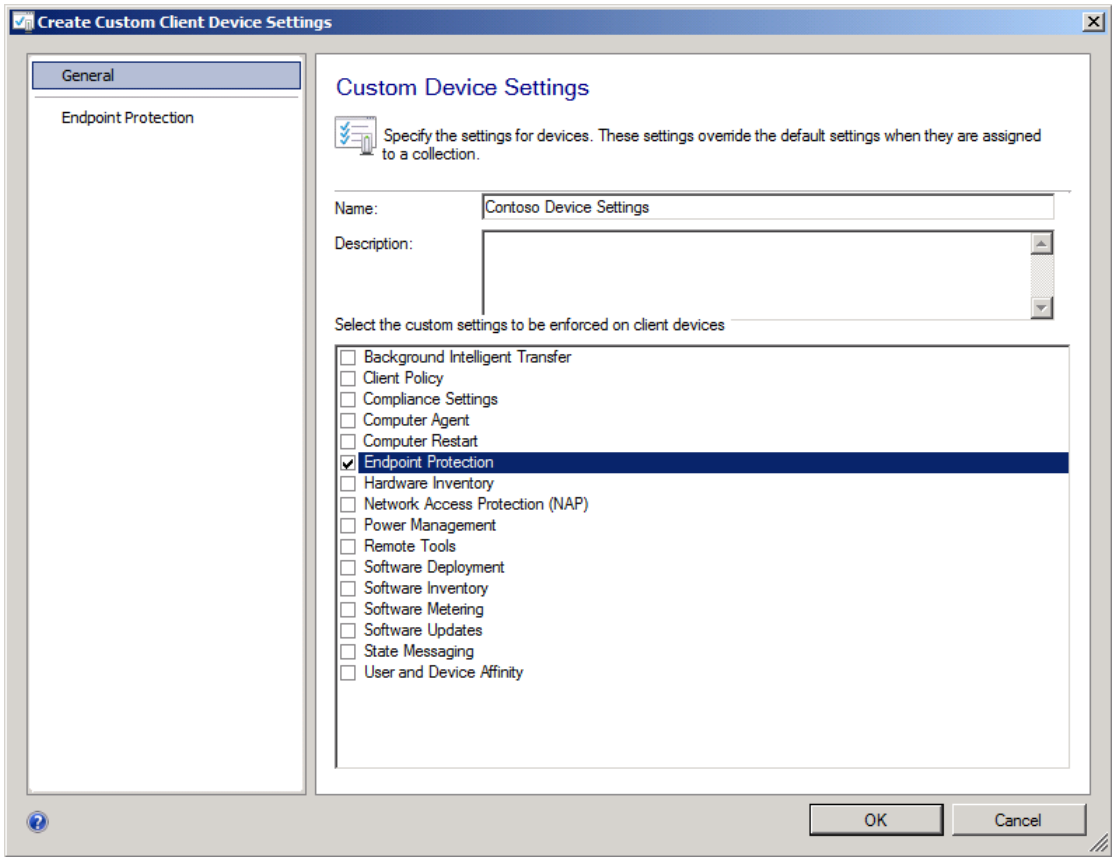
16) Close the **System Center 2012 Endpoint Protection** window . In the following procedure ,you will enable the Endpoint Protection client , which will allow scanning for malware and viruses on client computers. Click the **Administration** workspace , click **Client Settings** node , click **Create Custom Client Device Settings** on the Ribbon :



17) The **Create Custom Client Device Settings** window displayed :

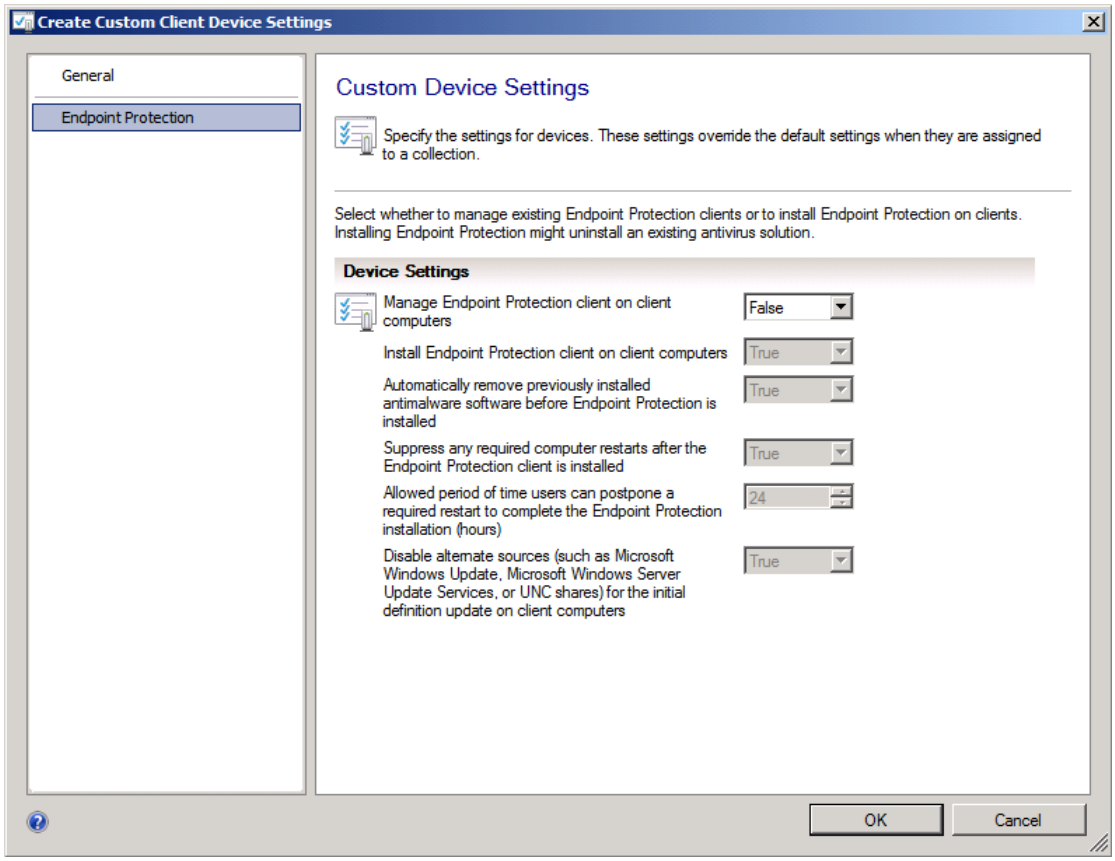


18) Enter a name in the **Name** box , and then select **Endpoint Protection** in **Select the custom settings to be enforced on client devices** box :

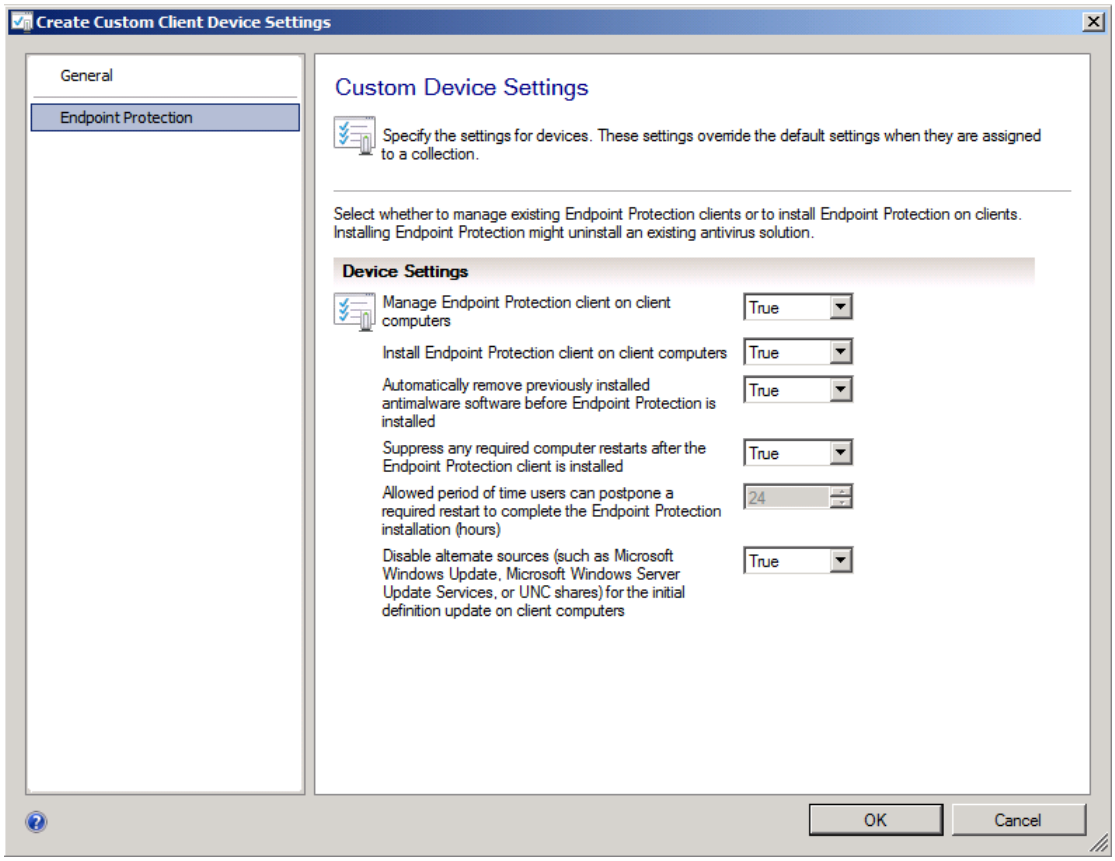


19) In the navigation pane , click **Endpoint Protection** :

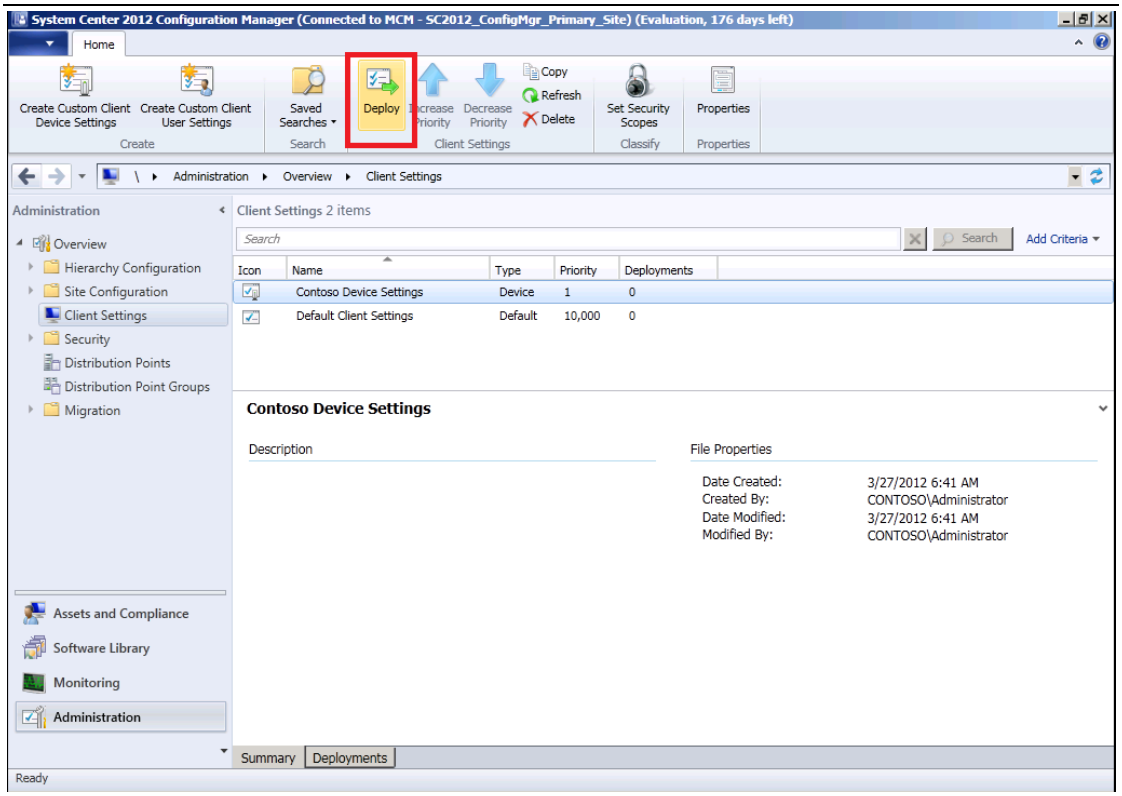
Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao



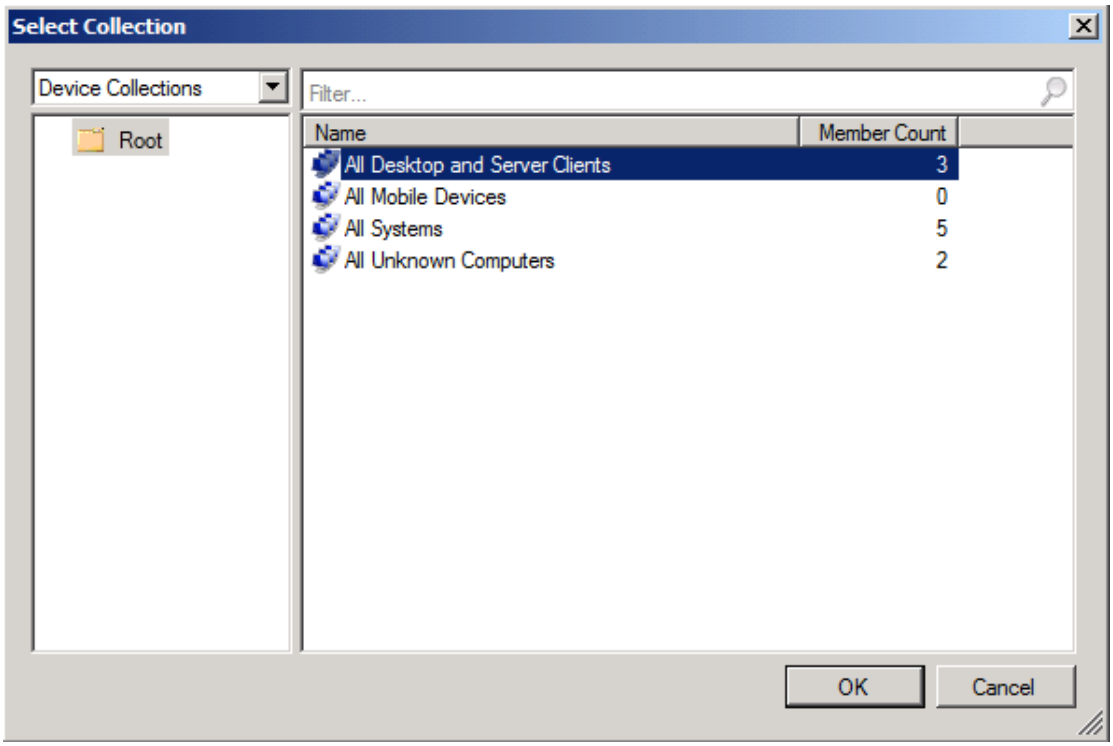
20) In the **Manage Endpoint Protection client on client computers** box , click **True** . The others settings , you can keep default :



21) Click **OK** , will back to **Client Settings** node , click just created Device Settings , click **Deploy** on the Ribbon :

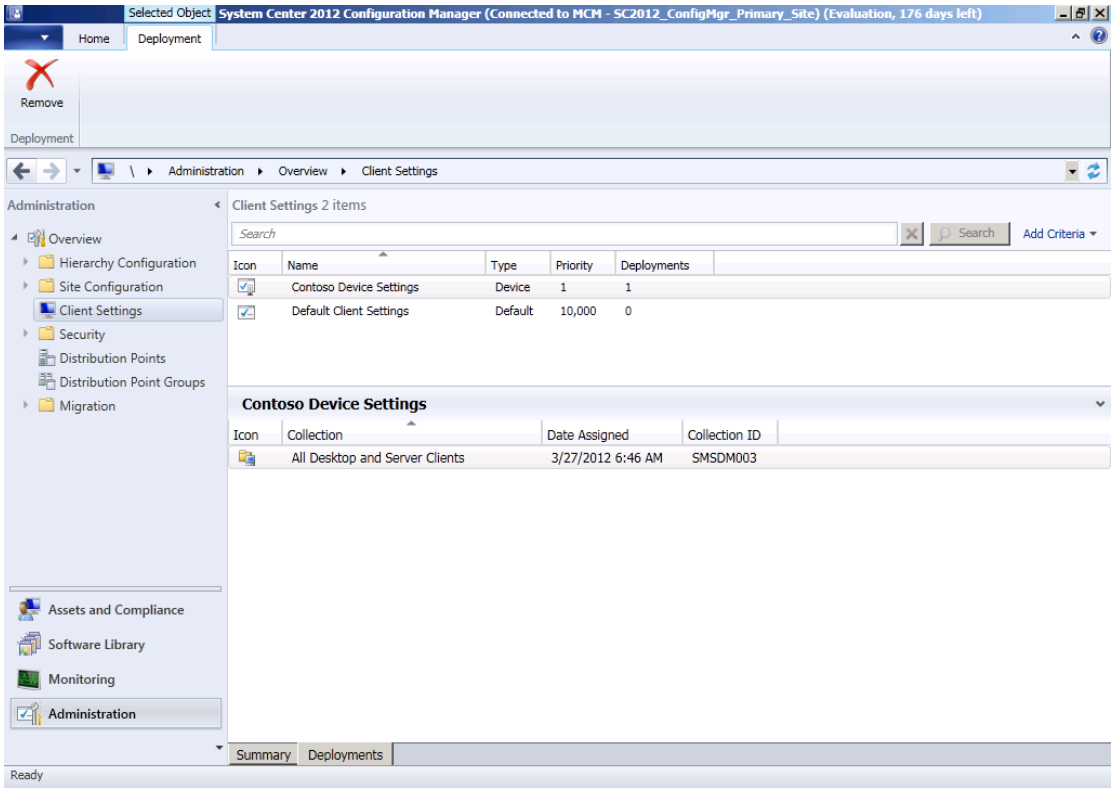


22) The **Select Collection** dialog box appears :

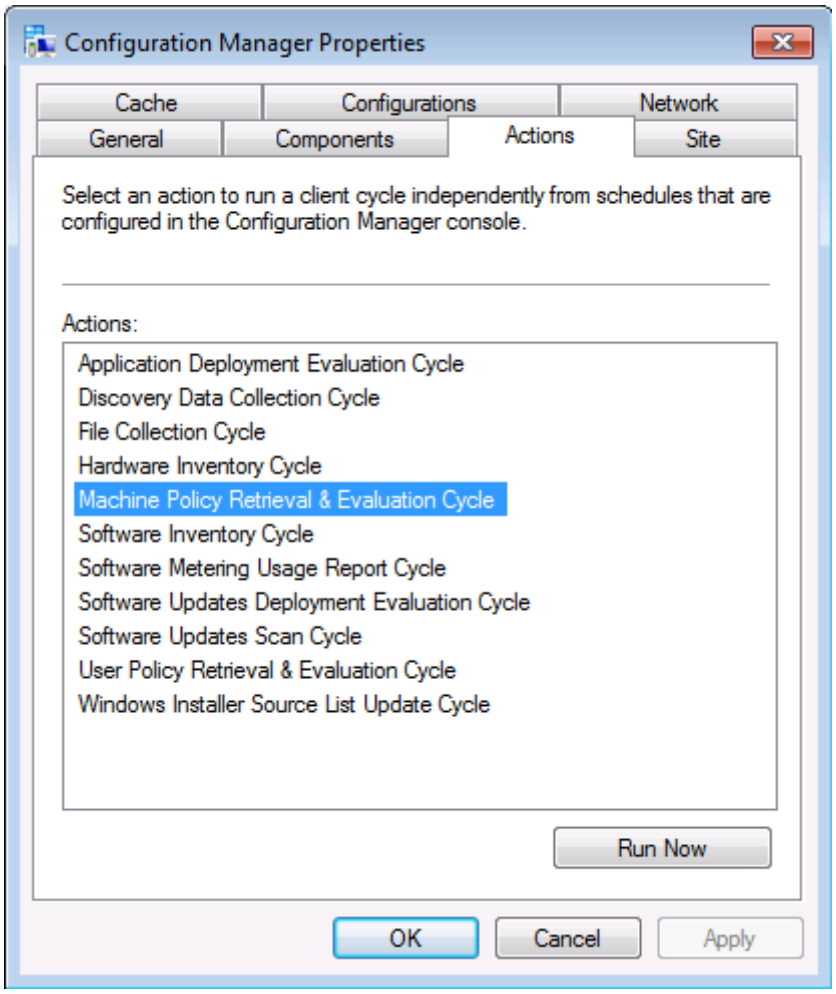


23) Click **All Desktop and Server Clients** , click **OK** , you can see this client

