Third Party Technical Guidelines

Configuration Guide

NICE®

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

APAC Region (Asia/Pacific)
Tel: +852-8338-9818
Fax: +852-2802-1800
email: support.apac@nice.com

The Americas Region (North, Central, South America)
Tel: 1-800-6423-611
Fax: +720-264-4012
email: support.americas@nice.com

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

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

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

North America
Tel: 1-800-663-5601
Fax: +201-356-2197
email: na_sales@nice.com

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

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

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

7: Working with XBAP or ASPX (ASP.NET) 155

8: Microsoft SQL Server 171

A: Discontinued Technical Notes 257

B: Using Real-Time Solutions with App-V 261

C: Using Real-Time Solutions with Citrix Streaming 265

Introduction

The Third-Party Technical Guidelines is a one-stop-shop document for information about third-party software application compatibility with NICE systems.

This document should be used by NICE customers and customer service organizations in order to verify the compatibility of third-party software to NICE products in addition to specific configuration information.

This document consolidates information published in a number of Technical Notes listed in the Discontinued Technical Notes appendix of this document, see **Discontinued Technical Notes** on page 257.

This document serves as general guidelines and applies to all existing NICE Interaction Management/NICE Perform versions.

Updates for specific product versions may be issued separately based on these guidelines. NICE, at its sole discretion, may decide to change the general guidelines or deviate from them for a specific product version.

This document should apply in cases where it contradicts a previous Technical Note.

This document will be updated periodically upon availability of new third party software versions following the rules of certification as described in the *Third-Party Software Certification Policy*.

Revision History

Revision	Modification Date	Software Version	Description
A1	November 2010		▪ Updated SQL support. See **Microsoft SQL Server** on page 171 ▪ Updated Antivirus. See **Antivirus** on page 199
A2	February 2011		▪ Updated Microsoft service packs support and requirements. See **Microsoft Software Service Packs Certified by NICE Systems** on page 22 ▪ Added compatibility for Microsoft Windows 7 64-bit, and updated compatibility by NICE Perform release. See **Windows 7 32-bit/64-bit** on page 94 ▪ Added new section for silent installations. See **Using the Silent Installation to Install NICE Perform Release 3.x and NICE Interaction Management Release 4.1 Client Applications** on page 96 ▪ Updated procedures for installing client-side components on Microsoft Windows 7. See **Manually Installing NICE Perform Release 3.x and NICE Interaction Management 4.1 Client Applications** on page 99
A3	March 2011		▪ Updated the section on Microsoft Windows 7. See **Windows 7 32-bit/64-bit** on page 94 ▪ Added new chapter for Daylight Savings Time. See **Daylight Savings Time** on page 197

Revision	Modification Date	Software Version	Description
A4	May 2011		■ Added NICE Interaction Management Release 4.1 compatibility. ■ Updated Compatibility with Microsoft Windows 7 for 32/64 bit. See **NICE Perform Client Applications Compatibility** on page 94 ■ Added Internet Explorer compatibility. See **Internet Explorer 9** on page 131 ■ Added Logger version 9.07 to anti-virus tables. ■ Added Sophos 9.5.
A5	June 2011		■ Formatting changes. ■ Added EPO 4.5 to **NICE Products and Antivirus Certifications Matrix - NICE Perform Release 3, SP3 and Higher** on page 214
A6	July 2011		■ Updated **Remote Desktop Connection** for Microsoft Windows Server 2008. See **Enabling Remote Connection on Microsoft Windows Server 2008** on page 249 ■ Added support for Internet Explorer 6. See **Internet Explorer 6** on page 107 ■ Added Sophos 9.7.
A7	September 2011		■ Updated **Table 2-1: Microsoft Software Service Packs certified by NICE Systems**

Revision	Modification Date	Software Version	Description
A8	November 2011		▪ Added SP1 for SQL Server 2008 R2 in **Microsoft Software Service Packs Certified by NICE Systems** on page 22.
			▪ Updated ROD Client information in **Windows 7 32-bit/64-bit** on page 94
			▪ Added **Microsoft .NET Framework 4 Requirement for NICE Interaction Management 4.1** on page 149
			▪ Updated DST patch list in **Microsoft Daylight Savings Time Updates** on page 198.
			▪ Added McAfee ePO 4.6 in **McAfee ePO** on page 201, **NICE Products and Antivirus Certifications Matrix - Version 8.90** on page 209, and **NICE Products and Antivirus Certifications Matrix - NICE Perform Release 3, SP3 and Higher** on page 214.
			▪ Added Sophos exclusions in **Sophos** on page 208.
A9	November 2011		▪ Added SP3 for SQL Server 2008 in **Microsoft Software Service Packs Certified by NICE Systems** on page 22.
			▪ Added information regarding machine and domain names with non-ASCII characters in **Localization** on page 80.
			▪ Added note regarding support for 32-bit version Internet Explorer in **Internet Explorer** on page 105.

Revision	Modification Date	Software Version	Description
B0	January 2012		▪ Updated **Windows 7 32-bit/64-bit** on page 94.
B1	July 2012		▪ Added information for avoiding false positives to **SEP** on page 202.
			▪ Added information to **NICE Products and Antivirus Certifications Matrix - NICE Perform Release 3, SP3 and Higher** on page 214.
			▪ Updated the table in **Microsoft Daylight Savings Time Updates** on page 198.

Revision	Modification Date	Software Version	Description
B2	December 2012		■ Replaced SP1 with SP2 for all SQL 2008 R2 in **Table 2-1: Microsoft Software Service Packs certified by NICE Systems** ■ Updated BSF Tool kit for NICE Perform Releases 3.1 and 3.2 - Not Supported on Windows 7 64 bit. See **Table 4-2: Compatibility With Microsoft Windows 7 32-bit and 64-bit by Release** ■ Updated VRA Compatibility With Microsoft Windows 7 for NPR4.1 in **Table 4-2: Compatibility With Microsoft Windows 7 32-bit and 64-bit by Release** ■ Added supported Internet Explorer version by Sentinel Client. See **Internet Explorer** on page 105. ■ Updated IE8 General Description and Conclusions on **page 121**. ■ Updated IE9 General Description and Conclusions on **page 131**. ■ Added McAfee limitation on **page 202**. ■ Added TDM Logger 9.4 with Antivirus Certification in **NICE Products and Antivirus Certifications Matrix - NICE Perform Release 3, SP3 and Higher** on page 214. ■ Added Trend Micro OfficeScan 10.5 and Trend Micro OfficeScan 10.6 to **NICE Products and Antivirus Certifications Matrix - NICE Perform Release 3, SP3 and Higher** on page 214.

Revision	Modification Date	Software Version	Description
B3	March 2013		▪ Added **Microsoft .NET Framework 4.5 with NICE Perform 3.2/3.5 and NICE Interaction Management 4.1** on page 151 ▪ Updated **NICE Perform R3.5/NICE Interaction Management 4.1 Known Issues with Internet Explorer 8** on page 122 ▪ Updated **NICE Perform Release 3.1/3.2/3.5 and NICE Interaction Management 4.1 Known Issues with Internet Explorer 9** on page 132
B4	July 2013		▪ Updated **Table 2-1: Microsoft Software Service Packs certified by NICE Systems** ▪ Added **Internet Explorer 10** on page 134 ▪ Updated **Microsoft Daylight Savings Time Updates** on page 198. ▪ Updated **General Limitations** on page 200 ▪ Updated **NICE Products and Antivirus Certifications Matrix - NICE Perform Release 3, SP3 and Higher** on page 214 (added: McAfee 8.8/8.8i and Sophos 10.2)
B5	July 2013		▪ Updated **Internet Explorer** on page 105 (small correction in the **Contents**).

Revision	Modification Date	Software Version	Description
B6	October 2013		▪ Updated **Internet Explorer 10** on page 134. Added the section **Adding the NICE Interaction Management Web Application URL to the Compatibility View Settings List** on page 135. ▪ Added the appendix, **Using Real-Time Solutions with App-V** on page 261. ▪ Added the appendix **Using Real-Time Solutions with Citrix Streaming** on page 265.
B7	November 2013		▪ Updated **Microsoft Client Operating Systems**: 　▪ Updated **Reporter Viewer** on page 97, and **NICE ScreenAgent** on page 97. 　▪ Added **PO Client** and **NICE Insight to Impact Bridge** on page 98 ▪ Updated **Manually Installing NICE Perform Release 3.x and NICE Interaction Management 4.1 Client Applications** on page 99 (updated the note that appears before the procedure). ▪ Added section for Release 4.1.46 for XBAP. See **Microsoft .NET Framework 4.5 with NICE Perform 3.2/3.5 and NICE Interaction Management 4.1** on page 151 and **Microsoft .NET Framework 4.0 and up with NICE Interaction Management 4.1.46 and Later** on page 154.

Revision	Modification Date	Software Version	Description
B8	December 2013		Fixed issue with landscape page not displaying correctly in PDF for **Table 4-2: Compatibility With Microsoft Windows 7 32-bit and 64-bit by Release**
B9	January 2014		Fixed information regarding Microsoft Internet Explorer 10. See **Internet Explorer 10** on page 134. Removed the Citrix chapter. The information is now in the Virtualization Guide.
C1	March 2014		Added Internet Explorer 11 support. See **Internet Explorer 11** on page 137. Added an SEP limitaion. See **SEP** on page 202.
C2	May 2014	4.1.47	▪ Added Windows 8/8.1 support for client machines. See **Windows 8 and Windows 8.1 32-bit/64-bit** on page 101. ▪ Updated the information for **Internet Explorer 11** on page 137. ▪ Added about XBAP limitations. See **Microsoft .NET Framework 4.0 and up with NICE Interaction Management 4.1.46 and Later** on page 154. ▪ DCR 1004: A solution to Installing XBAP When Hardening Kit is Installed was found and implemented. The Topic was removed from the guide.

Revision	Modification Date	Software Version	Description
C3	September 2014	4.1.4x	▪ Updated **NICE Products and Antivirus Certification Matrices** on page 209(added separate table for NICE Interaction Management Release 4.1). ▪ Added **Working with XBAP or ASPX (ASP.NET)** on page 155
C5	November 2014	4.1	▪ **DCR 1111** Added chapter **Uninstalling XBAP** on page 164. ▪ **DCR 1113** Added a Before You Begin section to **Installing the NICE Security Certificate for XBAP** on page 156.

Scope of this Guide

Software Version

This guide is updated for:

- NICE Engage Platform 6.3
- NICE Interaction Management Release 4.1
- Real-Time Solutions 4.9
- NICE Perform 3.2 / 3.5

What is included in this guide?

Guidelines for third party software with NICE applications.

What is not included in this guide?

Topic	Where to Find this Topic...
NICE Screen Agent software	*ScreenAgent Installation and Configuration Guide*
Microsoft .NET framework	*Certified Servers Guide*
Setting up a client computer to work with ASPX	*Workstation Setup Guide*
Microsoft Daylight Savings Time configurations	*Maintenance Guide*

[This page intentionally left blank]

Microsoft Software Service Packs Certified by NICE Systems

This chapter summarizes the Microsoft Software Service Packs Certified by NICE Systems.

Contents

Microsoft Software Service Packs Certified by NICE Systems

Product	NICE Interaction Management
	NICE Perform
	NICE Perform eXpress
	Version 8.9
	SMB
Release	NICE Perform Release I
	NICE Perform Release II
	NICE Perform Release 3
	NICE Perform Release 3.1
	NICE Perform Release 3.2
	NICE Perform Release 3.5
	NICE Interaction Management Release 4.1
	NICE Perform eXpress 1.0
	NICE Perform eXpress 2.1
	Version 8.9
Synopsis	Provides information regarding the latest Microsoft Software Service Packs certified by NICE Systems.

The following table consists of information regarding the latest Microsoft Software Service Packs certified by NICE Systems.

Table 2-1: Microsoft Software Service Packs certified by NICE Systems

Microsoft Software	Service Pack	NICE Release	Comment
Windows 2000	SP4	■ NICE Version 8.9 ■ NICE Perform ■ Release 1 SP7 ■ Release 2 SP5 ■ Release 3 SP3 ■ Release 3 SP4 ■ Release 3.1 ■ Release 3.2	Supported by: ■ Set Security ■ ROD ■ Reporter Viewer ■ ScreenAgent ■ Screen Sense Agent ■ NICE Player Codec Pack ■ Nice Standalone Player ■ Survey Manager

Microsoft Software	Service Pack	NICE Release	Comment
Windows Server 2003 R2 Standard Edition 32-bit	SP2	■ NICE Version 8.9 ■ NICE Perform 　■ Release 1 SP7 　■ Release 2 SP5 　■ Release 3 SP3 　■ Release 3 SP4 　■ Release 3.1 　■ Release 3.2 　■ Release 3.5 ■ NICE Interaction Management Release 4.1 - supported only for upgrades ■ NICE Perform eXpress 　■ Release 1.0 　■ Release 2.1	
Windows Server 2003 R2 Enterprise Edition 32-bit	SP2	■ NICE Version 8.9 ■ NICE Perform 　■ Release 1 SP7 　■ Release 2 SP5 　■ Release 3 SP3 　■ Release 3 SP4 　■ Release 3.1 　■ Release 3.2 　■ Release 3.5 ■ NICE Interaction Management Release 4.1 - supported only for upgrades	

Microsoft Software	Service Pack	NICE Release	Comment

Windows Server 2003 R2 Standard Edition 64-bit	SP2	■ NICE Perform
		   ■ Release 3.1
		   ■ Release 3.2
		   ■ Release 3.5
		■ NICE Interaction Management Release 4.1 - supported only for upgrades
			DB Server Only

Windows Server 2003 R2 Enterprise Edition 64-bit	SP2	■ NICE Perform
		   ■ Release 3.1
		   ■ Release 3.2
		   ■ Release 3.5
		■ NICE Interaction Management Release 4.1 - supported only for upgrades
			DB Server Only

Windows XP	SP2	■ NICE Version 8.9
		■ NICE Perform
		   ■ Release 1 SP7
		   ■ Release 2 SP5
		   ■ Release 3 SP3
		   ■ Release 3 SP4
		   ■ Release 3.1
		   ■ Release 3.2
		   ■ Release 3.5
		■ NICE Interaction Management Release 4.1
			Client Side Only

Microsoft Software	Service Pack	NICE Release	Comment

Windows XP	SP3	■ NICE Perform
		   ■ Release 3 SP4
		   ■ Release 3.1
		   ■ Release 3.2
		   ■ Release 3.5
		■ NICE Interaction Management Release 4.1
			Client Side Only

Windows Vista Business	SP2	NICE Perform
		   ■ Release 3 SP4
		   ■ Release 3.1
			Client Side Only

Windows Vista Enterprise Edition	SP2	■ NICE Perform
		   ■ Release 3.1
		   ■ Release 3.2
		   ■ Release 3.5
		■ NICE Interaction Management Release 4.1
			Supported by:
			■ Set Security
			■ ROD
			■ Reporter Viewer
			■ ScreenAgent
			■ Desktop Analysis Agent RTS
			■ NICE Player Codec Pack
			■ Nice Standalone Player
			■ Survey Manager
			■ Media Library

Microsoft Software	Service Pack	NICE Release	Comment

Windows 7	SP1	■ NICE Perform
		  ■ Release 3.1
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1
			Supported Client Side Applications Only

Windows Server 2008 Standard Edition 32-bit	SP2	■ NICE Perform
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1
		■ NICE Perform eXpress Release 2.1	

Windows Server 2008 Enterprise Edition 32-bit	SP2	■ NICE Perform
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1	

Windows Server 2008 Standard Edition 64-bit	SP2	■ NICE Perform
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1	

Windows Server 2008 Enterprise Edition 64-bit	SP2	■ NICE Perform
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1	

Microsoft Software	Service Pack	NICE Release	Comment

Windows Server 2008 R2 Enterprise Edition 64-bit		■ NICE Perform
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1	

Windows Server 2008 R2 Standard Edition 64-bit		■ NICE Perform
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1	

Windows Server 2008 R2 Standard Edition 64-bit	SP1	■ NICE Perform
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1	

Windows Server 2008 R2 Enterprise Edition 64-bit	SP1	■ NICE Perform
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1	

SQL Server 2005 Standard Edition 32-bit	SP3	■ NICE Perform
		  ■ Release 3 SP3
		  ■ Release 3 SP4
		    Release 3.1
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1 - supported only for upgrades	

Microsoft Software	Service Pack	NICE Release	Comment

SQL Server 2005 Standard Edition 64-bit	SP3	■ NICE Perform
		   ■ Release 3 SP4
		   ■ Release 3.1
		   ■ Release 3.2
		   ■ Release 3.5
		■ NICE Interaction Management Release 4.1 - supported only for upgrades	

SQL Server 2005 Enterprise Edition 64-bit	SP3	■ NICE Perform
		   ■ Release 3 SP4
		   ■ Release 3.1
		   ■ Release 3.2
		   ■ Release 3.5
		■ NICE Interaction Management Release 4.1 - supported only for upgrades	

SQL Server 2005 Standard Edition 32-bit	SP4	■ NICE Perform
		   ■ Release 3 SP3
		   ■ Release 3 SP4
		     Release 3.1
		   ■ Release 3.2
		   ■ Release 3.5
		■ NICE Interaction Management Release 4.1 - supported only for upgrades	

Microsoft Software	Service Pack	NICE Release	Comment

SQL Server 2005 Standard Edition 64-bit	SP4	■ NICE Perform
		    ■ Release 3 SP4
		    ■ Release 3.1
		    ■ Release 3.2
		    ■ Release 3.5
		 ■ NICE Interaction Management Release 4.1 - supported only for upgrades	

SQL Server 2005 Enterprise Edition 64-bit	SP4	■ NICE Perform
		    ■ Release 3 SP4
		    ■ Release 3.1
		    ■ Release 3.2
		    ■ Release 3.5
		 ■ NICE Interaction Management Release 4.1 - supported only for upgrades	

SQL Server 2008 Standard Edition 32-bit	SP1	■ NICE Perform
		    ■ Release 3.2
		    ■ Release 3.5
		 ■ NICE Interaction Management Release 4.1	

SQL Server 2008 Standard Edition 64-bit	SP1	■ NICE Perform
		    ■ Release 3.2
		    ■ Release 3.5
		 ■ NICE Interaction Management Release 4.1	

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2008 Enterprise Edition 64-bit	SP1	■ NICE Perform 　■ Release 3.2 　■ Release 3.5 ■ NICE Interaction Management Release 4.1	
SQL Server 2008 Standard Edition 32-bit	SP2	■ NICE Perform 　■ Release 3.2 　■ Release 3.5 ■ NICE Interaction Management Release 4.1	
SQL Server 2008 Standard Edition 64-bit	SP2	■ NICE Perform 　■ Release 3.2 　■ Release 3.5 ■ NICE Interaction Management Release 4.1	
SQL Server 2008 Enterprise Edition 64-bit	SP2	■ NICE Perform 　■ Release 3.2 　■ Release 3.5 ■ NICE Interaction Management Release 4.1	
SQL Server 2008 Standard Edition 32-bit	SP3	■ NICE Perform 　■ Release 3.2 　■ Release 3.5 ■ NICE Interaction Management Release 4.1	
SQL Server 2008 Standard Edition 64-bit	SP3	■ NICE Perform 　■ Release 3.2 　■ Release 3.5 ■ NICE Interaction Management Release 4.1	

Microsoft Software	Service Pack	NICE Release	Comment

SQL Server 2008 Enterprise Edition 64-bit	SP3	▪ NICE Perform
		  ▪ Release 3.2
		  ▪ Release 3.5
		▪ NICE Interaction Management Release 4.1	

SQL Server 2008 R2 Standard Edition 32-bit	SP1	▪ NICE Perform
		  ▪ Release 3.2
		  ▪ Release 3.5
		▪ NICE Interaction Management Release 4.1	

SQL Server 2008 R2 Standard Edition 64 -bit	SP1	▪ NICE Perform
		  ▪ Release 3.2
		  ▪ Release 3.5
		▪ NICE Interaction Management Release 4.1	

SQL Server 2008 R2 Enterprise Edition 64-bit	SP1	▪ NICE Perform
		  ▪ Release 3.2
		  ▪ Release 3.5
		▪ NICE Interaction Management Release 4.1	

SQL Server 2008 R2 Standard Edition 32-bit	SP2	▪ NICE Perform
		  ▪ Release 3.2
		  ▪ Release 3.5
		▪ NICE Interaction Management Release 4.1	

SQL Server 2008 R2 Standard Edition 64-bit	SP2	▪ NICE Perform
		  ▪ Release 3.2
		  ▪ Release 3.5
		▪ NICE Interaction Management Release 4.1	

Microsoft Software	Service Pack	NICE Release	Comment

SQL Server 2008 R2 Enterprise Edition 64-bit	SP2	■ NICE Perform
		  ■ Release 3.2
		  ■ Release 3.5
		■ NICE Interaction Management Release 4.1	

[This page intentionally left blank]

Microsoft Server Operating Systems

This chapter provides information regarding Microsoft Server Operating Systems. This includes secure solutions, updates, and guidelines.

Contents

Windows 2000 Update Rollup 1 for Service Pack 4

Product	Microsoft Windows 2000 Update Rollup 1 for Service Pack 4
Release	
Synopsis	

As part of NICE's continuing effort to provide its customers with a secure solution, and in accordance with our policy regarding service pack certification, NICE has certified **Microsoft Windows 2000 Update Rollup 1 for Service Pack 4.**

The Update Rollup contains:

- All security updates produced for Microsoft Windows 2000 from the time SP4 was released and up to April 30, 2005, when the contents of the Update Rollup were finalized for testing by Microsoft.
- A number of updates that help increase system security and reliability, reduce support costs, and support the current generation of PC hardware.

By including the most important updates for Microsoft Windows 2000, the Update Rollup makes it easier for customers to improve security of Microsoft Windows 2000 systems, keep these systems up to date, and build new deployment images.

Because the number of updates included in the Update Rollup is significantly lower than the number typically included in a service pack, and because Microsoft has already released most of the contents included in the Update Rollup as individual updates and hotfixes, the Update Rollup should require less pre-deployment testing and planning.

Individual hotfixes made since SP4, but not included in the Update Rollup, remain available as individual downloads.

No Future Service Packs

Microsoft believes the Update Rollup meets customer needs more effectively and with less disruption than a new service pack, and there will be no Service Pack 5 (SP5) for Microsoft Windows 2000. SP4 becomes the final service pack for Microsoft Windows 2000.

For details about **Microsoft Windows 2000 Update Rollup 1 for Service Pack 4,** see:

http://support.microsoft.com/default.aspx/kb/891861

> **NOTE:** Teknor PC based Renaissance systems are currently not certified for Microsoft Windows 2000 Update Rollup 1 for Service Pack 4.

For More information, please contact NICE.

Windows Server 2003 Service Pack 2 NICE Product Support

Product	Microsoft Windows Server 2003 Service Pack 2 Support
Release	
Synopsis	This section provides information about NICE support for Microsoft Windows Server 2003 R2, Service Pack 2.

Overview

This section provides information regarding NICE products support for Microsoft Windows Server 2003, Service Pack (SP2).

> **Important!**
> - All NICE servers must be installed with Microsoft Windows Server 2003 SP2.
> - All clients must be installed with .Net 2.0 (side-by-side or pure), as Microsoft has a known issue in Net 1.1 with Microsoft Windows Server 2003 SP2.
> - On computers that have .Net2.0, serialization HF (KB914460) must be installed.
> - On Microsoft Windows Server 2003 SP2, only the NICE Perform versions that support .Net 2.0 can be installed. This is relevant for servers and the workstations. See TN0736: NICE Product Support for Microsoft .Net3.0.

Server Side

No.	Release Version	Status
		OK
	NICE Perform RI (from SP7)	OK (See **Limitations** on page 41**)**
	NICE Perform RII (from SP4)	OK (See **Limitations** on page 41**)**
	NICE Perform 9.09	OK
	NICE Perform R3	OK (See **Limitations** on page 41**)**
	NICE Perform R3.1	OK
	NICE Perform R3.2	OK

No.	Release Version	Status
	NICE Perform R3.5	OK
	NICE Interaction Management R4.1	For upgrades only

Windows Server 2003 Service Pack 2 Installation Procedure

Before You Begin

Before installation, check via **My computer > Properties** that the server is installed with Microsoft Windows Server 2003, SP1, and not with Microsoft Windows Server 2003 SP2.

Figure 3-1: System Properties - General Tab
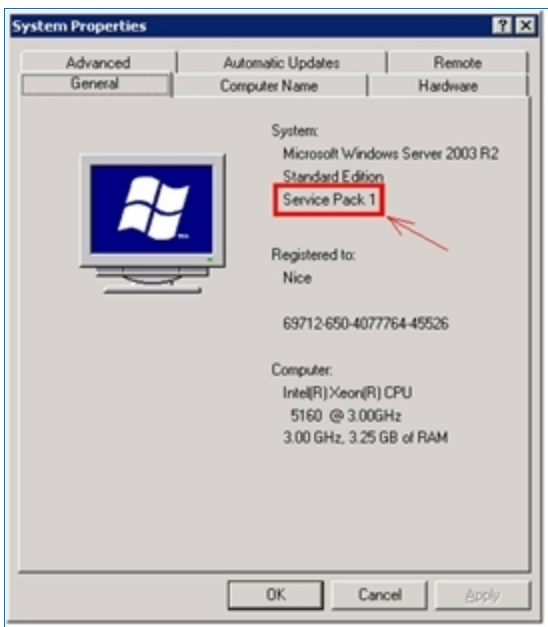
For Loggers only: Verify that the status of the Distributed Transaction Coordinator service is started. If it is not, then you must start it before running the SP installation.

Figure 3-2: Services Window
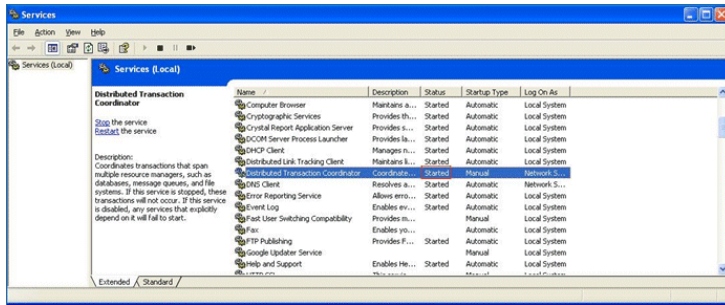
 To install Microsoft Windows Server 2003 SP2:

1. Run **Windows Server 2003 SP2 .exe** file.

   Figure 3-3: Software Update Installation Wizard Window
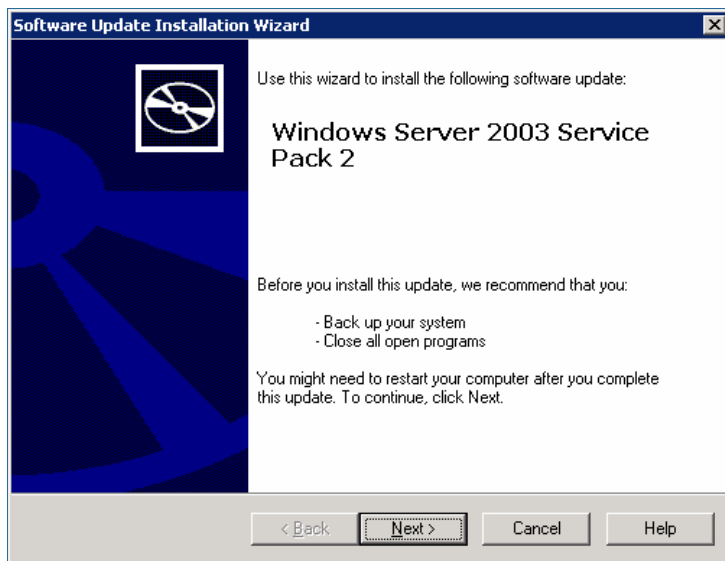
2. Click **Next**.

Figure 3-4: License Agreement
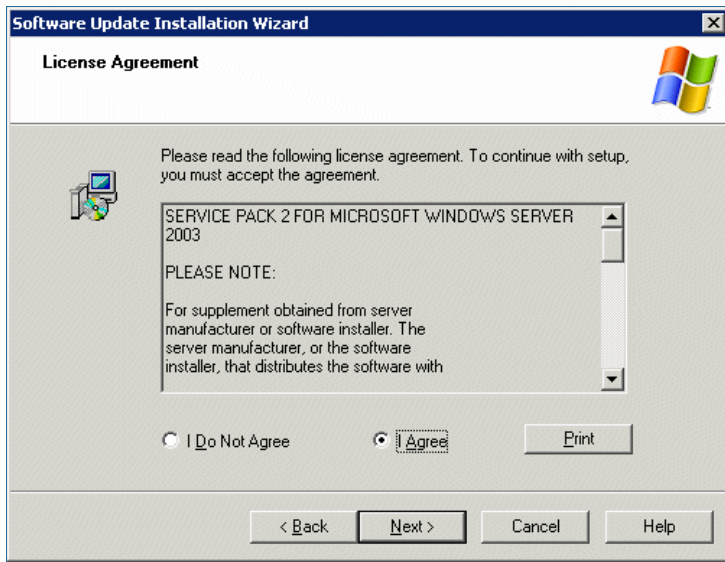
3. Select **I agree,** and click **Next**.

Figure 3-5: Select Options Window
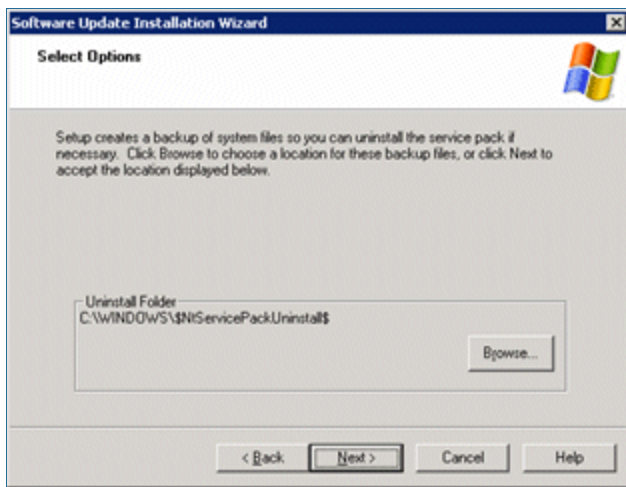
4. Click **Next**.

Figure 3-6: License Agreement Window
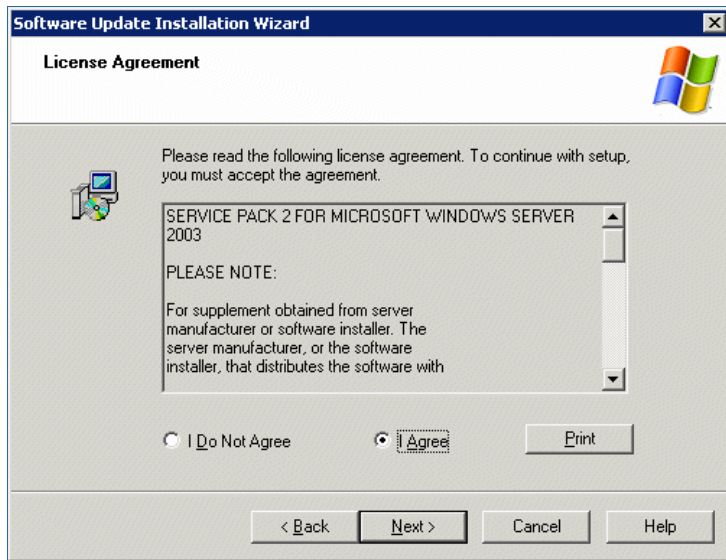
5.   Click **Finish** to complete the installation.

The server reboots.

Limitations

■   Recording On demand (ROD) Desktop will not work if a client has .Net1.1 side by side with
.Net2.0, and if the servers are installed with Microsoft Windows Server 2003, SP2.

■   If ROD Desktop is needed and the clients have .Net1.1 side by side with .Net2.0, please contact
NICE Customer Support.

■   If the client has .Net2.0 pure, then the ROD desktop will function properly.

■   For new ScreenSense server installations on top of NICE Perform Release II SP4 and NICE
Perform Release 3 SP2, a new .msi installation file is available in the HF directory. The
ScreenSense server must be installed from this file.

Windows Server 2003 Service Pack 1 Integration with NICE Servers

Product	Microsoft Windows Server 2003 Service Pack 1 Integration with NICE Servers
Release	
Synopsis	

As part of NICE's continuous effort to provide its customers with a secure solution, and in accordance with our policy regarding service pack certification, NICE has certified Microsoft Windows Server 2003 Service Pack 1. Microsoft Windows Server 2003 Service Pack 1 provides advanced and significant security features, including a built-in firewall, an improved IIS security mechanism, program signature validation, thus further enhancing NICE's secure platform.

For details about Microsoft Windows Server 2003 Service Pack 1, see
http://support.microsoft.com/default.aspx/kb/889101.

This section provides instructions for installing and configuring Microsoft Windows Server 2003 Service Pack 1 for NICE Servers running Microsoft Windows Server 2003 Standard or Appliance edition.

> **NOTE:** The procedures described in this section can be used for NICE Servers running NICE Perform.

Overview

This section provides guidelines for installing and configuring Microsoft Windows Server 2003 Service Pack 1 on NICE Servers.

Microsoft Windows Server 2003 Service Pack 1 provides the following enhanced security features:

- ▪ A built-in firewall
- ▪ Enhanced security for Internet Explorer
- ▪ Checks for a valid signature of programs during installation

By default, a firewall closes all ports to incoming network packets. This section explains how to open a port permanently (known as statically opened ports), and to define specific applications for which the firewall will open the necessary listening ports. These listening ports will remain open only when, and as long as, these applications are running (known as dynamically opened ports).

This section provides instructions for installing Microsoft Windows Server 2003 Service Pack 1 on NICE Servers, and describes how to security-tune your servers so that full-functionality of the system is obtained. Security-tuning is performed in the Windows Firewall.

> **NOTE:** After you complete security-tuning NICE components, we recommend that you monitor all recording components at the site to ensure that they are running properly.

Known Issues and Limitations

- ISA Logger version 8.9 does not support Windows 2003 SP1.

- NICE SNMP Manager 8.8/9.01 does not support Windows 2003 SP1.

- Audio Manager running on NICE CLS 8.9 will not function properly after installing Windows 2003 SP1. This means that Executive Connect and /or Playback via Turret (PVT) will not work. For additional information contact NICE regarding installing Microsoft Windows Server 2003 Service Pack 1.

Installing Windows Server 2003 Service Pack 1 on NICE Servers

> **Important!**
>
> Before installing Microsoft Windows Server 2003 Service Pack 1, close NICE applications and stop all NICE services.

If there is enough space on Disk C, go directly to **Running the Microsoft Windows Server 2003 Service Pack 1 Setup** on page 49.

If there is not enough space on Disk C for SP installation, perform all the following steps.

- **Moving Unused Files - NiceLog Loggers** below.

- **Moving Log Files - NiceCLS Servers** on the next page.

- **Running the Disk Cleanup Wizard** on page 46.

- **Copying the Service Pack 1 Installation File** on page 48.

- **Running the Microsoft Windows Server 2003 Service Pack 1 Setup** on page 49.

Moving Unused Files - NiceLog Loggers

This procedure must be performed for NiceLog Logger Versions 8.9 and 9.0.

◆ To move the unused files:

- Move the installation files from Drive C: (usually found in C:\installs\i386) to Drive D: (the root folder).

Figure 3-7: Installs Folder
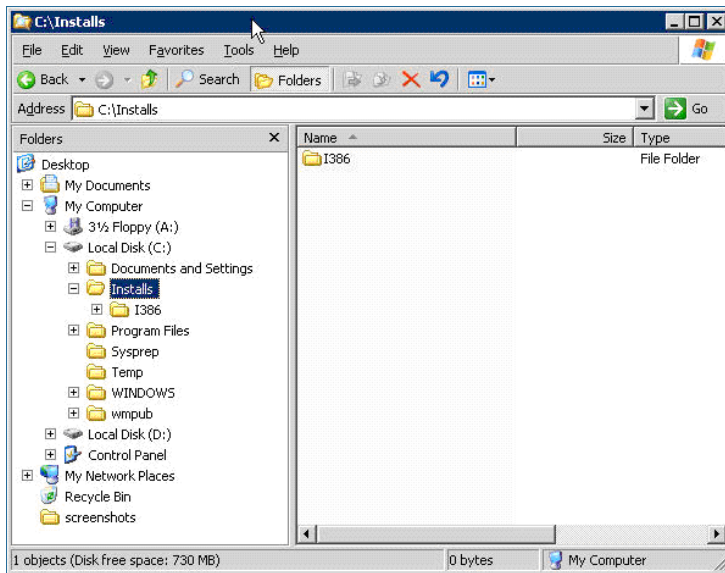
Moving Log Files - NiceCLS Servers

This section describes how to move the NiceCLS log files from Drive C: to Drive D:. This procedure must be performed for machines running NiceCLS Version 8.9.

❖ **To move the log files:**

1. In Drive D:, create the following folder: **D:\NICECTI\Log.**

Figure 3-8: \Log Folder
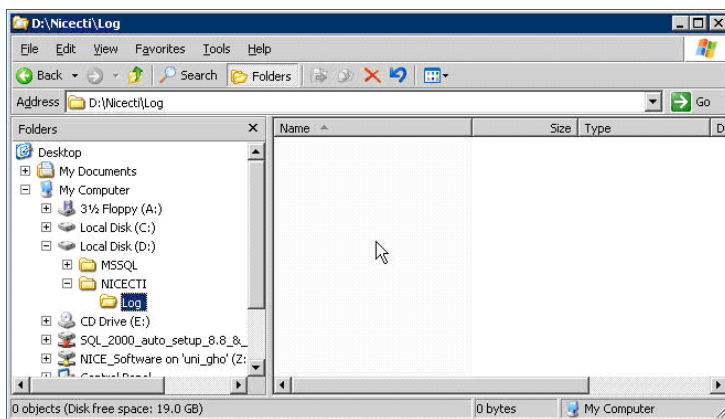
2. From the **Start** menu, select **Run** > **Regedit**.

3. Navigate to the following Registry key:

   HKLM\SOFTWARE\NICECTI\SYSTEM\LOG_DLL

Figure 3-9: Registry Editor
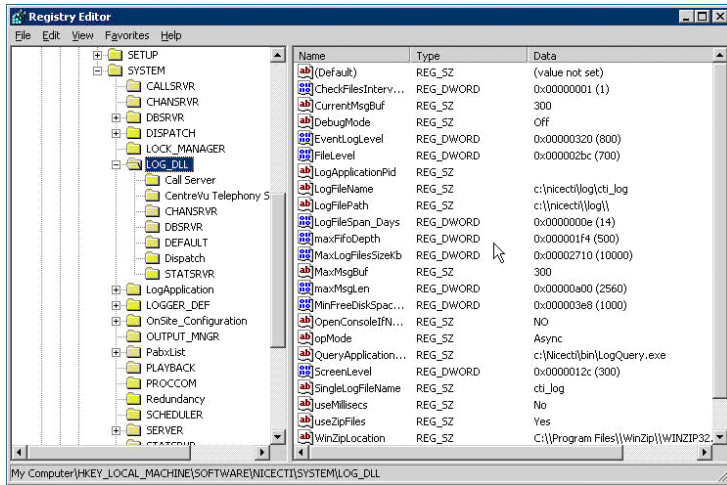
4. Set the value of LogFilePath as shown below:

Figure 3-10: LogFilePath
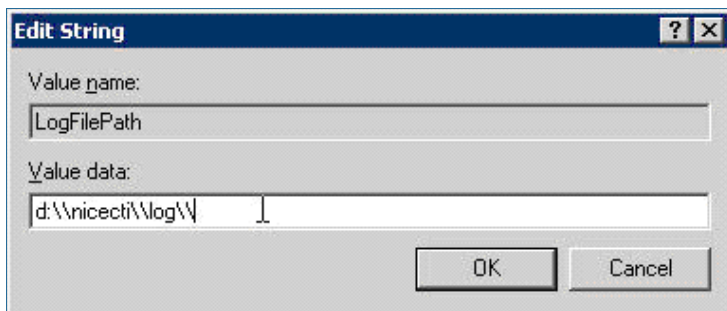
5. Click **OK**.

