

Microsoft System Center 2012 Configuration Manager RTM Endpoint Protection Document

Mar.25 2012



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**.

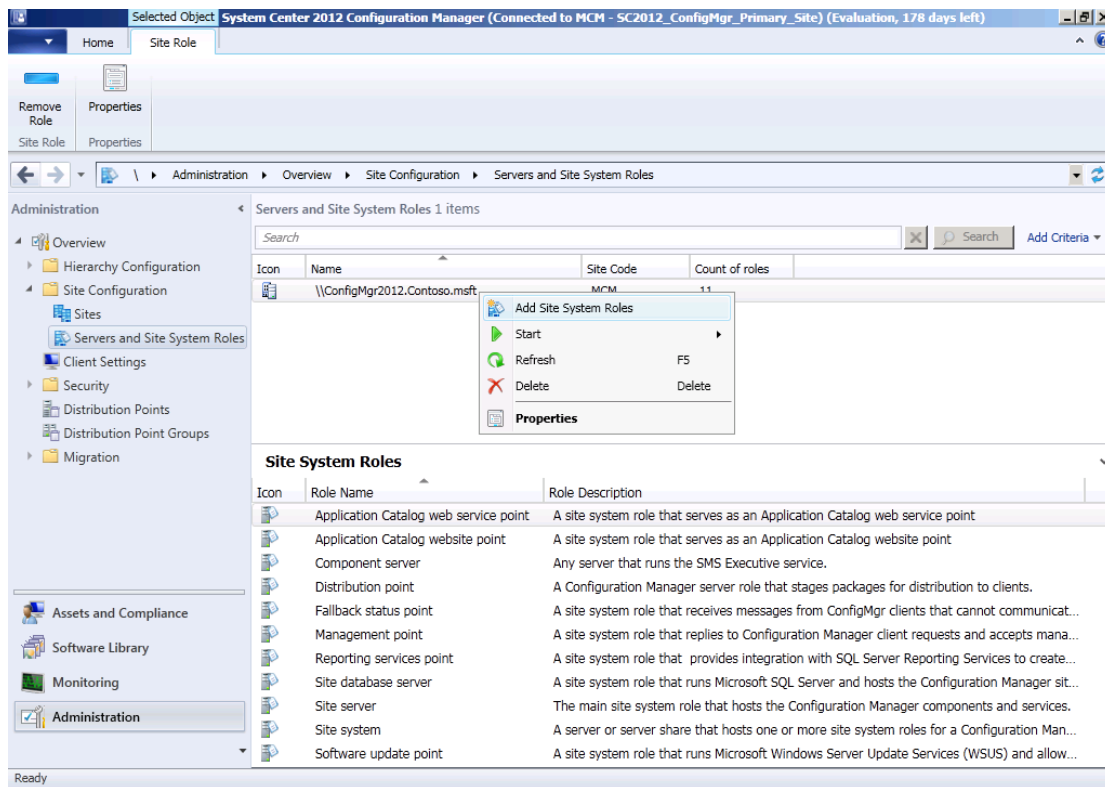
This process is no longer described in this part.

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**》

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** :

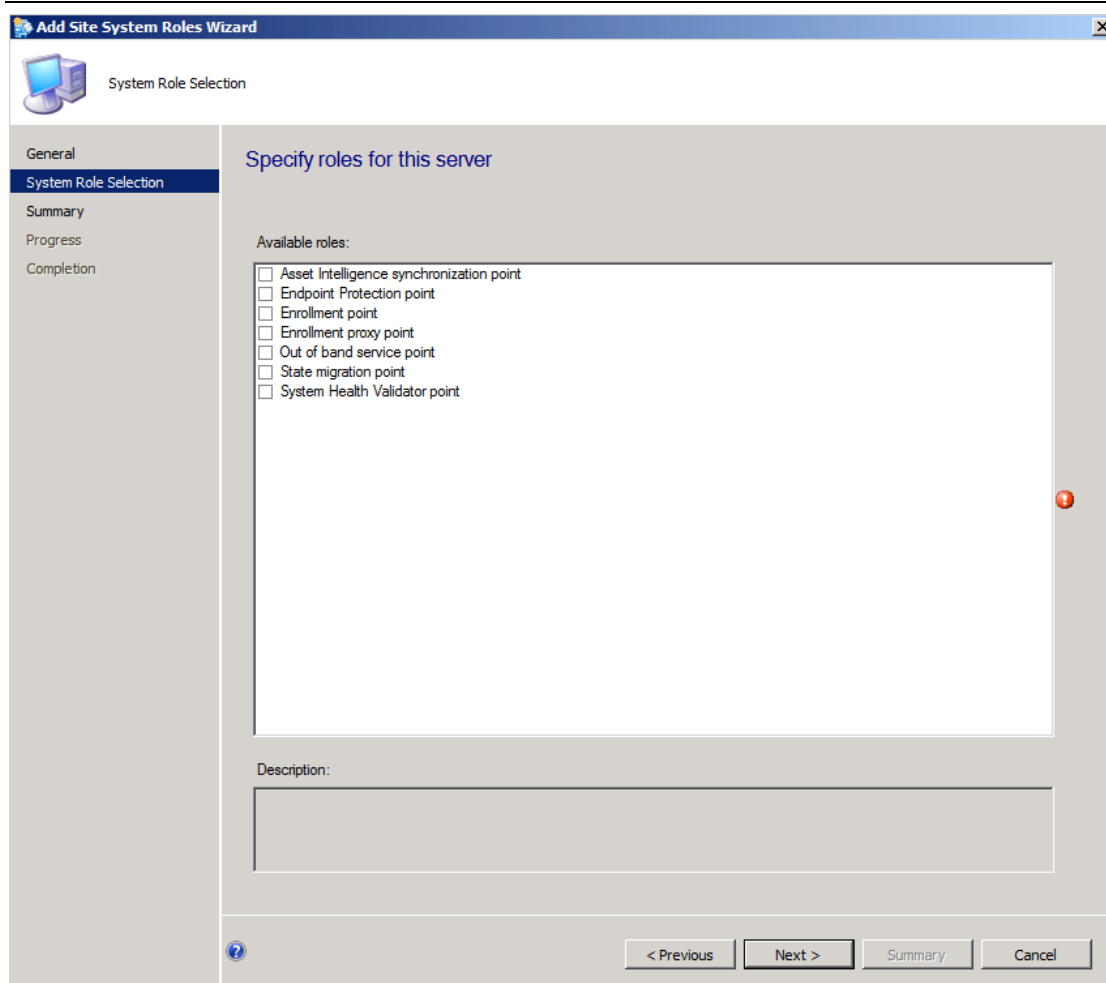


2) The **Add Site System Roles Wizard General** dialog box appears :

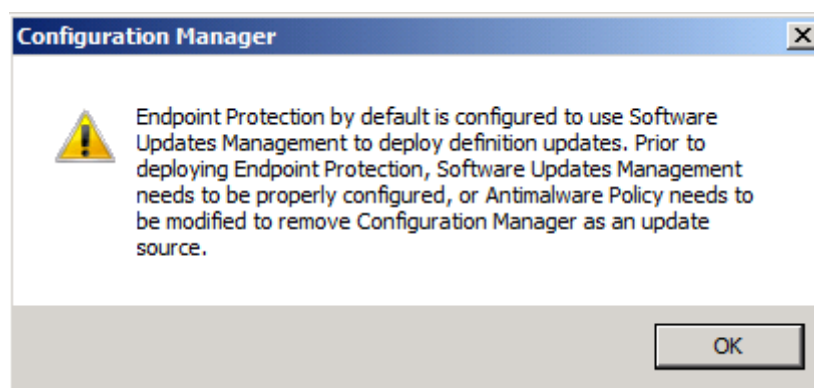
**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

The screenshot shows the 'Add Site System Roles Wizard' dialog box with the 'General' tab selected. The left sidebar contains links for 'General', 'System Role Selection', 'Summary', 'Progress', and 'Completion'. The main area is titled 'Select a server to use as a site system'. It includes a 'Name' field with the example 'server1.corp.contoso.com' and a 'Browse...' button. Below is a 'Site code' dropdown menu showing 'MCM - SC2012_ConfigMgr_Primary_Site'. There are two checkboxes: 'Specify an FQDN for this site system for use on the Internet' (unchecked) and 'Require the site server to initiate connections to this site system' (unchecked). The 'Specify an FQDN' section has an 'Internet FQDN' field with the example 'internetsrv2.contoso.com'. The 'Require the site server' section has a 'Site System Installation Account' section with two radio buttons: 'Use the site server's computer account to install this site system' (selected) and 'Use another account for installing this site system' (unchecked). Below the radio buttons is a text field and a 'Set...' button. The 'Active Directory membership' section has two fields: 'Active Directory forest' and 'Active Directory domain', both containing 'Contoso.msft'. At the bottom are buttons for '< Previous', 'Next >', 'Summary', and 'Cancel'.

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

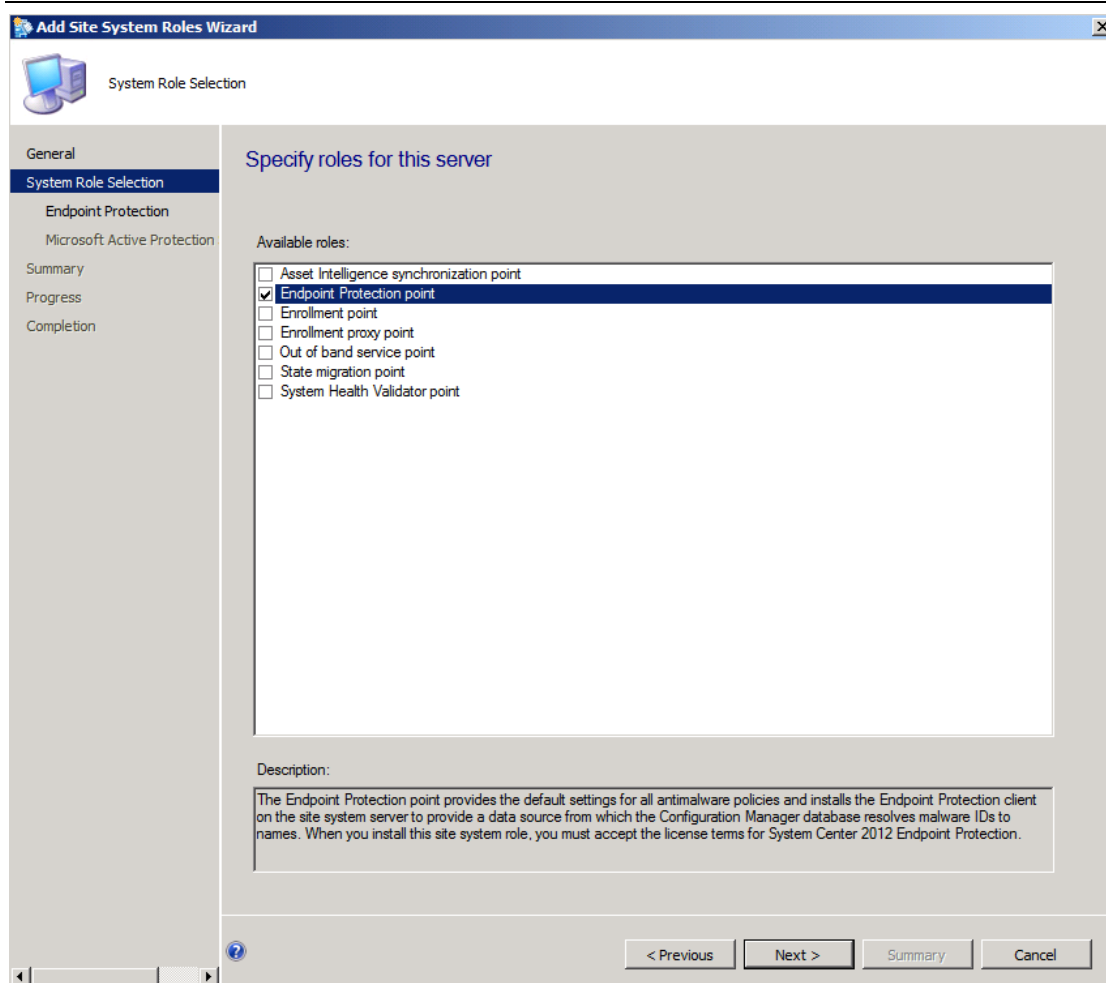


4) Under **Available roles** , select **Endpoint Protection point** , a **Configuration Manager** warning dialog box appears :



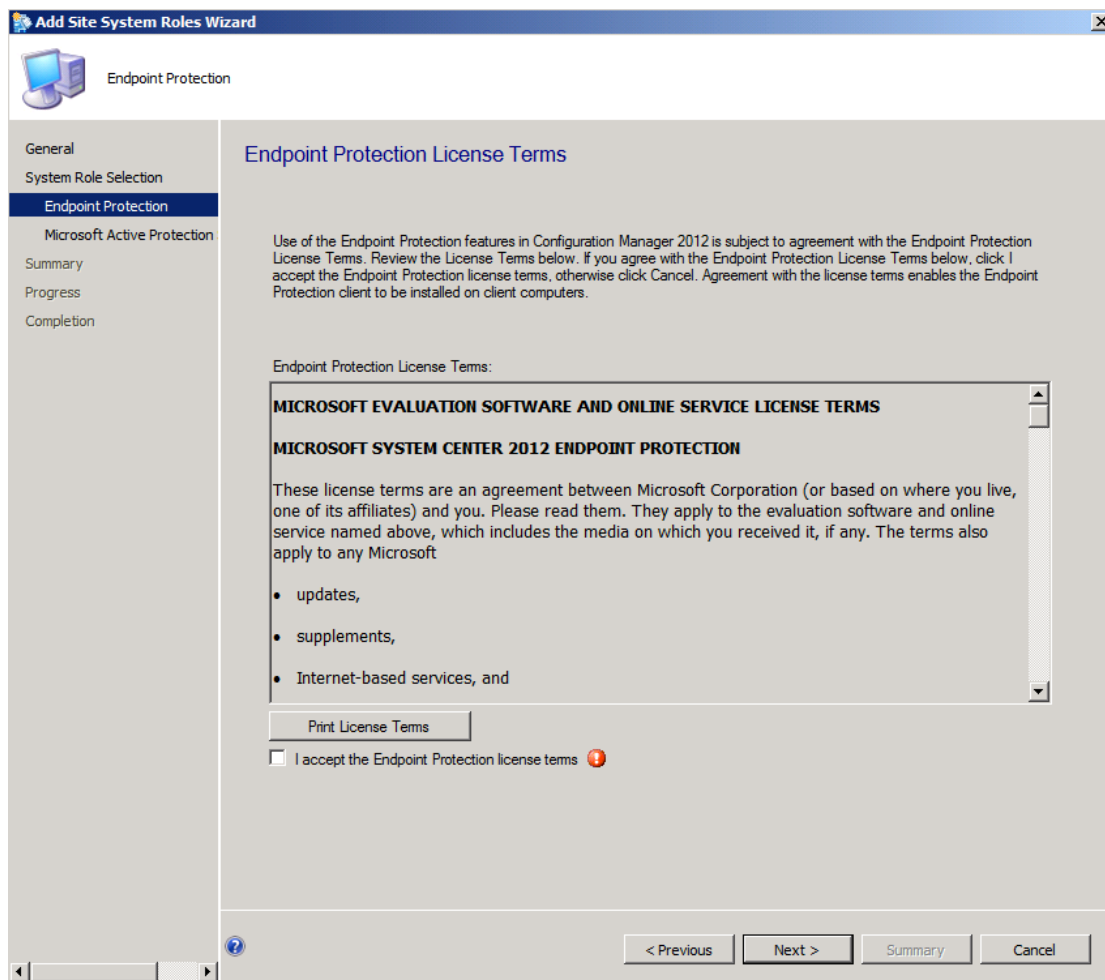
5) Click **OK** , will display select result :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

Add Site System Roles Wizard

Microsoft Active Protection Service

General
System Role Selection
Endpoint Protection
Microsoft Active Protection
Summary
Progress
Completion

Specify Microsoft Active Protection Service membership type

The Microsoft Active Protection Service (MAPS) membership type you choose will be applied to all EndPoint Protection antimalware policies. MAPS is a worldwide online community that includes System Center Endpoint Protection users. By joining MAPS, System Center Endpoint Protection will automatically send information to Microsoft to help Microsoft determine which software to investigate for potential threats and to help improve System Center Endpoint Protection's effectiveness. This community also helps stop the spread of new malicious software infections.

You can choose to join the MAPS community with either a Basic or Advanced membership. The type of information that is sent in reports to Microsoft depends on your level of MAPS membership. In some instances, personal information might unintentionally be sent to Microsoft. However, Microsoft will not use this information to identify you or to contact you.

For more information about MAPS and the information collected for reports, please read the MAPS membership levels below and the Privacy Statement at <http://go.microsoft.com/fwlink/?LinkID=223678>.

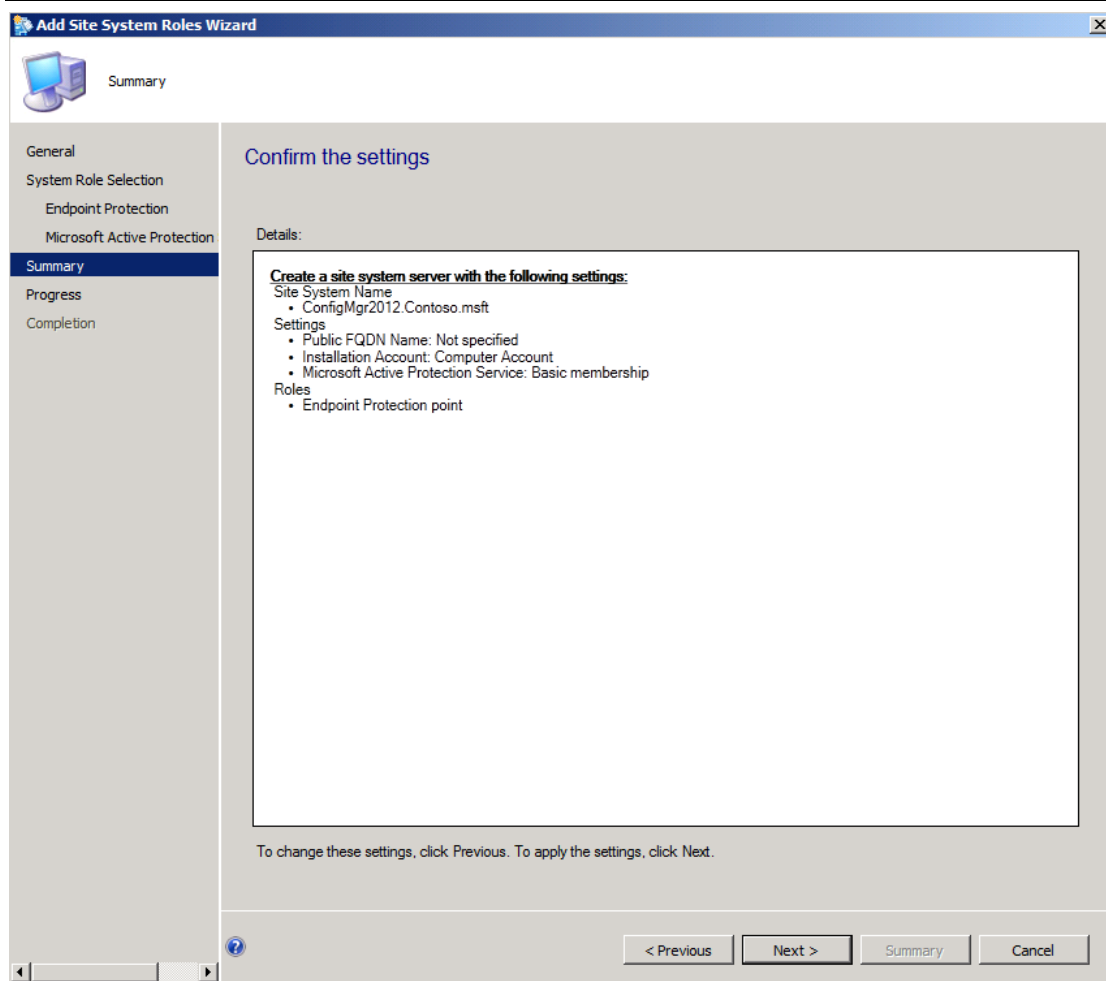
☐ Do not join MAPS
No information will be sent to Microsoft. You will not be alerted if unclassified software is detected running on your computer.

☒ Basic membership
Send information to Microsoft when System Center Endpoint Protection detects software or changes to your computer by software that has not yet been analyzed for risks. This information may include the actions that you apply to such software or that System Center Endpoint Protection applies automatically, according to your settings.

