Symantec Endpoint Protection 12.1.6 for Customer Interaction Center Servers and Subsystems

Technical Reference

Interactive Intelligence Customer Interaction Center® (CIC)

Version 2016

Last updated January 14, 2016

(See Change Log for summary of changes.)

Abstract

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

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

Installation

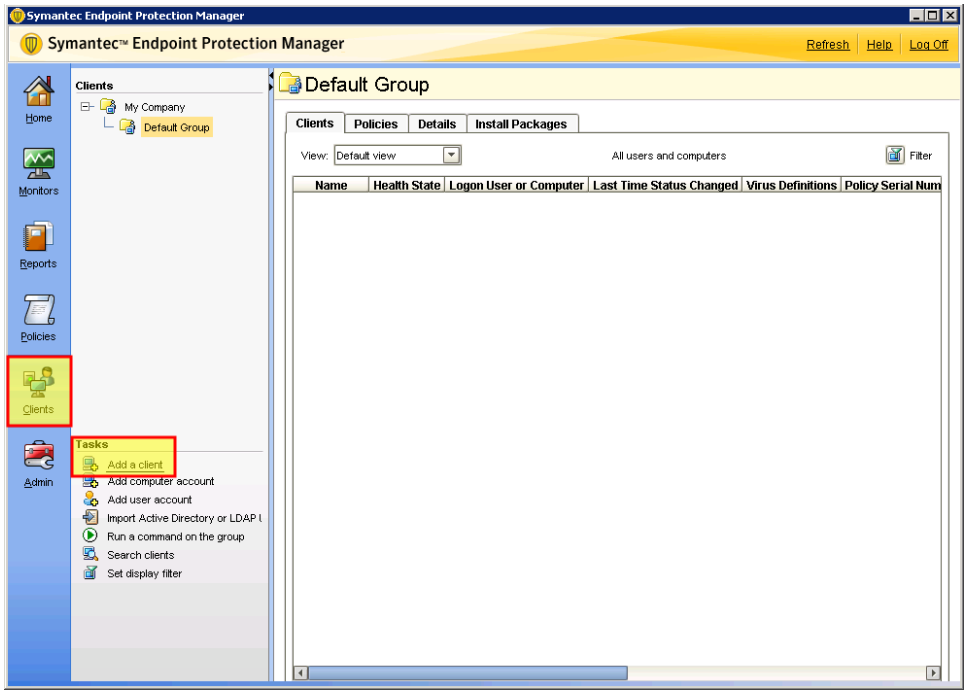
This topic contains the specific selections that you must choose when deploying Symantec Endpoint Protection on an Interactive Intelligence product server in a Customer Interaction Center environment.

1. Open Symantec Endpoint Protection Manager.

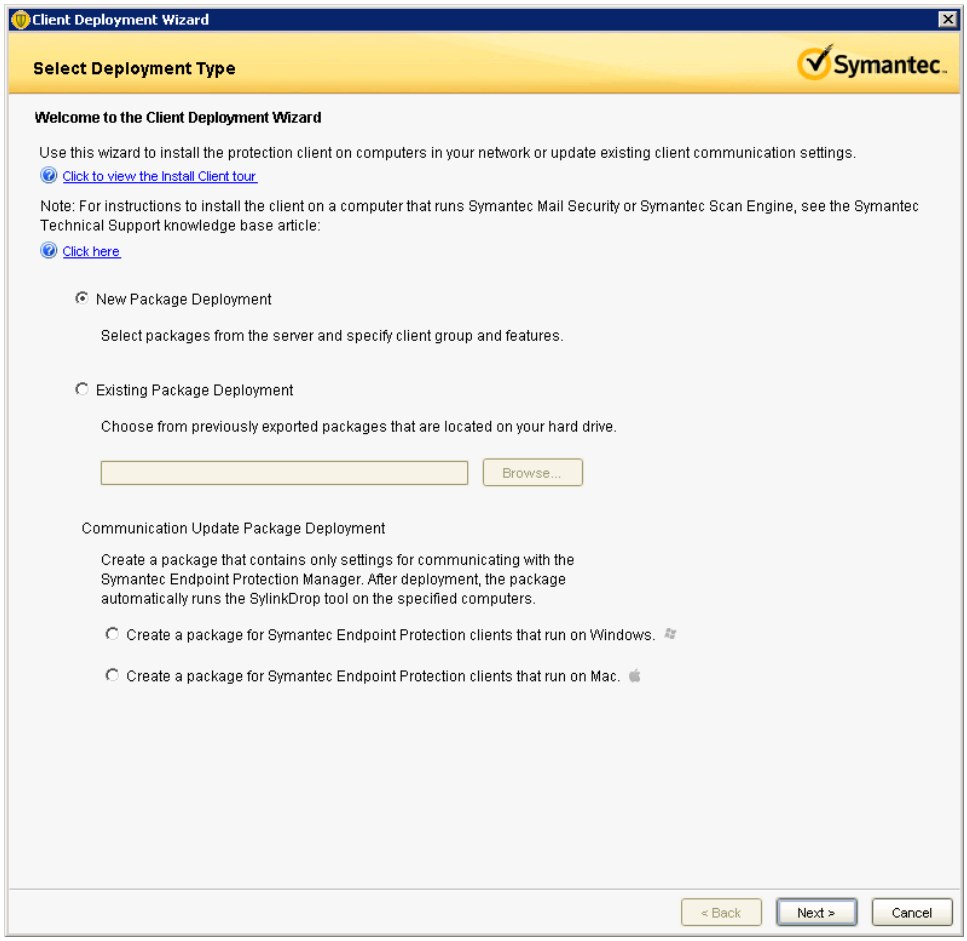
   The **Symantec Endpoint Protection Manager** window appears.