6. Set the value of LogFileName as shown below:

Figure 3-11: LogFileName
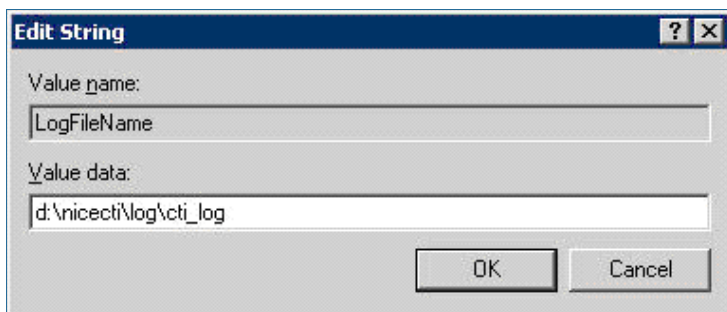
7. Click **OK**.

Running the Disk Cleanup Wizard

◆ <u>To run the Disk Cleanup wizard:</u>

1. Double-click **My Computer.**

2. Right-click on **Drive C:** and select **Properties**. The Local Disk Properties window appears.

Figure 3-12: My Computer
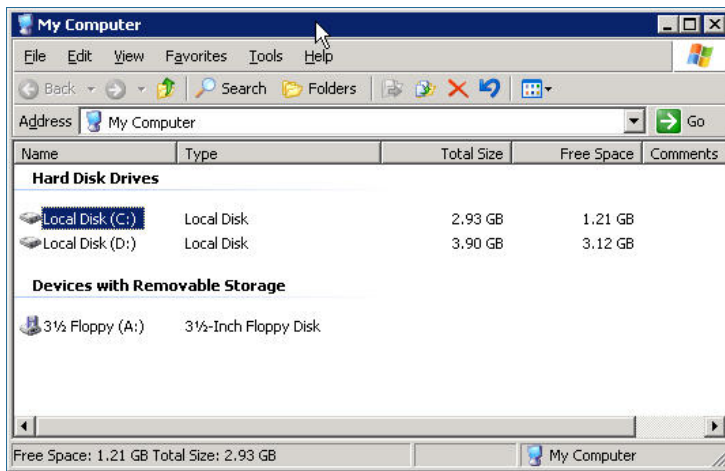
Figure 3-13: Local Disk (C): Properties Window
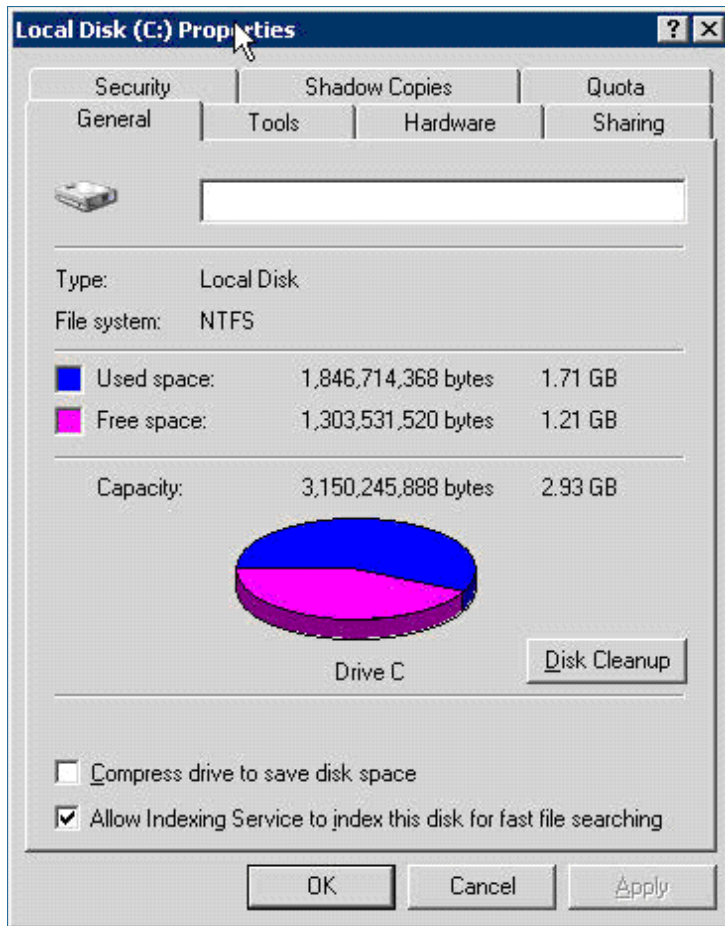
3. Click **Disk Cleanup**. In the Files to delete list, select all the files on the list. See Figure Figure 3-14.

Figure 3-14: Disk Cleanup for Drive C: Window
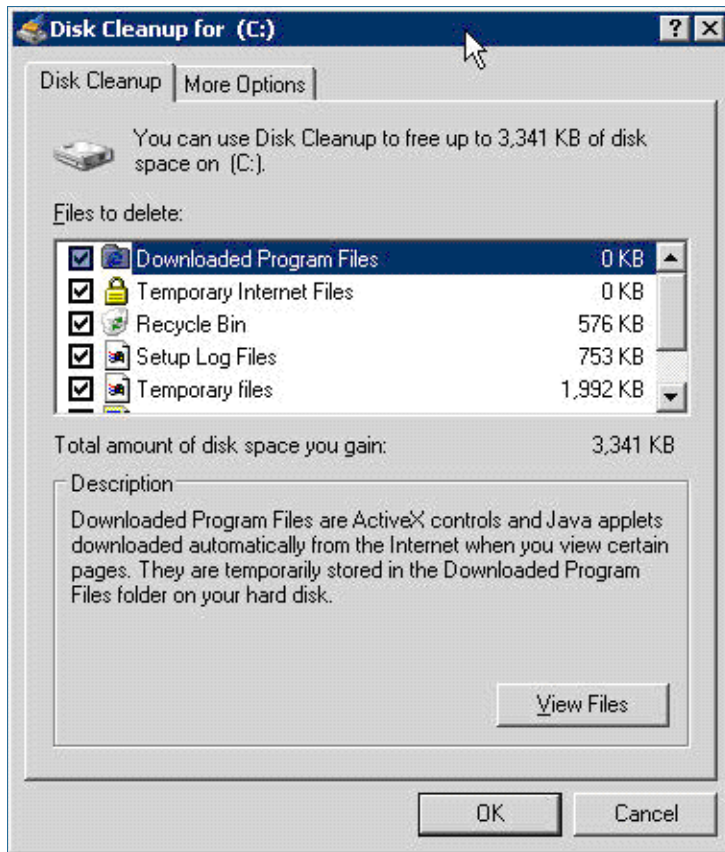
4. Click **OK**. Disk Cleanup will clean all the selected files.

Copying the Service Pack 1 Installation File

> ❗ IMPORTANT
>
> Since Windows Setup is generally extracted to the default drive (Drive C:), you must copy and execute the setup file from Drive D:.

◈ **To copy the Service Pack 1 installation file:**

▪ Copy the Service Pack 1 installation file to Drive D:. See Figure 3-15.

3: Microsoft Server Operating Systems

Installing Windows Server 2003 Service Pack 1 on NICE Servers

Figure 3-15: :\SP1 Folder
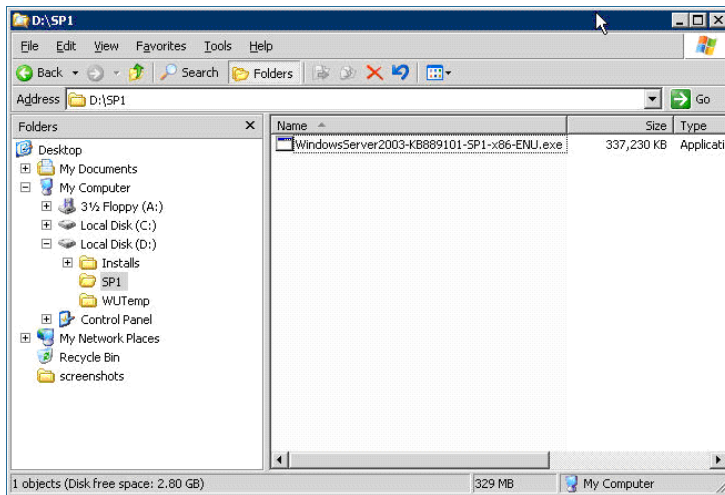
Running the Microsoft Windows Server 2003 Service Pack 1 Setup

To run the Microsoft Windows Server 2003 Service Pack 1 setup:

1. Double-click **WindowsServer2003-KB889101-SP1-x86-ENU.exe.**

   The file will be extracted to Drive D:. The Windows Server 2003 Service Pack 1 Setup wizard starts.

Figure 3-16: Windows Server 2003 Service Pack 1 Setup Wizard

2. Click **Next**. The License Agreement window appears.

Figure 3-17: Windows Server 2003 Service Pack 1 Setup Wizard - License Agreement
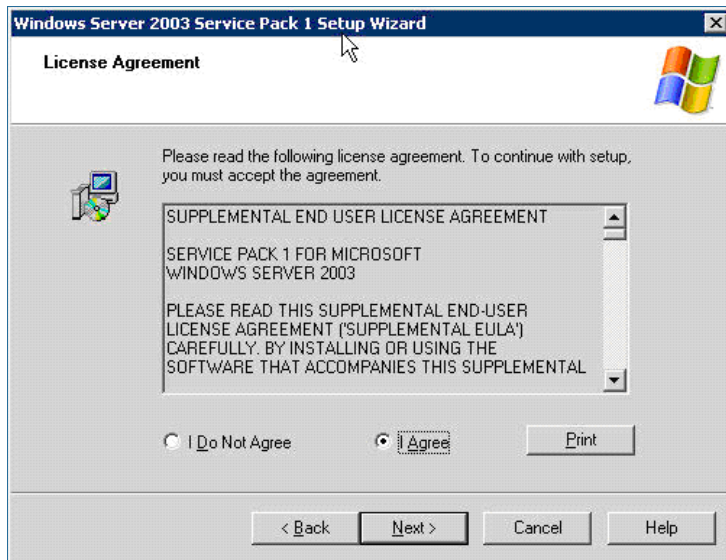
3. Select **I Agree** and click **Next**. The Windows Select Options window appears.

Figure 3-18: Select Options Window
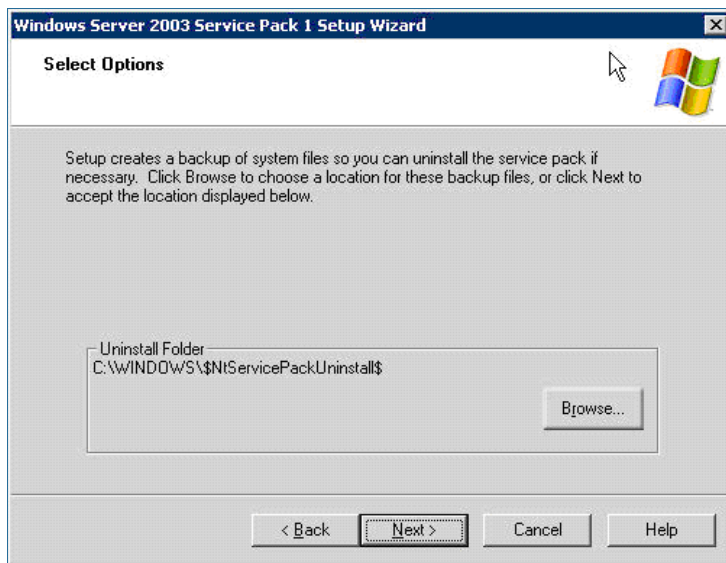
4. Click **Browse** and select Drive D. Click **OK**. The Select Options window will now appear as shown below.

Figure 3-19: Select Options Window
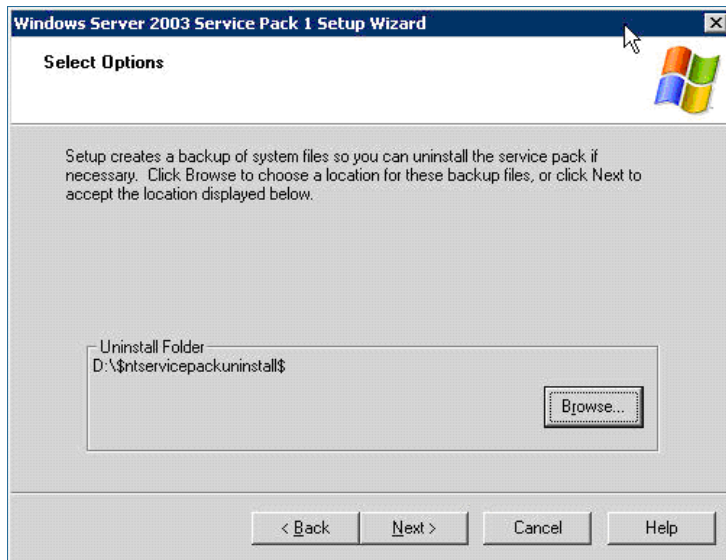
> 📄 **NOTE:** If you have enough space on Disk C for SP installation (and you skipped the previous steps for moving to Disk D) leave the default path for uninstall folder - **C:\WINDOWS\$NtServicePackUninstall$**.

5. Click **Next**. The installation process starts. When the installation is complete, the Complete window appears.

Figure 3-20: Select Options - Complete Window
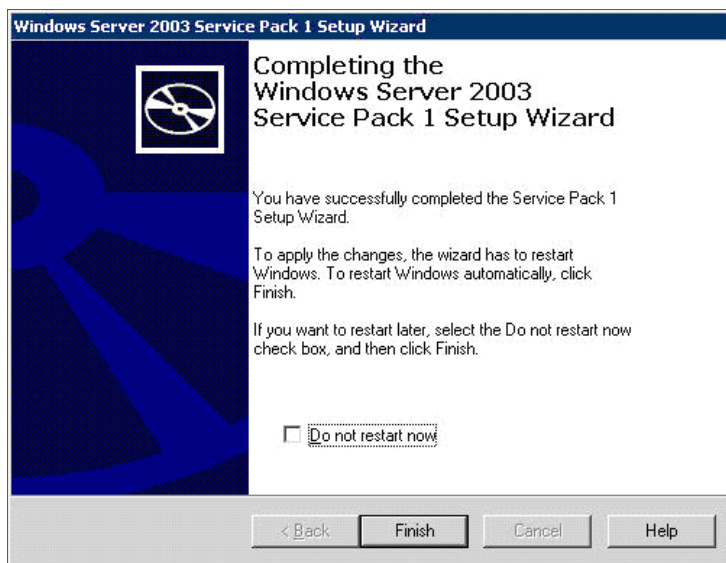
6. Click **Finish**. Your server will now restart.

> 📝 **NOTE:** The restart process will take a bit longer than usual.

Security-Tuning Your System

Security-tuning your system involves:

- **Enabling the Windows Firewall Service** below.
- **Opening Ports** below.
- **Adding Applications to the Exceptions List** on page 55.
- **Activating the Windows Firewall** on page 56.

Enabling the Windows Firewall Service

After you install Microsoft Windows Server 2003 Service Pack 1, it is possible to enable the Windows Firewall service.

◆ To enable the Windows Firewall service:

1. Open the **Control Panel** and double-click **Windows Firewall**. The following message appears.

   Figure 3-21: Windows Firewall Message
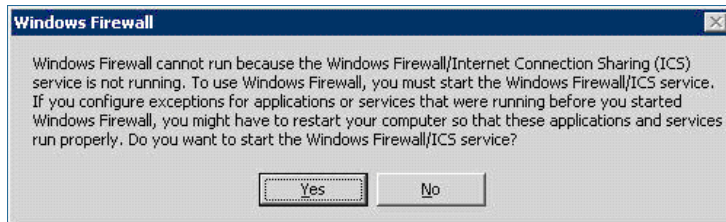
2. Click **Yes** and close the Windows Firewall application. The Windows Firewall service is now enabled, however, the Windows Firewall is not active yet.

Opening Ports

◆ To add ports to the firewall:

1. From the **Start** menu, select **Settings > Control Panel > Windows Firewall**.

   The Windows Firewall window appears.

Figure 3-22: Windows Firewall Window
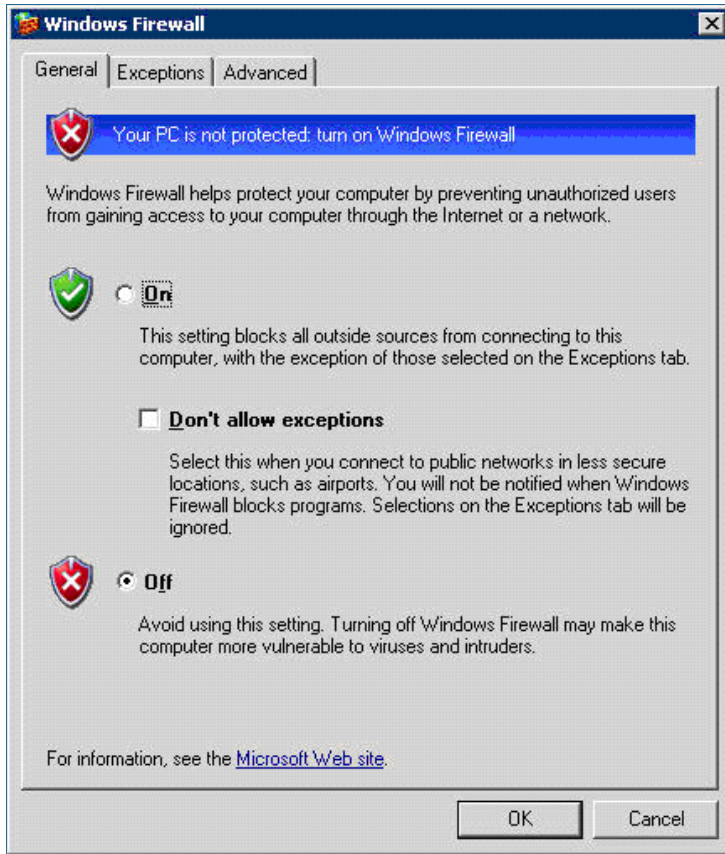
> NOTE: The Windows Firewall is still not set to On. Do not set it to On yet!

2. Click the **Exceptions** tab.

Figure 3-23: Windows Firewall Window - Exceptions Tab
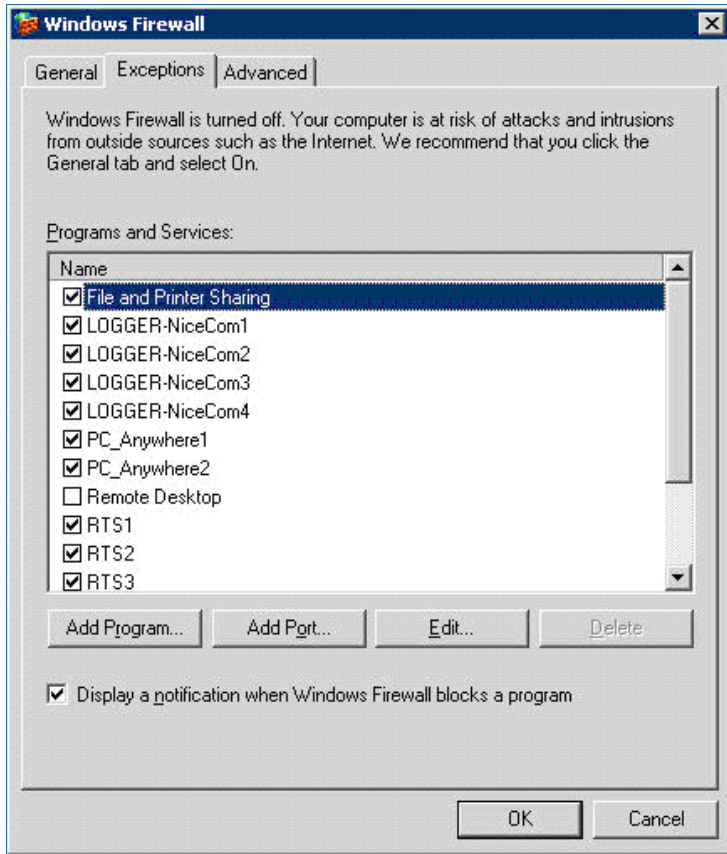
> 🔲 **NOTE:** Ensure that Display a notification when Windows Firewall blocks a
> program is selected.

3. Click **Add Port**. The Add a Port window appears.

Figure 3-24: Add a Port Window
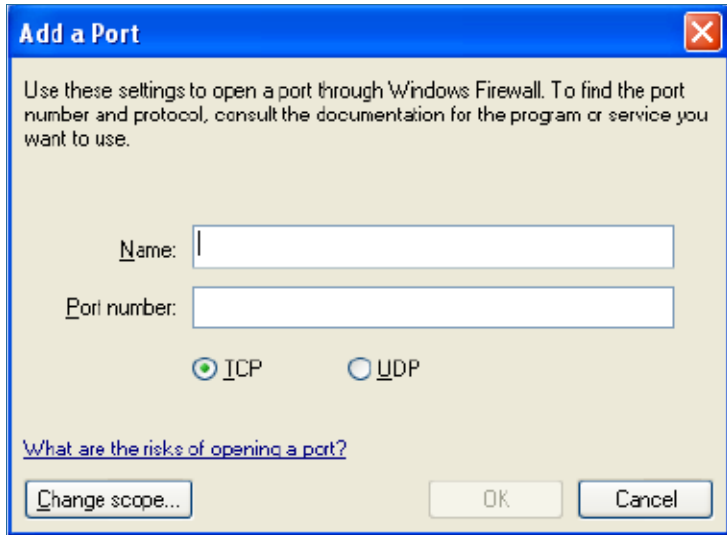
4. Referring to **Network Usage by NICE Systems** on the next page, add the port and click **OK**. Repeat this step for all NICE ports.

Adding Applications to the Exceptions List

When certain applications run for the first time, a warning message may appear asking if you want to unblock the application. Clicking Unblock will add the application to the firewall Exceptions List, enabling you to run the application.

◆ **To add an application to the Exceptions list:**

1. **Start** the NICE Server and **run** all system modules. The following Windows Security Alert may appear.

Figure 3-25: Windows Security Alert (Example)

2. Click **Unblock**. The application is added to the Exceptions list.

Activating the Windows Firewall

After you complete adding all exceptions to the Windows Firewall, the Windows Firewall must be activated.

◆ To activate the Windows Firewall:

1. In the Control Panel, double-click **Windows Firewall**. The Windows Firewall opens.

2. Click the **General** tab.

   Figure 3-26: Windows Firewall - General Tab
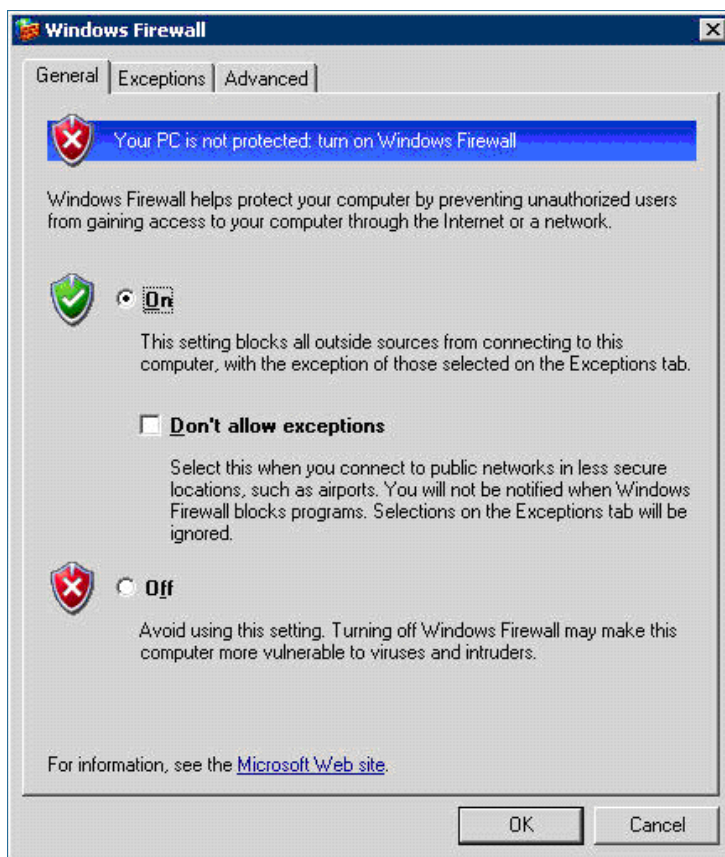
3. Select **On** and click **OK**. The Window Firewall is now active.

Network Usage by NICE Systems

Following are general comments regarding network usage by the system:

- The port used by the CAPI can be configured on both the NiceCLS side and the application side. Changes can be done from the registry. Certain drivers use the CAPI in order to communicate with the Call Server. In these cases you must change the port number in the driver too. All those mentioned configurations are configured from the Registry.

- Ports 161,162, 6665 are used between system components (UDP) for Nice SNMP service (NICE Supervision SNMP and/or Unicenter SNMP).

- Most internal server-server and client-server communication in the system is done through the Nicecomm layer. Nicecomm is limited to a maximum of 50 connections on the same port.

> **NOTE:**
>
> - The Integration (driver) may require opening a specific port(s) in order to communicate with the CTI server
>
> - The ports used by pcAnywhere are as follows:
>   - pcAnywhere 10.x and up: TCP 5631, TCP 5632
>   - pcAnywhere down from 10.x: TCP 65301, TCP 22

TCP/UDP Ports Used by NICE Servers Version 8.9

NiceCLS ServerServer Side

Table 3-1:
TCP/UDP Ports Used by NiceCLS Server

Port	Used By
TCP	
2050	CAPI (Can be configured to use other ports as well.)
1433	Database
UDP	
2005	Status Server
2002	Output manager
4387	Lock manager
34462	Lock manager

NiceLog Voice Logger

Table 3-2:
TCP/UDP Ports Used by NiceLog Voice Logger

Port	Used By
TCP	
2011	NiceCom
TCP	
2001	NiceCom
UDP	
2000	Nicecom
2012	

NiceScreen Logger

Table 3-3:
TCP/UDP Ports Used by NiceScreen Logger

Port	Used By
TCP	
2102	Nicecom
2152	Nicecom
TCP (Citrix Environment)	
3020>3020+n	n=number of agents
UDP	
2101	

RTS (Remote Tape Server)

Table 3-4:
TCP/UDP Ports Used by RTS

Port	Used By
TCP	
3001	
3002	
UDP	
3011	
3012	

Media Library

Table 3-5:
TCP/UDP Ports Used by Media Library

Port	Used By
UDP	
2000	

Printer Server

Table 3-6:
TCP/UDP Ports Used by Printer Server

Port	Used By
UDP	
2006	

Application Web Server

Table 3-7:
TCP/UDP Ports Used by Application Web Server

Port	Used By	Comment
TCP		
80		(HTTP)
8080		(HTTP)

Storage Center

Table 3-8:
TCP/UDP Ports Used by Storage Center

Port	Used By
TCP	
7200	

TCP/UDP Ports Used by NICE Servers Version 9

Web Applications Center

Table 3-9:
TCP/UDP Ports Used by the Web Applications Center

Port in 9.0	Used By	Comments
TCP		
80	WebServer	
8080	WebServer	
62070	User Admin	
62070	System Admin	
62071	Audit Trail	
62072	Rule Manager	

Port in 9.0	Used By	Comments
62073	Locate Service	
62074	Unified Query	
62075	Monitor	
62076	Playback Media Server	
62077	Playback resource manager	
62078	Playback media service	
62079	Rule engine	
62080	Coaching	
62081	My Universe	
62082	Call Flow Analysis	

Unicenter SNMP Manager

Table 3-10:
TCP/UDP Ports Used by Unicenter SNMP Manager

Port in 9.0	Used By	Comments
UDP		
161	UniCenter SNMP Manager	

NiceLog Logger

Table 3-11:
TCP/UDP Ports Used by NiceLog Logger Version 9

Port in 9.0	Used By	Comments
TCP		
2001	NiceLog Logger	

Port in 9.0	Used By	Comments
2011	NiceLog Logger	
UDP		
2000	NiceLog Logger	
2012	NiceLog Logger	

NiceScreen

Table 3-12:
TCP/UDP Ports Used by NiceScreen

Port in 9.0	Used By	Comments
TCP		
2001, 2102	Screen Agent for desktop	
3020	Screen Agent for terminal server	
30100	MML	
UDP		
30102	MML	

NICE Playback Server

Table 3-13:
TCP/UDP Ports Used by NICE Playback Server

Port in 9.0	Used By	Comments
TCP		
8000 -8003	PBS Link	
8010	PBS Link	

NICE Storage Center

Table 3-14:
TCP/UDP Ports Used by NICE Storage Center

Port in 9.0	Used By	Comments
TCP		
30002-30004	Storage Center	

NICE Interaction Center

Table 3-15:
TCP/UDP Ports Used by NICE Interaction Center

Port in 9.0	Used By	Comments
TCP		
62050,62051	Call Server	
62059	SNMP	
62060	Dispatch	Used by the SNMP logic
62061	Scheduler	Used by the SNMP logic
62069	RCM	

Database Server

Table 3-16:
TCP/UDP Ports Used by the Database Server

Port in 9.0	Used By	Comments
TCP		
1433	SQL Server	

Microsoft Windows Server 2003 Appliance Edition

Product	Microsoft Windows Server 2003 Appliance Edition
Release	
Synopsis	Commencing April 2005, the operating system configuration for NiceLog and Interaction Capture Unit product lines is changing from Microsoft Windows Server 2003 Standard Edition to Microsoft Windows Server 2003 Appliance Edition.

Microsoft Windows Server 2003 Appliance Edition is a joint venture of Nice Systems and Microsoft as part of our OEM membership. This now provides an optimized operating system for NiceLog logger and the Interaction Capture Unit based upon Microsoft Windows Server 2003 technology and is especially designed to address the different performance needs of our capturing platform.

Additionally Microsoft Windows Server 2003 Appliance Edition makes redundant the different services and operating system resources which are not being used by the recording platform. This will provide better performance on the one hand and enhanced security on the other hand, by disabling different components which are not being used and may be a potential for security breach.

Microsoft Windows Server 2003 Appliance Edition FAQ

Q: For which NICE server is Microsoft Windows Server 2003 Appliance Edition suitable?

A: Microsoft Windows Server 2003 Appliance Edition is suitable for NiceLog Loggers and the Interaction Capture Unit (as part of NICE Perform).

Q: Why is Microsoft Windows Server 2003 Appliance Edition is suitable only for NiceLog Logger and Interaction capture unit?

A: The reason is related to the fact that all other system components are a S/W only solution and the operating system is provided by the customer.

Q: Is there a special price for NiceLog Logger with Microsoft Windows Server 2003 Appliance Edition.

A: No. As from the official announcement every NiceLog Logger and Interaction Capture Unit will be shipped with Microsoft Windows Server 2003 Appliance Edition as default.

Q: Does the fact that I'm using Microsoft Windows Server 2003 Appliance Edition on the NiceLog Logger affects in any way Microsoft security patches and service pack related issues.

A: No. Microsoft Windows Server 2003 Appliance Edition has no affect on any MS security patches and service pack related issues. The list of certified MS security patches and service packs is available on the ExtraNICE and being updated constantly.

Q: Where can I buy a copy of Microsoft Windows Server 2003 Appliance Edition?

A: Microsoft Windows Server 2003 Appliance Edition is not available for a public use. Only Nice Systems is authorized to provide a copy and licensing of this Microsoft Windows edition.

Q: Does Microsoft Windows Server 2003 Appliance Edition affect in any way Nice Systems language support?

A: Microsoft Windows Server 2003 Appliance Edition is transparent from an end user standpoint.

Q: Is the Microsoft Windows Server 2003 Appliance Edition suitable for the 8.9 ISA based NiceLog Logger or just to the PCI?

A: Microsoft Windows Server 2003 Appliance Edition is applicable for both ISA and PCI based NiceLog Logger.

Overview

From April 2005, an Image CD (Ghost) will be shipped with each NICE High Density Logger, NICE Interaction Capture Unit or Nicelog version 8.9 ISA, instead of Microsoft Windows Server 2003 installation CDs.

This Image CD (Ghost) can also be used to recover the logger in a case of a crisis on site

> ❗ **Important!**
>
> ▪ This Image CD (Ghost) is for use only with systems sent from April 2005.
>
> ▪ The installation will only function properly with CPUs shipped after April 2005, otherwise you may be prompted to replace your CPU.
>
> ▪ See below to verify if your CPU version is approved, if not it will be necessary replace your CPU.
>
> **Figure 3-27: NICE CPU Verification Tool**
>
>
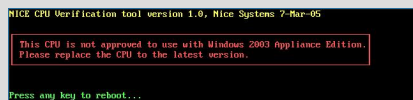
Each shipment includes the following items:

▪ 1 x 1.44 MB Bootable diskette:

Label: Windows Server 2003 Appliance Recovery – Network Installation Diskette.

▪ 2 x Image CD (Ghost):

Label: Image CD for PCI Logger / ICU / ISA Logger 8.9 W2K3 Appliance (CD # 1 of 2).

Label: Image CD for PCI Logger / ICU / ISA Logger 8.9 W2K3 Appliance (CD # 2 of 2).

▪ 1 x Windows installation files CD.

Label: MS Installation files for W2K3 Appliance edition (I386).

> 📝 **NOTE:** This CD contains Windows installation files for further installation.

Recovering the Logger

There are several options to recover the Logger:

- **Replacing the Failed HDD with a Preloaded HDD** below (Most recommended option).
- **Installing the Image CD (Ghost) from a Logger DVD Device** on the facing page.
- **Installing the Image CD (Ghost) from a Workstation** on page 70.

Replacing the Failed HDD with a Preloaded HDD

◆ To Replace the Failed HDD with a Preloaded HDD

NICE Systems Ltd. recommends ordering a preloaded HDD for fast replacement at the site. Each preloaded HDD is compatible to a specific platform
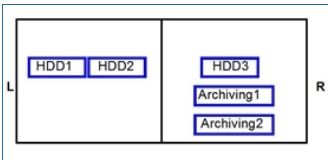
Platform	Preloaded HDD
NICE High Density Logger v9.0	36GB or 72GB SCSI HDD
NICE Interaction Capture Unit	250GB IDE HDD
NiceLog Logger ISA 8.9	36GB or 72GB SCSI HDD

- Contact support@nice.com to order this preloaded HDD.

Installation Notes

- The preloaded HDD contains the Windows application only.
- After the installation, you will need to install the Logger S/W from the CDs you received with your system.
- Where there are two or more HDDs installed, the master HDD is HDD1

Table 3-17: NiceLog Storage Device Configuration

Configuration	Description
Up to three hard drives and up to two archiving devices 	Hard drive assembly: from ID.0 to ID.2. 1st HDD ID 0 2nd HDD (optional): ID 1 3rd HDD (optional): ID 2 Archiving device assembly: 1st Device (optional): ID 6 (SCSI)/Master (IDE) 2nd Device (optional): ID 5 (SCSI)/Master (IDE)

- After replacing the HDD, Found New Hardware message boxes will appear, click **Cancel** on all message boxes.

  Continue installing the NICE S/W according to Installing the NiceLog High Density Logger Software installation manuals for versions 8.9 and 9.0 on the ExtraNICE.

- After the NICE S/W Installation is completed, all Found New Hardware message boxes will disappear.

- For RAID devices see NICE High Density Logger Hardware Guide (PCI Loggers) and Nice Technical Reference Guide-Short Term Storage Devices (ISA Loggers). Replace the faulty HDD with a regular HDD (not preloaded HDD) and rebuild your HDD from the RAID device.

Installing the Image CD (Ghost) from a Logger DVD Device

> **NOTE:** Where there is a faulty HDD, replace this HDD before installing the Image CD (Ghost).

◆ To Install the Image CD (Ghost) Installation from a DVD Device:

1. Configure the BIOS Boot Sequence to startup from the DVD device. (From the BIOS: **BIOS FEATURES SETUP > BOOT SEQUENCE)**.

2. Insert the 1st CD installation Image CD (Ghost) [Label – Image CD for PCI Logger / ICU / ISA Logger 8.9 W2K3 Appliance (CD # 1 of 2)] into the DVD device.

3. **Reboot** the system.

4. From the **Microsoft Windows 98 Startup Menu** select **1 (NICE Products Images…)** and press **Enter**.

   Figure 3-28: Microsoft Windows 98 Startup Menu
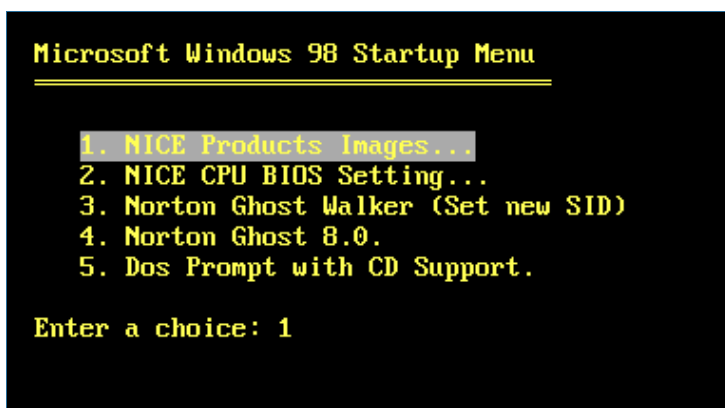
> **❗ Important!**
>
> Use only menu options that are specifically mentioned! (The other options are for NICE Engineers only.)

5. From the next screen, select machine type (NiceLog PCI / ICU / NiceLog ISA 8.9) and press **Enter**.

Figure 3-29: Microsoft Windows 98 Startup Menu

6. The Image CD (Ghost) will start running automatically.

7. Wait for prompt and then replace the second CD [Label – Image CD for PCI Logger / ICU / ISA Logger 8.9 W2K3 Appliance (CD # 2 of 2)].

8. Select **OK** with the arrow buttons and press **Enter**.

◆ To Restore BIOS Factory Settings:

1. Insert the 1st CD installation Image CD (Ghost) [Label – Image CD for PCI Logger / ICU / ISA Logger 8.9 W2K3 Appliance (CD # 1 of 2)] to the DVD device.

2. From the **Microsoft Windows 98 Startup Menu** select **2 (NICE CPU BIOS Settings…)** and press **Enter.**

Figure 3-30: Microsoft Windows 98 Startup Menu
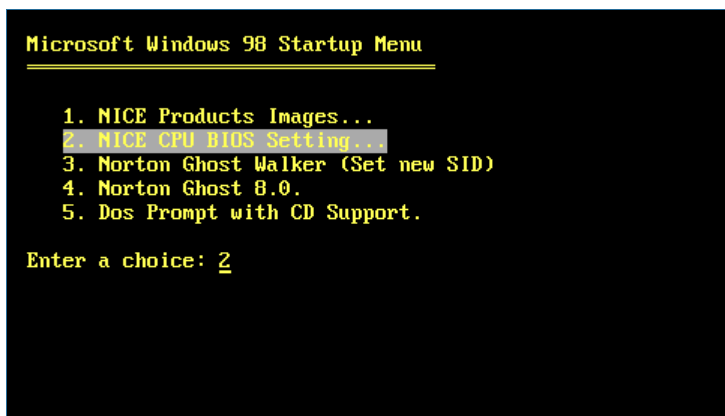
3. From the next screen, select machine CPU type (NiceLog PCI /ICU /ISA 8.9) and press **Enter**. This will restore the BIOS factory settings.

