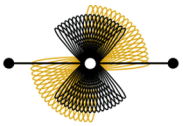


INTERACTIVE INTELLIGENCE
Deliberately Innovative

Symantec Endpoint Protection 12.1 RU1 for Customer Interaction Center Servers and Subsystems

Technical Reference

Version 4.0

Abstract

This document provides the procedures for installing and configuring Symantec Endpoint Protection 12.1 RU1 for Customer Interaction Center servers, such as Interaction Center, Interaction Media Server, and Interaction SIP Proxy.

Last Updated: April 15, 2013

Interactive Intelligence, Inc.
7601 Interactive Way
Indianapolis, Indiana 46278
Telephone/Fax (317) 872-3000
www.ININ.com

Copyright and Trademark Information

Interactive Intelligence, Inc.
7601 Interactive Way
Indianapolis, Indiana 46278
Telephone/Fax (317) 872-3000
www.ININ.com

Table of contents

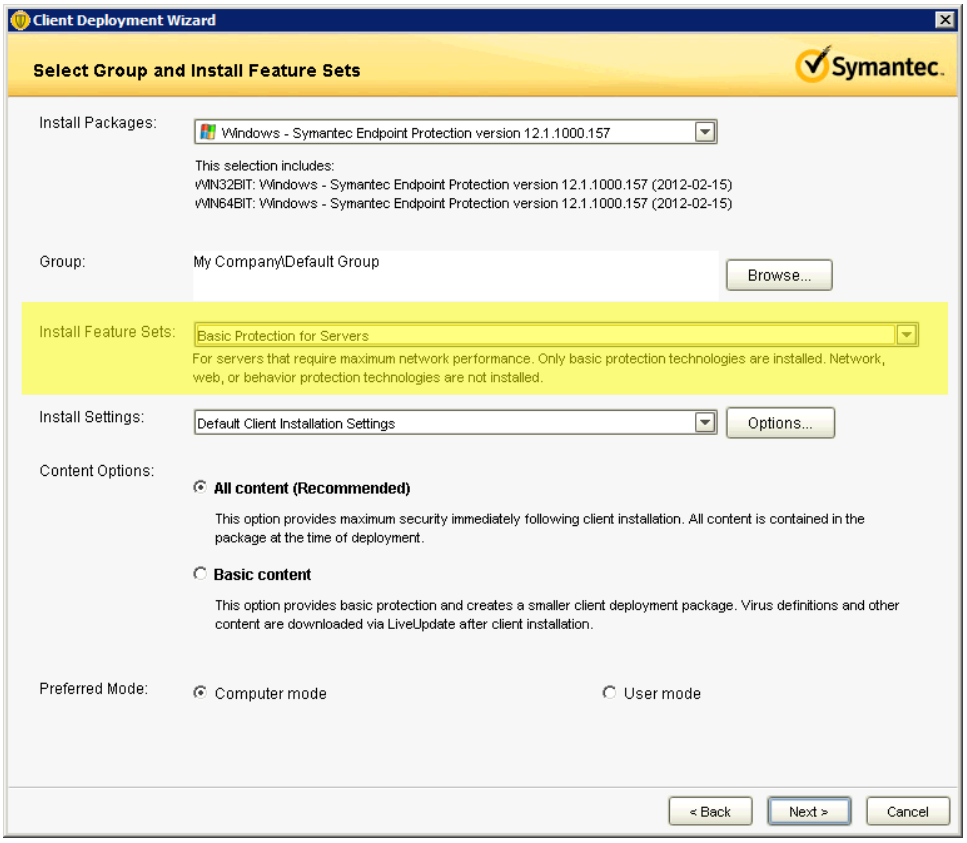
Overview

This document provides procedures for installing and configuring Symantec Endpoint Protection 12.1 Release Update 1 on Interactive Intelligence product servers in your Customer Interaction Center 4.0 environment.

Installation

This topic contains the specific selections that you must choose when deploying Symantec Endpoint Protection 12.1 RU1 on an Interactive Intelligence product server in a Customer Interaction Center 4.0 environment.

1. Use Symantec Endpoint Protection Manager to deploy the software to the Interactive Intelligence product server, such as Interaction Media Server, Interaction Center, or Interaction SIP Proxy.
2. Proceed with the installation until the **Select Group and Install Feature Sets** page of the **Client Deployment Wizard** is displayed.



