

Symantec Endpoint Protection 12.1.3 for Customer Interaction Center Servers and Subsystems

Technical Reference

Interactive Intelligence Customer Interaction Center® (CIC)

Version 2015

Last updated September 12, 2014

(See Change Log for summary of changes.)

Abstract

This document provides the procedures for installing and configuring Symantec Endpoint Protection 12.1.3 for Customer Interaction Center servers, such as a Customer Interaction Center server, Interaction Media Server, and Interaction SIP Proxy.

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, and the "Spirograph" logo design are registered trademarks of Interactive Intelligence, Inc. Interactive Intelligence Group, Inc., Interaction Center Platform, Interaction Monitor, Customer Interaction Center, EIC, Interaction Fax Viewer, Interaction Server, Interaction Voicemail Player, Interactive Update, Interaction Supervisor, Interaction Migrator, and Interaction Screen Recorder are trademarks of Interactive Intelligence, Inc. The foregoing products are ©1997-2014 Interactive Intelligence, Inc. All rights reserved.

Interaction Dialer and Interaction Scripter are registered trademarks of Interactive Intelligence, Inc. The foregoing products are ©2000-2014 Interactive Intelligence, Inc. All rights reserved.

Messaging Interaction Center and MIC are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2001-2014 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 ©2002-2014 Interactive Intelligence, Inc. All rights reserved.

Interaction Conference is a trademark of Interactive Intelligence, Inc. The foregoing products are ©2004-2014 Interactive Intelligence, Inc. All rights reserved.

Interaction SIP Proxy and Interaction EasyScripter are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2005-2014 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 ©2006-2014 Interactive Intelligence, Inc. All rights reserved.

Interaction Desktop is a trademark of Interactive Intelligence, Inc. The foregoing products are ©2007-2014 Interactive Intelligence, Inc. All rights reserved.

Interaction Process Automation is a trademark of Interactive Intelligence, Inc. Deliberately Innovative, Interaction Feedback, and Interaction SIP Station are registered trademarks of Interactive Intelligence, Inc. The foregoing products are ©2009-2014 Interactive Intelligence, Inc. All rights reserved.

Interaction Web Portal, Interaction Analyzer, and IPA are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2010-2014 Interactive Intelligence, Inc. All rights reserved.

Spotability is a trademark of Interactive Intelligence, Inc. ©2011-2014. All rights reserved.

Interaction Edge and Interaction Mobilizer are registered trademarks of Interactive Intelligence, Inc. Interaction SIP Bridge, Interactive Intelligence MarketplaceSM, Interactive Intelligence Communications as a ServiceSM, CaaS Quick SpinTM, and Interactive Intelligence CaaSSM are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2012-2014 Interactive Intelligence, Inc. All rights reserved.

Bay Bridge Decisions, Interaction Script Builder, and Interaction Speech Recognition are trademarks of Interactive Intelligence, Inc. The foregoing products are ©2013-2014 Interactive Intelligence, Inc. All rights reserved.

Interaction Collector, Interaction Decisions, Interactive Intelligence PureMatch, and Interactive Intelligence PureCloud are trademarks of Interactive Intelligence, Inc. PureCloudSM is a service mark of Interactive Intelligence, Inc. The foregoing products are ©2013-2014 Interactive Intelligence, Inc. ©2014. All rights reserved.

The *veryPDF* product is ©2000-2014 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

Overview	5
Installation	6
Configuration	9
Change Log	22

Overview

This document provides procedures for installing and configuring Symantec Endpoint Protection 12.1.3 on Interactive Intelligence product servers in your Customer Interaction Center environment.

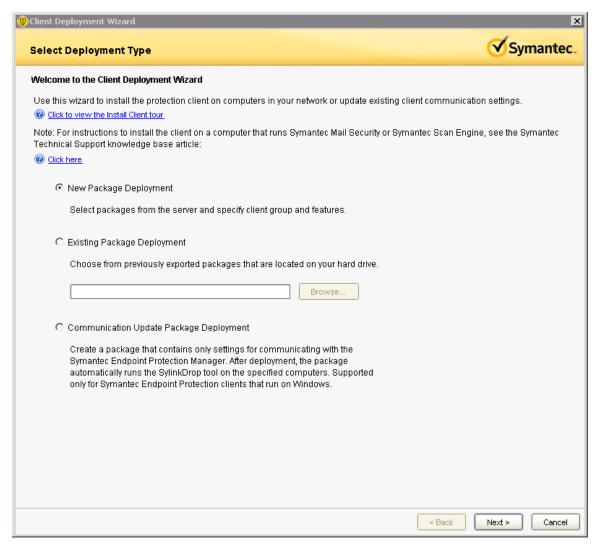
Installation

This topic contains the specific selections that you must choose when deploying Symantec Endpoint Protection 12.1.3 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.