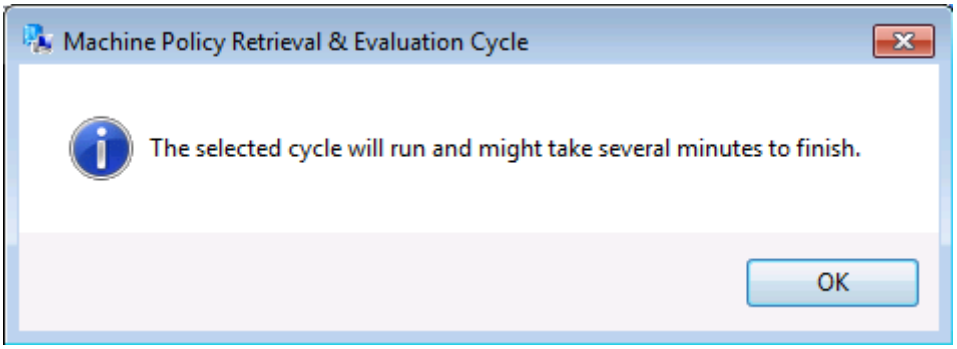
settings will deployed :



24) Logon to **Client** computer , in **Control Panel** , click **System and Security** , and then start **Configuration Manager** , Click the **Actions** tab , click **Machine Policy Retrieval & Evaluation Cycle** , and then click **Run Now** :

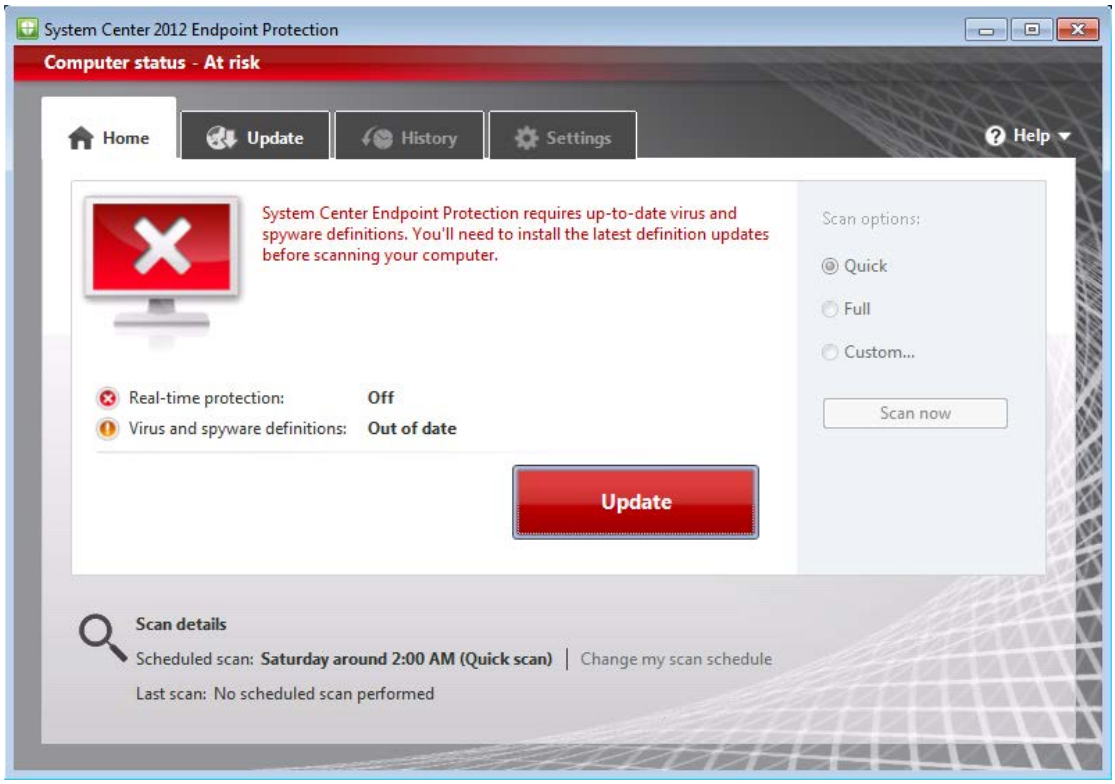


25) A **Machine Policy Retrieval & Evaluation Cycle** message box appears indicating the action was initiated :



26) Click **OK** . The **System Center 2012 Endpoint Protection** agent is installed on the **Client** computer . On the **Start** menu , click **System Center 2012**

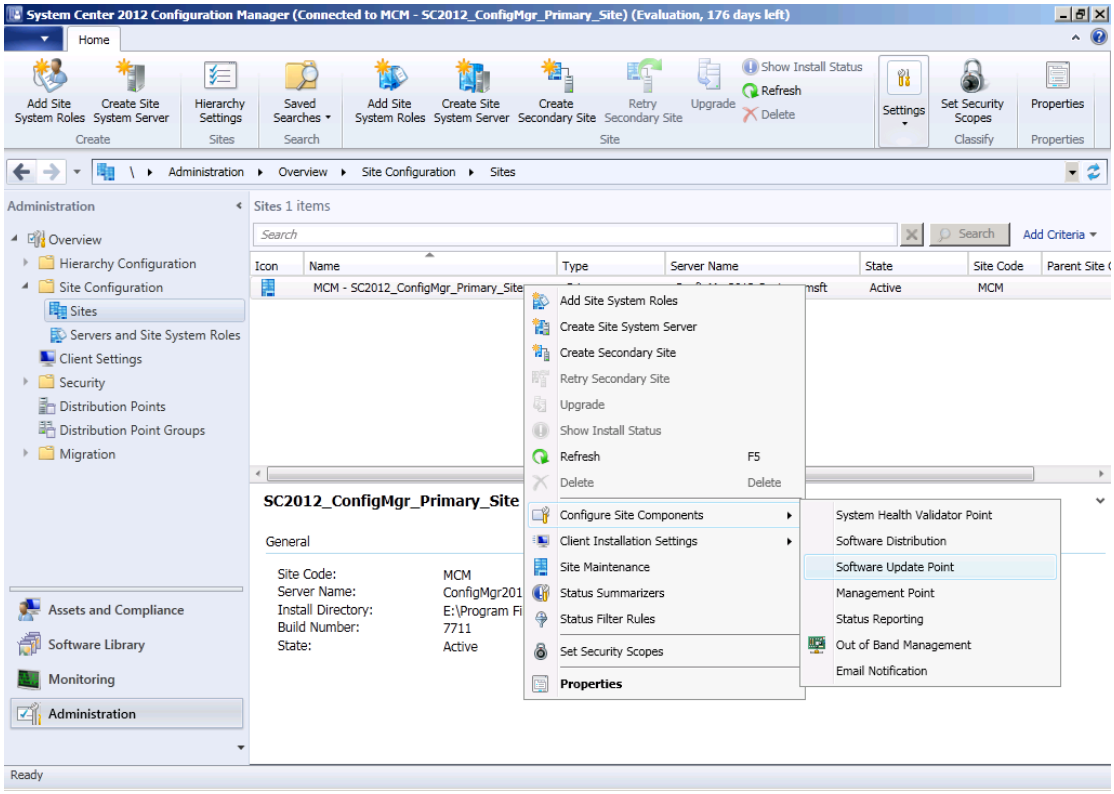
Endpoint Protection , the **System Center 2012 Endpoint Protection** window appears displaying the current status of the Endpoint Protection client :



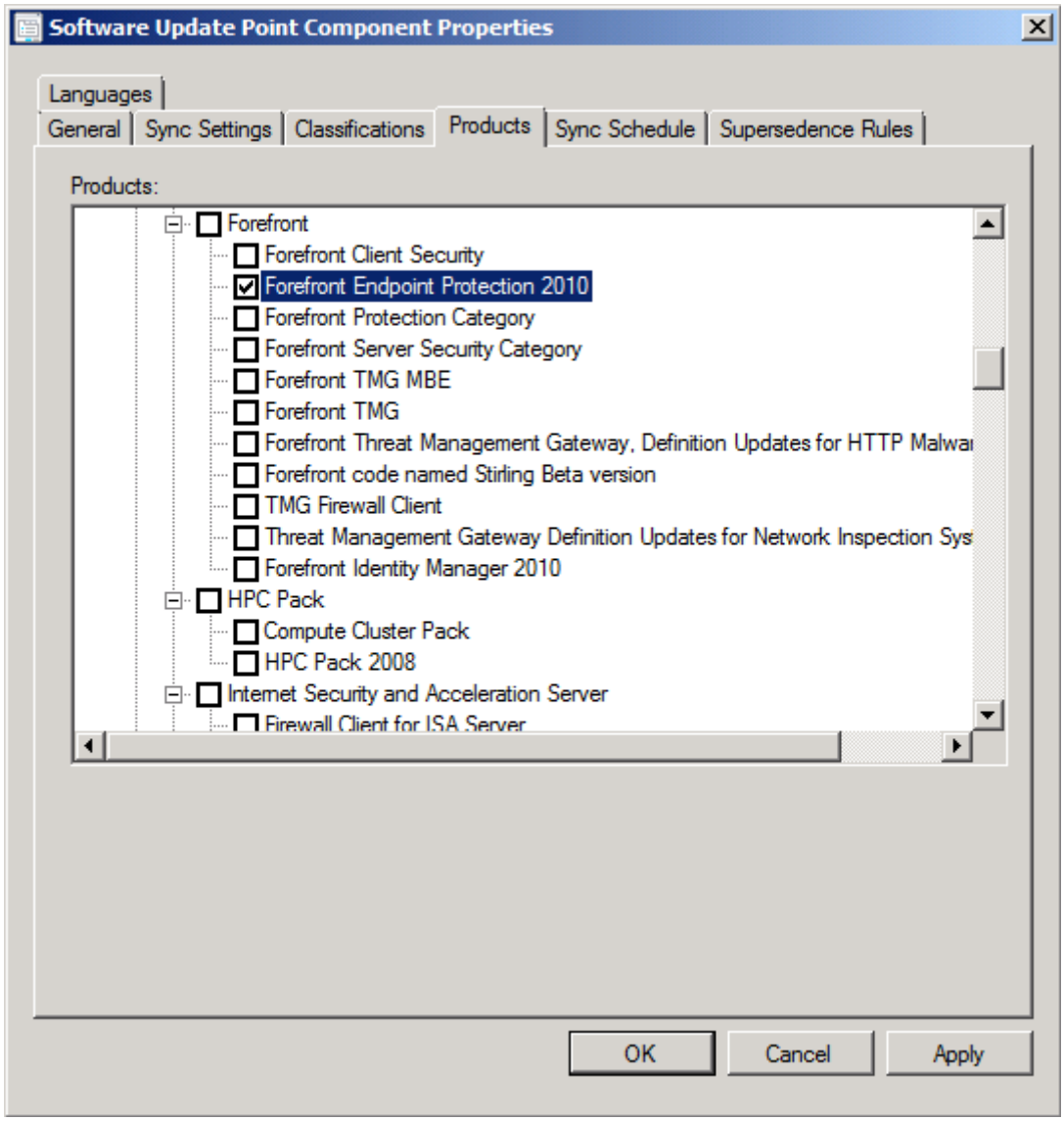
27) Close the **System Center 2012 Endpoint Protection** window.

5. Synchronize Endpoint Protection Updates :

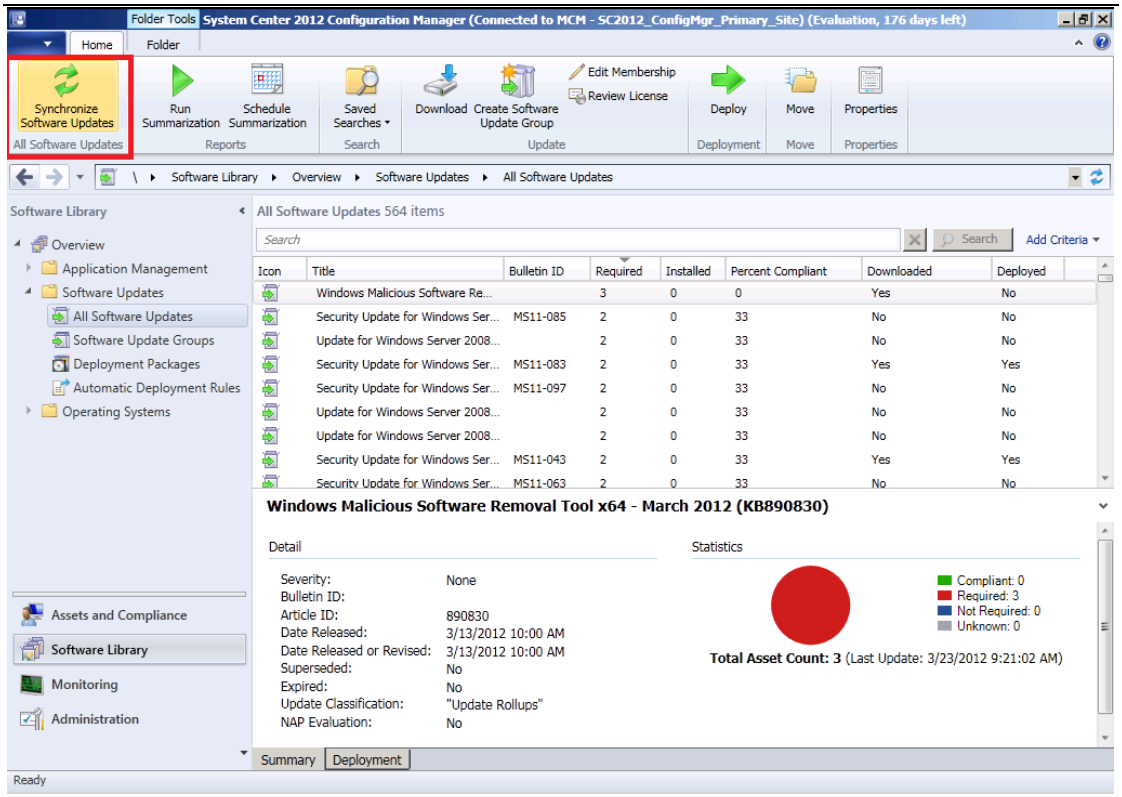
1) Click **Administration** workspace , expand **Site Configuration** , click **Sites** , right-click site server name , and then click **Configure Site Components** --- **Software Update Point** :



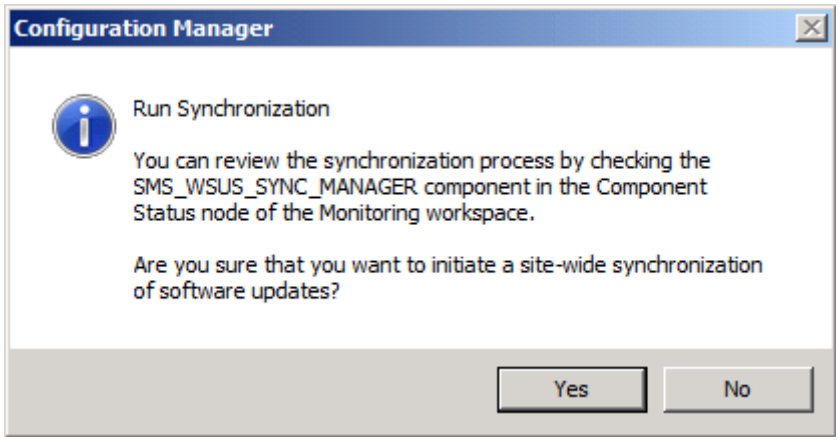
2) The **Software Update Point Component Properties** dialog box appears , click **Products** tab and select **Forefront Endpoint Protection 2010** :



3) Click **OK** , click **Software Library** workspace , expand **Software Updates** , click **All Software Updates** , and then click **Synchronize Software Updates** in the Ribbon :

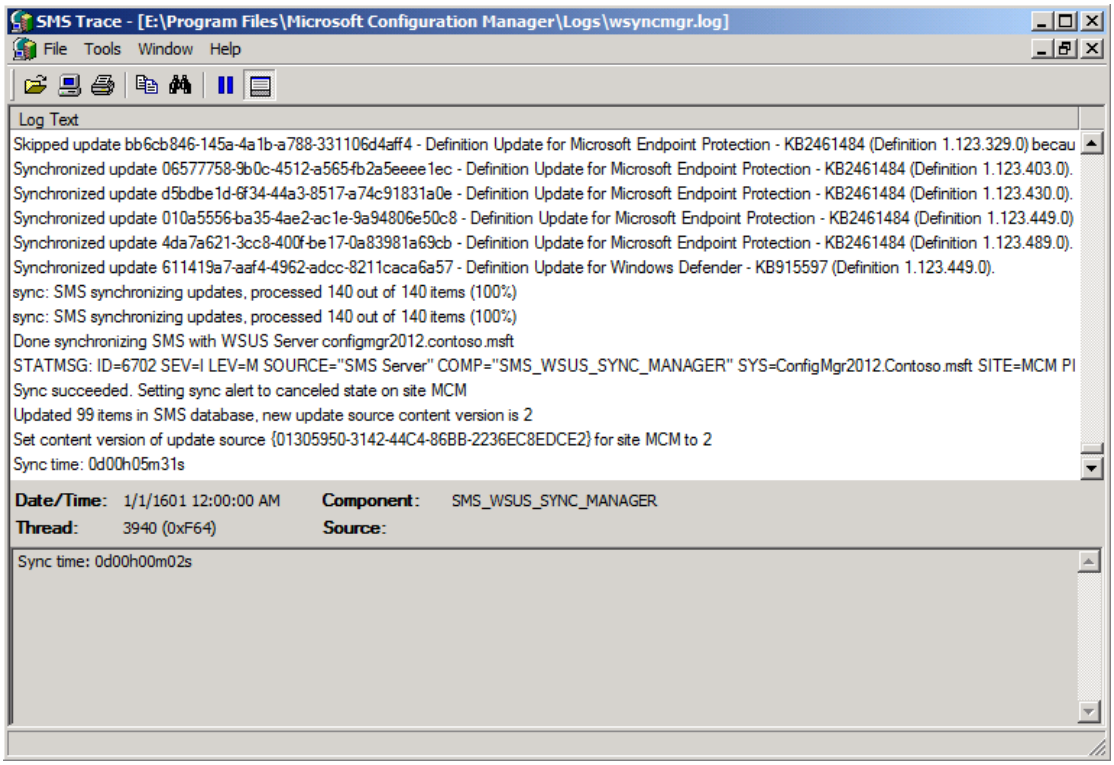


4) A **Configuration Manager** dialog box appears :



5) Click **Yes** , the synchronization will started , you can check the **wsyncmgr.log** :