3. In the **Install Feature Sets** list box, select the **Basic Protection for Servers** item.

> **Caution!**
>
> It is very important that you select the **Basic Protection for Servers** item from the **Install Feature Sets** list box. Other installation feature sets greatly reduce the performance and capacity of Interactive Intelligence servers.

4. Select the **Next** button.
5. Finish the installation wizard.

Configuration

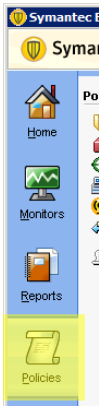
This topic provides the procedure for configuring Symantec Endpoint Protection 12.1 RU1 after you have deployed it to an Interactive Intelligence product server in a Customer Interaction Center 4.0 environment.

Important!

To successfully complete this procedure, ensure that the documentation for the Interactive Intelligence product on which you are configuring Symantec Endpoint Protection 12.1 RU1 is available. The product documentation for your Interactive Intelligence product provides specific information regarding the directories and file types that you must exclude from the Auto-Protect feature.

To configure Symantec Endpoint Protection 12.1 RU1 on an Interactive Intelligence product server, do the following steps:

1. From the **Start** menu, select **All Programs** > **Symantec Endpoint Protection Manager** > **Symantec Endpoint Protection Manager Tools**.
2. In the left pane of the **Symantec Endpoint Protection Manager** window, select the **Policies** object.

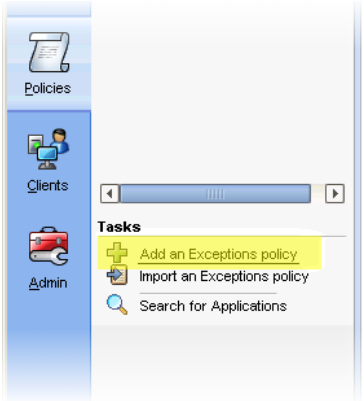


Important!

You can only define a Tamper Protection Exception through System Endpoint Protection Manager. You cannot configure this feature through the client software.

3. In the **Policies** area, select the **Exceptions** item.

4. In the **Tasks** area, select the **Add an Exceptions policy** item.

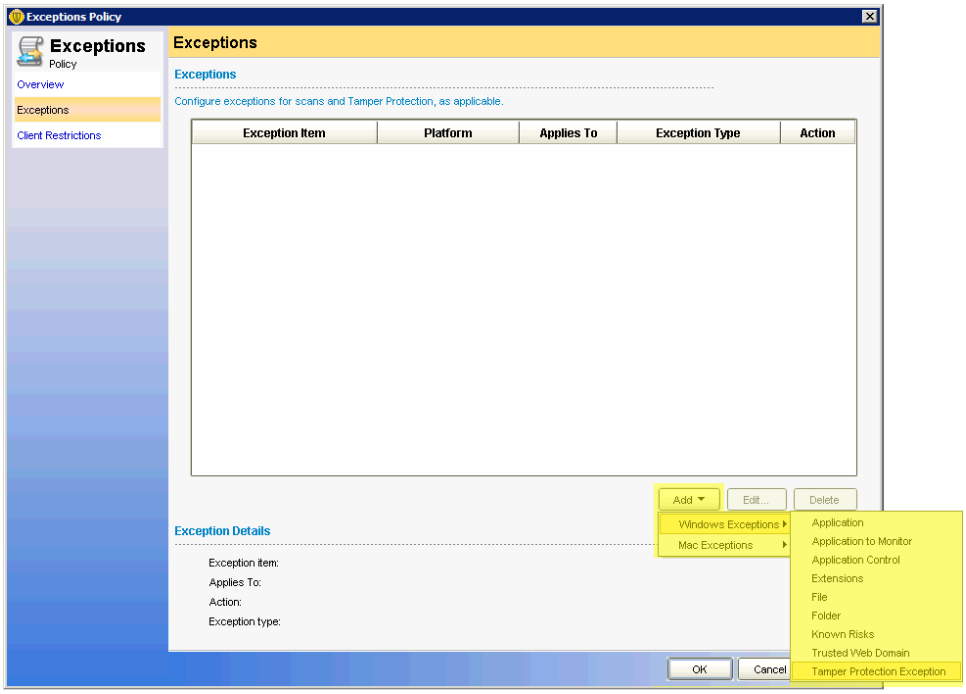


This new exception policy will be for all Interactive Intelligence product servers.