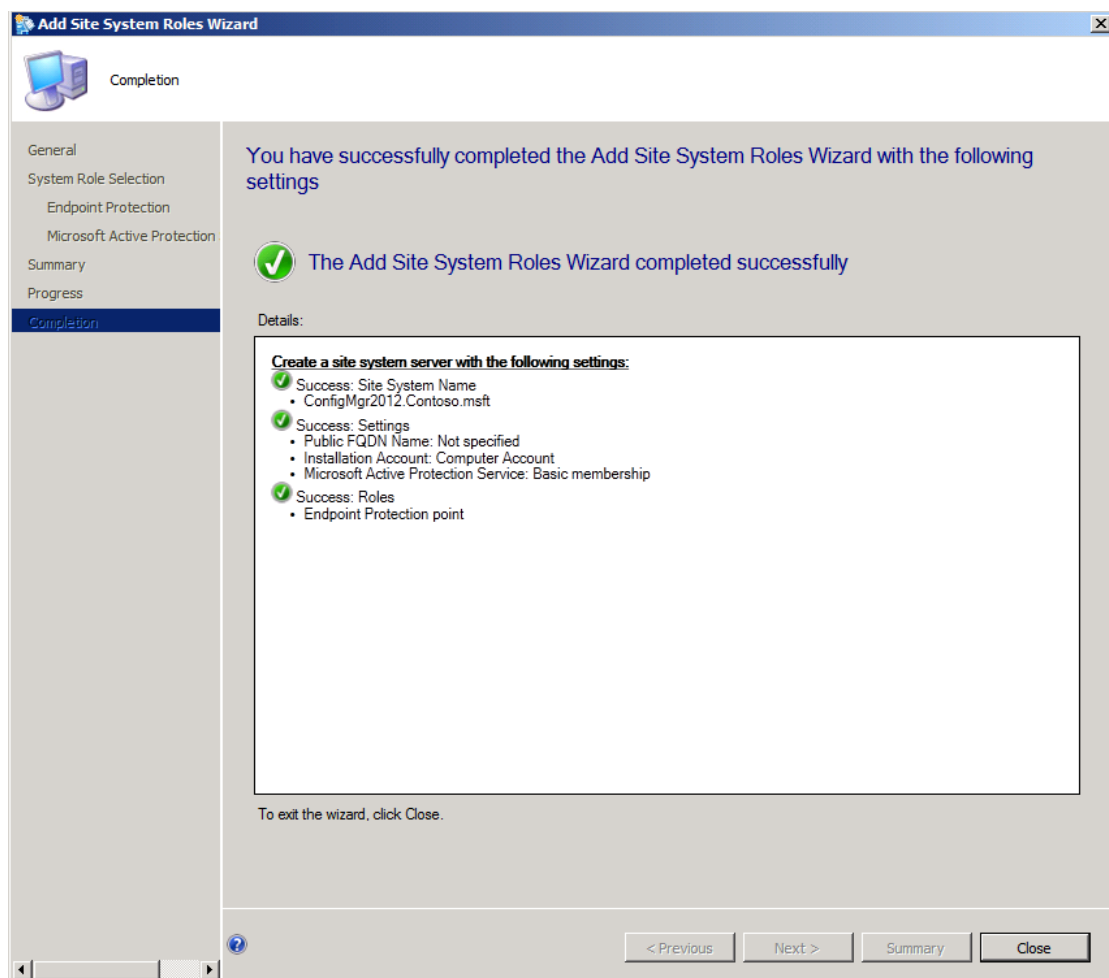
☐ Advanced membership
In addition to the information sent to Microsoft under the Basic membership, Advanced membership reports may include additional details about the software System Center Endpoint Protection detects, including the location of such software, file names, how the software operates, and how it has impacted your computer.

< Previous Next > Summary Cancel

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

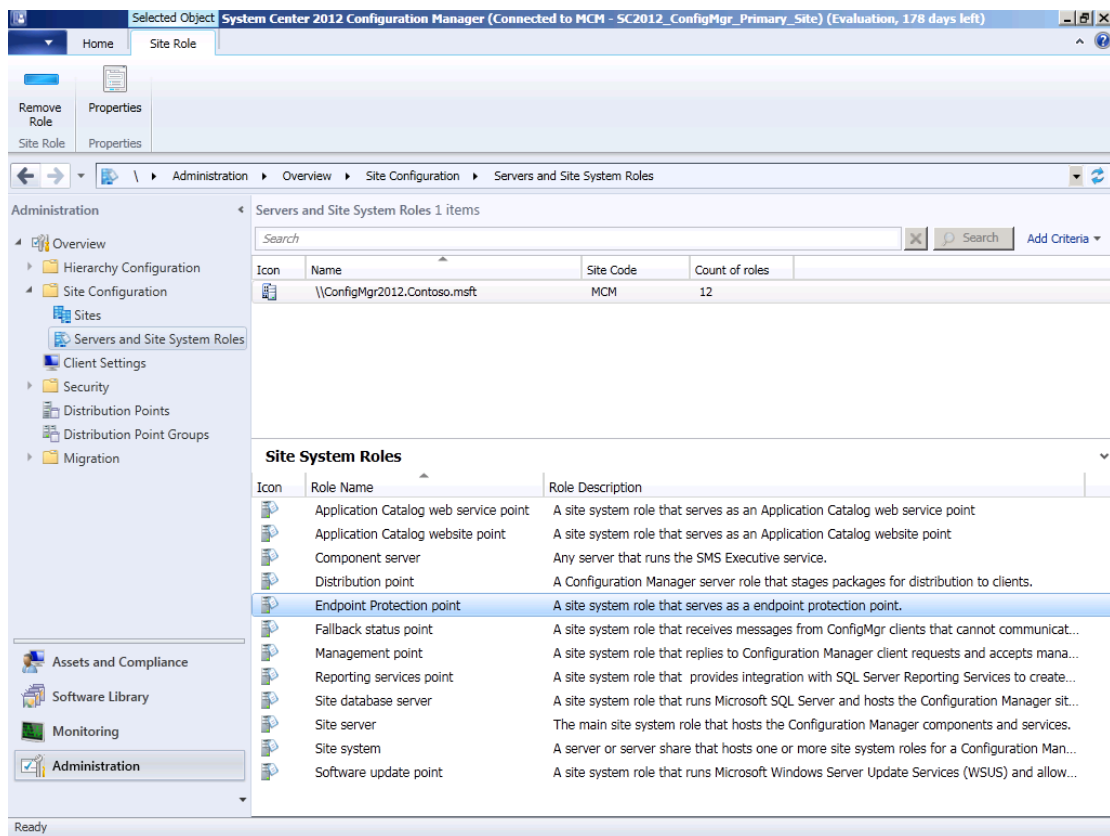


9) Click **Next** , the **Completion** dialog box appears indicating that the wizard completed successfully :

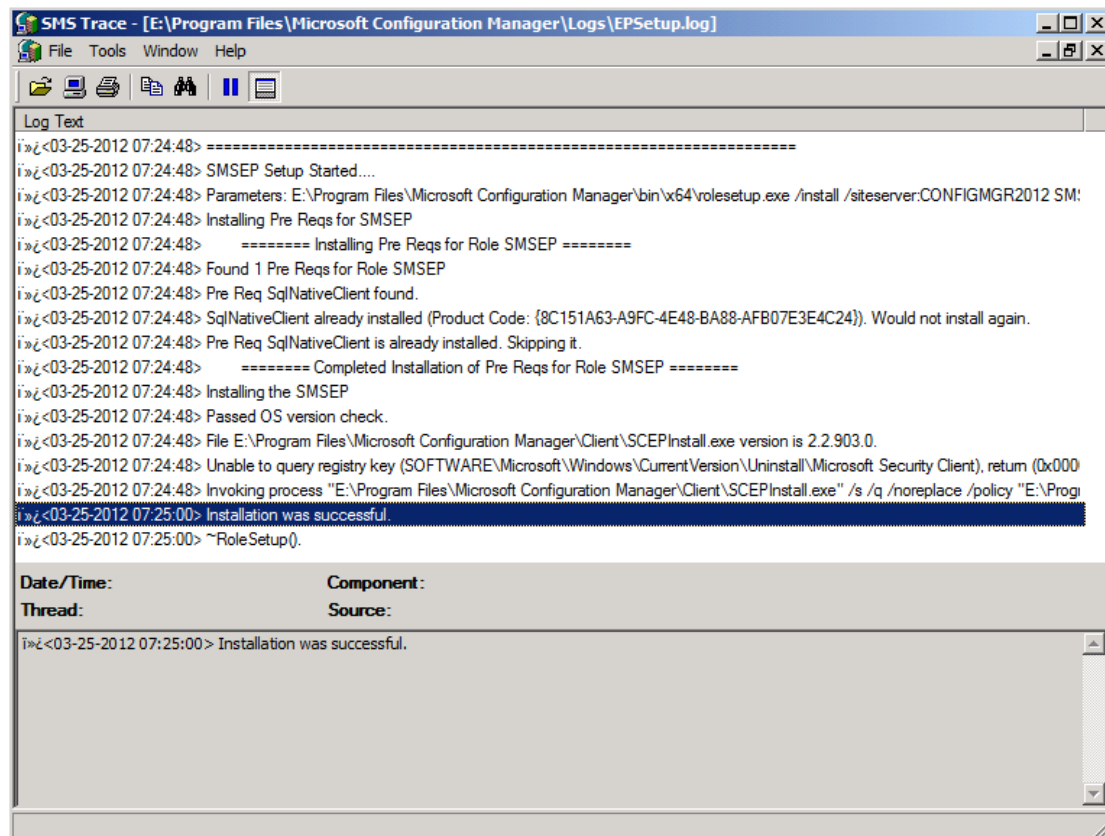


10) Click **Close** . You may need to refresh the list of **Site System Roles** on the site system to view the **Endpoint Protection point** site system role :

System Center 2012 Configuration Manager RTM Endpoint Protection Document

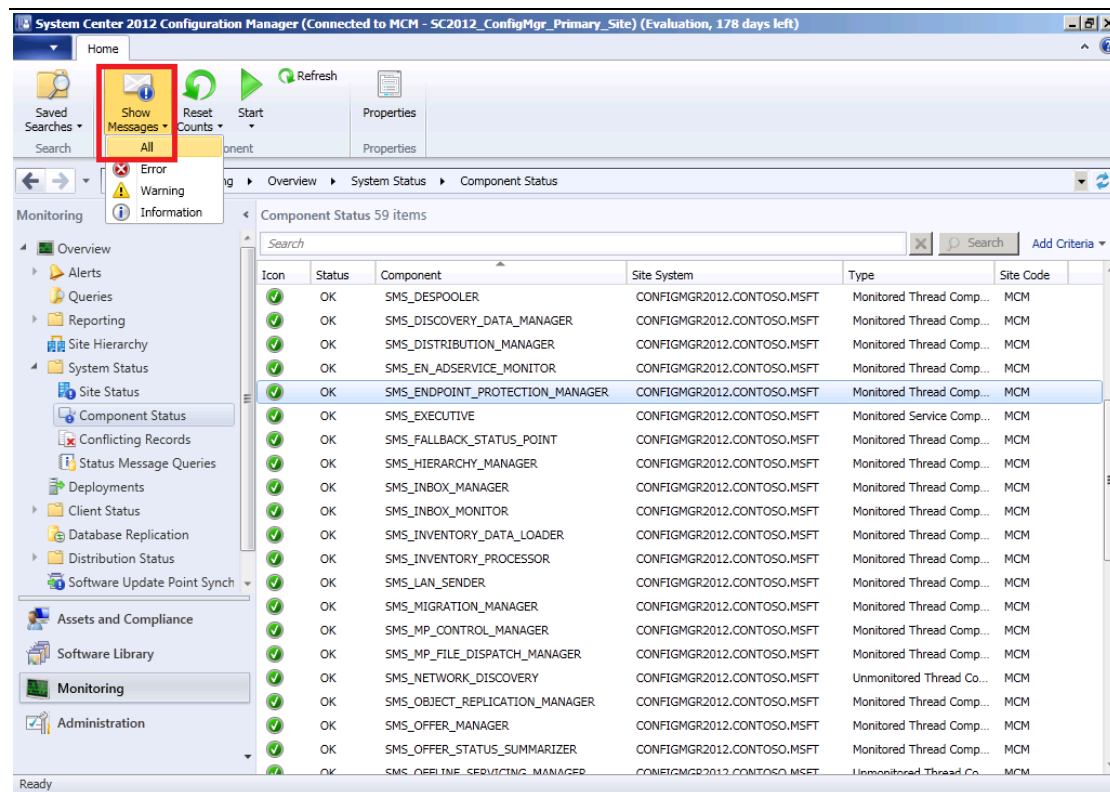


11) Open **EPSetup.log** , you can see the installation was successful :

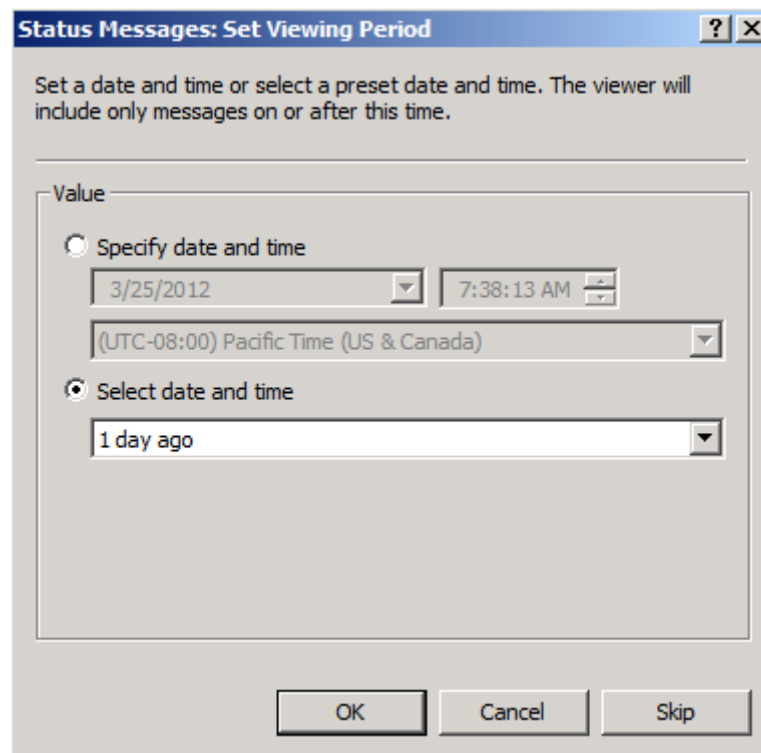


12) Click the **Monitoring** workspace , in the navigation pane , expand **System Status** , and then click **Component Status** , click **SMS_ENDPOINT_PROTECTION_MANAGER** , and the on the **Ribbon** , click **Show Messages** , click **All** :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

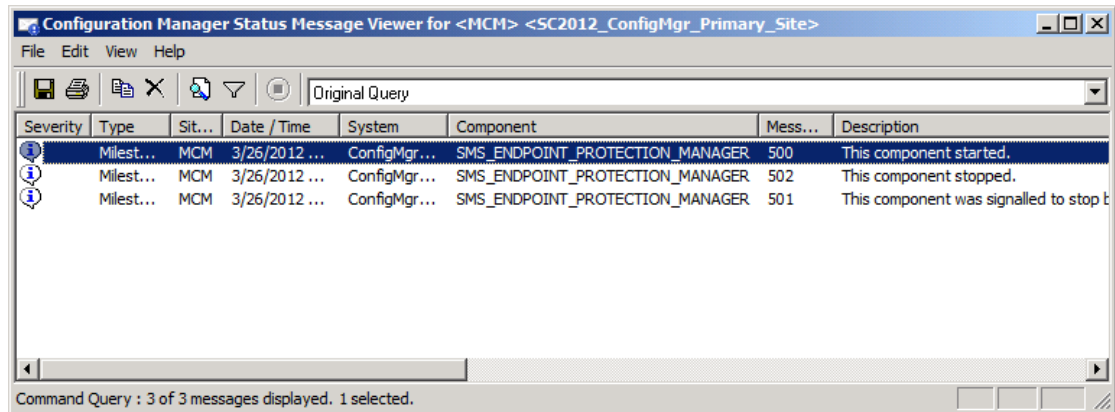


13) The **Status Messages : Set Viewing Period** dialog box appears prompting for the age of status messages to display :

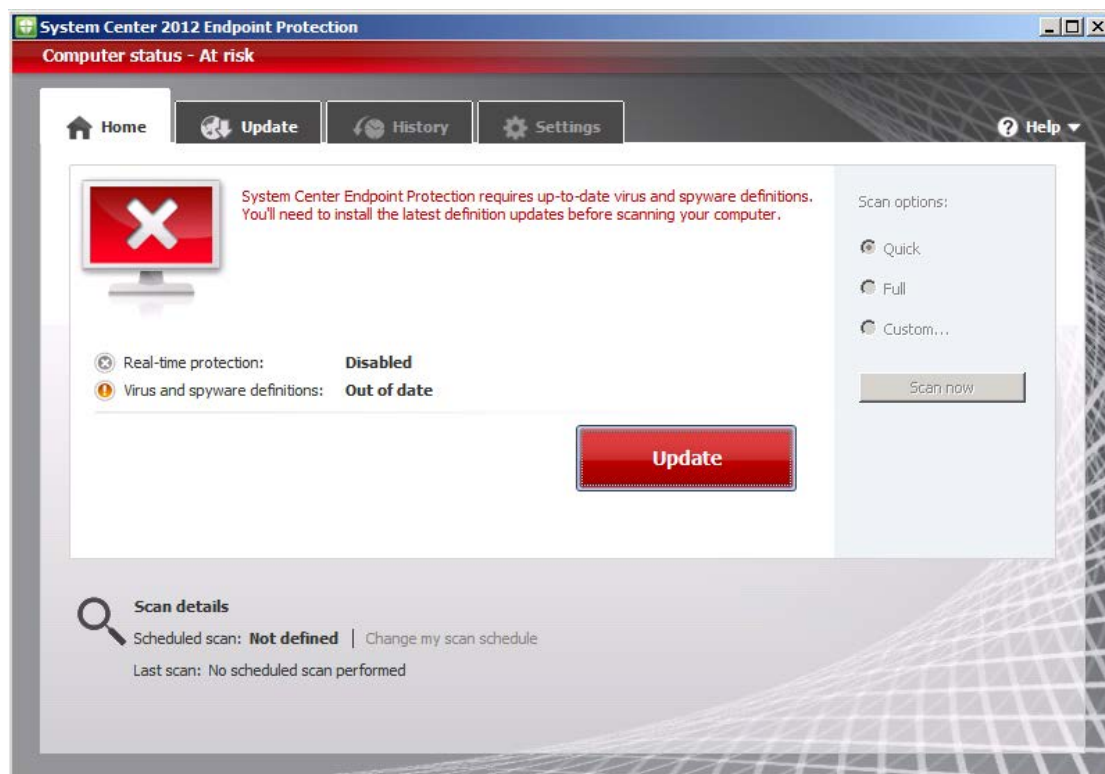


Justin Gao 高扬
yanga@microsoft.com
http://blogs.technet.com/b/justin_gao

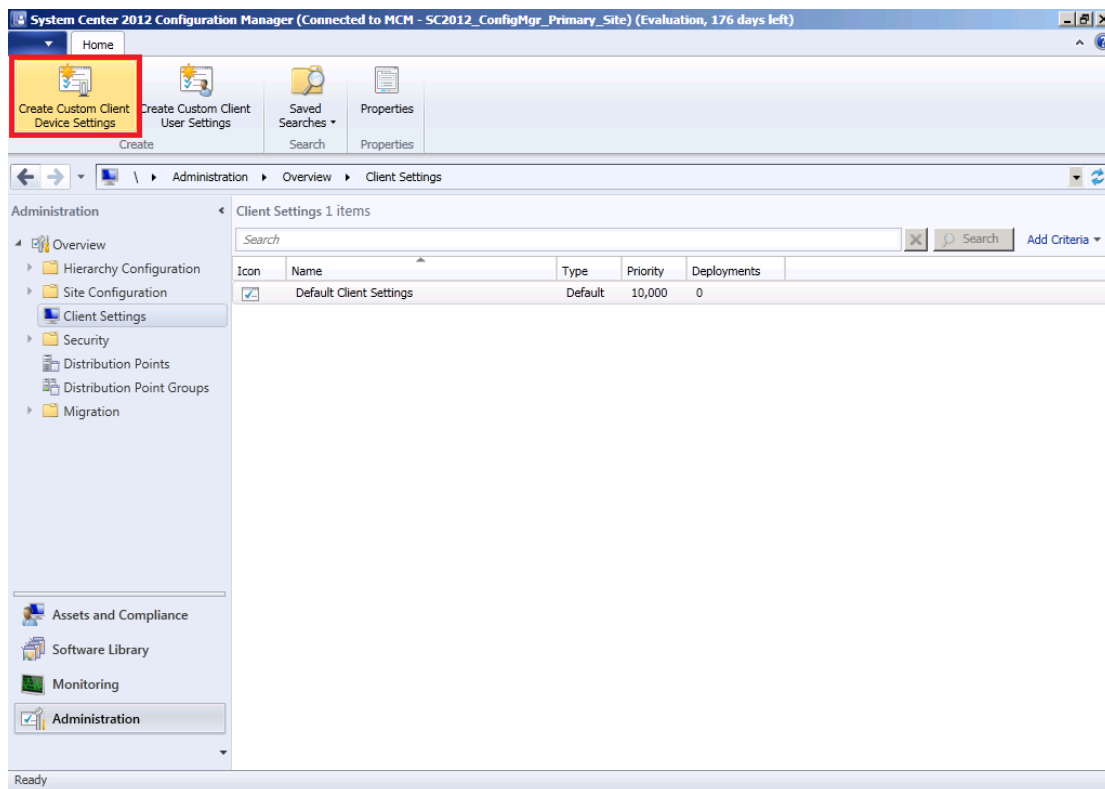
14) Click **OK** to view messages for the past 24 hours . Notice a message with an ID of **500** , this message indicates that the component was started . This is an indication that the Endpoint Protection point has been installed successfully :