🔘 Symanl	ec Endpoint Protection Manager		
🔘 Syr	mantec™ Endpoint Protectio	Manager	Refresh Help Log Off
And the second s	Clients Clients My Company	Cients Policies Details Install Packages	
Monitors		View: Default view All users and computers Name Health State Logon User or Computer Last Time Status Changed Virus Det	Filter
Reports			
Policies			
Clients			
<u>A</u> dmin	Add a client Add computer account Add user account Import Active Directory or LDAP I. Import Active Directory or LDAP I. <td< th=""><th></th><th>•</th></td<>		•

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.

💮 Client Deployment Wi	izard	×
Select Group and	I Install Feature Sets	Symantec.
Install Packages:	Windows - Symantec Endpoint Protection version 12.1. - English This selection includes: - English WIN32BIT: Windows - Symantec Endpoint Protection version 12.1. - English WIN64BIT: Windows - Symantec Endpoint Protection version 12.1. - English	T
Group:	My Company\Default 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:	 C All content (Recommended) This option provides maximum security immediately following client installation. All content is contain the time of deployment. 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. 	
Preferred Mode:	C Computer mode C User mode	
	< Back	Next > Cancel

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 12.1.3 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 12.1.3 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 12.1.3 on an Interactive Intelligence product server, do the following steps:

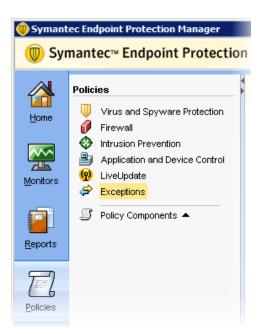
- 1. From the Start menu, select All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools.
- 2. In the left pane of the Symantec Endpoint Protection Manager window, select the Policies object.



Important!

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

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



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

Policies	
Clients	Image: Constraint of the second se

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

The **Exceptions Policy** window appears.

- 12. 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.

Exceptions Policy					×
Exceptions Policy	Exceptions				
	Exceptions				
Overview	Configure exceptions for scans and Tamper I	Protection as applicable			
Exceptions	comigure exceptions for scans and ramper	riotection, as applicable.		1	
Client Restrictions	Exception Item	Platform	Applies To	Exception Type	Action
				Add 🕶 Edit	Delete
	Exception Details			Windows Exceptions	 Application
				Mac Exceptions	 Application to N
	Exception item:				Extensions
	Applies To:				File Folder
	Action:				Known Risks
	Exception type:				Trusted Web D
					Tamper Protect
				OK Canc	el DNS or Host Fi

The Add Tamper Protection Exception dialog box appears.

amper Protection Exceptio	n	
pecify a file that you want to ex	clude from Tan	nper Protection.
Prefix variable:		File (include full path):
		D:N3NC\ServerN3LRAU.exe

- 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.

13. 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)

- \${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.

Add Security Risk Folder Exception		×
Security Risk Folder Exception		
Specify a folder that you want to exclude from security i	risk scans.	
Prefix variable:	Folder:	
	E:V3VC/Logs	
Specify the type of scan that excludes this folder: Security Risk	Specify the type of security risk scan: 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.
- 14. 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

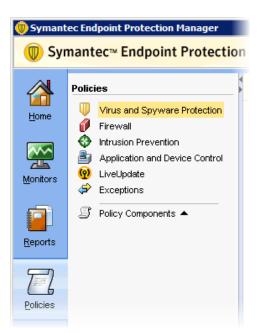
- .ivp
- .dxs
- .ihd
- .i3pub
- .xml
- .inin.db
- .ininlog (CIC log file format)
- .ininlog.ininlog_idx (CIC log index file format)

c. Select the **Add** button.

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

Add Security Risk Extension Exceptions	×
Security Risk Extension Exceptions	
Specify file extensions that you want to exclude from security risk scans.	
ininlog_idx ininlog i3pub ihd dxs ivp i3c i3p ent	
Add Specify the type of security risk scan: All Scans	

- d. Repeat this series of steps for each file extension in the list.
- 15. Ensure that the **All Scans** list item is displayed in the **Specify the type of security risk scan** box.
- 16. 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.
- 17. In the **Symantec Endpoint Protection Manager** window, select the **Virus and Spyware Protection** object.