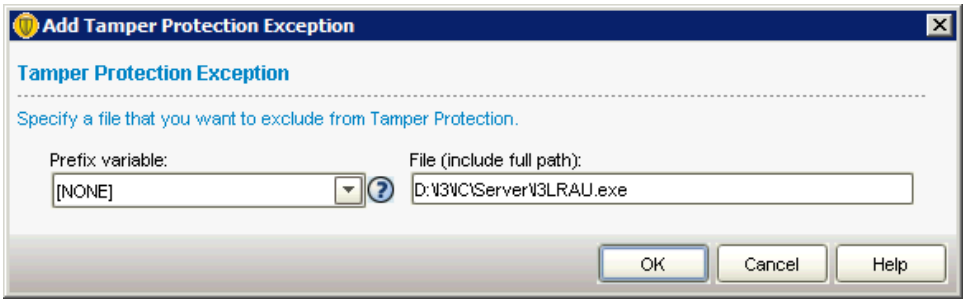
The **Exceptions Policy** window is displayed.

5. If you are configuring the antivirus software on an Interaction Center server, do the following steps:

   a. In the lower-right area of the **Exceptions Policy** window, select **Add** > **Windows Exceptions** > **Tamper Protection Exception**.



   The **Add Tamper Protection Exception** dialog box is displayed.



   b. In the **File (include full path)** box, enter a file from the following list:

- I3LRAU.exe
- RemocoServerU.exe
- HostServerU.exe
- ProcessAutomationServerU.exe

c. Select the **OK** button.

> **Important!**
>
> When you specify a file, you must include the full path, including the drive letter. You set the installation directory when you installed Interaction Center. Verify the path where these files are located.

d. Repeat this series of steps for each file in the list.

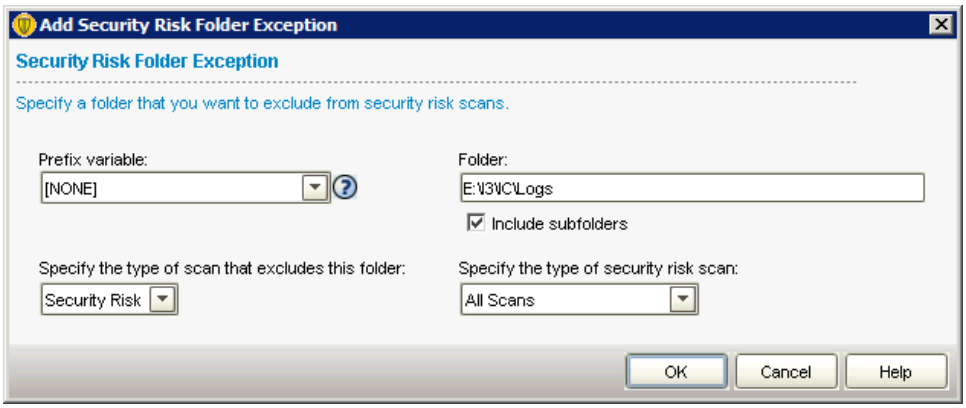
6. Do the following steps for each directory listed in the antivirus exclusion information in your Interactive Intelligence product documentation:

   a. In the lower-right area of the **Exceptions Policy** window, select **Add** > **Windows Exceptions** > **Folder**.

      The **Add Security Risk Folder Exception** dialog box is displayed.

   b. In the **Folder** box, enter a directory from the directory exclusion list in the product documentation.

> **Important!**
>
> Ensure that you enable the **Include subfolders** check box for each directory exclusion.



   c. In the **Specify the type of scan that excludes this folder** list box, select **Security Risk**.

   d. In the **Specify the type of security risk scan** list box, select **All Scans**.

   e. Select the **OK** button.

   f. Repeat this series of steps for each directory in the list.