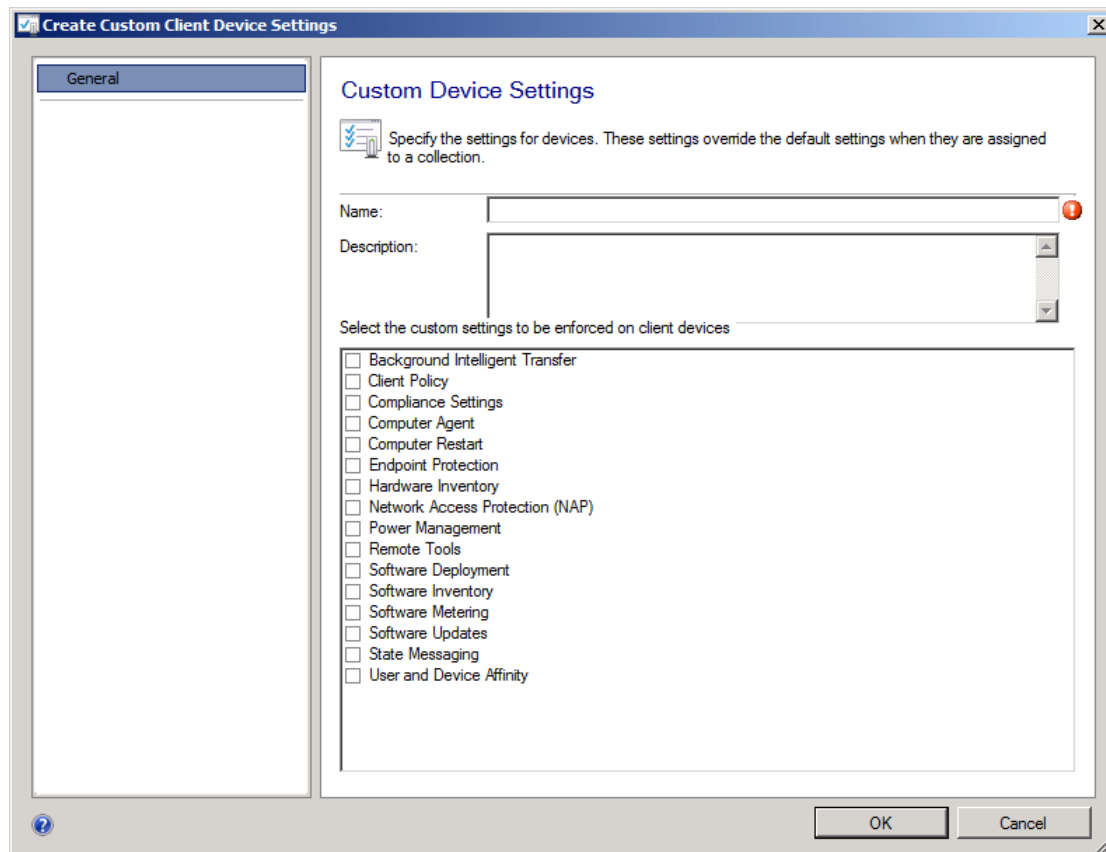
15) On the **Start** menu , click **System Center 2012 Endpoint Protection** , the **System Center 2012 Endpoint Protection** window appears , the status is **Computer status – At risk** :



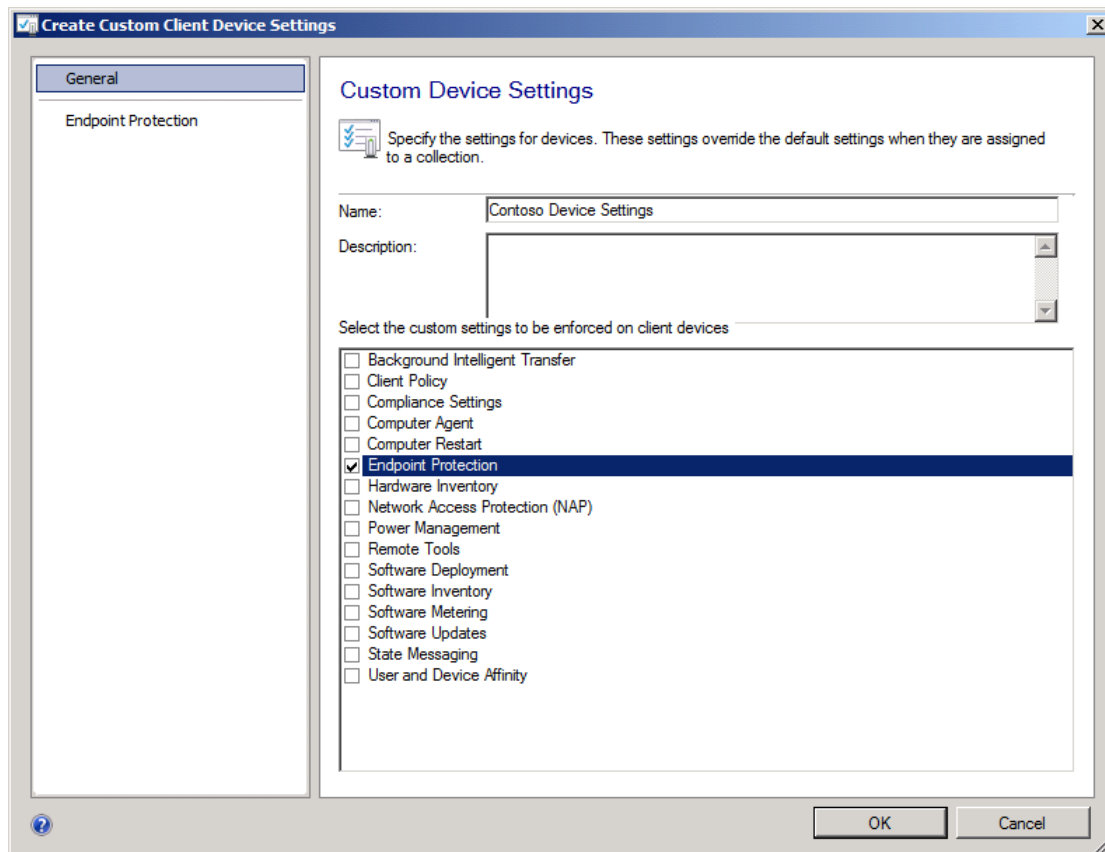
16) Close the **System Center 2012 Endpoint Protection** window . In the following procedure ,you will enable the Endpoint Protection client , which will allow scanning for malware and viruses on client computers. Click the **Administration** workspace , click **Client Settings** node , click **Create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



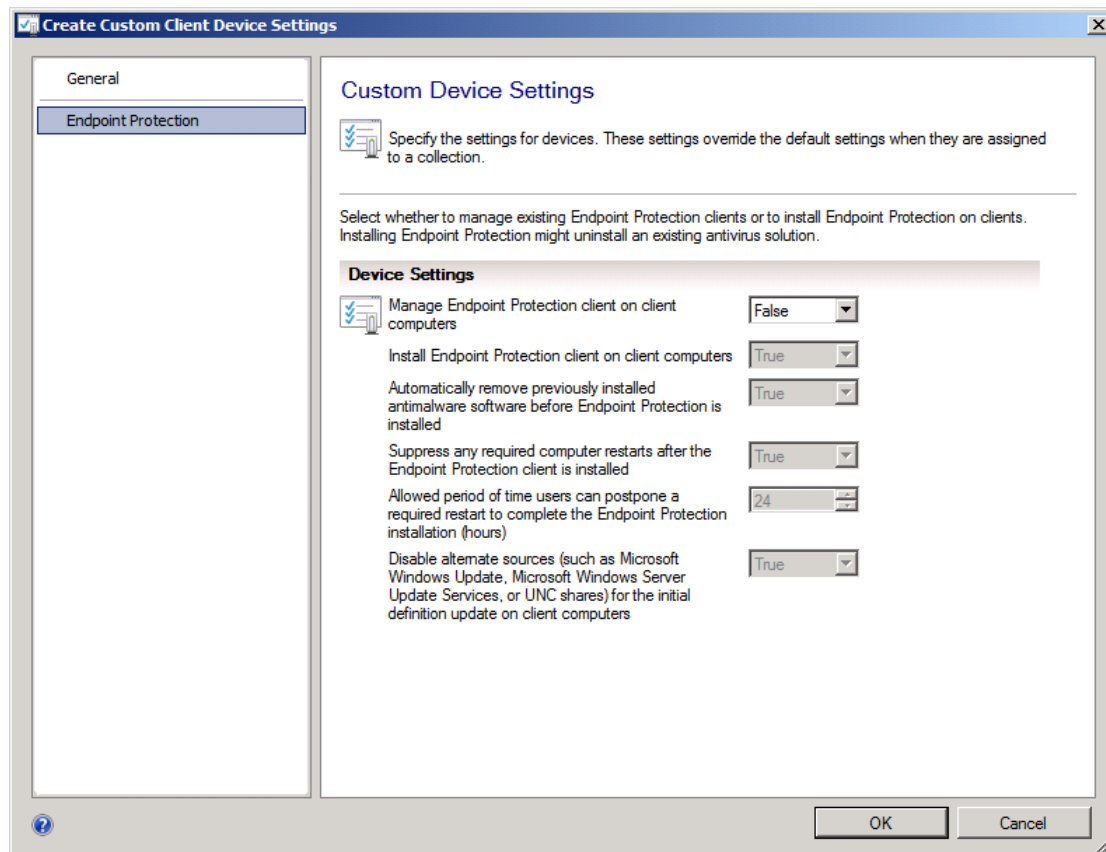
17) The **Create Custom Client Device Settings** window displayed :



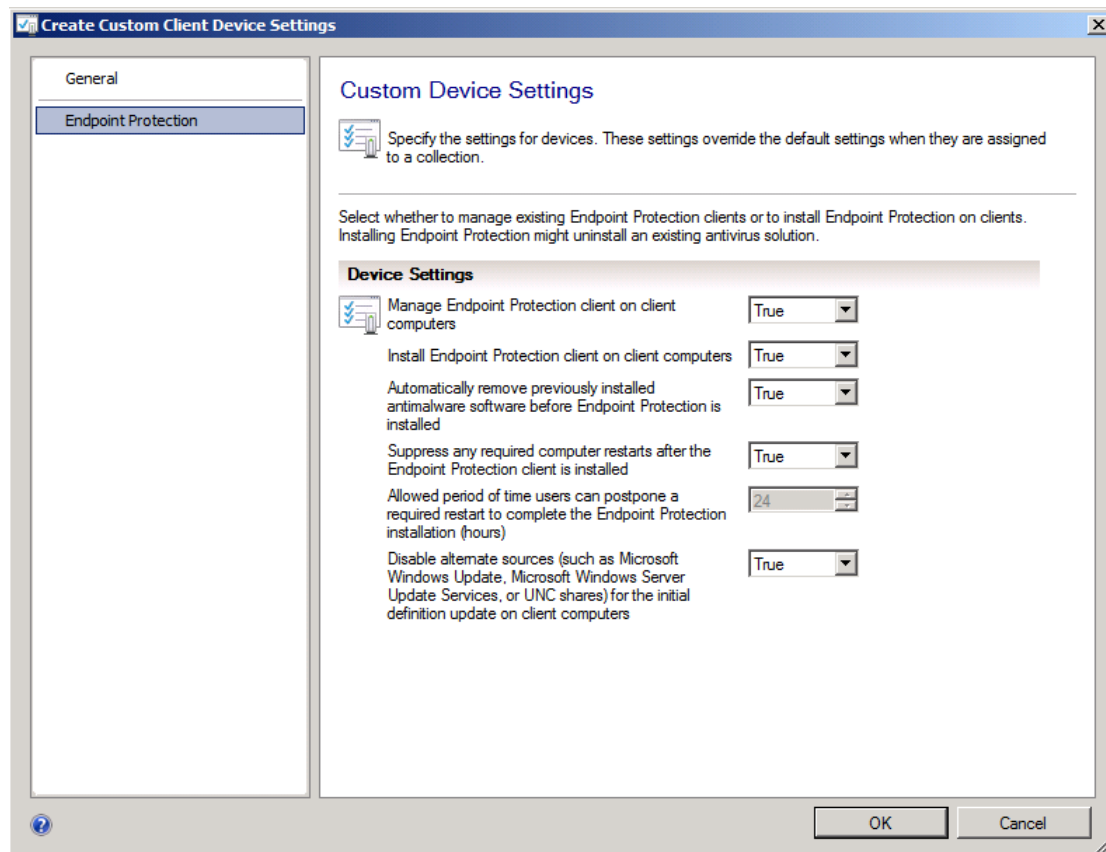
18) Enter a name in the **Name** box , and then select **Endpoint Protection** in **Select the custom settings to be enforced on client devices** box :



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

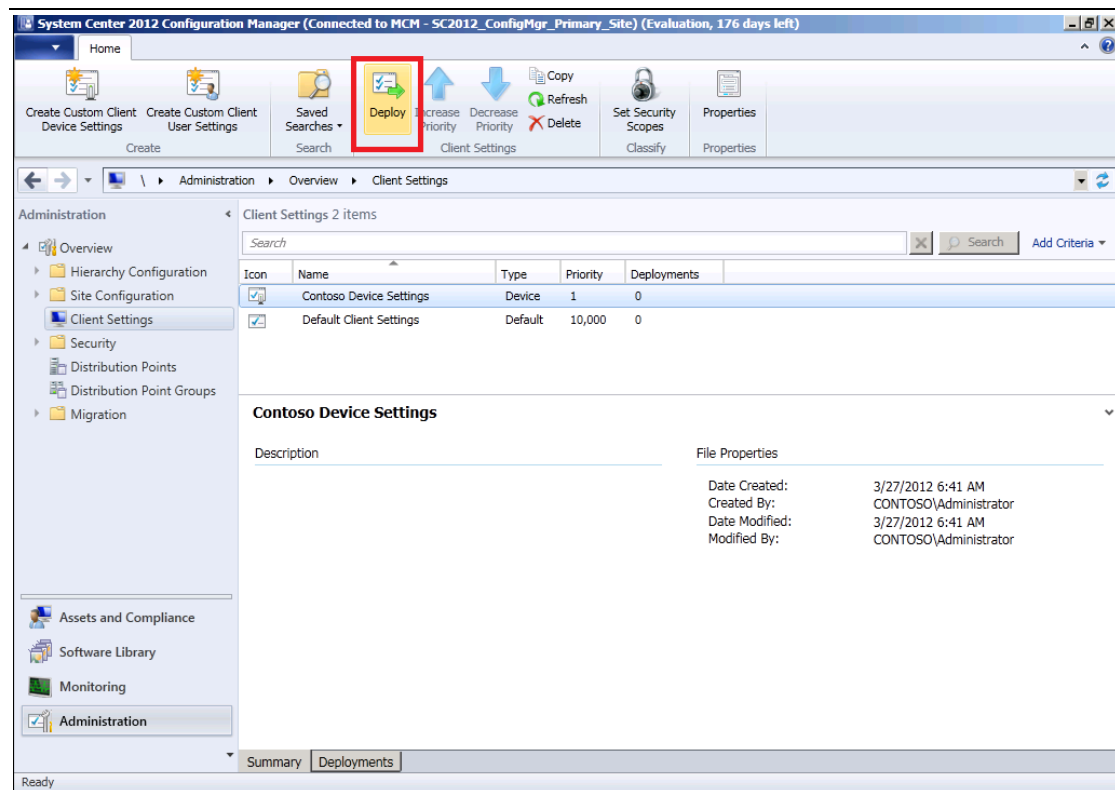


20) In the **Manage Endpoint Protection client on client computers** box , click **True** . The others settings , you can keep default :

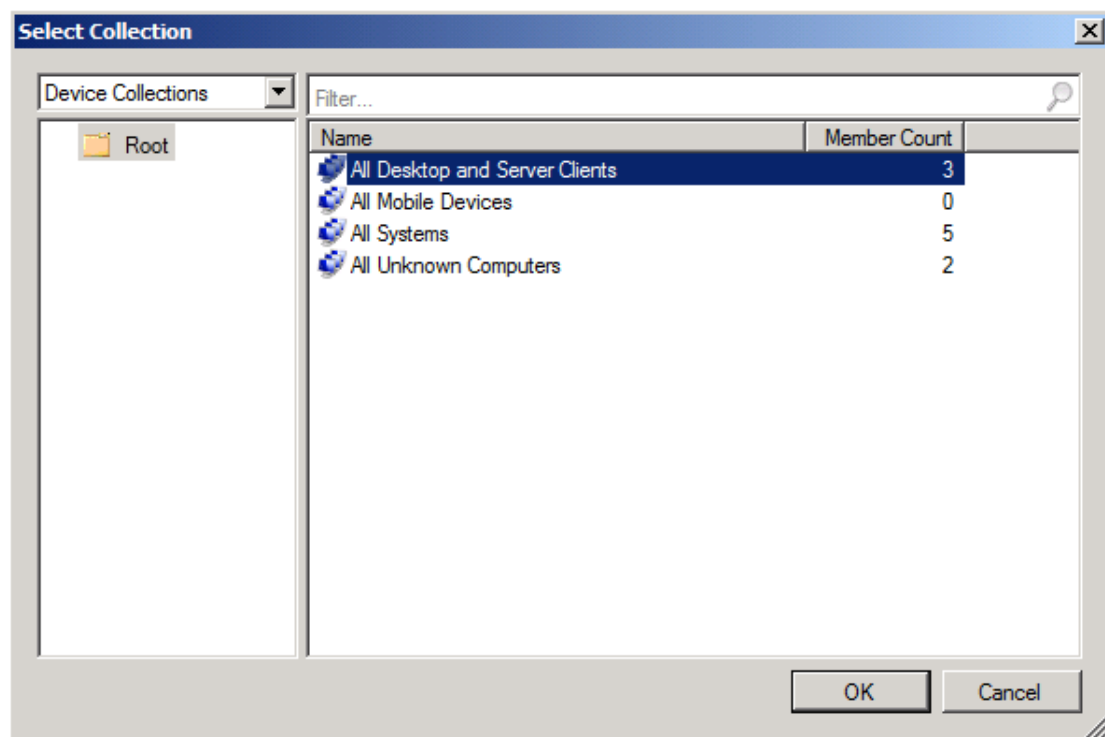


21) Click **OK** , will back to **Client Settings** node , click just created Device Settings , click **Deploy** on the Ribbon :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

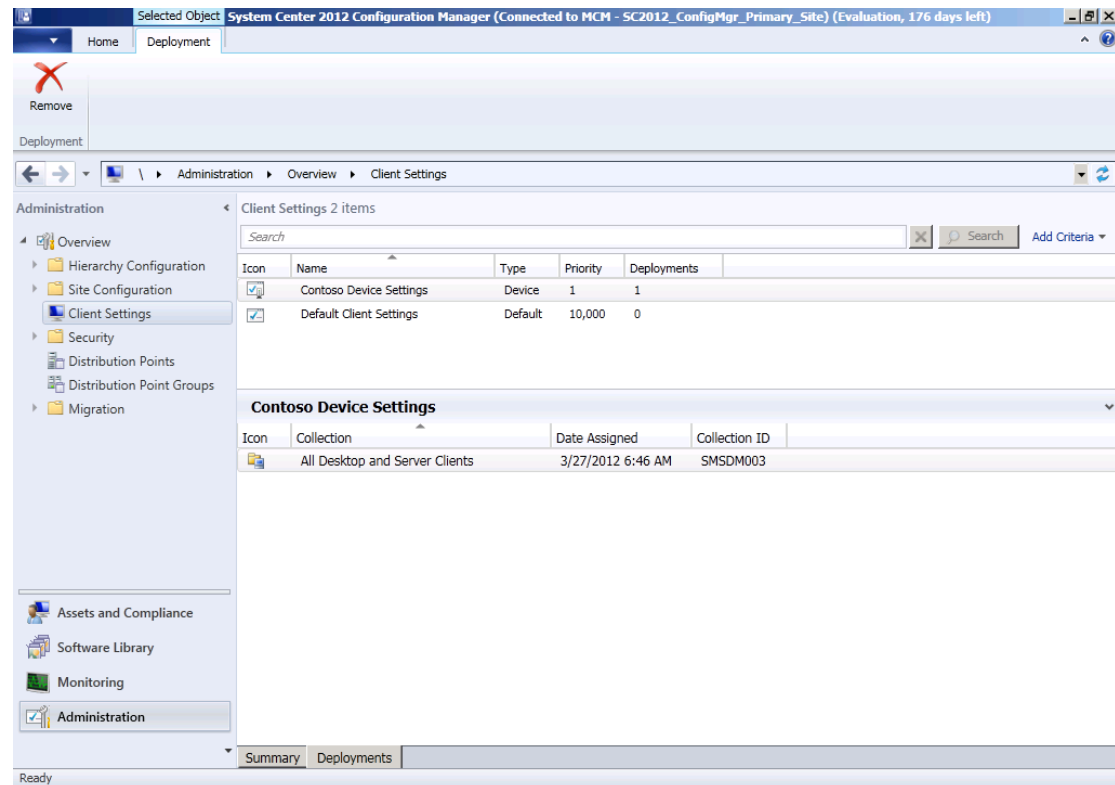


22) The **Select Collection** dialog box appears :

