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:	B0
Distribution Status:	Published
Publication Date:	November 2014

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 **www.niceusergroup.org** 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

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

Revision	Modification Date	Software Version	Description
A3	September 2011		■ Added Security Permissions section for NICE Interaction Management Release 4.x

A4	November 2011		■ Removed the following sections from Security Permissions section for NICE Interaction Management Release 4.x:
			  ■ Unified Environment/SMB
			  ■ Semi-Distributed Environment
			  ■ New Semi-Distributed Environment
			■ Added:
			  ■ ITI Connect Server on page 87
			■ Updated table:
			  ■ Service Settings: NICE Services on page 75

A5	August 2012		■ Added:
			  ■ NICE Interactions Center on page 88
			  ■ NICE Sentinel on page 90
			  ■ NICE Media Interconnect on page 92
			  ■ Configuring SQL Server Permissions on page 106
			  ■ Using Secure Communication and Media Encryption on page 117

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

Revision	Modification Date	Software Version	Description

A7	January 2013		Removed the following sections from this guide:
			■ Security Permissions for NICE Perform Release 3.x
			This section can now be found in the *Microsoft Windows Authentication Guide (for NICE Perform Releases 3.2 &3.5*)
			■ Security Permissions for NICE Interaction Management Release 4.1
			This section can now be found in the *Microsoft Windows Authentication Guide (for NICE Interaction Management Release 4.1*)
			■ List of User Rights
			This section can now be found within the Security Permissions sections in both of the following guides:
			  ■ *Microsoft Windows Authentication Guide (for NICE Perform Releases 3.2 &3.5*)
			  ■ *Microsoft Windows Authentication Guide (for NICE Interaction Management Release 4.1*)

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
B0	November 2014	N/A	■ 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. ■ Updated guide for NICE Engage Platform.

[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

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.

Important!

- See tables per NICE Engage Platform/NICE Interaction Management/NICE Perform Release:
  - **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.

Excluded Files and Folders for NICE Perform 3.x

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	

NICE Server	Default Path	Files
Nice Screen Logger	D:\MMLStorage D:\Program Files\Nice Systems\Multimedia Logger\Datasystem	DAT files TBL files
NICE Sentinel	D:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data	MDF files
		LDF files
Speech to Text and Words Search Pack	D:\Program Files\NICE Systems\Nice Content Analysis Server\MediaCache	WAV files
		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.

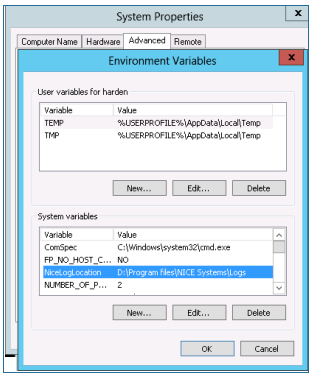
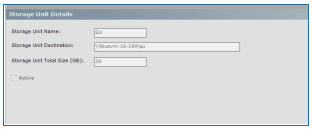
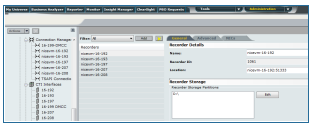
NICE Server	Default Path	Files
Advanced Interaction Recorder		
■ Package and binaries folder	D:\Program Files\NICE systems\	
■ Log files folder	D:\Program Files\NICE systems\	
■ Metadata management folder	D:\Program Files\NICE systems\	
■ Recording Folders (partitions)	User defined path in SRT: <Recording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