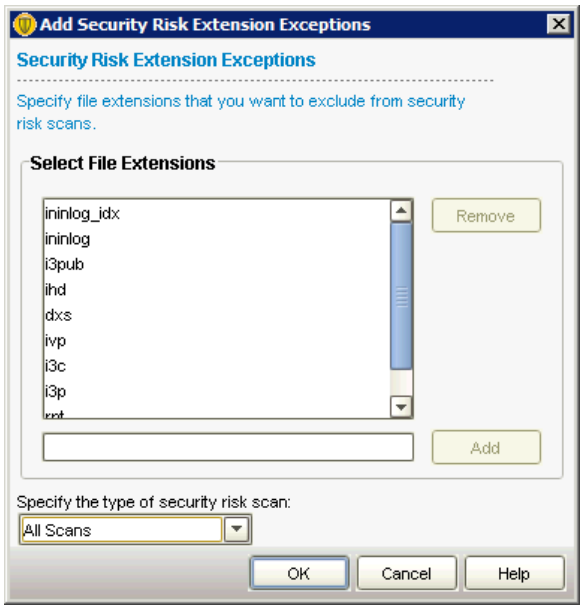
7. Do the following steps for each file extension listed in the antivirus exclusion information in your Interactive Intelligence product documentation:

   a. In the lower-right area of the **Exceptions Policy** window, select **Add** > **Windows Exceptions** > **Extension**.

   b. In the box below the **Select File Extensions** list box, enter a file extension from the antivirus file exclusion list in the documentation for your Interactive Intelligence product.

   c. Select the **Add** button.

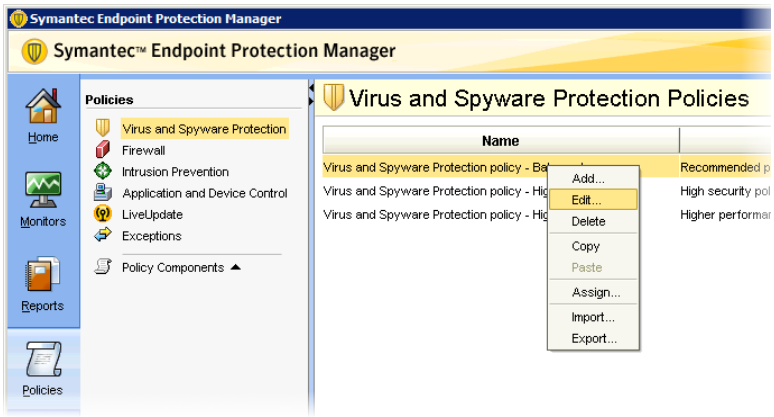
      The specified extension is displayed in the **Select File Extensions** list box.



d. Repeat this series of steps for each file extension in the list.

8. After you have added all documented file extension exclusions, select the **OK** button.
9. In the **Symantec Endpoint Protection Manager** window, select the **Virus and Spyware Protection** object.

10. In the **Virus and Spyware Protection Policies** pane, right-click the policy that you added and select **Edit** from the resulting shortcut menu.