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

🛞 Symant	ec Endpoint Protection Manager				
🔘 Syr	mantec™ Endpoint Protect	io	n Manager		
	Policies	_	🛡 Virus and Spyware F	Protectio	on Policies
<u>H</u> ome	 Virus and Spyware Protection Firewall 		Name		
Monitors	 Intrusion Prevention Application and Device Control LiveUpdate Exceptions 		Virus and Spyware Protection policy - Ba Virus and Spyware Protection policy - Hig Virus and Spyware Protection policy - Hig	Add Edit Delete Copy	Recommended p High security pol Higher performar
Reports	Policy Components		-	Paste Assign Import Export	
Policies					

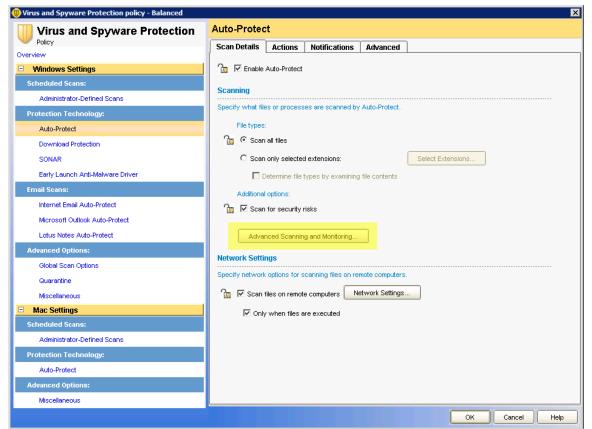
The Virus and Spyware Protection policy window for the selected policy appears.

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



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

20. 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.

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

Advanced Scanning and Monitoring
Scan Files When
Specify activities that trigger automatic scans.
🚡 🔿 Scan when a file is accessed or modified
🚡 🗹 Scan when a file is backed up
Model in the second
Floppy Settings
Specify options for scanning floppies.
🌆 🔽 Check floppies for boot viruses when accessed
When a boot virus is found:
Leave alone (log only)
Other Options
☐ 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)'
🚡 🗹 Preserve file times
OK Cancel Help

- 22. Select the \mathbf{OK} button.
- 23. In the **Symantec Endpoint Protection Manager** window, select the **LiveUpdate** object.



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

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

🔘 Symant	ec Endpoint Protection Manager		
🔘 Syr	nantec™ Endpoint Protection	n Manager	
	Policies	liveUpdate P @	olicies
Home	Virus and Spyware Protection Firewall	LiveUpdate Settings	iveUpdate Conter
	Intrusion Prevention	Name	
	Application and Device Control	LiveUpdate Settings policy	Create
<u>M</u> onitors	LiveUpdate		Add
	🖨 Exceptions		Edit
	Policy Components		Delete
	<u> </u>		Сору
<u>R</u> eports			Paste
			Assign
\Box			Import
6			Export
Policies			

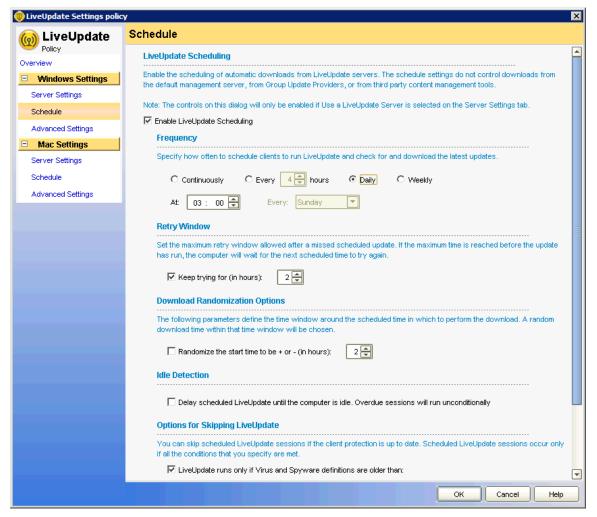
The LiveUpdate Settings policy window appears.

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



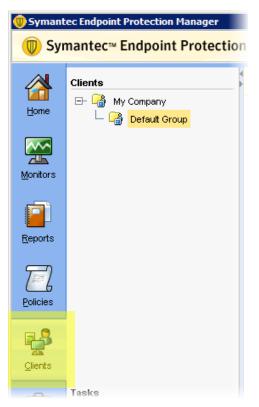
The **Schedule** pane appears on the right side of the window.

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



27. When you have finished configuring the update schedule, select the **OK** button.

28. In the left pane of the Symantec Endpoint Protection Manager window, select the Clients object.



29. 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.

- 30. 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

anager		Refresh Help	<u>L</u> (
aDefault Group		Policy serial number:	
Clients Policies Details Install Pac	kages		
Policy inheritance is ON			
✓ Inherit policies and settings from parent group	"My Company"		
	my company		
Location-independent Policies and Setti	ngs		
Policies		Settings	
Custom Intrusion Prevention	Off	LiveUpdate Content Policy Settings	
System Lockdown	Off	<u>Client Log Settings</u>	
Network Application Monitoring	Off	Communications Settings	
		External Communications Settings	
		<u>General Settings</u>	
Location-specific Policies and Settings			n de
 Settings for Location: Default Location-specific Policies: 		Add a p	Edi olicy
Virus and Spyware Protection policy	- Balanced		Task
	Calaricool		Task
		-	Task
Application and Device Control policy			Task
 Application and Device Control policy LiveUpdate Settings policy 			Task
			Task
ININ Server Exceptions			

Change Log

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.

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