Figure 3-31: Microsoft Windows 98 Startup Menu

NICE S/W Installation

Configure the IP address and the computer name according to your network identification.

You must create the **E** partition on the HDD accordingly.

◈ To create a partition:

1. Right-click **My Computer**, select **Manage**.

2. Select **Computer management (Local) > Storage > Disk Management.**

3. Right-click the **third partition** and select **New Partition** from the drop down context menu.

Figure 3-32: Disk Management
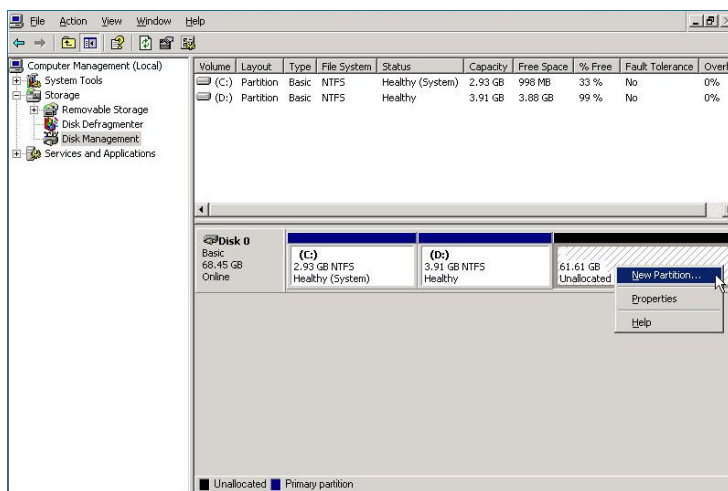
4. From the New Partition Wizard, select **Next** (keeping the default settings) until you open the Format Partition window.

Figure 3-33: New Partition Wizard
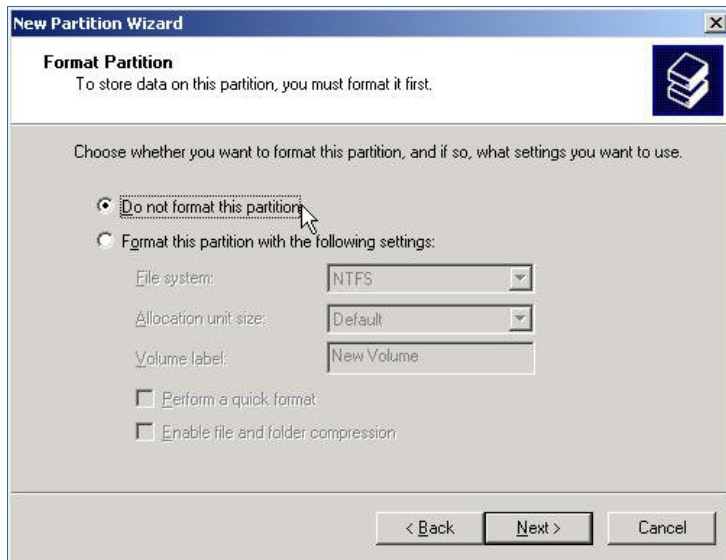
5.   Ensure that **Do not format this partiton** checkbox is marked and complete the Wizard.

6.   Continue installing NICE S/W, see Installing the NiceLog High Density Logger Software installation manuals for versions 8.9 and 9.0 on the ExtraNICE.

7.   After the NICE S/W installation is completed, all Found New Hardware message boxes will disappear.

Installing the Image CD (Ghost) from a Workstation

> **NOTE:** Where there is a faulty HDD, replace this HDD before installing the Image CD (Ghost).

◆ To Check for Workstation NetBIOS configuration:

1.   Click **Start > Settings > Network and Dial-up Connections.**

2.   Right-click the **Local Area Connection** icon, and click **Properties**.

Figure 3-34: Check for Workstation NetBIOS Configuration
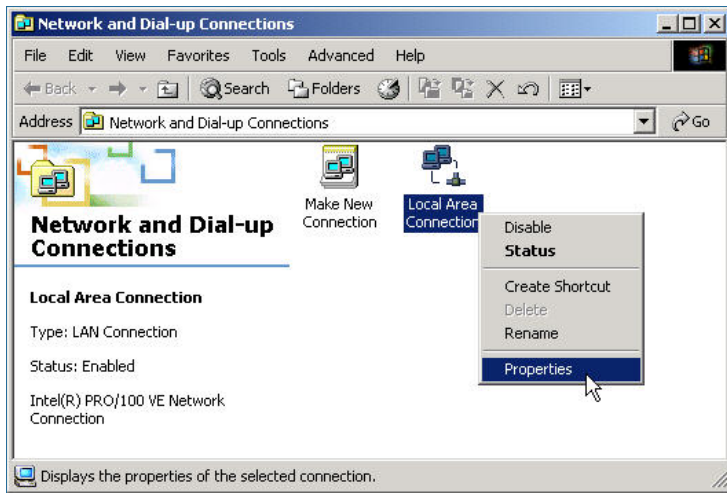
3. From the **Local Area Connection Properties** window, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 3-35: Local Area Connection Properties Window
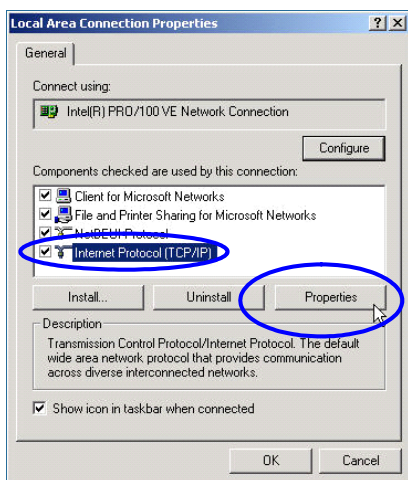
The Internet Protocol (TCP/IP) Properties window opens.

4. Click **Advanced** to reach the **Advanced TCP/IP Settings** window.

Figure 3-36: Internet Protocol (TCP/IP) Properties Window
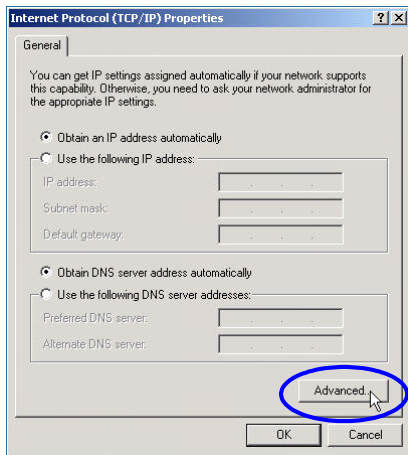
5. From the **Advanced TCP/IP Settings** window, select the **WINS** tab, and then select Enable **NetBIOS over TCP/IP.**

Figure 3-37: Advanced TCP/IP Settings - WINS Tab
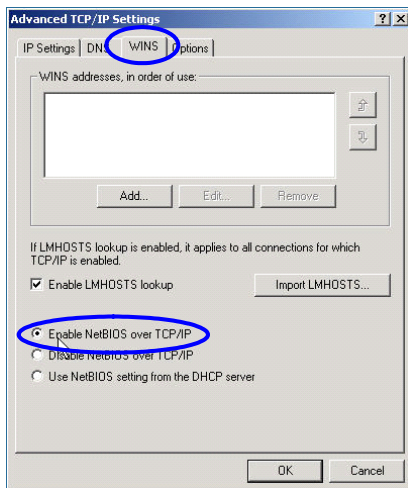
6. Close all open dialogs.

◆ To Share Workstation CD-ROM:

1. Open **My Computer** and right-click **CD-ROM**.

2. Navigate to **My Computer > CD-ROM > Sharing….**

    The Compact Disc Properties window opens.

Figure 3-38: Sharing...
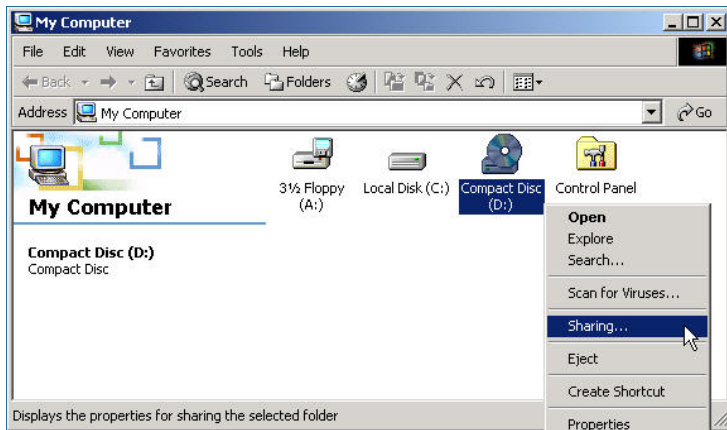
3. Click the **Sharing** tab, and select **Share this folder**.

4. In the **Share name** text box, type in **CDROM with no spaces but with CAPITAL LETTERS.**

5. Click **Permissions** to access the **Permissions for CDROM** window.

Figure 3-39: Compact Disc (D:) Properties - Sharing Tab
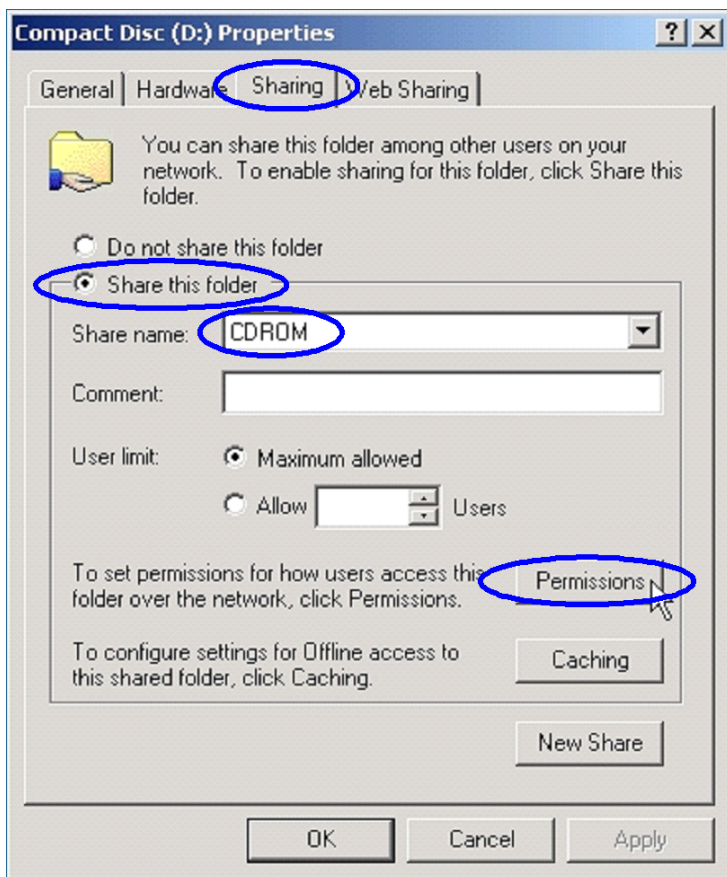
6. From the **Permissions for CDROM** window, ensure that the **Everyone** group is defined with a **Read** permission.

Figure 3-40: Share Permissions Window
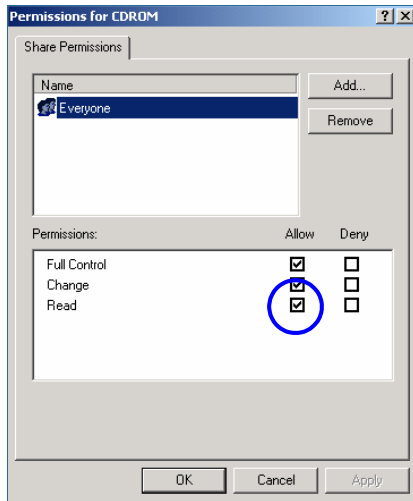
7. Close all open dialogs.

8. Insert the 1st Image CD (Ghost) [Label: Image CD for PCI Logger / ICU / ISA Logger 8.9 W2K3 Appliance (CD #1 of 2)] in the Workstation CD-ROM.

◆ To Set Workstation, Domain / Workgroup, User Name and Password:

1. Note down the following Workstation information:

▪ Full computer name (Up to 15 characters)_____(1)

(For example – NICE-Systems)

▪ Domain / Workgroup name (Up to 15 characters)_____(2)

(For example – GROUPNAME)

▪ Write Workstation local Username and Password information:

▪ Workstation local Login Username_____(3)

▪ Workstation local Login Password_____(4)

▪ **NOTE:** For Computer Name and Workgroup / Domain name:

Right-click **My computer > Properties > Network Identification** tab to see the System Properties window.

Figure 3-41: System Properties - Network Identification Tab
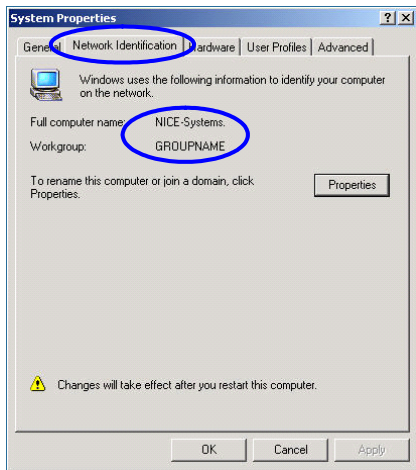
◆ To Install the Image CD (Ghost):

1. In the Logger, configure to startup from the floppy drive.

   (From the BIOS: **BIOS FEATURES SETUP > BOOT SEQUENCE**)

2. Insert the Diskette [Label – Windows Server 2003 Appliance Recovery – Network Installation Diskette] to the Floppy drive.

> **⬞ Important!**
>
> Verify that the write protect tab on the diskette is closed. (Enable rewrite on diskette)

3. **Reboot** the Logger.

◆ To Upload the Image from the Workstation CD-ROM:

> **⬞ Important!**
>
> Use only menu options that are specifically mentioned! (The other options are for NICE CS Engineers only.)

1. From the **MS DOS 6.22 Startup Menu**, select **1 (NICE Products Images…)** and press **Enter**.

   The window opens.

   Figure 3-42: MS-DOS 6.22 Startup Menu
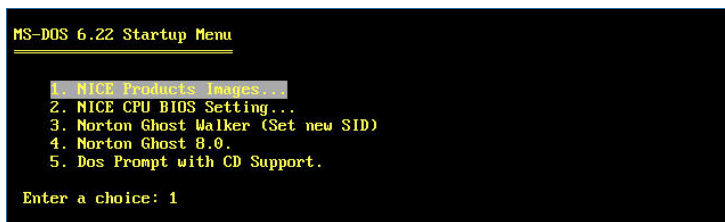
2. From the **MS-DOS 6.22 Startup Menu** now select machine type (1 – NiceLog PCI / 2 - ICU / 3 – NiceLog ISA 8.9) and press **Enter**.

Figure 3-43: MS-DOS 6.22 Startup Menu
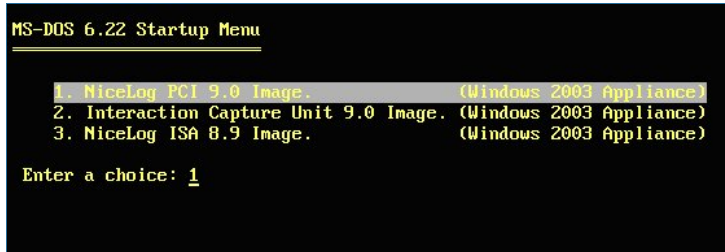
3. Wait a few seconds for the **Download Ghost Image from Workstation CD Drive via Network** window and then fill in the details,see **To Set Workstation, Domain / Workgroup, User Name and Password:** on page 74.

Enter workstation name

Enter workgroup/domain

Enter work station user name

4. Wait a few seconds and then type your user name.

5. Type your password.

6. When prompted to create a password, type **N** and press **Enter**.

The Image CD (Ghost) will start running automatically.

7. Wait for the prompt and then replace the second CD [Label – Image CD for PCI Logger / ICU / ISA Logger 8.9 W2K3 Appliance (CD # 2 of 2)].

8. Select **OK** and press **Enter**.

9. At the end of the installation a **Network Installation Done** notification appears.

10. Press **Enter** to confirm.

◈ **To Restore BIOS Factory Settings:**

1. Reboot the system (**ALT+CTRL+DEL**).

2. From the **MS-DOS 6.22 Startup Menu** select **2 (NICE CPU BIOS Settings…)** and press **Enter**.

Figure 3-44: MS-DOS 6.22 Startup Menu
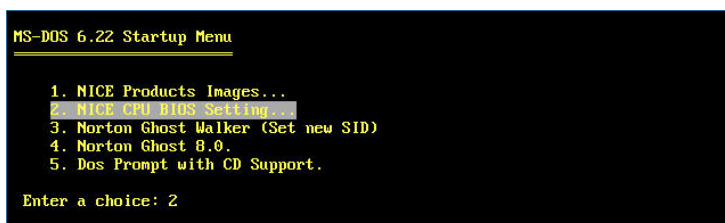
3. From the next screen, select your machine CPU type (NiceLog PCI / ICU / NiceLog ISA 8.9 BIOS Settings) and press **Enter** to restore the BIOS factory settings.

Figure 3-45: MS-DOS 6.22 Startup Menu

```
MS-DOS 6.22 Startup Menu


    1. NiceLog PCI 9.0 BIOS Setting. (PC-620G4)
    2. NiceLog ICU 9.0 BIOS Setting. (PROX-1753)
    3. NiceLog ISA 8.9 BIOS Setting. (PROX-1635)

Enter a choice: 1
```

4. Wait a few seconds, the system will reboot automatically.

> ❗ **Important!**
>
> Remove the diskette from the floppy drive while rebooting.

5. For Software Installation, see **NICE S/W Installation** on page 69.

6. Continue installing NICE S/W, see *Installing the NiceLog High Density Logger Software installation manuals for versions 8.9 and 9.0* on ExtraNICE.

[This page intentionally left blank]

4

Microsoft Client Operating Systems

This chapter provides information regarding Microsoft Client Operating Systems. This includes secure solutions, updates, and guidelines.

Contents

General

Localization

NICE does not support machine names and/or domain names with non-ASCII characters (IRI) on Client workstations.

Windows XP

NICE Product Support for Windows XP Service Pack 3

Product	NICE Product Support for Microsoft Windows XP Service Pack 3
Release	NICE Perform® Release 3 SP4, NICE Perform Release 3.1, Release 3.2, Release 3.5, and Version 8.9, NiceCall Focus III
Synopsis	This section describes NICE product support for Microsoft Windows XP Service Pack 3

Overview

This section provides information regarding NICE product support for Microsoft Windows XP, Service Pack 3.

Microsoft Windows XP, Service Pack 3 was certified on Version 8.9, NiceCall Focus III, Nice Perform Release 3 SP4 and on NICE Perform Release 3.1, for all client side applications as follows:

Server Side Support

NiceCall Focus III

Client Side Support

- NICE SetSecurity Application
- NICE Reporter Viewer
- NICE ScreenAgent
- NICE ScreenSense Agent
- NICE Player
- Record on Demand (ROD)
- Survey Manager
- Remote Tape Server (RTS)
- Media Library
- VoIP Recording Agent (VRA)

Security-Tuning Guidelines for NICE Software Components Running Windows XP Service Pack 2

Product	Security-Tuning Guidelines for NICE Software Components Running Microsoft Windows XP Service Pack 2
Release	
Synopsis	

Overview

This section provides guidelines for NICE components running on client workstations which run on Microsoft Windows XP.

Microsoft recently released Service Pack 2 for Windows XP. In addition to including all previous hot fixes, Service Pack 2 provides the following enhanced security features:

- A built-in firewall

- Enhanced security for Internet Explorer

- Checks for a valid signature of programs during installation

By default, a firewall closes all ports to incoming network packets. Unlike other firewalls which enable you to open a port permanently (known as - statically opened ports), the firewall installed with Service Pack 2 enables you to define specific applications for which the firewall will open the necessary listening ports. These listening ports will remain open only when, and as long as, these applications are running (known as - dynamically opened ports). You do this by adding the applications you want to the firewall Exceptions List.

Sometimes when an application runs for the first time, a warning message appears asking if you want to unblock the application. Unblocking an application will automatically add its name to the firewall Exceptions List. Other times, you will have to add the application manually to the firewall Exceptions List.

The purpose of this section is to provide a summary of the tested NICE software components in this environment, and describe the needed security-tuning for obtaining full-functionality of the system. Security-tuning is performed in the firewall and in Internet Explorer.

> **NOTE:** After you complete security-tuning NICE components, we recommend that you monitor all recording components at the site to ensure that they are running properly.

Preinstallation Requirements

If NICE Web applications Version 8.8 are installed at your site, before installing Microsoft Windows XP Service Pack 2, you must install NICE Web Applications Support Package for Microsoft Windows XP SP2 Client on the Web Server.

> **NOTE:**
>
> - For 8.9 systems (NiceCLS and Client/Server Applications Version 8.9), NICE Web Applications Support Package for Windows XP SP2 Client should be installed on top of Service Pack 4, and 8.9 Web Applications Feature Pack.
>
> - The NICE Web Applications Support Package for Windows XP SP2 Client can be found on www.extranice.com.

◆ **To install the NICE Web Applications Support Package for Microsoft Windows XP SP2 Client:**

- On the **Web Server**, navigate to the location **<Installation Path >\Universe,** and replace the **QueryCriteria.asp** file with the **QueryCriteria.asp** file dated 29 August 2004.

Security-Tuning List

Table 4-1:
Security-Tuning List

NICE Component	Security-Tuning			Comments
	Firewall		Internet Explorer	
	Unblock	Manually Add to Firewall Exceptions Tab		
NICE ScreenAgent Version 8.8	NICE ScreenAgent See **Firewall Unblock Example** on page 86.	-		

NICE Component	Security-Tuning			Comments
	Firewall		Internet Explorer	
	Unblock	Manually Add to Firewall Exceptions Tab		
NICE Perform ScreenAgent	NICE ScreenAgent See **Firewall Unblock Example** on page 86.	-		
NICE ScreenSense Version 8.8	-	-		
NICE Client/Server Applications Version 8.8	NICE Supervision Media Library Printer Server NICE RTS See **Firewall Unblock Example** on page 86.	NICE Administrator See **Adding NICE Administrator to the Exceptions List** on page 88.		

NICE Component	Security-Tuning		Internet Explorer	Comments
	Firewall			
	Unblock	Manually Add to Firewall Exceptions Tab		
NICE Client/Server Applications Version 8.9	NICE Supervision Media Library Printer Server NICE RTS See **Firewall Unblock Example** on the next page**.**	NICE Administrator See **Adding NICE Administrator to the Exceptions List** on page 88.		
NICE SNMP Manager Version 8.9	-	Add from the following location: C:\WINDOWS\system32\snmptrap.exe See **Adding snmptrap.exe to the Exceptions List** on page 91.		

NICE Component	Security-Tuning			Comments
	Firewall		Internet Explorer	
	Unblock	Manually Add to Firewall Exceptions Tab		
NICE Web Applications Version 8.8			Install Crystal Smart Viewer for ActiveX. See **Crystal Smart Viewer for ActiveX Guideline** on the facing page.	See Note (1).
NICE Perform Web Applications				

You must install the NICE Web Applications Support Package for Microsoft Windows XP SP2 Client on the Web Server.

Security-Tuning Your System

Firewall Unblock Example

> 📋 **NOTE:** Although this section provides one firewall unblock example only (ScreenAgent), a similar Windows Security Alert message appears when NICE Supervision, Media Library, Printer Server, and NICE RTS run for the first time.

When certain applications run for the first time, a warning message appears asking if you want to unblock the application. Clicking Unblock will add the application to the Firewall Exceptions List, enabling you to run the application. See Figure 4-1.

Figure 4-1: Windows Security Alert

Crystal Smart Viewer for ActiveX Guideline

When you select the **Reports** tab, an Internet Explorer Security Warning message appears, asking if you want to install the Crystal Smart Viewer for ActiveX. Click **Install**. See Figure 4-2.

Figure 4-2: Internet Explorer - Security Warning
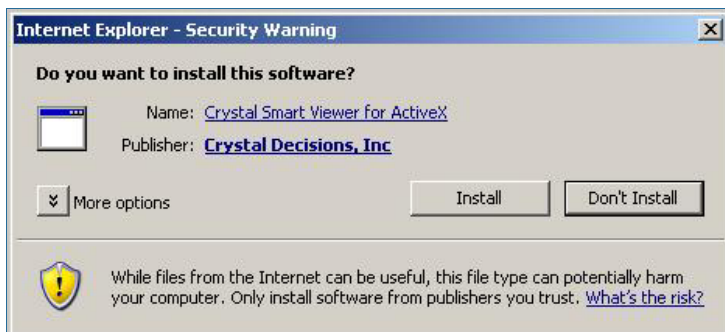
Manually Adding Programs to the Firewall Exceptions List

Opening the Firewall

◈ **To open the firewall:**

1. From the **Start** menu, select **Settings > Control Panel > Windows Firewall**.

   The Windows Firewall window appears.

Figure 4-3: Windows Firewall - General Tab
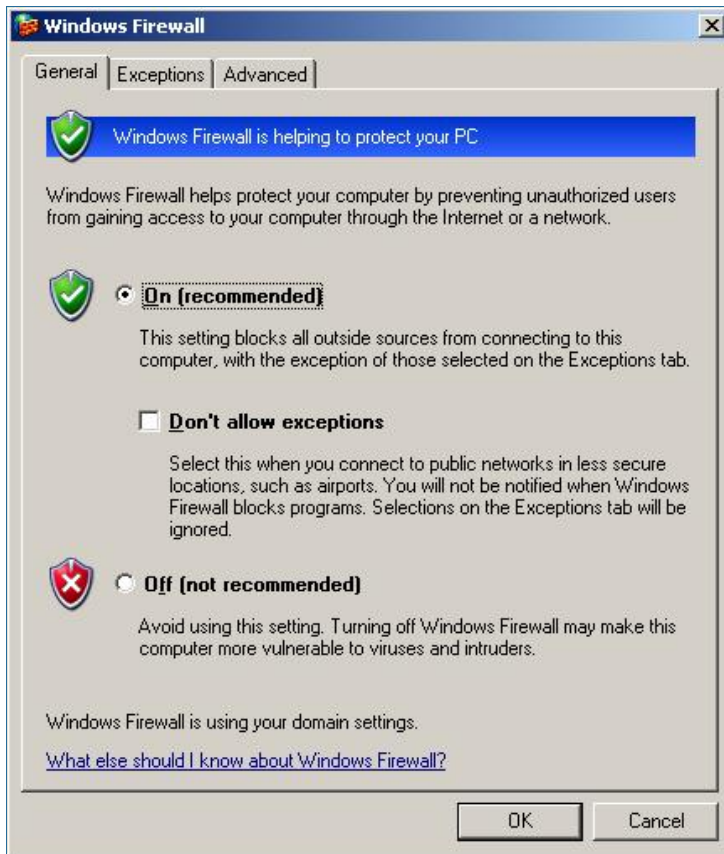
2. Ensure that **On (recommended)** is selected.

Adding NICE Administrator to the Exceptions List

When you add NICE Administrator to the Exceptions List, you do not need to click **Browse** and locate its executable in its installation folder. By default NICE Administrator appears in the Programs list in the Add a Program window.

◆ To add NICE Administrator to the Exceptions list:

1. In the Windows Firewall window, click the **Exceptions** tab.

   The **Exceptions** tab appears as shown below. **File and Printer Sharing** and **Remote Assistance** appear selected.

Figure 4-4: Windows Firewall - Excedptions Tab
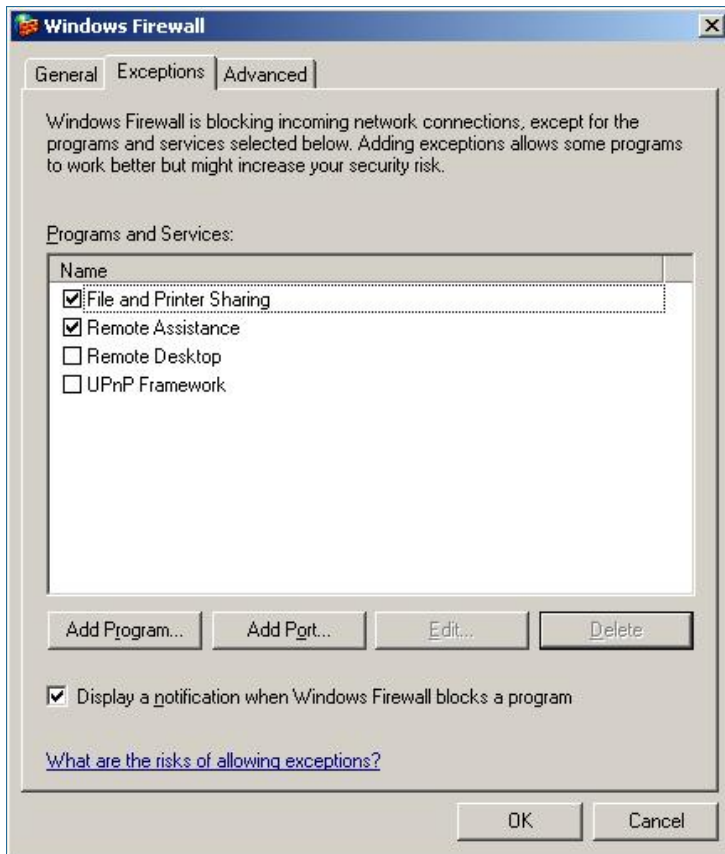
📋 **NOTE:** Ensure that Display a notification when Windows Firewall blocks a program is selected.

2. Click **Add Program.**

   The Add a Program window appears.

3. In the Add a Program window, select **NICE Administrator**.

Figure 4-5: Add a Program
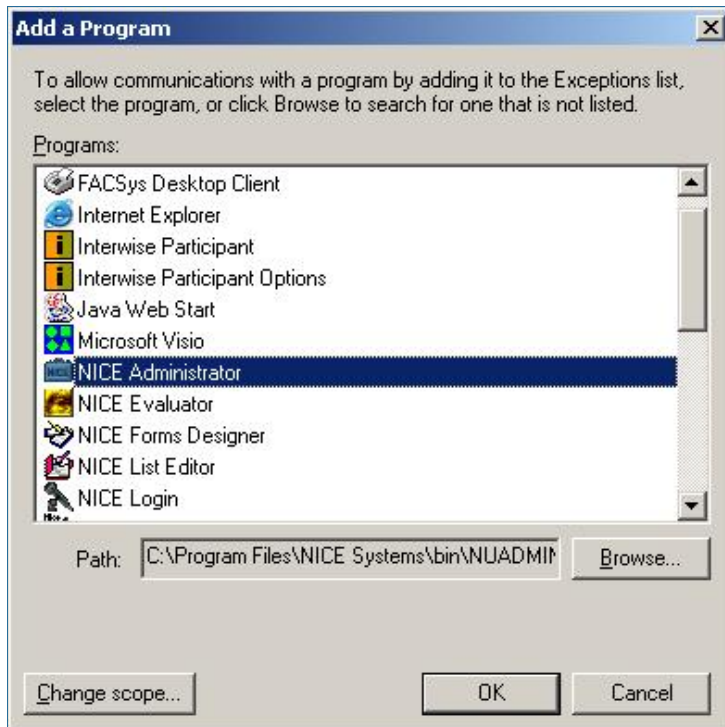
4. Click **OK**. NICE Administrator now appears in the **Exceptions** tab.

Figure 4-6: Windows Firewall - Exceptions Tab
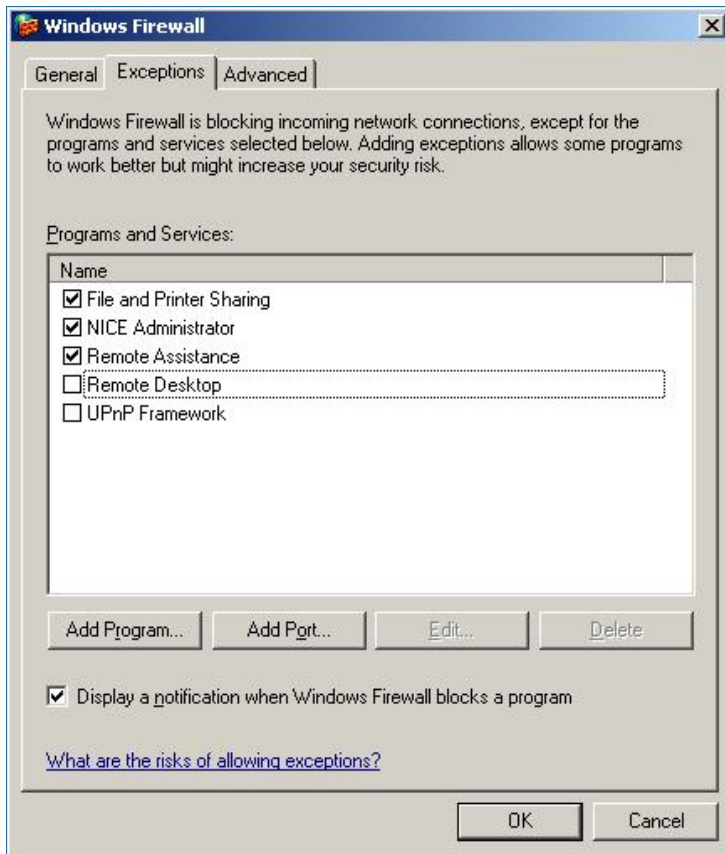
5. In the **Exceptions** tab, click **OK**.

Adding snmptrap.exe to the Exceptions List

snmptrap.exe does not appear in the Programs list in the Add a Program window. To add snmptrap.exe, you must click **Browse**, then locate **snmptrap.exe** in the **C:\WINDOWS\system32** directory.

To add snmptrap.exe to the Exceptions list:

1. In the Windows Firewall window, in the **Exceptions** tab, click **Add Program.**

   The Add a Program window appears.

2. Click **Browse**, go to **C:\WINDOWS\system32** and select **snmptrap.exe**.

Figure 4-7: Browse Window
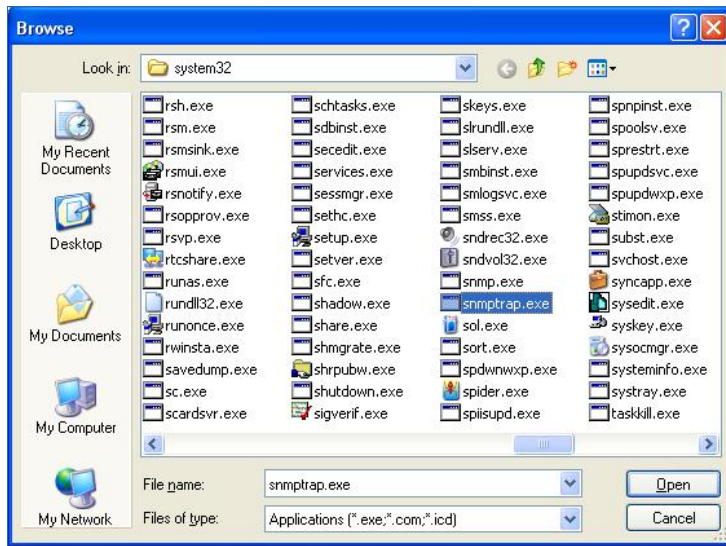
3. Click **Open**. snmptramp.exe is now added to the Exceptions list.

Figure 4-8: Windows Firewall - Exceptions Tab
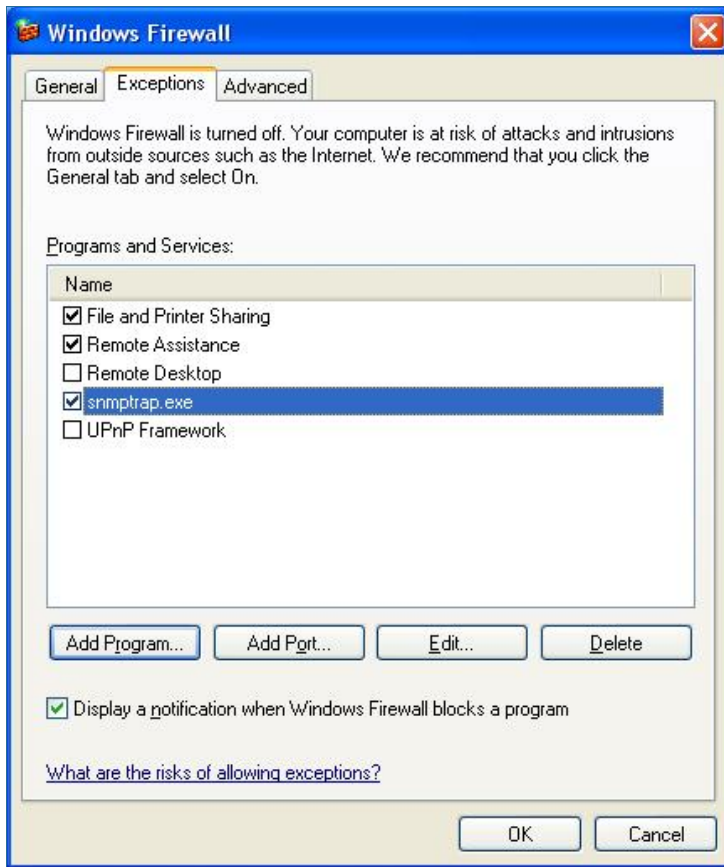
4. Click **OK**.

Windows 7 32-bit/64-bit

NICE Perform Client Applications Compatibility

NICE Systems supports the following editions of Microsoft Windows 7 in both 32-bit and 64-bit configurations:

■ Microsoft Windows 7 Professional Edition

■ Microsoft Windows 7 Enterprise Edition

■ Microsoft Windows 7 Ultimate Edition

The following table shows the compatibility of NICE Perform client applications with Microsoft Windows 7 for Releases 3.1, 3.2, and 3.5, and NICE Interaction Management Release 4.1:

> ! **Important!**
>
> ■ NICE Applications and the Set Security feature support only the 32-bit version of Internet Explorer.
>
> ■ (*) These components must be installed with the UAC turned **OFF**.