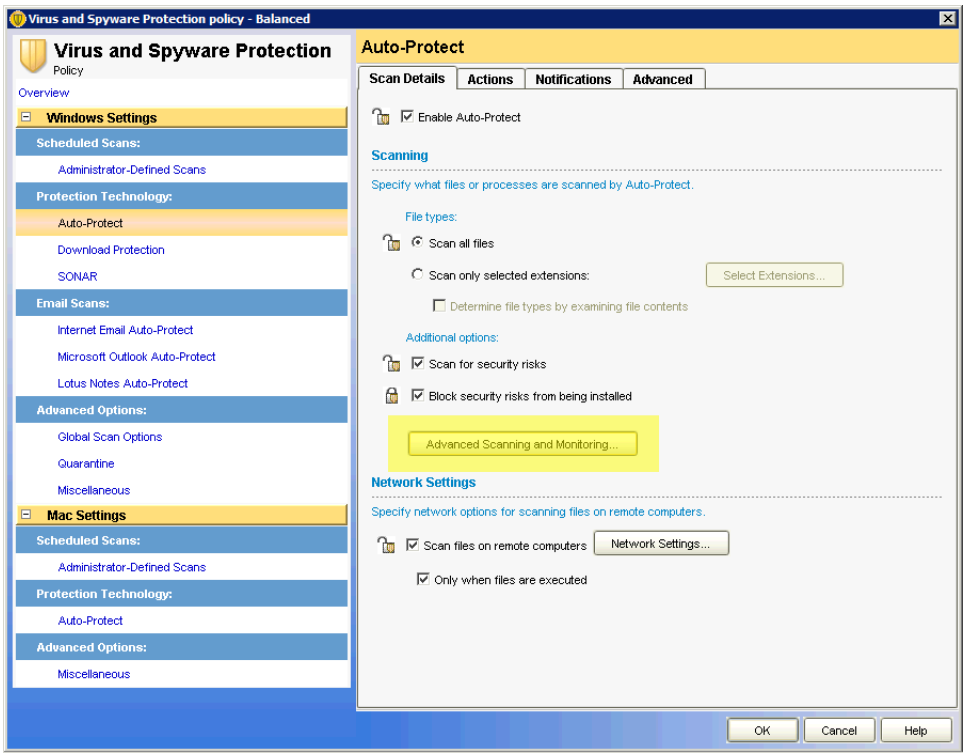


The **Virus and Spyware Protection policy** window for the selected policy is displayed.

11. In the left pane, select **Windows Settings** > **Protection Technology** > **Auto-Protect**.

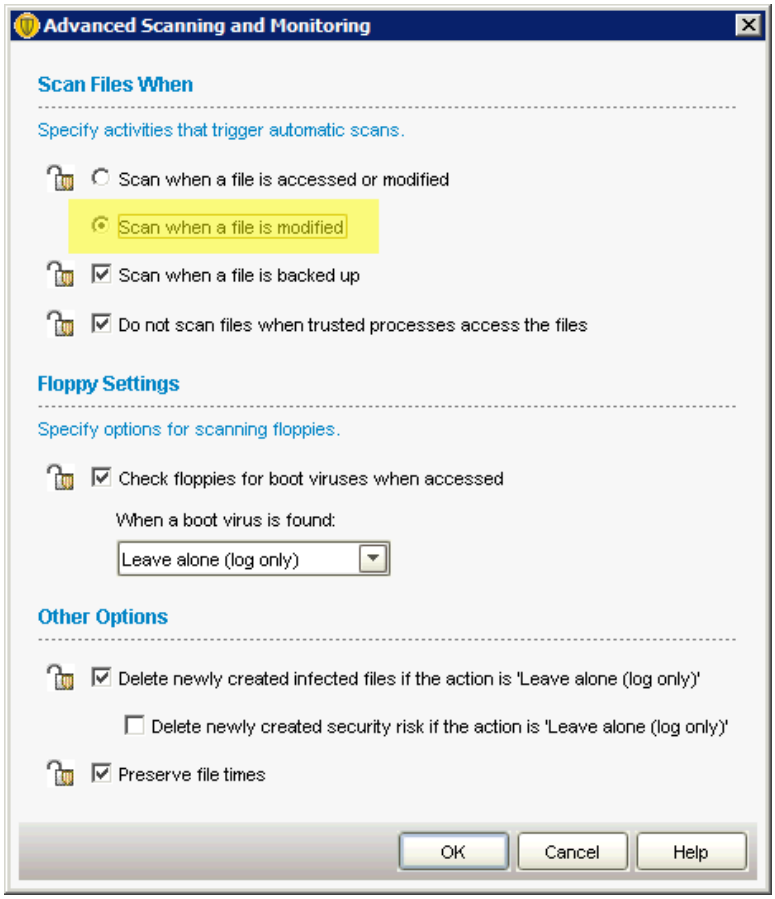
The **Auto-Protect** pane is displayed on the right side of the window.

12. On the **Scan Details** tab of the **Auto-Protect** pane, select the **Advanced Scanning and Monitoring** button.



The **Advanced Scanning and Monitoring** dialog box is displayed.