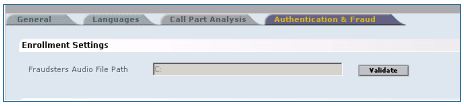
NICE Server	Default Path	Files
■ Archiving Folders	User defined path in SRT: <Archiving directory>	*.nmf
CTI / VRSP	D:\Program files\NICE Systems\CTI	
Database	E:\<SQL Data Files>	MDF files
	F:\<SQL Log Files>	LDF files
Data Mart	E:\<SQL Data Files>	MDF files
	F:\<SQL Log Files>	LDF files
Interactions 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 D:\Program Files\Nice Systems\Multimedia Logger\Datasystem	DAT files TBL files
NICE Sentinel	D:\<SQL Data Files>	MDF files
	D:\<SQL Log Files>	LDF files
Speech-to-Text Pack	D:\<Storage Area>	
	D:\Program Files\NICE Systems\Nice Content AnalysisServer	
	D:\Storage Area for a Content Analysis\Index	
Storage Center	E:\<SC_Archive_Directory>	NMF files
Text Analysis Pack	E:\<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	Log files
	All operating systems: D:\Ntlogger	
Windows Media Server	D:\<Publishing _Point_Directory>	
Word Search Pack	D:\Program Files\NICE Systems\Nice Content AnalysisServer\MediaCache E:\<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%  	
■ Metadata Management folder	D:\Program Files\NICE systems\	*.s3db*
■ Recording Folders (partitions)	User defined path in SRT: <Recording directory>  	*.nmf
■ Archiving Folders	User defined path in SRT: <Archiving directory> 	*.nmf
CTI / VRSP	D:\Program files\NICE Systems\CTI	
Database	E:\<SQL Data Files>	MDF files
	F:\<SQL Log Files>	LDF files
Data Mart	E:\<SQL Data Files>	MDF files
	F:\<SQL Log Files>	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 D:\Program Files\Nice Systems\Multimedia Logger\Datasystem	DAT files TBL files
NICE Sentinel	D:\<SQL Data Files> D:\<SQL Log Files>	MDF files 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	*.*
■ Authentication & Fraud Engine (Nuance) audio folder	User defined path in plugin <Fraudsters audio file path>  	*.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: D\Program files\NICE Systems\RTI Connect\Bin\PersistentDBWriterDatabase	*.bkp *.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	
Standard Word Search Server	D:\Program Files\NICE Systems\Nice Content AnalysisServer\MediaCache E:\<WorkArea>	
Storage Center	E:\<SC_Archive_Directory>	NMF files
Stream Server with Windows Media Services	D:\<Publishing _Point_Directory>	
Text Analysis Engine	E:\<WorkArea>	
Text Mining Engine	E:\<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	Log files
	All operating systems: 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.

To disable firewalls:

- 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.