Table 4-2: Compatibility With Microsoft Windows 7 32-bit and 64-bit by Release

Application	Release 3.1		Release 3.2		Release 3.5		Release 4.1	
	Windows 7 32-bit	Windows 7 64-bit	Windows 7 32-bit	Windows 7 64-bit	Windows 7 32-bit	Windows 7 64-bit	Windows 7 32-bit	Windows 7 64-bit
Screen Agent	Supported as of UP 3.1.18 (*)	Supported as of UP 3.1.18(*)	Supported as of UP 3.2.9 (*)	Supported as of UP 3.2.9 (*)	Approved	Approved	Approved	Approved
ROD Client	Approved (*)	Not Supported	Approved	Approved	Approved	Approved	Approved	Approved
Standalone NICE Player and NICE Player Codec Pack	Approved (*)	Approved (*)	Approved	Approved	Approved	Approved	Approved	Approved

Application	Release 3.1		Release 3.2		Release 3.5		Release 4.1	
	Windows 7 32-bit	Windows 7 64-bit	Windows 7 32-bit	Windows 7 64-bit	Windows 7 32-bit	Windows 7 64-bit	Windows 7 32-bit	Windows 7 64-bit
Reporter Viewer	Approved (*)	Not Supported	Approved	Approved	Approved	Approved	Approved	Approved
NICE Applications (including Set Security)	Approved (*)	Approved (*)	Approved	Approved	Approved	Approved	Approved	Approved
Survey Manager	Approved	Approved	Approved	Approved	Approved	Approved	Approved	Approved
VRA	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Approved	Approved
Media Library	Approved	Approved	Approved	Approved	Approved	Approved	Approved	Approved
BSF Tool kit	Approved	Not Supported	Approved	Not Supported	Approved	Approved	Approved	Approved
NICE Sentinel Remote Client	Approved (*)	Approved (*)	Approved	Approved	Approved	Approved	Approved	Approved
ScreenSense Agent	Not Supported	Not Supported	Supported as of UP 3.2.11 (*)	Supported as of UP 3.2.11 (*)	N/A	N/A	N/A	N/A
Desktop Analytics (using PO Client)	N/A	N/A	N/A	N/A	Approved	NICE Approval	Approved	NICE Approval

Applicatio n	Release 3.1		Release 3.2		Release 3.5		Release 4.1	
	Window s 7 32-bit	Window s 7 64-bit	Window s 7 32-bit	Window s 7 64-bit	Window s 7 32-bit	Window s 7 64-bit	Window s 7 32-bit	Window s 7 64-bit
RTS	Approve d	Approve d	Approve d	Approve d	Approve d	Approve d	Approve d	Approve d

Using the Silent Installation to Install NICE Perform Release 3.x and NICE Interaction Management Release 4.1 Client Applications

> **NOTE:** The commands listed below are applicable to both Microsoft Windows 7 32-bit and 64-bit operating systems.

Use the following commands to install NICE Perform/NICE Interaction Management client-side applications using the silent installation on workstations running Microsoft Windows 7 (usually from a central deployment server, such as SMS/SCCM 2007, etc.):

- **Set Security Application** below.
- **ScreenSense Agent** below.
- **NICE Player and NICE Player Codec Pack** on the facing page.
- **Reporter Viewer** on the facing page.
- **NICE ScreenAgent** on the facing page.
- **Record on Demand** on page 98.
- **PO Client** on page 98
- **NICE Insight to Impact Bridge** on page 98

Set Security Application

Enter in the Command line:

SetSecurityApp.exe Server <*nnnn*>

in which "*nnnn*" is the Host Name, or the IP Address, or the FQDN of the NICE Perform/NICE Interactions Management Applications server.

ScreenSense Agent

Enter in the Command line:

AgentSilentInstallation.bat

> ☐ **NOTE:** Before running this command, you must define the name of the NICE Perform Applications Server in the **AgentSilentInstallation.bat** file.

NICE Player and NICE Player Codec Pack

Enter in the Command line:

> **msiexec /i "Nice Player.msi" /qn**
>
> **msiexec /i "Nice Player Codec Pack.msi" /qn**

Reporter Viewer

For NICE Perform Release 3.x

Enter in the Command line:

> **msiexec /i "ReporterViewer.msi" /qn**

For NICE Interaction Management Release 4.1

Enter in the command line:

> **ReporterViewer.exe /S /D=<ReporterViewer installation folder>**

NICE ScreenAgent

For NICE Perform Release 3.x

Enter in the Command line:

> **Setup.exe**

> ☐ **NOTE:** Before running this command, you must configure the agent.cfg configuration file and place it with the **setup.exe**. file.

For NICE Interaction Management Release 4.1

◆ **To install NICE ScreenAgent using a silent installation:**

1. Copy the NICE ScreenAgent installation folder to a temporary location on the server on which you want to run the silent installation.

2. Extract the **.msi** files by running the following command in the Run window:

   <Path\Setup.exe file> /t:<Path\target folder> /c

Here **<Path\Setup.exe file>** is the path to the Setup file in the NICE ScreenAgent installation folder and **<Path\target folder>** is the path to the folder to which you want to extract the .msi files.

> **❗ IMPORTANT**
>
> You must leave a space (not an underscore) after **<path to Setup.exe file>** and after **<target folder>** .

This command extracts two .msi files to the target folder:

- ☐ **screenagentxp.msi** - (32-bit installation)
- ☐ **screenagentxp64.msi** - (64-bit installation)

3. To install the NICE ScreenAgent software, run one of the following procedures (for details about configuring the parameters see *Configuring NICE ScreenAgent Installation Parameters*, in the *ScreenAgent Installation and Configuration Guide*):

- ☐ If you are running the silent installation locally on each client machine, in the Run window, run the following command:

  msiexec.exe /i <full path to .msi file> /q SYSADMIN = <Application Server Host Name>

> **❗ Important!**
>
> You must leave a space (not an underscore) after msiexec, after /i, after <full path to .msi file>, and after q.

-or-

- ☐ If you are deploying NICE ScreenAgent using a publishing application, configure the publishing application to run the relevant .msi file.

> **🗅 NOTE:**
>
> You can use any publishing application that supports .msi files.

After completing the installation, you configure the NICE ScreenAgent in the System Administrator.

Record on Demand

Enter in the Command line:

> **msiexec /i "RODSetup.msi" /qn SERVERURL=<*nnnn*> LAUNCH="No" ALLUSERS=1**

in which "*nnnn*" is the Host Name

PO Client

Enter in the command line:

> **msiexec /i "Full path to the NICE Real-Time Client.msi" /qn STANDALONE="1" EGDEFAULTP="full path for project.XML"**

NICE Insight to Impact Bridge

Enter in the command line:

msiexec /i "full path to the NICE Insight to Impact Bridge.msi file" /qn EGHOST="
Application Server HostName "

Manually Installing NICE Perform Release 3.x and NICE Interaction Management 4.1 Client Applications

> **NOTE:**
>
> The procedures listed below are applicable to all NICE Perform Release 3.x and NICE Interaction Management 4.1 client-side components on workstations running Microsoft Windows 7 32-bit or 64-bit operating systems.
>
> Keep in mind that:
>
> ■ In NICE Perform Release 3.x, UAC must be turned off before installing client-side applications marked by an asterisk (*) in **Windows 7 32-bit/64-bit** on page 94. After installation is finished the UAC should be turned on.
>
> ■ In NICE Interaction Management Release 4.1, UAC can be turned on during the installation of the client-side applications.

◆ **To install NICE Perform Release 3.x and NICE Interaction Management 4.1client-side applications on workstations with Microsoft Windows 7:**

1. Locate the application installation directory.

    The default path for NICE Player, NICE Player Codec Pack, Reporter Viewer, and Record on Demand is:
    \\server_name\...\Program Files\NICE Systems\Applications\Client Side Applications

2. Copy the required application installation file(s) to the local computer.

3. Log in to the workstation using a User with Administrative privileges.

4. Refer to **Windows 7 32-bit/64-bit** on page 94 to see if the component requires that the UAC be turned **Off**. If the UAC can remain on, run the installation wizard.

    If the UAC must be turned off, do one of the following:

    ■ If you logged in under the Built-in Administrator, in the Local Group Policy Editor window, set the **User Account Control: Admin Approval Mode for the Built-in Administrator** policy to **Disabled**.

Figure 4-9: Local Group Policy Editor Window
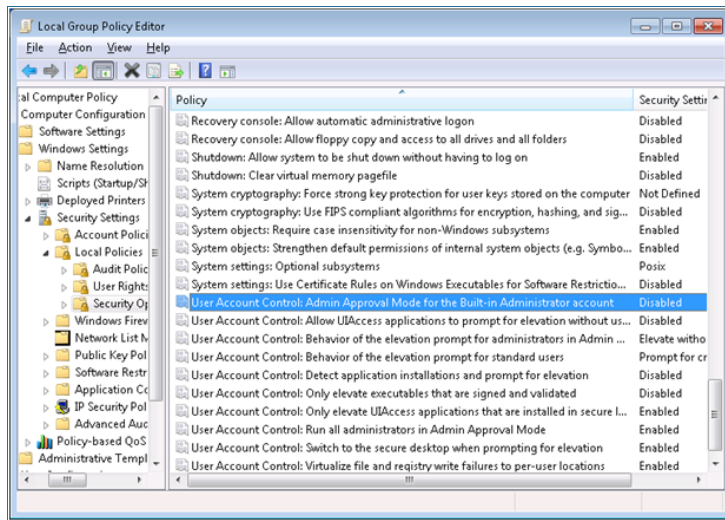
- If you logged in under another user with Administrative privileges, in the Local Group Policy Editor window, set the **User Account Control: Run all administrators in Admin Approval Mode** policy to **Disabled**.

Figure 4-10: Local Group Policy Editor Window
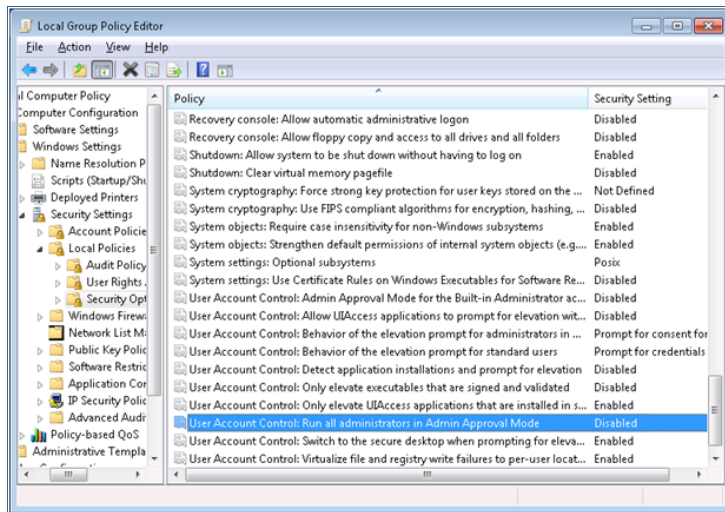
5. Run the installation wizard.

Windows 8 and Windows 8.1 32-bit/64-bit

NICE Interaction Management Client Applications Compatibility

NICE Interaction Management 4.1.47 and later supports the following editions of Microsoft Windows 8 and Microsoft Windows 8.1, in both 32-bit and 64-bit configurations:

- Microsoft Windows 8 Professional Edition
- Microsoft Windows 8 Enterprise Edition
- Microsoft Windows 8.1 Professional Edition
- Microsoft Windows 8.1 Enterprise Edition

The following table shows the compatibility of NICE Interaction Management Release 4.1 47 and later client applications with Microsoft Windows 8/8.1:

Table 4-3: Compatibility With Microsoft Windows 8 and 8.1 32-bit and 64-bit for Release 4.1.47 and later

Application	Windows 8 32-bit	Windows 8 64-bit	Windows 8.1 32-bit	Windows 8.1 64-bit
Screen Agent	Approved	Approved	Approved	Approved
ROD	Approved	Approved	Approved	Approved
Standalone NICE Player and NICE Player Codec Pack	Approved	Approved	Approved	Approved
Reporter Viewer	Approved	Approved	Approved	Approved
NICE Applications (including Set Security)	Approved	Approved	Approved	Approved
Survey Manager	Not Supported	Approved	Not Supported	Not Supported
VRA	Approved	Approved	Approved	Approved
Media Library	Approved	Approved	Approved	Approved
BSF Tool Kit	Approved	Approved	Approved	Approved
NICE Sentinel Remote Client	Not Supported	Approved	Not Supported	Approved

Application	Windows 8 32-bit	Windows 8 64-bit	Windows 8.1 32-bit	Windows 8.1 64-bit
Real-Time Designer 📔 **NOTE:** The Real-Time Designer cannot be installed on Windows 8/8.1 in VMware view. The Real-Time Designer requires .NET Framework 4 to be installed side-by-side with .NET Framework 4.5 (the Windows 8/8.1 default).	Approved	Approved	Approved	Approved
Real-Time Client 📔 **NOTE:** The Real-Time Client requires .NET Framework 4 to be installed side-by-side with.NET Framework 4.5 (the Windows 8/8.1 default)	Approved	Approved	Approved	Approved

Using the Silent Installation to Install NICE Interaction Management Release 4.1 Client Applications

Use the following commands to install NICE Interaction Management client-side applications with the silent installation on workstations running Microsoft Windows 8 and Windows 8.1:

▪ **Set Security Application** below

▪ **NICE Player and NICE Player Codec Pack** on the facing page

▪ **NICE Screen Agent** on the facing page

▪ **Record on Demand** on page 104

Set Security Application

This describes how to install the SetSecurity Application.

◈ **To install the SetSecurity Application:**

▪ At the command-line prompt, type SetSecurityApp.exe Server <***nnnn***>.

Where ***nnnn*** is the Host Name, IP Address, or the FQDN of the NICE Interactions Management Applications server.

NICE Player and NICE Player Codec Pack

This topic describes how to install the NICE Player and NICE Player Codec Pack.

◆ To use NICE Player and NICE Player Codec Pack:

■ At the command-line prompt, type:

msiexec /i "Nice Player.msi" /qn

msiexec /i "Nice Player Codec Pack.msi" /qn

NICE Screen Agent

This section describes how toinstall NICE ScreenAgent by using the silent installation Use one of the following methods:

■ Run the silent installation locally on each client machine on which you want to install NICE ScreenAgent.

■ Use a publishing application to deploy NICE ScreenAgent on all the client machines.

◆ To install NICE ScreenAgent using a silent installation:

1. Copy the NICE ScreenAgent installation folder to a temporary location on the server where you want to run the silent installation.

2. Extract the **.msi** files by running the following command in the **Run** window:

<Path\Setup.exe file> /t:<Path\target folder> /c

where **<Path\Setup.exe file>** is the path to the Setup file in the NICE ScreenAgent installation folder and **<Path\target folder>** is the path to the folder with the **.msi** files to be extracted.

This command extracts two .msi files to the target folder:

■ **screenagentxp.msi - (32-bit installation)**

■ **screenagentxp64.msi - (64-bit installation)**

3. To install the NICE ScreenAgent software, run *one* of the following procedures:

■ For local manual installation, in the **Run** window on each client machine, type the following command:

msiexec.exe /i <full path to .msi file> /q SYSADMIN = <Application Server Host Name>

   📋 **NOTE:**

You must leave a space (not an underscore) after <path to Setup.exe file> and after <target folder>.

You must leave a space (not an underscore) after msiexec, after /i, after <full path to .msi file>, and after q.

Or

■ For a batch installation, configure the publishing application to run the relevant **.msi** file.

NOTE: You can use any publishing application that supports **.msi** files. After completing the installation, configure the NICE ScreenAgent in the System Administrator.

Record on Demand

This topic describes how to install the Record on Demand application.

To use Record on Demand:

▪ At the command-line prompt, type the following:

msiexec /i "RODSetup.msi" /qn SERVERURL=<*nnnn*> LAUNCH="No" ALLUSERS=1

Where ***nnnn*** is the Host Name.

Manually Installing NICE Interaction Management 4.1 Client Applications

NOTE: The procedures listed below are applicable to all NICE Interaction Management 4.1 client-side components on workstations running Microsoft Windows 8/8.1 operating systems.

In NICE Interaction Management Release 4.1 systems, UAC can be turned on while installing client-side applications.

To manually install NICE Interaction Management 4.1 client-side applications on workstations with Microsoft Windows 8 or Microsoft Windows 8.1:

1. Log in to the workstation with a valid user with administrative privileges.

2. Locate the application installation directory. The default path for NICE Player, NICE Player Codec Pack, Reporter Viewer, and Record on Demand is:

   \\server_name\...\Program Files\NICE Systems\Applications\Client Side Applications

3. Copy the required application installation file(s) to the local computer.

4. Run the installation wizard.

5

Internet Explorer

This chapter describes compatibility of Internet Explorer with NICE Web Applications.

> ❗ **Important!**
>
> NICE Applications and the Set Security feature support only the 32-bit version of Internet Explorer.

Contents

Working with an XBAP Page

- When using XBAP, the **Tool** menu disappears from the Internet Explorer tool bar. To view the tool menu, you can do one of the following:

  - Open a new tab. The **Tools** menu will be available in the new tab.

  - Click the **Internet Options** button in Internet Explorer and use the **Internet Options** window. If this button does not appear, right-click in the Button bar and add it.

- The URL address to any NICE Interaction Management projects you were using will be different when using XBAP.

  Instead of the ASPX link **http://<server name>/NiceApplications/Desktop/webpage/DeskTopWebForm.aspx**, the new address will be **http://<server name>/NiceApplications/Desktop/XbapApplications/NiceDesktop.XBAP**.

- NICE Interaction Management 6.3 is designed to work only with XBAP, but not with ASPX.

If you previously created shortcuts/favorites,then replace all previously saved links to the new address.

Internet Explorer 6

Compatibility of NICE Web Applications with Internet Explorer 6

Product	NICE Interaction Management, NICE Perform, NiceUniverse Web Application, NICE Sentinel
Release	NICE Interaction Management R4.1 NICE Perform: R3 SP3/SP4, R3.1, R3.2, R3.5 NiceUniverse Web Application 8.9 NICE Sentinel: R2.1, R2.5
Synopsis	This section describes the compatibility of Internet Explorer 6 with NICE Web Applications when Internet Explorer 6 is installed on: Windows 2000 Professional Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition Windows XP

General Description

General tests were performed using Internet Explorer 6 (IE6) with:

- NICE Universe Web Applications 8.9
- NICE Perform
  - Release 1
  - Release IPC 9.09
  - Release 2
  - Release 3
  - Release 3.1
  - Release 3.2
  - Release 3.5
- NICE Interaction Management Release 4.1
- NICE Sentinel
  - Release 2.1
  - Release 2.5

The following table describes the compatibility between all supported Operating Systems and NICE Applications.

Table 5-1:
Operating System

Operating System	Web Apps 8.9	NP R1	NP R2	IPC 9.09	NP R3	NP R3.1	NP R3.2	NP R3.5	NIM 4.1	
Windows Server 2003 R2 Standard/ Enterprise	P	P	P	P	P	P	P	P	P	
Windows XP	P	P	P	P	P	P	P	P	P	
Windows 2000 Professional	P	P	P	P	P	P				

Internet Explorer 7

Compatibility of NICE Web Applications with Internet Explorer 7

Product	NICE Perform, NiceUniverse Web Application, NICE Sentinel
Release	NICE Interaction Management R4.1 NICE Perform: R3 SP3/SP4, R3.1, R3.2, R3.5 NiceUniverse Web Application 8.9 NICE Sentinel: R2.1, R2.5
Synopsis	This section describes the compatibility of Internet Explorer 7 with NICE Web Applications when Internet Explorer 7 is installed on: Windows Vista Business Windows Vista Enterprise Windows Server 2008 Standard/Enterprise Edition Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition Windows XP

General Description

General tests were performed using Internet Explorer 7 (IE7) with:

- NICE Universe Web Applications 8.9
- NICE Perform
  - Release 1
  - Release IPC 9.09
  - Release 2
  - Release 3
  - Release 3.1
  - Release 3.2
  - Release 3.5
- NICE Interaction Management Release 4.1
- NICE Sentinel
  - Release 2.1

■ Release 2.5

The following table describes the compatibility between all supported Operating Systems and NICE Applications.

After installing Internet Explorer 7, the internet settings must be changed on all Operating Systems. See **Changing Internet Explorer 7 Settings After Installation** on page 113

Table 5-2:
Operating System
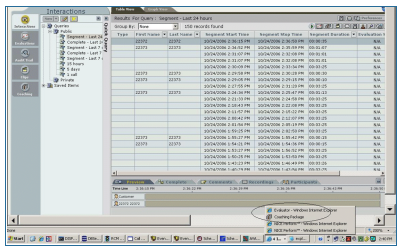
Operating System	Web Apps 8.9	NP R1	NP R2	IPC 9.09	NP R3	NP R3.1	NP R3.2	NP R3.5	NIM 4.1		NICE Sentinel R2.1	NICE Sentinel R2.5
Windows Vista Business					P	P					P	P
Windows Vista Enterprise						P	P	P	P		P	P
Windows Server 2008 Standard/Enterprise							P	P	P		P	P
Windows Server 2003 R2 Standard/ Enterprise	P	P	P	P	P	P	P	P	P		P	P
Windows XP	P	P	P	P	P	P	P	P	P		P	P

Known Issues

The following section describes known issues when using Internet Explorer 7.

Table 5-3:
Known Issues

Issue	Description	Release
	NICE Perform Web applications should not be used in **Internet Explorer 7** tab or **Quick** ab modes. They must be operated in a **Single** tab usage. **Note**: In Release 3.1 and above, you *can* use **NICE Perform Web applications** in tab and **Quick** tab mode, however, you *cannot* open more than one session of NICE Perform at the same time.	■ NICE Perform R 1 ■ NICE Perform R 2 ■ NICE Perform R 3 ■ Release IPC 9.09 ■ Universe Web Applications Version 8.9

Issue	Description	Release
	In the NICE Perform Applications, different windows appear in minimized mode. The affected windows are as follows: *For Release 1:* Opening Coaching Package window. Playing Screen Interaction Coaching - Creating, opening and deleting. Creating clips. Clicking Evaluate. *For Releases 2 and 3* Coaching window appears normally. After the form is filled, click the Send button, the coaching closes to minimized mode. Saving interactions. **Note**: This issue occurs when only .NET 1.1 and .NET 1.1 SP1 are installed on the client workstation. Sending interactions by E-mail. **Note**: This issue occurs when only .NET 1.1 and .NET 1.1 SP1 are installed on the client workstation. The following graphic shows how some of these windows can be opened.	▪ NICE Perform R 1 ▪ NICE Perform R 2 ▪ NICE Perform R 3 (Contact Center) ▪ Release IPC 9.09
	A pop-up block appears when you want to view a report. You must remove it so that you can view the report. **Note:** This issue occurs when only .NET 1.1 and .NET 1.1 SP1 are installed on the client workstation.	NICE Perform R 1

Issue	Description	Release
	Triggers for the ScreenSense Agent, which were defined on an HTML page with Internet Explorer 6, do not work with Internet Explorer 7 and vice versa.	NICE Perform R 2 NICE Perform R 3

Changing Internet Explorer 7 Settings After Installation

When Internet Explorer 7 is installed, the following issues are created:

■ Internet Explorer 7 **resets the cache to 10 MB**. It is important to **resize the cache size to 200 MB** when working with NICE Perform Applications. See **Changing the Cache Size** below.

■ The font is **Clear Type**, which appears blurred, and you may want to return to the **Black and White** font. See **Changing the Font Used by Internet Explorer 7** on the next page.

■ The application server is **not automatically added to the trusted site list**, and it is important to **do so manually.** See **Internet Explorer 8** on page 121.

Changing the Cache Size

Perform the following procedure to modify the cache size.

◈ **To modify the cache size:**

1. Open Internet Explorer.

2. Click **Tools**, and select **Internet Options**.

3. In the **General** tab, under **Browsing History**, click **Settings**. The **Temporary Internet Files and History Settings** window appears.

Figure 5-1: Temporary Internet Files and History Settings Window
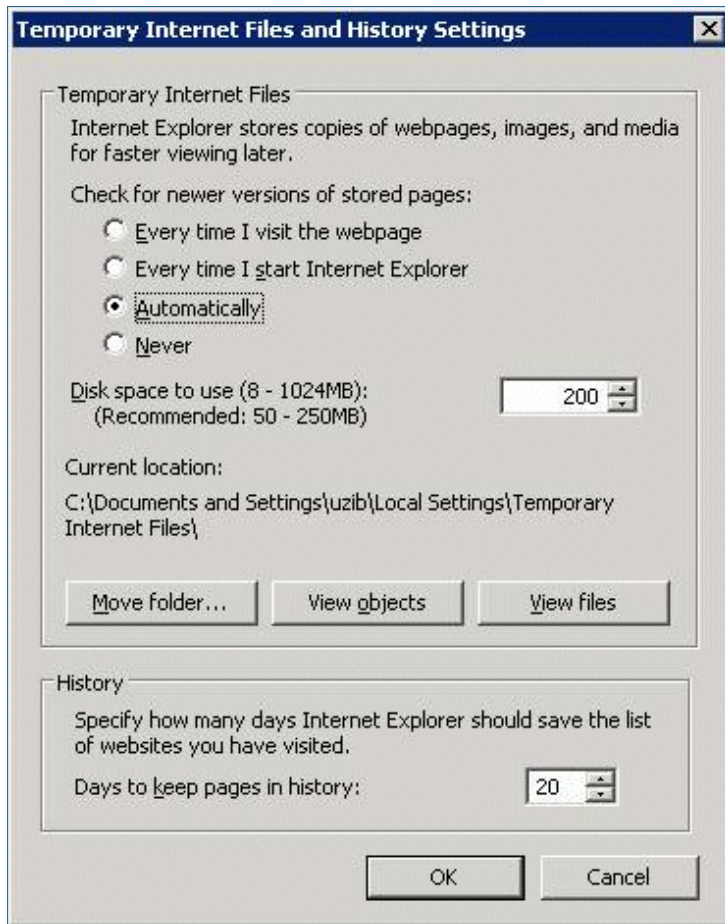
4. By default, **Check for newer versions of stored pages** is set to **Every time I visit the webpage**. Set it to **Automatically**, and set the **Disk space to use** to **200**. Click **OK** to confirm the changes.

Changing the Font Used by Internet Explorer 7

The following graphic illustrates the difference between the **Clear Type** font and the **Black and White** font:

Figure 5-2: Example of Clear Type/Black and White Font
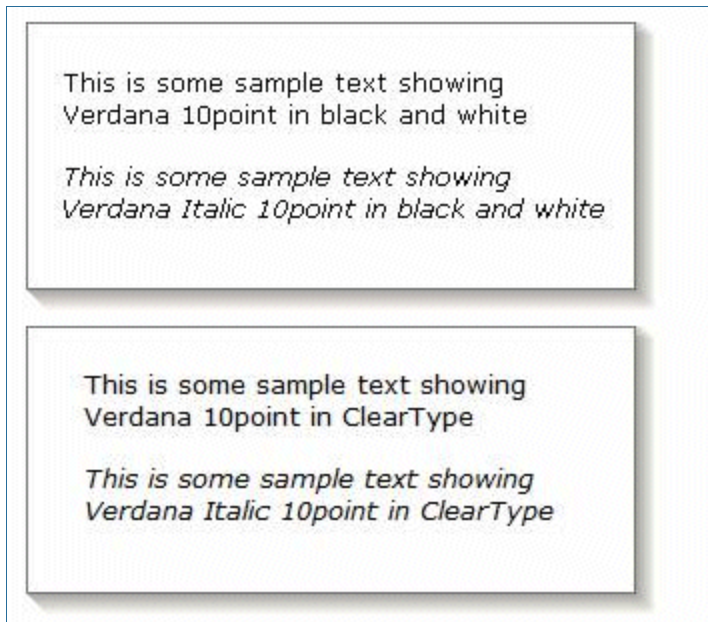
If you are not satisfied with the **Clear Type** font, perform the following procedure to change it to **Black and White**.

◆ To modify the font:

1. Open Internet Explorer.

   Figure 5-3: Internet Explorer Window
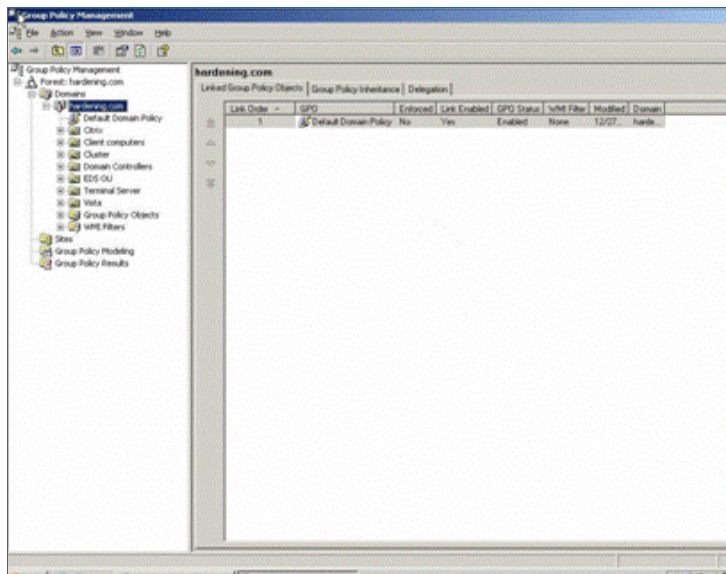
2. Click **Tools**, select **Internet Option**, and click **Advanced**. The following window appears.

Figure 5-4: Internet Options - Advanced Tab
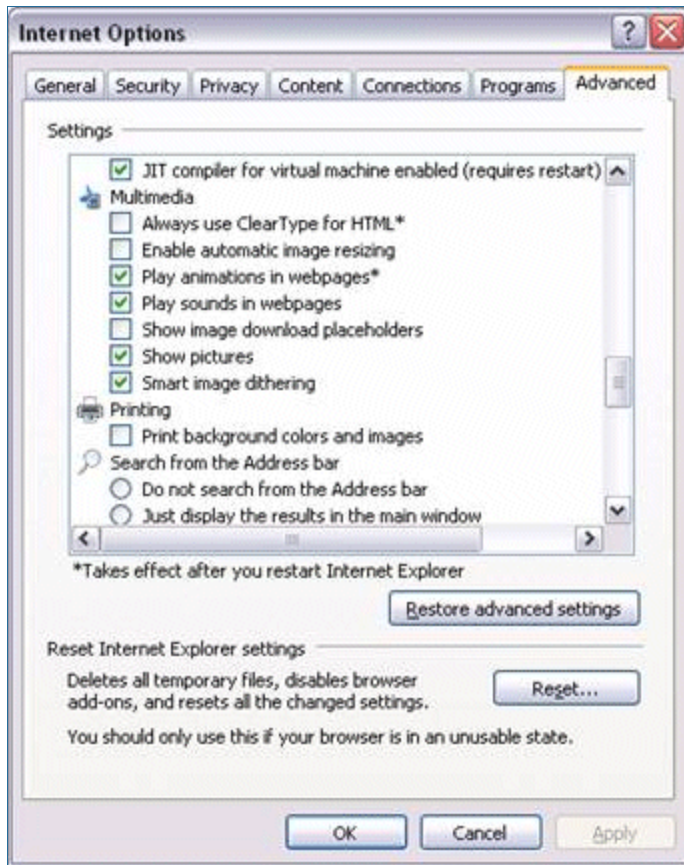
3. Clear **Always use Clear Type for HTML**, and click **OK** to confirm.

4. Restart Internet Explorer and Microsoft Outlook.

See the **http://blogs.msdn.com/ie/archive/2006/02/03/524367.aspx** link for further information.

Manually Adding NICE Perform Applications to the Trusted Site List

Perform the following procedure to manually add the application server to the trusted site list.

NICE Perform Release 3.1 supports Internet Explorer 7 in both the **Quick** tab and **Single** tab modes.

◈ To enable login to NICE Perform in an IE7 environment:

1. On the Domain Controller do the following: In the Run window, type **gpmc.msc** and click **OK**.

    The Group Policy Management window appears.

Figure 5-5: Group Policy Management Window
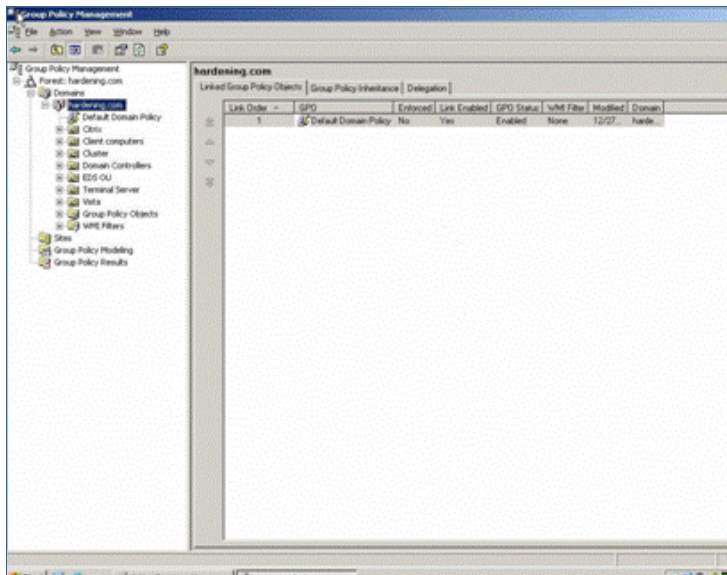
2. Right-click the **GPO** you created when you created the User Account Control and click **Edit**.

> **NOTE:** Complete instructions for setting up the User Account Control can be found in NICE Perform Release 3.1: Microsoft Windows Vista Enterprise SP1 Workstation Configuration Guide, "Setting up the User Account Control in an Active Directory".

3. Select **Computer Configuration > Administrator Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Pages**.

The Group Policy Object Editor window appears.

Figure 5-6: Group Policy Object Editor Window
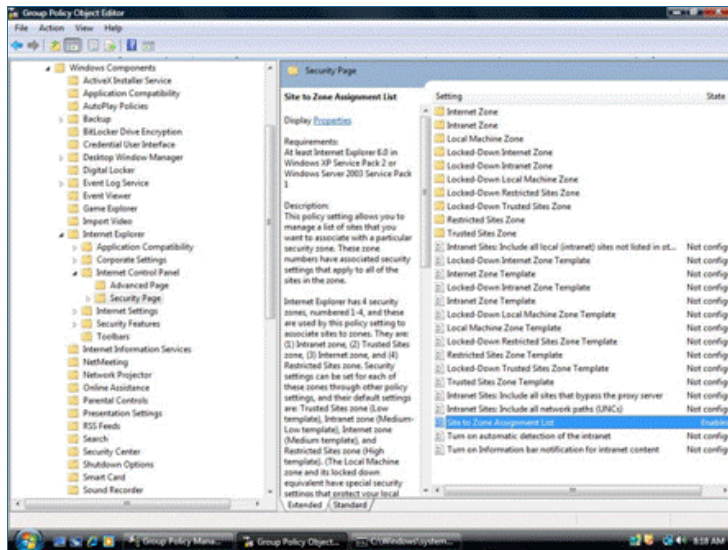
4. Double-click the **Site to Zone Assignment List** policy.

   The Site to Zone Assignment List Properties window appears.

Figure 5-7: Site to Zone Assignment List Properties Window
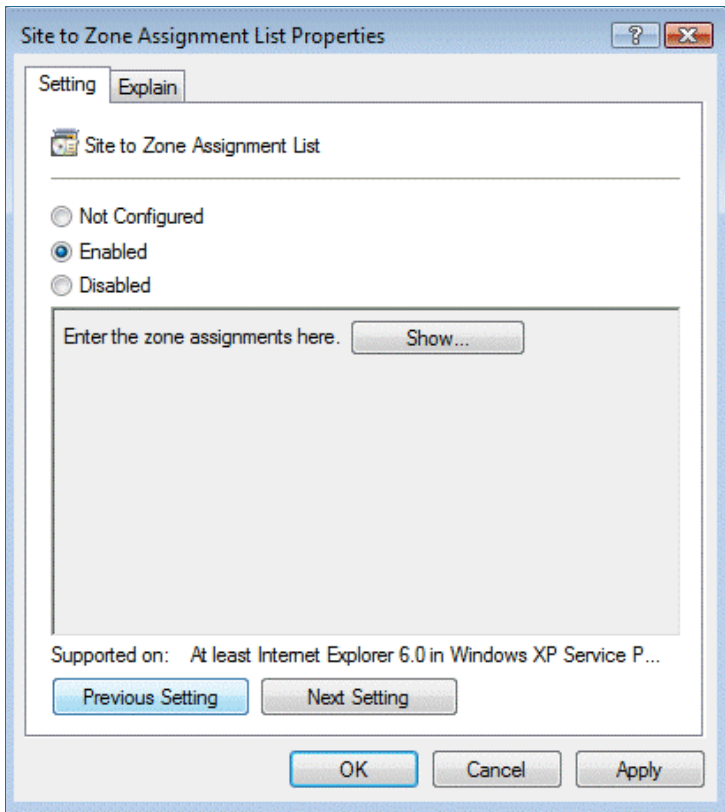
5. Select **Enabled** and click **Show.**
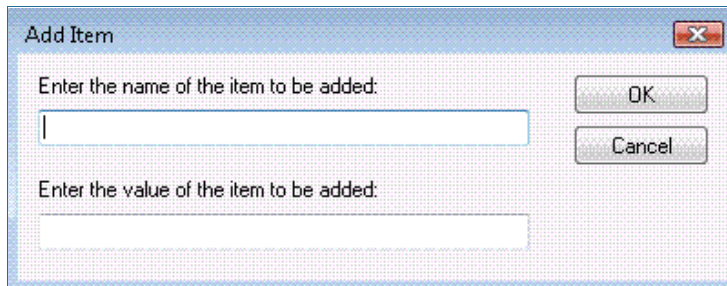
    The Show Contents window appears.

    Figure 5-8: Show Contents Window
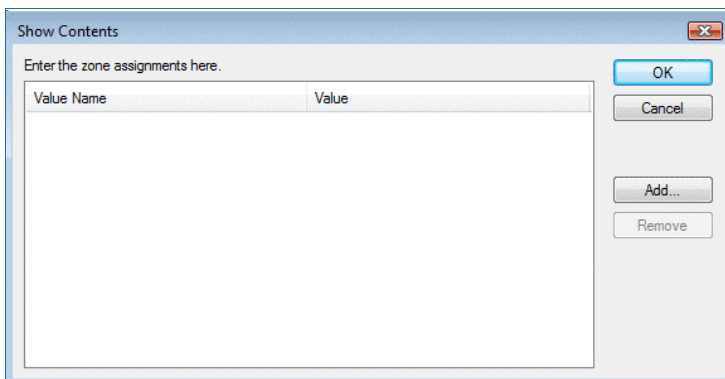
6. Click **Add.**

    The Add Item window appears.

Figure 5-9: Add Item Window

7. In the **Enter the name of the item to be added** field, enter the name of the Web Application Site.

8. Enter the digit **2** in the **Enter the value of the item to be added** field and click **OK**.

    The Show Contents window reappears.

9. Click **OK**.

    The Site to Zone Assignment List Properties window reappears.

10. Click **OK**.

    The Group Policy Object Editor Window reappears.

11. Close the Group Policy Object Editor Window.

Internet Explorer 8

Compatibility of NICE Web Applications with Internet Explorer 8 32-bit

Product	NICE Interaction Management, NICE Perform, NiceUniverse Web Application, NICE Sentinel
Release	NICE Interaction Management R4.1
	NICE Perform: R3 SP3/SP4, R3.1, R3.2, R3.5
	NiceUniverse Web Application 8.9
	NICE Sentinel: R2.1, R2.5
Synopsis	This section describes the compatibility of Internet Explorer 8 with NICE Web Applications when Internet Explorer 8 is installed on:
	Windows XP SP3
	Windows Vista Enterprise SP1
	Windows 7 Professional SP1 32/64-bit
	Windows 7 Enterprise SP1 32/64-bit
	Windows 7 Ultimate SP1 32/64-bit
	Windows Server 2003 R2 Standard Edition 32bits
	Windows Server 2003 R2 Enterprise Edition 32bits
	Windows Server 2008 Standard Edition 32bits
	Windows Server 2008 Standard Edition 64bits
	Windows Server 2008 Enterprise Edition 32bits
	Windows Server 2008 Enterprise Edition 64bits
	Windows Server 2008 R2 Standard Edition
	Windows Server 2008 R2 Enterprise Edition

General Description and Conclusions

General tests were performed using Internet Explorer 8 (IE8) with:

- NICE Universe Web Applications 8.9
- NICE Perform
  - Release 3.1
  - Release 3.2

- ▪ Release 3.5
- ▪ NICE Interaction Management Release 4.1
- ▪ NICE Sentinel
    - ▪ Release 2.1
    - ▪ Release 2.5

Conclusions

The NICE Interaction Management/NICE Perform Applications Suite and NiceUniverse Web Application 8.9 are compatible with all tested operating systems with the following limitation: You should only run one NICE Interaction Management/NICE Perform Applications Suite or NiceUniverse Web Application per browser. See **NICE Perform R3.5/NICE Interaction Management 4.1 Known Issues with Internet Explorer 8** below.