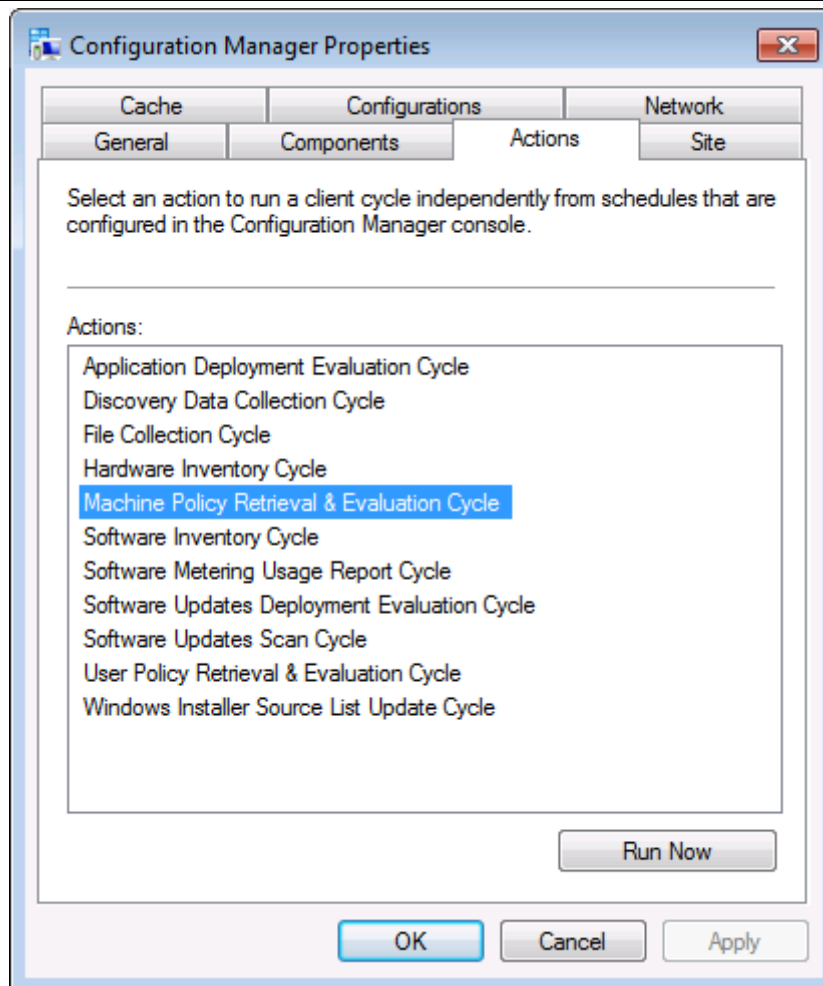


23) Click **All Desktop and Server Clients** , click **OK** , you can see this client

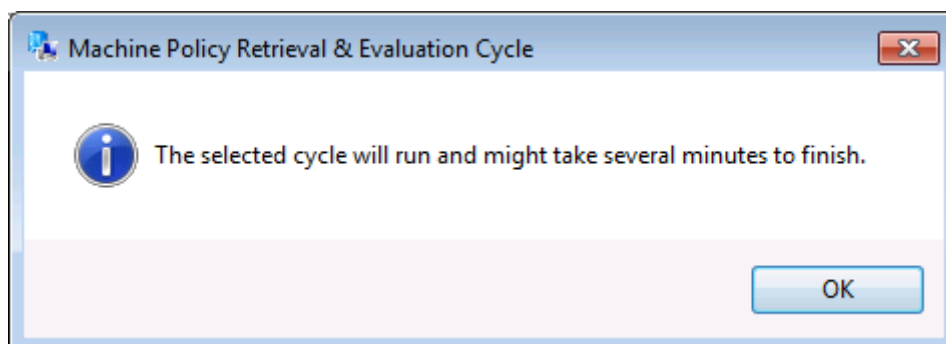
settings will be deployed :



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** :

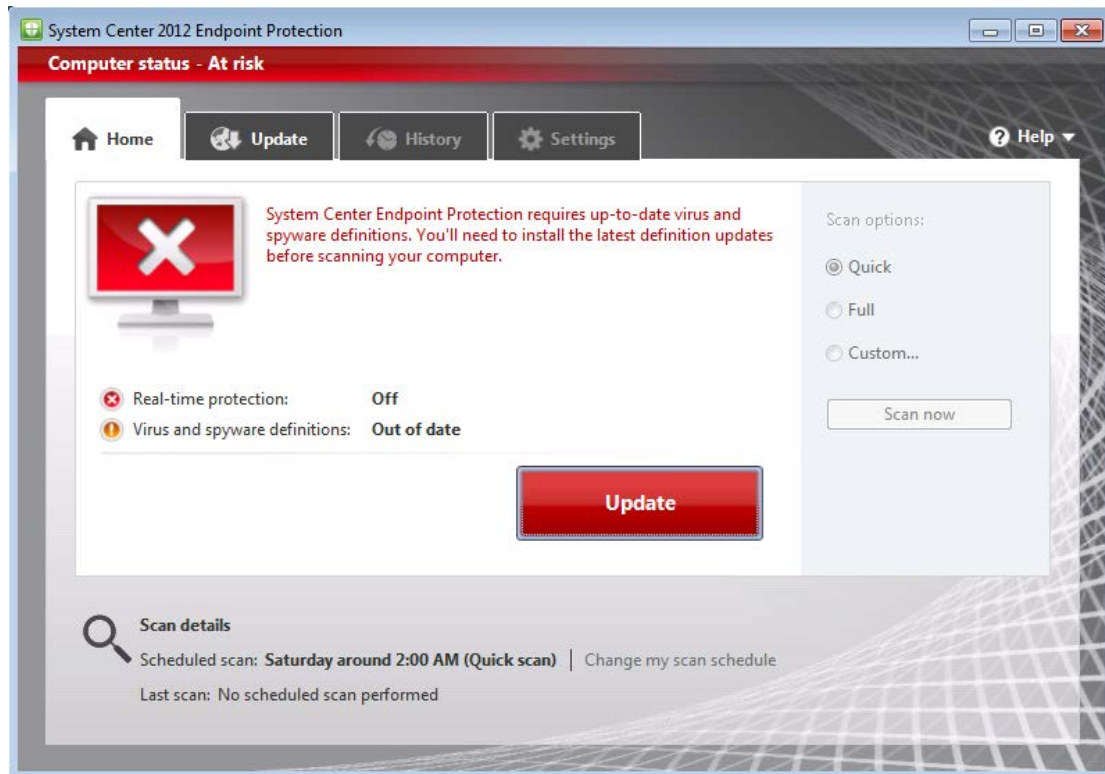


25) A **Machine Policy Retrieval & Evaluation Cycle** message box appears indicating the action was initiated :



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 :

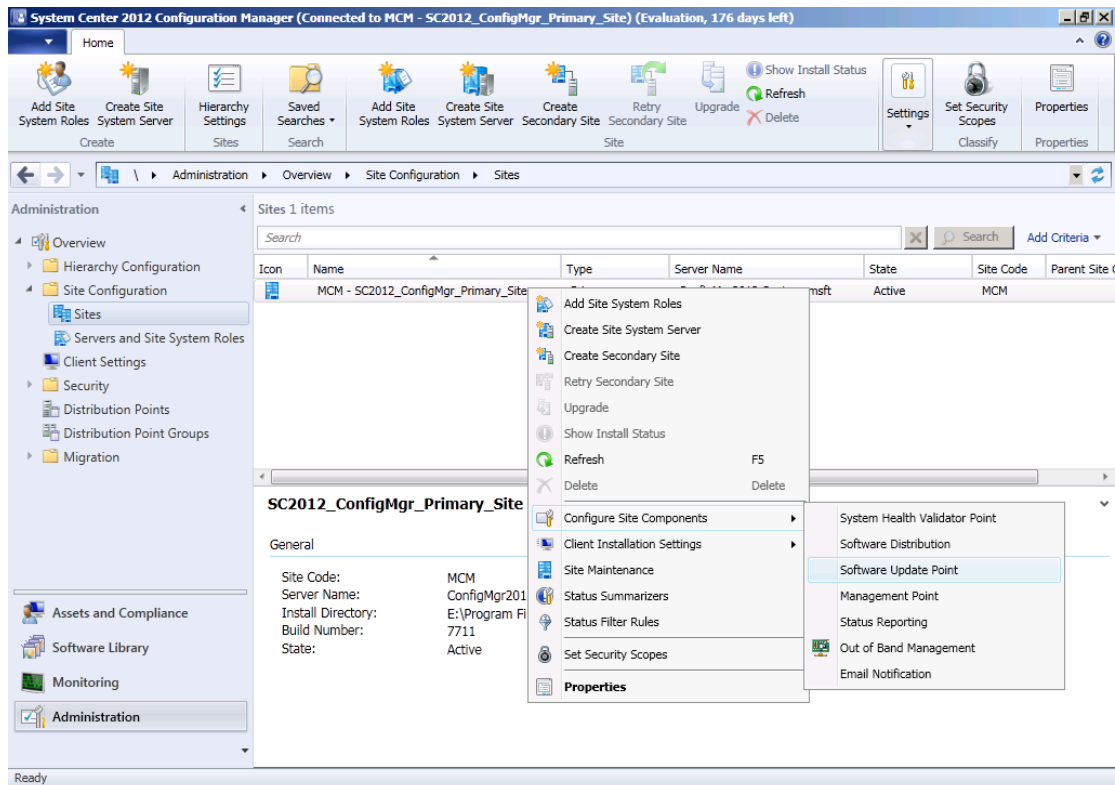


27) Close the **System Center 2012 Endpoint Protection** window.

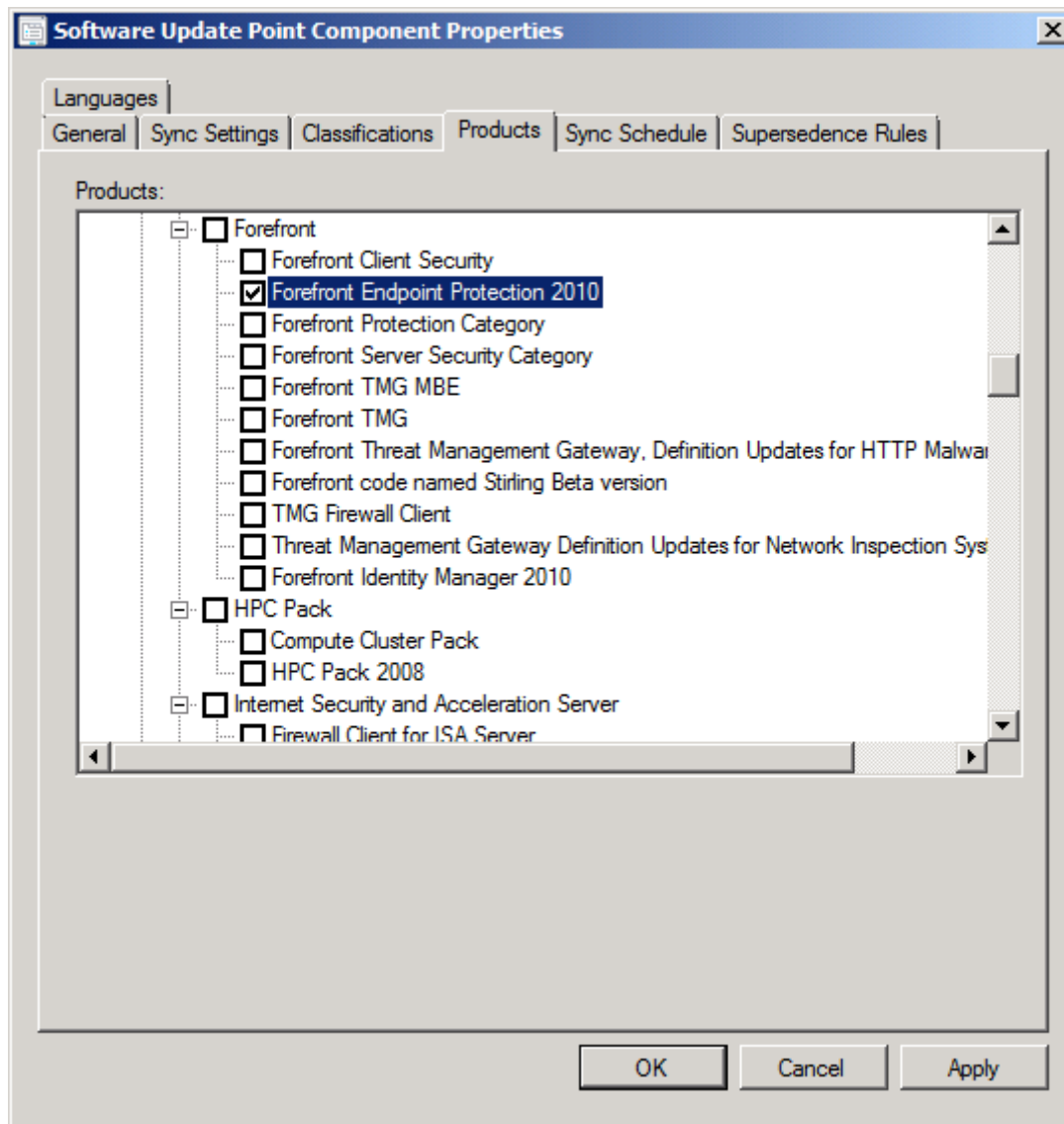
5. Synchronize Endpoint Protection Updates :

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

Software Update Point :

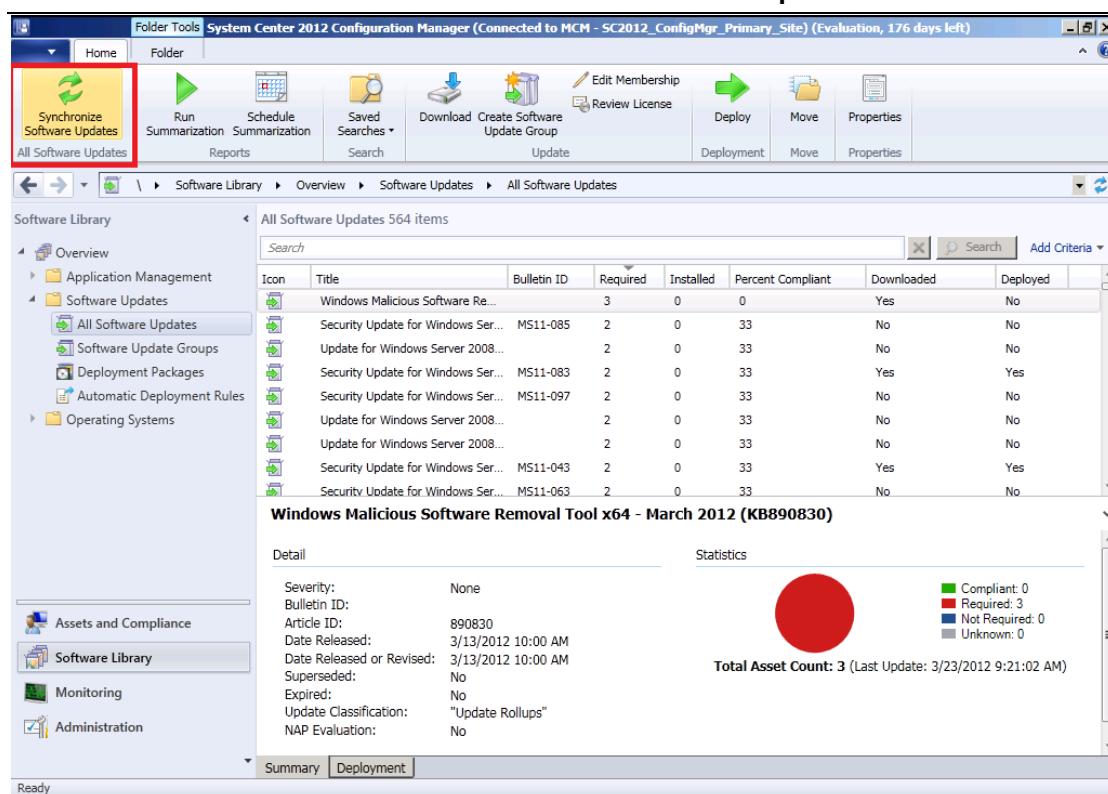


2) The **Software Update Point Component Properties** dialog box appears , click **Products** tab and select **Forefront Endpoint Protection 2010** :

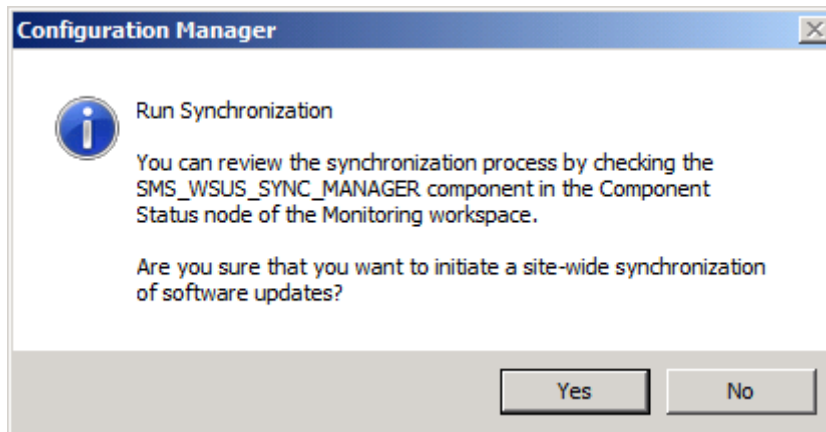


3) Click **OK** , click **Software Library** workspace , expand **Software Updates** , click **All Software Updates** , and then click **Synchronize Software Updates** in the Ribbon :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

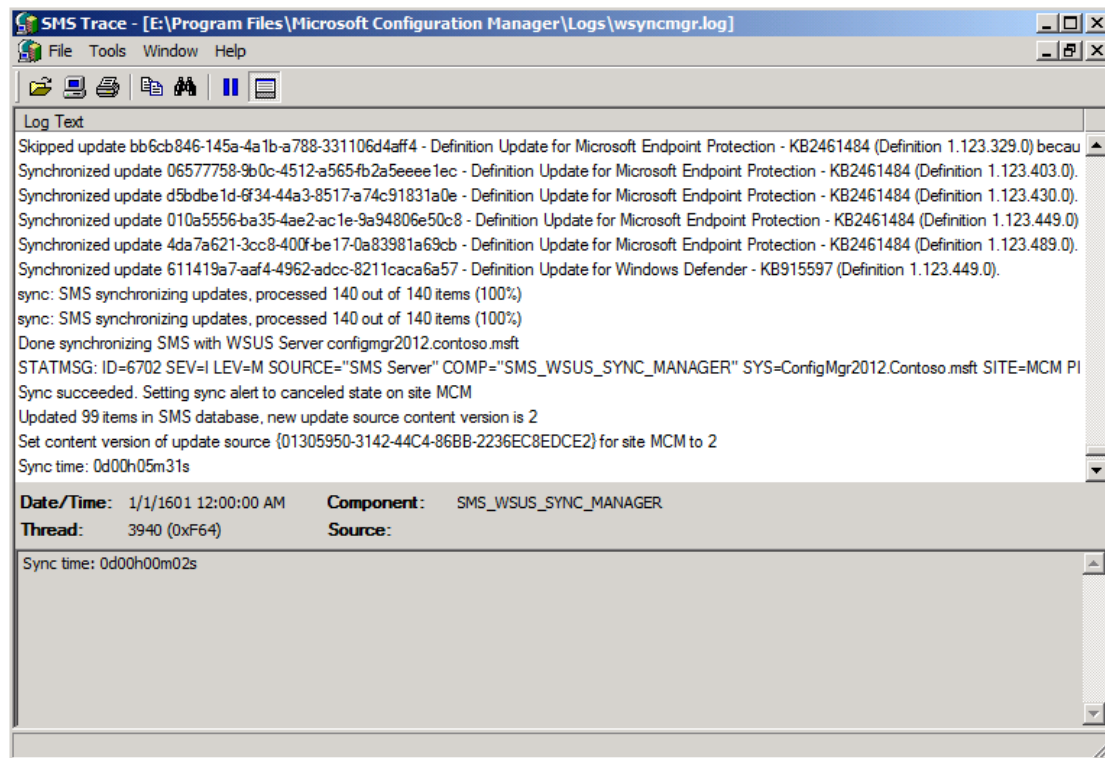


4) A Configuration Manager dialog box appears :



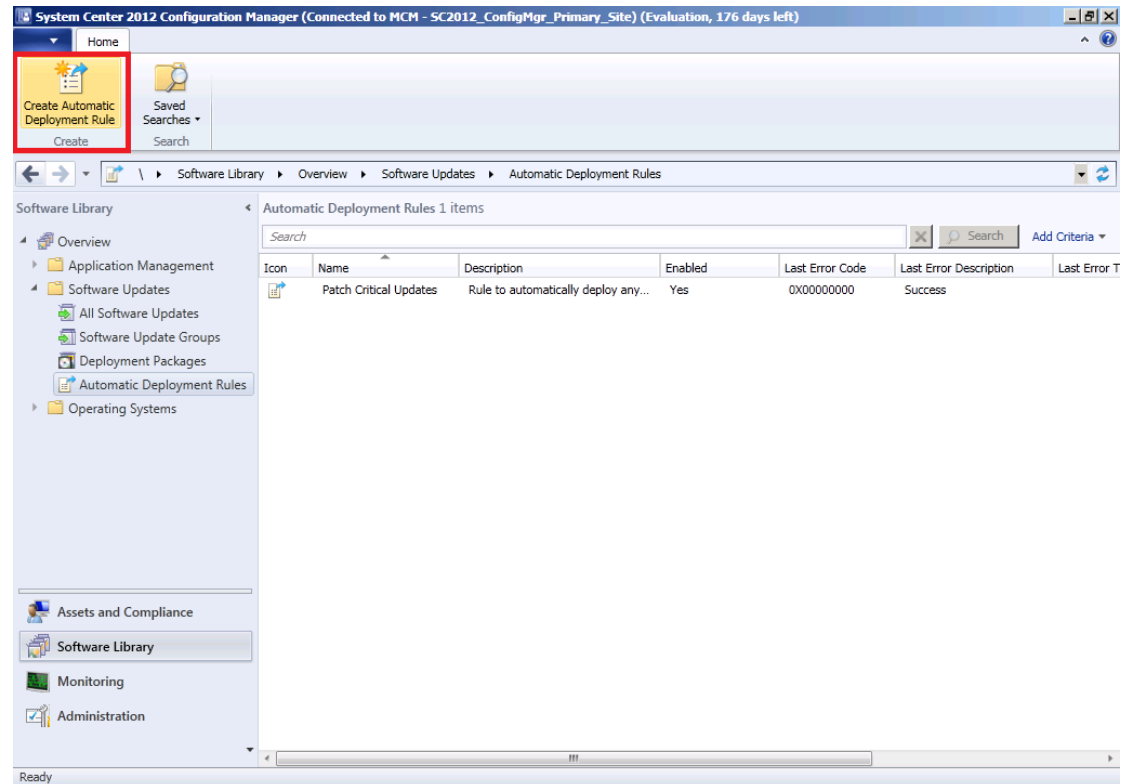
5) Click **Yes** , the synchronization will started , you can check the **wsyncmgr.log** :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



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 :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

The screenshot shows the 'Create Automatic Deployment Rule Wizard' dialog box, specifically the 'General' tab. The left sidebar lists various configuration options: General, Deployment Settings, Software Updates, Evaluation Schedule, Deployment Schedule, User Experience, Alerts, Download Settings, Deployment Package, Download Location, Language Selection, Summary, Progress, and Completion. The main area is titled 'Specify the settings for this automatic deployment rule'. It contains several input fields and options: 'Name' is set to 'Endpoint Protection Updates', 'Description' is 'System Center 2012 Endpoint Protection Updates', and there is a 'Select Deployment Template...' button. Below this, it says 'Specify the target collection for the software update deployment.' with a 'Collection' dropdown set to 'All Desktop and Server Clients' and a 'Browse...' button. A note explains that automatic deployment rules define criteria for software updates. Two radio buttons are present: 'Add to an existing Software Update Group' (unselected) and 'Create a new Software Update Group' (selected). Another note asks whether to enable deployment after the rule runs, with the 'Enable the deployment after this rule is run' checkbox checked. At the bottom, there are buttons for '< Previous', 'Next >', 'Summary', and 'Cancel'.