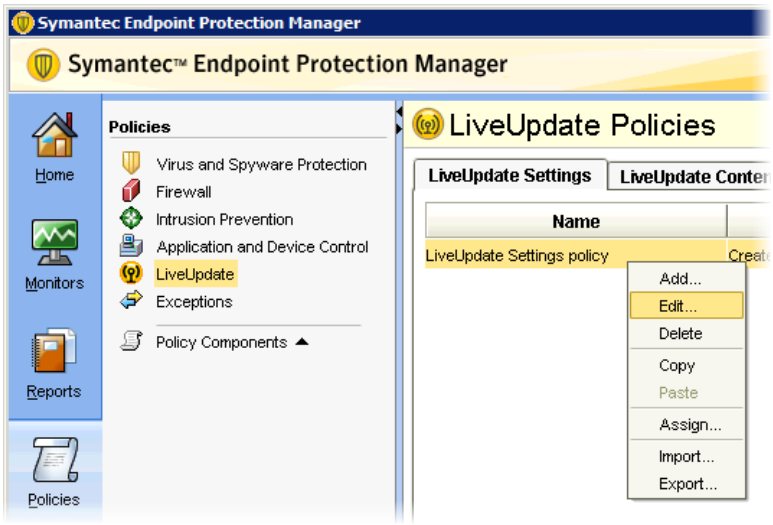
13. In the **Scan Files When** area, select the **Scan when a file is modified** option.



14. Select the **OK** button.
15. In the **Symantec Endpoint Protection Manager** window, select the **LiveUpdate** object.

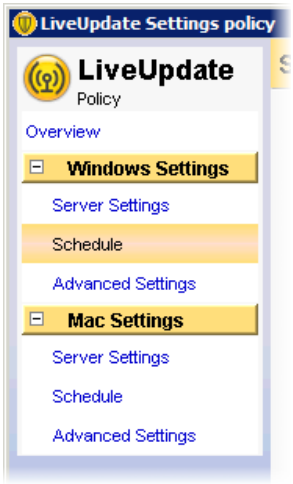
The **LiveUpdate Policies** pane is displayed on the right side of the window.

16. On the **LiveUpdate Setting** tab, right-click the **LiveUpdate Settings** policy item and select **Edit** from the resulting shortcut menu.



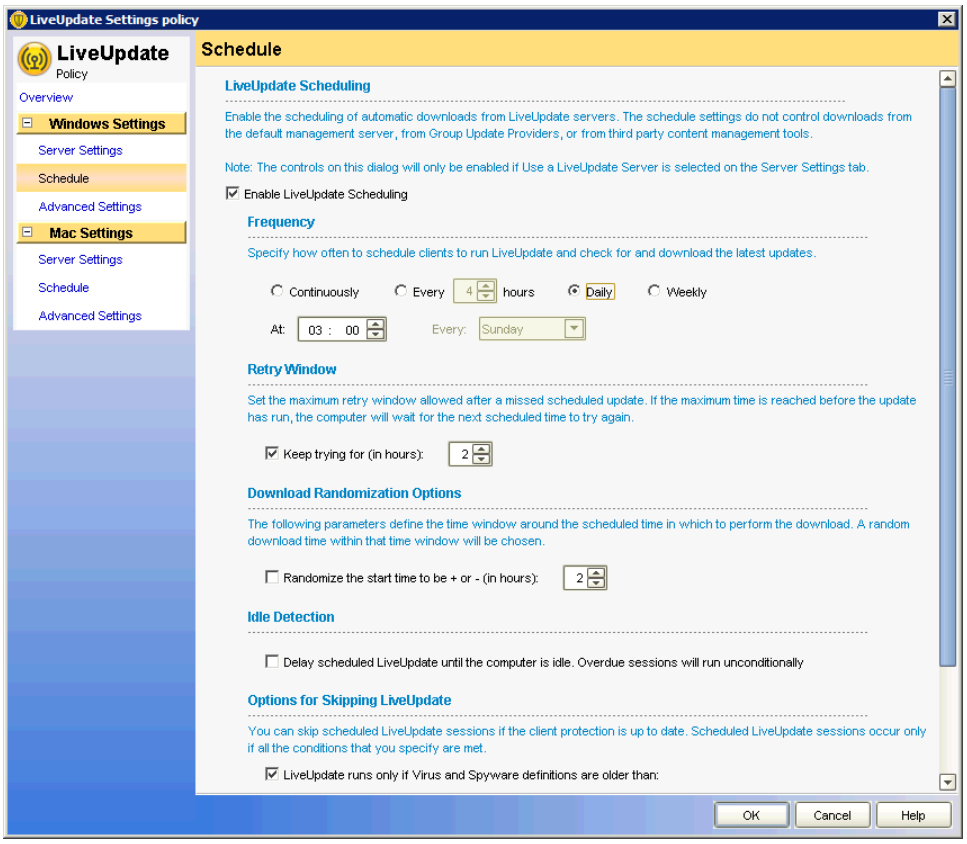
The **LiveUpdate Settings policy** window is displayed.