NICE Perform R3.5/NICE Interaction Management 4.1 Known Issues with Internet Explorer 8

The following section describes NICE Perform Release 3.5/NICE Interaction Management known issues when using Internet Explorer 8, grouped according to application.

NICE Perform Release 3.x and NICE Interaction Management 4.1 Applications

Issue 1

The NICE Interaction Management/NICE Perform Web application URL must be added to the Trusted Site list. See **Manually Adding NICE Interaction Management/NICE Perform Applications to the Trusted Site List** on page 124.

Issue 2

NICE Interaction Management/NICE Perform Web applications can be used in **Internet Explorer 8** tab or **Quick** tab modes. However, in these modes, you can run one tab only with the NICE Interaction Management/NICE Perform Applications suite.

Issue 3

When the NICE Application Server is identified as an **Internet** site, the following message may appear:

NICE Perform®
Applications Suite requires
Microsoft .NET framework
version 3.5 or higher
Installed on this computer.

Install the proper version
and restart the Web
browser.

See **Adding the NICE Interaction Management/NICE Perform Web Application URL to the Local Intranet Site List** on page 128.

Issue 4

To correctly display the NICE Interaction Management/NICE Perform Application, the default documentation mode in Internet Explorer 8 should be Quirks mode. If a different mode is used, the application screen appears as shown below:
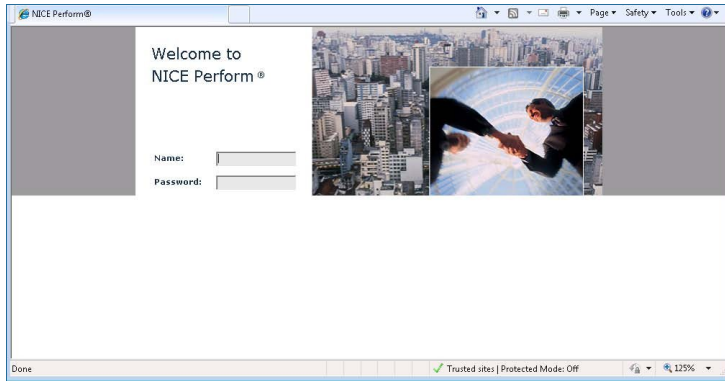
NICE Perform Applications - Release 3 SP3/SP4 and Release 3.1

Issue 1

The NICE Perform Web applications URL must be added to the Trusted Site list. See **Manually Adding NICE Interaction Management/NICE Perform Applications to the Trusted Site List** on the next page.

Issue 2

NICE Perform Web applications can be used in **Internet Explorer 8** tab or **Quick** tab modes. However, in these modes, you can run one tab only with the NICE Perform Applications suite.

NICE Universe 8.9 Web Application

Issue 1

You must configure IE8 to work with the *Protected mode* set to off. See **Configuring Internet Explorer 8/9 to Disable Protected Mode** on page 127.

Issue 2

NiceUniverse 8.9 Web Applications can be used in **Internet Explorer 8** tab or **Quick** tab modes. However, in these modes, you can run one tab only with NiceUniverse 8.9 Web Application suite.

> **NOTE:** There is no limitation on the number of open tabs per browser when only one tab is running the NICE Perform Applications suite or NiceUniverse Web Application.

Manually Adding NICE Interaction Management/NICE Perform Applications to the Trusted Site List

Perform the following procedure to manually add the Applications server to the trusted site list.

NICE Perform Release 3.x and NICE Interaction Management Release 4.1 support Internet Explorer 8/9 in both the **Quick** tab and **Single** tab modes.

❖ **To enable login to NICE Interaction Management/NICE Perform in an IE8/9 environment:**

1. On the Domain Controller do the following: In the **Run** window, type **gpmc.msc** and click **OK**.

   The Group Policy Management window appears.

   Figure 5-10: Group Policy Management Window
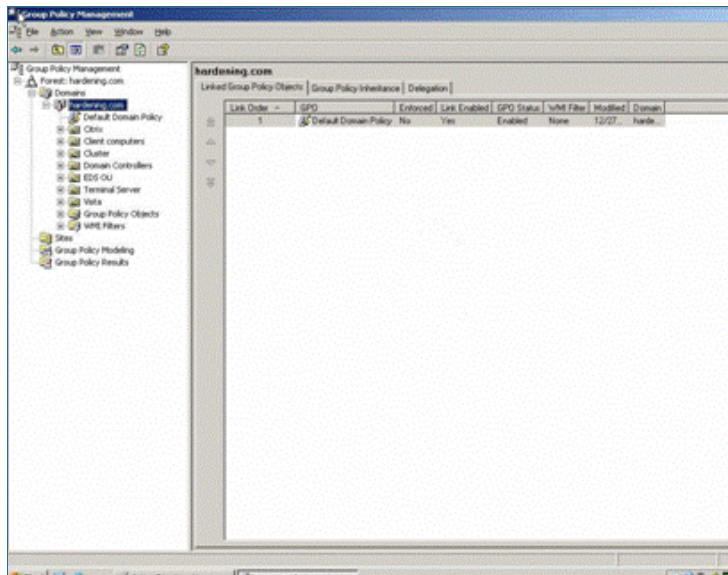
2. Right-click the **GPO** you created when you created the User Account Control and click **Edit.**

   > **NOTE:** Complete instructions for setting up the User Account Control can be found in the Microsoft Windows Vista Enterprise SP1 Workstation Configuration Guide, in the chapter: Setting up the User Account Control in an Active Directory.

3. Select **Computer Configuration > Administrator Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Pages**.

   The Group Policy Object Editor window appears.

Figure 5-11: Group Policy Object Editor Window
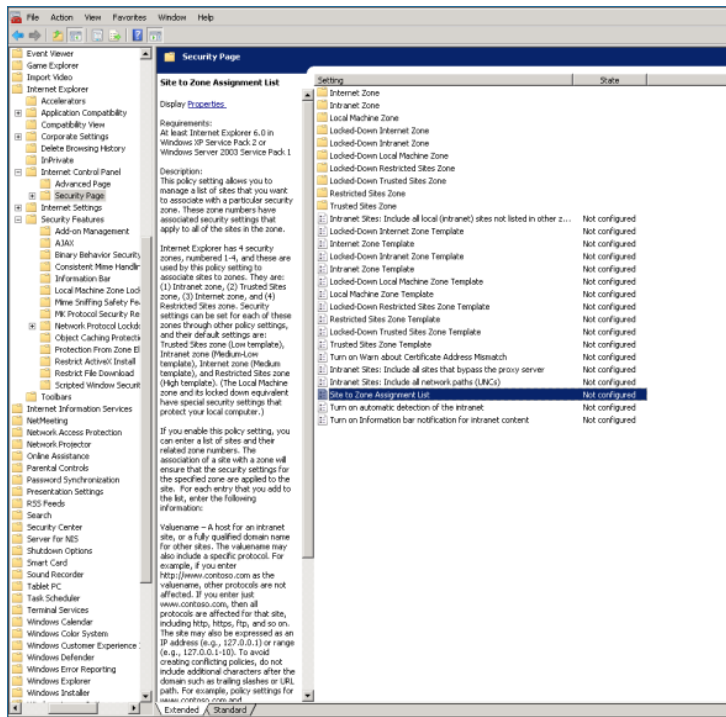
4. Double-click the **Site to Zone Assignment List** policy.

    The Site to Zone Assignment List Properties window appears.

Figure 5-12: Site to Zone Assignment List Properties Window
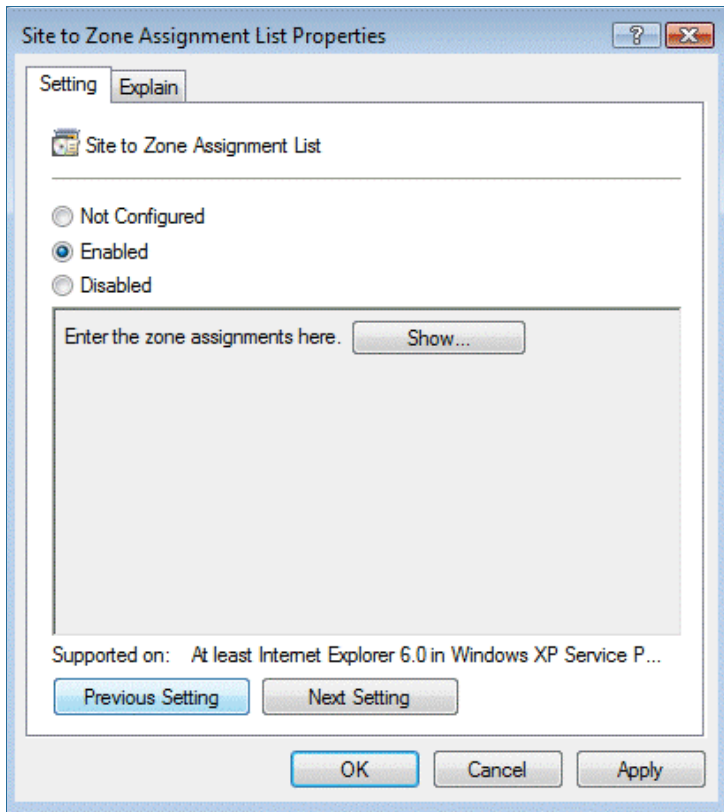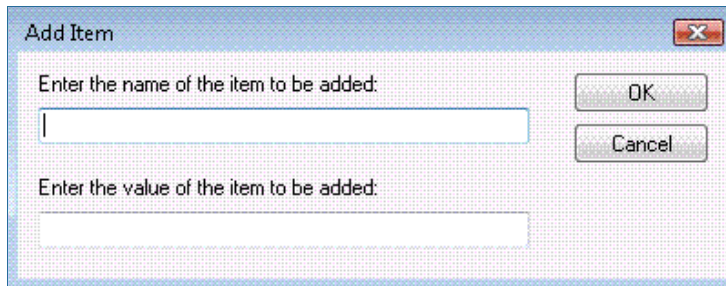
5. Select **Enabled** and click **Show.**

    The Show Contents window appears.

    Figure 5-13: Show Contents Window
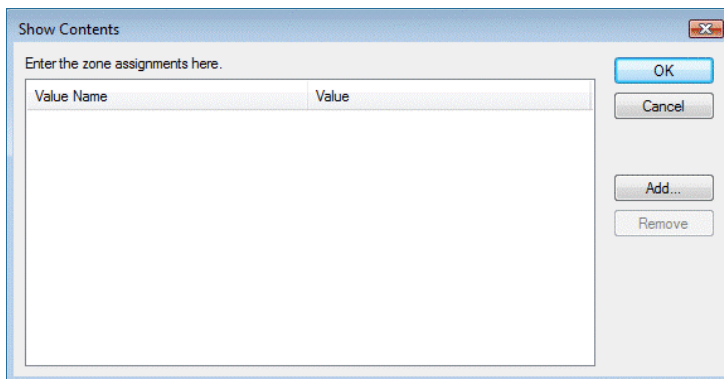
6. Click **Add.**

    The Add Item window appears.

Figure 5-14: Add Item Window

7. In the **Enter the name of the item to be added** field, enter the name of the Web Application Site.

8. In the **Enter the value of the item to be added** field, enter the digit **2** and click **OK**.

    The Show Contents window reappears.

9. Click **OK**.

    The Site to Zone Assignment List Properties window reappears.

10. Click **OK**.

    The Group Policy Object Editor Window reappears.

11. Close the Group Policy Object Editor Window.

Configuring Internet Explorer 8/9 to Disable Protected Mode

Perform the following procedure to configure Internet Explorer 8/9 to disable *Protected Mode*.

◆ **To disable** *Protected Mode***:**

1. Run Internet Explorer 8/9.

    When working with Windows Server 2008 or Windows Vista, right-click the Internet Explorer icon and select **Run as Admin.**

2. On the **Menu Bar**, select **Tools,** and then **Internet Options.**

    The Internet Options windows appears:

Figure 5-15: Internet Options Window
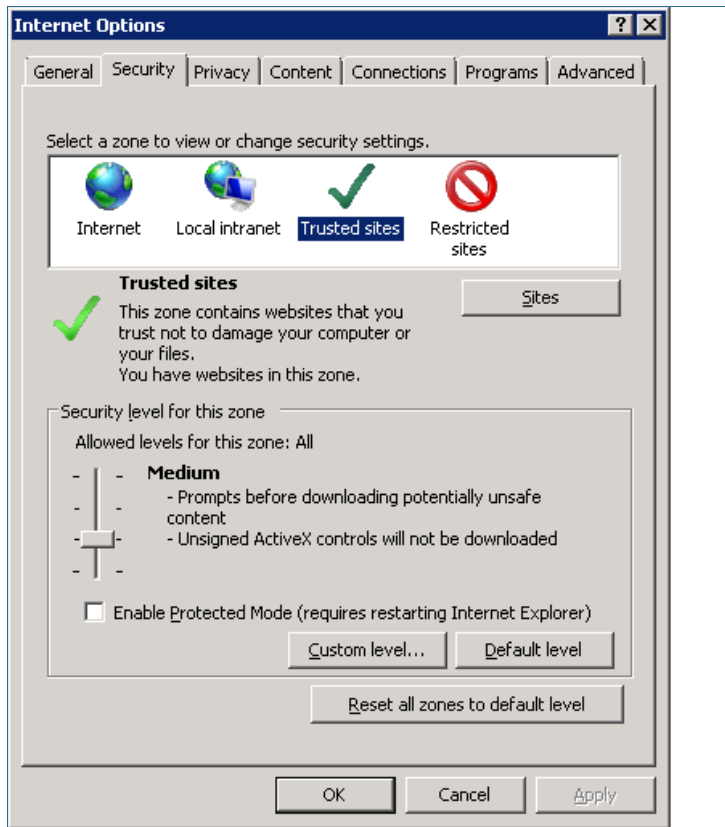
3. Click the **Security** tab. In the Security level for this zone area, make sure that **Enable Protected Mode** is not selected.

4. Click **OK**.

Adding the NICE Interaction Management/NICE Perform Web Application URL to the Local Intranet Site List

◆ **To add the NICE Perform Web application URL to the Local Intranet Site list:**

1. In the **Tools** menu of the Internet Explorer, select **Internet Options**.

2. Click the **Security** tab.

Figure 5-16: Internet Options - Security Tab
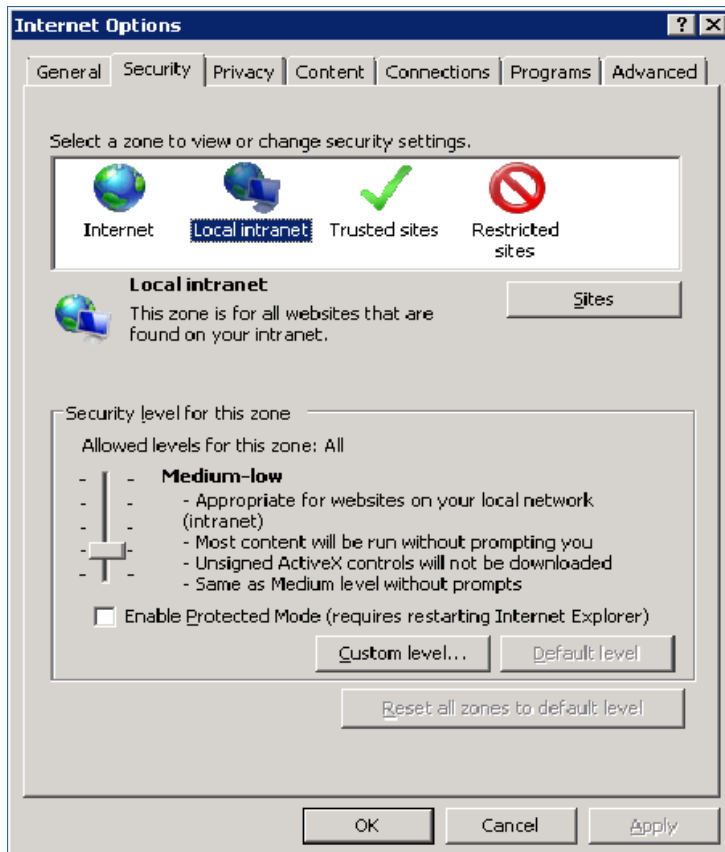
3. Click .

4. Click **Sites**.

   The Local Intranet window appears.

Figure 5-17: Local Intranet Window
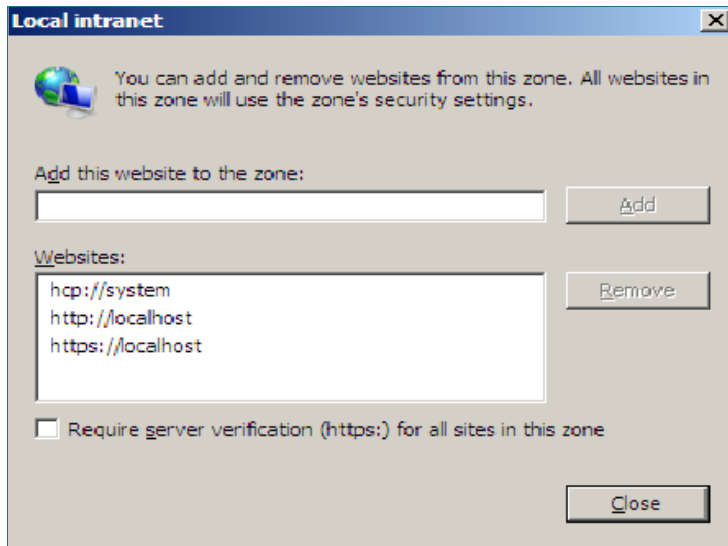
5. Enter the NICE Interaction Management/NICE Perform Web applications URL in the **Add this website to the zone** field.

6. Click **Add**.

7. Click **Close**.

8. Click **OK**.

Internet Explorer 9

Compatibility of NICE Web Applications with Internet Explorer 9 32-bit

Product	NICE Interaction Management, NICE Perform, NICE Sentinel
Release	NICE Interaction Management R4.1 NICE Perform: R3.1, R3.2, R3.5 NICE Sentinel: R2.1, R2.5
Synopsis	This section describes the compatibility of Internet Explorer 9 with NICE Web Applications when Internet Explorer 9 is installed on: Windows Vista Enterprise SP2 Windows 7 Professional SP1 32/64-bit Windows 7 Enterprise SP1 32/64-bit Windows 7 Ultimate SP1 32/64-bit Windows Server 2008 Standard Edition 32-bit Windows Server 2008 Standard Edition 64-bit Windows Server 2008 Enterprise Edition 32-bit Windows Server 2008 Enterprise Edition 64-bits Windows Server 2008 R2 Standard Edition 64-bit Windows Server 2008 R2 Enterprise Edition 64-bit

General Description and Conclusions

General tests were performed using Internet Explorer 9 (IE9) with:

- NICE Perform
  - Release 3.1
  - Release 3.2
  - Release 3.5
- NICE Interaction Management Release 4.1
- NICE Sentinel
  - Release 2.1
  - Release 2.5

Conclusions

The NICE Interaction Management/NICE Perform Applications Suites are compatible with all tested operating systems with the following limitation:

You should only run one NICE Interaction Management/NICE Perform Applications Suite per browser.

See **NICE Perform Release 3.1/3.2/3.5 and NICE Interaction Management 4.1 Known Issues with Internet Explorer 9** below.

NICE Perform Release 3.1/3.2/3.5 and NICE Interaction Management 4.1 Known Issues with Internet Explorer 9

The following section describes known issues when using Internet Explorer 9:

Issue 1

The NICE Interaction Management/NICE Perform Web application URL must be added to the Trusted Site list. See **Manually Adding NICE Interaction Management/NICE Perform Applications to the Trusted Site List** on page 124.

Issue 2

NICE Interaction Management/NICE Perform Web applications can be used in Internet Explorer 9 tab or Quick tab modes. However, in these modes, you can run one tab only with the NICE Interaction Management/NICE Perform Applications suite.

Issue 3

When the NICE Application Server is identified as an **Internet** site, the following message may appear:

NICE Perform®
Applications Suite requires
Microsoft .NET framework
version 3.5 or higher
Installed on this computer.

Install the proper version
and restart the Web
browser.

See **Adding the NICE Interaction Management/NICE Perform Web Application URL to the Local Intranet Site List** on page 128.

Issue 4

You must configure IE9 to work with the Protected mode set to off. See **Configuring Internet Explorer 8/9 to Disable Protected Mode** on page 127.

Issue 5

To correctly display the NICE Interaction Management/NICE Perform Application, the default documentation mode in Internet Explorer 8 should be Quirks mode. If a different mode is used, the application screen appears as shown below:

Internet Explorer 10

Compatibility of NICE Web Applications with Internet Explorer 10 32-bit

Product	NICE Interaction Management, NICE Perform
Release	NICE Interaction Management R4.1 NICE Perform 3.2 NICE Perform 3.5
Synopsis	Windows 7 Professional SP1 32/64-bit Windows 7 Enterprise SP1 32/64-bit Windows 7 Ultimate SP1 32/64-bit Windows Server 2008 R2 SP1 Standard Edition 64-bit Windows Server 2008 R2 SP1 Enterprise Edition 64-bit

General Description and Conclusions

General tests were performed using Internet Explorer 10 (IE10) with NICE Interaction Management Release 4.1 and NICE Perform Release 3.2 and 3.5.

Conclusions

The NICE Interaction Management and NICE Perform Applications Suites are compatible with all tested operating systems with the following limitations:

- You should only run one NICE Interaction Management Applications Suite per browser.
- When opening the Package and Evaluation windows in NICE Perform 3.2, these windows become inactive and move behind the main window. To use these windows, click their icons in the taskbar.

See **NICE Interaction Management 4.1 Known Issues with Internet Explorer 10** below.

NICE Interaction Management 4.1 Known Issues with Internet Explorer 10

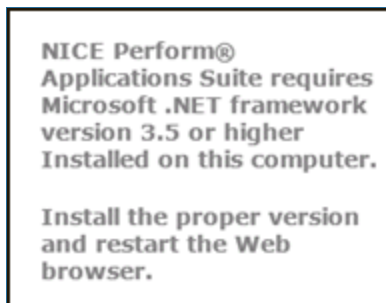The following section describes known issues when using Internet Explorer 10:

When the NICE Application Server is identified as an **Internet** site, the following message may appear:

NICE Perform Applications Suite requires Microsoft.NET framework version 3.5 or higher Installed on this computer. Instal the proper version and restart the Web browser.
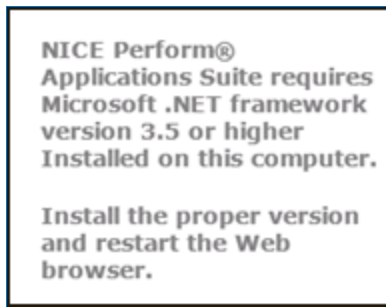
```
NICE Perform®
Applications Suite requires
Microsoft .NET framework
version 3.5 or higher
Installed on this computer.

Install the proper version
and restart the Web
browser.
```
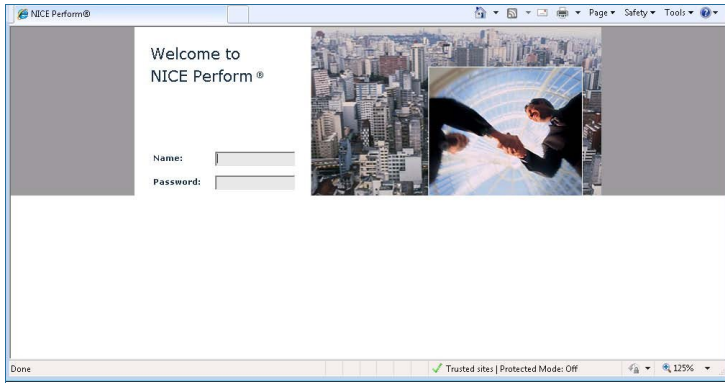
See **Adding the NICE Interaction Management/NICE Perform Web Application URL to the Local Intranet Site List** on page 128.

Adding the NICE Interaction Management Web Application URL to the Compatibility View Settings List

To ensure that NICE Interaction Management works properly when using Microsoft Internet Explorer 10, you should make sure to add the URL from the application server to the Windows Compatibility View settings.

◆ **To add the NICE Interaction Management Application URL to the Compatibility List:**

1. In the **Tools** menu of Internet Explorer, click **Compatibility View Settings**. The Compatibility View Settings dialog box is displayed.

Figure 5-18: Compatibility View Settings
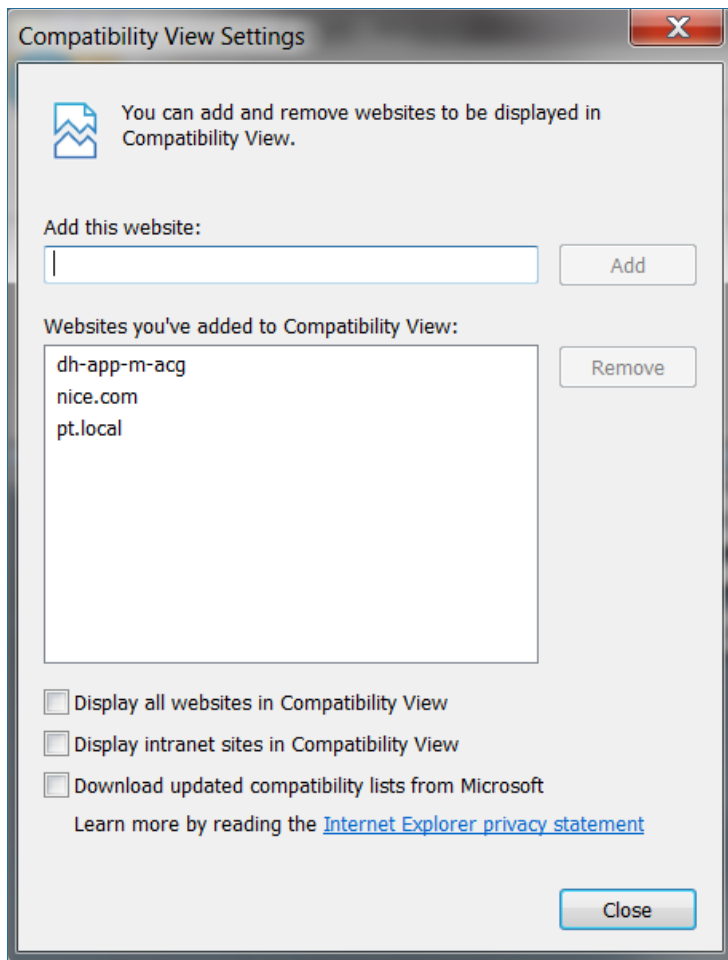
2. Type the Application Server URL for the instance of NICE Interaction Management that you are using. For example, **dh-app-m-acg**.

3. Click **Add**.

Internet Explorer 11

Compatibility of NICE Web Applications with Internet Explorer 11 32, 64-bit

Product	NICE Interaction Management,
Release	NICE Interaction Management R4.1
Synopsis	Windows 8 Professional 32/64-bit
	Windows 8 Enterprise 32/64-bit
	Windows 8.1 Professional 32/64-bit
	Windows 8.1 Enterprise 32/64-bit
	Windows 7 Professional SP1 32/64-bit
	Windows 7 Enterprise SP1 32/64-bit
	Windows 7 Ultimate SP1 32/64-bit
	Windows Server 2008 R2 SP1 Standard Edition 64-bit
	Windows Server 2008 R2 SP1 Enterprise Edition 64-bit

General Description and Conclusions

General tests were performed using Internet Explorer 11 (IE11) with NICE Interaction Management Release 4.1.

Conclusions

The NICE Interaction Management is compatible with all tested operating systems with the following limitations:

■ You should only run one NICE Interaction Management Applications Suite per browser.

■ You should only use the XBAP technology with the Windows 8.1 client system.

■ For Internet Explorer 11 on Windows 8.1, you must have NICE Interaction Management Release 4.1.46 or above.

See **NICE Interaction Management 4.1 Known Issues with Internet Explorer 11** on the next page**.**

NICE Interaction Management 4.1 Known Issues with Internet Explorer 11

The following section describes known issues when using Internet Explorer 11:

When the NICE Application Server is identified as an **Internet** site, the following message may appear:

NICE Perform Applications Suite requires Microsoft.NET framework version 3.5 or higher Installed on this computer. Install the proper version and restart the Web browser.

> NICE Perform®
> Applications Suite requires
> Microsoft .NET framework
> version 3.5 or higher
> Installed on this computer.
>
> Install the proper version
> and restart the Web
> browser.
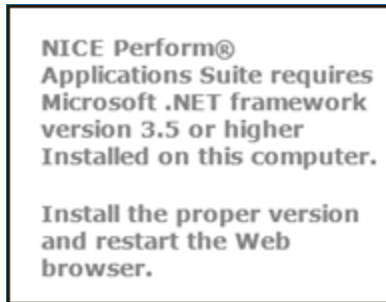
See **Adding the NICE Interaction Management Web Application URL to the Compatibility View Settings List** below

Adding the NICE Interaction Management Web Application URL to the Compatibility View Settings List

To ensure that NICE Interaction Management works properly when using Microsoft Internet Explorer 11, you should make sure to add the URL from the application server to the Windows Compatibility View settings.

◆ **To add the NICE Interaction Management Application URL to the Compatibility List:**

1. In the Tools menu, click **Compatibility View Settings**. The Compatibility View Settings dialog box is displayed.

Figure 5-19: Compatibility View Settings
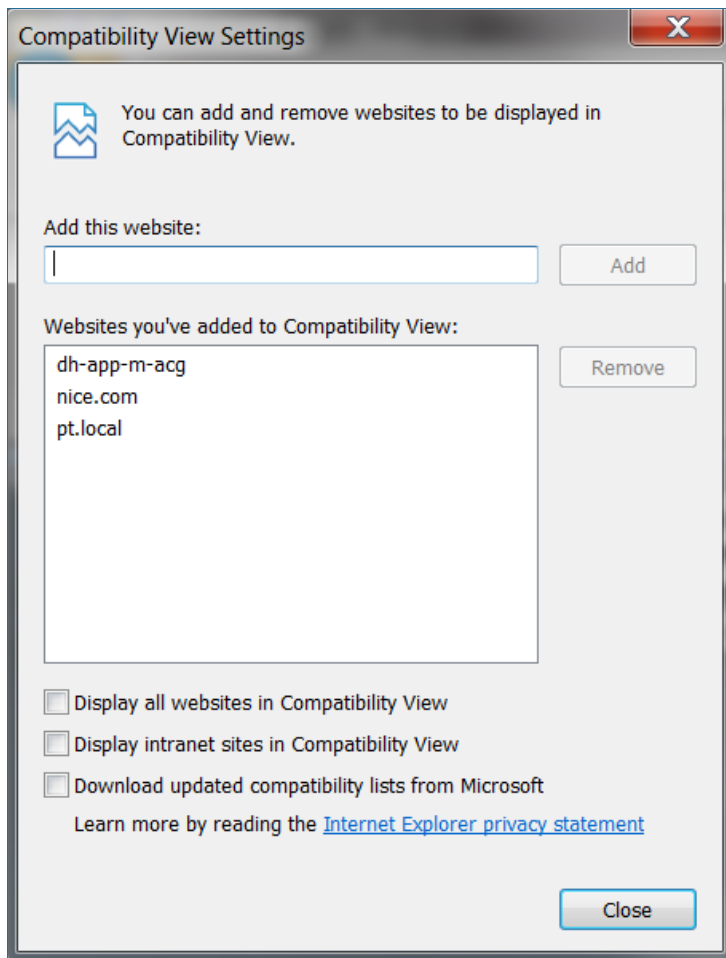
2. In the Add this website field, enter the Application Server URL for the instance of NICE Interaction Management that you are using. For example, **dh-app-m-acg**.

3. Click **Add**.

[This page intentionally left blank]

6

Microsoft .NET Framework

This chapter provides information, support, and solutions for Microsoft .NET Framework.

Contents

Nice Applications Software Requirements

Product	NiceLog & NiceUniverse
Release	
Synopsis	

Nice Applications suite version 8.8, runs today with MDAC 2.6.1 SP1 installed. This software is also installed when installing the Nice Applications suite. In those instances where there is a lower MDAC version installed, it must be upgraded.

The installation will detect the lower version and install the MDAC 2.6.1 SP1. The upgrade can also be a higher version than 2.6.1 SP1 such as 2.7 and in this case use the following procedure to upgrade the MDAC.

To upgrade the MDAC file:

1. Access the Microsoft downloads from

   http://www.microsoft.com/data/download.htm

2. Click **Microsoft Data Access Components** and select the MDAC version you require.

   Download and install the relevant file.

> **NOTE:** For OS in different languages, a suitable MDAC should be download (by choosing the language from the Combo Box

NICE Interactions Center Server Workaround for Microsoft .NET 3.5 Framework

Product	NICE Perform
Release	NICE Perform® Release 3
Synopsis	This section describes the workaround to enable configuration of the Integration software on the NICE Perform Release 3 SP4 Interactions Center server, when Microsoft .NET 3.5 Framework is installed.

Problem

The Integration software cannot be configured on the NICE Perform Release 3 SP4 Interactions Center server, when Microsoft .NET Framework 3.5 is installed. An error message that .NET 2.0 SP1 is not supported, is received.

Workaround

To work around the problem, uninstall both .NET Framework 3.5 and .NET Framework 2.0 SP1. Then install .NET Framework 2.0 and configure the Integration software. After verifying successful installation and operation, re-install .NET Framework 3.5, which automatically installs .NET 2.0 SP1.

◆ **To Work around the Problem:**

1. Uninstall Microsoft .NET Framework 3.5.:

    a. Navigate to: **Start > Settings > Control Panel > Add or Remove Programs**.

    b. Select **Microsoft .Net 3.5 Framework**.

    c. Click **Change/Remove**.

    Microsoft .NET Framework 3.5. is uninstalled.

2. Uninstall Microsoft Framework .NET 2.0 SP1.:

    a. Navigate to: **Start > Settings > Control Panel > Add or Remove Programs**.

    b. Select **Microsoft .Net 2.0 SP1 Framework**.

    c. Click **Change/Remove**.

    Microsoft .NET Framework 2.0 SP1 is uninstalled.

3. Install Microsoft .NET Framework 2.0.:

    Install Microsoft .NET Framework 2 from the CD provided by Microsoft. Follow installation instructions.

4. Configure the Integration software:

    a.   Insert the NICE Perform Release 3 Interactions Center CD.

    b.   Navigate to **Integration > Connection Manager > Drivers**.

    c.   Select **SP4.**

    d.   Double-click **setup.exe.**

       The Integration software is configured.

5.   Verify that the NICE Perform Release 3 Interactions Center has successfully configured the Integration software and is fully operational. This is assured when no error messages are displayed.

6.   Install MS .NET Framework 3.5:

Install MS .NET Framework 3.5 from the CD provided by Microsoft. Follow installation instructions.

This installation will also install .NET 2.0 SP1.

NICE Support for Microsoft .NET Framework

Product	.NET Framework Support
Release	Version 8.9, NICE Perform® Release I, II, 3, and 3.1 and above
Synopsis	This section describes support for Microsoft .NET Framework (versions 1.1, 2.0, 3.0 and 3.5) by NICE products, from V8.9 system through NICE Perform Releases I, II, 3, and 3.1 and above. This section incorporates previous NICE technical support notes for Microsoft .NET Framework (versions 1.1, 2.0 and 3.0.).

Overview

This section provides information regarding NICE products support for Microsoft .NET Framework (versions 1.1, 2.0, 3.0 and 3.5).

NICE Logger Requirements

The following NICE Logger versions require Microsoft .NET Framework 2.0:

- Logger PCI 9.01 SP8 and above
- Logger PCI 9.03 SP3 and above
- Logger 9.06
- Logger VoIP 9.12

Microsoft .NET Framework Server-Side Support

The following table lists the NICE release versions and indicates which version supports Microsoft .NET Framework (versions 1.1, 2.0, 3.0, 3.5, 4, and 4.5)

Table 6-1:
NICE Release Versions support Microsoft .NET Framework - Server-Side

No.	Release Version	Status
		Approved for all environments, except Playback Organizer version 2.
	NICE Perform Release I	Only .NET 1.1 is approved.

No.	Release Version	Status
	NICE Perform Release II	For Service Packs prior to SP4: Only .NET 1.1 is approved. For Service Packs SP4 and above: .NET 2.0 and .NET 3.0 are approved. For Service Packs SP5: .NET 3.5 is approved.
	IPC 9.09	.NET 1.1 and .NET 2.0 are approved. If .NET 2.0 is installed on server, run relevant SetSecurity applicable to .NET 2.0.
	NICE Perform Release 3	Prior to and including SP1, only .NET 1.1 is approved. For SP2 and above, .NET 2.0 is required; see the warning below. .NET 3.0 is approved. For SP4, .NET 3.5 is approved. See **NICE Logger Requirements** on the previous page**.**
	NICE Perform Release 3.1 and above/NICE Interaction Management 4.1	.NET 2.0 is required. See the warning below. .NET 2.0 Service Pack 1 is approved. .NET 3.0 is approved. .NET 3.0 Service Pack 1 is approved. .NET 3.5 is approved. .NET 3.5 SP1 is approved. .NET 4.0 is approved. .NET 4.5 is approved*.

Notes:

Microsoft .NET Framework 3.5 is required for the Telephony Services Server.

Installing Microsoft .NET Framework 3.5 Service Pack 1 also installs .NET Framework 2.0 Service Pack 2 and .NET Framework 3.0 Service Pack 2. Installing Microsoft .NET Framework 4.0 also installs Microsoft .NET Framework 3.5 Service Pack 1.

*Microsoft .NET Framework 4.5 may be installed on the server-side machine, but it is not required.

> ⚠️ **WARNING!**
>
> .NET Framework 2.0 must be installed before installing the Applications Suite.
>
> If you started installing the Applications Suite without .NET 2.0 Framework, the Applications Suite installation will fail. To solve this problem, abort the Applications Suite installation, install .NET 2.0 Framework, and then run the Applications Suite installation again.

Microsoft .NET Framework Client-Side Support

The following table lists the NICE release versions and indicates which version supports Microsoft .NET Framework (versions 1.1, 2.0, 3.0, 3.5, 4, and 4.5).

Table 6-2:
NICE Release Versions support Microsoft .NET Framework - Client-Side

No.	Release Version	Status
	8.90	Approved.
	NICE Perform Release I	Approved with Applications SP7 and above. Must be installed side by side with.NET 1.1 and the relevant hot fixes. See *RN0444 NICE Perform Applications V9.01.7.42 (SP7)* for the list of known issues.
	NICE Perform Release II	Approved with Applications SP3. Must be installed side by side with.NET 1.1 and the relevant hot fixes. See *RN0431 NICE Perform RII Applications 9.08.3.09 (SP3)* for the list of known issues. SP4 resolves the known issues which are described in RN0431. However, .NET 1.1 and .NET 2.0 must be installed side by side. For Service Pack SP5: .NET 3.5 is approved.
	IPC 9.09	.NET 1.1 and .NET 2.0 are approved. If .NET 2.0 is installed on server, run relevant SetSecurity applicable to .NET 2.0.