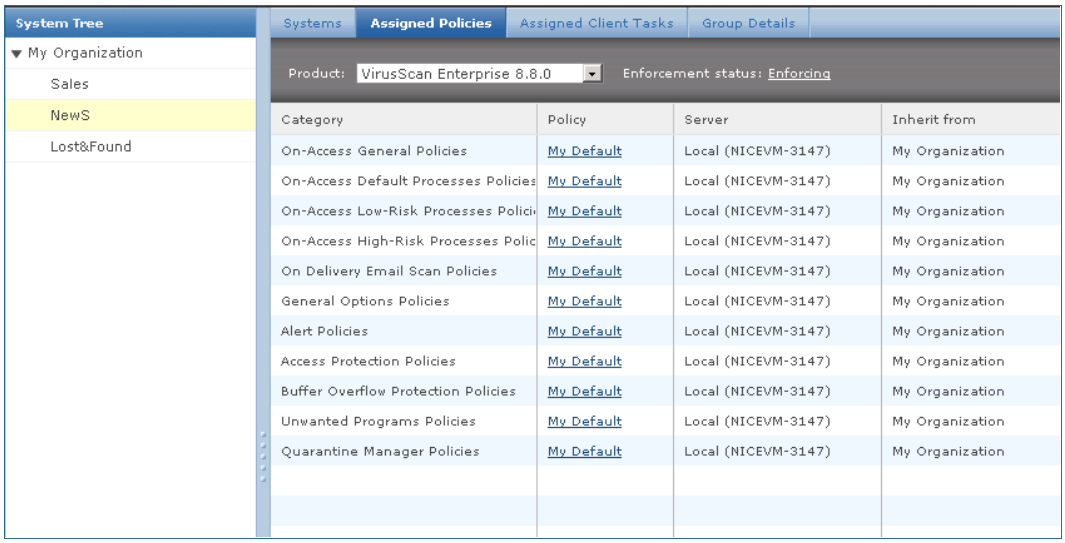
Disabling Buffer Overflow Protection

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



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

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

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

Disabling Heuristic Scanning

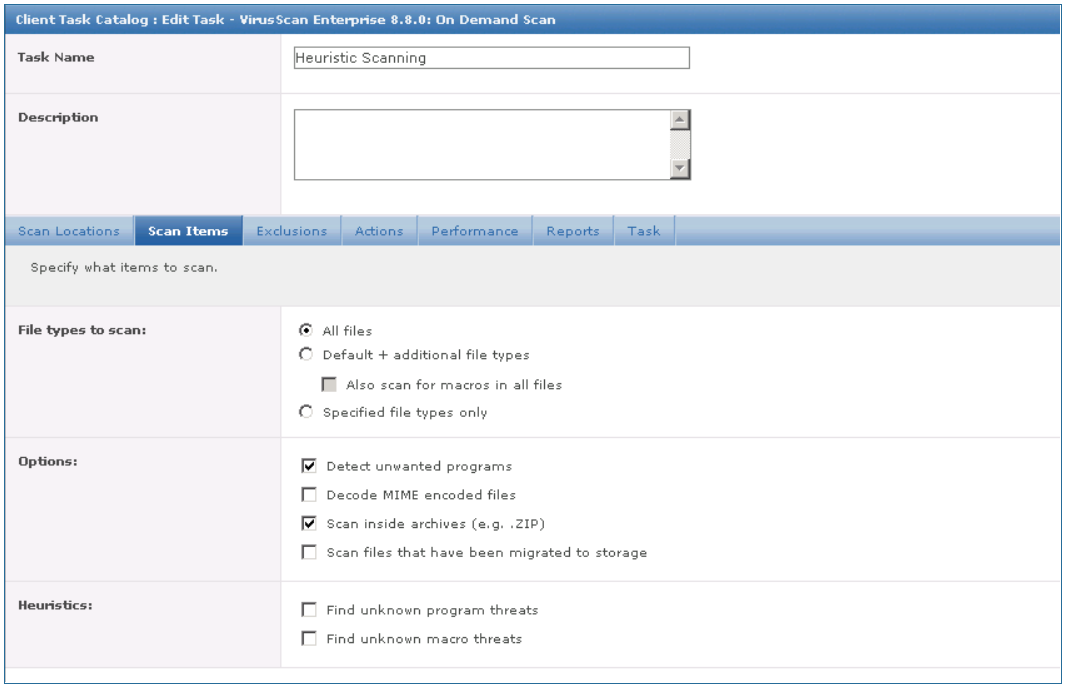
Heuristic scanning can be disabled if it impairs performance.

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**.

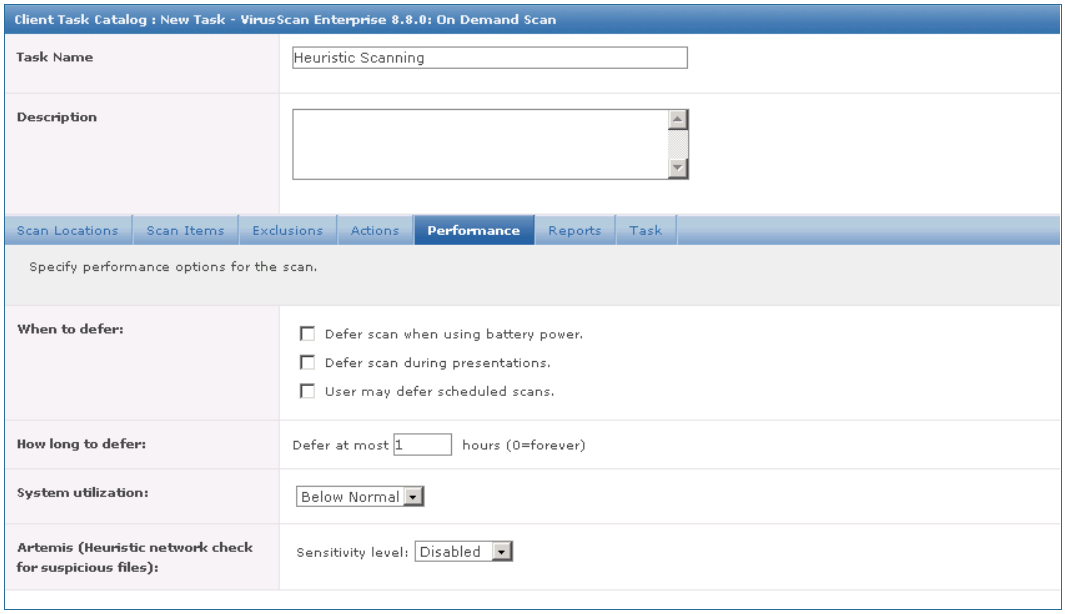
8. Create a new task, and in **Task Name** type an appropriate name for it.
9. Click the **Scan Items** tab.