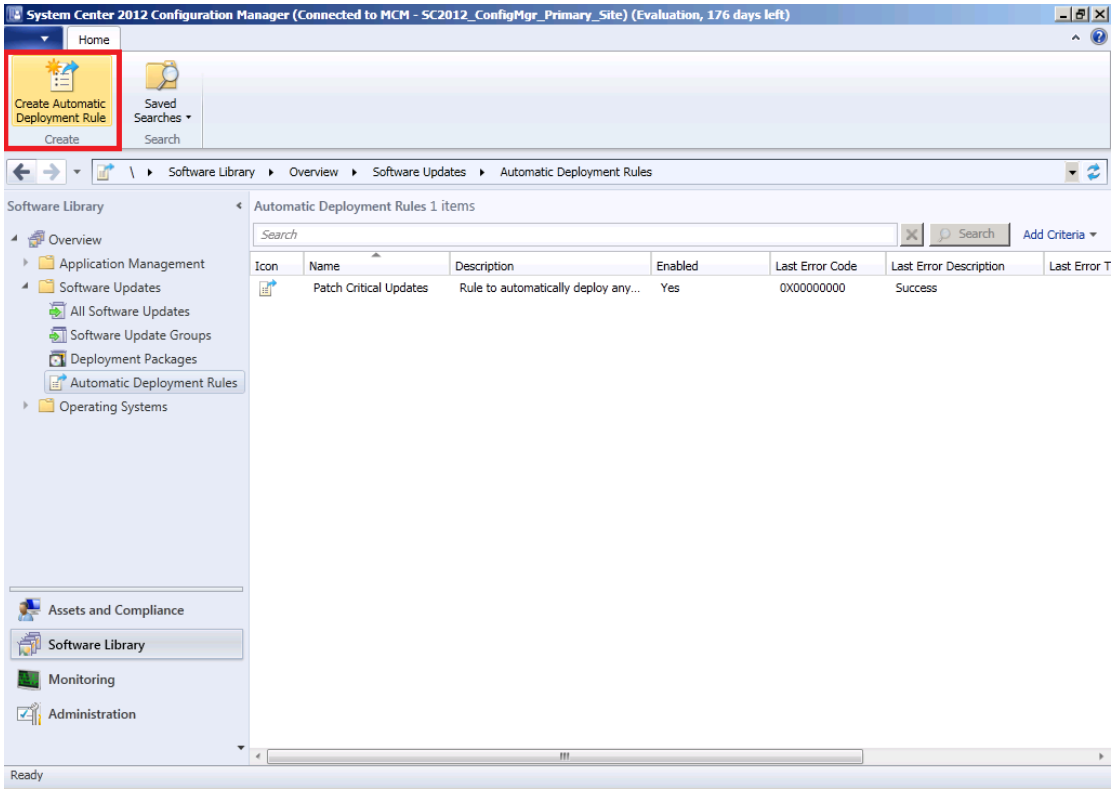
Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao



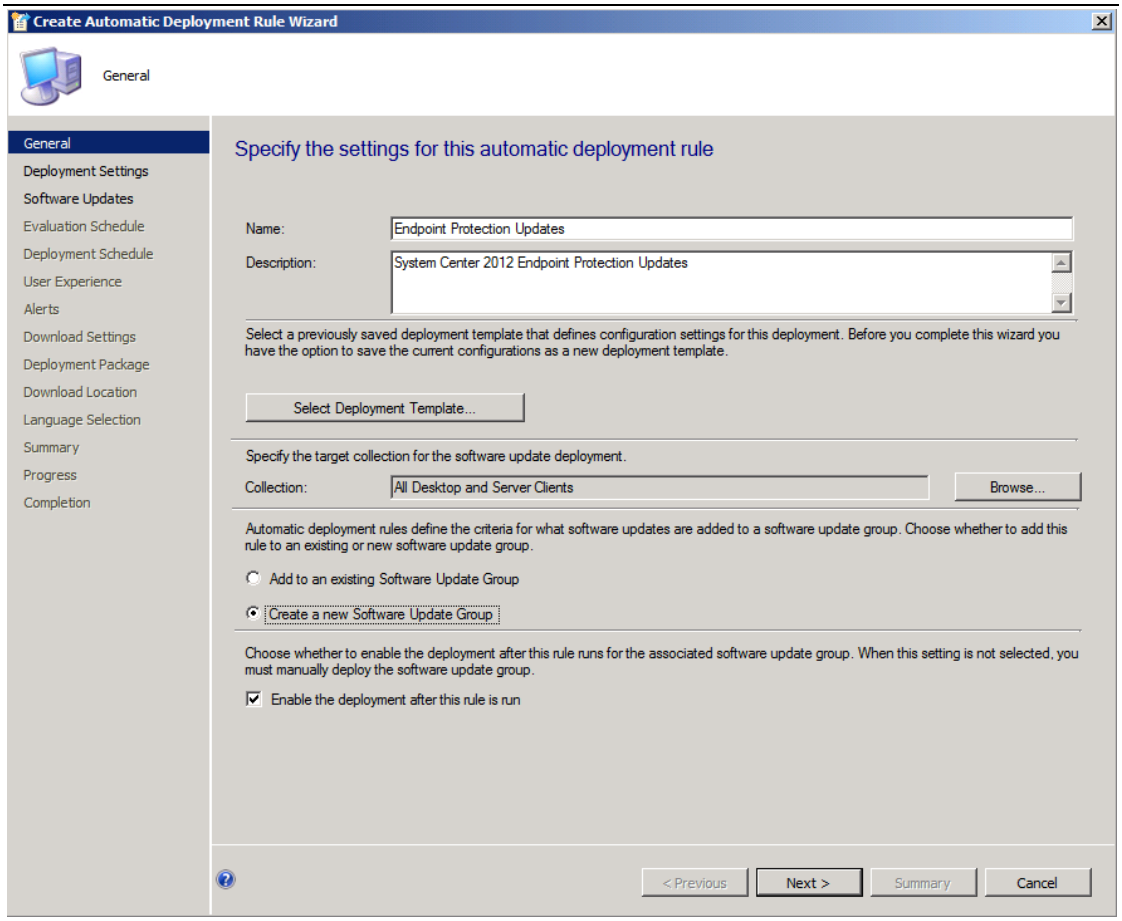
Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

6. Create Automatic Deployment Rules :

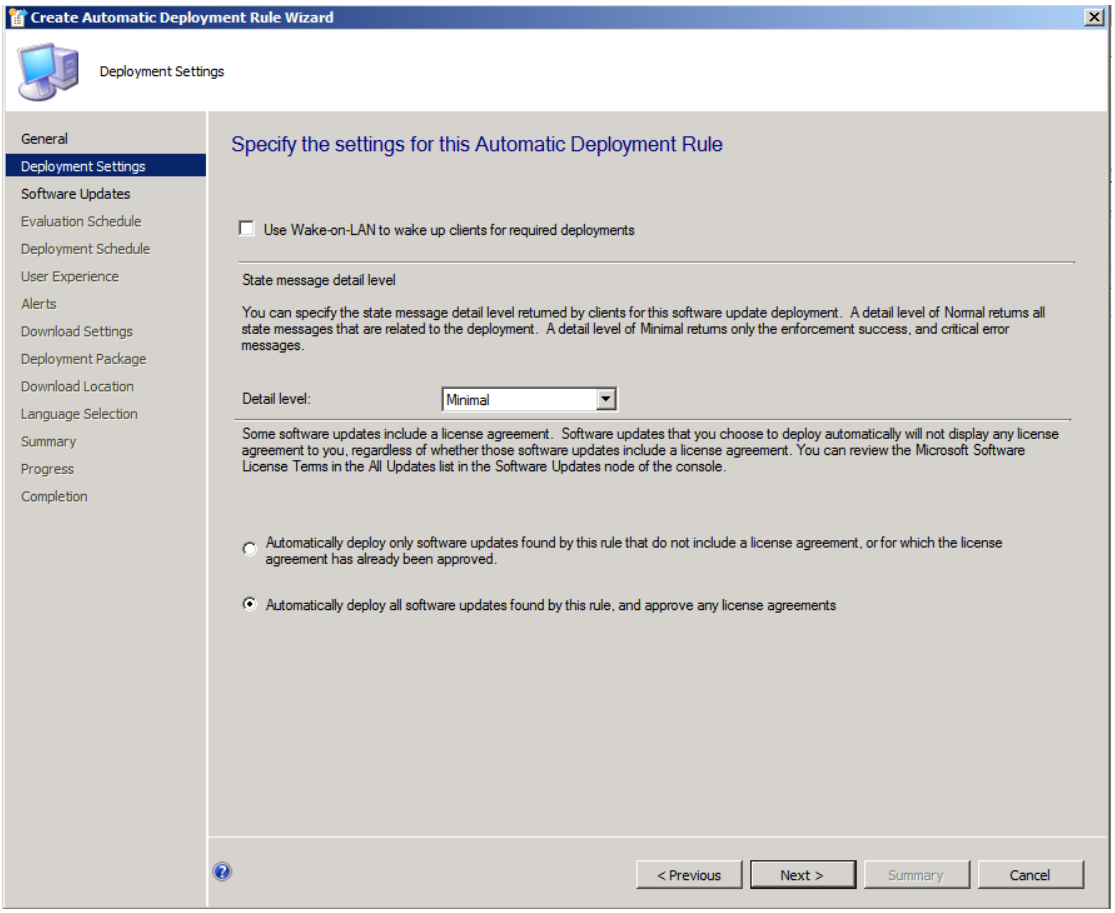
1) Click **Software Library** workspace , expand **Software Updates** , click **Automatic Deployment Rules** , click **Create Automatic Deployment Rule** in the Ribbon :



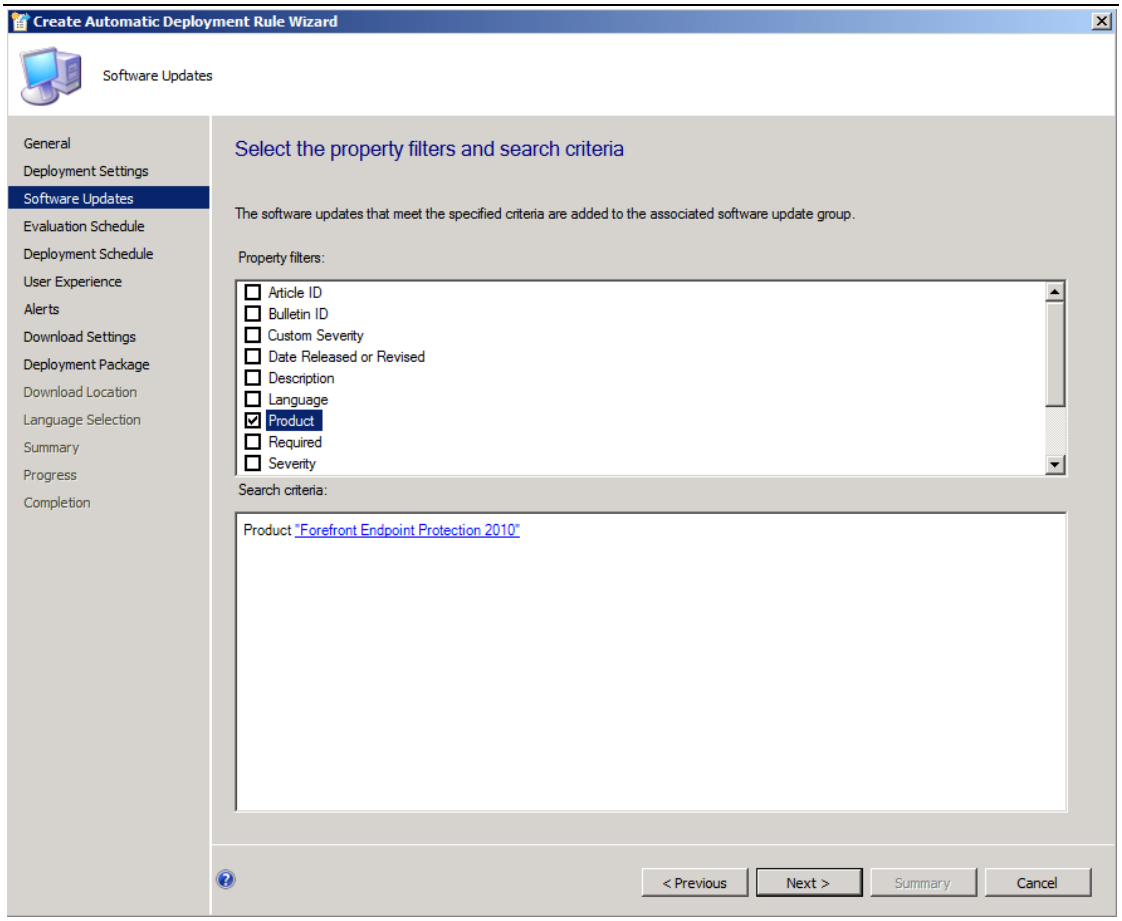
2) The **Create Automatic Deployment Rule Wizard General** dialog box appears , you can type or select some settings :



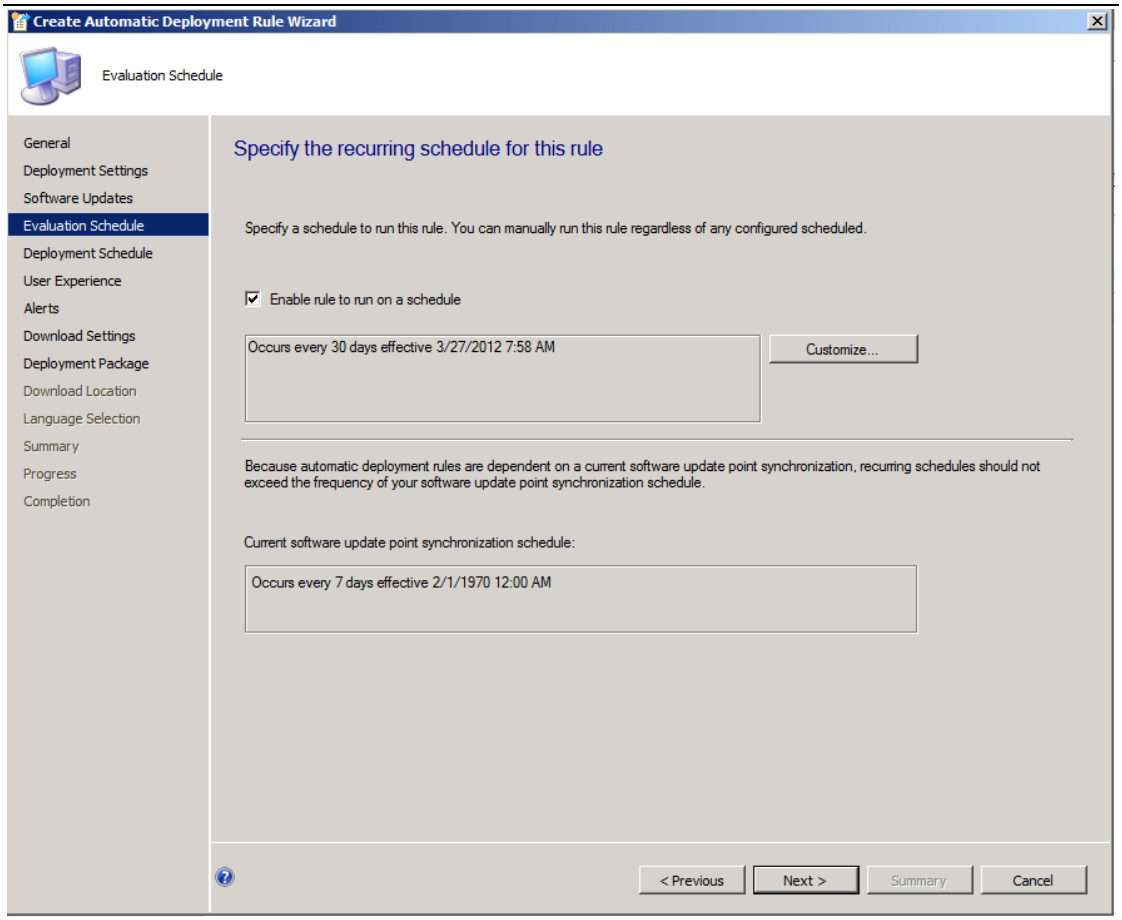
3) Click **Next** , the **Deployment Settings** dialog box appears :



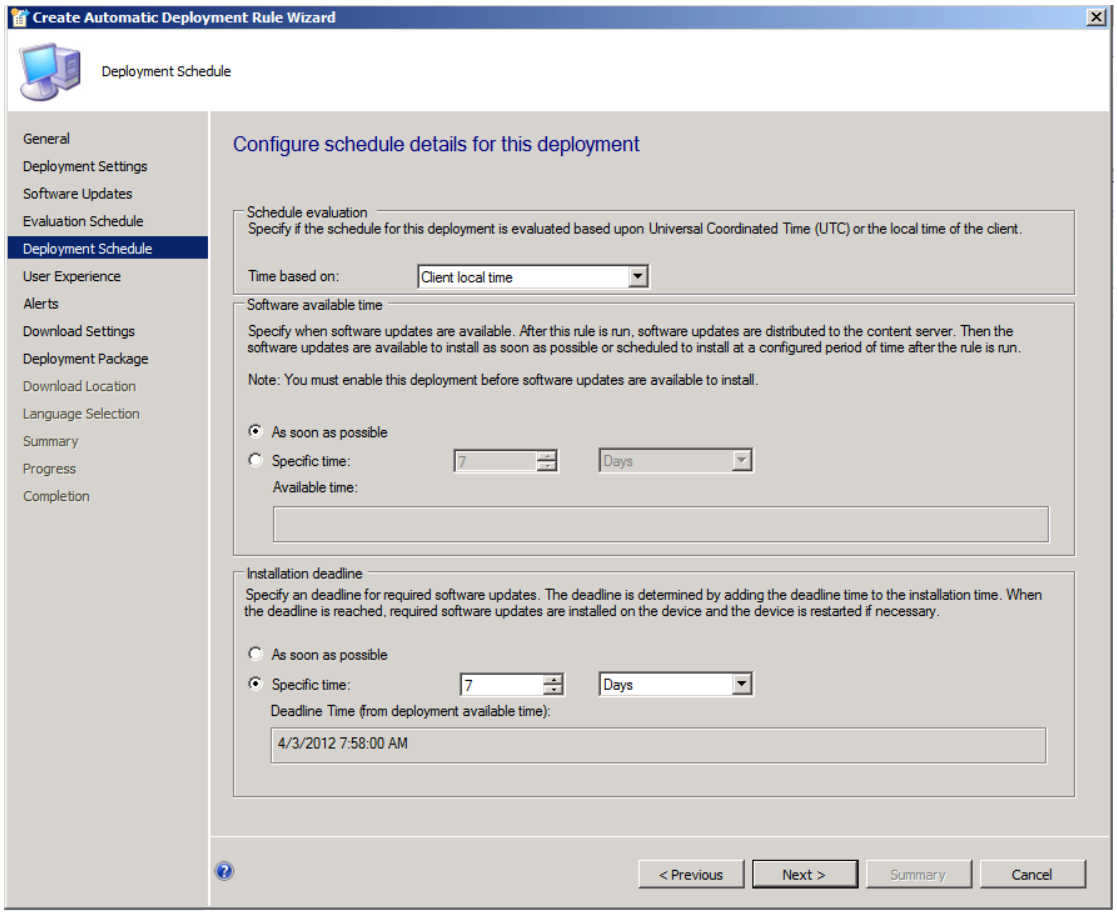
4) Click **Next** , the **Software Updates** dialog box appears , select **Product** in **Property filters** , and select **Forefront Endpoint Protection 2010** in **Search criteria** :



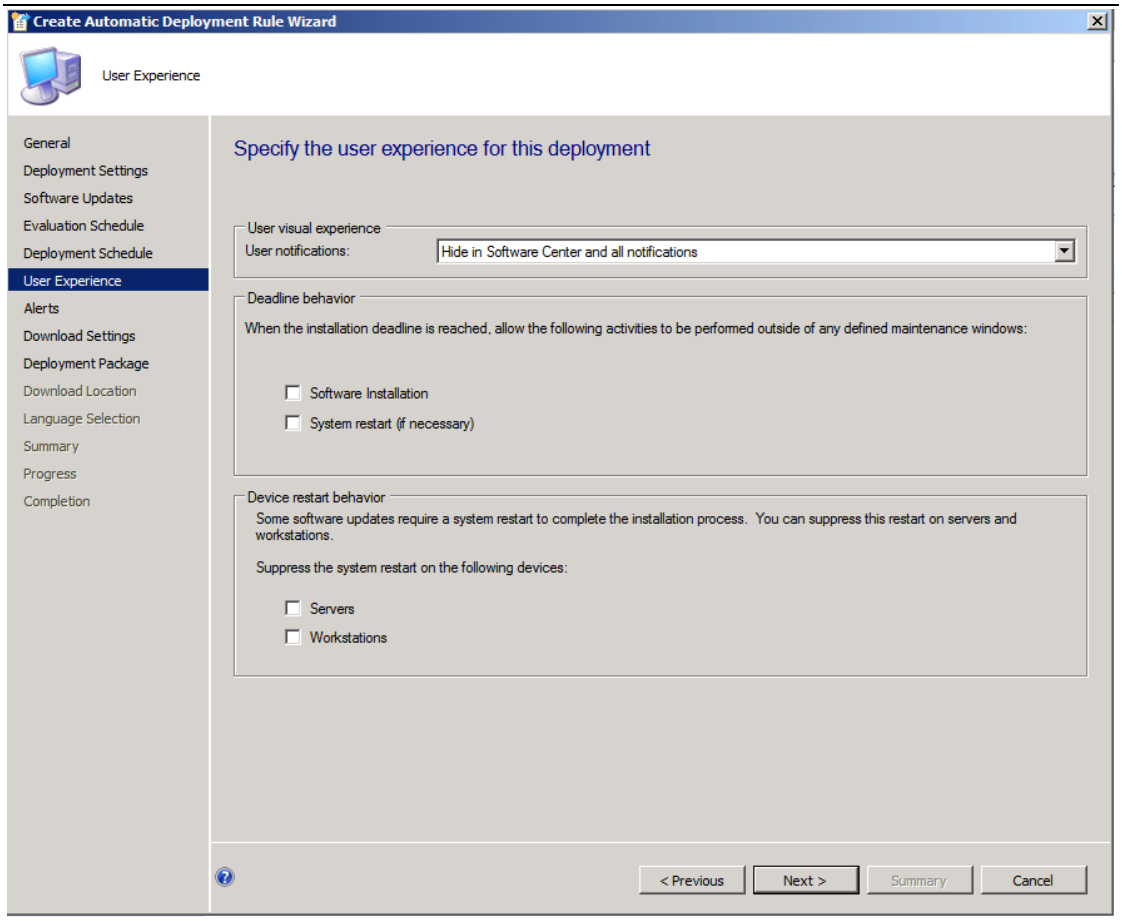
5) Click **Next** , the **Evaluation Schedule** dialog box appears :



