## Third Party Security and Backup Application Guidelines

### Third Party

Release:	Cross-Release
	NICE Engage Platform
	NICE Interaction Management 4.1
	NICE Perform 3.2/3.5
Document Revision:	В0
Distribution Status:	Published
Publication Date:	November 2014



Information in this document is subject to change without notice and does not represent a commitment on the part of NICE Systems Ltd. The systems described in this document are furnished under a license agreement or nondisclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of NICE Systems Ltd. and protected by United States and international copyright laws.

Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of NICE Systems Ltd., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

#### All contents of this document are: Copyright © 2014 NICE Systems Ltd. All rights reserved.

This product is protected by one or more of the US patents listed at www.nice.com/Patents

The full list of NICE marks are the trademarks or registered trademarks of Nice Systems Ltd. For the full list of NICE trademarks, visit <u>www.nice.com/Nice-Trademarks</u>. All other marks used are the property of their respective proprietors.

For assistance, contact your local supplier or nearest NICE Systems Customer Service Center:

#### EMEA Region (Europe, Middle East, Africa) Tel: +972-9-775-3800 Fax: +972-9-775-3000 email: support@nice.com

The Americas Region (North, Central, South America) Tel: 1-800-6423-611 Fax: +720-264-4012

email: support.americas@nice.com

#### International Headquarters-Israel

Tel: +972-9-775-3100 Fax: +972-9-775-3070 email: info@nice.com

#### North America

Tel: 1-800-663-5601 Fax: +201-356-2197 email: na\_sales@nice.com

France Tel: +33-(0)1-41-38-5000 Fax: +33-(0)1-41-38-5001

#### APAC Region (Asia/Pacific)

Tel: +852-8338-9818 Fax: +852-2802-1800 email: support.apac@nice.com

#### Israel

Tel: 09-775-3333 Fax: 09-775-3000 email: support@nice.com

#### **United Kingdom**

Tel: +44-8707-22-4000 Fax: +44-8707-22-4500

#### Germany

Tel: +49-(0)-69-97177-0 Fax: +49-(0)-69-97177-200

#### Hong-Kong

Tel: +852-2598-3838 Fax: +852-2802-1800

NICE invites you to join the NICE User Group (NUG).

Visit the NUG Website at <u>www.niceusergroup.org</u> and follow the instructions.

All queries, comments, and suggestions are welcome! Please email: nicebooks@nice.com

For more information about NICE, visit www.nice.com

## CONTENTS

1: About This Guide	5
Document Revision History	6
2: Antivirus Software Configuration	11
Overview	
Antivirus Real Time Scan	13
Daily Scan	14
Weekly Scan	15
Folders and Files Exclusion	
Disabling Firewalls	24
Using McAfee VirusScan Enterprise 8.8	25
Disabling Buffer Overflow Protection	25
Disabling Heuristic Scanning	
Excluding Folders	
Configuring an Update Task	
Using Symantec Endpoint Protection	
Disable Heuristic Scanning	
Configure SONAR	33
Configure LiveUpdate	33
Using Trend Micro OfficeScan	
Configuring Scheduled Updating of the OfficeScan Server	
Configuring Automatic Update	
Allowing Required Email Messages	
Live Updates	
CPU Priority	
Additional Configurations	41
Additional Recommendations	

43

### 3: SQL Backup

SQL Backup Guidelines	44
Overview	44
Schedule	44
Backup Files Location	44
Implementation Guidelines	45
Backup Tools	45
Database Configuration Guidelines	

# 1

### **About This Guide**

This guide details general application configuration guidelines for various security and backup activities. Applying these guidelines ensures that your site's specific configurations comply with those required by the NICE Engage Platform/NICE Interaction Management/NICE Perform environment.

You must adhere to these guidelines when deploying third party application on servers running NICE applications. Following these guidelines minimizes the risk of the third party applications interfering with the NICE System operation.

You can deploy the security and backup policies on servers running NICE applications following these guidelines without the need to contact NICE for additional certification of the third party software applications.

#### Important!

These guidelines are designed to best suit NICE System performance only, and should not be considered general security and backup recommendations.

The guidelines included in the guide are divided into the following topics:

#### Contents

Document Revision History	 6
Boournerreviererrierer	 ~

### **Document Revision History**

Revision	Modification Date	Software Version	Description
A3	September 2011		<ul> <li>Added Security Permissions section for NICE Interaction Management Release 4.x</li> </ul>
A4	November 2011		<ul> <li>Removed the following sections from Security Permissions section for NICE Interaction Management Release 4.x:</li> <li>Unified Environment/SMB</li> <li>Semi-Distributed Environment</li> <li>New Semi-Distributed Environment</li> <li>Added:         <ul> <li>ITI Connect Server on page 87</li> <li>Updated table:                 <ul> <li>Service Settings: NICE Services on</li> </ul> </li> </ul> </li> </ul>
			page 75
A5	August 2012		<ul> <li>Added:</li> <li>NICE Interactions Center on page 88</li> <li>NICE Sentinel on page 90</li> <li>NICE Media Interconnect on page 92</li> <li>Configuring SQL Server Permissions on page 106</li> <li>Using Secure Communication and Media Engeneration support 117</li> </ul>