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

Deployment Settings

General

Deployment Settings

Software Updates

Evaluation Schedule

Deployment Schedule

User Experience

Alerts

Download Settings

Deployment Package

Download Location

Language Selection

Summary

Progress

Completion

Specify the settings for this Automatic Deployment Rule

☐ Use Wake-on-LAN to wake up clients for required deployments

State message detail level

You can specify the state message detail level returned by clients for this software update deployment. A detail level of Normal returns all state messages that are related to the deployment. A detail level of Minimal returns only the enforcement success, and critical error messages.

Detail level: Minimal

Some software updates include a license agreement. Software updates that you choose to deploy automatically will not display any license agreement to you, regardless of whether those software updates include a license agreement. You can review the Microsoft Software License Terms in the All Updates list in the Software Updates node of the console.

☐ Automatically deploy only software updates found by this rule that do not include a license agreement, or for which the license agreement has already been approved.

☒ Automatically deploy all software updates found by this rule, and approve any license agreements

< Previous Next > Summary Cancel

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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

The screenshot shows the 'Create Automatic Deployment Rule Wizard' dialog box, specifically the 'Software Updates' step. The left-hand navigation pane lists several steps: General, Deployment Settings, **Software Updates** (which is currently selected and highlighted in blue), Evaluation Schedule, Deployment Schedule, User Experience, Alerts, Download Settings, Deployment Package, Download Location, Language Selection, Summary, Progress, and Completion. The main area of the dialog is titled 'Select the property filters and search criteria'. Below this title, it states: 'The software updates that meet the specified criteria are added to the associated software update group.' There are two sections: 'Property filters:' and 'Search criteria:'. The 'Property filters' section contains a list of checkboxes: Article ID, Bulletin ID, Custom Severity, Date Released or Revised, Description, Language, **Product** (which is checked), Required, and Severity. The 'Search criteria' section contains a text box with the text 'Product: "Forefront Endpoint Protection 2010"'. At the bottom of the dialog, there are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'. The 'Next >' button is highlighted.

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

The screenshot shows the 'Create Automatic Deployment Rule Wizard' dialog box, specifically the 'Evaluation Schedule' step. The left-hand navigation pane lists various steps: General, Deployment Settings, Software Updates, Evaluation Schedule (which is currently selected and highlighted), Deployment Schedule, User Experience, Alerts, Download Settings, Deployment Package, Download Location, Language Selection, Summary, Progress, and Completion. The main content area is titled 'Specify the recurring schedule for this rule'. It contains a text box with the instruction: 'Specify a schedule to run this rule. You can manually run this rule regardless of any configured scheduled.' Below this is a checkbox labeled 'Enable rule to run on a schedule', which is checked. To the right of the checkbox is a 'Customize...' button. Below the checkbox is a text box containing the schedule: 'Occurs every 30 days effective 3/27/2012 7:58 AM'. Below this text box is a horizontal line. Below the line is a paragraph of text: 'Because automatic deployment rules are dependent on a current software update point synchronization, recurring schedules should not exceed the frequency of your software update point synchronization schedule.' Below this paragraph is another text box containing the schedule: 'Occurs every 7 days effective 2/1/1970 12:00 AM'. At the bottom of the dialog box, there are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'. The 'Next >' button is the one to be clicked according to the instructions.

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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

The screenshot shows the 'Create Automatic Deployment Rule Wizard' window, specifically the 'Deployment Schedule' step. The left sidebar contains a list of steps: General, Deployment Settings, Software Updates, Evaluation Schedule, **Deployment Schedule** (selected), User Experience, Alerts, Download Settings, Deployment Package, Download Location, Language Selection, Summary, Progress, and Completion. The main area is titled 'Configure schedule details for this deployment' and contains three sections: 'Schedule evaluation' with a dropdown set to 'Client local time'; 'Software available time' with radio buttons for 'As soon as possible' (selected) and 'Specific time' (set to 7 Days); and 'Installation deadline' with radio buttons for 'As soon as possible' and 'Specific time' (selected, set to 7 Days, resulting in a deadline of 4/3/2012 7:58:00 AM). At the bottom are buttons for '< Previous', 'Next >', 'Summary', and 'Cancel'.

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

The screenshot shows the 'Create Automatic Deployment Rule Wizard' window, specifically the 'User Experience' step. The left-hand navigation pane lists several steps: General, Deployment Settings, Software Updates, Evaluation Schedule, Deployment Schedule, User Experience (which is currently selected and highlighted in blue), Alerts, Download Settings, Deployment Package, Download Location, Language Selection, Summary, Progress, and Completion. The main area of the wizard is titled 'Specify the user experience for this deployment'. It contains three sections: 'User visual experience' with a dropdown menu for 'User notifications' set to 'Hide in Software Center and all notifications'; 'Deadline behavior' with a text box stating 'When the installation deadline is reached, allow the following activities to be performed outside of any defined maintenance windows:' and two unchecked checkboxes for 'Software Installation' and 'System restart (if necessary)'; and 'Device restart behavior' with a text box stating 'Some software updates require a system restart to complete the installation process. You can suppress this restart on servers and workstations.' and another text box stating 'Suppress the system restart on the following devices:' with two unchecked checkboxes for 'Servers' and 'Workstations'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'. A help icon (?) is located at the bottom left of the main area.

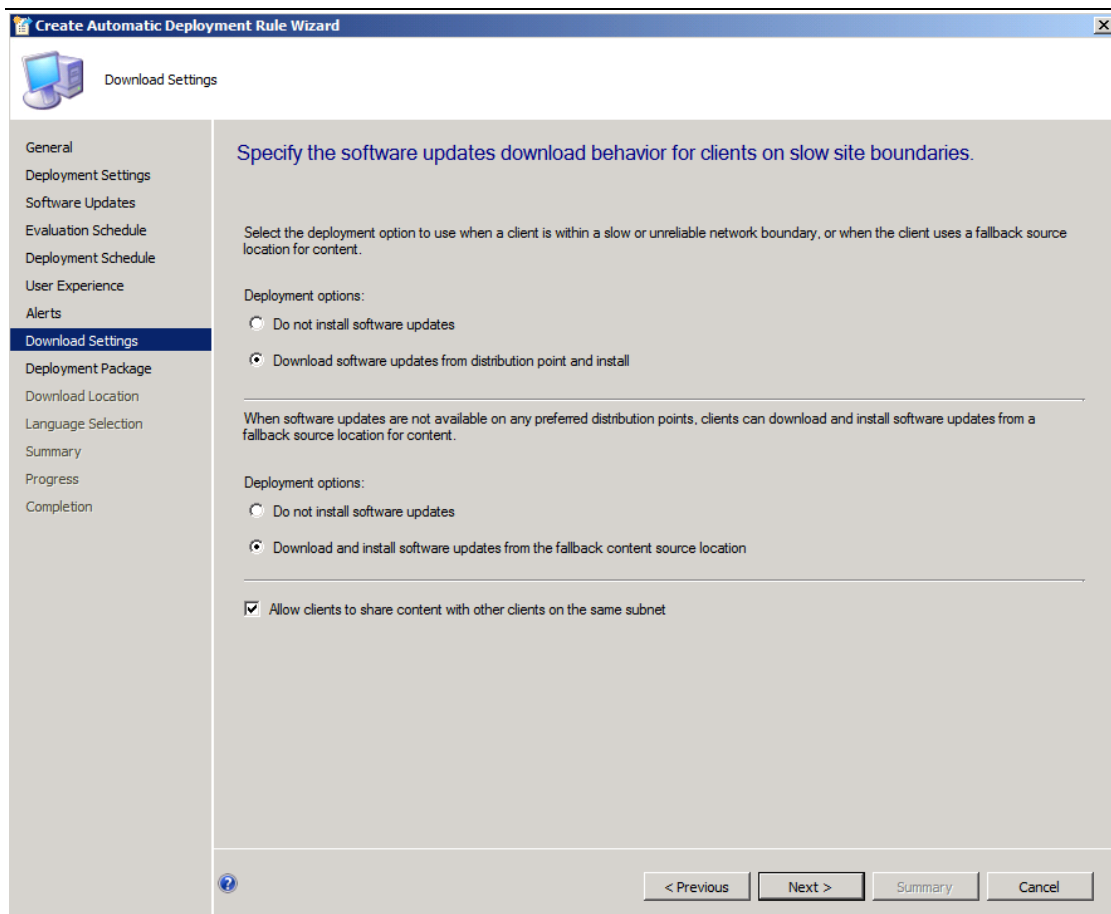
8) Click **Next** , the **Alerts** dialog box appears , you can select **Generate an alert when the following conditions are met** :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

The screenshot shows the 'Create Automatic Deployment Rule Wizard' dialog box, specifically the 'Alerts' tab. The left sidebar contains a list of steps: General, Deployment Settings, Software Updates, Evaluation Schedule, Deployment Schedule, User Experience, Alerts (selected), Download Settings, Deployment Package, Download Location, Language Selection, Summary, Progress, and Completion. The main area is titled 'Specify software update alert options for this deployment'. It contains two sections: 'Configuration Manager alerts' and 'Operations Manager alerts'. In the 'Configuration Manager alerts' section, there is a checkbox 'Generate an alert when the following conditions are met' which is checked. Below it, there are three input fields: 'Client compliance is below the following percent:' with a value of 90, 'Offset from the deadline:' with a value of 7, and 'Alerts are generated after the installation deadline is reached. Deadline time:' with a value of 4/10/2012 7:58:00 AM. The 'Operations Manager alerts' section has a text description and two unchecked checkboxes: 'Disable Operations Manager alerts while software updates run' and 'Generate Operations Manager alert when a software update installation fails'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

Create Automatic Deployment Rule Wizard

Deployment Package

General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Distribution Points
Download Location
Language Selection
Summary
Progress
Completion

Select deployment package for this automatic deployment rule

The deployment package contains the software update files associated with this rule that will be available to clients as part of the deployment. You can select an existing deployment package or create a new one.

☐ Select deployment package:

☐ Create a new deployment package:

Name:
SC2012 Endpoint Protection Updates

Description:
SC2012 Endpoint Protection Updates

Package source (Example): \\<server>\<folder path>
\\configmgr2012\SoftwareUpdates\SC2012EP

Sending priority:
Medium

< Previous Next > Summary Cancel

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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

Create Automatic Deployment Rule Wizard

Distribution Points

General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Distribution Points
Download Location
Language Selection
Summary
Progress
Completion

Specify the distribution points or distribution point groups to host the content

Distribution points or distribution point groups:

Filter...

Name	Description	Associations
\\ConfigMgr2012.Contoso.msft	Distribution point	

Add Remove

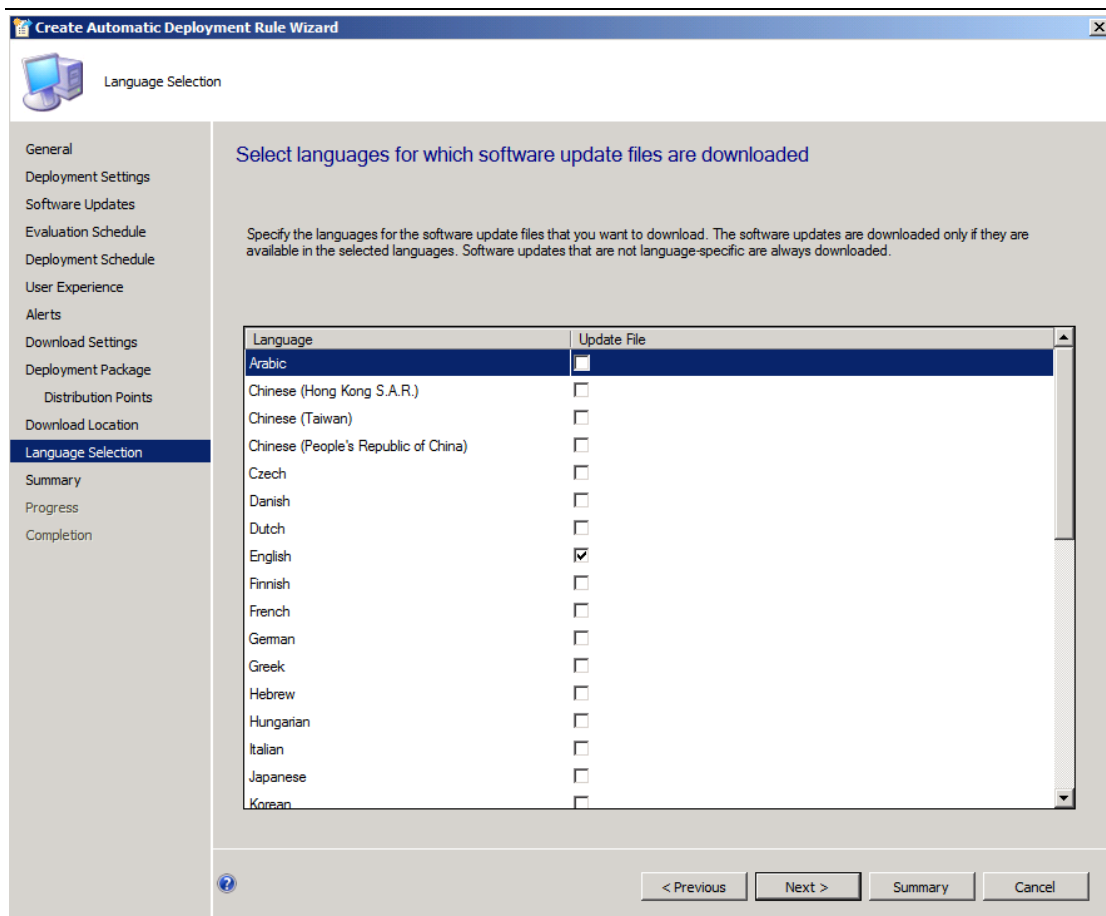
< Previous Next > Summary Cancel

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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

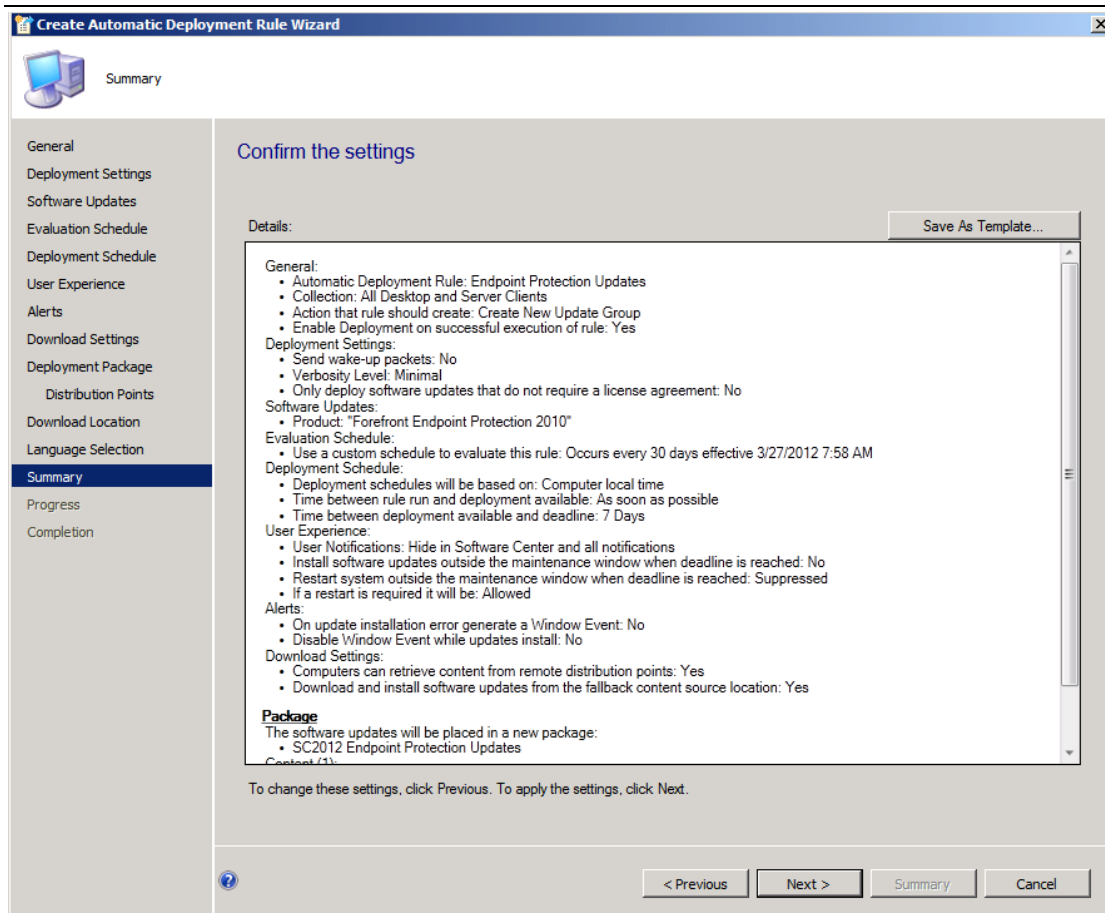
The screenshot shows the 'Create Automatic Deployment Rule Wizard' window. The title bar reads 'Create Automatic Deployment Rule Wizard'. On the left is a navigation pane with the following items: General, Deployment Settings, Software Updates, Evaluation Schedule, Deployment Schedule, User Experience, Alerts, Download Settings, Deployment Package, Distribution Points, **Download Location** (highlighted), Language Selection, Summary, Progress, and Completion. The main area is titled 'Specify download location for this Automatic Deployment Rule'. It contains the following text: 'If your site server does not have an Internet connection, you can download the software updates from a different computer and save them to a network location accessible by the site server.' Below this are two radio buttons: 'Download software updates from the Internet' (which is selected) and 'Download software updates from a location on my network:'. Under the second option is a text box with the example '\\<server>\<folder path>' and a 'Browse...' button. A 'Note:' section follows, stating: 'When the deployment package contains all required software updates, select "Download software updates from the Internet". The software updates files will be validated, but will not be downloaded again.' At the bottom are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