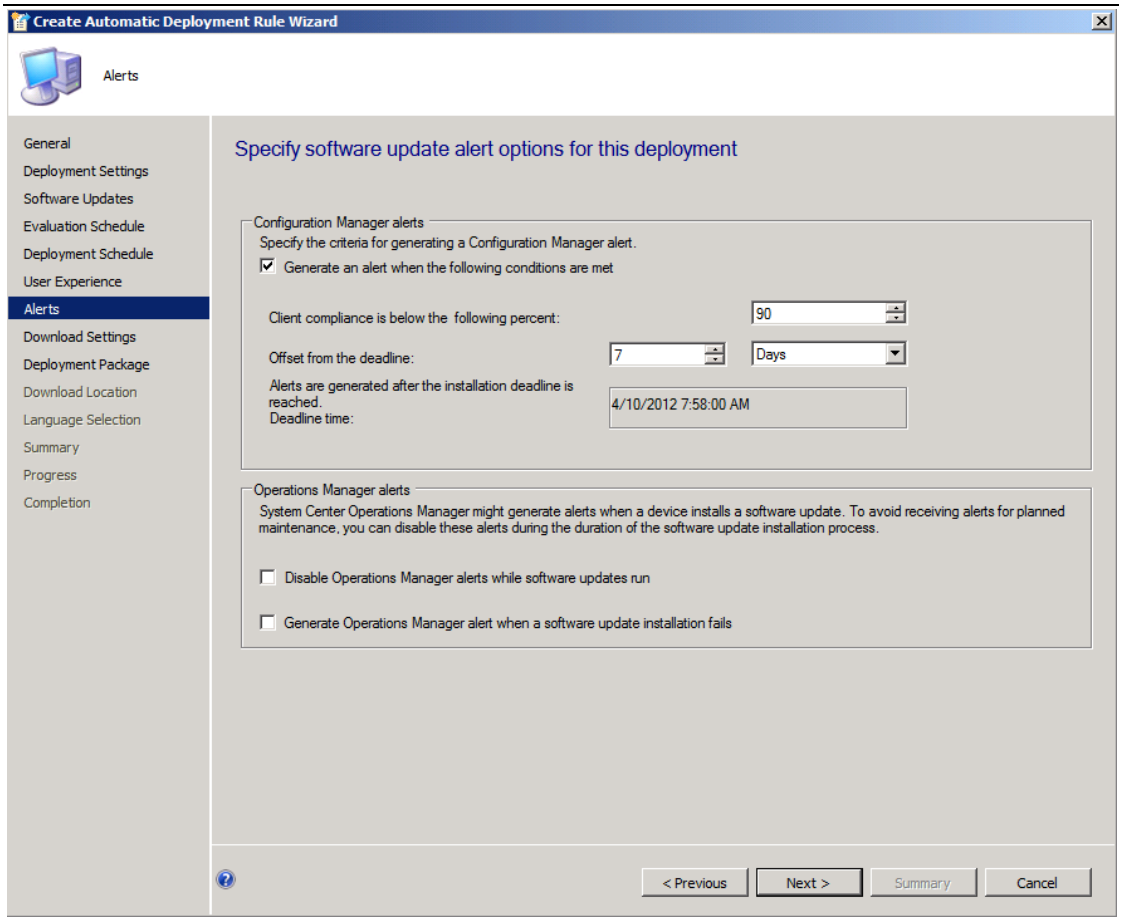
6) Click **Next** , the **Deployment Schedule** dialog box appears :



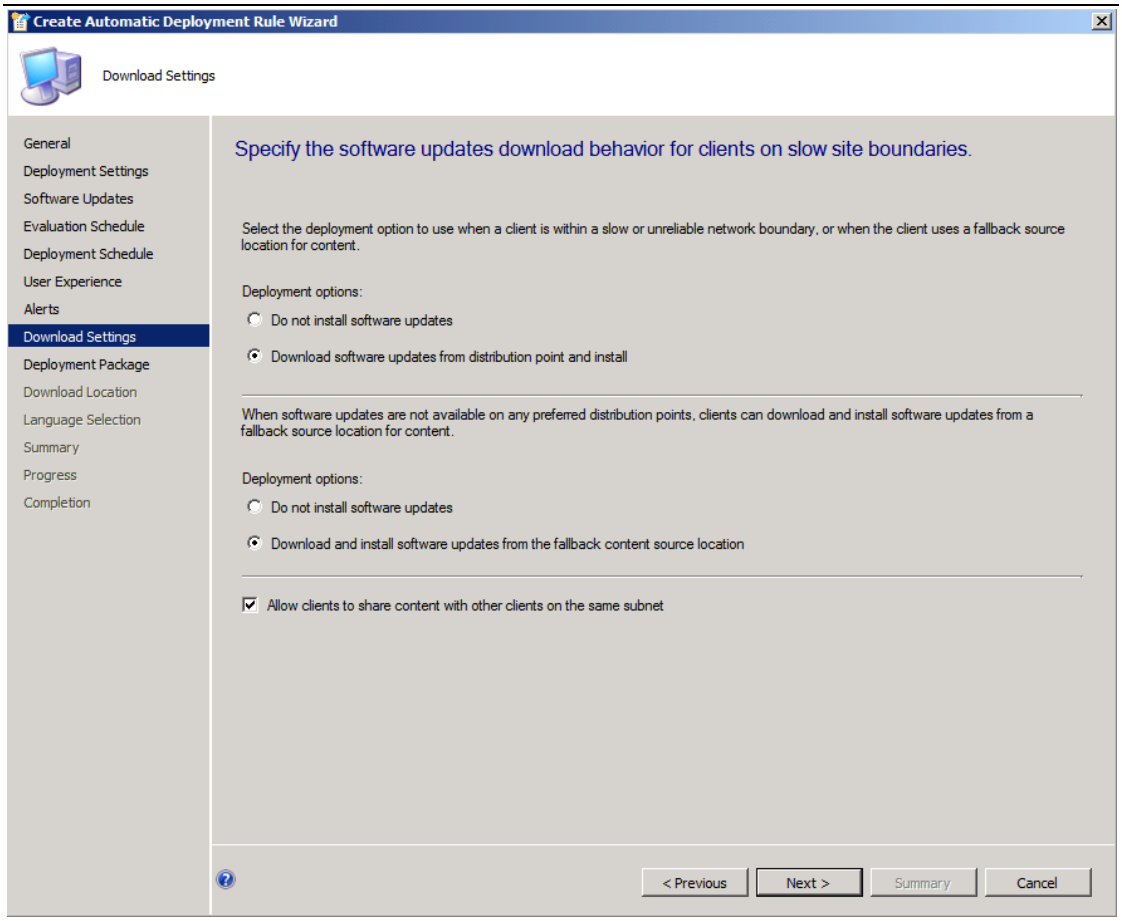
7) Click **Next** , the **User Experience** dialog box appears :



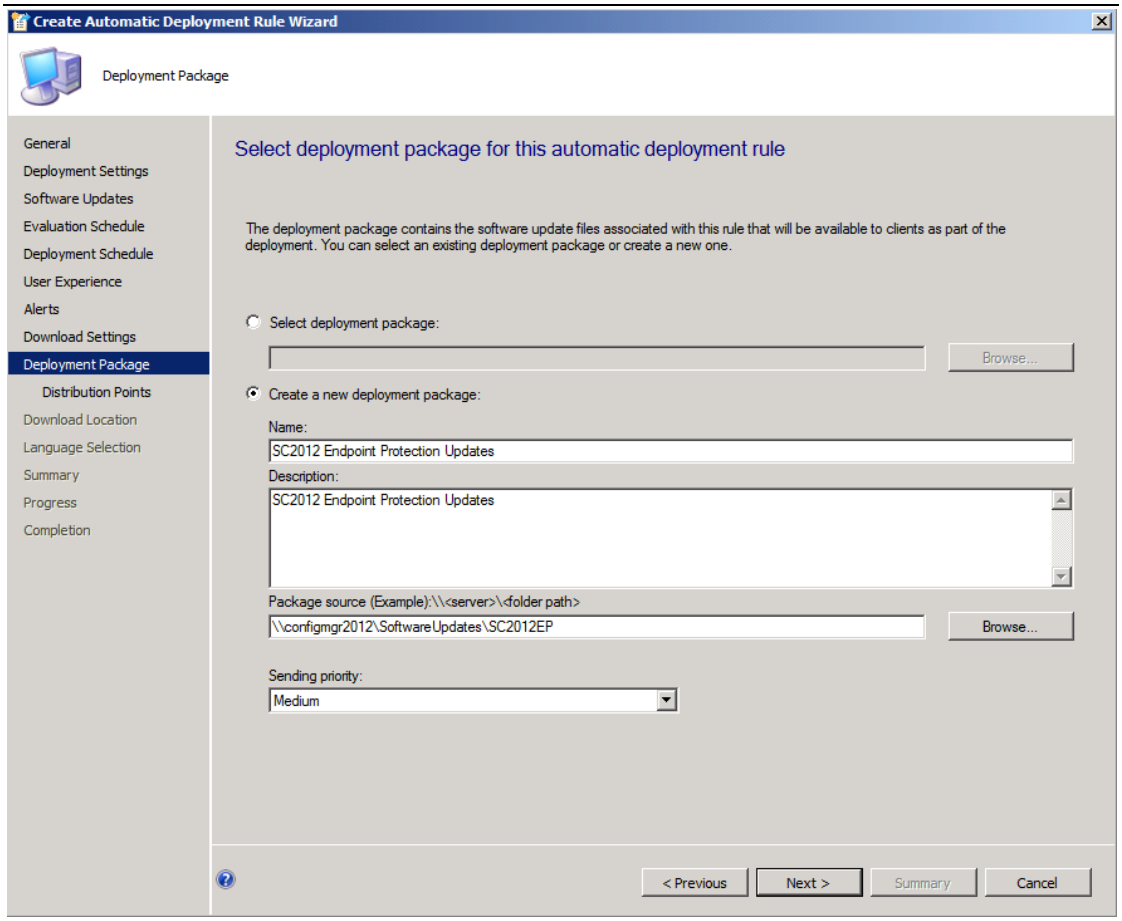
8) Click **Next** , the **Alerts** dialog box appears , you can select **Generate an alert when the following conditions are met** :



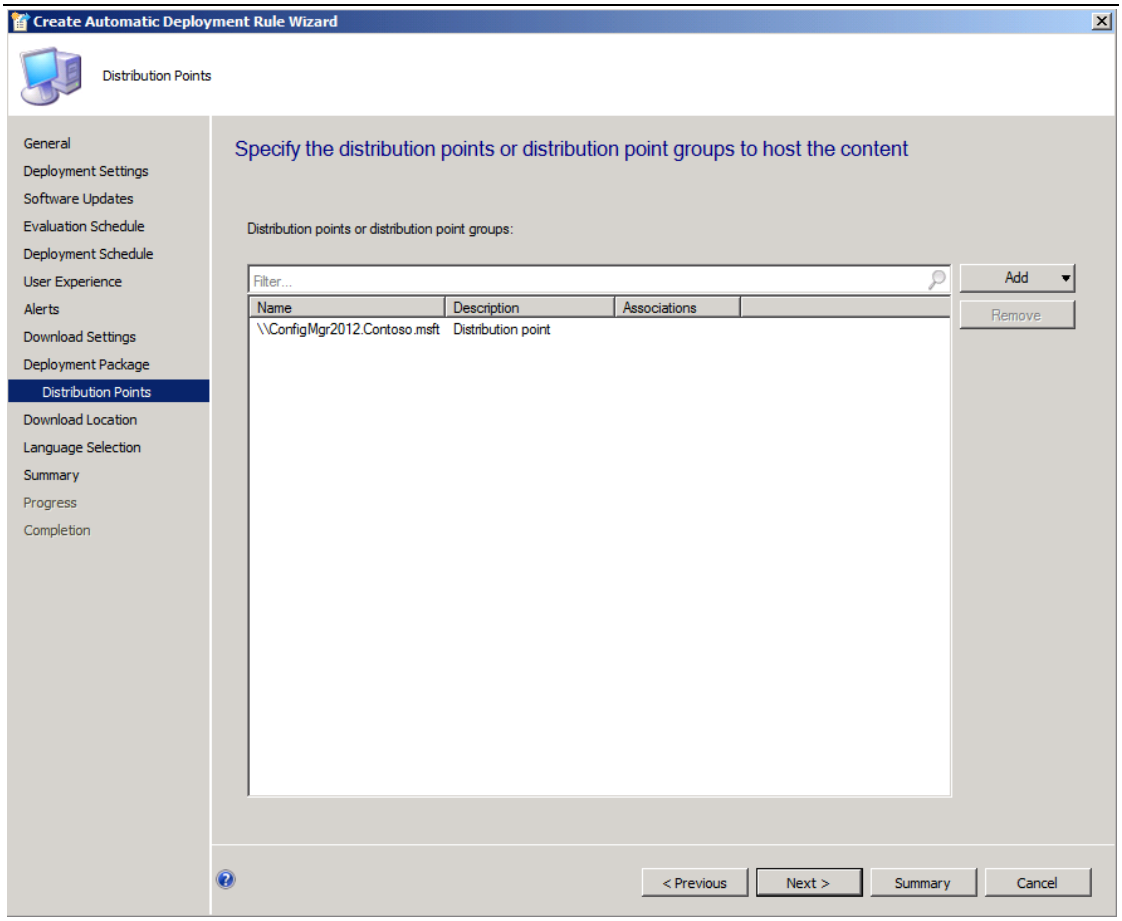
9) Click **Next** , the **Download Settings** dialog box appears , under **Deployment options** , click **Download software updates from distribution point and install** :



10) Click **Next** , the **Deployment Package** dialog box appears , click **Create a new deployment package** and input some information :

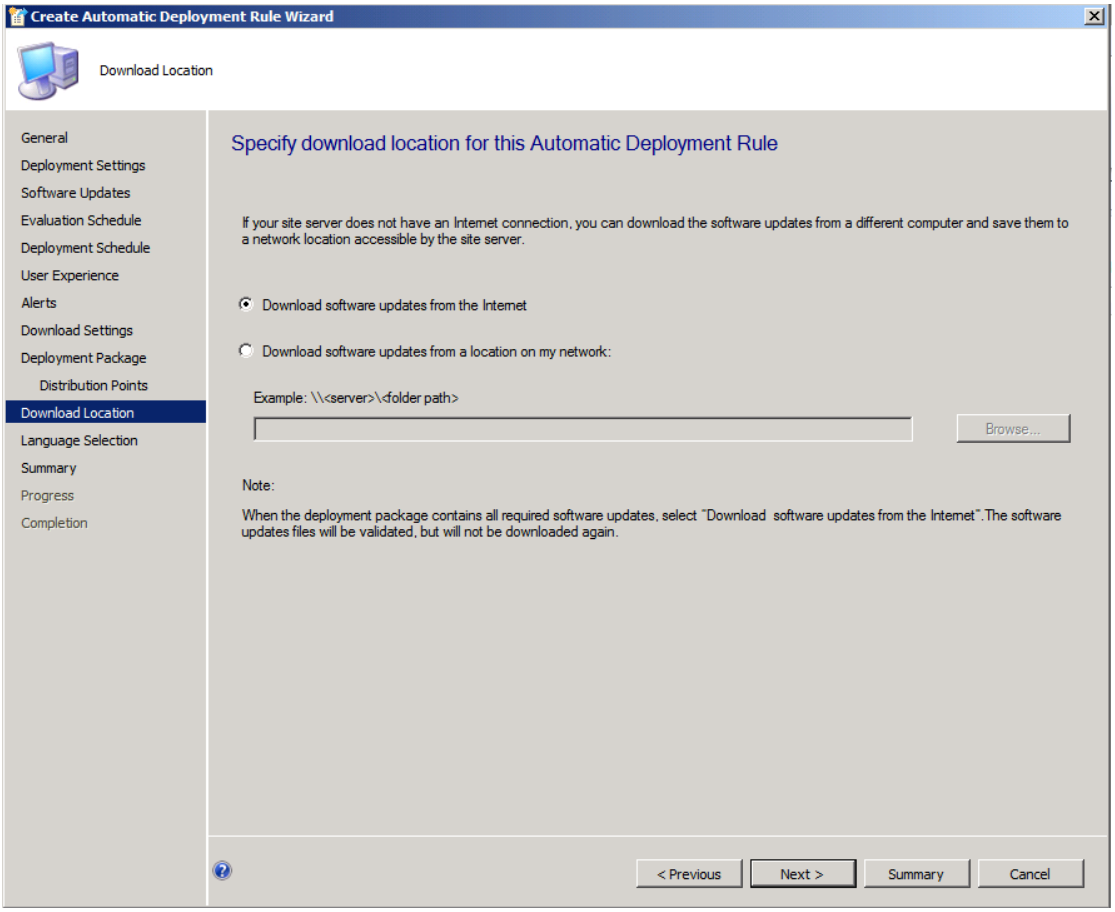


11) Click **Next** , the **Distribution Points** dialog box appears , click **Add** to adding a DP :



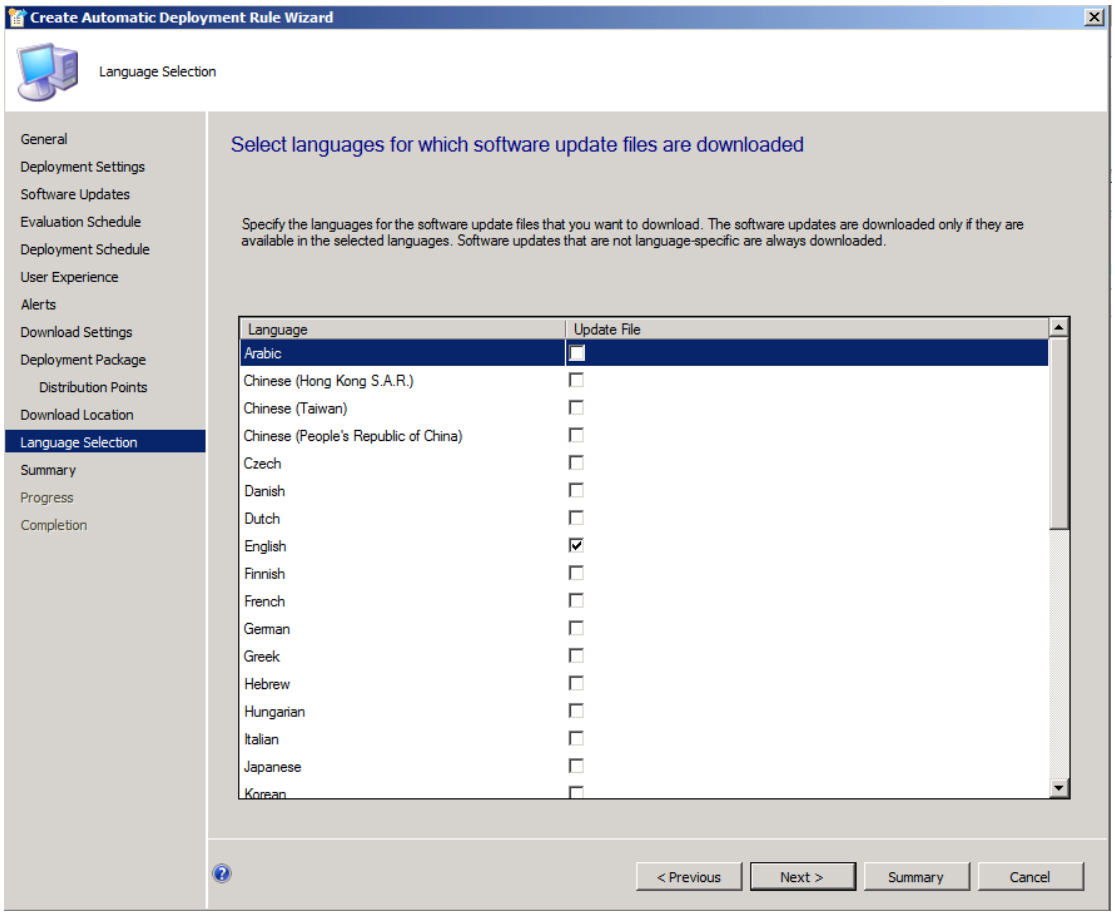
12) Click **Next** , the **Download Location** dialog box appears :