17. In the left pane, select **Windows Settings** > **Schedule**.

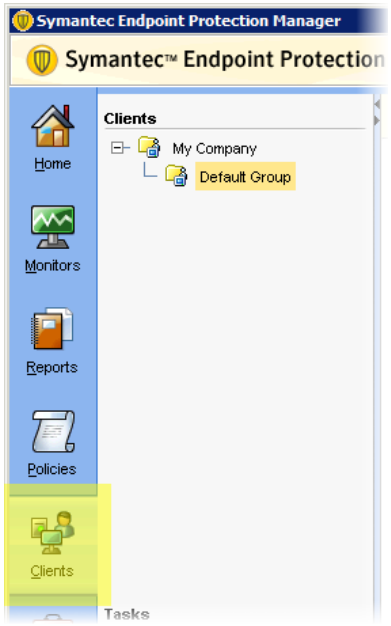


The **Schedule** pane is displayed on the right side of the window.

18. In the **Schedule** pane, use the available controls to set the update process to occur during off-peak hours.



19. When you have finished configuring the update schedule, select the **OK** button.
20. In the left pane of the **Symantec Endpoint Protection Manager** window, select the **Clients** object.

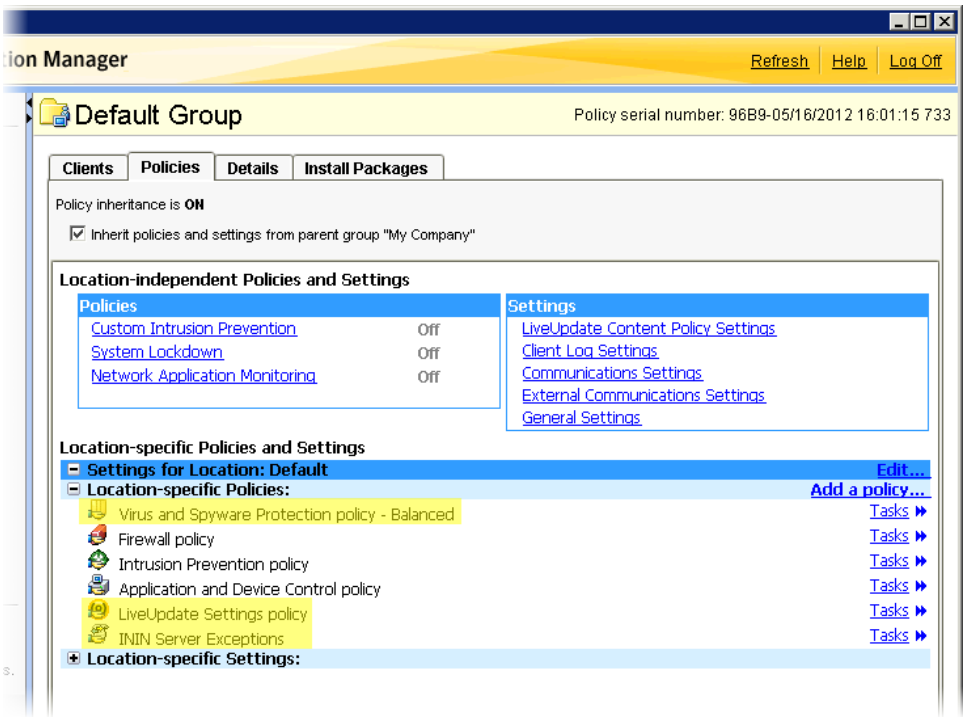


21. In the **Clients** area, select the group to which you have assigned your Interactive Intelligence product servers.

    The configuration pane for the selected group is displayed on the right side of the window.

22. In the **Location-specific Policies and Settings** area, ensure that the following items that you modified for your Interactive Intelligence product server are being issued:

    - Virus and Spyware Protection policy
    - LiveUpdate Settings policy
    - Exceptions policy



Change Log

The following changes have been made to this document since release:

Date	Change
June 15, 2012	Initial Release
July 5, 2012	Added admonishment about the importance of selecting the correct installation type
April 15, 2013	Added content stating that the reader must verify the paths of excluded files