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



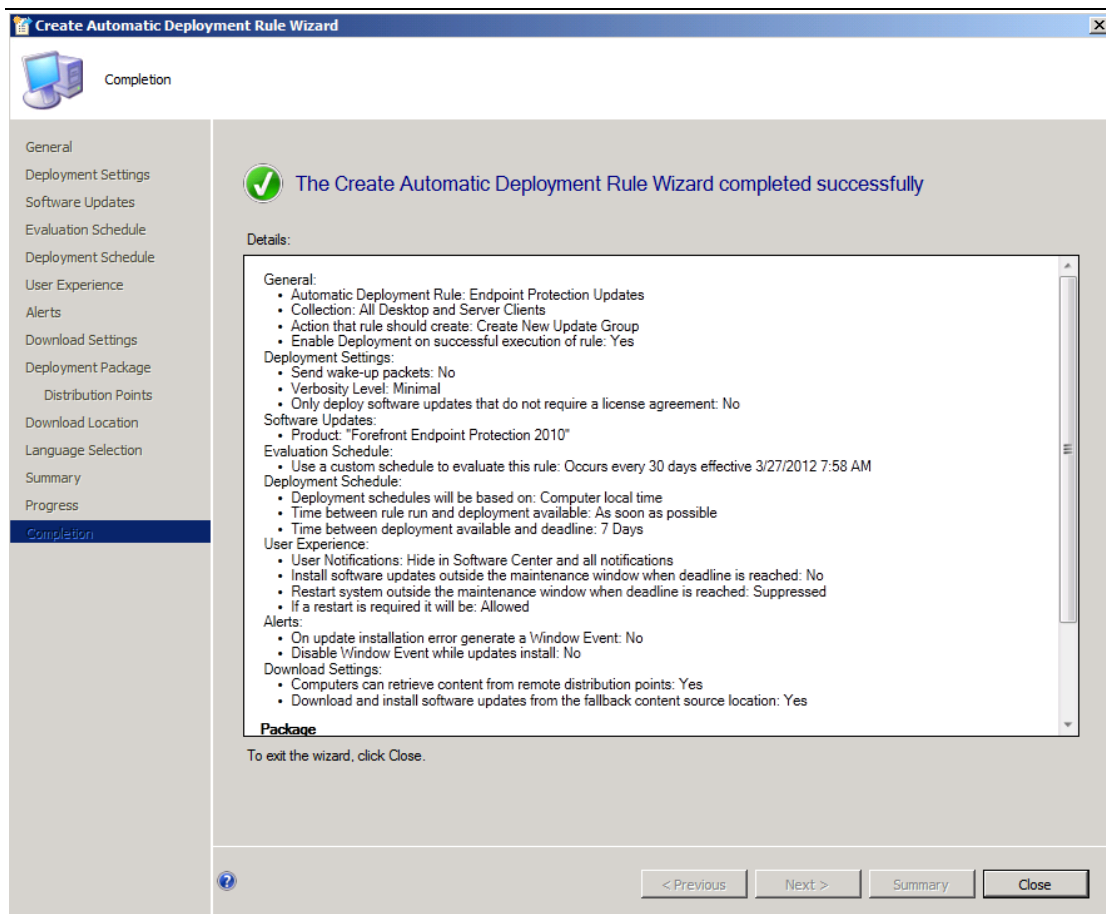
14) Click **Next** , the **Summary** dialog box appears :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



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

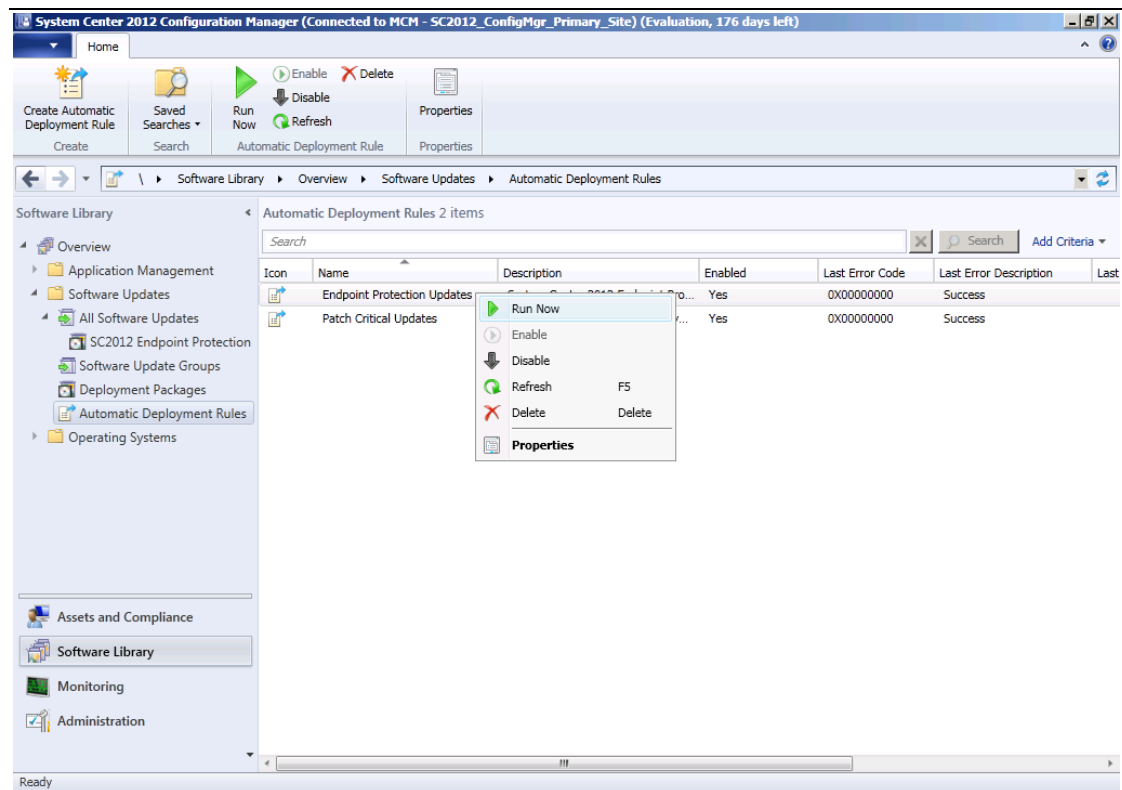
**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



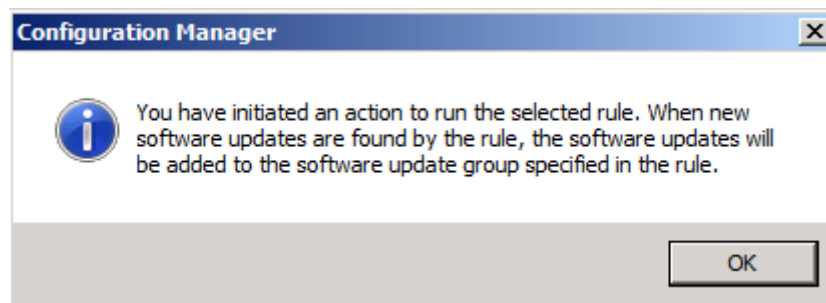
16) Click **Close** , right-click just created automatic deployment rule , click **Run**

Now :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



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



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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

The screenshot shows the System Center 2012 Configuration Manager console. The breadcrumb navigation path is: Software Library > Overview > Software Updates > All Software Updates > SC2012 Endpoint Protection Updates. The left-hand pane shows the 'Software Library' tree with 'SC2012 Endpoint Protection' selected. The main pane displays a table of updates. The 'Downloaded' and 'Deployed' columns for all four updates are highlighted with a red box. Below the table, the details for 'Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.123.489.0)' are shown, including a 'Statistics' section with a pie chart and a 'Total Asset Count: 3 (Last Update: Never)'.

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant	Downloaded	Deployed
	Definition Update for Microsoft End...		0	0	0	Yes	Yes
	Definition Update for Microsoft End...		0	0	0	Yes	Yes
	Definition Update for Microsoft End...		0	0	0	Yes	Yes
	Definition Update for Microsoft End...		0	0	0	Yes	Yes

Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.123.489.0)

Detail

Severity: None
Bulletin ID:
Article ID: 2461484
Date Released: 3/27/2012 6:49 AM
Date Released or Revised: 3/27/2012 6:49 AM
Superseded: No
Expired: No
Update Classification: "Definition Updates"
NAP Evaluation: No

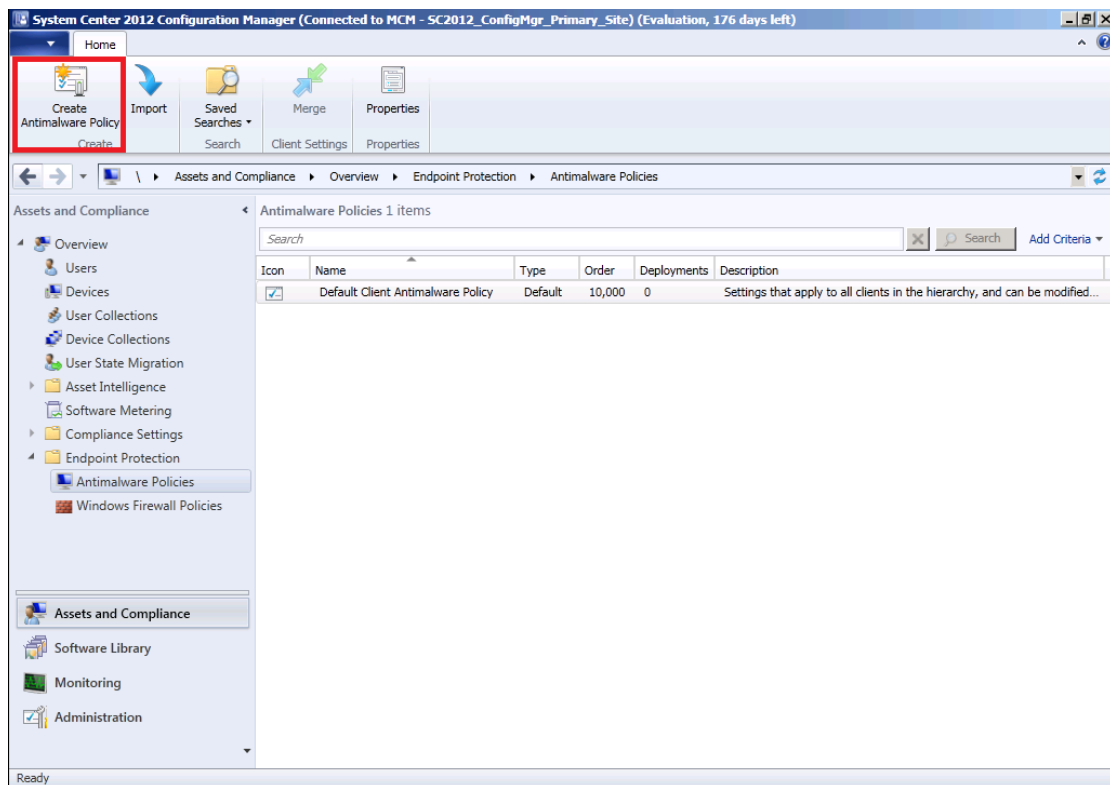
Statistics

Compliant: 0
Required: 0
Not Required: 0
Unknown: 3

Total Asset Count: 3 (Last Update: Never)

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 :

Create Antimalware Policy

General

- Scheduled scans
- Scan settings
- Default actions
- Real-time protection
- Exclusion settings
- Advanced
- Threat overrides
- Microsoft Active Protection Service
- Definition updates

Endpoint Protection Antimalware Policy

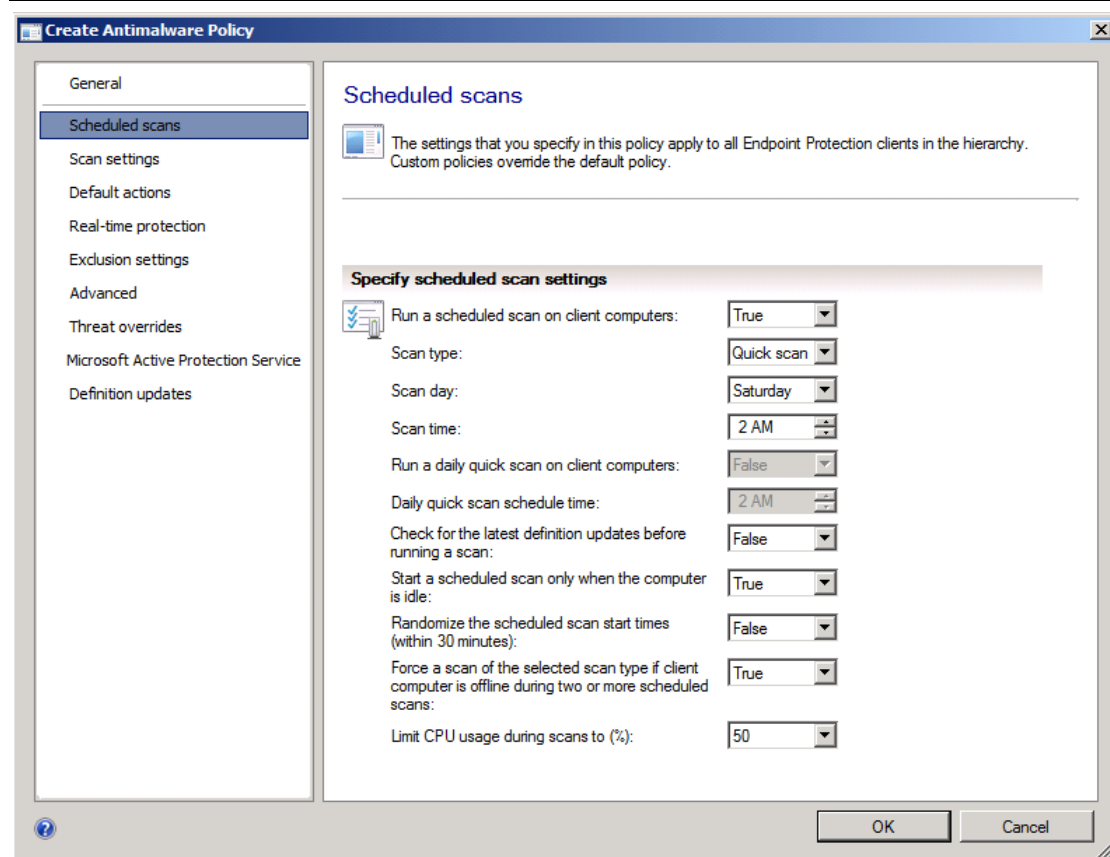
Specify the name and a description for this Endpoint Protection antimalware policy. The settings defined in this policy override the default settings when this policy is assigned to a collection.

Name:

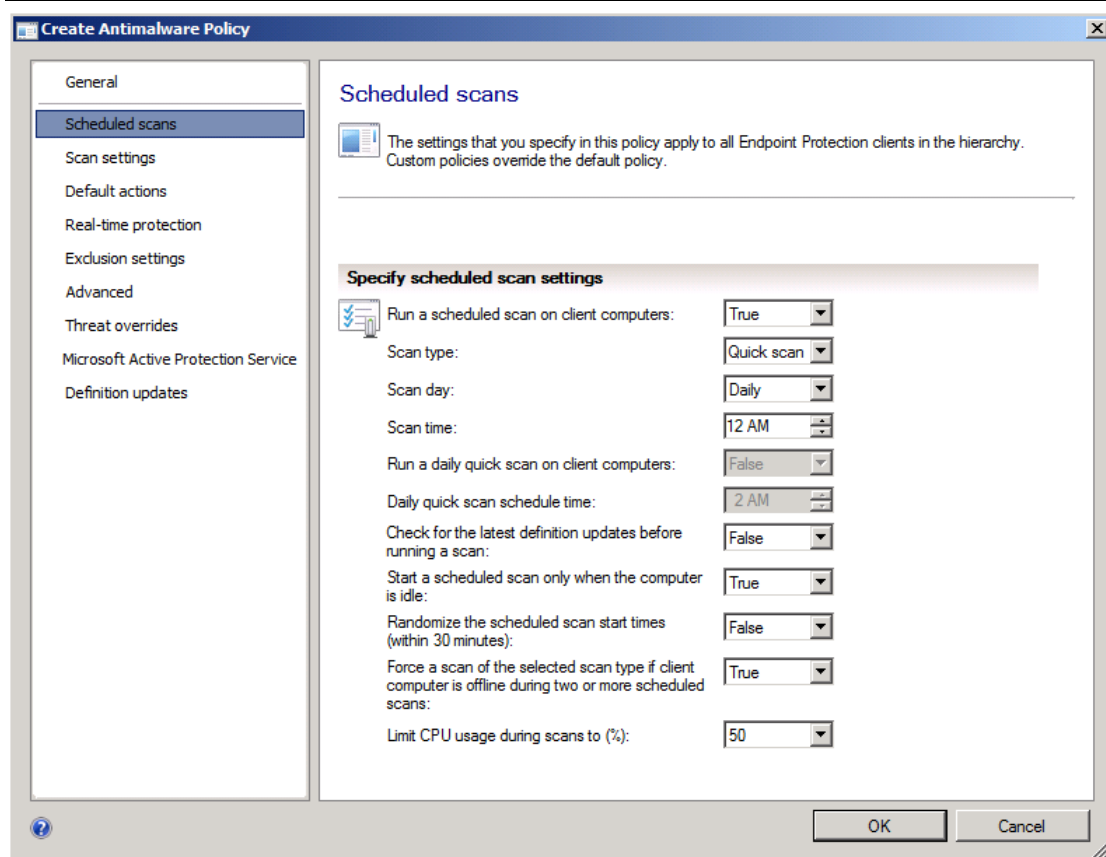
Description:

OK Cancel

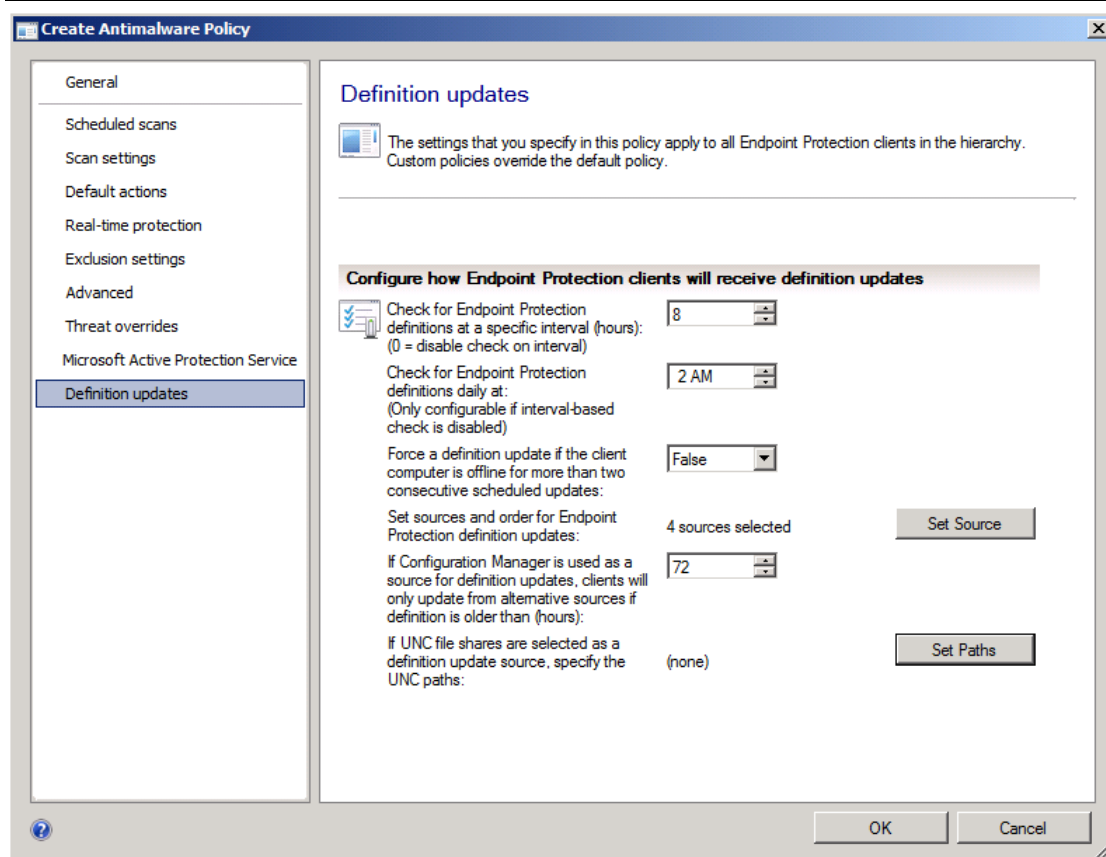
3) In the **Name** box , type name , and then click **Scheduled scans** :



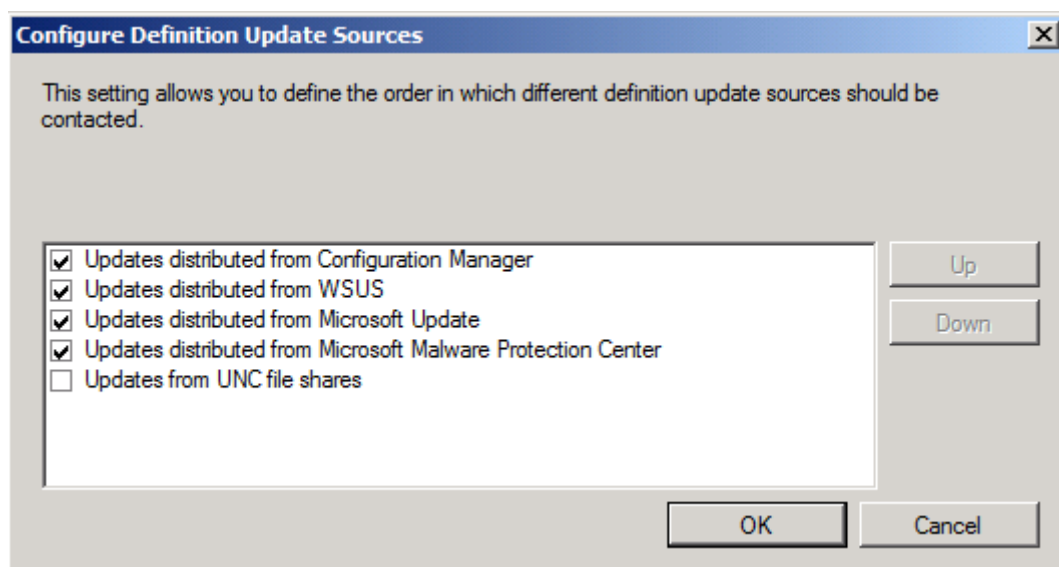
4) In the **Scan day** box ,click **Daily** , in the **Scan time** box , click **12AM** , you are configuring additional settings for visual confirmation of the implementation of the custom policy :