Revision	Modification Date	Software Version	Description
A6	November 2012		Updated:
			Folders and Files Exclusion on page 16
			Semi-Distributed Environment on page 25
			Distributed Environment on page 37
			User Accounts for NICE Services on page 70
			General Limitations on page 71
			Required Permissions per Server Type on page 77
			Using Secure Communication and Media Encryption on page 117

RevisionModificationSoftwareDescriptionDateVersion	
A7 January 2013 Removed the foldor Security Perm Release 3.x This section of Microsoft Win (for NICE Perm Interaction M This section of Microsoft Win (for NICE Inter Release 4.1) List of User R This section of Security Perm the following security Perm the follo	owing sections from this guide: missions for NICE Perform can now be found in the indows Authentication Guide aform Releases 3.2 & 3.5 ) missions for NICE lanagement Release 4.1 can now be found in the indows Authentication Guide eraction Management Rights can now be found within the missions sections in both of guides: if Windows Authentication for NICE Perform Releases ) if Windows Authentication for NICE Interaction

Revision	Modification Date	Software Version	Description
A8	July 2013		Updated Folders and Files Exclusion on page 16 to include information about cluster environments
			Added the following sections with details for configuring the three antivirus software products most commonly used in NICE Interaction Management systems:
			Using McAfee VirusScan Enterprise 8.8 on page 25
			Using Symantec Endpoint Protection on page 32
			Using Trend Micro OfficeScan on page 36
			Added Allowing Required Email Messages on page 38
A9	September 2014	N/A	Added Disabling Firewalls on page 24 to include NICE Systems recommendations about firewalls.
			Updated Excluded Files and Folders for NICE Interaction Management 4.x. on page 17 to include information about new NICE servers and components and updated NICE Interaction Management path for Windows Server 2003 servers.
			Added Configure SONAR on page 33
В0	November 2014	N/A	<ul> <li>Updated Folders and Files Exclusion on page 16 to include information about new NICE servers and components and updated NICE Engage Platform path for Windows Server 2003 servers.</li> </ul>

[This page intentionally left blank]

# 2

### **Antivirus Software Configuration**

This section includes guidelines for configuring antivirus software running on NICE Engage Platform/NICE Interaction Management/NICE Perform servers. These guidelines are designed to allow better performance and operation of the NICE system and generally apply to any antivirus software.

Customers, business partners, and NICE engineers should use these guidelines for configuring or verifying the configuration of antivirus software.

**NOTE**: These guidelines are provided for NICEserver performance. Customers should make their own risk analysis while implementing these guidelines.

#### Contents

Overview	12
Antivirus Real Time Scan	13
Daily Scan	14
Weekly Scan	15
Folders and Files Exclusion	16
Disabling Firewalls	24
Using McAfee VirusScan Enterprise 8.8	25
Using Symantec Endpoint Protection	
Using Trend Micro OfficeScan	
Allowing Required Email Messages	
Live Updates	
CPU Priority	40
Additional Configurations	41
Additional Recommendations	42

### Overview

NICE Systems supports two approaches for antivirus software certification: proactive certification or by using the guidelines in this section.

As part of the proactive approach NICE Systems has certified specific antivirus software applications according to NICE third party software certification policy. For a complete compatibility list, see the *Third Party Technical Guidelines*.

Alternatively, you can use the guidelines in this section and use any antivirus software application. These guidelines are general and designed to ensure the performance of NICE Systems.

### **Antivirus Real Time Scan**

The antivirus scan is a resource consuming action, and should therefore not be enabled during working hours. If Real Time Scan is enabled during working hours, it may cause performance issues and interfere with standard system operations.

### **Daily Scan**

Daily scans should be performed during non-working hours. The folders which appear in the *Folders and Files Exclusion* should not be scanned.

### Weekly Scan

Weekly scans should be performed during weekends when the system is idle. Idle time is dependent upon Storage Center and Interactions Analytics load. The folders which appear in the *Folders and Files Exclusion* can be scanned.

### **Folders and Files Exclusion**

The following tables contain a list of all the files that should be excluded from the scheduled scan (Read & Write). These folders and files should be excluded from the antivirus scan, since they are used during NICE operations.

1	Im	portant!
=	Se Re	e tables per NICE Engage Platform/NICE Interaction Management/NICE Perform lease:
		Excluded Files and Folders for NICE Perform 3.x below
	•	Excluded Files and Folders for NICE Interaction Management 4.x. on the facing page
	_	

- Excluded Files and Folders for NICE Engage Platform on page 19
- All the paths in the table below are the default installation paths. If you used a different path in your installation, you must use the same path for the excluded files.