Figure 2-4: Scan Item Tab



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



12. In the **Artemis (Heuristic network check for suspicious files)** section, in the **Sensitivity level** drop-down 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

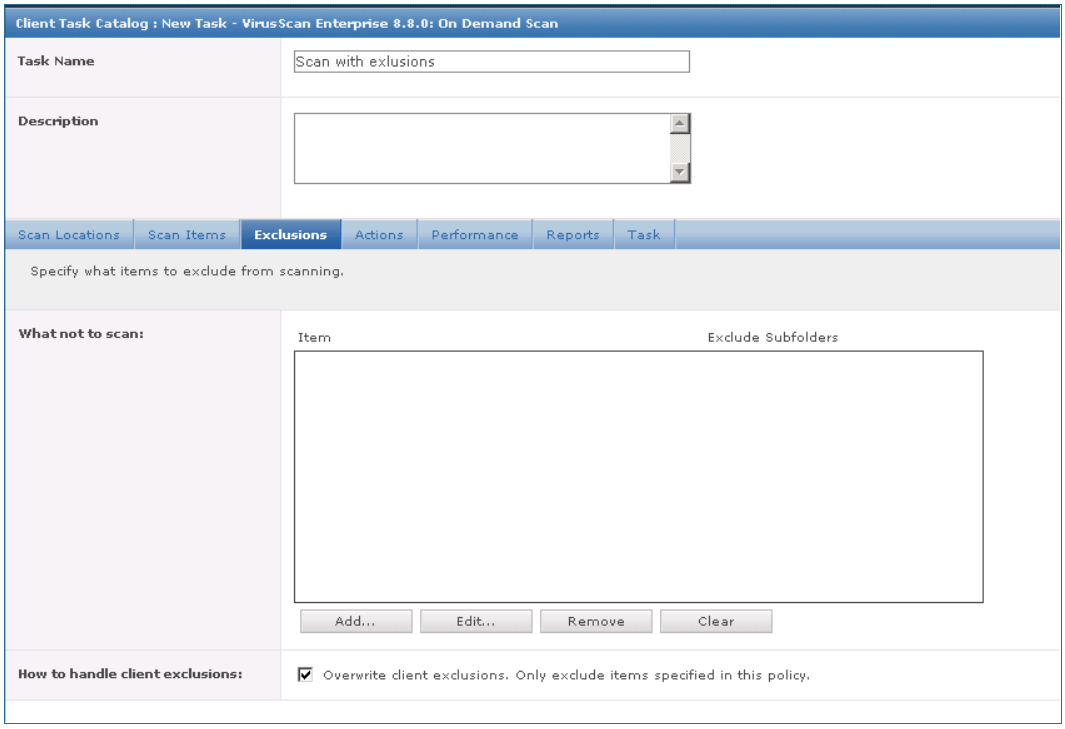
The folders and files listed in **Folders and Files Exclusion** on page 16 should be excluded from virus scanning because they are used during NICE operations.

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**.