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

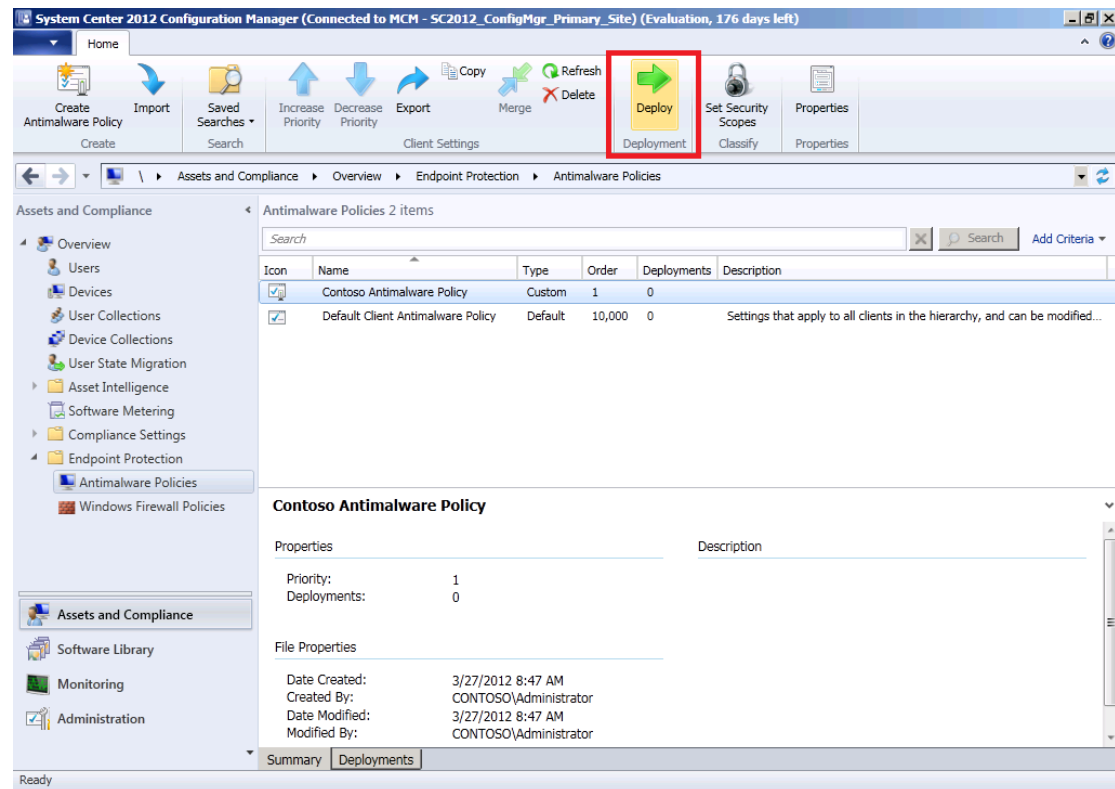


6) Click **Set Source** , the Configure Definition Update Sources dialog box appears , you can select your needs update source and priority :

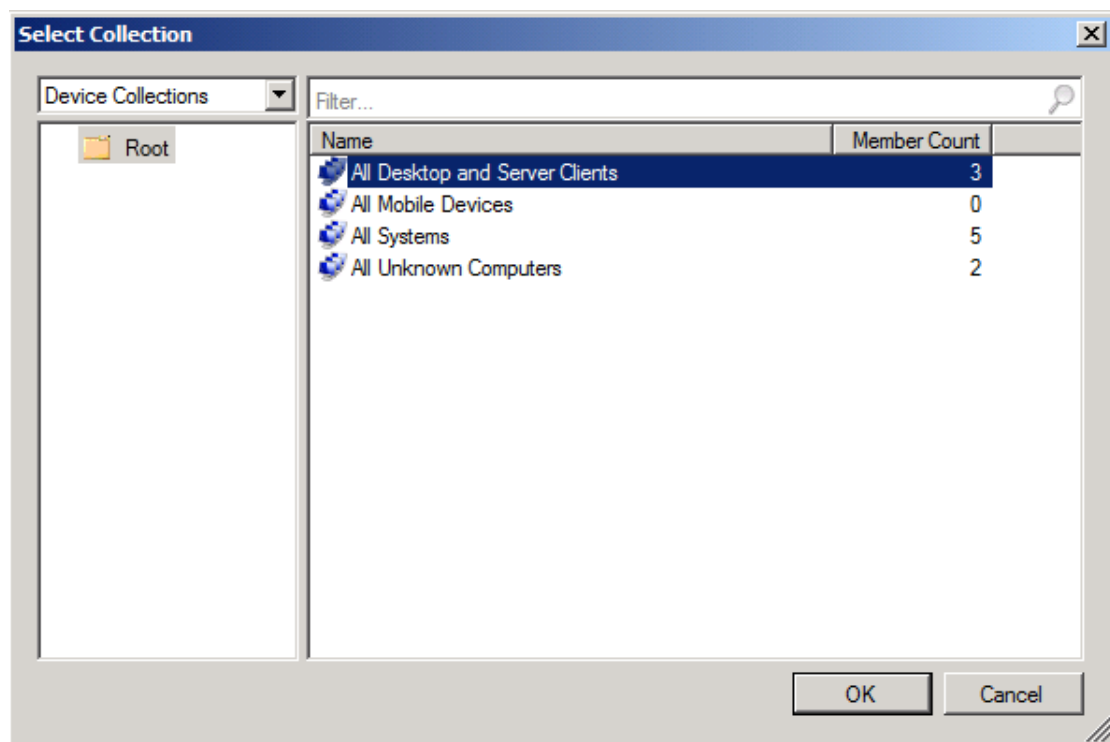


7) Click **OK** twice . In the results pane , click just created policy , and then on

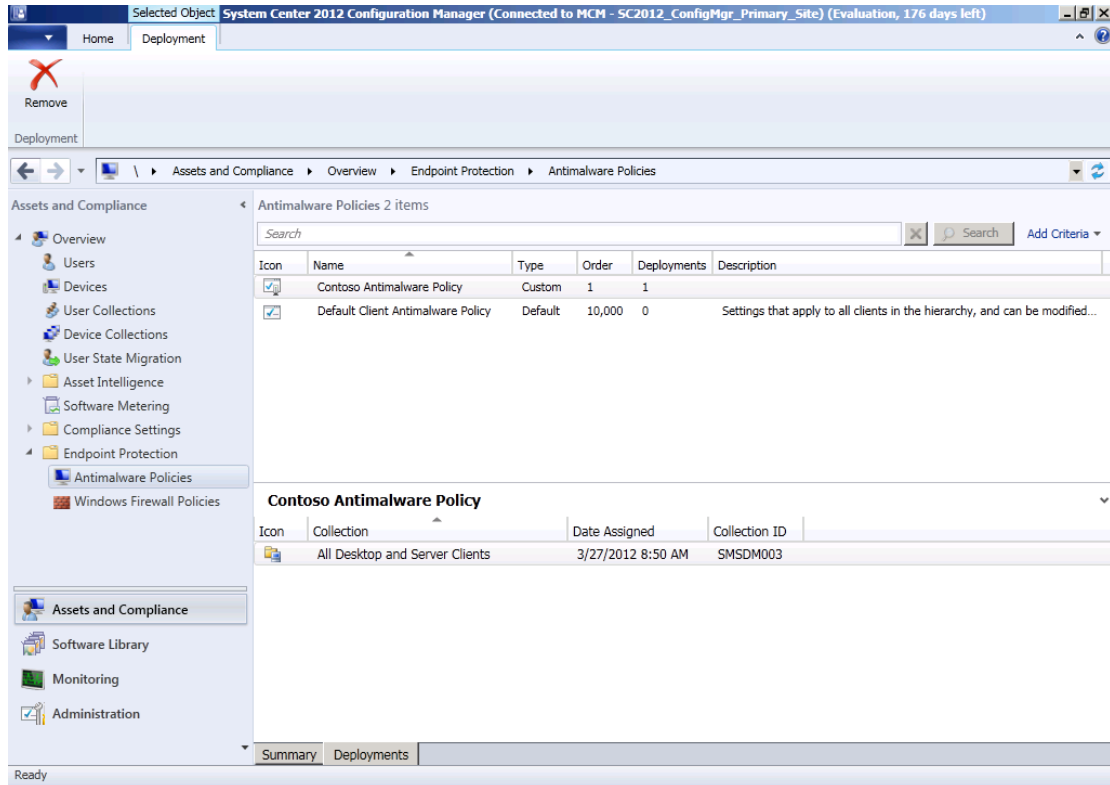
the Ribbon , click **Deploy** :



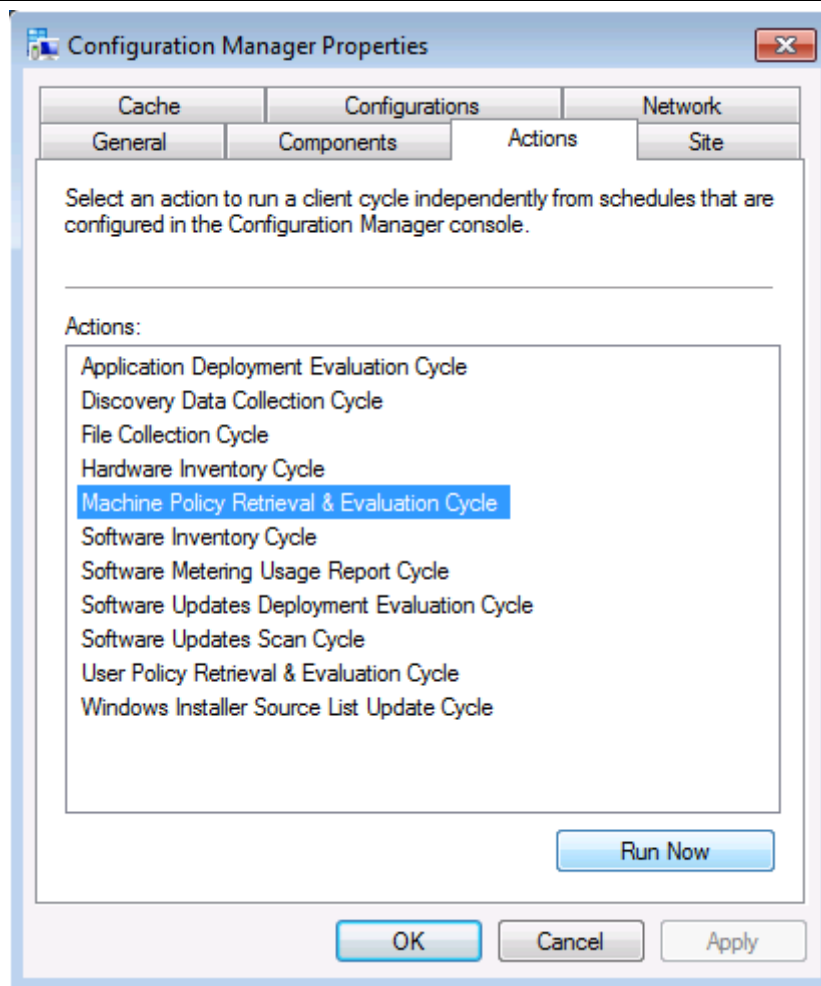
8) A **Select Collection** dialog box appears :



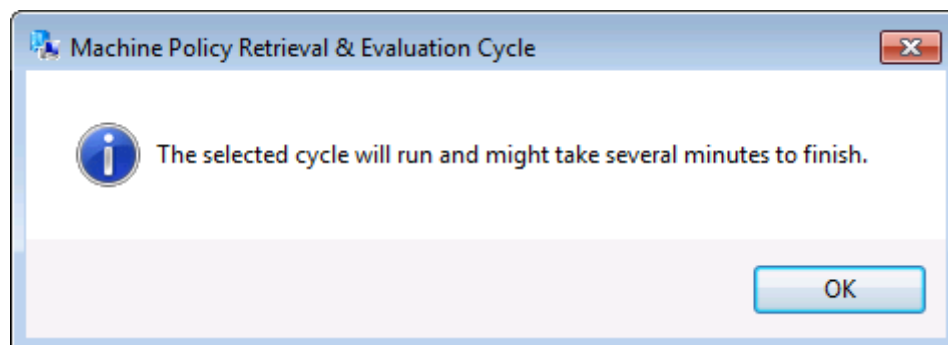
9) Select any **Device Collections** and click **OK** , you can saw this policy having been deployed to one collection :



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** :

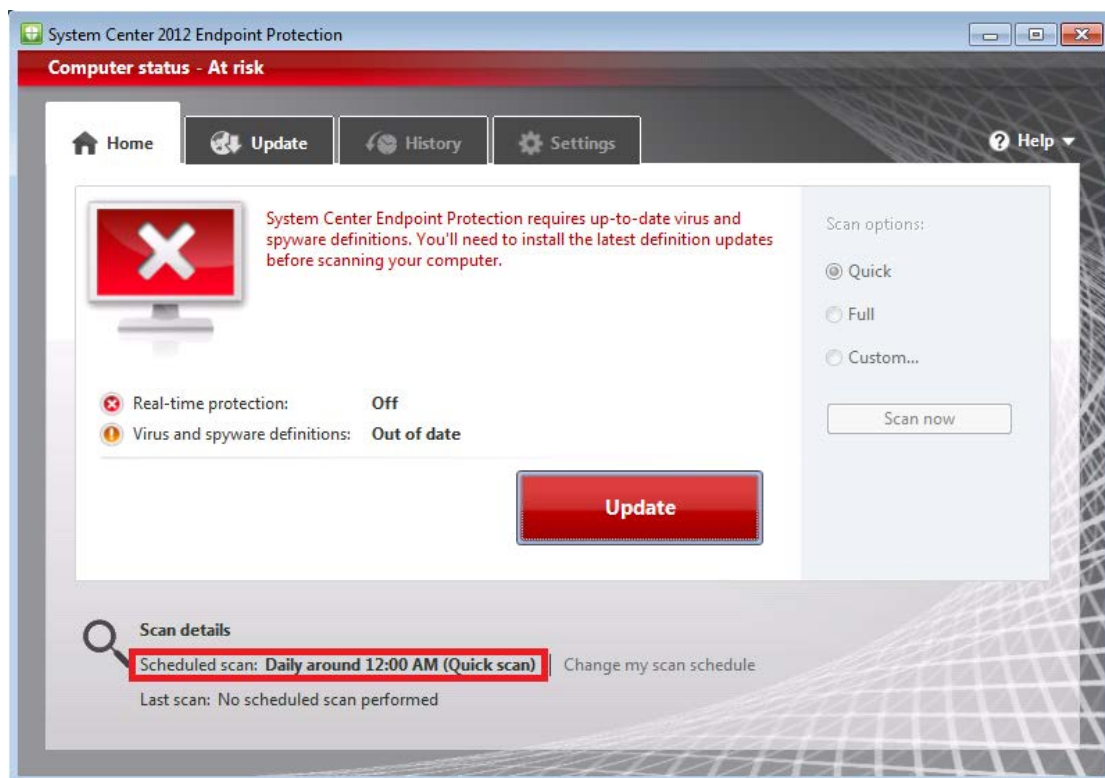


11) A **Machine Policy Retrieval & Evaluation Cycle** message box appears :



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 ,

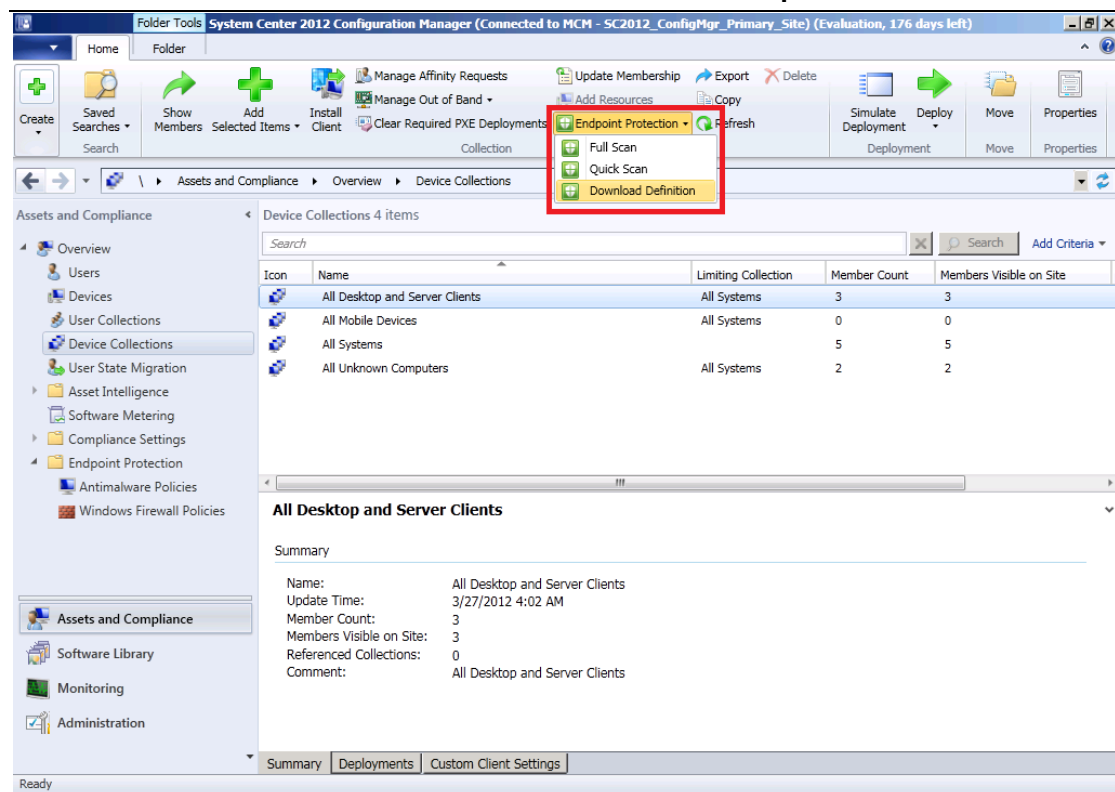
around midnight :



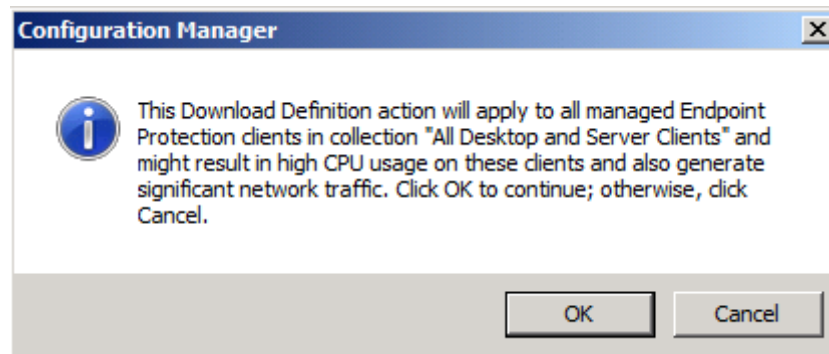
13) This process has not initiated a definition update cycle which occurs automatically every eight hours. You will force it to occur in the next procedure. Close the **System Center 2012 Endpoint Protection** window.