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

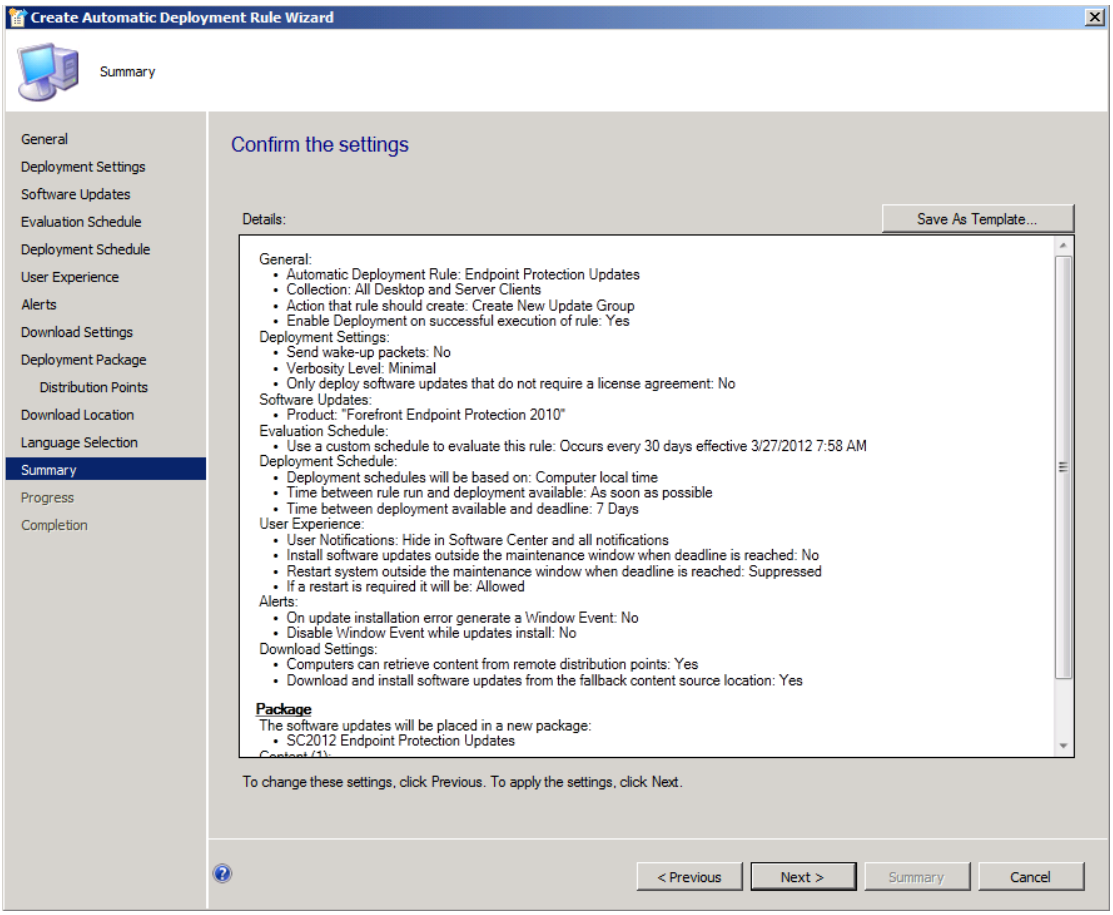


13) Click **Next** , the **Language Selection** dialog box appears :

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

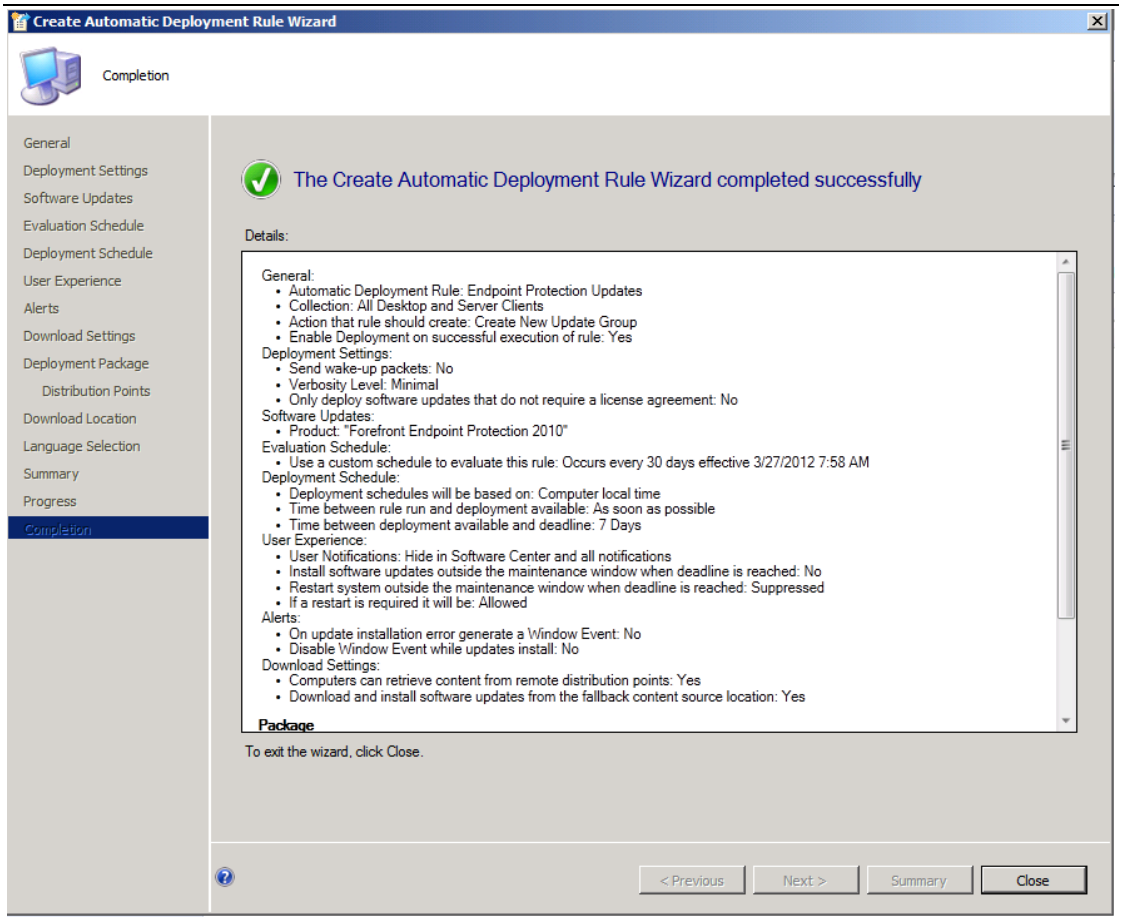


14) Click **Next** , the **Summary** dialog box appears :

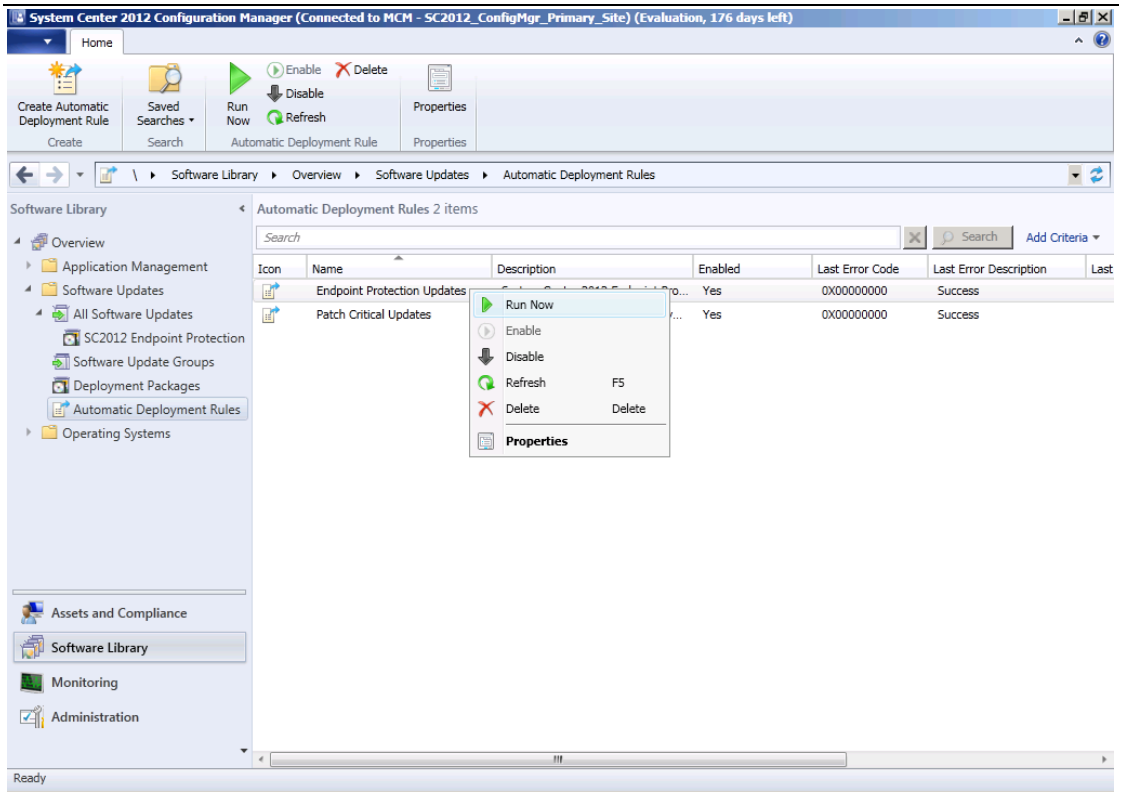


15) Confirm and review all settings and click **Next** to complete :

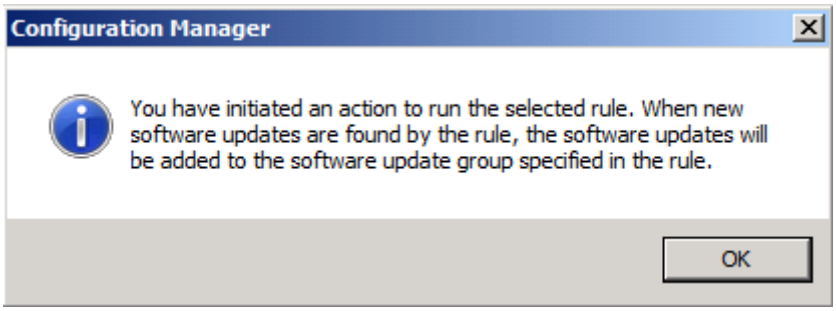
Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao



16) Click **Close** , right-click just created automatic deployment rule , click **Run Now** :



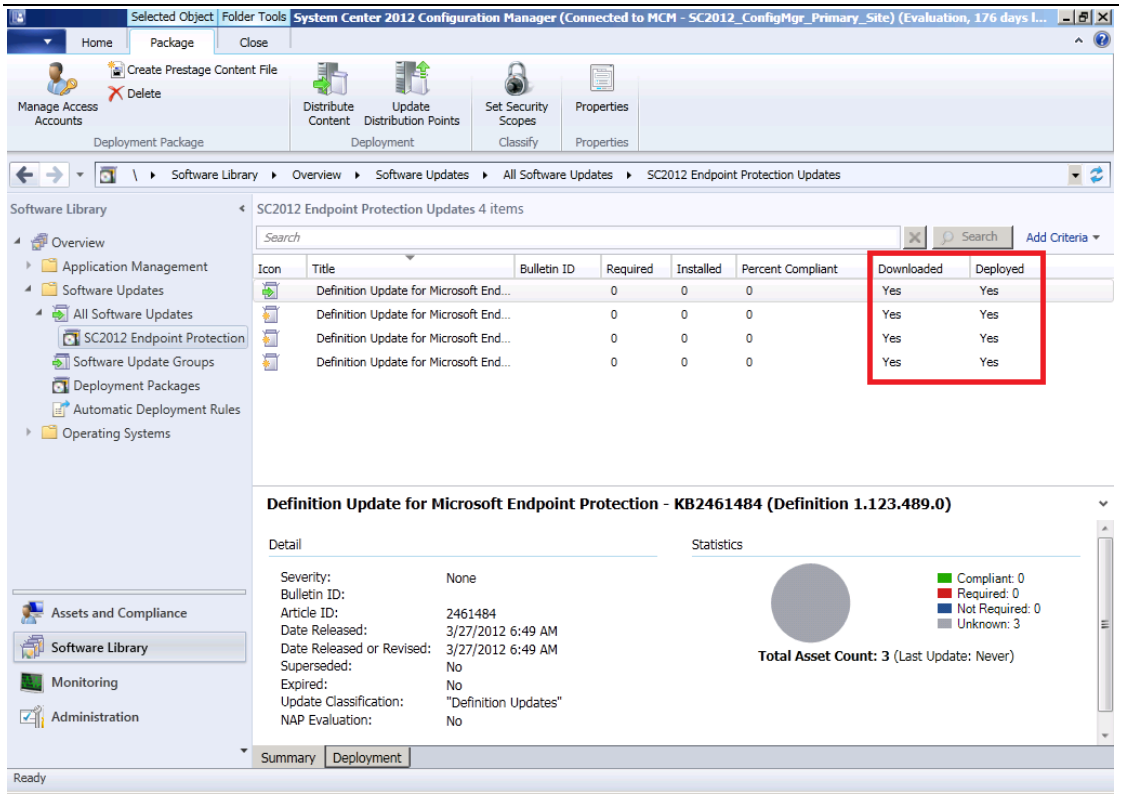
17) A **Configuration Manager** dialog box appears :



18) Click **OK** will start to run this rule . Wait some minutes, you can see the result :

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

System Center 2012
Configuration Manager RTM
Endpoint Protection Document



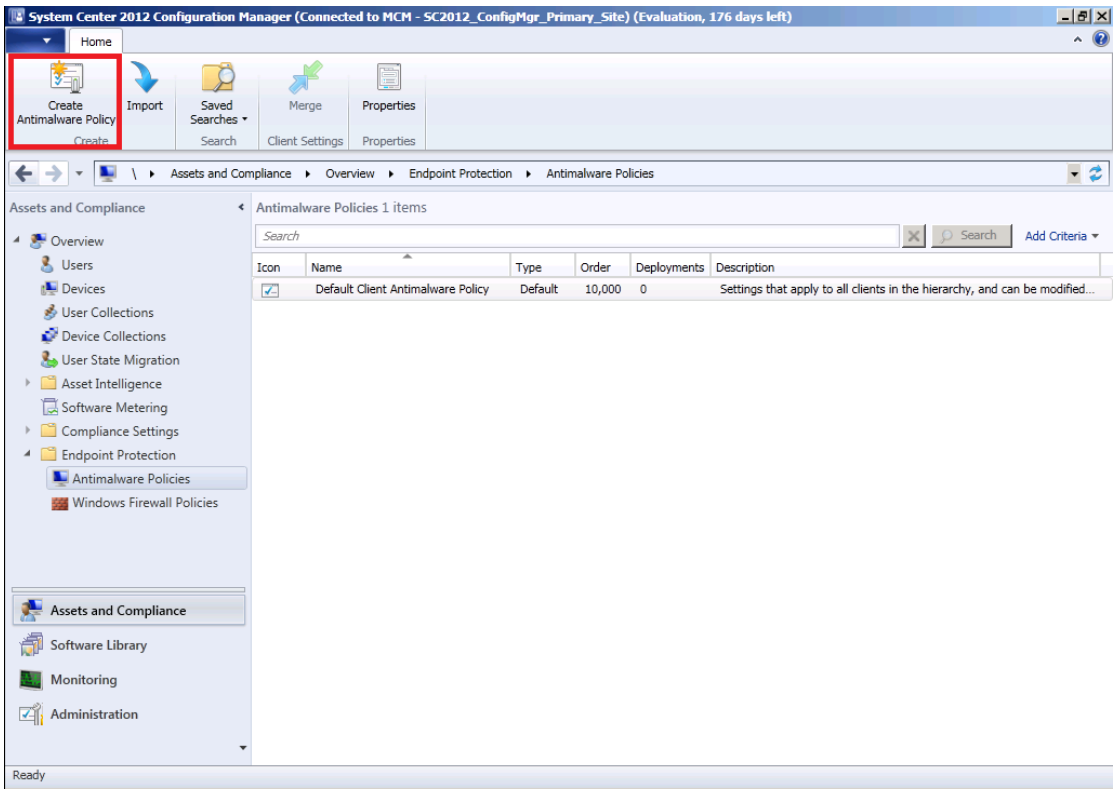
Justin Gao 高扬

yanga@microsoft.com

http://blogs.technet.com/b/justin_gao

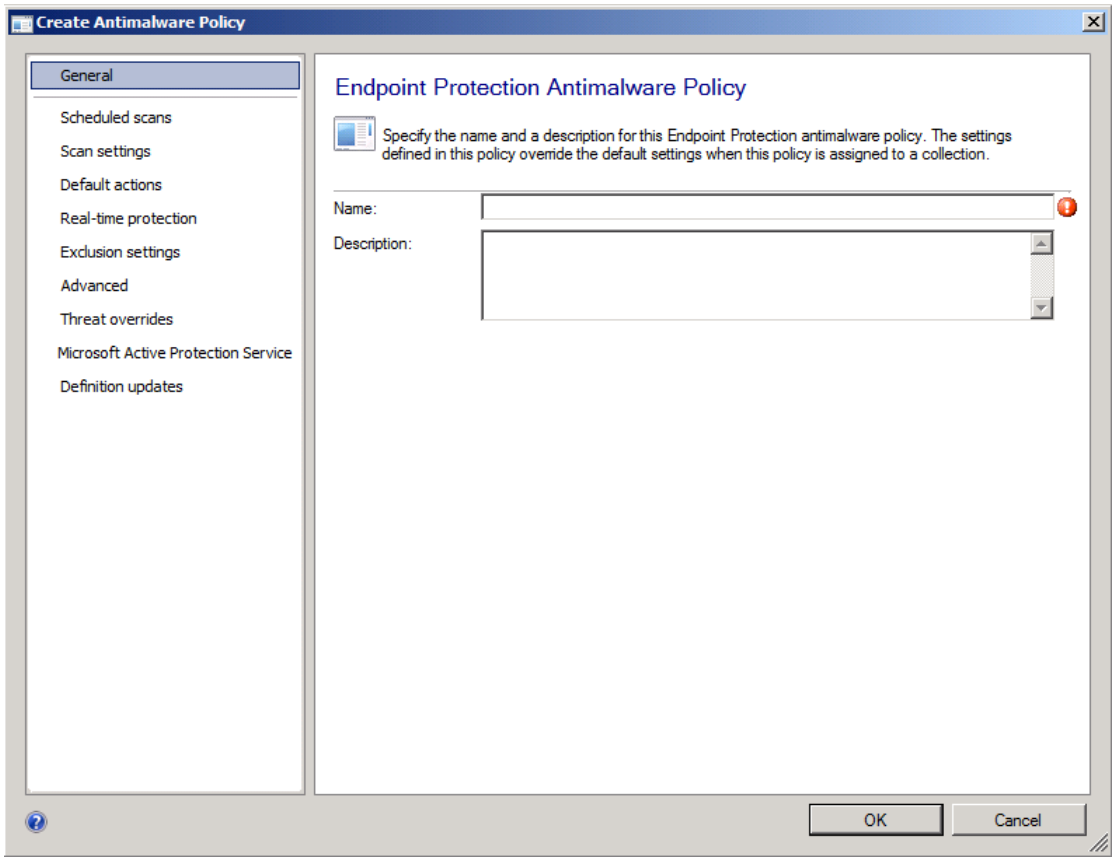
7. Configure Custom AntiMalware Policies and deploy Policy and updates :