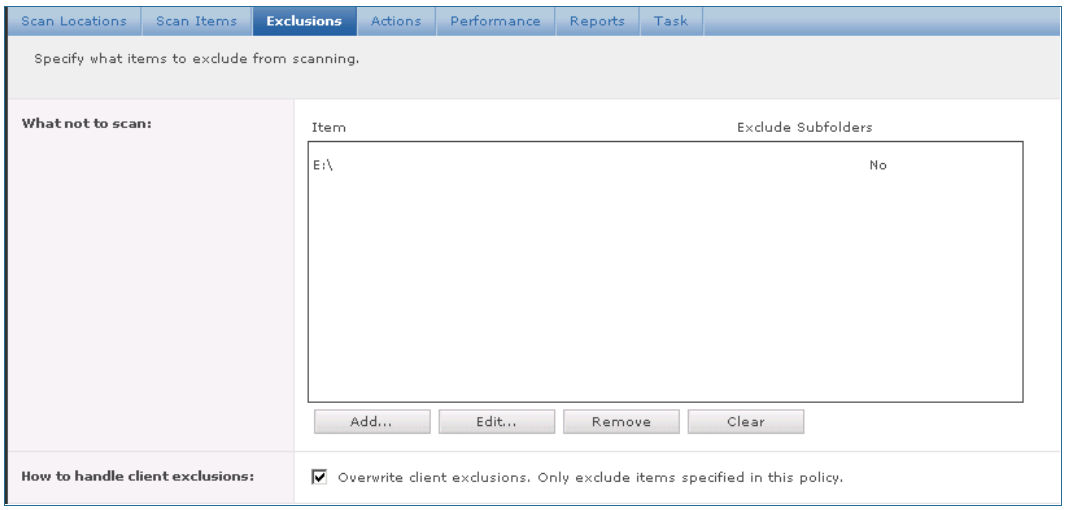
8. Create a new task, and in **Task Name** type a name for it.
9. Click the **Exclusions** tab.

Figure 2-6: Exclusions Tab



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



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**.

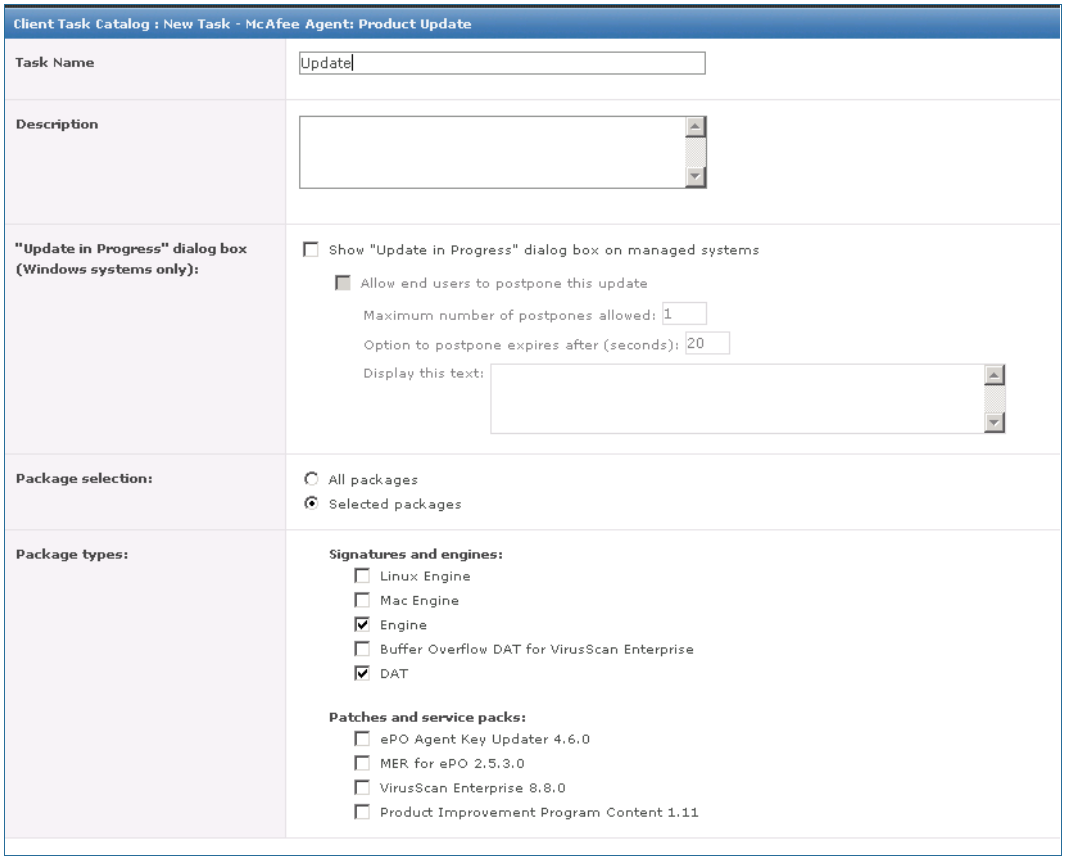
Configuring an Update Task

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.