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** :

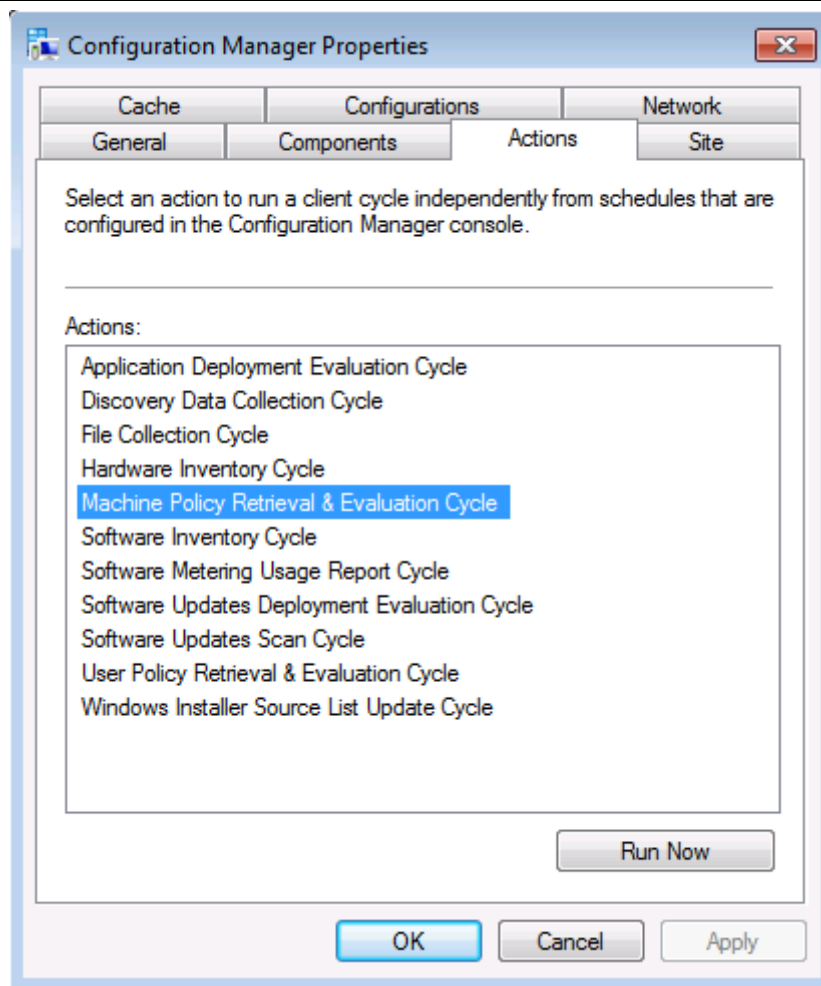
**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



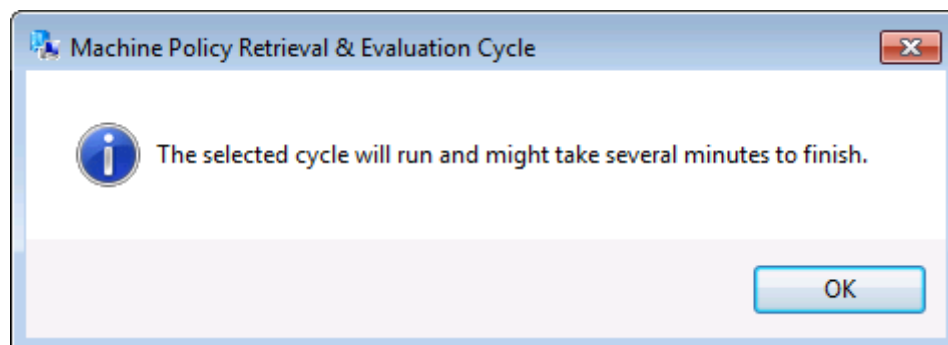
15) A **Configuration Manager** message box appears :



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** :

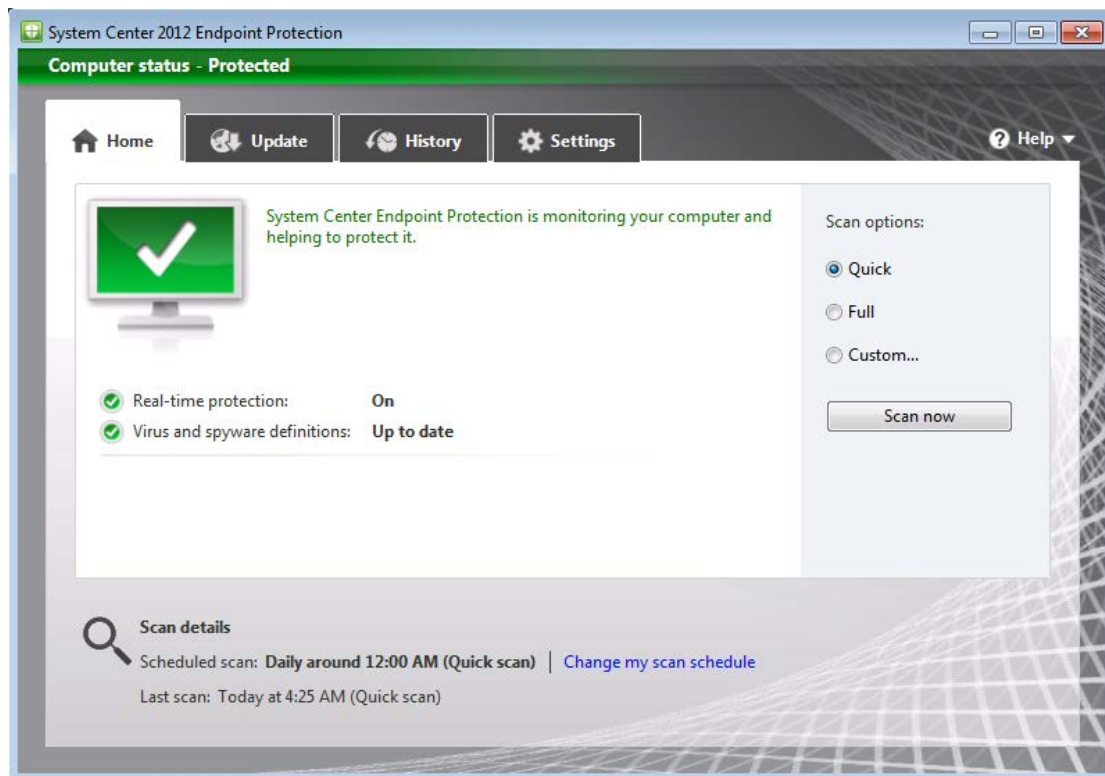


17) A **Machine Policy Retrieval & Evaluation Cycle** message box appears :

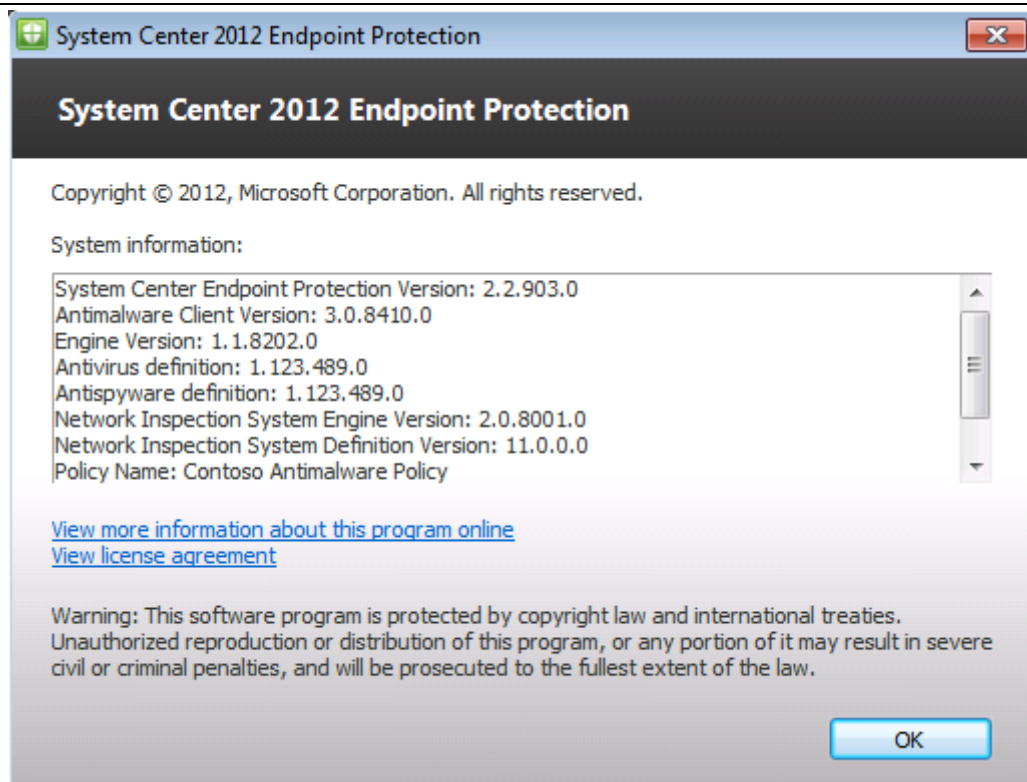


18) Click **OK** . The Endpoint Protection definition will be downloaded on the **Client** computer . Waiting some minutes , on the **Start** menu , click **System Center 2012 Endpoint Protection** , the **System Center 2012 Endpoint Protection** window

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 :

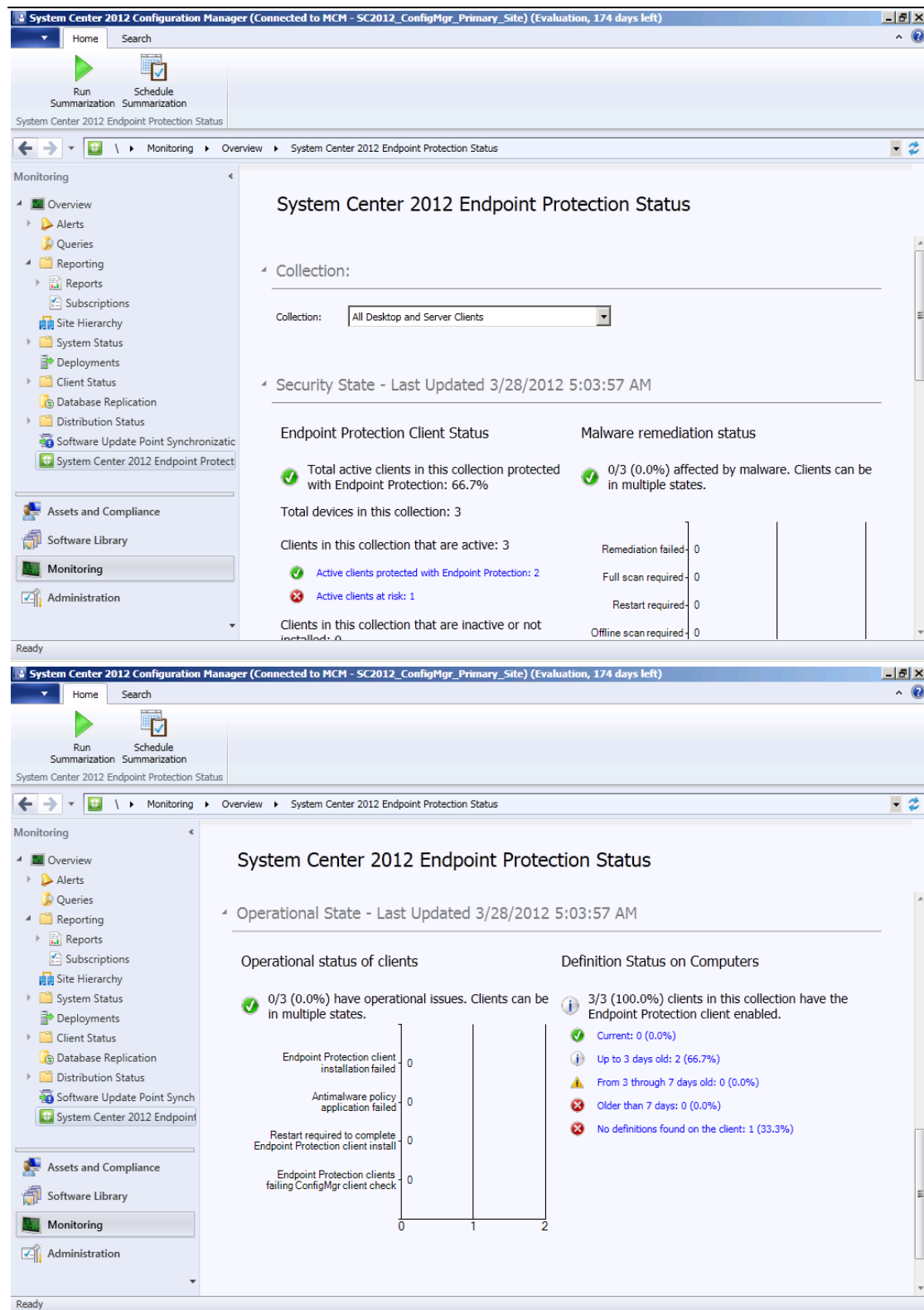


19) Click **Help** , you can see about information :



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** :

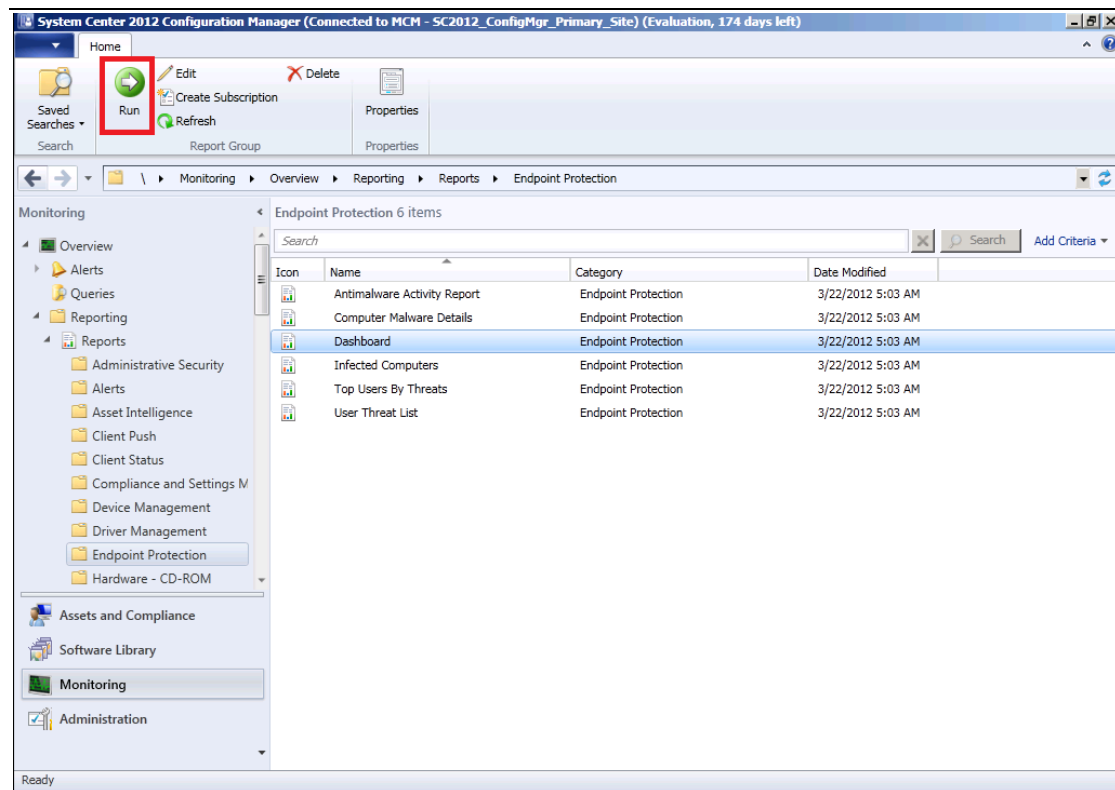
System Center 2012 Configuration Manager RTM Endpoint Protection Document



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

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



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** :

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**

The screenshot shows a web-based interface for viewing a report. The window title is "Dashboard". Inside, there is a section for report parameters:

- Report Category: Endpoint Protection
- Report Name: Dashboard
- Report Description: Endpoint Protection dashboard

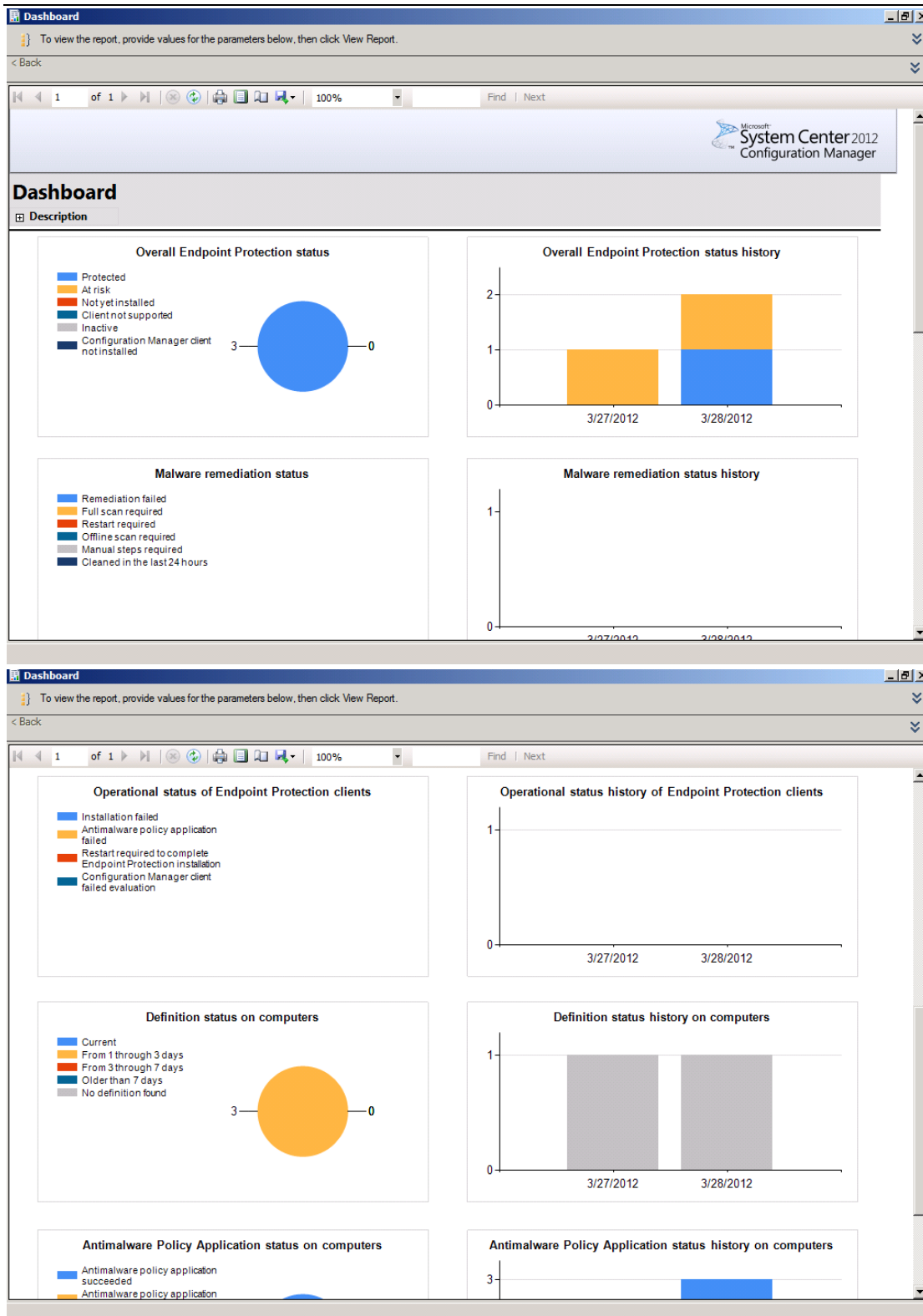
Below this, there are input fields for report parameters:

- Collection: All Desktop and Server Clients (with a "Values..." link)
- Start Date: 3/21/2012 (with a "Values..." link)
- End Date: 3/28/2012 (with a "Values..." link)

A "< Back" link is located below the date fields. A "View Report" button is positioned to the right of the parameter fields. At the bottom of the window, there is a navigation bar with various icons (back, forward, search, etc.), a "100%" zoom level, and a "Find | Next" search bar. The main content area of the report is currently blank.

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

System Center 2012 Configuration Manager RTM Endpoint Protection Document



Operational status of Endpoint Protection clients

- Installation failed
- Antimalware policy application failed
- Restart required to complete Endpoint Protection installation
- Configuration Manager client failed evaluation

Operational status history of Endpoint Protection clients

Definition status on computers

- Current
- From 1 through 3 days
- From 3 through 7 days
- Older than 7 days
- No definition found

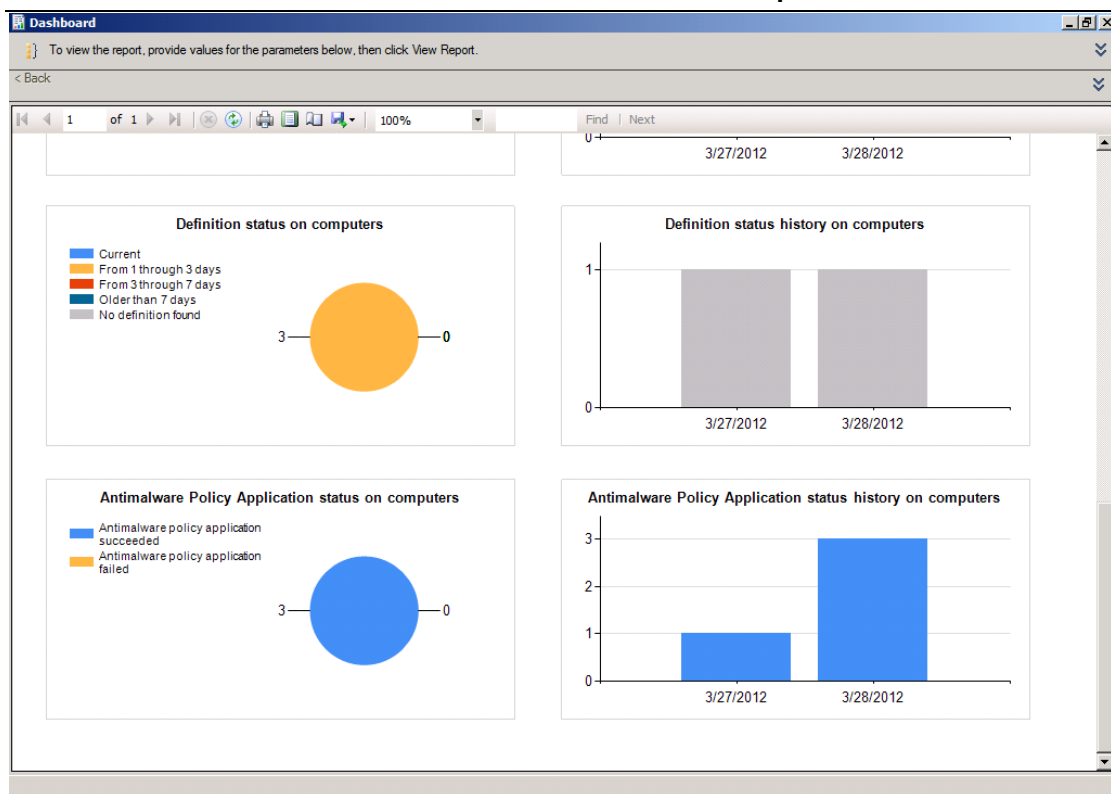
Definition status history on computers

Antimalware Policy Application status on computers

- Antimalware policy application succeeded
- Antimalware policy application

Antimalware Policy Application status history on computers

**System Center 2012
Configuration Manager RTM
Endpoint Protection Document**



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