NICE Server	Default Path	Files
CTI / VRSP	D:\Program files\NICE Systems\CTI	
Database	E:\Program Files\Microsoft SQL server\MSSQL10.x\MSSQL\DATA	MDF files
	F:\Program Files\Microsoft SQL Server\MSSQL10.x\MSSQL\DATA	LDF files
Data Mart	E:\Program Files\Microsoft SQL Server\MSSQL10.x\MSSQL\DATA	MDF files
	F:\Program Files\Microsoft SQL Server\MSSQL10.x\MSSQL\DATA	LDF files
Interactions Center	D:\Program Files\NICE Systems\Interactions Center\Bin	
	D:\Program Files\NICE Systems\Interactions Center\Data	
	D:\Program Files\NICE Systems\Interactions Center\Log	

Excluded Files and Folders for NICE Perform 3.x

NICE Server	Default Path	Files
Nice Screen Logger	D:\MMLStorage	DAT files
	D:\Program Files\Nice Systems\Multimedia Logger\Datasystem	TBL files
NICE Sentinel	D:\Program Files\Microsoft SQL	MDF files
	Server\MSSQL.1\MSSQL\Data	LDF files
Speech to Text and Words	D:\Program Files\NICE Systems\Nice Content	WAV files
Search Pack	Analysis Server\MediaCache	WAV1 files
		WAV2 files
		WAV3 files
	D:\Storage Area for a Content Analysis\Index	INX files
		INX2 files
Storage Center	D:\SC_Archive_Directory	NMF files
NICELog Voice Logger / VoIP Logger	D:\Ntlogger	
	The unformatted partition	

#### Excluded Files and Folders for NICE Interaction Management 4.x.

NICE Server		Default Path	Files
Advanced Interaction Recorder			
=	Package and binaries folder	D:\Program Files\NICE systems\	
=	Log files folder	D:\Program Files\NICE systems\	
	Metadata management folder	D:\Program Files\NICE systems\	
=	Recording Folders (partitions)	User defined path in SRT: <recording directory=""></recording>	*.nmf

NICE Server	Default Path	Files
Archiving Folders	User defined path in SRT: <archiving directory=""></archiving>	*.nmf
CTI / VRSP	D:\Program files\NICE Systems\CTI	
Database	E:\ <sql data="" files=""></sql>	MDF files
	F:\ <sql files="" log=""></sql>	LDF files
Data Mart	E:\ <sql data="" files=""></sql>	MDF files
	F:\ <sql files="" log=""></sql>	LDF files
Interactions Center	D:\Program Files\NICE Systems\Interactions Center\Bin	
	D:\Program Files\NICE Systems\Interactions Center\Data	
	D:\Program Files\NICE Systems\Interactions Center\Log	
Nice Screen Logger	E:\MMLStorage	DAT files
	D:\Program Files\Nice Systems\Multimedia Logger\Datasystem	TBL files
NICE Sentinel	D:\ <sql data="" files=""></sql>	MDF files
	D:\ <sql files="" log=""></sql>	LDF files
Speech-to-Text Pack	D:\ <storage area=""></storage>	
	D:\Program Files\NICE Systems\Nice Content AnalysisServer	
	D:\Storage Area for a Content Analysis\Index	
Storage Center	E:\ <sc_archive_directory></sc_archive_directory>	NMF files
Text Analysis Pack	E:\ <workarea></workarea>	

NICE Server	Default Path	Files
NICELog Voice Logger / VoIP Logger	Windows Server 2008: C:\ProgramData\NICE Systems\IPCapture C:\ProgramData\NICE Systems\Logger The raw partition	Log files
	C:\Documents and Settings\All Users\Application Data\Nice C:\Documents and Settings\All Users\Application Data\NICE Systems The unformatted partition All operating systems: D:\Ntlogger	Log files
Windows Media Server	D:\ <publishing_point_directory></publishing_point_directory>	
Word Search Pack	D:\Program Files\NICE Systems\Nice Content AnalysisServer\MediaCache E:\ <workarea></workarea>	

#### Excluded Files and Folders for NICE Engage Platform

NICE Server	Default Path	Files
Advanced Interaction Recorder		
Package and binaries folder	D:\Program Files\NICE systems\	

NICE Server	Default Path	Files
Log files folder	%NiceLogLocation%         System Properties         Image: Advanced Reader         Image: Advanced Reader	
Metadata Management folder	D:\Program Files\NICE systems\	*.s3db*
Recording Folders (partitions)	User defined path in SRT: <recording directory=""></recording>	*.nmf
Archiving Folders	User defined path in SRT: <archiving directory=""></archiving>	*.nmf
CTI / VRSP	D:\Program files\NICE Systems\CTI	
Database	E:\ <sql data="" files=""></sql>	MDF files
	F:\ <sql files="" log=""></sql>	LDF files
Data Mart	E:\ <sql data="" files=""></sql>	MDF files
	F:\ <sql files="" log=""></sql>	LDF files

NICE Server	Default Path	Files
Interactions Center	D:\Program Files\NICE Systems\Interactions Center\Bin	
	D:\Program Files\NICE Systems\Interactions Center\Data	
	D:\Program Files\NICE Systems\Interactions Center\Log	
Nice Screen Logger	E:\MMLStorage	DAT files
	D:\Program Files\Nice Systems\Multimedia Logger\Datasystem	TBL files
NICE Sentinel	D:\ <sql data="" files=""></sql>	MDF files
	D:\ <sql files="" log=""></sql>	LDF files
Real Time Authentication		
Enrollment Engine	D:\Program files\NICE Systems\	*.nmf
Authentication Engine	D:\Program files\NICE Systems	*.nmf
	C:\windows\system32\MSMQ	* *
<ul> <li>Authentication &amp; Fraud Engine (Nuance) audio folder</li> </ul>	User defined path in plugin <fraudsters audio="" file<br="">path&gt;</fraudsters>	*.nmf
Real Time Insight Manager	C:\windows\system32\MSMQ	* *
Insight-to-Impact Connect	Desktop Tagging persistency folder: D:\Program files\NICE Systems\RTI Connect\Bin \RealTimeModeBackUps	*.bkp
	DB Writer handler persistency folder:	*.bkp
	D\Program files\NICE Systems\RTI Connect\Bin\ PersistentDBWriterDatabase	*.fsd_alive *.fsd_dead *.fsd_temp