1) Click the **Assets and Compliance** workspace , expand **Endpoint Protection** , click **Antimalware Policies** , click **Create Antimalware Policy** on the Ribbon :

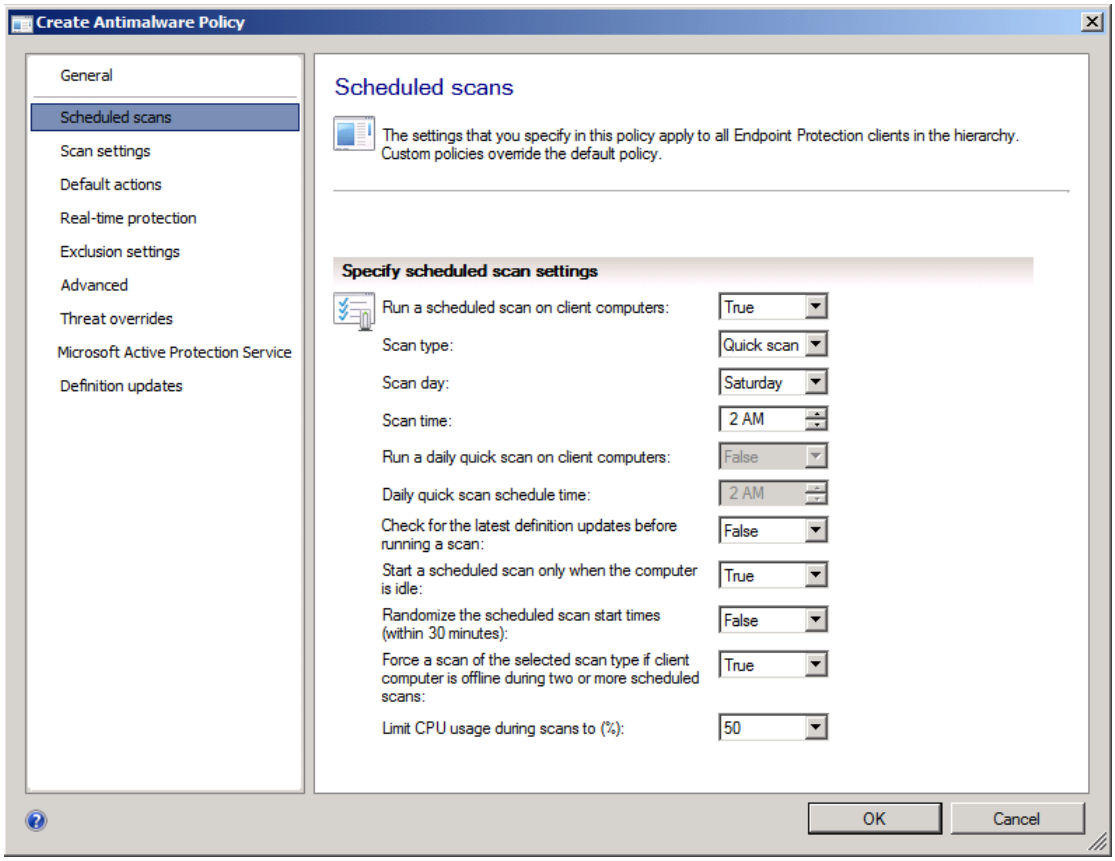


2) The **Create Antimalware Policy** dialog box appears :

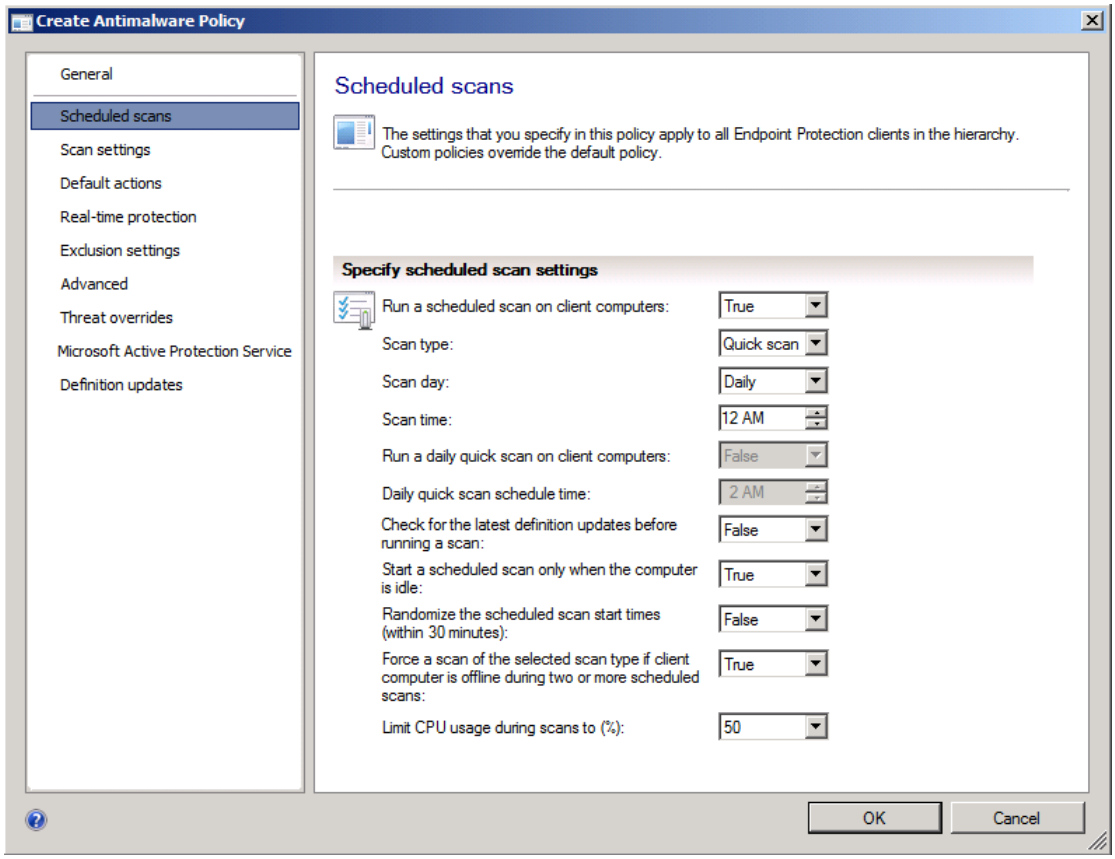
Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao



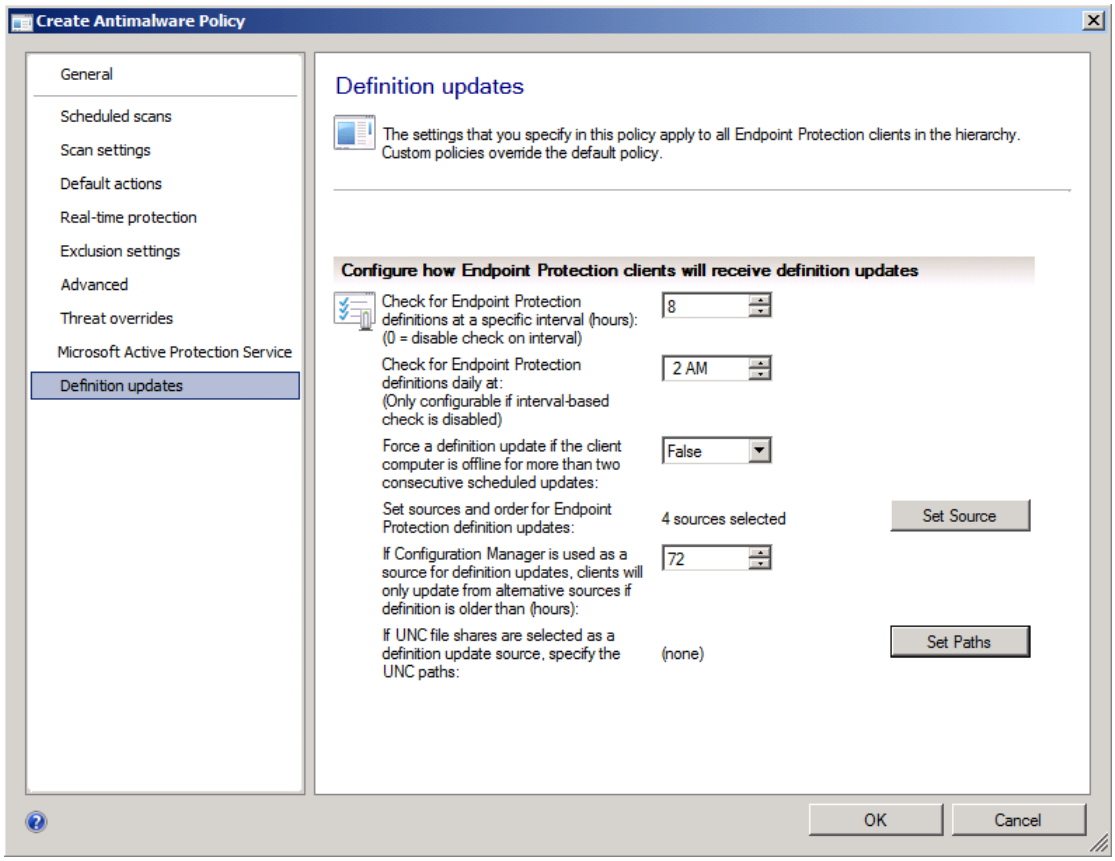
3) In the **Name** box , type name , and then click **Scheduled scans** :



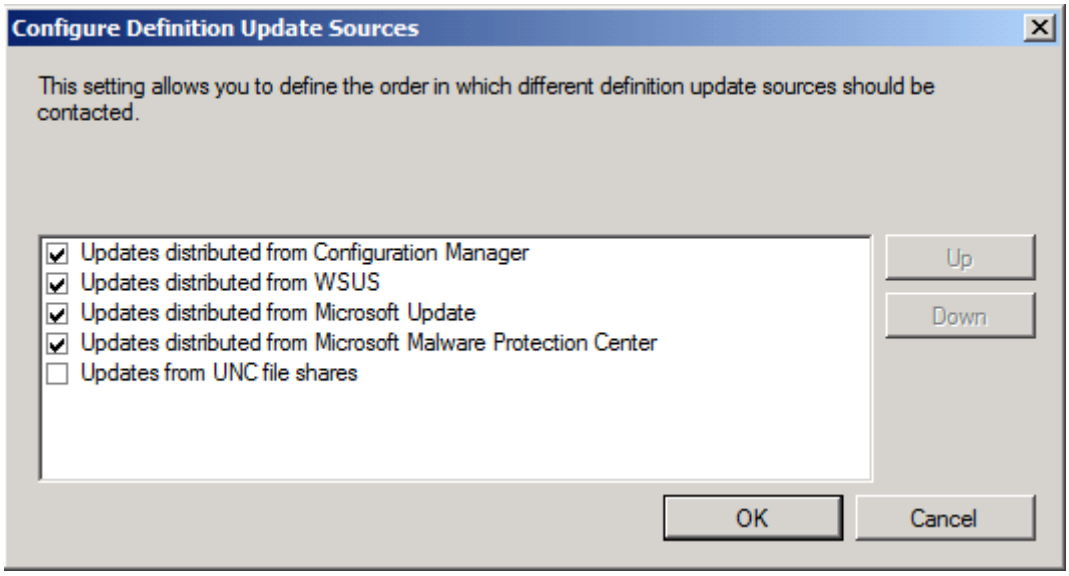
4) In the **Scan day** box ,click **Daily** , in the **Scan time** box , click **12AM** , you are configuring additional settings for visual confirmation of the implementation of the custom policy :



5) In the navigation pane , click **Definition updates** :

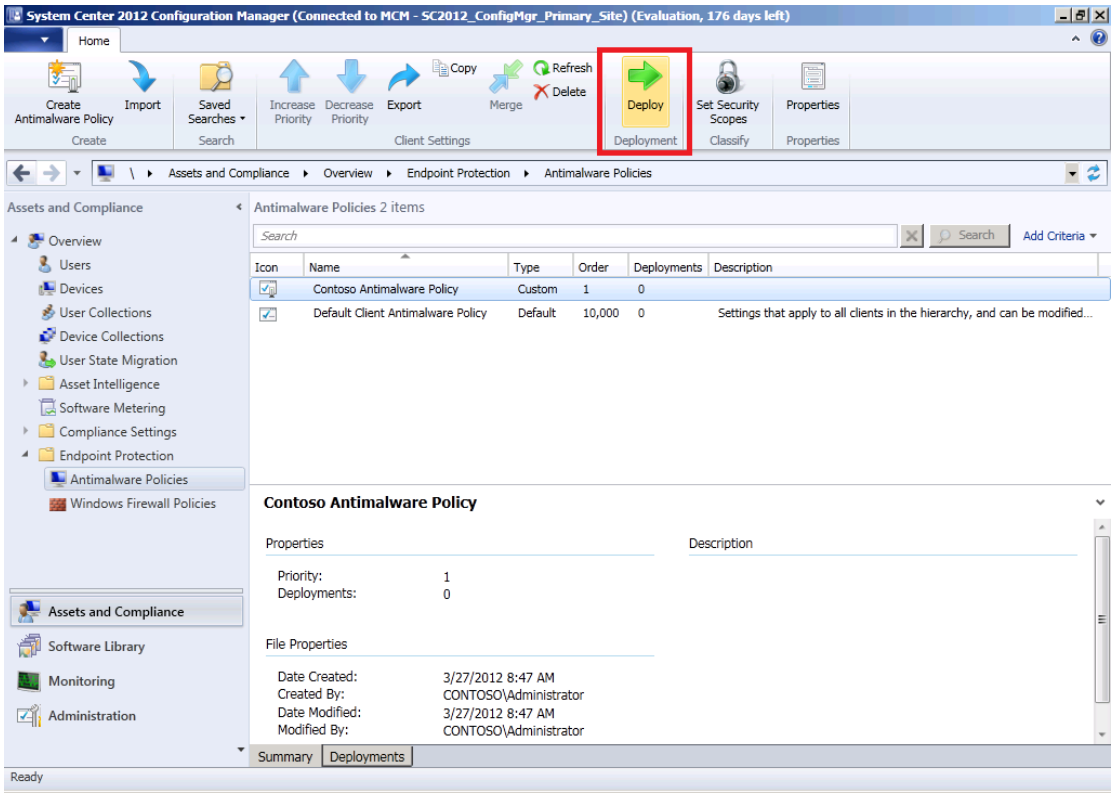


6) Click **Set Source** , the Configure Definition Update Sources dialog box appears , you can select your needs update source and priority :

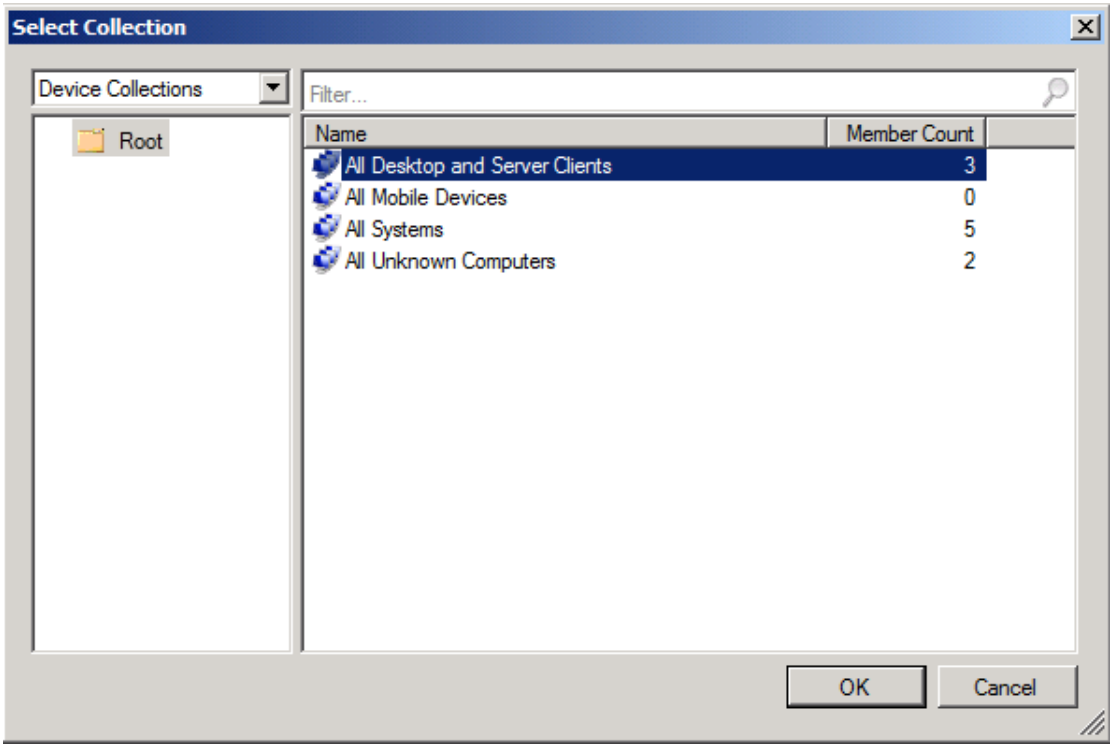


7) Click **OK** twice . In the results pane , click just created policy , and then on

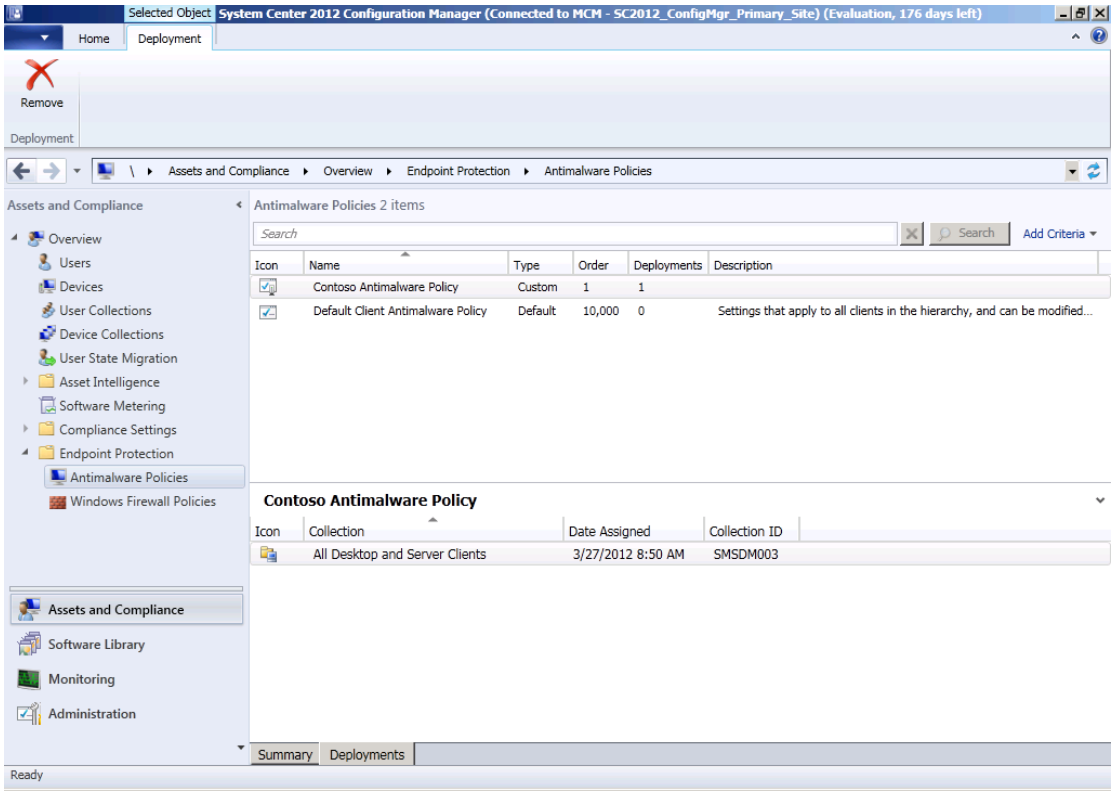
the Ribbon , click **Deploy** :