2. On the left side of the **Symantec Endpoint Protection Manager** window, select the **Clients** icon.

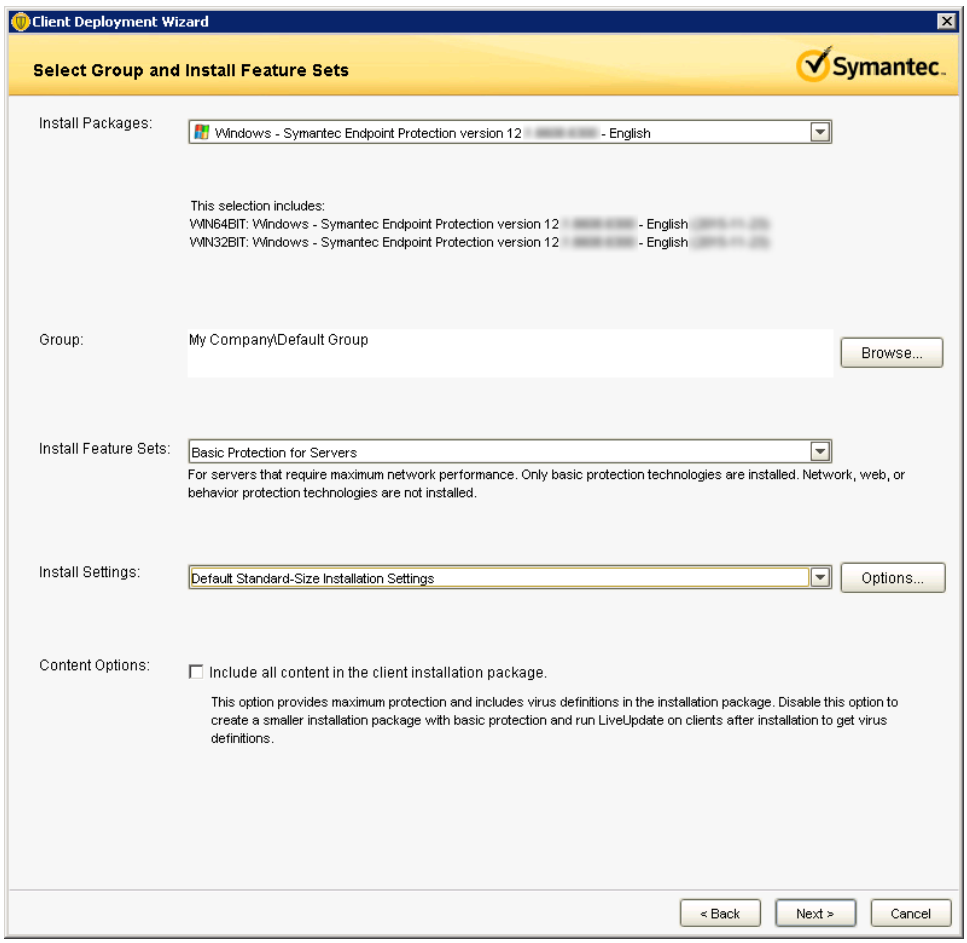
3. In the **Tasks** list in the lower left area of the window, select **Add a client**.



   The **Client Deployment Wizard** dialog box appears.



4. In the **Select Deployment Type** page of the wizard, select the **New Package Deployment** option.
5. Select the **Next** button.
6. Proceed with the installation until the **Select Group and Install Feature Sets** page of the wizard appears.



7. 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. If you use another method of installing Symantec Endpoint Protection than the one provided in this procedure, you must ensure that the installation uses only the **Basic Protection for Server** option.

8. Select the **Next** button.
9. Finish the installation wizard.

Configuration

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

> **Important!**
>
> To successfully complete this procedure, ensure that the documentation for the Interactive Intelligence product on which you are configuring Symantec Endpoint Protection 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.

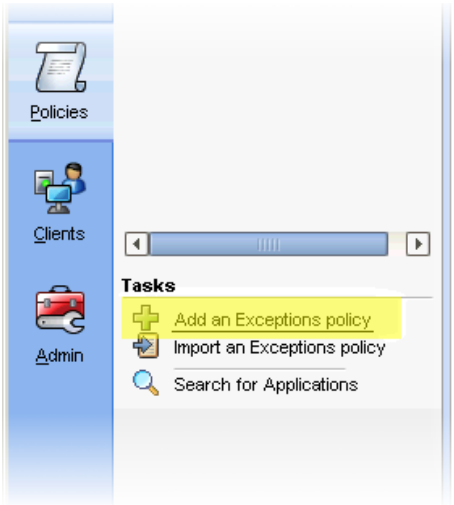
To configure Symantec Endpoint Protection on an Interactive Intelligence product server, do the following steps:

1. From the Start menu, select All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager.
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.

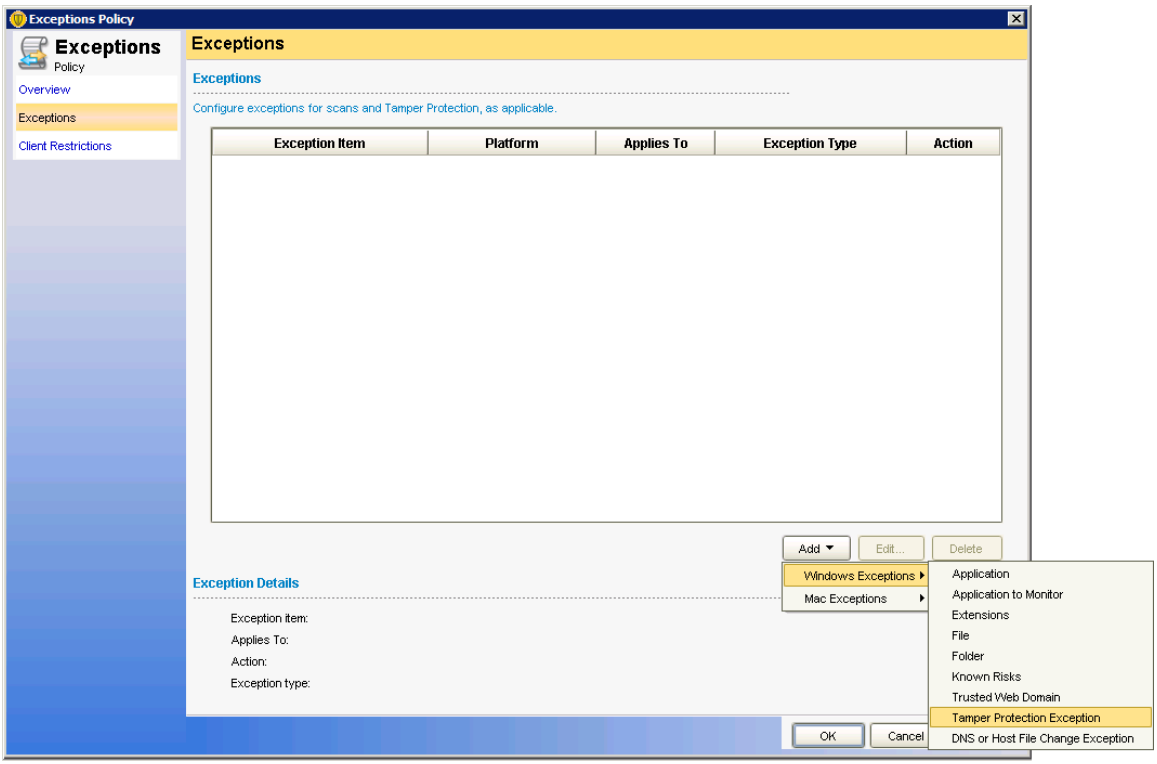


This new exception policy will be for all Interactive Intelligence product servers.

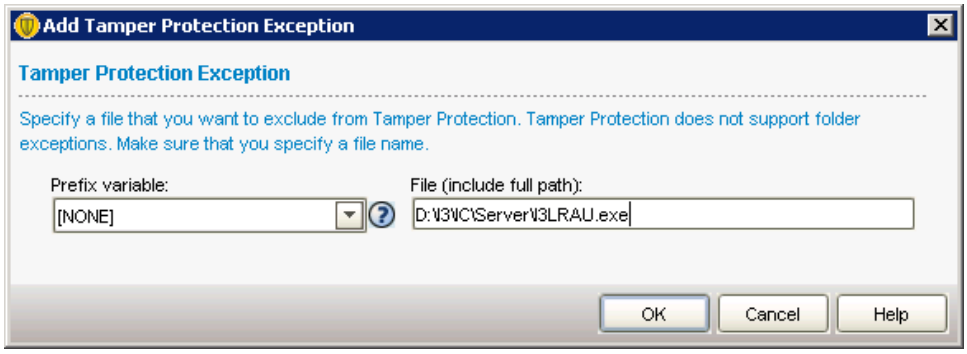
The **Exceptions Policy** window appears.

5. If you are configuring the antivirus software on a Customer 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 appears.



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 Customer 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 in the following list:

- *(ICDrive)*`\I3\IC\Recordings`

(or the directory where recordings and temporary recordings are stored)

Note:

(ICDrive) is a variable that represents the letter of the hard drive where you installed the product, such as `C:` or `D:`.

- *(ICDrive)*`\ININ_Tracing`
- *(ICDrive)*`\I3\IC\Logs`

  (The drive may be D: or E:, depending on the product and configured location.)
- *(ICDrive)*`\I3\IC\Mail`
- *(ICDrive)*`\I3\IC\Persistence`
- *(ICDrive)*`\I3\IC\PMQ`
- *(ICDrive)*`\I3\IC\Server\Firmware`
- *(ICDrive)*`\I3\IC\Server\LRA`
- *(ICDrive)*`\I3\IC\Work`
- All directories and included subdirectories that are specified as server parameters in Interaction Administrator
- All directories and subdirectories that the Customer Interaction Center switchover system mirrors

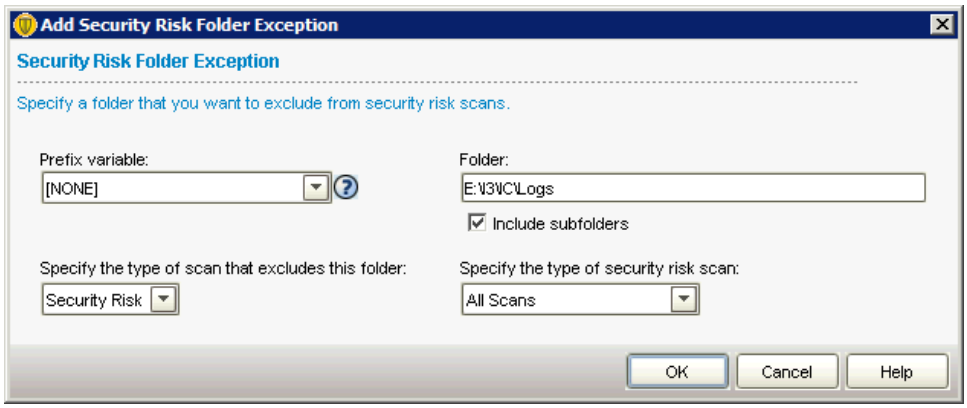
a. In the lower-right area of the **Exceptions Policy** window, select **Add** > **Windows Exceptions** > **Folder**.

   The **Add Security Risk Folder Exception** dialog box appears.

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:

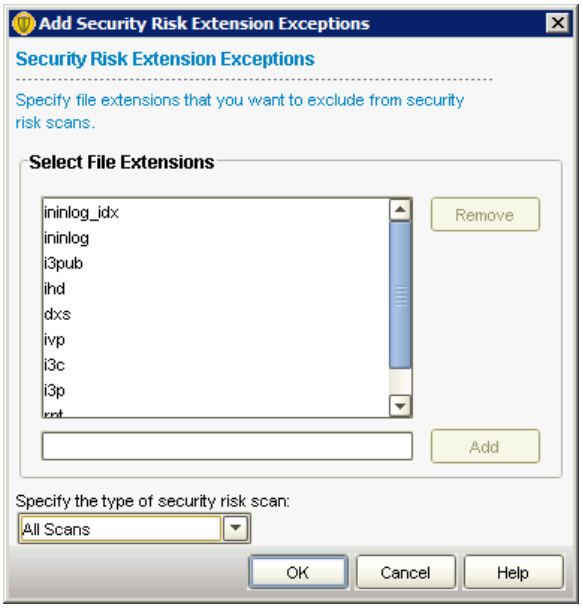
   a. In the lower-right area of the **Exceptions Policy** window, select **Add** > **Windows Exceptions** > **Extension**.

b. In the box below the **Select File Extensions** list box, enter a file extension from the following list:

- `fbma`
- `rpt`
- `i3p`
- `i3c`
- `ivp`
- `dxs`
- `ihd`
- `i3pub`
- `xml`
- `db`
- `ininlog` (CIC log file format)
- `ininlog_idx` (CIC log index file format)

c. Select the **Add** button.

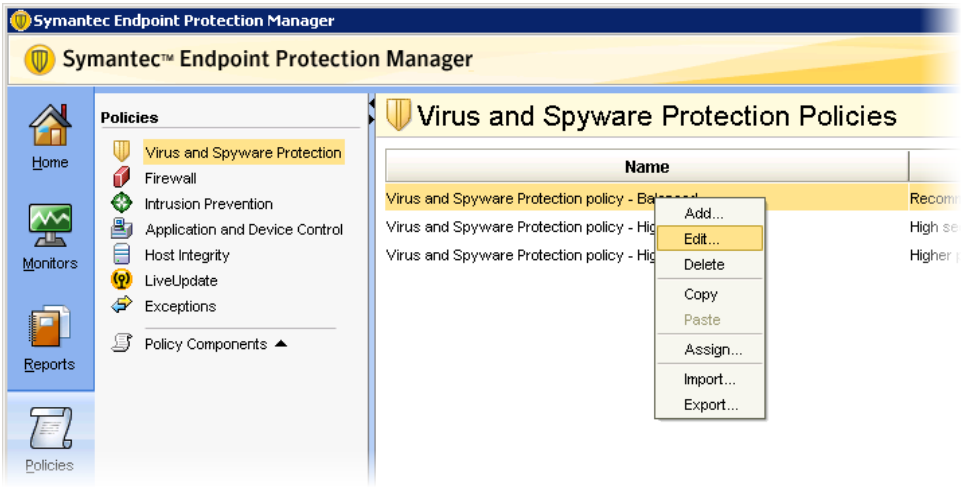
The specified extension appears in the **Select File Extensions** list box.



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

8. Ensure that the **All Scans** list item is displayed in the **Specify the type of security risk scan** box.
9. After you have added all documented file extension exclusions and selected the type of scans to not apply to the file extensions, select the **OK** button.
10. In the **Symantec Endpoint Protection Manager** window, select the **Virus and Spyware Protection** object.

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

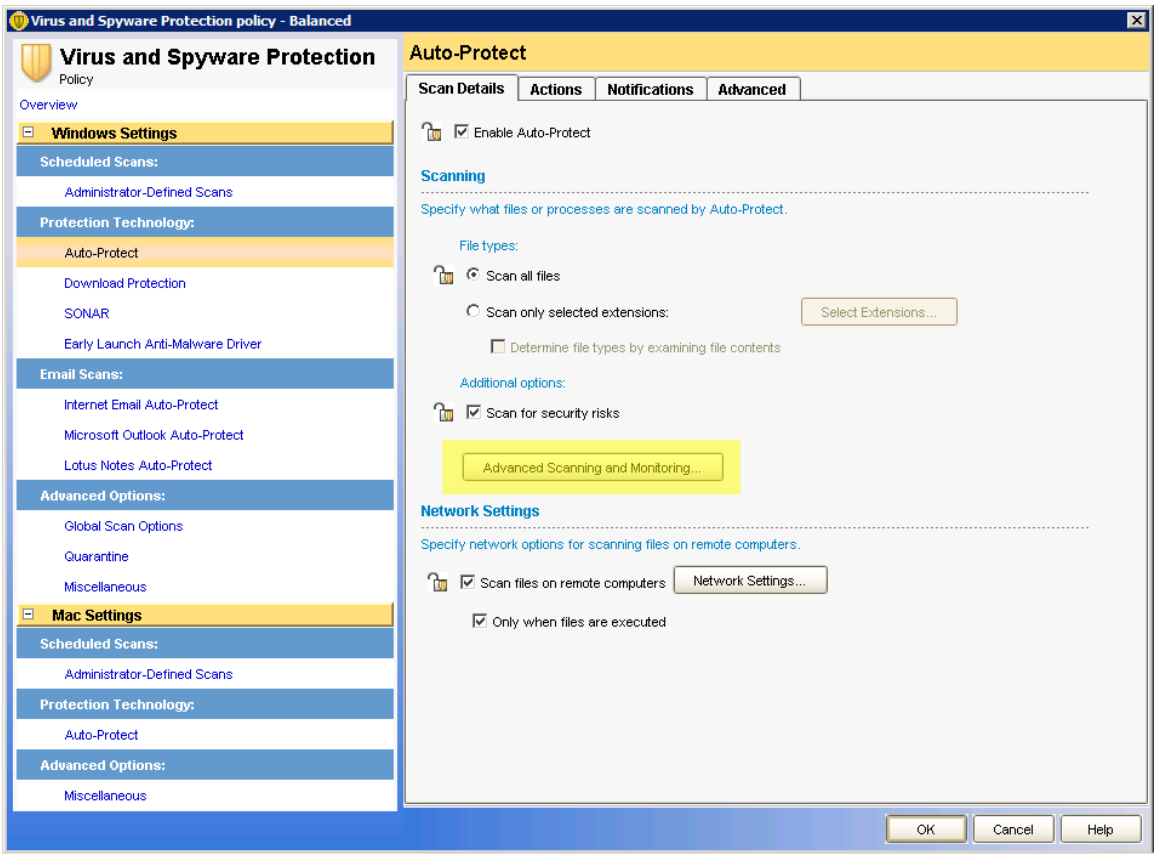


The **Virus and Spyware Protection policy** window for the selected policy appears.

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

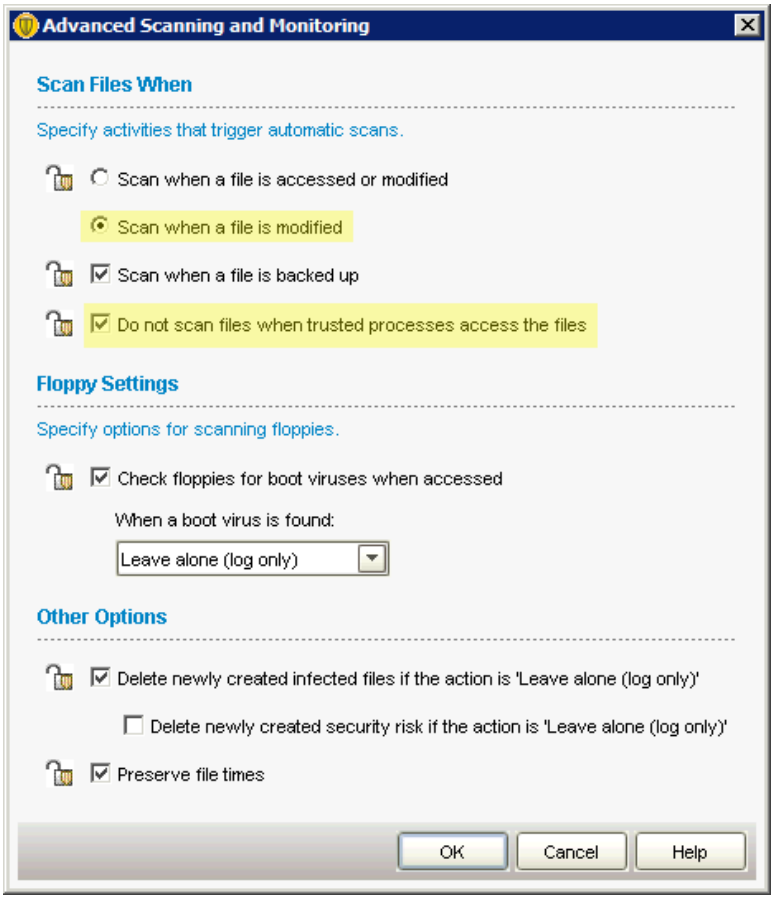
The **Auto-Protect** pane appears on the right side of the window.

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



The **Advanced Scanning and Monitoring** dialog box appears.

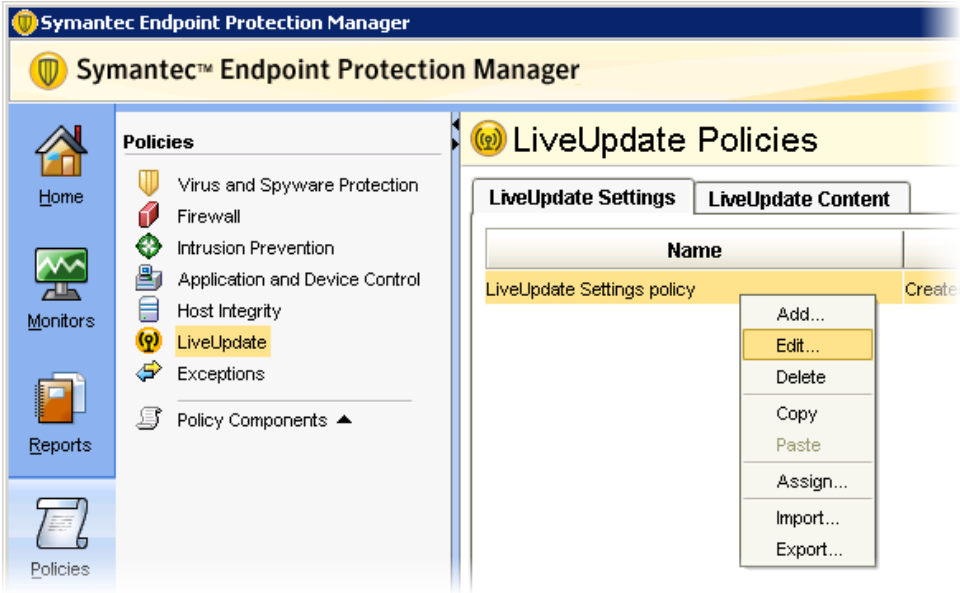
14. In the **Scan Files When** area, do the following steps:
    a. Select the **Scan when a file is modified** option.
    b. Enable the **Do not scan files when trusted processes access the files** check box.



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

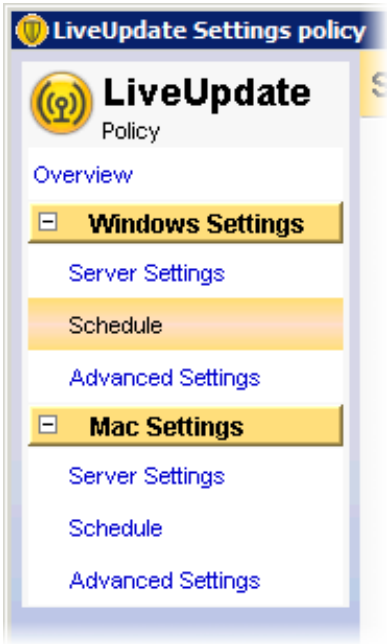
The **LiveUpdate Policies** pane appears on the right side of the window.

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



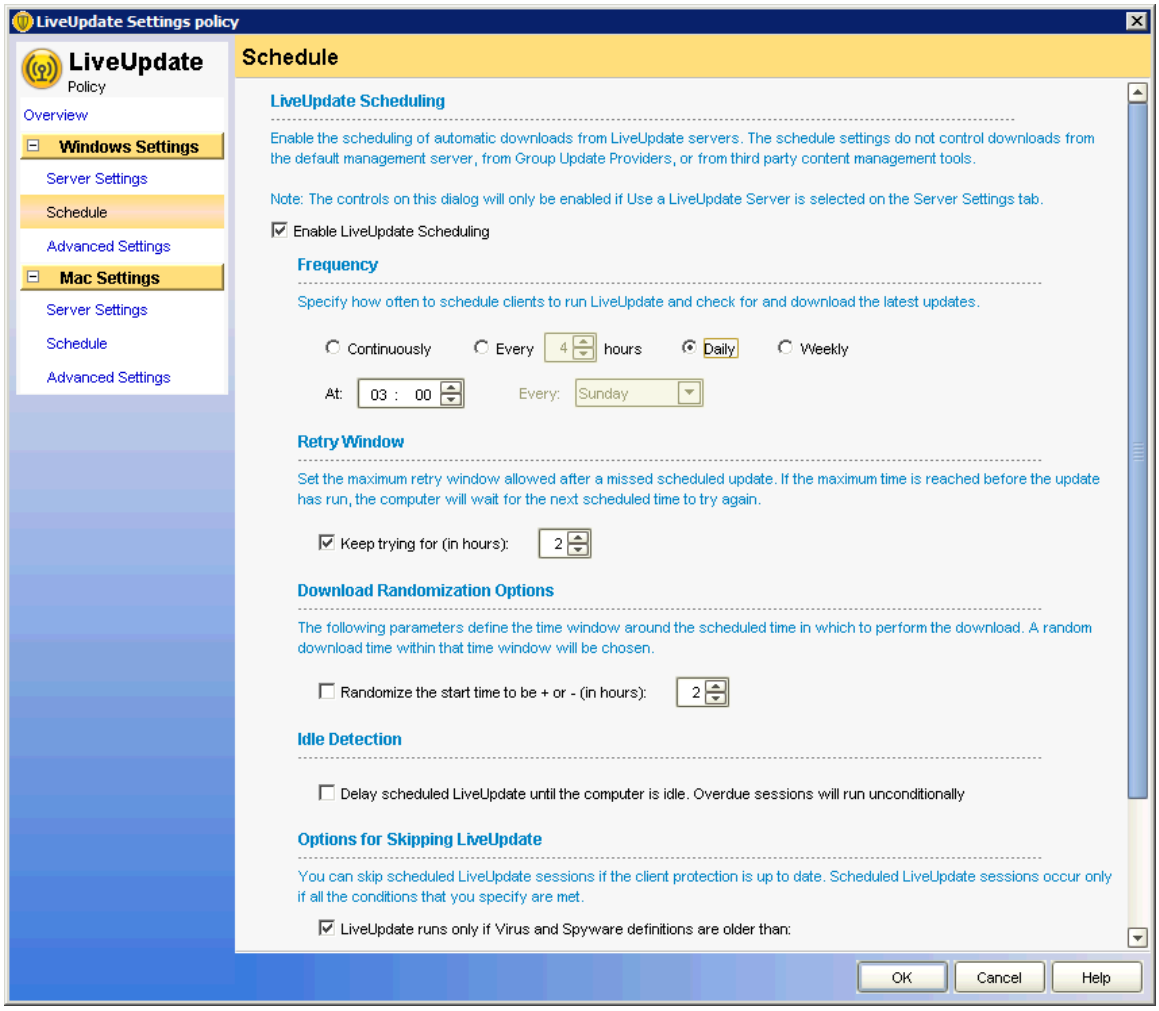
The **LiveUpdate Settings policy** window appears.

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

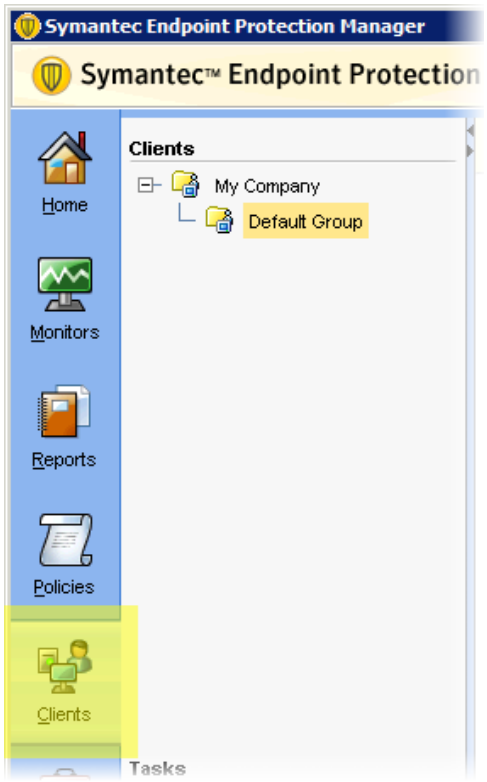


The **Schedule** pane appears on the right side of the window.

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



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

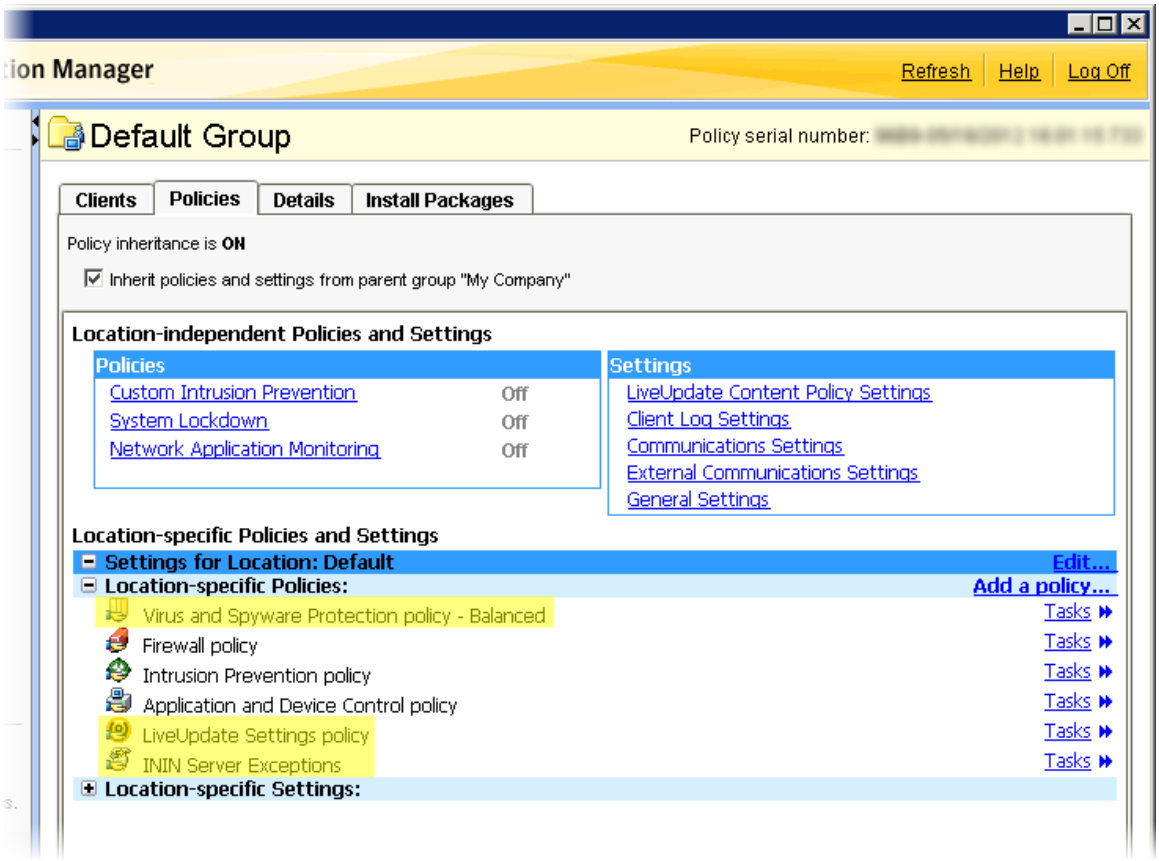


22. In the **Clients** area, select the group to which you have assigned your Interactive Intelligence product servers.

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

23. 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


ion Manager
Refresh
Help
Log Off
Default Group
Policy serial number:
Clients
Policies
Details
Install Packages
Policy inheritance is ON
Inherit policies and settings from parent group "My Company"
Location-independent Policies and Settings
Policies
Custom Intrusion Prevention
Off
System Lockdown
Off
Network Application Monitoring
Off
Settings
LiveUpdate Content Policy Settings
Client Log Settings
Communications Settings
External Communications Settings
General Settings
Location-specific Policies and Settings
Settings for Location: Default
Edit...
Location-specific Policies:
Add a policy...
Virus and Spyware Protection policy - Balanced
Tasks
Firewall policy
Tasks
Intrusion Prevention policy
Tasks
Application and Device Control policy
Tasks
LiveUpdate Settings policy
Tasks
ININ Server Exceptions
Tasks
Location-specific Settings:

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
March 18, 2013	Updated for 12.1.2
April 15, 2013	Added content stating that the reader must verify the paths of excluded files
October 1, 2013	Updated for 12.1.3
September 12, 2014	Added directories and extensions to exclude from scanning.
November 3, 2014	Updated for 12.1.4
January 14, 2016	Updated for 12.1.6