NICE Server	Default Path	Files
Speech to Text Engine	D:\ <storage area=""> D:\Program Files\NICE Systems\Nice Content AnalysisServer D:\Storage Area for a Content Analysis\Index</storage>	
Standard Word Search Server	D:\Program Files\NICE Systems\Nice Content AnalysisServer\MediaCache E:\ <workarea></workarea>	
Storage Center	E:\ <sc_archive_directory></sc_archive_directory>	NMF files
Stream Server with Windows Media Services	D:\ <publishing_point_directory></publishing_point_directory>	
Text Analysis Engine	E:\ <workarea></workarea>	
Text Mining Engine	E:\ <workarea></workarea>	
NICELog Voice Logger / VoIP Logger	Windows Server 2008: C:\ProgramData\NICE Systems\IPCapture C:\ProgramData\NICE Systems\Logger The raw partition	Log files
	C:\Documents and Settings\All Users\Application Data\Nice C:\Documents and Settings\All Users\Application Data\NICE Systems The unformatted partition All operating systems:	Log files
	D:\Ntlogger	

In addition, when any of the NICE servers is configured as a clustered component using Microsoft Failover Cluster (MSCS), cluster-aware antivirus software must be used, and all files in the following folders should be excluded from virus scanning on such servers:

- The path of the \mscs folder on the quorum drive, for example, the Q:\mscs folder.
- The %Systemroot%\Cluster folder.
- The temp folder for the Cluster Service account, for example, the \clusterserviceaccount\Local Settings\Temp folder (only with operating systems preceding Microsoft Windows Server 2008).

More information can be found at http://support.microsoft.com/kb/250355.

### **Disabling Firewalls**

All antivirus software have integrated firewalls and are installed by default on the systems. Default firewall settings can cause network issues and negatively impact the functioning of NICE's software.



The default setting for all integrated antivirus firewall software should be changed from Enabled to Disabled. See the relevant documentation for this information.

### Using McAfee VirusScan Enterprise 8.8

If you are using McAfee VirusScan Enterprise 8.8, perform the procedures described in this section to do the following:

- Disable buffer overflow protection.
- Disable heuristic scanning.
- Exclude folders from virus scanning.
- Configure an update task.

### **Disabling Buffer Overflow Protection**

Buffer overflow protection is a resource-consuming feature and should therefore be disabled for all NICE servers.

#### To disable buffer overflow protection in McAfee VirusScan Enterprise 8.8:

- 1. Log on to ePolicy Orchestrator.
- 2. Click Menu > System > System Tree.
- 3. In the System Tree pane, under My Organization, select your group.
- 4. Click the **Assigned Policies** tab.
- 5. In the Product drop-down list, select VirusScanEnterprise 8.8.0.

Figure 2-1: Assigned Policies for VirusScanEnterprise 8.8.0

System Tree	Systems Assigned Policies As	signed Client Tasks	Group Details	
▼ My Organization				
Sales	Product: VirusScan Enterprise 8.8.0  Finforcement status: Enforcing			
NewS	Category	Policy	Server	Inherit from
Lost&Found	On-Access General Policies	My Default	Local (NICEVM-3147)	My Organization
	On-Access Default Processes Policies	My Default	Local (NICEVM-3147)	My Organization
	On-Access Low-Risk Processes Polici	My Default	Local (NICEVM-3147)	My Organization
	On-Access High-Risk Processes Polic	My Default	Local (NICEVM-3147)	My Organization
	On Delivery Email Scan Policies	My Default	Local (NICEVM-3147)	My Organization
	General Options Policies	My Default	Local (NICEVM-3147)	My Organization
	Alert Policies	My Default	Local (NICEVM-3147)	My Organization
	Access Protection Policies	My Default	Local (NICEVM-3147)	My Organization
	Buffer Overflow Protection Policies	My Default	Local (NICEVM-3147)	My Organization
	Unwanted Programs Policies	My Default	Local (NICEVM-3147)	My Organization
:	Quarantine Manager Policies	My Default	Local (NICEVM-3147)	My Organization

- 6. In the Category column, find Buffer Overflow Protection Policies and then click My Default in the Policy column next to it.
- 7. In the Settings for drop-down list, select Server.

#### Figure 2-2: Settings for Server

VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default		
Settings for: Server		
Buffer Overflow Protection Repor	ts	
Prevent exploited buffer overflows from executing arbitrary code on your computer.		
Buffer overflow settings:	Enable buffer overflow protection     Warning mode     Protection mode	
Client system warning:	₩ Show the messages dialog box when a buffer overflow is detected	

- 8. In the Buffer overflow settings section, clear the Enable buffer overflow protection checkbox.
- 9. In the **Settings for** drop-down list, select **Workstation**.