No.	Release Version	Status
	NICE Perform Release 3	For Release 3 SP1, only .NET 1.1 is approved. Above Release 3 SP1, .NET 1.1, .NET 2.0 and .NET 3.0 are approved. See *RN0466 NICE Perform Applications Suite Release 3 (SP1)* for the list of known issues. For Release 3 SP2 and above, .NET 2.0 is required. For Release 3 SP4, .NET 3.5 is approved. See **Microsoft .NET Framework Server-Side Support** on page 145
	NICE Perform Release 3.1 and above/NICE Interaction Management 4.1	.NET 2.0 is required. .NET 2.0 Service Pack 1 is approved. .NET 3.0 is approved. .NET 3.0 Service Pack 1 is approved. .NET 3.5 is approved. .NET 3.5 SP1 is approved. .NET 4.0 is approved. .NET 4.5 is approved*.

Notes:

Installing Microsoft .NET Framework 3.5 Service Pack 1 also installs Microsoft .NET Framework 2.0 Service Pack 2 and Microsoft .NET Framework 3.0 Service Pack 2. See Figure 1-1 (from the .NET Framework Developer's Guide). Installing Microsoft .NET Framework 4.0 also installs Microsoft .NET Framework 3.5 Service Pack 1.

*Microsoft .NET Framework 4.5 may be installed on the client-side machine, but it is not required.

Figure 6-1: .NET Framework Developer's Guide

Microsoft .NET Framework 4 Requirement for NICE Interaction Management 4.1

Microsoft .NET Framework 4 is now required for all NICE Interaction Management 4.1 sites. See the *Certified Servers Guide* for more details about requirements.

SRT release 2.5.6 and later will check for Microsoft .NET Framework 4. SRT releases before 2.5.6 will not fail if Microsoft .NET Framework 4 is installed, but also will **not** notify if Microsoft .NET Framework 4 is not installed. Therefore, you must manually check whether Microsoft .NET Framework 4 is installed by looking at the components in the Add/Remove Programs window.

If IIS is installed after Microsoft .NET Framework 4, change the Application Pool to .NET2 as described below.

To change the Application Pool to .NET2:

1. Select **Start > Run**. The Run window appears.

2. Enter **inetmgr** and then click **OK**.

   The Internet Information Services (IIS) Manager window appears.

   Figure 6-2: Internet Information Services (IIS) Manager Window
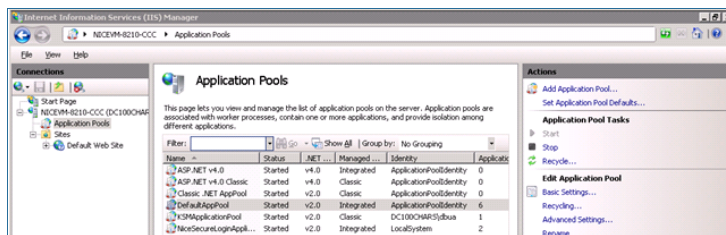
3. In the **Connections** pane on the left side, click **Application Pools**.

4. In the **Application Pools** list, double-click **DefaultAppPool**. The Edit Application Pool window appears.

Figure 6-3: Edit Application Pool Window
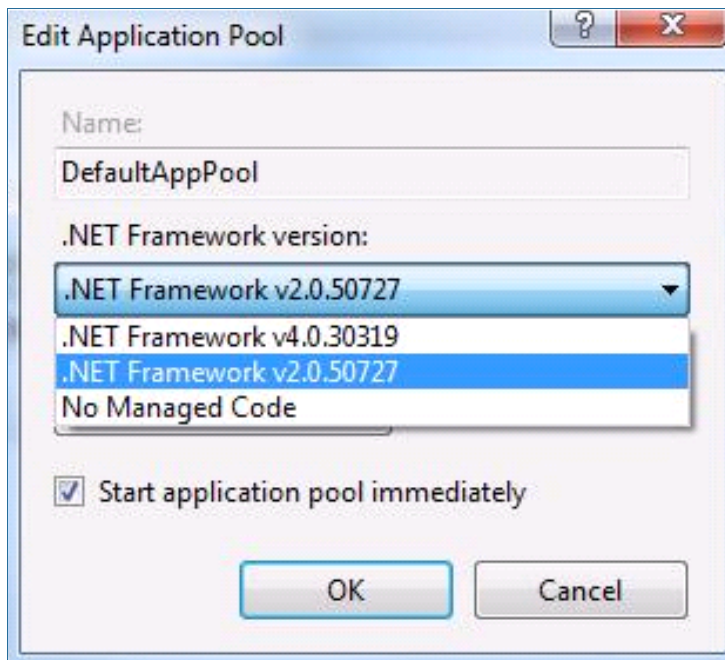
5. From the .NET Framework dropdown menu, select **.NET Framework v2.0.50727**.

6. Click **OK**.

7. In the **Actions** pane on the right side, click **Recycle**.

Microsoft .NET Framework 4.5 with NICE Perform 3.2/3.5 and NICE Interaction Management 4.1

> **NOTE:**
>
> ■ The information in this section is relevant when using ASP.NET. For example you will have a URL with an .aspx exention as shown in the following example:
>
> `http://<server name>/NiceApplications/Desktop/webpage/DeskTopWebForm.aspx`
>
> ■ For .Net4.0 support and up using NICE Interaction Management 4.1.46, please see **Microsoft .NET Framework 4.0 and up with NICE Interaction Management 4.1.46 and Later** on page 154

Microsoft .NET Framework version 4.5 has been tested and approved for use with NICE Perform 3.2/ 3.5, and with NICE Interaction Management 4.1

Installing Microsoft .NET 4.5 on machines may cause a problem with the login procedure to NICE Perform/NICE Interaction Management. The following error message may appear during the initialization phase.

Figure 6-4: Error Message During Initialization Phase of NICE Perform/NICE Interaction Management

To fix this problem, the EnableIEHosting value of the registry subkey HKLM/SOFTWARE/MICROSOFT/.NETFramework must be set to 1. For more details please read the Microsoft article Application Compatibility in the .NET Framework 4.5.

◆ **To work around the problem:**

1. Click **Start**>**Search**, and in the search field, type **Regedit**.

Figure 6-5: Regedit Search Results
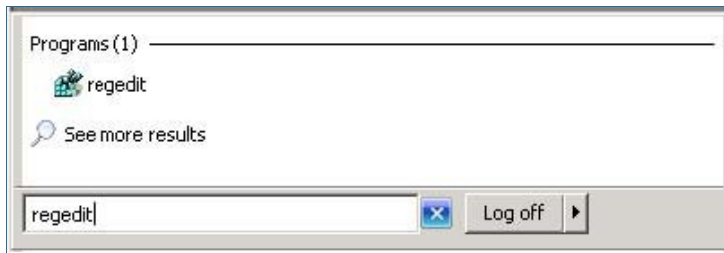
2. Right-click the **Regedit** icon and select **Run as Administrator** from the menu.

3. Enter the correct user credentials for working with registries.

4. Follow the link mentioned above to find the required registry folder.

📌 **NOTE:** The registry path is different for 32-bit and 64-bit Windows operating systems:

■ 32-bit: HKLM\SOFTWARE\MICROSOFT\.NETFramework

■ 64-bit: HKLM\SOFTWARE\Wow6432Node\Microsoft\.NETFramework

5. Right-click in the registry folder and select **New**>**DWORD (32-bit) Value** to create a new DWORD value key.

Figure 6-6: Creating a New DWORD Value Key in the .NET Framework Registry
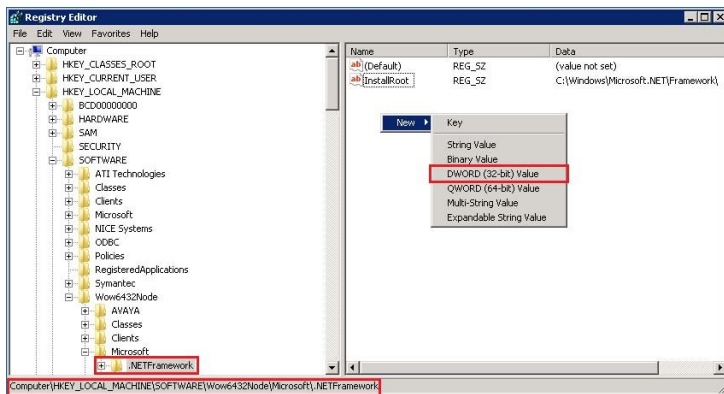
6. Rename the new key as follows: **EnableIEHosting**

Figure 6-7: New EnableIEHosting DWORD
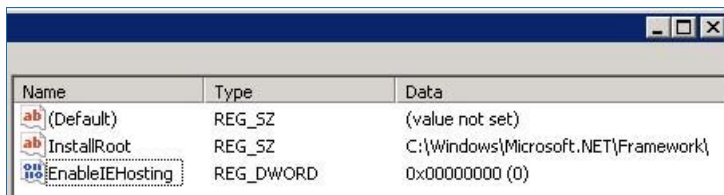
7. Right-click the EnableIEHosting key and select **Modify** from the menu.

Figure 6-8: Modify New EnableIEHosting DWORD
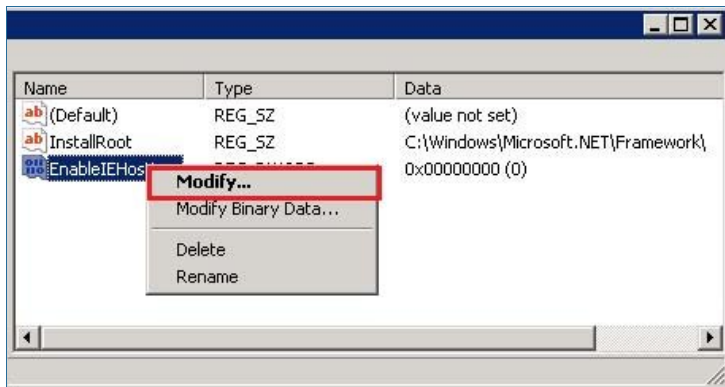
8. In the Edit DWORD (32-bit) Value window that appears, type **1** in the **Value data** field and click **OK**.

Figure 6-9: DWORD Value
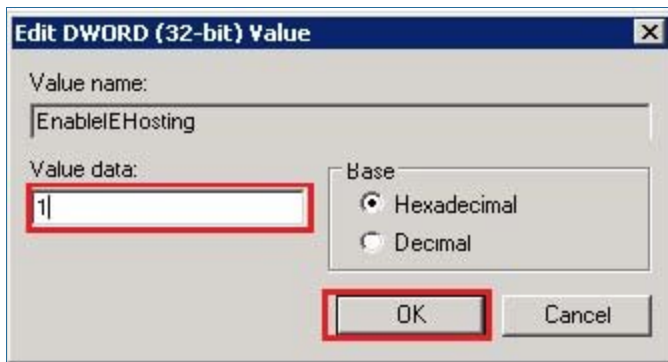
📄 **NOTE:** If this procedure must be performed on multiple client/server machines, use the SCCM/SMS package that contains the registry file to create the EnableIEHosting registry subkey.

Microsoft .NET Framework 4.0 and up with NICE Interaction Management 4.1.46 and Later

If your client machine has the Microsoft .NET Framework version 4.0 and up, when you sign in to NICE Interaction Management, you will notice that the extension is .XBAP. You must note the following when working with an XBAP page.

- Internet Explorer 10 works with XBAP only when using compatibility mode (Compatibility mode is the Microsoft Internet Explorer default mode). For information on using NICE Interaction Management in compatibility mode, see **Adding the NICE Interaction Management Web Application URL to the Compatibility View Settings List** on page 135.

- If you changed your system configuration to work with .NET Version 4.5 when using Release 4.1.45, you can revert back to the original system configuration if you install NICE Interaction Management 4.1.46 or later.

- When using XBAP, the **Tool** menu disappears from the Internet Explorer tool bar. To view the tool menu, you can do one of the following:

    - Open a new tab. The **Tools** menu will be available in the new tab.

    - Click the **Internet Options** button in Internet Explorer and use the **Internet Options** window. If this button does not appear, right-click in the Button bar and add it.

- The URL address to any NICE Interaction Management projects you were using will be different when using XBAP.

    Instead of the ASPX link **http://<server name>/NiceApplications/Desktop/webpage/DeskTopWebForm.aspx**, the new address will be **http://<server name>/NiceApplications/Desktop/XbapApplications/NiceDesktop.XBAP**.

- NICE Interaction Management 6.3 is designed to work only with XBAP, but not with ASPX.

    If you previously created shortcuts/favorites,then replace all previously saved links to the new address.

For information on setting up the client computer to work with ASPX, see *Using ASPX to Log In To NICE Interaction Management When Using .NET 4.0 or Higher* in the *Workstation Setup Guide*.

Working with XBAP or ASPX (ASP.NET)

Beginning with NICE Interaction Management 4.1.46, XBAP can be used to log in to NICE Interaction Management / NICE Engage Platform when the client workstation is working with Microsoft .NET4.0 or higher.

Why XBAP?

XBAP is a Windows Presentation Foundation (WPF) technology deployed with ClickOnce by Microsoft. It allows Internet Explorer (IE) hosting when .NET4.5 is installed.

If you are working on a system with Microsoft .NET 4.0 or higher, XBAP is automatically used to sign in to NICE Interaction Management / NICE Engage Platform.

Limitation:

Internet Explorer 10 works with XBAP only when using compatibility mode (Compatibility mode is the Microsoft Internet Explorer default mode).

For information on using NICE Interaction Management / NICE Engage Platform in compatibility mode, see the section *Internet Explorer* in *Third-Party Guidelines*.

Why ASPX?

ASPX is used if you are working with a .NET version lower than 4.0.

Contents

Using XBAP

When using with Microsoft .Net Version 4.0 or higher, you automatically log in to an XBAP page. If you need to log in to NICE Interaction Management in ASPX, you must manually configure your client machine to use ASPX .

Contents

Installing the NICE Security Certificate for XBAP

This section describes how to install XBAP with the NICE XBAP Security Certificate. This procedure prevents the security warning messages from appearing on the clients workstations. See Figure 7-8 in **Using XBAP Without the NICE Security Certificate**.

Before You Begin

- You must have Microsoft .NET 4.0 or higher installed on your client machine.

- You must install NICE Interaction Management / NICE Engage Platform.

- Enter the URL for the NICE Interaction Management / NICE Engage Platform Application Server to the trusted site groups in Internet Explorer.

- Deploy the NICE XBAP Security Certificate to workstations using a Group Policy (GPO).

- Install XBAP on workstations.

> **NOTE:** XBAP can only work with the latest UrlScan. If you installed UrlScan before 20 July 2014, download the latest version from the Software Download Center (SDC) and install it according to the instructions in the *Hardening Guide for Windows 2008 R2*.

To install the NICE XBAP Security Certificate:

1. On the relevant Active Directory Domain Controller (DC) Server, download and install the NICE XBAP Security Certificate by doing the following:

   a. From the NICE Software Download Center, download the ZIP file containing the NICE XBAP Security Certificate ZIP file. For example: **NICEVerisignXBAP.zip**.

   b. Extract the content of the NICE Security Certificate ZIP file.

> **NOTE:** File names in the NICE XBAP Security Certificate ZIP file may change.

c. Follow Microsoft instructions in **http://technet.microsoft.com/en-us/library/cc770315 (vws.10).aspx** for deploying the NICE XBAP Security Certificate by creating an Active Directory Group Policy.

d. In the Group Policy, import the extracted ***.p7b** certificate to the **Trusted publishers** folder.

Figure 7-1: Trusted Publishers Folder
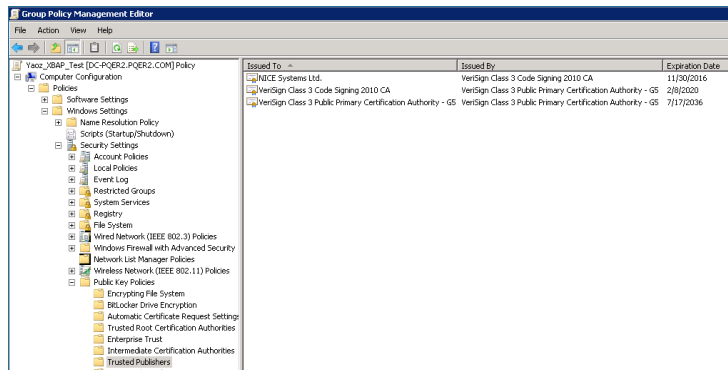
e. In the Group Policy, move the file **VeriSign Class 3 Code Signing 2010 CA** to the **Intermediate Certifications Authorities** folder.

Figure 7-2: Intermediate Certifications Authorities Folder
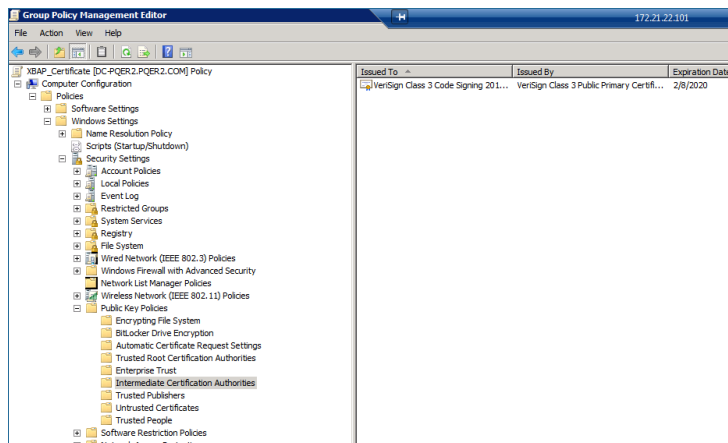
> **NOTE:** The **Public Primary** Security Certificate is included by default in every machine,
> and is not mandatory for the Group Policy Object (GPO).

2. In the workstation computer, when logging in for the first time, open a new Internet Explorer window and enter the following URL: **http://<server name>/nice**. The server name is the name of the NICE Interaction Management / NICE Engage Platform Applications Server.

The following window appears:

Figure 7-3: NICE Interaction Management / NICE Engage Platform Applications Suite Security Windows
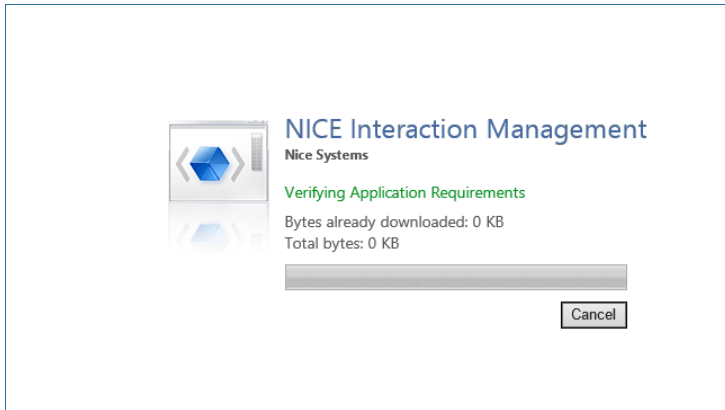
3. Once the installation finishes, you are prompted to log into NICE Interaction Management / NICE Engage Platform with your credentials.

> **NOTE:**
>
> ■ When using XBAP the Internet Explorer **Tools** menu item disappears from the display.
>
> **Figure 7-4: Normal Internet Explorer Display**
>
>
>
> **Figure 7-5: XBAP Internet Explorer Display**
>
>
>
> ■ When using XBAP the URL address changes from **.aspx** to **NICEDesktop.xbap**.
>
> **Figure 7-6: XBAP URL**
>
>
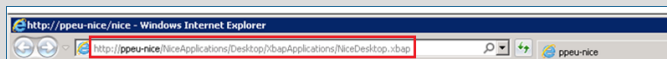
Using XBAP Without the NICE Security Certificate

This topic describes how to prepare the client machine to work with XBAP.

> **NOTE:**
>
> ■ If you followed the instructions in **Installing the NICE Security Certificate for XBAP** on page 156, XBAP is already installed and you do not need to follow this procedure.
>
> ■ To avoid the **Application Run - Security Warning Window** on the next page security warning, follow the procedure described in **Installing the NICE Security Certificate for XBAP** on page 156.

Before you begin, note the following:

■ You must have Microsoft .NET 4.0 or higher installed on your client machine.

■ Enter the site for your NICE Interaction Management application server in the Local Intranet Group in Internet Explorer.

■ Install XBAP on the client machine.

To install XBAP:

1. Open a new Internet Explorer window and enter the following URL:

   :http://<server name>/nice or : **https://<server name>/nice**.

   The server name is the name of the NICE Interaction Management / NICE Engage Applications Server.

   The following windows appear:

Figure 7-7: NICE Interaction Management / NICE Engage Platform Applications Suite Verifying Application Requirements Window
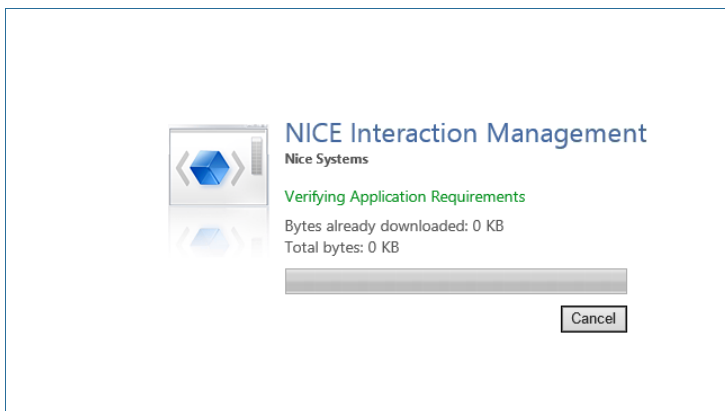
Figure 7-8: Application Run - Security Warning Window
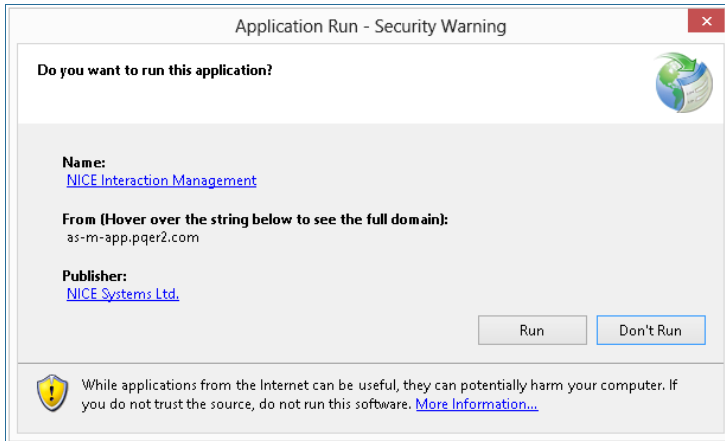
2. Click **Run** and wait for the XBAP installation to finish.

3. After the successful installation, you are prompted to log into NICE Interaction Management / NICE Engage Platform with your credentials.

> **NOTE:**
>
> ☐ Administrative rights are not required for this action.
>
> ☐ When using XBAP the Internet Explorer **Tools** menu item disappears from the display.
>
> **Figure 7-9: Normal Internet Explorer Display**
>
>
>
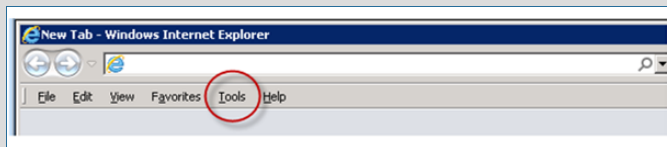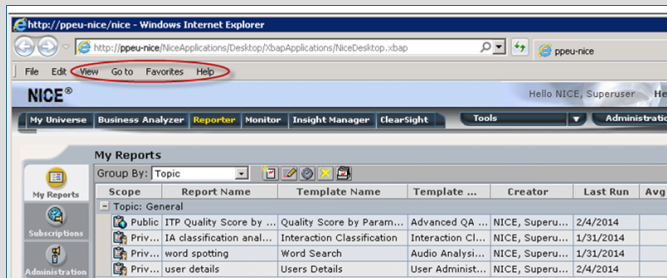> **Figure 7-10: XBAP Internet Explorer Display**
>
>
>
> ☐ When using XBAP the URL address changes from **.aspx** to **NICEDesktop.xbap**.
>
> **Figure 7-11: XBAP URL**
>
>
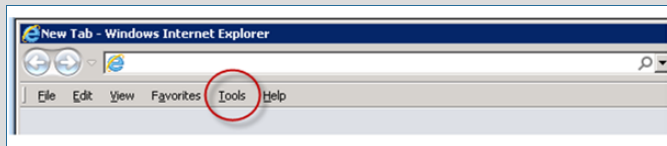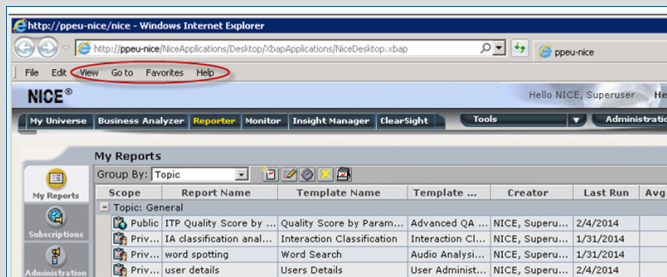
Configuring XBAP with NICE Interaction Management 4.1.4x

If you are already using NICE Interaction Management 4.1.46 or higher, and have .NET 4.0 or higher installed on the client machine, you can switch to using XBAP.

◈ **To switch to XBAP if you are using .NET 4.0:**

1. Log in to NICE Interaction Management at `http://<ServerName>/nice or https://<ServerName>/nice`.

   Where the server name is the name of the NICE Interaction Management Applications Server.

2. Install the XBAP applications as described in **Using XBAP Without the NICE Security Certificate** on page 158.

◈ **To switch to XBAP if you are using .NET 4.5:**

1. From the search box in the **Start** menu, type `regedit`.

2. From the menu list, right-click regedit and select Run as Administrator.

3. Enter the correct user credentials

4. In the Registry Editor, browse to the registry folder. The registry folder that you need differs for 32-bit and 64-bit systems.

   For 32-bit: `HKLM\SOFTWARE\MICROSOFT\.NETFramework`

   For 64-bit: `HKLM\SOFTWARE\Wow6432Node\Microsoft\.NETFramework`

5. Right-click `EnableIEHosting` and select **Delete**.

6. Click **Yes** to confirm that you want to delete this key from the Registry.

7. Install the XBAP applications as described in **Using XBAP Without the NICE Security Certificate** on page 158.

Using XBAP with Release 4.1 and 6.3 on Same Site

XBAP has to be installed with the same version across the site to work.

> ❗ **Important!**
>
> Both NICE Interaction Management 4.1.48 and NICE Engage 6.3.4 include integration with XBAP 7.0.0.0.
>
> This procedure is only applicable for NICE Interaction Management 4.1.47 and below.

In sites that use NICE Interaction Management and NICE Engage Platform 6.3, different versions of XBAP may be installed. In such cases, when attempting to use XBAP an Application Deployment Error appears.

Figure 7-12: Application Deployment Error
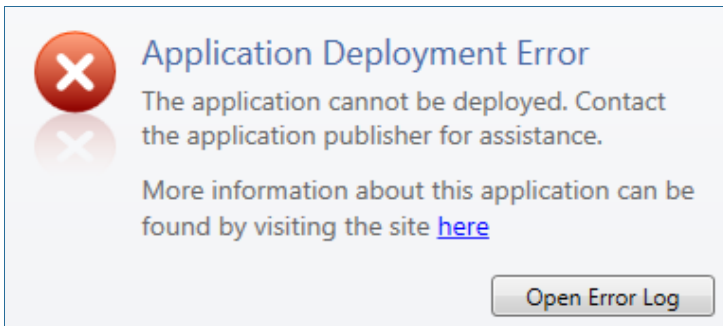
Resolve this error by setting XBAP to the same release on all Application Servers.

Before You Begin

This procedure is only applicable for NICE Interaction Management Release 4.1 4.1.47 and below. If a higher version is installed, do not complete this procedure.

◆ **To set the same XBAP version for all releases:**

1. Determine which Application Server hosts NICE Engage Platform, and which Application Server hosts NICE Interaction Management.

2. In the Application Server that hosts NICE Interaction Management, create a backup of the **XbapApplications** folder which is located in:

   <drive>:\Program files\NICE\Systems\Applications\Desktop\XbapApplications

3. In the Application Server that hosts NICE Engage Platform, copy the **XbapApplications** folder.

4. Paste the **XbapApplications** folder into the same location in the NICE Interaction Management Application Server.

5. Clear the catch in Internet Explorer (IE) by doing the following:

   a. Open IE and from the **Safety** drop-down menu, select **Safety > Delete Browsing History...**

Figure 7-13: Internet Explorer Safety Tab
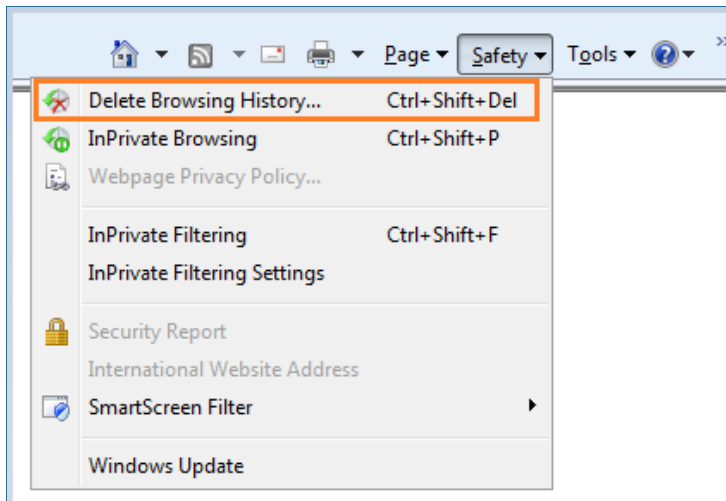
The Delete Browsing History window appears.

b. In the Delete Browsing History make sure the following options are selected:

  ▪ Temporary Internet files

  ▪ Cookies

  ▪ History

Figure 7-14: Delete Browsing History
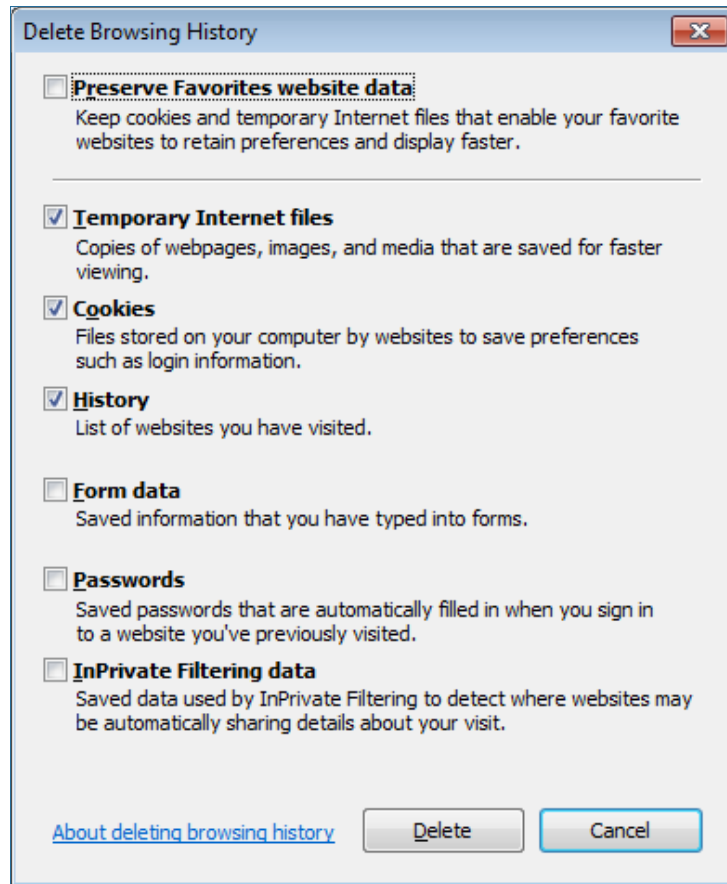
c. Click **Delete**.

6. In the NICE Interaction Management Application Server, Restart the following services:

- Microsoft Internet Information Server (IIS)
- NICE System Administrator

Uninstalling XBAP

In case an error occurs during XBAP deployment, use this section to uninstall XBAP.

After XBAP is uninstalled, it is automatically installed again, when Internet Explorer is next run.

◈ **To uninstall XBAP:**

1. In the client workstation, close Internet Explorer.

2. Navigate to: **<user>\AppData\Local**.

3. Delete the **Apps** folder.

4. Run Internet Explorer and start NICE Interaction Management / NICE Engage Platform. XBAP installs again on the workstation.

Using ASPX (ASP.NET)

To log in to NICE Interaction Management / NICE Engage Platform in ASPX, you must manually configure your client machine to use ASPX .

> **NOTE:** XBAP is used only for NICE Interaction Management Version 4.1.46 and higher.

Contents

Setting up ASPX with .NET 4.0

If Microsoft .Net 4.0 is installed on the client machine, do the following:

◆ **To set up ASPX for .NET 4.0:**

1. In the Windows Internet Explorer window, from **Tools** select **Internet Options**.

Figure 7-15: Internet Options Window
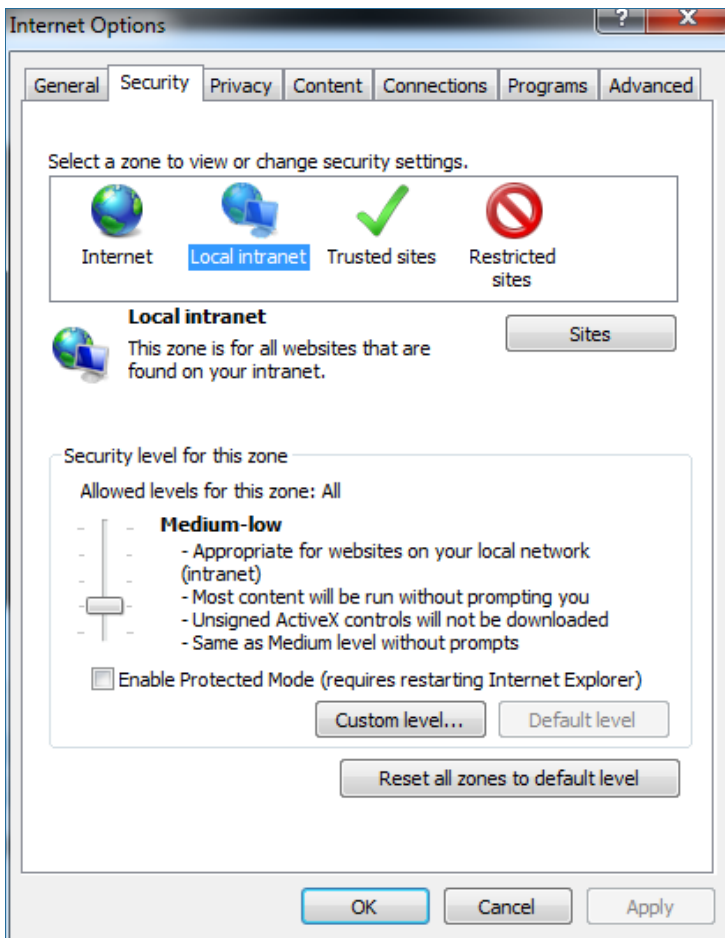
2. In the **Security** tab, select **Local intranet**, and then click **Sites**.

    The Local Intranet window appears.

Figure 7-16: Local Internet Window
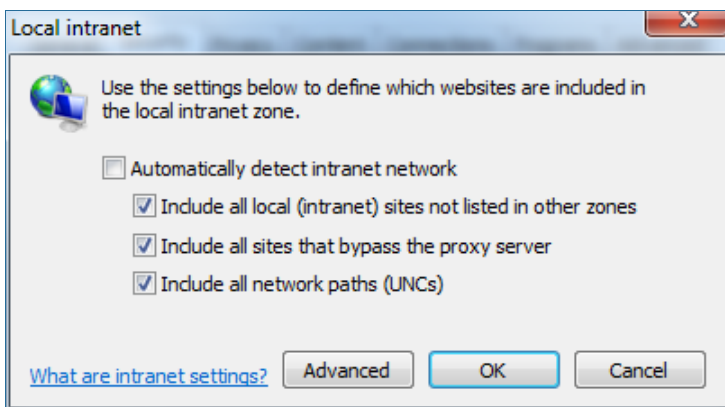
3. Click **Advanced**.

   The Local Intranet-Add Website window appears.

   Figure 7-17: Add Websites
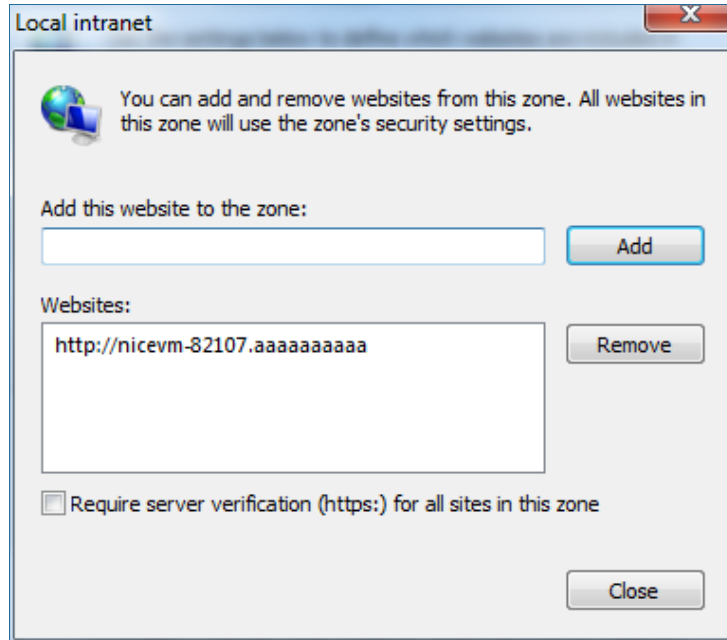
4. Enter the name of the NICE application server in the **Add this website to the zone** field.

5. Click **Add**.

6. Click **Close** to close the window.

7. Click **OK** to close the Internet Options window.

8. Run the NICE SetSecurity Application. See *NICE SetSecurity Application* in the *Workstation Setup Guide*.

Setting up ASPX with .NET 4.5

If you are using Microsoft .NET 4.5 and need to use ASPX, you must do the following in the Registry Editor, then follow the directions in **Setting up ASPX with .NET 4.0** on page 166.

➭ **To make changes in the Registry Editor**

1. From the search box in the **Start** menu, type `regedit`.

2. From the menu list, right-click regedit and select **Run as Administrator**.

3. Enter the correct user credentials

4. In the Registry Editor, use the path below to browse to the `.NETFramework` registry folder. Select that folder.

The registry folder that you need differs for 32-bit and 64-bit systems:

- For 32-bit: `HKLM\SOFTWARE\MICROSOFT\.NETFramework`
- For 64-bit: `HKLM\SOFTWARE\Wow6432Node\Microsoft\.NETFramework`

5. Right-click the correct folder and go to New then select DWORD (32-bit) Value.

Figure 7-18: DWORD Value
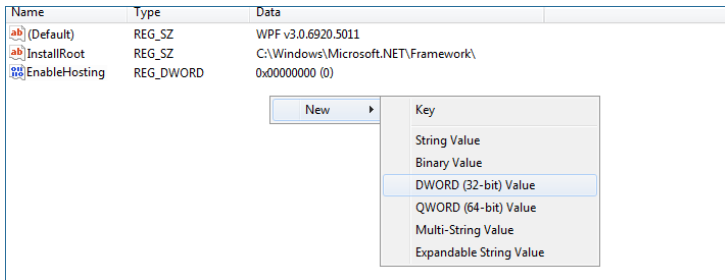
6. Rename the new key **EnableIEHosting**.

7. Right-click the **EnableIEHosting** key that you just created and select **Modify**.

8. The Edit DWORD (32-bit) Value window appears.

Figure 7-19: Edit DWORD Value
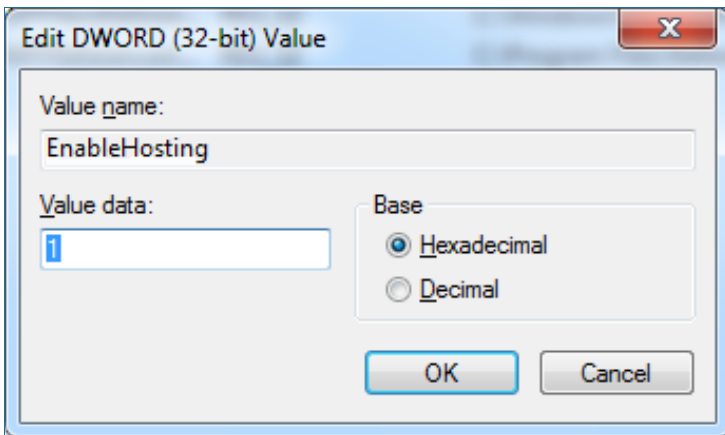
9. In the Edit DWORD (32-bit) Value window, type 1 in the **Value** data field.

[This page intentionally left blank]

8

Microsoft SQL Server

This chapter describes support for the various Microsoft SQL Server versions.

Contents

SQL Server 2000 SP4

Product	SQL Server 2000 SP4
Release	
Synopsis	

Microsoft SQL Server 2000 SP4 was tested on all NICE components running with Microsoft SQL Server 2000 as set out in the table below.

Table 8-1:
Microsoft SQL Server 2000 SP4

SQL Server 2000 Type	Component	OS
SQL Server 2000 Server Edition	CLS 8.70	Windows NT Server
	CLS 8.80	Windows 2000 Server
	CLS 8.90	Windows 2003 Standard Edition
	CLS 8.93	Windows 2003 Standard Edition
	NICE Perform	Windows 2003 Standard Edition
SQL Server 2000 Personal Edition	NCF I	Windows NT WS
	NCF II	Windows 2000 Professional
	NCF III	Windows XP
	Loggers Only 8.80	Windows 2000 Professional
	Loggers Only 8.90	Windows 2003 Standard Edition
	Advantage	Windows 2000 Professional

SQL Server 2005 for NICE Perform Release 3

Product	NICE Perform®
Release	NICE Perform Release 3
Synopsis	This section describes the Microsoft SQL Server versions supported by NICE Perform Release 3.

NICE Perform Release 3 uses Microsoft SQL Server 2005 (Standard Edition) for its database and Data Mart infrastructure.

NICE upgraded to SQL Server 2005 for its outstanding security and advanced business intelligence capabilities, as well as its improved performance and maintainability.

Supported SQL Server Versions

NICE Perform Release 3 is designed for optimal use of SQL Server 2005, with new features such as:

- **Media Encryption** – For securing the cryptographic information that is used for encrypting the captured voice and screen media, and is stored in the Cryptographic Database.
- **NICE Perform - IEX Integration.**
- **Interaction Analytics' ClearSight**^{TM} – For Root-Cause Analysis.
- **Interaction Analytics' Transcription (Speech to Text).**

For a detailed overview of SQL Server 2005 additional benefits see Microsoft's The Business Value of Upgrading to SQL Server 2005 white paper, (October 2005).

For all new installations, SQL Server 2005 Standard Edition is used by default. Use of SQL Server 2000 will not be allowed for any new installation of NICE Perform Release 3.

Existing implementations using SQL Server 200, either 8.9 or NICE Perform Releases 1 and 2, wishing to upgrade to NICE Perform Release 3, will also require database migration.

Existing implementations of NICE Perform Release 3 pre-GA version, using SQL Server 2000, will be able to continue using the existing SQL Server 2000 installation for a limited time, unless they want to take immediate advantage of the NICE Perform Release 3 features mentioned above. NICE Perform Feature Pack 1, which is expected mid 2008, will require SQL Server 2005. Therefore, NICE strongly recommend prompt migration to SQL Server 2005 for all customers.

SQL Server Clustering

SQL Server 2005 Standard Edition supports SQL Server clustering.

SQL Server clustering also requires Microsoft Windows Server 2003 Enterprise Edition and certified hardware.

SQL Server Licensing

Customers can purchase SQL Server software and licenses from NICE or provide SQL Server software and licenses on their own.

> **NOTE:** The NICE Perform Application Suites do not include SQL Server software and licenses for the database servers.

SQL Server Software and Licenses Purchased from NICE Systems

Customers can purchase the following types of SQL Server 2005 Standard Edition licenses from NICE:

Table 8-2:
SQL Server Licenses

SQL Server License	Price List Item	Description
Server and Client Access License (CAL)	SQL-CAL-LIC	User based licensing suitable for deployments where only a limited number of users are using the NICE applications.
		The customer needs to purchase as many CALs as the number of users/devices that access the SQL Server directly or indirectly.
		Each Device CAL permits one device, used by any user to access the SQL Server.
		Each User CAL permits one user, using any device, to access the SQL Server.
		Any Device and User CAL combination can be used: You may select to purchase the minimum number of required CALs based on number of seats or number of users, but the purchase order must include a certain minimum number of CALs (see note below).
Per-Processor License	SQL-CPU-LIC	SQL Server Per-Processor licensing is based on the number of CPUs on the server machine that runs the SQL Server. A Per-Processor license supports an unlimited number of users.
		To encourage the use of dual-core processors, Microsoft charges the same amount of money per processor, regardless of the number of cores in the processor.

> 📝 **NOTE:**
>
> SQL-CAL-LIC and SQL-CPU-LIC price list items see SQL Server 2005 only. For a limited time, you may continue and use the former DUAL-CPU-SQL price list item to order additional Per-Processor licenses for SQL Server 2000 for existing pre-GA installations of NICE Perform Release 3. See **Special Notes for New and Old Price Lists** on page 177 below.
>
> - User based licensing shall be used for the NICE Perform Interaction Package only. For all NICE Perform application packages other than the Interaction Package, and for Interaction Package deployments with a large number of users/seats (50 or more users/seats), Per-Processor (CPU) based licensing shall be used.
>
> - In user based licensing, a CAL is required for each user/seat that accesses the database server directly or indirectly. Hence, users of the ROD application also require CALs.
>
> - For user based licensing, the purchase order must include a minimum of five CALs, (5 SQL-CAL-LIC).

If the SQL Server software and licenses are purchased from NICE, then NICE provides the customer with the SQL Server Auto-Setup Installation CD and a printed SQL Server End-User License Agreement (EULA) stating the number of licenses and their type. The Auto-Setup CD can also be used to upgrade an existing SQL Server 2000 installation to SQL Server 2005.

SQL Server software and licenses purchased from NICE cannot be used for any purpose other than to serve NICE products. The SQL Server installation is embedded in the NICE Perform SQL Server Auto-Setup installation and cannot be separated from it. The installation is performed by a certified installer of NICE or a business partner.

The SQL Server Auto-Setup installation is followed by the NICE Perform Database Suite installation and the NICE Perform Application Server installation.

Customer-Provided SQL Server Software and Licenses

NICE allows customers to provide SQL Server software and licenses on their own.

In this case, the customer is responsible for providing a machine with an installed SQL Server. The following is required:

- The server machine must satisfy the minimal hardware and network connectivity requirements published by NICE.

- The SQL Server configuration must fully comply with the NICE Perform SQL Server configuration requirements.

- The customer must present valid SQL Server licenses for the servers to be used by NICE applications. See SQL Server License Requirements below.

The NICE Perform Database Suite installation ensures that the SQL Server configuration meets NICE requirements. The Database Suite installation may automatically stop if the SQL Server configuration deviates from the NICE guidelines, to prevent any future performance difficulties or system malfunctioning that may arise. If the server is improperly configured, the installation clearly presents the configuration problem encountered, so the customer can make the necessary corrections.

The customer takes full responsibility for the support of the SQL Server, and communicates directly with Microsoft. However, the customer needs to follow NICE maintenance and backup guidelines and consult NICE on any configuration change. NICE remains fully responsible for the NICE Perform database itself.

Upgrading from SQL Server 2000 to SQL Server 2005

The NICE Perform Release 3 upgrades do not include SQL Server 2005 software and licenses.

In case an upgrade from SQL Server 2000 to SQL Server 2005 is required, customer needs to purchase new SQL Server 2005 licenses from NICE or provide the necessary software and licenses independently. SQL Server 2000 licenses cannot be reused.

There are no discounts on SQL Server licenses sold by NICE for SQL Server upgrade. Same prices apply to both new SQL Server licenses and upgrades from SQL Server 2000 to SQL Server 2005.

SQL Server License Requirements

For all NICE Perform application packages, other than the Interaction Package, an SQL Server CPU-based licensing scheme should be employed. Here are a few examples on how to use SQL Server Per-Processor licenses for different deployments.

Single Site Deployment

In most deployments, the NICE Perform database and the Data Mart database are installed on and managed by the same SQL Server.

Customer needs to purchase as many SQL Server Per-Processor licenses as the number of CPUs on the server machine that runs the SQL Server. For example, a dual-processor machine requires two Per-Processor licenses. SQL Server 2005 Standard Edition supports up to four CPUs.

In some deployments, for scalability reasons, the Data Mart will be installed on and managed by a separate SQL Server. In this type of deployment, additional SQL Server Per-Processor licenses must be purchased.

Multi-Data Hub Deployment

A data hub is a combination of a NICE Perform Application Server and Database at a certain site.

A multi-data hub deployment includes several such data hubs located in different sites, of which one is considered the **Primary Data Hub** and the others are considered to be **secondary Data Hubs**. Usually, the Primary Data Hub site also features the Data Mart database, installed on and managed by a separate SQL Server.

An adequate number of Per-Processor licenses should be purchased according to the number of CPUs on each server machine that runs SQL Server, both for Database Server(s) and Data Mart.

> **NOTE:** In a multi-data hub deployment, all SQL Server instances must have the same SQL Server version.

Network Management Station (NMS)

NICE NMS uses a Microsoft SQL Server database to store and efficiently manage the information contained in the NICE Management Information Base (MIB) file.

The NMS uses its own SQL Server 2000 Standard Edition installation, separated from the NICE Perform database and Data Mart database.

> **NOTE:** The NICE Perform Application Suites, including NICE Perform SMB Applications, do not include the NMS software. The NMS should be ordered separately (NMS-NP-SRV price list item).

The NMS requires a single SQL Server 2000 Standard Edition CAL, which is included in the NMS license (NMS-NP-SRV price list item). There is no need to separately order an SQL Server license.

If Unicenter Remote Admin Client is used on remote workstations, an additional CAL is required for each Remote Admin Client. The additional CAL is included in the Remote Admin Client license (NMS-NP-CLNT price list item). There is no need to separately order an SQL Server license.

NICE Perform SMB

NICE Perform SMB also employs Microsoft SQL Server 2005 Standard Edition. The NICE Perform SMB Applications packages include 10 Client Access Licenses (CALs). Additional CALs can be purchased using the SQL-CAL-LIC price list item.

Special Notes for New and Old Price Lists

The new price list for release 3, with SQL-CAL-LIC and SQL-CPU-LIC price list items, is effective as of **June 1st, 2007.**

After June 1st 2007, orders for Release 3 that do not include the new price list items, will be treated based on the new GA price list, and NICE will assume that the customer will supply the SQL Server software and licenses on its own. **Orders for new Release 3 installations that include DUAL-CPU-SQL will be rejected.**

Orders for upgrades from NICE Perform Release 3 pre-GA version that wish to continue using SQL Server 2000, require NICE Product Management and Project Management approval (commitment).

After June 1st 2007, orders for Release 3 will no longer include the NMS software and licenses by default. The NMS software and licenses must be explicitly ordered using the adequate price list item.

SQL Server 2008

Enabling Microsoft Distribute Transaction Coordinator (MSDTC) to Function in Multi Site Environments

Product	NICE Perform, NICE Interaction Management
Release	NICE Perform Release 3.x NICE Interaction Management Release 4.1
Synopsis	This section describes procedures that enable MSDTC to function properly in multi site environments.

The SQL Server uses Microsoft Distribute Transaction Coordinator (MSDTC) to execute distributed transactions.

A distributed transaction is a transaction between two SQL Servers. NICE Perform/NICE Interaction Management creates a distributed transaction in multi site environments, for instance when the Rule Engine writes storage tasks from the secondary site to the master site.

MSDTC will not function properly in an environment where the two servers are using the same Windows OS image, for example where the 'Ghost' program is used to copy the Windows image to the disk. The reason for the problem is that both servers that are installed from the same image, have an identical key in the MSTDC section in the SQL Server registry.

If the distributed transaction fails and the registry keys are different, there may be other reasons for the failure. See **Final Verification** on page 191.

This document describes how to fix the problem without re-installing the entire system.

> **Important!**
>
> Make sure that your system is fully backed up before proceeding.

The process includes the following steps:

1. Removing the Network DTC Access.

2. Uninstalling the DTC.

3. Removing the MSDTC key from the registry.

4. Installing the MSDTC.

5. Re-installing the network DTC access.

6. Restoring the original security settings.

Removing the Network Distribute Transaction Coordinator (DTC) Access

The following procedure enables you to remove the DTC access.

◆ **To remove the network DTC access:**

1. Select **Start**, and select **Settings > Control Panel > Add or Remove Programs**. The Add or Remove window appears.

Figure 8-1: Add or Remove Programs Window
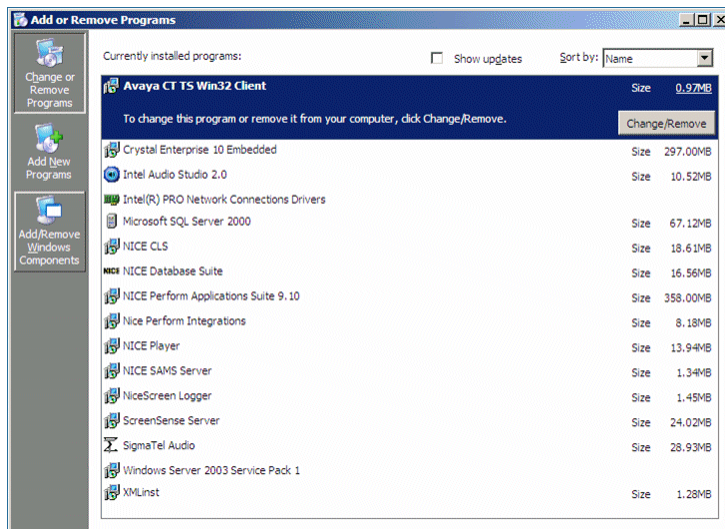
2. Click **Add/Remove Windows Components**.

The Windows Components Wizard starts.

Figure 8-2: Windows Component Wizard
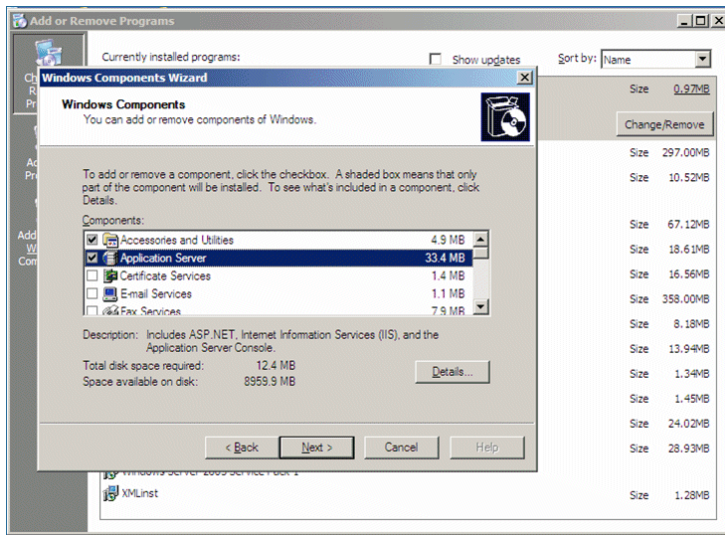
3. In the **Components** list, select **Applications Server**, and click **Details**. The Application Server window appears.

Figure 8-3: Application Server Window
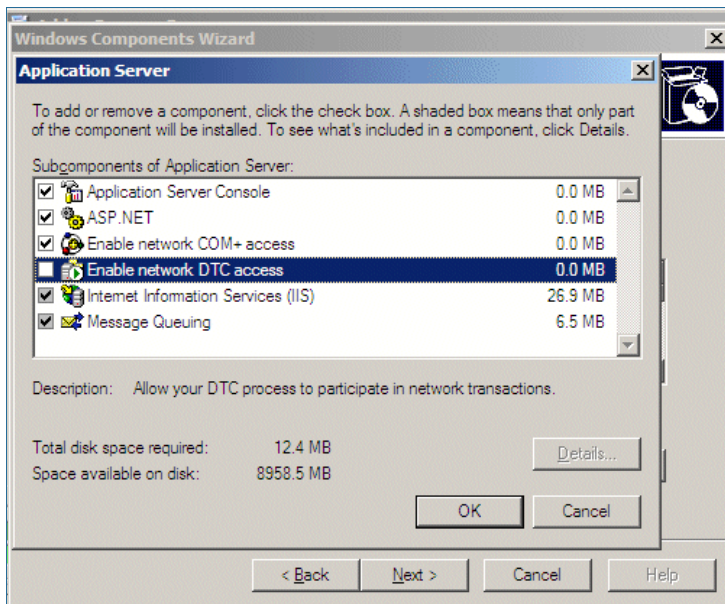
4. **Clear** the **Enable network DTC access** checkbox.

5. Click **OK**. The Windows Components Wizard window reappears.

6. Click **Next**. The Configuring Components window appears.

Figure 8-4: Configuring Components Window
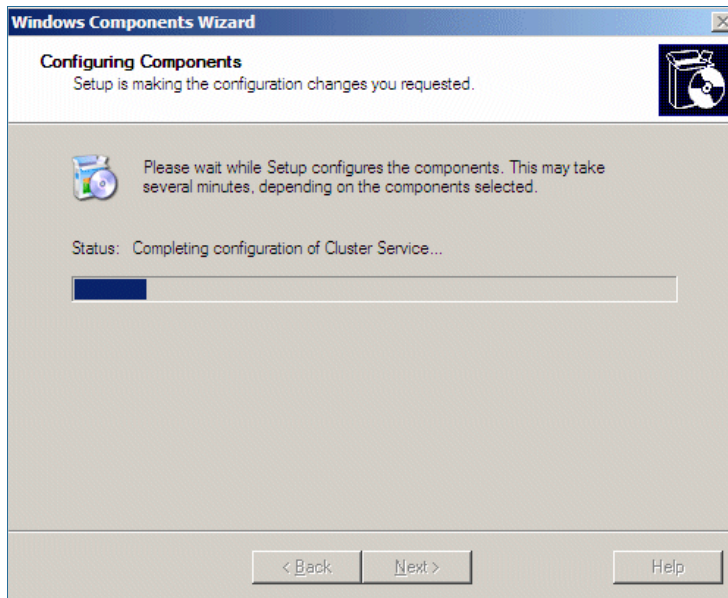
7. When the configuration of the Cluster Service is completed, click **Next**. The Completing the Windows Components Wizard window appears.

Figure 8-5: Completing the Windows Components Window

8. Click **Finish** to close the wizard.

Uninstalling the DTC

◆ To uninstall the DTC:

1. Click **Start**, and select **Run**. Type cmd, and click **OK**. The following window appears.

Figure 8-6: C:\WINDOWS\System32\cmd.exe
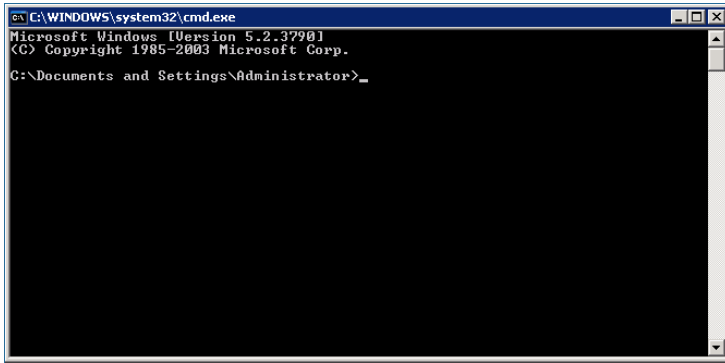
2. To stop the MSDTC, enter the following command: **net stop msdtc**.

Figure 8-7: C:\WINDOWS\System32\cmd.exe
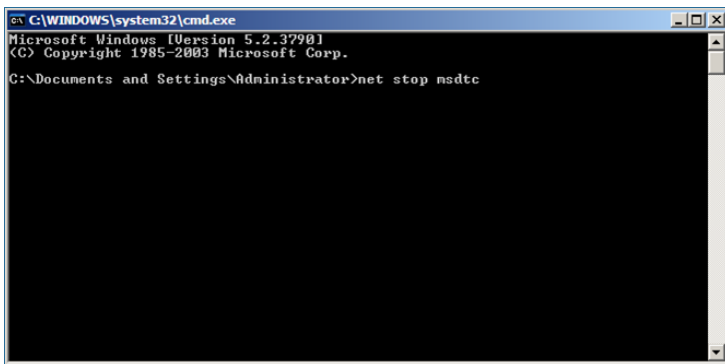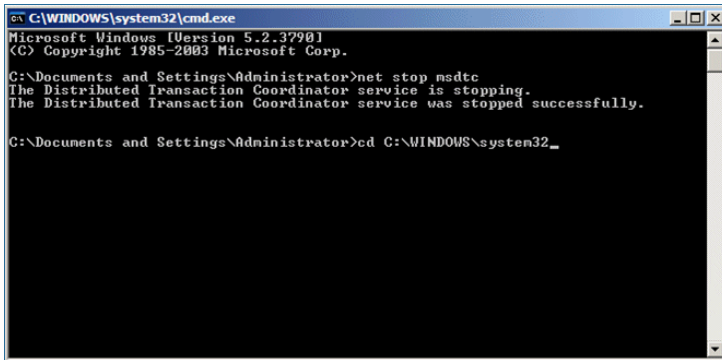
The following window appears.

Figure 8-8: C:\WINDOWS\System32\cmd.exe
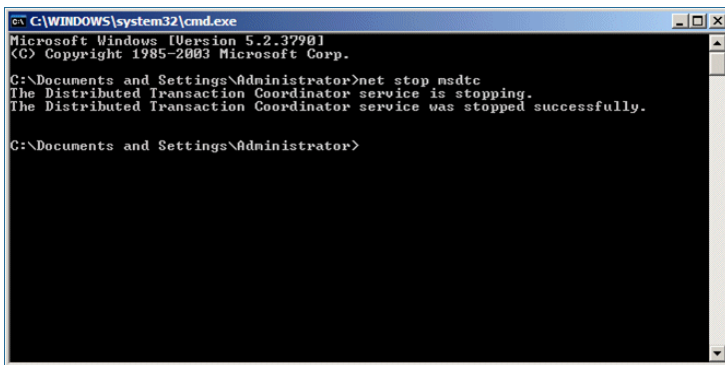
3. Change the directory to **c:\WINDOWS\system32**

Figure 8-9: C:\WINDOWS\System32\cmd.exe

The following window appears.

Figure 8-10: C:\WINDOWS\System32\cmd.exe
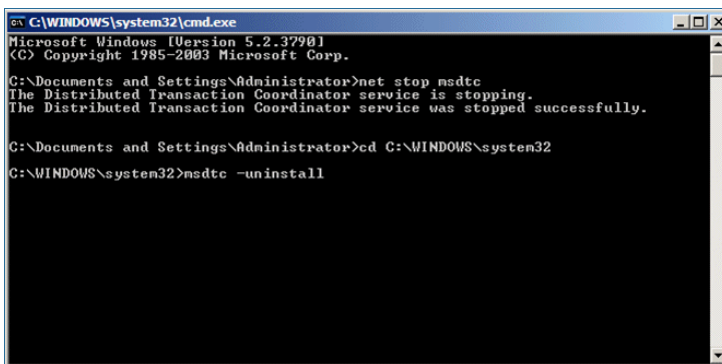
4. Write command **msdtc -uninstall** to uninstall MSDTC, as shown in the following window.

Figure 8-11: C:\WINDOWS\System32\cmd.exe
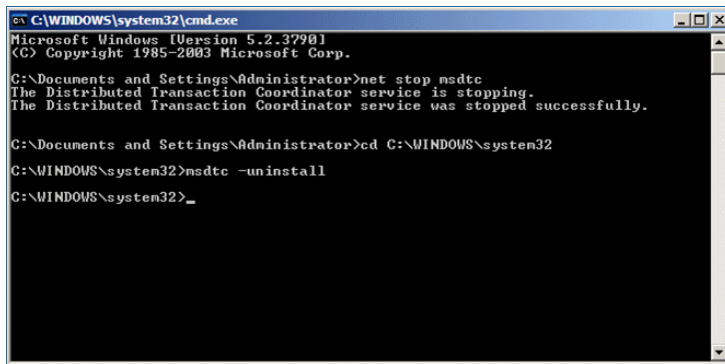
When the uninstall is completed, the following window appears.

Figure 8-12: C:\WINDOWS\System32\cmd.exe

Removing the MSDTC Key from the Registry

❖ **To remove the MSDTC key from the registry:**

1. Navigate to **Start**, and select **Run**.

Figure 8-13: Run Window
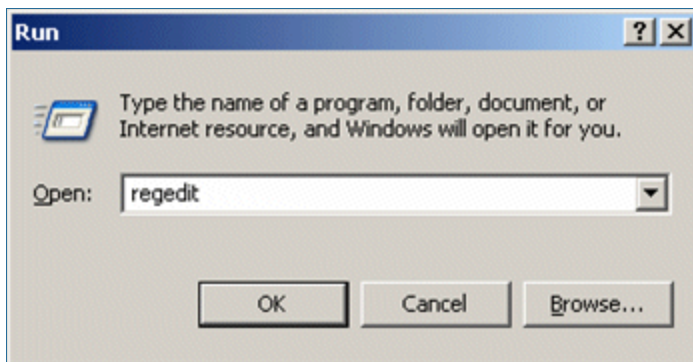
2. In the **Open** field, type **regedit** and click **OK**. The Registry Editor window appears.

Figure 8-14: The Registry Editor
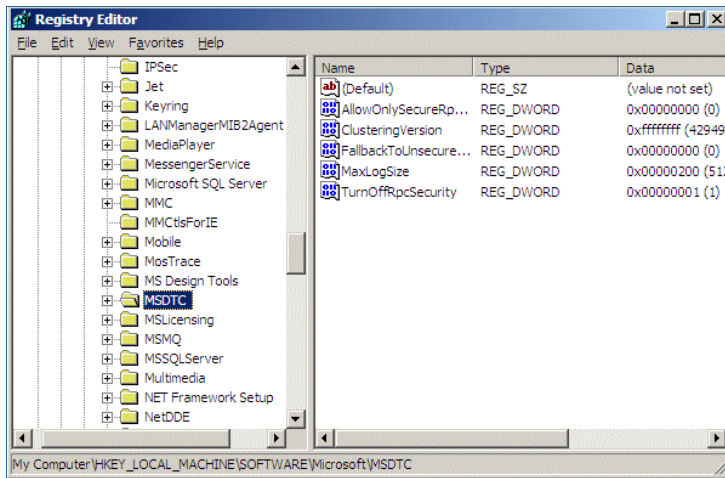
3. Right-click **MSDTC**, and select **Delete**. The following dialog box appears.

Figure 8-15: Confirm Key Delete Message
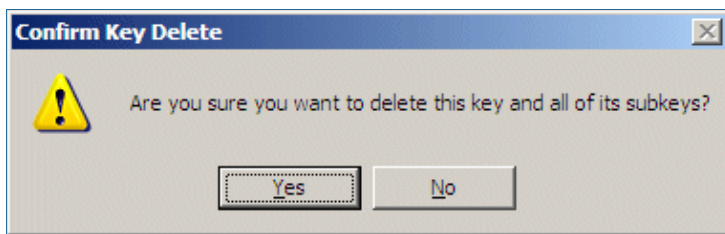
4. Click **Yes**. **MSDTC** is deleted from the Registry Editor.

Figure 8-16: Registry Editor
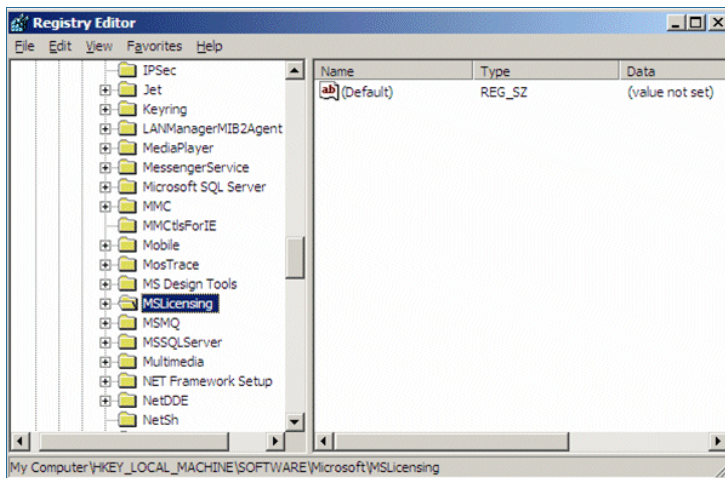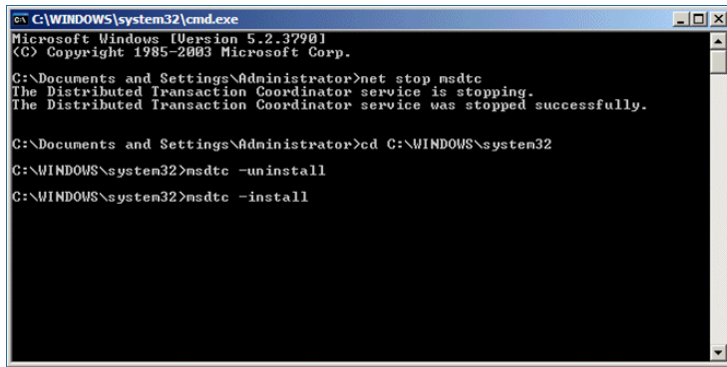
5. Close the Registry Editor.

Re-Installing the MSDTC

◆ To re-install the MSDTC:

1. In the command prompt window, type the command **msdtc -install.**

   Figure 8-17: C:\WINDOWS\System32\cmd.exe

2. When the installation is completed, the following window appears.

   Figure 8-18: C:\WINDOWS\System32\cmd.exe

Re-Installing Network DTC Access

This procedure is very similar to the To remove network DTC access procedure. See **Removing the Network Distribute Transaction Coordinator (DTC) Access** on page 179

◆ To re-install network DTC access:

1. Select **Start**, and select **Settings > Control Panel > Add or Remove Programs**. The Add or Remove window appears.

2. Click **Add/Remove Windows Components**. The Windows Components Wizard starts.

3. In the **Components** list, select **Applications Server**, and click **Details**. The Applications Server window appears.

Figure 8-19: Applications Server Window
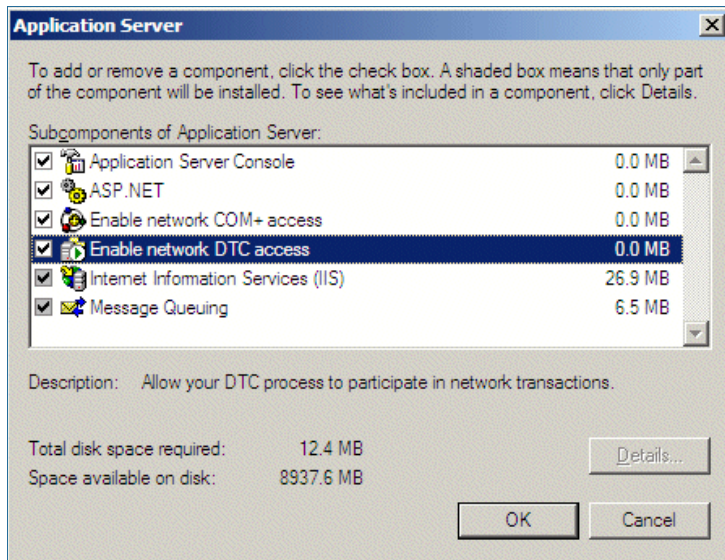
4. Select the **Enable network DTC access** checkbox, and click **OK**. The Windows Components Wizard window reappears.

5. Click **Next**. The Configuring Components window appears.

6. When the configuration of the Cluster Service is completed, click **Next**. The Completing the Windows Components Wizard window appears.

**Figure 8-20: Completing the Windows Components Window**

7. Click **Finish** to close the wizard.

Restoring the Original Security Settings

Since MSTDC has been re-installed, the security definitions required by the NICE system must be reset.

◆ **To restore the original security settings:**

1. Select **Start**, and select **Settings > Control Panel > Administrative Tools > Component Services**. The Component Services window appears.

   Figure 8-21: Component Services Window
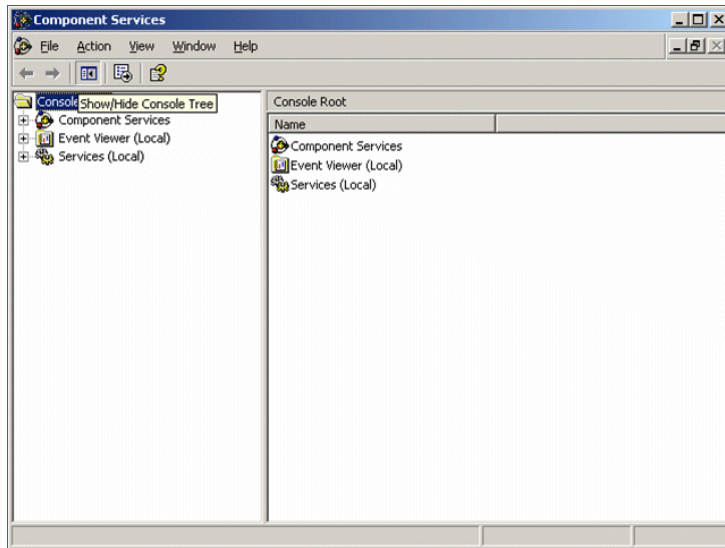
2. Expand **Computer Services**, and **Computers**. The following window appears:

   Figure 8-22: Component Services Window
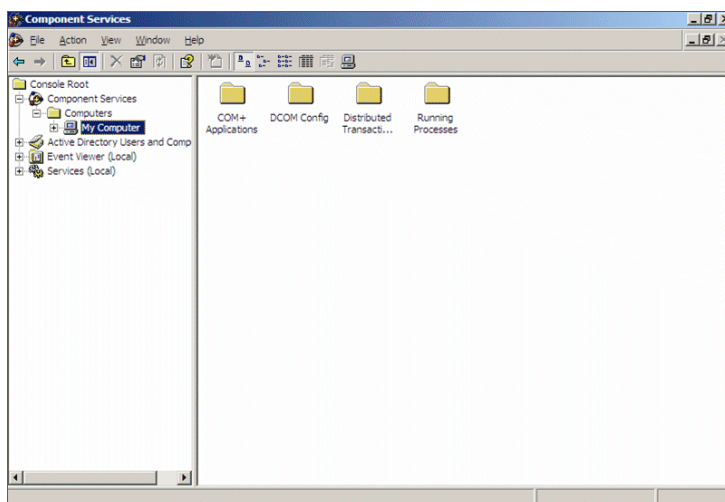
3. Right-click **My Computer**, and select **Properties**. The My Computer Properties window appears.

Figure 8-23: My Computer Properties Window
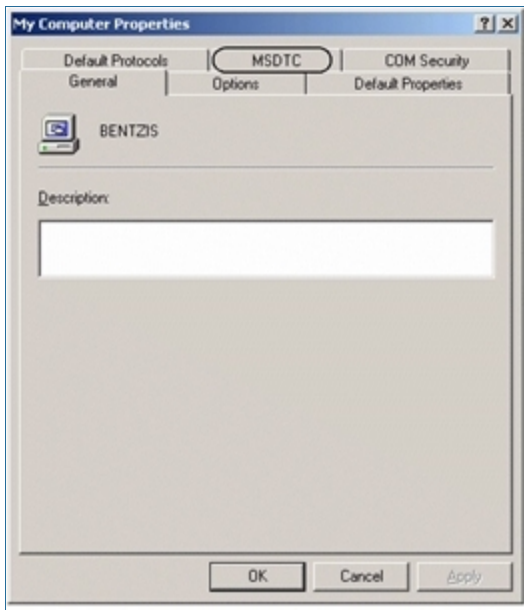
4. Click the **MSDTC** tab. The following window appears.

Figure 8-24: My Computer Properties - MSDTC Tab
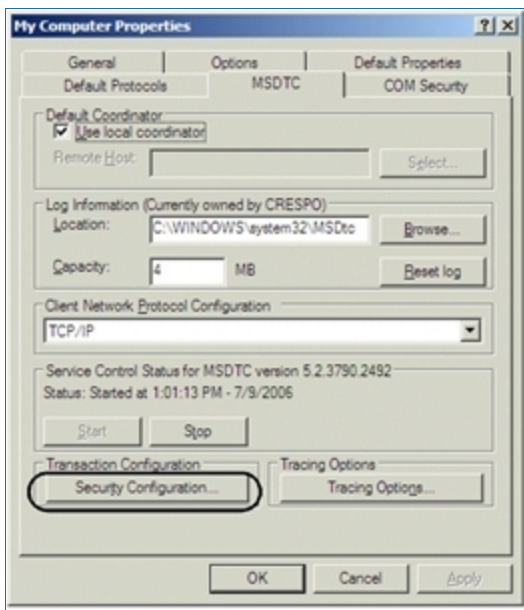
5. Click the **Security Configuration** button. The Security Configuration window appears.

Figure 8-25: Security Configuration Window
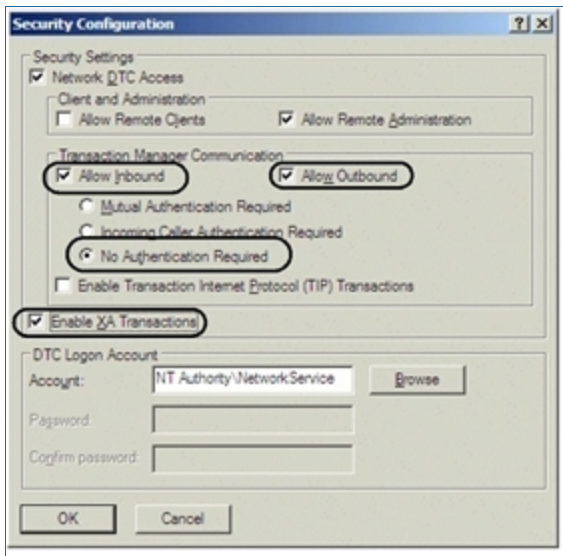
6.   Make sure that the settings are identical to those in the above window, in particular:

■   The **Allow Inbound, Allow Outbound** and **Enable XA Transactions** checkboxes must be marked.

■   The **No Authentication Required** radio button must be selected.