8) A **Select Collection** dialog box appears :

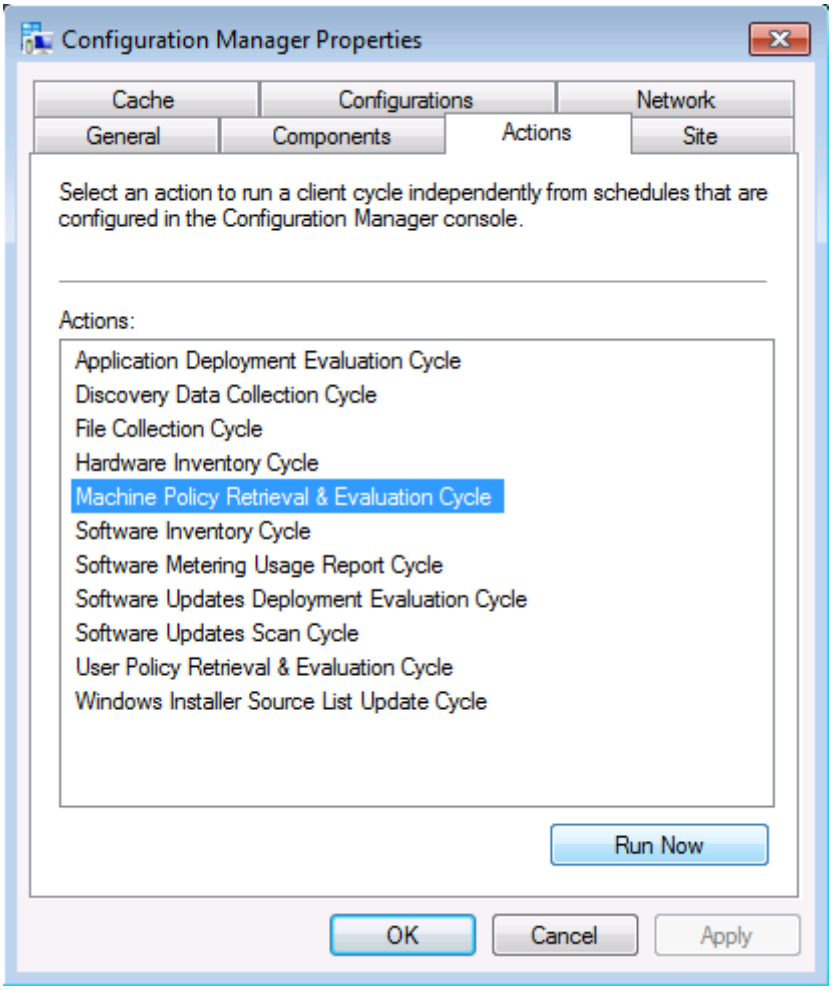


9) Select any **Device Collections** and click **OK** , you can saw this policy having been deployed to one collection :

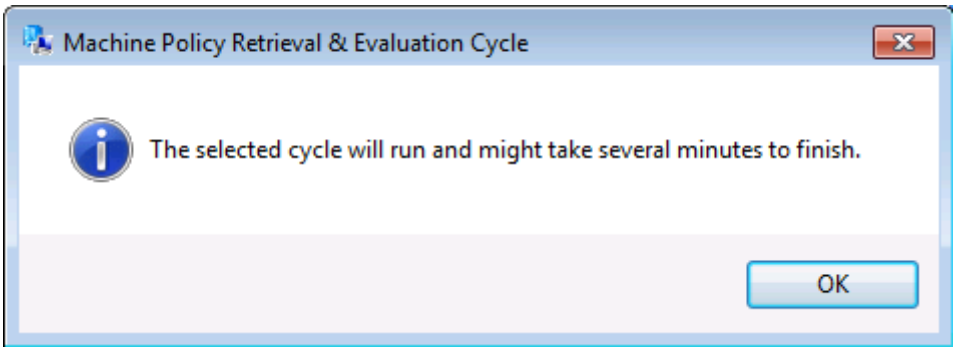


10) Logon **Client** computer , in **Control Panel** , click **System and Security** , and then start **Configuration Manager** , click the **Actions** tab , click **Machine Policy Retrieval & Evaluation Cycle** , and then click **Run Now** :

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

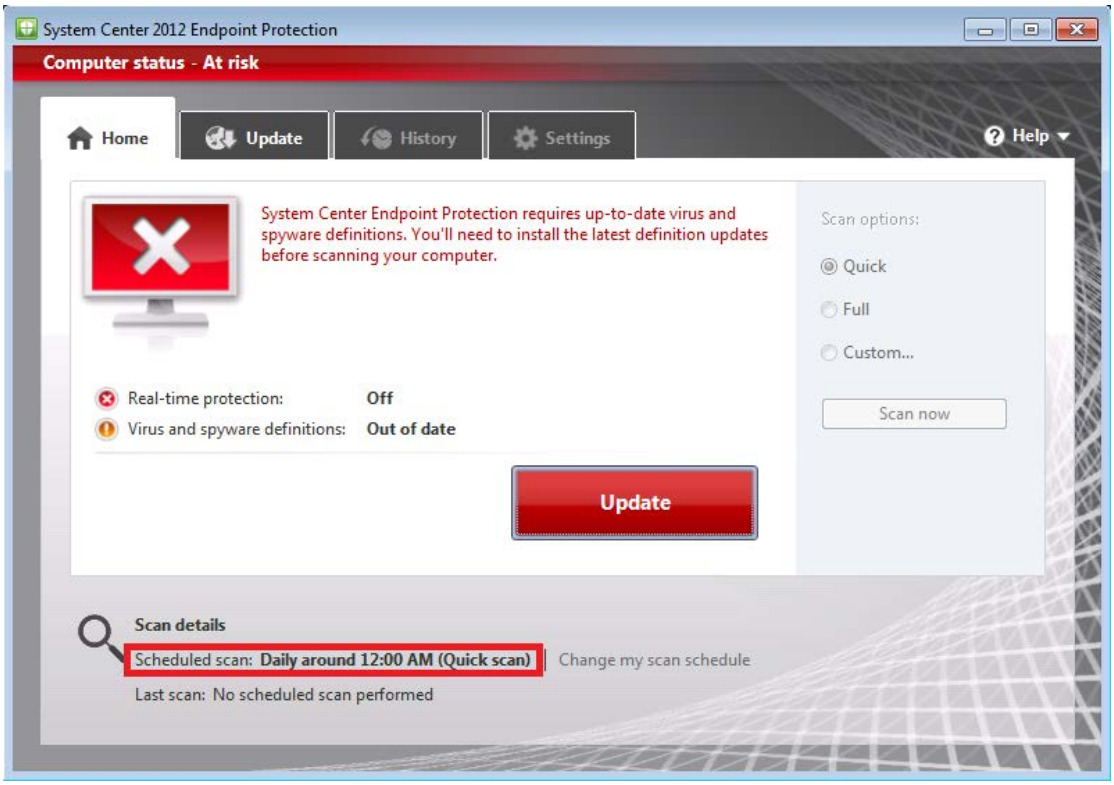


11) A **Machine Policy Retrieval & Evaluation Cycle** message box appears :



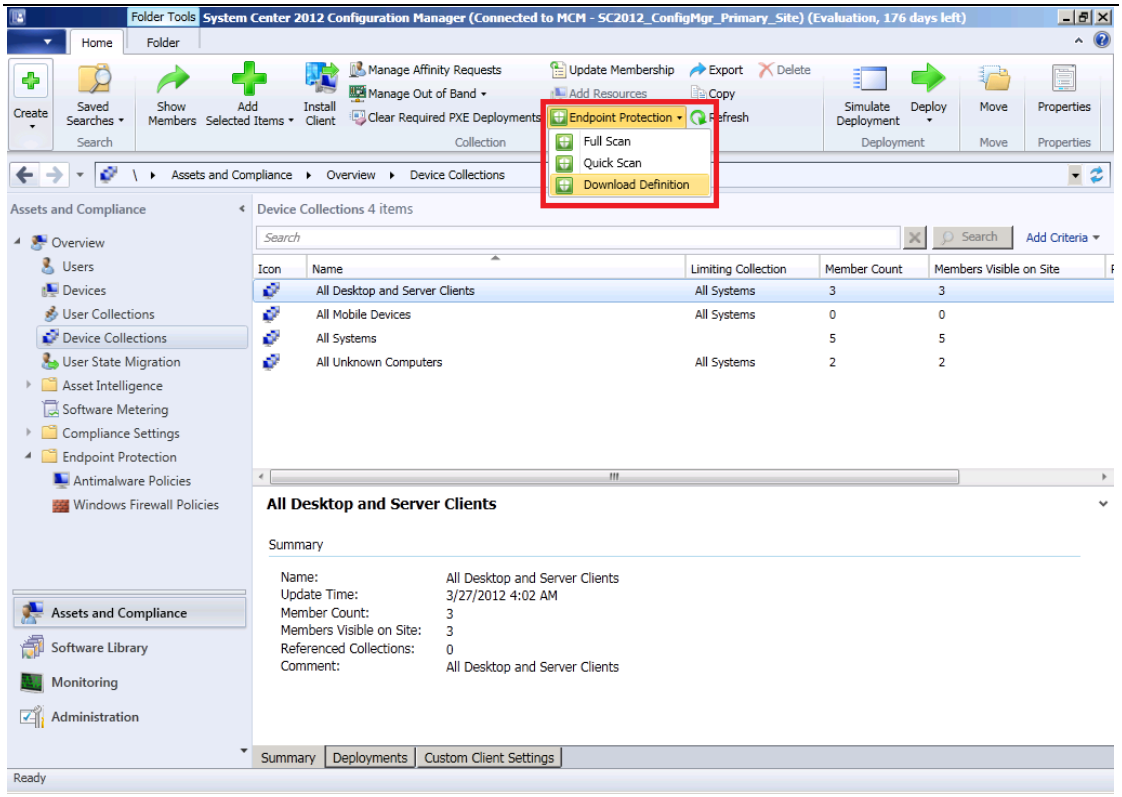
12) Click **OK** . On the **Start** menu , click **System Center 2012 Endpoint Protection** , The **System Center 2012 Endpoint Protection** window appears , under **Scan details** , it indicated that the scan schedule is now for **daily** quick scans ,

around midnight :

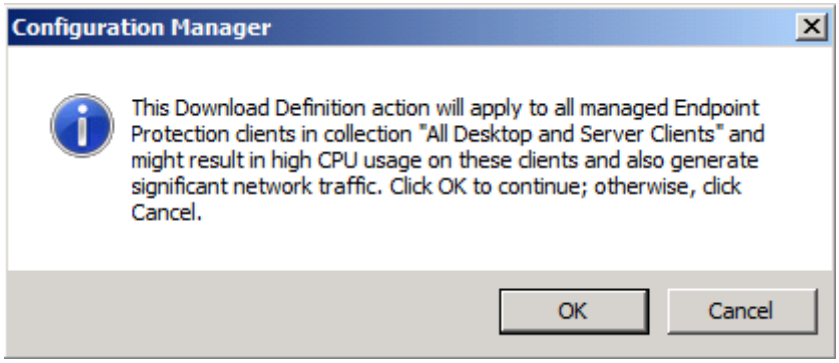


13) This process has not initiated a definition update cycle which occurs automatically every eight hours. You will force it to occur in the next procedure .Close the **System Center 2012 Endpoint Protection** window.

14) Logon to **ConfigMgr2012** server , click the **Assets and Compliance** workspace , click **Device Collections** , click **All Desktop and Server Clients** , and then on the Ribbon , click **Endpoint Protection** , click **Download Definition** :

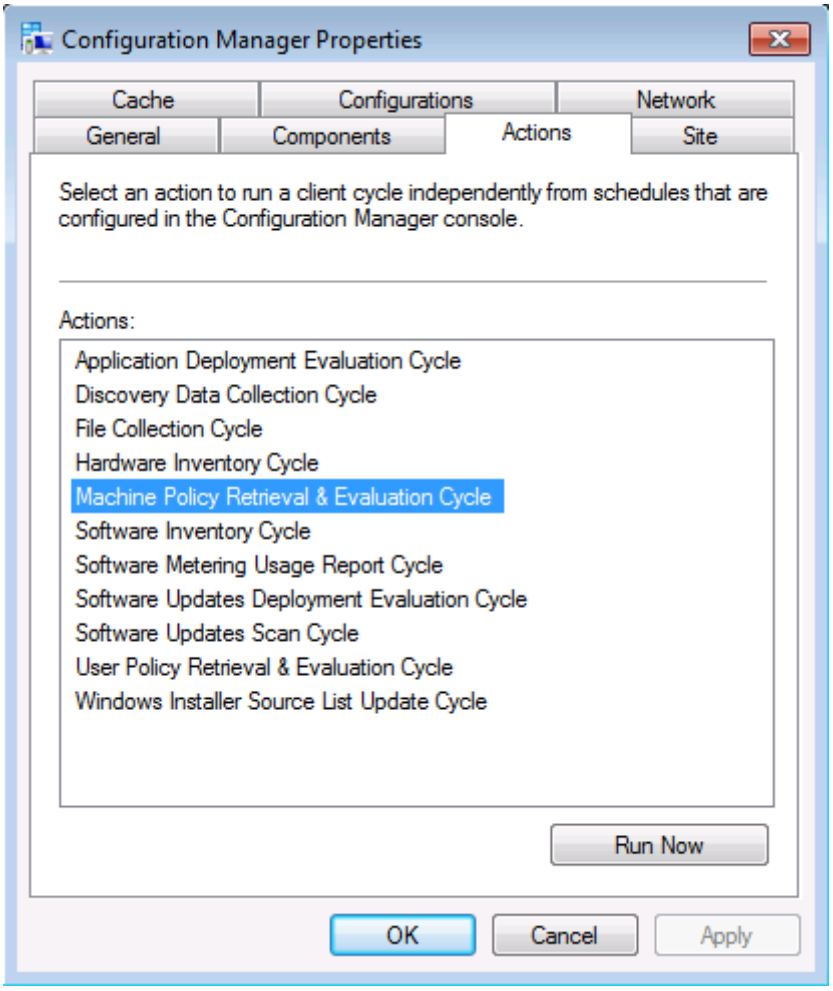


15) A **Configuration Manager** message box appears :

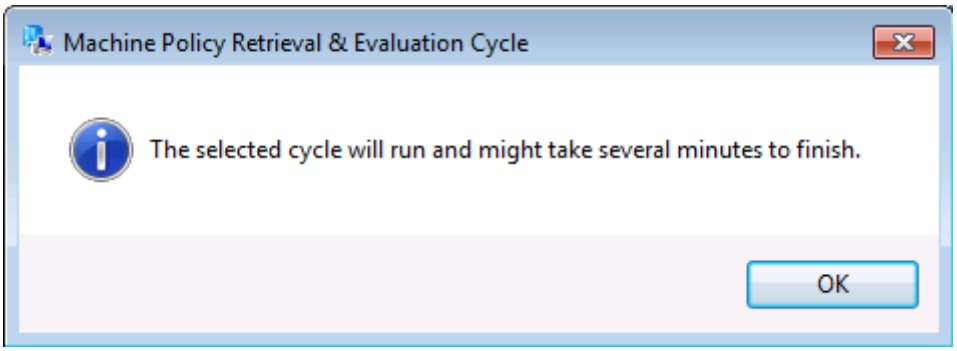


16) Click **OK** , clients will need to retrieve policies in order to process the request to download definitions . You can force policy retrieval in the next procedure. Logon to **Client** computer , in Control Panel , click System and Security , and then start Configuration Manager , click the Actions tab , click **Machine Policy Retrieval & Evaluation Cycle** , and then click **Run Now** :

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

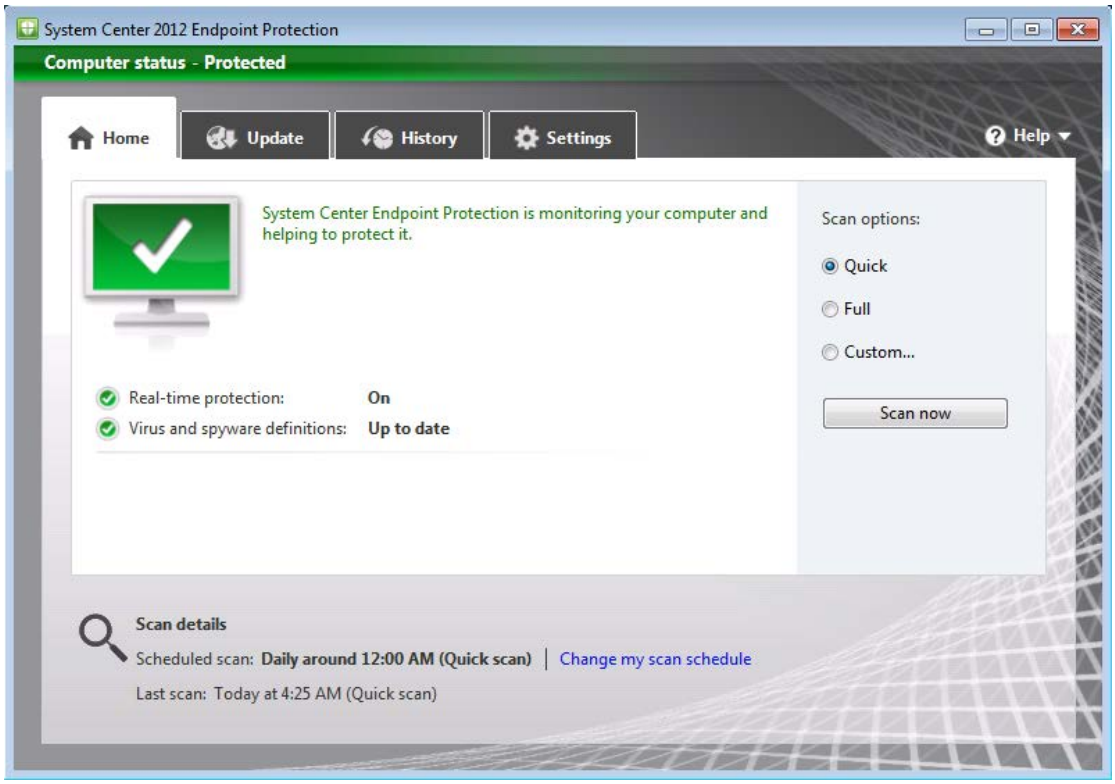


17) A **Machine Policy Retrieval & Evaluation Cycle** message box appears :