Figure 2-3: Settings for Workstation

VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default		
Settings for: Workstation 💌		
Buffer Overflow Protection Reports		
Prevent exploited buffer overflows from executing arbitrary code on your computer.		
Buffer overflow settings:	Enable buffer overflow protection     Warning mode     Protection mode	
Client system warning:	Show the messages dialog box when a buffer overflow is detected	

- 10. In the Buffer overflow settings section, clear the Enable buffer overflow protection checkbox.
- 11. Click Save.

### **Disabling Heuristic Scanning**

Heuristic scanning can be disabled if it impairs performance.

To disable heuristic scanning in McAfee VirusScan Enterprise 8.8:

- 1. Log on to ePolicy Orchestrator.
- 2. Click Menu > System > System Tree.
- 3. In the System Tree pane, under My Organization, select your group.
- 4. Click the Assigned Client Tasks tab and then click Actions.
- 5. In the drop-down menu, click New Client Task Assignment.
- 6. In the **Product** drop-down list, select **VirusScan Enterprise 8.8.0**.
- 7. In the Task type field, select On Demand Scan.

- 8. Create a new task, and in **Task Name** type an appropriate name for it.
- 9. Click the **Scan Items** tab.

#### Figure 2-4: Scan Item Tab

Client Task Catalog : Edit Task - Virus Scan Enterprise 8.8.0: On Demand Scan		
Task Name	Heuristic Scanning	
Description	× *	
Scan Locations Scan Items Exe	clusions Actions Performance Reports Task	
Specify what items to scan.		
File types to scan:	<ul> <li>All files</li> <li>Default + additional file types</li> <li>Also scan for macros in all files</li> <li>Specified file types only</li> </ul>	
Options:	<ul> <li>✓ Detect unwanted programs</li> <li>□ Decode MIME encoded files</li> <li>✓ Scan inside archives (e.gZIP)</li> <li>□ Scan files that have been migrated to storage</li> </ul>	
Heuristics:	<ul> <li>Find unknown program threats</li> <li>Find unknown macro threats</li> </ul>	

- 10. In the **Heuristics** section, clear the **Find unknown program threats** and **Find unknown macro threats** checkboxes.
- 11. Click the **Performance** tab.

#### Figure 2-5: Performance Tab

Client Task Catalog : New Task - VirusScan Enterprise 8.8.0: On Demand Scan		
Task Name	Heuristic Scanning	
Description		
Scan Locations Scan Items E	clusions Actions Performance Reports Task	
Specify performance options for the scan.		
When to defer:	<ul> <li>Defer scan when using battery power.</li> <li>Defer scan during presentations.</li> <li>User may defer scheduled scans.</li> </ul>	
How long to defer:	Defer at most 1 hours (0=forever)	
System utilization:	Below Normal 💌	
Artemis (Heuristic network check for suspicious files):	Sensitivity level: Disabled 💌	

- 12. In the Artemis (Heuristic network check for suspicious files) section, in the Sensitivity level dropdown list, select Disabled.
- 13. Click the other tabs and add relevant information if necessary.
- 14. Click Save.
- 15. Select the task created in the Task Name section and click Next. The Schedule page appears.
- 16. Schedule the running time of the task as desired and then click Next.
- 17. Review the task settings and then click Save.

### **Excluding Folders**

The folders and files listed in **Folders and Files Exclusion** on page 16 should be excluded from virus scanning because they are used during NICE operations.

#### To exclude folders in McAfee VirusScan Enterprise 8.8:

- 1. Log on to ePolicy Orchestrator.
- 2. Click Menu > System > System Tree.
- 3. In the System Tree pane, under My Organization, select your group.
- 4. Click the Assigned Client Tasks tab and then click Actions.
- 5. In the drop-down menu, click New Client Task Assignment.
- 6. In the **Product** drop-down list, select **VirusScan Enterprise 8.8.0**.
- 7. In the Task type field, select On Demand Scan.

- 8. Create a new task, and in Task Name type a name for it.
- 9. Click the **Exclusions** tab.

#### Figure 2-6: Exclusions Tab

Client Task Catalog : New Task - VirusScan Enterprise 8.8.0: On Demand Scan					
Task Name		Scan with exlusions			
Description					
Scan Locations	Scan Items	Exclusions Actions Performance Reports Task			
Specify what items to exclude from scanning.					
What not to scar	nt	Item     Exclude Subfolders       Add     Edit			
How to handle cl	ient exclusions	• Overwrite client exclusions. Only exclude items specified in this policy.			

10. To add an excluded folder, click **Add** and specify the path of the folder to exclude.

Figure 2-7: List of Exclusions after Adding an Excluded Folder

Scan Locations	Scan Items	Exclusions	Actions	Performance	Reports	Task			
Specify what it	Specify what items to exclude from scanning.								
What not to sca	n:	Item					Exclude Su	ubfolders	
		E:\						No	
		4	Add	Edit	Remo	ve	Clear		
How to handle c	ient exclusions	: 🔽 ov	erwrite clie	nt exclusions. Or	nly exclude	items spe	ecified in this p	olicy.	

- 11. Repeat Step 10 to define all the necessary exclusions.
- 12. Click the other tabs and add relevant information if necessary.

- 13. Click Save.
- 14. Select the task created in the Task Name section and click Next. The Schedule page appears.
- 15. Schedule the task as desired and then click Next.
- 16. Review the task settings and then click **Save**.

### Configuring an Update Task

NICE highly recommends that you update your antivirus software on a daily basis.

#### To configure an update task in McAfee VirusScan Enterprise 8.8:

- 1. Log on to ePolicy Orchestrator.
- 2. Click Menu > System > System Tree.
- 3. In the System Tree pane, under My Organization, select your group.
- 4. Click the Assigned Client Tasks tab and then click Actions.
- 5. In the drop-down menu, click New Client Task Assignment.
- 6. In the **Product** drop-down list, select **McAfee Agent**.
- 7. In the Task type field, select Product Update.
- 8. Create a new task, and in Task Name type an appropriate name for it.

Client Task Catalog : New Task - McAf	ee Agent: Product Update
Task Name	Update
Description	
"Update in Progress" dialog box (Windows systems only):	<ul> <li>Show "Update in Progress" dialog box on managed systems</li> <li>Allow end users to postpone this update</li> <li>Maximum number of postpones allowed: 1</li> <li>Option to postpone expires after (seconds): 20</li> <li>Display this text:</li> </ul>
Package selection:	<ul> <li>C All packages</li> <li>C Selected packages</li> </ul>
Package types:	Signatures and engines: Linux Engine Mac Engine Engine Buffer Overflow DAT for VirusScan Enterprise DAT Patches and service packs: ePO Agent Key Updater 4.6.0 MER for ePO 2.5.3.0 VirusScan Enterprise 8.8.0 Product Improvement Program Content 1.11

#### Figure 2-8: Product Update Task

- 9. In the **Package selection** section, select **All packages** or **Selected packages**. By default, the **Selected packages** option is selected.
- 10. In the **Package types** section, select the package types. By default, the **Engine** and **DAT** options are selected.
- 11. Configure other options with relevant information if necessary.
- 12. Click Save.
- 13. Select the task created in the Task Name section and click Next. The Schedule page appears.
- 14. Schedule the running time of the task as desired and then click **Next**.
- 15. Review the task settings and then click **Save**.

### **Using Symantec Endpoint Protection**

If you are using Symantec Endpoint Protection, perform the procedures described in this section to do the following:

- Disable Heuristic Scanning
- Configure SONAR
- Configure LiveUpdate

### **Disable Heuristic Scanning**

Heuristic scanning can be disabled if it impairs performance.

#### To disable heuristic scanning with Symantec Endpoint Protection:

- 1. In a web browser log on to Symantec Endpoint Protection Manager. The Symantec Endpoint Protection Manager Console opens.
- 2. In the left-hand column, click the **Policies** tab. The **Policies** pane appears.
- 3. In the Policies pane, click Virus and Spyware Protection. The Virus and Spyware Protection Policies pane appears.
- 4. In the **Virus and Spyware Protection Policies** pane, click the appropriate policy that you use from the list. The Virus and Spyware Protection Policy window for the policy selected opens.
- 5. In the Virus and Spyware Protection Policy window, under **Windows Settings**, click **Global Scan Options**.

Virus and Spyware Protection	Global Scan Options
Policy	Insight Settings:
Windows Settings	Changes made for these settings will affect all antivirus scanning.
Scheduled Scans:	Con V Enable Insidit for: Symantec trusted
Administrator-Defined Scans	What is Insight?
Protection Technology:	Bloodhound(TM) Detection Settings
Auto-Protect	Configure Bloodhound(TM) detection to scan files for susnicious behavior
Download Protection	Configure Endouriouring (1m) dedealor to acur mes for exercise service.
SONAR	T Enable Bloodhound(TM) heuristic virus detection Automatic
Email Scans:	What is Bloodhound?
Internet Email Auto-Protect	Scan Network Drive
Microsoft Outlook Auto-Protect	Specify options for scanning network drives.
Lotus Notes Auto-Protect	Ask for a password before scanning a mapped network drive
Advanced Options:	Change Password
Global Scan Options	
Quarantine	Shared Insight Cache
Miscellaneous	Configure Shared Insight Cache settings to improve scan performance on virtual machines.
Mac Settings	🗖 Enable Shared Insight Cache 🔲 Require SSL
Scheduled Scans:	Hostname: Port: 9005
Administrator-Defined Scans	Username:
Protection Technology:	
Auto-Protect	Change Password
Advanced Options:	What is Shared Insight Cache?
Miscellaneous	

Figure 2-9: Virus and Spyware Protection Policy Window

- 6. Clear the Enable Bloodhound(TM) heuristic virus detection checkbox.
- 7. Click OK.

### **Configure SONAR**

SONAR provides real-time protection, detecting potentially malicious applications running on your computers.

SONAR uses heuristics, as well as reputation data to detect emerging and unknown threats. SONAR provides an additional level of protection on your client computers and complements your existing antivirus, spyware protection, and intrusion prevention.

If SONAR impairs performance of servers running NICE software, disable it.

If your system requires SONAR to be enabled, configure all exclusions using the guidelines in the **Folders** and **Files Exclusion** on page 16 section.

### Configure LiveUpdate

NICE highly recommends that you update your antivirus software on a daily basis. In Symantec Endpoint Protection, you can configure the schedule of automatic downloads from LiveUpdate servers.

#### • To configure live update with Symantec Endpoint Protection:

- 1. In a web browser, log on to Symantec Endpoint Protection Manager. The Symantec Endpoint Protection Manager Console opens.
- 2. In the left-hand column, click the **Policies** tab.
- 3. In the **Policies** pane, click **LiveUpdate**. The **LiveUpdate Policies** pane appears.

#### Figure 2-10: LiveUpdate Policies

💿 Symantec Endpoint Protection Manager					
🔘 Syr	mantec <sup>™</sup> Endpoint Protection	n Manager		Re	iresh Help Log.Off
Home	Policies	LiveUpdate Policies     LiveUpdate Settings     LiveUpdate Cettings	content		]
Monitors	Intrusion Prevention     Application and Device Control     LiveUpdate     Exceptions	Name LiveUpdate Settings policy	Created automatically durin	Description g product installation.	Location Use Count
Reports	③ Policy Components ▲				
Policies	Tasks				
∆dmin	<ul> <li>Import a LiveUpdate Settings polk</li> <li>Search for Applications</li> </ul>				
		Recent changes appear below:		1	1
		Added shared policy upon system install		Time March 13, 2013 4:56:52 PM EET	Administrator

4. In the LiveUpdate Policies pane, on the LiveUpdate Settings tab, click LiveUpdate Settings policy. The LiveUpdate Settings policy window opens.

🚮 LiveUpdate	Schedule
Policy	LiveUpdate Scheduling
Mindowe Softinge	Enable the scheduling of automatic downloads from LiveUpdate servers. The schedule settings do not control downloads from
Server Settings	the default management server, from Group Update Providers, or from third party content management tools.
Schedule	Note: The controls on this dialog will only be enabled if Use a LiveUpdate Server is selected on the Server Settings tab.
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 Continuousty C Every 4 hours C Daily C Weekly
Advanced Settings	
	At: 21 : 55 🗭 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 part scheduled time to try ensign
	Keep trying for (in hours):
	Download Randomization Options
	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).
	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 all the conditions that you specify are met.
	✓ LiveUpdate runs only if Virus and Spyware definitions are older than:
	2 🚔 C hours @ days
	V Livel Indete whe call if the aliest is disconnected from Sumariae Endpoint Protection for were them
	Envelopudae roms unity in the client is associated from symanice chaptain Protection for more than:
	8 C minutes (* hours

Figure 2-11: LiveUpdate Settings Policy Window

- 5. Edit the policy as required.
- 6. In the left-hand pane, expand the **Schedule** section and set an appropriate time for running LiveUpdate.
- 7. Click OK.

### Using Trend Micro OfficeScan

If you are using Trend Micro OfficeScan, perform the procedures described in this section to do the following:

- Configure scheduled updating of the OfficeScan server.
- Configure automatic updating of OfficeScan clients.

## Configuring Scheduled Updating of the OfficeScan Server

NICE highly recommends that you update the antivirus software installed on the OfficeScan Server on a daily basis.

#### To configure scheduled updates of the OfficeScan server:

- 1. Log on to the OfficeScan management console. The OfficeScan management console opens.
- 2. In the right-hand pane, navigate to Updates > Server > Scheduled Update.

#### Figure 2-12: OfficeScan Management Console - Scheduled Updates

⑦ TREND: OfficeScan™					
Current server: nicevm-3147					
	Server Scheduled Update				
Scan Now for All Domains         Update Server Now         Image: Construction of the Server Now					
	Components to Update				
Summary	✓ Networked Computer Components				
+ Security Compliance	🕂 🔽 Antivirus	Antivirus			
+ Networked Computers	+ 🗸 Anti-sovware				
+ Smart Protection	Damage Cleanup Services	Damane Cleanun Services			
– Updates					
Summary					
- Server	Update Schedule				
Scheduled Update	O Hourly				
Manual Update	O Daily     Start time: 00 • (hh     Weekly, every Sunday • Update for period of 2 • ho				
Update Source					
+ Networked Computers	O Monthly, on day 01 💌				
Rollback	Save Cancel				

- 3. Select the Enable scheduled update of the OfficeScan server checkbox.
- 4. In the **Components to Update** section, select the applicable components.
- 5. In the **Update Schedule** section, select **Daily** (highly recommended) and set the applicable parameters.
- 6. Click Save.

### **Configuring Automatic Update**

NICE highly recommends that you update the antivirus software installed on OfficeScan clients (networked computers) on a daily basis.

#### To configure automatic update of OfficeScan clients:

- 1. Log on to the OfficeScan management console. The OfficeScan management console opens.
- 2. In the right-hand pane, navigate to Updates > Networked Computers > Automatic Update.

Figure 2-13: OfficeScan Management Console - Automatic Update

	an™			
Current server: nicevm-3147				
	Automatic Update (Network	ed Computers)		
Update Server Now	Clients are triggered to update com	ponents when certain events occur or during the specified update schedule.		
	Event-triggered Update			
Summary	✓ Initiate component update on a	lients immediately after the OfficeScan server downloads a new component		
+ Security Compliance	✓ Include roaming and offline client(s)			
+ Networked Computers	Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)			
+ Smart Protection	Perform Scan Now after update	(excluding roaming clients)		
- Updates	Schedule-based Undate	· · · · · · · · · · · · · · · · · · ·		
Summary + Server	C Minute(s)			
- Networked Computers	C Hour(s)	Start time: 01 🗸 : 00 🗸 (hh:mm)		
Automatic IIndate	Daily	Update for a period of 4 💌 hour(s)		
Manual Undate	C Weekly, every Sunday 🔍			
Update Source				
Rollback	Save Cancel			

- 3. In the **Event-triggered Update** section, select the applicable checkboxes.
- 4. In the **Schedule-based Update** section, select **Daily** (highly recommended) and set the applicable parameters.
- 5. Click Save.

### **Allowing Required Email Messages**

After McAfee VirusScan Enterprise 8.8 is installed on NICE Engage Platform/NICE Interaction Management/NICE Perform servers using the default installation options, email messages, in particular, NICE Playback Organizer (PBO) requests and password recovery messages, cannot be sent from these servers. This occurs because the McAfee antivirus software blocks all outgoing traffic on port 25 (SMTP communication).

After McAfee VirusScan Enterprise 8.8 is installed on the relevant NICE server, configure the antivirus software not to block port 25.

#### To unblock port 25 in McAfee VirusScan Enterprise 8.8:

- 1. Click Start > All Programs > McAfee > VirusScan Console. The VirusScan Console opens.
- 2. Right-click **Access Protection** and click **Properties**. The Access Protection Properties window opens.
- 3. Click the Access Protection tab.
- 4. Under Categories, select Anti-virus Standard Protection.
- 5. Clear the check marks in the **Block** and **Report** columns for the **Prevent mass mailing worms from sending mail** rule.
- 6. Click OK.

### **Live Updates**

NICE highly recommends that the antivirus software is updated on a daily basis. It is recommended to schedule the automatic update for a time when the network traffic is low.

Low network traffic refers to customer network and not to NICE Engage Platform/NICE Interaction Management/NICE Perform system.

### **CPU** Priority

It is recommended to set the CPU usage (utilization) to the lowest value. Note that not all antivirus software allows configuring the CPU usage (utilization).

### **Additional Configurations**

Buffer overflow protection is a resource consuming application and should therefore be disabled for all NICE Servers.

If you choose to enable this option, you might experience performance issues in your system.

Heuristic scanning should be disabled in case of performance issues.

### **Additional Recommendations**

In order to maintain performance of your machines during scans, see Microsoft Virus Scanning recommendations: http://support.microsoft.com/kb/822158.

This information is provided for reference purposes only.

# 3

### SQL Backup

This section provides guidelines for backing up NICE Engage Platform/NICE Interaction Management/NICE Perform SQL databases.

	Contents
SQL Backup Guidelines	
Database Configuration Guidelines	46

### **SQL Backup Guidelines**

### Overview

Customers can implement their own database backup policies for NICE Engage Platform/NICE Interaction Management/NICE Perform databases.

#### **NOTE**:

Each backup schedule provides a different level of recovery. Customers should match recovery levels according to their needs.

The customer is responsible for database backup operations. They should ensure that there is enough free space for the database and backups.

Customers MUST NOT restore the SQL database from the backup to production system without first consulting with NICE Customer Services.

Backup software should be used when the size of any of the NICE server databases are approximately 1TB and larger. SQL Backup jobs should not be used in such a scenario.

### Schedule

The backup schedule should include full backup, differential backup, and log backup. The backup plan must include all NICE databases and system databases.

Below is a sample backup schedule:

- **Full Backup**: once a week during off/low peak hours.
- Differential Backup: daily backup during off/low peak hours.
- Log Backup: for sites that include the Media Encryption solution, the nice\_crypto database is set to Full Recovery Model. Hourly backup is recommended.

#### Important!

The **Full Recovery Model** is approved only for DR3.X environments with SQL Server database mirroring.

### **Backup Files Location**

Database backup files should be stored for long term storage at a remote location, and not on the server's hard drive.

### **Implementation Guidelines**

If the customer's backup policy *does not* include the regular NICE Engage Platform/NICE Interaction Management/NICE Perform backup jobs, they should be disabled. In this situation, the relevant NICE Sentinel alarms should also be disabled.

Disable the following SQL Jobs on the Database server:

- Nice Differential Backup
- Nice Full Backup
- Nice Log Backup

Disable the following SQL Jobs on the Data Mart server:

- Nice Differential Backup
- Nice Full Backup
- Nice Log Backup

If the environment consist of multi Data Hub deployment, SQL backup jobs on all Data Hubs must be disabled.

### Backup Tools

Customers can use any off-the-shelf Microsoft SQL Server Backup tools that suits their backup and restore needs while taking into consideration that the NICE Engage Platform/NICE Interaction Management/NICE Perform database backup must be performed during off peak or low peak hours.

### **Database Configuration Guidelines**

NICE Engage Platform/NICE Interaction Management/NICE Perform databases can be configured for the **Full Recovery Model** taking into consideration the following:

- SQL Server log backups are essential.
- In the Full Recovery Model, all transactions are logged in the transactional log until they are backed up. Therefore, log backups must be created on a regular basis. Hourly backup is recommended.
- Transactional log disk space monitoring is essential. If the transactional log is not purged due to backup failure, new transactions and/or calls will not be added to the database.

#### Important!

NICE server databases configured with the **Full Recovery Model** are supported only for DR3.X environments with SQL Server database mirroring.