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**

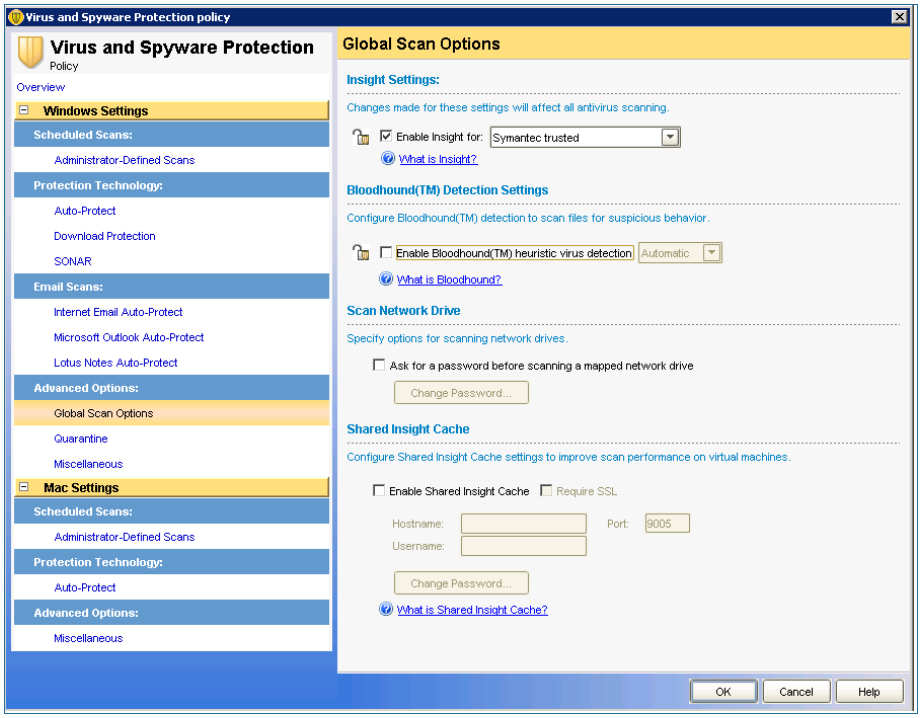
Disable Heuristic Scanning

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**.

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.