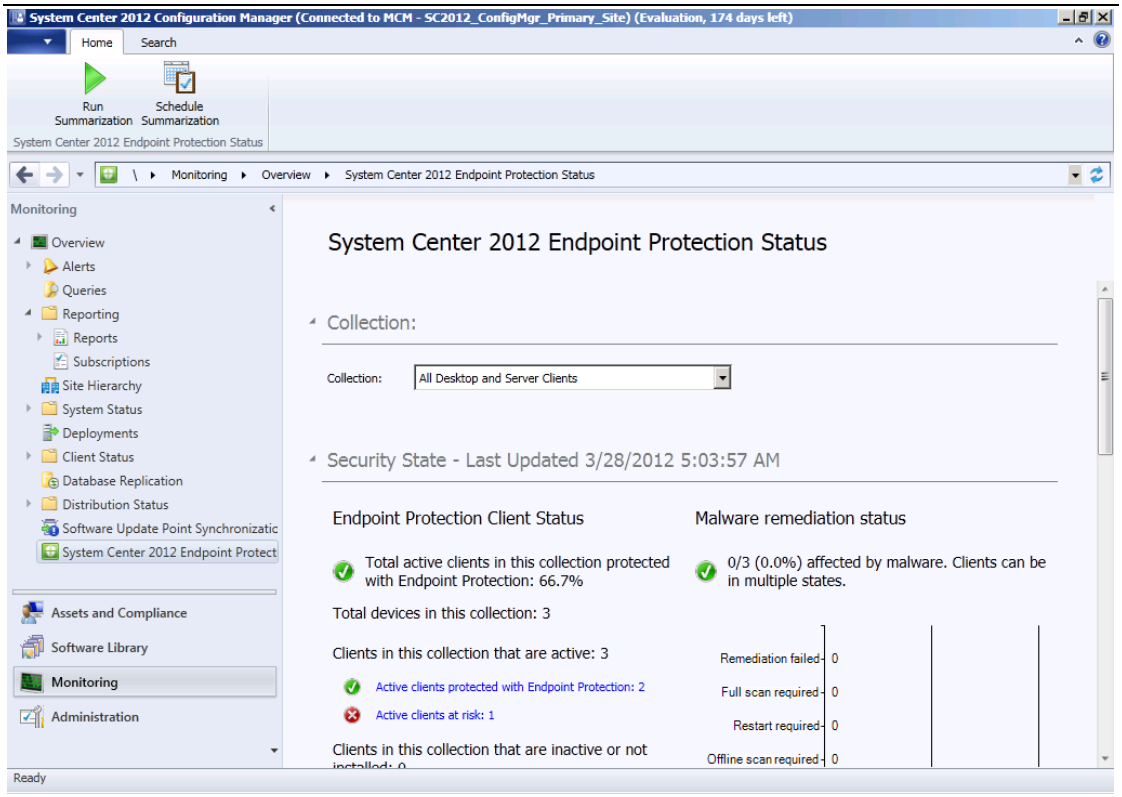
18) Click **OK** . The Endpoint Protection definition will be downloaded on the **Client** computer . Waiting some minutes , on the **Start** menu , click **System Center 2012 Endpoint Protection** , the **System Center 2012 Endpoint Protection** window

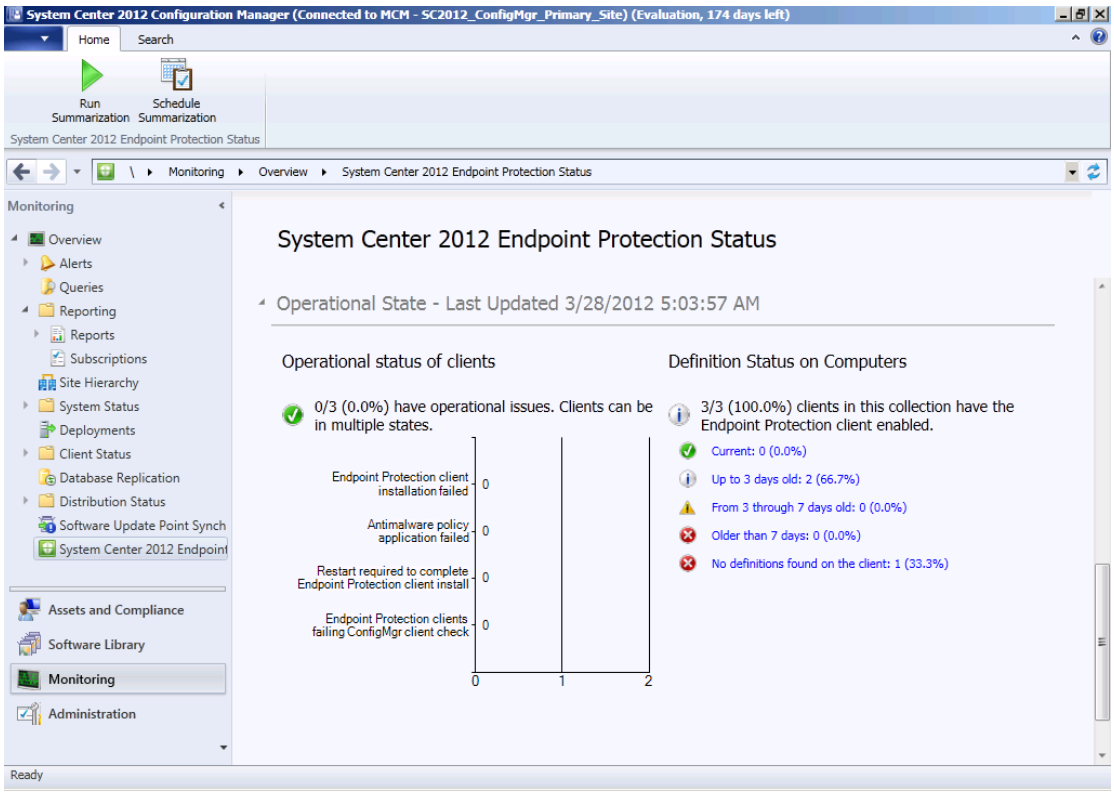
Appears displaying current status of the Endpoint Protection client , which now should be **Protected** . Notice that **Virus and spyware definitions** shows a status with a newer definition file :



19) Click **Help** , you can see about information :

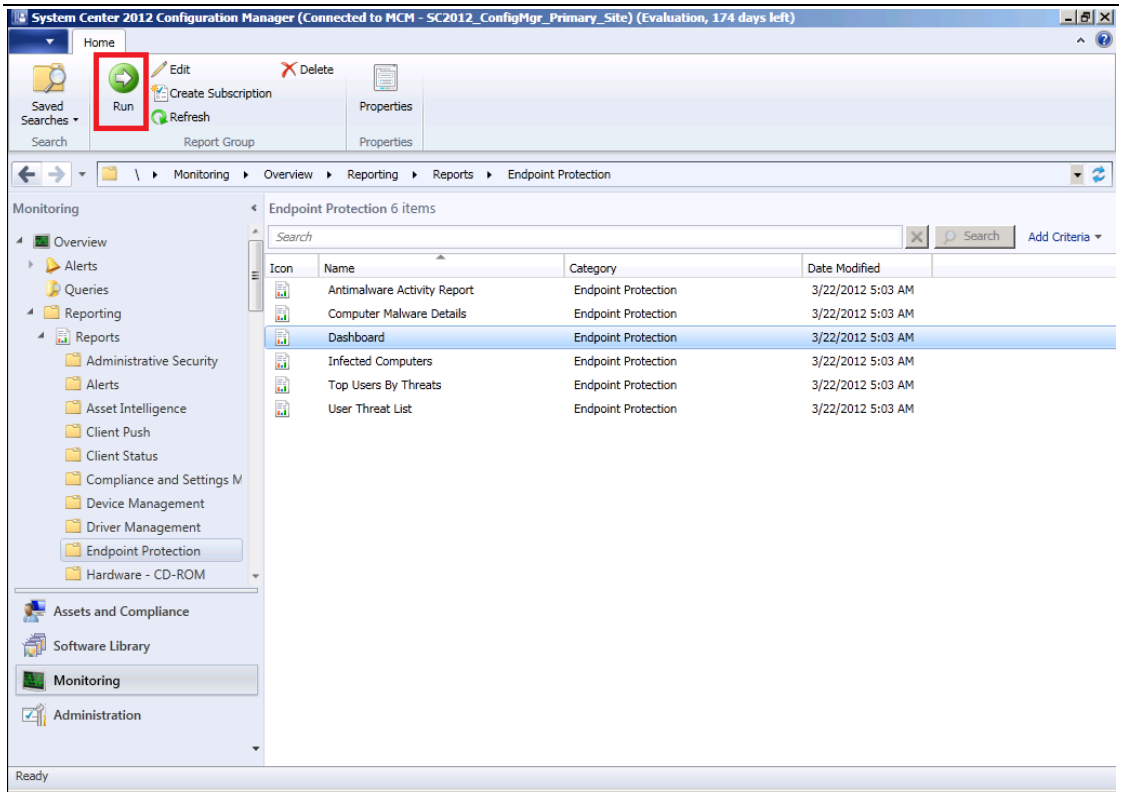
20) Click **OK** to close . Click the **Monitoring** workspace , click **System Center 2012 Endpoint Protection Status** , you can see the newest **Security State** and **Operational State** :





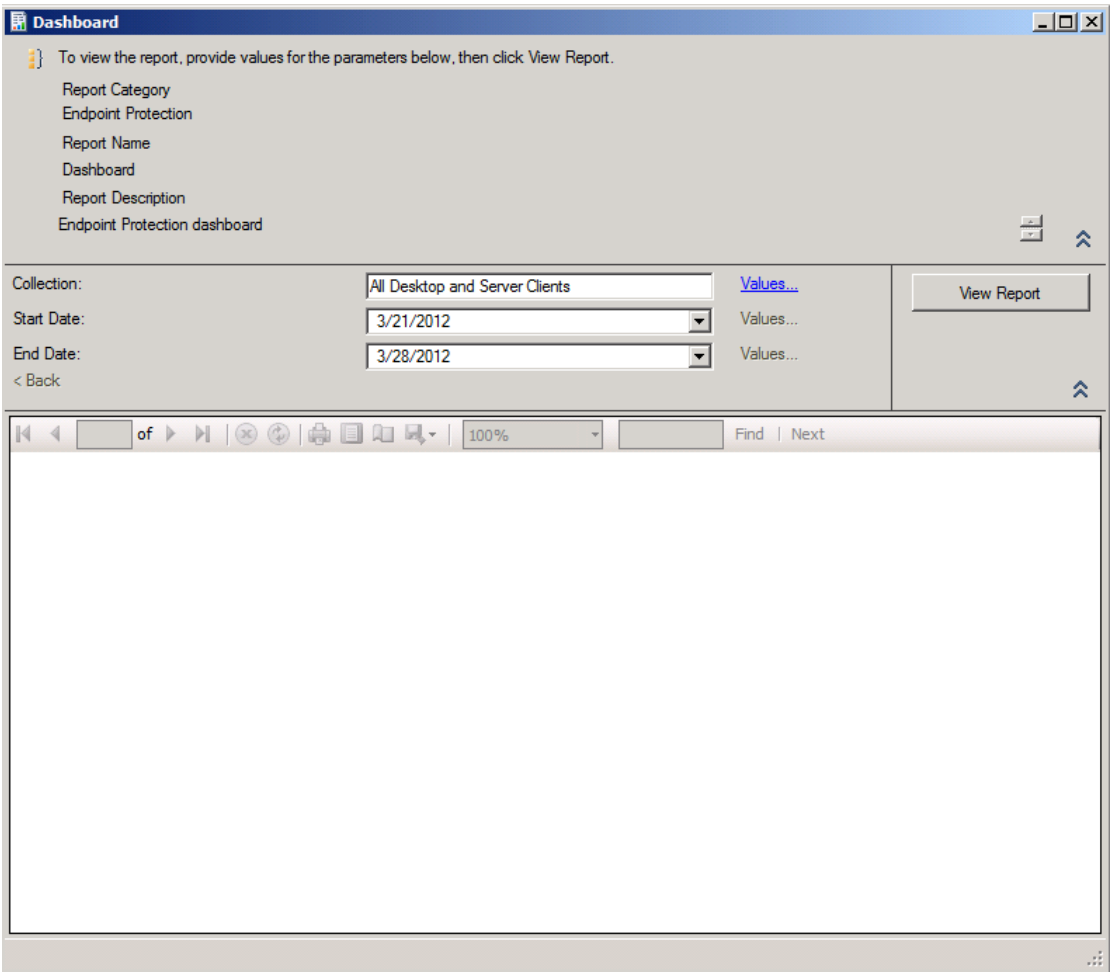
21) Expand **Reporting** , expand **Reports** , and then click **Endpoint Protection** , in the results pane , click **Dashboard** , and then on the Ribbon click **Run** :

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

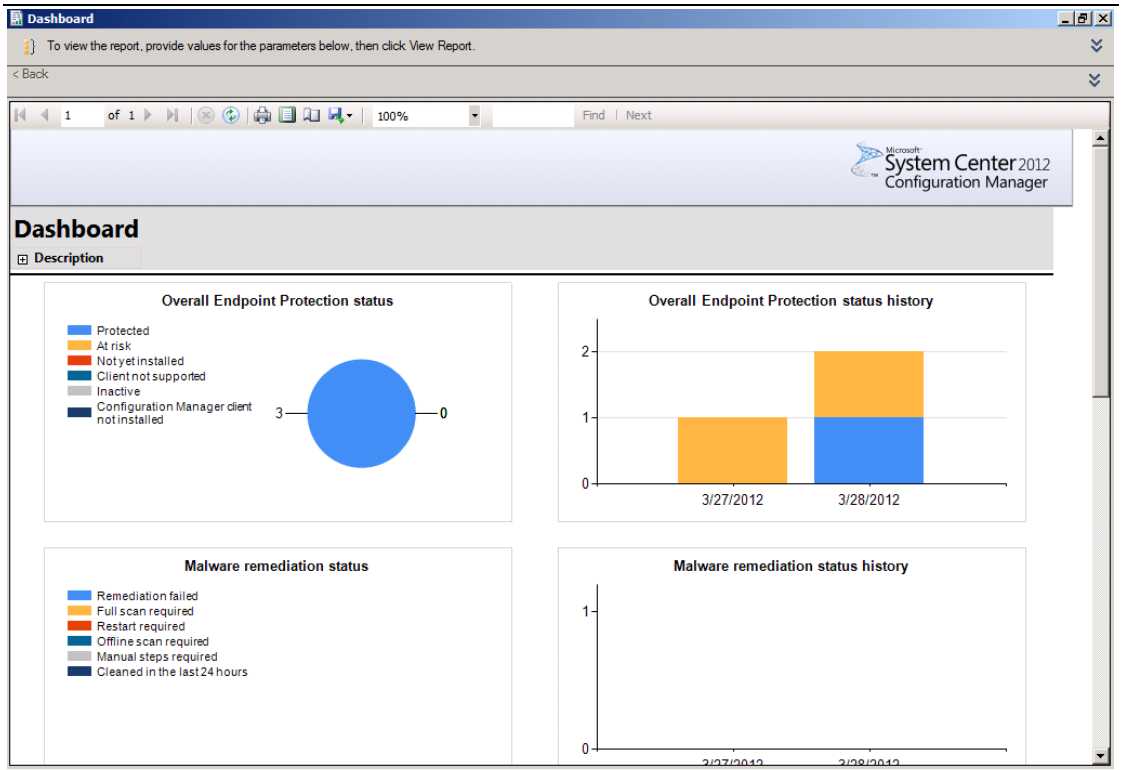


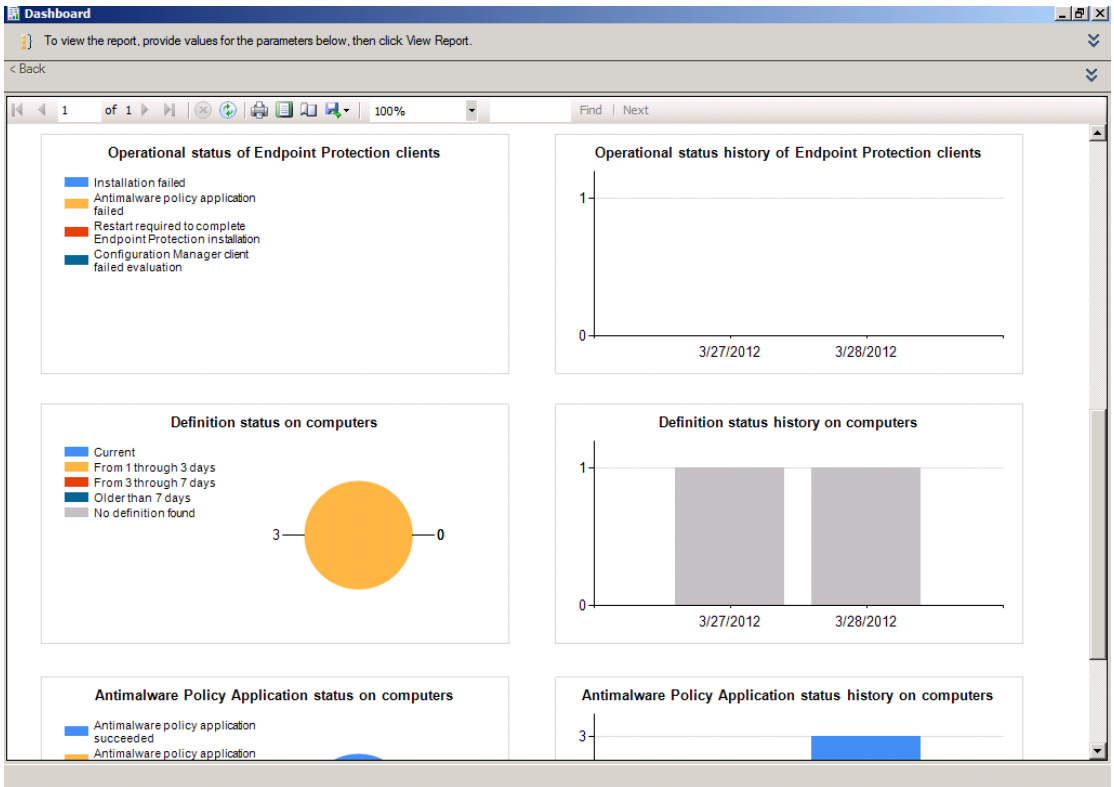
22) The **Dashboard** window appears . After **Collection** , click **Values...** , the **Parameter Value** dialog box appears , under **Collection** , click **All Desktop and Server Clients** , and then click **OK** :

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

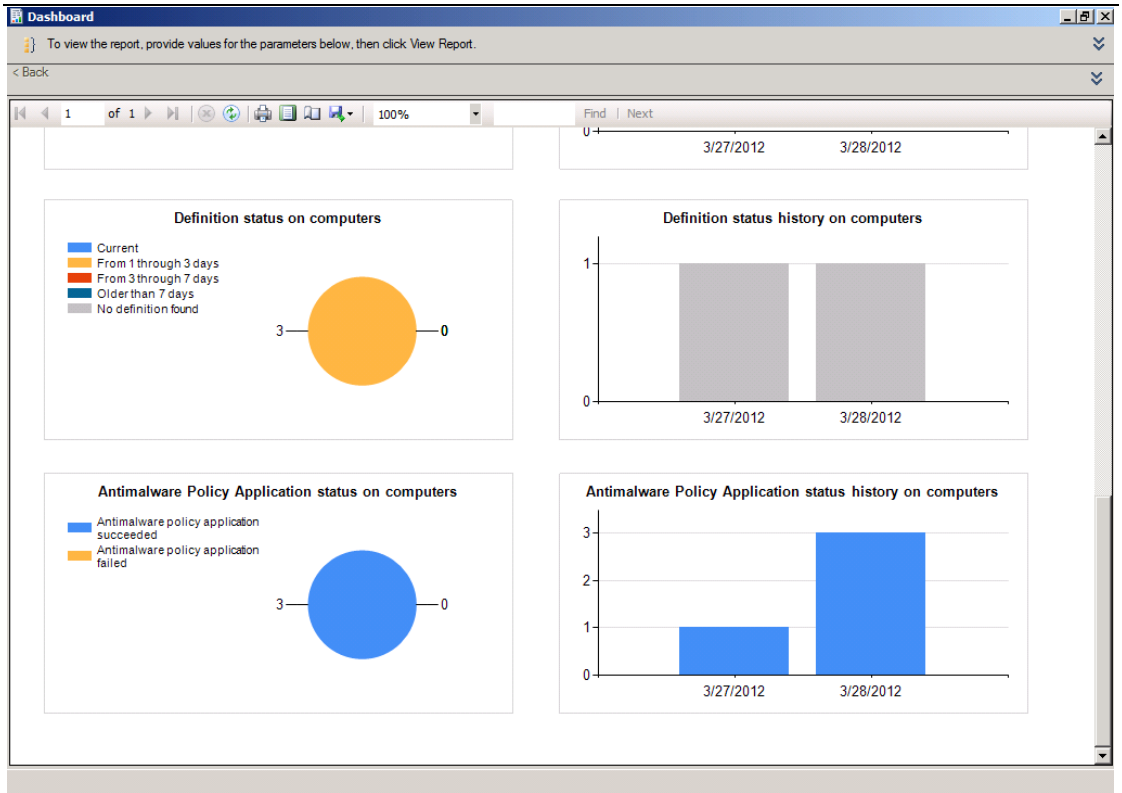


23) Click **View Report** , the **Dashboard** Report window appears :





Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao



24) Now I have finished System Center 2012 Configuration Manager RTM Endpoint Protection document .

Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao