

Symantec Endpoint Protection 12.1.2 for Customer Interaction Center Servers and Subsystems

Technical Reference

Version 4.0

Last Updated: April 15, 2013

Abstract

This document provides the procedures for installing and configuring Symantec Endpoint Protection 12.1.2 for Customer Interaction Center servers, such as Interaction Center, Interaction Media Server, and Interaction SIP Proxy.

Interactive Intelligence 7601 Interactive Way Indianapolis, Indiana 46278 Telephone/Fax: 1(317) 872-3000 www.ININ.com

Copyright and Trademark Information

Interactive Intelligence, Interactive Intelligence Customer Interaction Center, Interaction Administrator, Interaction Attendant, Interaction Client, Interaction Designer, Interaction Tracker, Interaction Recorder, ION, icNotify, Interaction Mobile Office, Interaction Optimizer, Insurance Content Management, and the "Spirograph" logo design are registered trademarks of Interactive Intelligence, Inc. Interaction Center Platform, Interaction Monitor, Customer Interaction Center, EIC, Interaction Fax Viewer, Interaction Server, Interaction Voicemail Player, Interactive Update, Interaction Supervisor, Interaction Migrator, Interaction Melder, and Interaction Screen Recorder are trademarks of Interactive Intelligence, Inc. The foregoing products are ©1997-2013 Interactive Intelligence, Inc. All rights reserved.

Interaction Dialer and *Interaction Scripter* are registered trademarks of Interactive Intelligence, Inc. The foregoing products are ©2000-2013 Interactive Intelligence, Inc. All rights reserved.

Messaging Interaction Center and *MIC* are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2001-2013 Interactive Intelligence, Inc. All rights reserved.

e-FAQ and *Interaction Director* are registered trademarks of Interactive Intelligence, Inc. *e-FAQ Knowledge Manager*, *Interaction FAQ*, and *Interaction Marquee* are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2002-2013 Interactive Intelligence, Inc. All rights reserved.

Interactive Intelligence Live Conference is a trademark of Interactive Intelligence, Inc. The foregoing products are ©2004-2013 Interactive Intelligence, Inc. All rights reserved.

Interaction SIP Proxy and Interaction EasyScripter are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2005-2013 Interactive Intelligence, Inc. All rights reserved.

Interaction Gateway is a registered trademark of Interactive Intelligence, Inc. *Interaction Media Server* is a trademark of Interactive Intelligence, Inc. The foregoing products are ©2006-2013 Interactive Intelligence, Inc. All rights reserved.

Interaction Desktop is a trademark of Interactive Intelligence, Inc. The foregoing products are ©2007-2013 Interactive Intelligence, Inc. All rights reserved.

Interaction Message Indicator, Interaction Feedback, Interaction Process Automation, and Interaction SIP Station are trademarks of Interactive Intelligence, Inc. Deliberately Innovative is a registered trademark of Interactive Intelligence, Inc. The foregoing products are ©2009-2013 Interactive Intelligence, Inc. All rights reserved.

Interaction Web Portal, Interaction Analyzer, IPA, Latitude Software & Design are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2010-2013 Interactive Intelligence, Inc. All rights reserved.

Interaction Edge and *Interaction SIP Bridge* are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2012-2013 Interactive Intelligence, Inc. All rights reserved.

Interaction Media Streaming Server is a trademark of Interactive Intelligence, Inc. The foregoing products are ©2013 Interactive Intelligence, Inc. All rights reserved.

Spotability is a trademark of Interactive Intelligence, Inc. ©2011-2013. All rights reserved.

The veryPDF product is ©2000-2005 veryPDF, Inc. All rights reserved.

This product includes software licensed under the Common Development and Distribution License (6/24/2009). We hereby agree to indemnify the Initial Developer and every Contributor of the software licensed under the Common Development and Distribution License (6/24/2009) for any liability incurred by the Initial Developer or such Contributor as a result of any such terms we offer. The source code for the included software may be found at http://wpflocalization.codeplex.com.

A database is incorporated in this software which is derived from a database licensed from Hexasoft Development Sdn. Bhd. ("HDSB"). All software and technologies used by HDSB are the properties of HDSB or its software suppliers and are protected by Malaysian and international copyright laws. No warranty is provided that the Databases are free of defects, or fit for a particular purpose. HDSB shall not be liable for any damages suffered by the Licensee or any third party resulting from use of the Databases.

Other brand and/or product names referenced in this document are the trademarks or registered trademarks of their respective companies.

DISCLAIMER

INTERACTIVE INTELLIGENCE (INTERACTIVE) HAS NO RESPONSIBILITY UNDER WARRANTY, INDEMNIFICATION OR OTHERWISE, FOR MODIFICATION OR CUSTOMIZATION OF ANY INTERACTIVE SOFTWARE BY INTERACTIVE, CUSTOMER OR ANY THIRD PARTY EVEN IF SUCH CUSTOMIZATION AND/OR MODIFICATION IS DONE USING INTERACTIVE TOOLS, TRAINING OR METHODS DOCUMENTED BY INTERACTIVE.

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

Table of contents

Symantec Endpoint Protection 12.1.2 for Customer Interaction Center Servers and Subsystems	
Copyright and Trademark Information	. 3
Table of contents	. 5
Overview	. 7
Installation	. 8
Configuration	. 9
Change Log	18

Overview

This document provides procedures for installing and configuring Symantec Endpoint Protection 12.1.2 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 12.1.2 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.

🛑 Client Deployment Wi	izard	×
Select Group and	I Install Feature Sets	Symantec.
Install Packages:	Mindows - Symantec Endpoint Protection version 12.1.2015.2015 - English	
	This selection includes: VMI32BIT: Windows - Symantec Endpoint Protection version 12.1.2015.2015 - English (2012-12-17) WIN64BIT: Windows - Symantec Endpoint Protection version 12.1.2015.2015 - English (2012-12-17)	
Group:	My CompanylDefault Group	Browse
Install Feature Sets:	Basic Protection for Servers For servers that require maximum network performance. Only basic protection technologies are installe behavior protection technologies are not installed.	ed. Network, web, or
Install Settings:	Default Client Installation Settings	Options
Content Options:	ⓒ All content (Recommended)	
	This option provides maximum security immediately following client installation. All content is contain the time of deployment.	ed in the package at
	C Basic content This option provides basic protection and creates a smaller client deployment package. Virus definit content are downloaded via LiveUpdate after client installation.	tions and other
Preferred Mode:		
	< Back	Next > Cancel

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 12.1.2 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 12.1.2 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 12.1.2 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.

🖲 Symantec Endpoint Protection Manager		
🔘 Syn	mantec™ Endpoint Protectio	on
Home Monitors Reports	Policies Image: Image	•
Policies		

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.

Exceptions Control Exceptions Control Exception Item Platform Applies To Exception Item Platform Applies To Exception Details Exception Item: Applies To: Action: Exception Item: Applies To: Action: Exception Item: Applies To: Action: Exception Itype:	Exceptions Policy						×
Overview Exceptions Configure exceptions for scans and Tamper Protection, as applicable. Exception Type Clent Restrictions Exception item Platform Applies To Exception Type Action Exception Details Exception tem: Application 4 Exception Details Exception tem: Application 4 Exception Type: Exception Type: Platform 4	属 Exceptions	Ex	ceptions				
Exceptions Configure exceptions for scans and Tamper Protection, as applicable. Clerd Restrictions Exception Item Platform Applies To Exception Type Action Exception Details Exception Details Exception tem: Application 4 Application 4 Application 5 Exception Details Exception type: Exception type: Platform 4 Exception 5 Application 4	,	Policy Excentions					
Clert Restrictions Exception Item Platform Applies To Exception Type Action Image: State of the state		Con	figure exceptions for scans and Tamp	er Protection, as applicable.			
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti		1	Exception Item	Platform	Applies To	Exception Type	Action
Exception Details Windows Exceptions Application Exception tem Application Application Comparison Application Application Comparison Application Appli							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Exception tem Application Application Comparison Application Application Comparison Application Appli							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details Windows Exceptions Application Application Application Application Cxception tem: Action: Exception type: Cxception type: Cxcepti							
Exception Details						Add 🔻 Edit	Delete
Exception item: Application Comparison Compa		Exc	ception Details			Windows Exception	
Applies To: Extensions File Common State S						Mac Exceptions	
Action: Exception type: Trusted Wet							
Exception type: Folder Known Risk							
Trusted Web							



Add Tamper Protection Exception	×
Tamper Protection Exception	
Specify a file that you want to exclude from Tan	per Protection.
Prefix variable:	File (include full path): D:V3VC\ServerV3LRAU.exe
	D. 1510 (Server I)SLIKAU.exe
	OK Cancel Help

- 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.

Add Security Risk Folder Exception	×
Security Risk Folder Exception	
Specify a folder that you want to exclude from security ris	sk scans.
Prefix variable:	Folder:
[NONE]	E:V3VCVLogs
	✓ Include subfolders
Specify the type of scan that excludes this folder:	Specify the type of security risk scan:
Security Risk 💌	All Scans
	OK Cancel Help

- 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.

🝈 Symantec Endpoint Protection Manager			
🔘 Syr	mantec™ Endpoint Protection		
Home Monitors Reports	Policies Virus and Spyware Protection Firewall Intrusion Prevention Application and Device Control LiveUpdate Exceptions Policy Components ▲		
Policies			

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



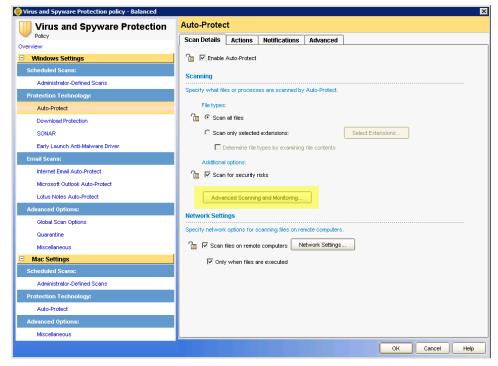
The Virus and Spyware Protection policy window for the selected policy is displayed.

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

🔍 Virus and Spyware Protection policy - Balanced			
Virus and Spyware Protection			
Overview			
Windows Settings			
Scheduled Scans:			
Administrator-Defined Scans			
Protection Technology:			
Auto-Protect			
Download Protection			
SONAR			
Early Launch Anti-Malware Driver			

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.

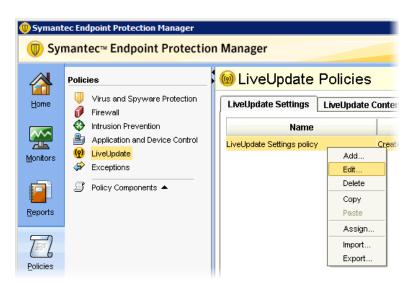
🕖 Adv	anced Scanning and Monitoring
Scar	Files When
Speci	fy activities that trigger automatic scans.
Դ	C Scan when a file is accessed or modified
	Scan when a file is modified
Դ	☑ Scan when a file is backed up
Դ	☑ Do not scan files when trusted processes access the files
Flop	y Settings
Speci	fy options for scanning floppies.
6	Check floppies for boot viruses when accessed
	When a boot virus is found:
	Leave alone (log only)
Othe	r Options
Դ	☑ Delete newly created infected files if the action is 'Leave alone (log only)'
	Delete newly created security risk if the action is 'Leave alone (log only)'
6	Preserve file times
	OK Cancel Help

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

Symantec Endpoint Protection Manager			
Opposite Symantee™ Endpoint Protection Opposite Symantee™ Opposite Symposite Symposite Symposite Symposite Symposite Symposite Symposite Symposite Symposite Opposite Symposite			
Home Monitors Reports	Policies Image: Image		
Policies			

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.

🕖 LiveUpdate Settings pol	icy
阙 LiveUpdate	Schedule
Overview	LiveUpdate Scheduling
Windows Settings	Enable the scheduling of automatic downloads from LiveUpdate servers. The schedule settings do not control downloads from the default management server, from Group Update Providers, or from third party content management tools.
Server Settings	Note: The controls on this dialog will only be enabled if Use a LiveUpdate Server is selected on the Server Settings tab.
Schedule Advanced Settings	I Enable LiveUpdate Scheduling
Mac Settings	Frequency
Server Settings	Specify how often to schedule clients to run LiveUpdate and check for and download the latest updates.
Schedule	C Continuously C Every 4 🖶 hours 💿 Daily C Weekly
Advanced Settings	At: 03 : 00 🖨 Every: Sunday 💌
	Retry Window
	Set the maximum retry window allowed after a missed scheduled update. If the maximum time is reached before the update has run, the computer will wait for the next scheduled time to try again. Image: Reep trying for (in hours): 2 Download Randomization Options 3
	The following parameters define the time window around the scheduled time in which to perform the download. A random download time within that time window will be chosen.
	□ Randomize the start time to be + or - (in hours): 2 ▲
	Idle Detection
	Delay scheduled LiveUpdate until the computer is idle. Overdue sessions will run unconditionally
	Options for Skipping LiveUpdate
	You can skip scheduled LiveUpdate sessions if the client protection is up to date. Scheduled LiveUpdate sessions occur only if all the conditions that you specify are met.
	☑ LiveUpdate runs only if Virus and Spyware definitions are older than:
	OK Cancel Help

- 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.

Symantec Endpoint Protection Manager		
Symantec [™] Endpoint Protection Symantec [™] Endpoint Symantec [™] E		
Home	Clients Clients My Company Company	
Monitors		
Peports		
Policies		
Clients	Tasks	

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

nager	Refresh Help L
Default Group	Policy serial number:
lients Policies Details Install Packages	
licy inheritance is ON	
Inherit policies and settings from parent group "My Company"	1
 Innerit policies and settings from parent group my company 	
ocation-independent Policies and Settings	
Policies	Settings
Custom Intrusion Prevention Off	LiveUpdate Content Policy Settings
System Lockdown Off	Client Log Settings
Network Application Monitoring Off	Communications Settings
	External Communications Settings
	General Settings
ocation-specific Policies and Settings	
Settings for Location: Default	Edi
Location-specific Policies:	Add a polic Task
Winter and Country Destaction policy - Dalamand	<u>105</u>
Virus and Spyware Protection policy - Balanced	Tod
🥑 Firewall policy	<u>Tas</u> Tad
 Firewall policy Intrusion Prevention policy 	Tasi
 Firewall policy Intrusion Prevention policy Application and Device Control policy 	Tasi Tasi
 Firewall policy Intrusion Prevention policy 	Task

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