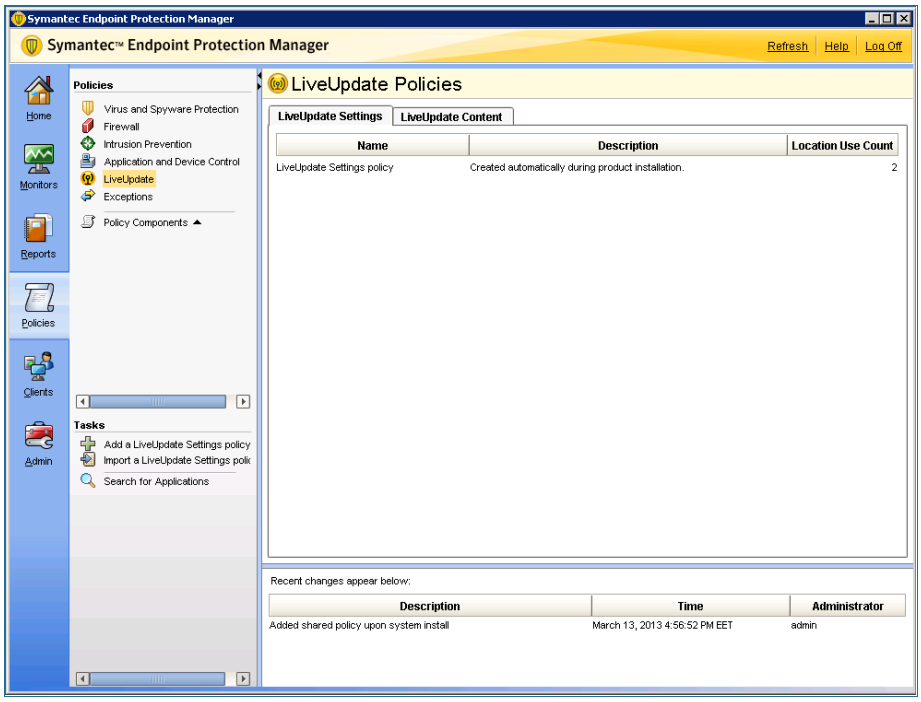
Configure LiveUpdate

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



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

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.

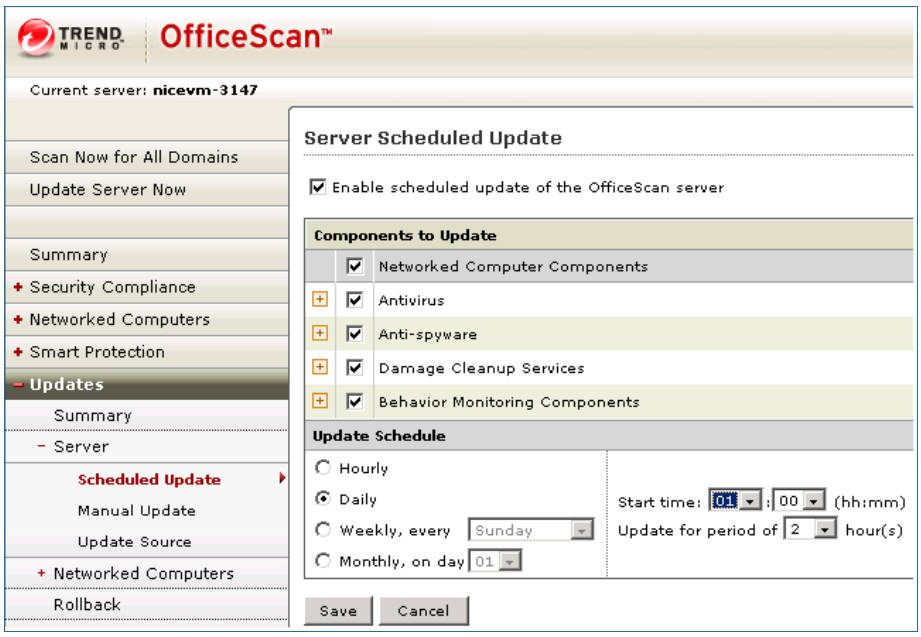
Configuring Scheduled Updating of the OfficeScan Server

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



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**.

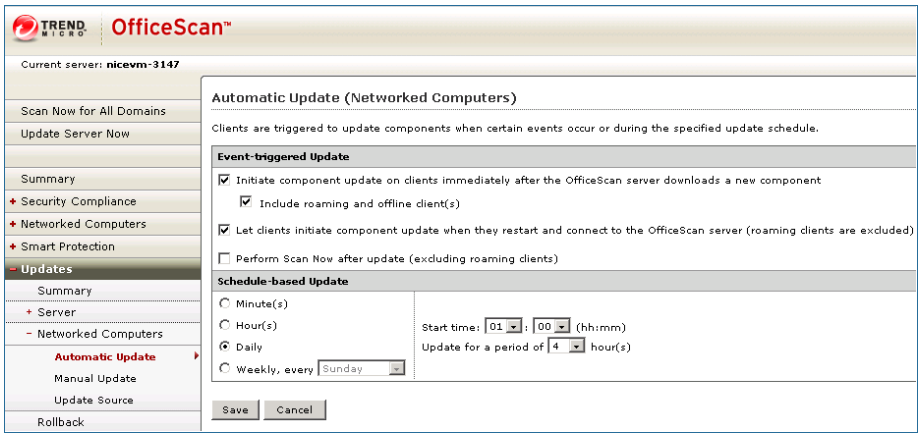
Configuring Automatic Update

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



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

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.