7.   Click **OK**. The My Computer Properties window re-appears.

8.   Click **OK**. The DTC Console Message dialog box appears.

Figure 8-26: Console Message
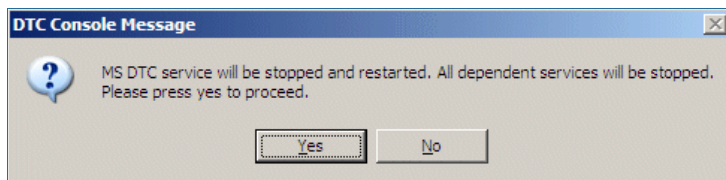
9.   Click **Yes**. The following message is issued:

Figure 8-27: DTC Console Message
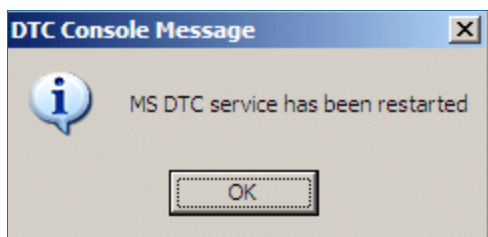
NOTE: If the SQL Server is already installed, you need to also restart the SQL Server service.

Final Verification

In the secondary site, execute the following query from the Query Analyzer:

BEGIN TRANSACTION

SELECT * FROM nice_rule_link.nice_admin.dbo.tblSCTasks

COMMIT

If there is an error in the output, there might be causes other than those that were discussed previously in this document, which resulted in the MSDTC failure.

To check for other causes for MSDTC failure:

1. Access the **Tools** folder of the NICE Application installation, and select the **DTCPing** utility.

2. In the **Remote Server Name** field, type the name or IP of the Master Database Server, as shown in the following illustration:

   Figure 8-28: MSDTC Simulation V1.9
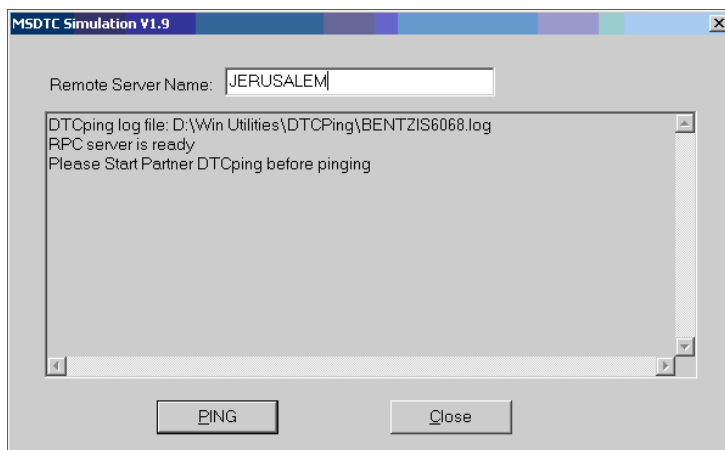
3. Click **PING**. The utility generates a log file with detailed information.

[This page intentionally left blank]

9

Microsoft Security Bulletins

This chapter describes Microsoft security bulletins.

Contents

Patch Management Tools

DBM Error on Loggers due to MS Security Patch KB921883

Product	DBM Error on Loggers
Release	
Synopsis	This section describes an issue as a result of installing a security patch.

General Description

■ This issue can occur either during a new Logger installation, or after installing the Microsoft Security Patch on an existing Logger.

This can affect all Loggers running on Microsoft Windows Server 2003 (HD, NCFIII, VoIP).

■ The Microsoft patch is KB 921883 (MS 06-040).

Problem Symptom

1. During Logger startup, the following messages can be seen in the LogSrv window, as well as in the Logger log file (LogFile.dat):

   BUG: DBM: DBM.DLL: Exception EAccessViolation in module DBM.DLL at 00026ECD. Access violation at address 01266ECD in module 'DBM.DLL'. Write of address 00 0 0 8/26/2006 6:48:07 AM

   BUG: DBM: DBM.DLL: MapFile Address: 00025ECD 0 0 8/26/2006 6:48:07 AM

2. Immediately after this, the window hangs as shown below, and the Logger will not initialize.

   Figure 9-1: NICE Digital Logger

   Additional information of the issue from MS point of view can be found on MS site: http://support.microsoft.com/kb/924054

Resolution

Install **MS Hot-fix KB924054**.

[This page intentionally left blank]

10

Daylight Savings Time

This chapter provides the Microsoft Daylight Savings Time (DST) updates supported by NICE Systems.

For Microsoft Daylight Savings Time configurations, see the *Maintenance Guide*.

Contents

Microsoft Daylight Savings Time Updates

The following table lists the Microsoft Daylight Savings Time Updates supported by NICE Systems:

Microsoft DST Updates	Supported in:	Comments
KB 928388	NICE Perform Release 3.1	Approved
KB 929120	NICE Perform Release 3.2	
KB 933360	NICE Perform Release 3.5	
KB 942763	NICE Interaction Management Release 4.1	
KB 951072		
KB 955839		
KB 970653		
KB 976098		
KB 981793		
KB 2158563		
KB 2443685		
KB 2570791		
KB 2633952		
KB 2756822		
KB 2779562		
KB 2863058		

11

Antivirus

This chapter includes installation instructions and limitations for Antivirus products on client computers and loggers.

> **NOTE:** The information in this chapter refers to software versions only. In addition, customers, business partners, and services must verify that the servers and Loggers meet the minimum hardware requirements as defined by the third party software vendor.

Contents

General Antivirus

- **Antivirus Certifications for NICE Products** below

Antivirus Certifications for NICE Products

Product	Antivirus Certifications for NICE Products
Release	
Synopsis	This section includes general instructions and limitations for Antivirus Certifications for NICE Products, NICE Products and Antivirus Certifications matrices, as well as procedures for installing antivirus products on client computers and Loggers.

General Instructions

A list of general instructions follows:

- During the installation of the antivirus software, all applications and screens must be closed.

- The same applies when upgrading the antivirus software.

- Scan and Live Updates should be scheduled to run in system idle time.

- Do not run Scan or Live Update during NICE software installation.

- Always set Scan Priority to Low.

General Limitations

- To avoid playback, performance, and retention issues, the destination paths of all Storage Units must be excluded from antivirus scans. See the *System Administrator - Configuration Guide* for more information regarding setting up Storage Units.

- When installing an antivirus on a cluster, take the following guidelines into account:

- The antivirus software should be cluster-aware. An application is cluster-aware if it has the following characteristics:

  - It uses TCP/IP as a network protocol.

  - It maintains data in a configurable location.

  - It supports transaction processing.

- On the clustered servers, Microsoft recommends excluding the following folders from antivirus scanning:

  - The path of the \mscs folder on the quorum hard disk. For example, exclude the **Q:\mscs** folder from virus scanning.

  - The **%Systemroot%\Cluster** folder.

  - The temp folder for the Cluster Service account. For example, exclude the **\clusterserviceaccount\Local Settings\Temp** folder from virus scanning.

McAfee ePO

- McAfee ePO 3.5 works with McAfee Antivirus 8.5/8.5i.

- McAfee ePO 4.0 works with McAfee Antivirus 8.5/8.5i and 8.7/8.7i.

- McAfee ePO 4.5 works with McAfee Antivirus 8.5i and 8.7.

- McAfee ePO 4.6 works with McAfee Antivirus 8.5i, 8.7i and 8.8

- Make sure that when using ePO for Microsoft patches update, the configured policy matches the NICE policy concerning Microsoft Windows updates and Service packs.

McAfee

- Make sure to **clear** the option to install the McAfee firewall. Do not install the firewall, as it would cause network problems.

- It is recommended to set the CPU Utilization for the On Demand Scan in McAfee AV to 10%.

- The McAfee's VirusScan version 8.0 feature Buffer Overflow Protection does not allow applications to overflow the buffer, including the CLS Log Manager. This causes the Log Manager to write logs (Channel server, Call server etc.) with a very long delay, or not write them at all. Therefore this feature should be disabled for all machines running CLS. See also to TN0640 McAfee ePO 3.5 and McAfee Antivirus Certification for NICE 8.80.

McAfee Limitation:

■ Memory Scan process in McAfee 8.5/8.7 on some TDM Loggers can cause the system to crash with BSOD. This problem was resolved in McAfee 8.7 Patch 3, and in later versions, but still exists in McAfee 8.5.

Do not use versions earlier than McAfee 8.7 Patch 3 on servers with TDM Loggers.

SEP

■ NICE Products support Symantec Endpoint Protection.

■ In some cases SEP 12.1 can detect NICE or even Microsoft binaries as malware and place them in the Quarantine folder. To prevent false-positive detection, follow the recommendations available in the Symantec white paper *Sizing and Scalability Recommendations for Symantec Endpoint Protection* (http://clientui-kb.symantec.com/resources/sites/BUSINESS/content/staging/DOCUMENTATION/4000/DOC4448/en_US/1.0/Endpoint%20Protection%20Sizing%20and%20Scalability%20Best%20Practices_%20v2.3.pdf).

Exceptions can be added from within the Symantec Endpoint Protection Manager console to provide false-positive mitigation on the client. For example, you can do the following:

■ Exclude your domain from Insight detection.

Figure 11-1: Exceptions Window
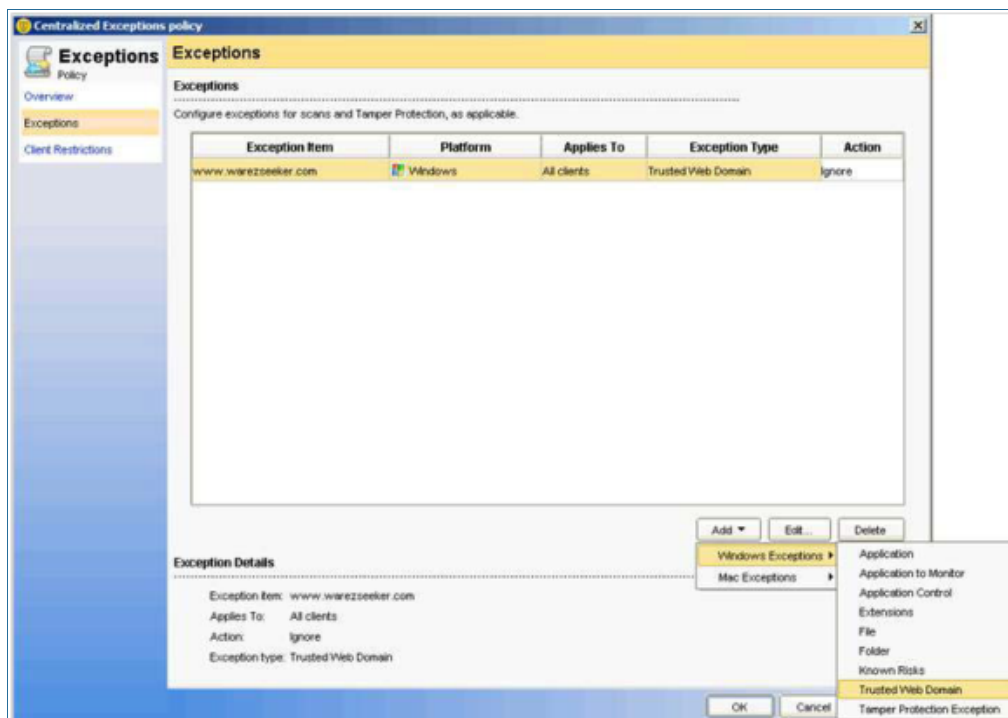
> 📋 **NOTE:** You can select **Trusted Web Domain**, to add a Web domain to the exceptions policy.

▢ Add exclusions or exceptions for critical files, folders, URLs, and IP addresses.

> 📋 **NOTE:** When you add exceptions, you can select more than one application, file, URL, or IP address at a time.

A known-good application can appear in the Risk Logs as a false-positive. You can configure log settings to allow the application and thereby prevent it from appearing in the Risk Log. This same functionality is also available in the SONAR Logs.

Figure 11-2: Risk Logs Window

For more information, see the *Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide*.

SEP Limitations

Starting with SEP (Symantec Endpoint Protection) version 12.1.2 and 12.1.4, the SEP firewall causes issues with Microsoft Cluster setup and functionality. To avoid this issue change the SEP settings to allow IP traffic.

To change the SEP settings:

1. Open Symantec Endpoint Protection (SEP).
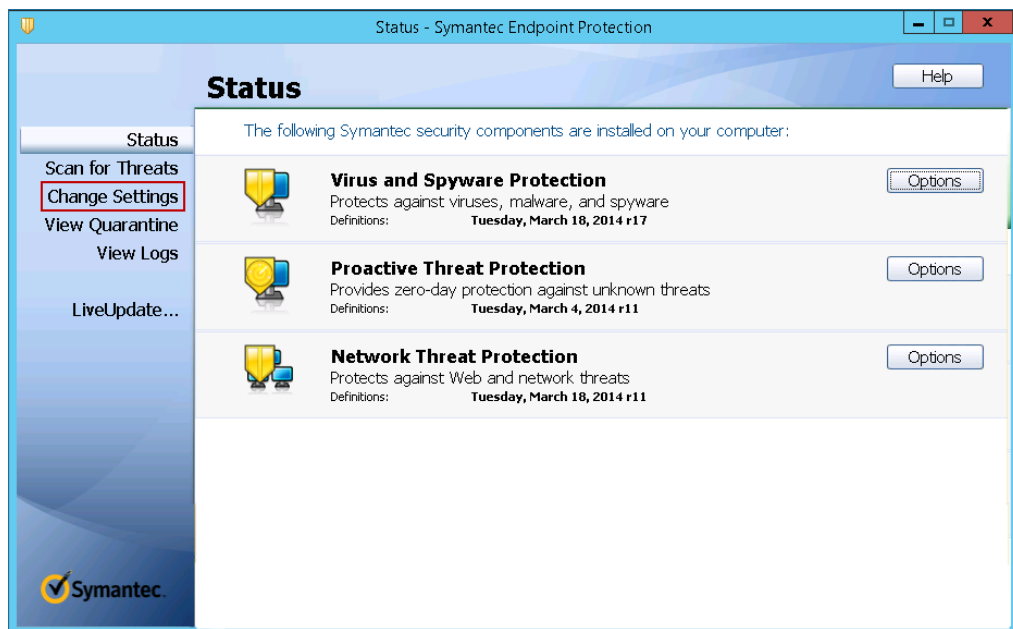
2. In the left column, click **Change Settings**. The Change Settings area appears on the right.
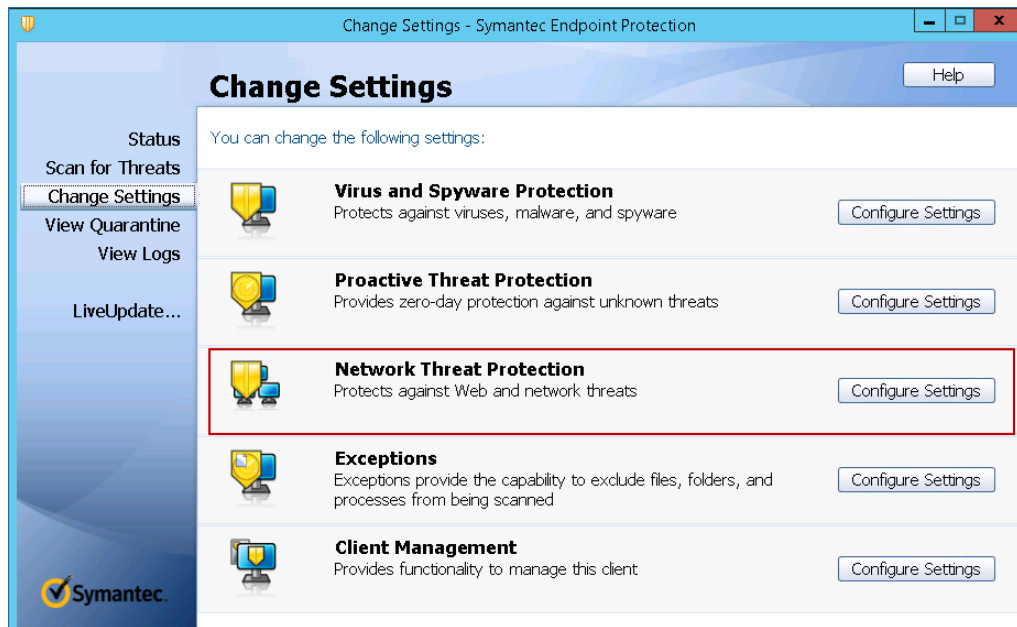
3. In the **Network Threat Protection** area, click **Configure Settings**. The Network Threat Protection Settings window appears.
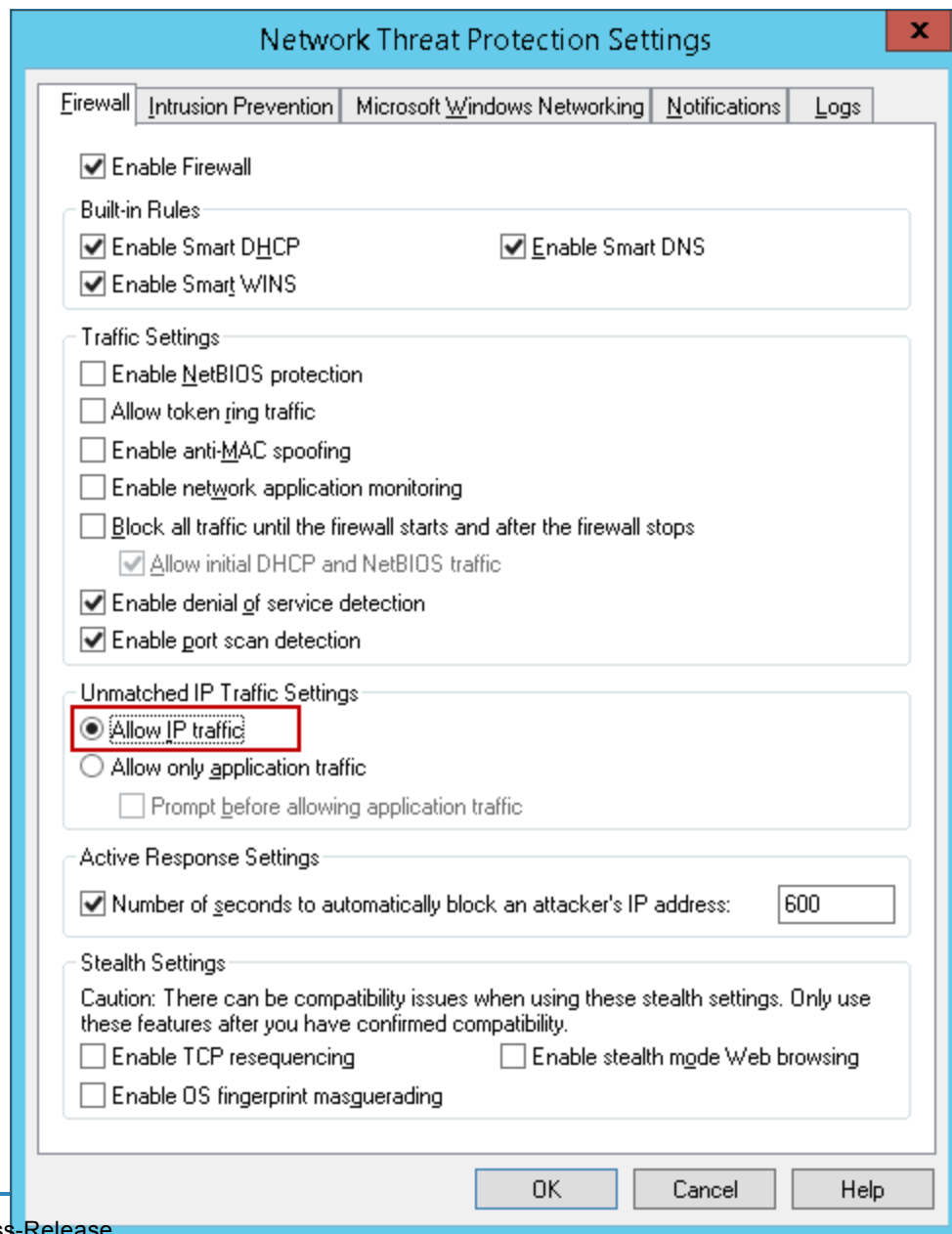
4. In the **Firewall** tab, in the **Unmatched IP Traffic Settings** area, select **Allow IP traffic**. By default, **Allow only application traffic** is selected.

5. Click **OK**.

6. Restart your computer.

Trend Micro

■ Trend Micro AV requires that the NICE servers belong to the same domain.

Sophos

■ Sophos 9.5 exception with Web: Web Intelligence feature in Sophos 9.5 should be disabled in case Nice Perform configured with Active Directory authentication, since it can cause crash of IE during login to Nice Perform with domain users. Web Intelligence feature can be enabled in case Nice Perform configured with Nice Authentication.

■ Sophos Exclusions: In a NICE Interaction Management 4.1 site with Sophos antivirus deployed, before beginning to use NDM to install or update the site, add psexec.exe to Exclusions list. Otherwise, it can cause a problem with running NDM Agents (http://www.sophos.com/en-us//threat-center/threat-analyses/adware-and-puas/PsExec.aspx).

NICE Products and Antivirus Certification Matrices

Table 11-1:
NICE Products and Antivirus Certifications Matrix - Version 8.90

NICE Products		SAV_ 10.1.5.5000	SEP 11.0 Client	SEP 11.0 Server	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/8.5i	McAfee 8.7/8.7i	Trend Micro OfficeScan 10	Trend Micro OfficeScan 10.5	Sophos 7.6	Sophos 9.0	Sophos 9.5
TDM Logger	9.01	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
	9.06	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	9.07	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VoIP Logger	9.10	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CLS	8.93	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NiceCall Focus III	8.90	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
NiceScreen Logger	8.9	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

NICE Products		SAV_ 10.1.5.5000	SEP 11.0 Client	SEP 11.0 Server	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/8.5i	McAfee 8.7/8.7i	Trend Micro OfficeScan 10	Trend Micro OfficeScan 10.5	Sophos 7.6	Sophos 9.0	Sophos 9.5
Storage Center	8.9	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Web Apps	8.9	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Manager	8.9	Yes	No	No	No	No	No	No	No	Yes	No	No	Yes	Yes	Yes

Note: Third-Party Software is approved per NICE product for all operating systems certified by NICE.

Table 11-2:
NICE Products and Antivirus Certifications Matrix - NICE Perform Release 1, Release 2, and Version 9.09

NICE Products		*SAV 10.1	SEP 11.0 Client	SEP 11.0 Server	*McAfee 8.0i	*McAfee ePO 3.5	McAfee ePO 4.5	McAfee 8.5	*TM Server Protect 5.5.8	Trend Micro OfficeScan 7.3	Trend Micro OfficeScan 8.0
TDM Logger	9.01	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	9.06	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VoIP Logger	9.12	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interaction Server		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NiceScreen Logger		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Playback Server (incl. NICE Feedback)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

NICE Products		*SAV 10.1	SEP 11.0 Client	SEP 11.0 Server	*McAfee 8.0i	*McAfee ePO 3.5	McAfee ePO 4.5	McAfee 8.5	*TM Server Protect 5.5.8	Trend Micro OfficeScan 7.3	Trend Micro OfficeScan 8.0
SNMP Manager (NMS)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Storage Center		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Media Library		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Application Server		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Audio Analysis		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
ScreenSense Server		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Reporter		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Database Server		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
* This antivirus was certified for NICE Perform Release 1 and NICE Perform Release 2											

NOTE: Third-Party Software is approved per NICE product for all operating systems certified by NICE.

Table 11-3:
NICE Products and Antivirus Certifications Matrix - NICE Perform Release 3, SP3 and Higher

NICE Products		*SAV 10.1.5.5000	SEP 11.0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/8.5i	McAfee 8.7/8.7i	McAfee 8.8/8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
TDM Logger	9.01	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes
	9.06	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
	9.07	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
	9.4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

1

NICE Products		*SAV 10.1.5.5000	SEP 11.0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/8.5i	McAfee 8.7/8.7i	McAfee 8.8/8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
VoIP Logger	9.10	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	9.12	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	10.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5 .5000	SEP 11 .0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/ 8.5i	McAfee 8.7/ 8.7i	McAfee 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
Interaction Server	Rel 3 SP 3 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5 .5000	SEP 11 .0 .0 Client	SEP 11 Server	SEP 12 1	McAfe e ePO 3.5	McAfe e ePO 4.0	McAfe e ePO 4.5	McAfe e ePO 4.6	McAfe e 8.5/ 8.5i	McAfe e 8.7/ 8.7i	McAfe e 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sopho s 7.6	Sopho s 9.0	Sopho s 9.5	Sopho s 9.7	Sopho s 10	Sophos 10. 2
NiceScr een Logger	Rel 3 SP 3 an d ab ov e	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5 .5000	SEP 11 .0. 0 Cli en t	SEP 11 Se rve r	SE P 1 2 1	Mc Afe e eP O 3.5	Mc Afe e eP O 4.0	Mc Afe e eP O 4.5	Mc Afe e eP O 4.6	Mc Afe e 8.5/ 8.5i	Mc Afe e 8.7/ 8.7i	Mc Afe e 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	So pho s 7.6	So pho s 9.0	So pho s 9.5	So pho s 9.7	So pho s 10	Sop hos 10. 2
Playbac k Server / Teleph ony Service s Server (incl. NICE Feedba ck)	Re l 3 SP 3 an d ab ov e	Yes	Y es	Ye s	Y e s	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5.5000	SEP 11.0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/8.5i	McAfee 8.7/8.7i	McAfee 8.8/8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
NMS	Rel 3 SP3 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5.5000	SEP 11.0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/8.5i	McAfee 8.7/8.7i	McAfee 8.8/8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
Storage Center	Rel 3 SP3 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5 .5000	SEP 11 .0 .0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/ 8.5i	McAfee 8.7/ 8.7i	McAfee 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
Media Library	Rel 3 SP3 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5 .5000	SEP 11.0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/ 8.5i	McAfee 8.7/ 8.7i	McAfee 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
Application Server	Rel 3 SP3 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

___

1

NICE Products		*SAV 10.1.5 .5000	SEP 11.0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/ 8.5i	McAfee 8.7/ 8.7i	McAfee 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
Audio Analysis Server	Rel3 SP3 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5 .5000	SEP 11 .0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/ 8.5i	McAfee 8.7/ 8.7i	McAfee 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
Screen Sense Server	Rel 3 SP3 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5 .5000	SEP 11 .0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/ 8.5i	McAfee 8.7/ 8.7i	McAfee 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
Reporter	Rel 3 SP3 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5 .5000	SEP 11.0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/ 8.5i	McAfee 8.7/ 8.7i	McAfee 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
Database Server	Rel 3 SP3 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1

NICE Products		*SAV 10.1.5.5000	SEP 11.0.0 Client	SEP 11 Server	SEP 121	McAfee ePO 3.5	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.5/ 8.5i	McAfee 8.7/ 8.7i	McAfee 8.8/ 8.8i	Trend Micro Office Scan 8.0	Trend Micro Office Scan 10	Trend Micro Office Scan 10.5	Trend Micro Office Scan 10.6	Sophos 7.6	Sophos 9.0	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2
Sentinel	Rel 3.1 and above	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
* In some cases SEP 12 can detect NICE's binaries as a potential security risk. For further details, see **SEP** on page 1.																						

NOTE: Third-Party Software is approved per NICE product for all operating systems certified by NICE.

1

Table 11-4:
NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1

NICE Products	SEP 11.00	SEP 12.1-12.1.4	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.7	McAfee 8.8	Trend Micro OfficeScan 10	Trend Micro OfficeScan 10.5	Trend Micro OfficeScan 10.6	Trend Micro OfficeScan 11	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2	Sophos 10.3
TDM Logger	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VoIP Logger	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Interaction Server	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NiceScreen Logger	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Playback Server / Telephony Services Server (incl. NICE Feedback)	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NMS	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

NICE Products	SEP 11.00	SEP 12.1-12.1.4	McAfee ePO 4.0	McAfee ePO 4.5	McAfee ePO 4.6	McAfee 8.7	McAfee 8.8	Trend Micro OfficeScan 10	Trend Micro OfficeScan 10.5	Trend Micro OfficeScan 10.6	Trend Micro OfficeScan 11	Sophos 9.5	Sophos 9.7	Sophos 10	Sophos 10.2	Sophos 10.3
Storage Center	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Media Library	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Application Server	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Audio Analysis Server	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ScreenSense Server	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Reporter	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Database Server	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Sentinel	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
* In some cases SEP 12 can detect NICE's binaries as a potential security risk. For further details, see **SEP** on page 1.																

McAfee

McAfee ePO 3.5 and McAfee Antivirus 8.0 Certification for NICE 8.80

Product	Antivirus Certification
Release	
Synopsis	This section displays the procedures for McAfee ePO 3.5 and McAfee Antivirus 8.0 Certification for NICE 8.80.

> **NOTE:**
>
> *Nice Perform certification includes the following components:
>
> Interaction Server, PBS, SNMP Manager, Storage Center, Application Server, Audio Analysis

Purpose and Scope

This section summarizes the certification that was performed for NICE 8.80 recording system when using McAfee 8.0 and EPO server 3.5 clients.

NICE Servers

Table 11-5:
NICE Servers

Server	NICE Version	CPU	RAM	OS + SP
NiceLog	8.80 SP8	233MHz	256MB	Windows 2000 Professional + SP4
CLS	8.80 (Core SP3, Integrations SP3)	2.4 GHz	512MB	Windows 2000 Server + SP4
Storage Center	8.80 SP5	800MHz	256MB	Windows 2000 Professional + SP4
Web Server	8.80 SP6	2.4 GHz	1GB	Windows 2000 Server + SP4

Test Description

Running the EPO Tasks

1. When the Logger is in resting state - no calls recorded and no calls are archived, start EPO task, then run recording system.

2. When the Logger is under high load (all calls are recorded and archived), then begin with EPO tasks.

In both scenarios, specify the EPO utilization that will keep all recording and archiving functions with no errors and/or exceptions.

Table 11-6:
EPO Tasks

Test	Test Description	Test Results	Performance for CPU and memory
Pre-EPO tests	Verify that in the specified system load, all calls are being recorded with no errors/exceptions, prior to EPO task run	SC archiving with default 10 connections caused high CommManager CPU. As a result, Logger failed to record by CLS commands, and many calls entered with exceptions (#8, 12 and 17) **To enable good Logger recording performance, we reduced the amount of SC connections to 3.**	■ Per connection, 2000-3000 files are being archived (per hour) ■ SC archiving only, takes about 30-40% CommManager CPU on the Logger

Test	Test Description	Test Results	Performance for CPU and memory
Simulate recordings problem	During system running with its specified performance, Running the EPO tasks in **100%** utilization	When running the EPO tasks in 100% utilization the Logger did not record any call, mostly with exception 8 ("unspecified error in Logger")	■ Scan32 takes almost 100% CPU CommManager is almost on 0% CPU ■ All calls entered with exception 8.
Reduce EPO Utilization to 30%	When running the ePO tasks on **30%** utilization the logger continued to function with no errors.	All calls are inserted to DB with Recorded "Yes" and Status "OK Voice is archived to Storage Center.	■ Storage Center archiving tasks takes about 30% CommManager CPU in the Logger. ■ CLS pause-resume recording commands takes about 30% CommManager CPU in the Logger. ■ Running the EPO tasks for an hour – all calls were recorded in status OK

Test	Test Description	Test Results	Performance for CPU and memory
Run EPO Utilization 50%	Set CommManager service from Task Manager to "Real Time" priority Run same test as #3, but with higher (**50%**) utilization	We expect to conclude if the process Priority definition is effective for the CommManager, in a way it keeps its required CPU, while EPO server tasks are not harmed (=not display error or stop running)	■ All calls were recorded with status OK ■ Logger runs with high CPU (not recommended in the long term)
Functionality test on McAfee servers	Certify functional actions with servers that are installed with McAfee 8.0	Passed successfully, to review the tests and actions response time. See attached test report (separate)	

Remarks and Notes

1. DAT update does not have Utilization setting option, it does not affect the performance; the most consuming-resources task is the Scan.

2. Enforcing the EPO task caused after a few hours of high load, the logger's CPU time rises dramatically to around 95%. At this point the entire machine hangs, the logger doesn't start unless the McAfee is disabled. When disabling the McAfee the logger manages to start, however the CPU of the machine remains very high.

3. From this, we conclude that it is recommended to set the CommManager priority to Real Time in the Task Manager.

Conclusions

The parameters affecting recording performance and recommendations:

a. CommManager priority: It is highly recommended to set the ComMngr process of the logger at the highest priority (real-time), to prevent the process of the EPO taking all of the CPU and thus preventing the logger from running during the execution of the ePO tasks. (Note: Priority reverts back to Normal after machine restart).

b. The number of open connections from the Storage Center to the logger; It is recommended to lower the number of connections from the default 10, to decrease the load on the logger. We found that 3 was the optimal solution for the above mentioned settings. With more open connections, about 50% of the calls were not recorded (regardless EPO) due to exception 8.

c. The Virus Scan task should run in utilization lower than 100% to enable the logger to keep functioning during the scan. In our settings it was found that 30% utilization didn't interrupt the logger's performance. We do not recommend a higher utilization than this.

> **NOTE:**
>
> VoIP and PCI loggers running on Windows 2000 are approved to use ePO 3.5. This is based on the following facts:
>
> ▪ PCI Loggers and VoIP loggers use a stronger CPU
>
> ▪ Certification for Windows 2000 ISA based loggers has been completed.

Troubleshooting

Problem

When updating the McAfee antivirus software, the logger capture card stops receiving interactions, resulting in a **Fatal** error message.

Solution

◈ **To troubleshoot, do the following**

1. Navigate to **Start**, and then select **Run**.

   The Run window appears.

   Figure 11-3: Run Window
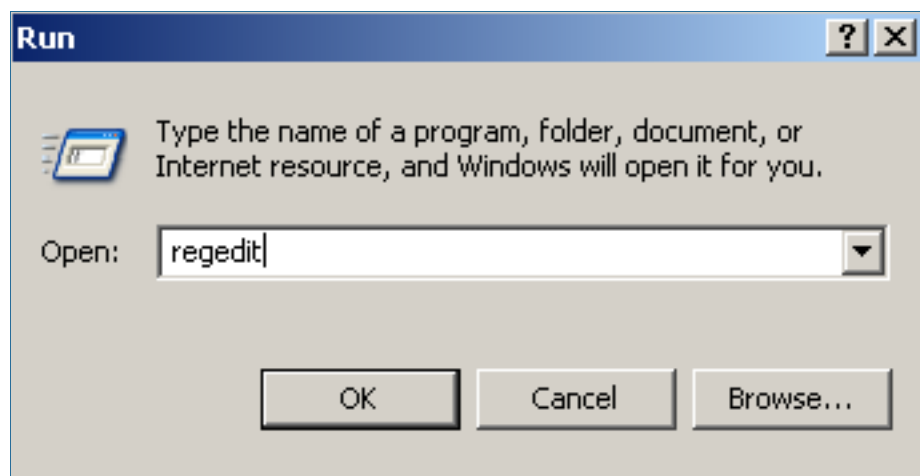
2. In the **Open** field, enter **regedit**, and click **OK**.

   The Registry Editor appears.

Figure 11-4: Registry Editor Window
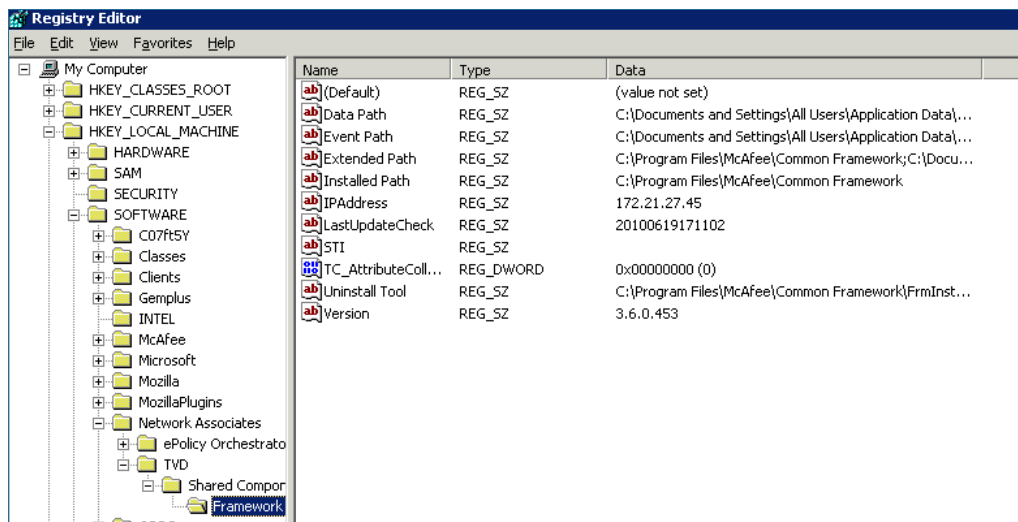
3. Navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Network Associates** > **TVD** > **Shared Components** > **Framework**.

Figure 11-5: New Menu- DWORD Value
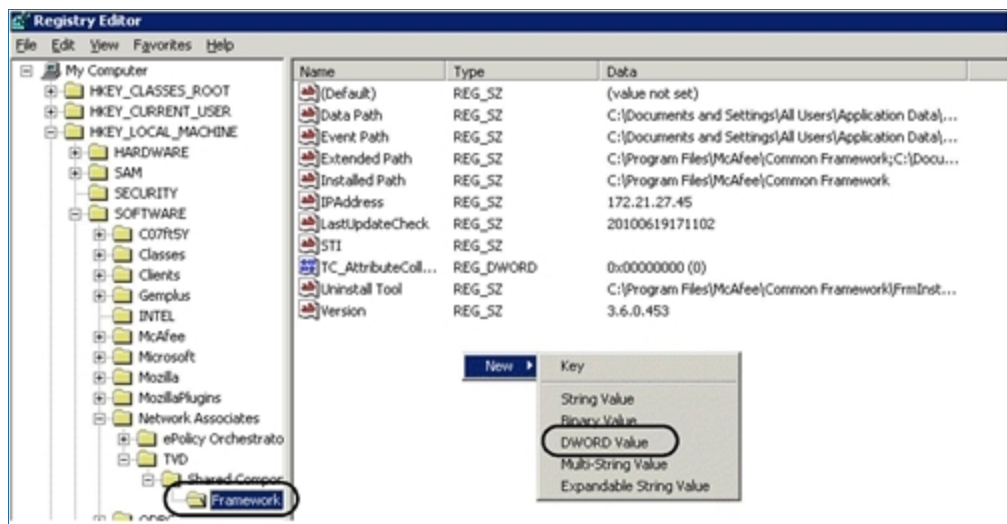
4. In the right-hand pane, right-click in the empty space, and select **New** > **DWORD Value**. A new registry key appears.

Figure 11-6: Registry Editor Window
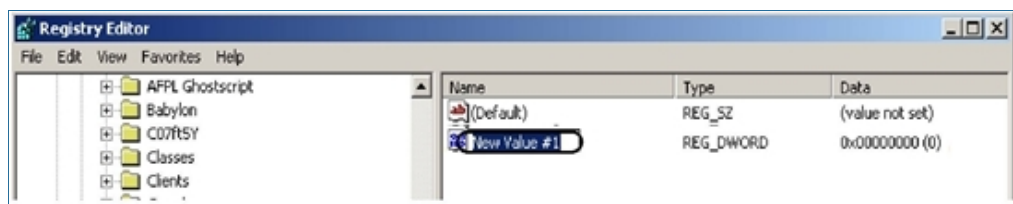
5. Change the name to **LowerWorkingThreadPriority**, and press **Enter**. The new file name **LowerWorkingThreadPriority** is reflected.

Figure 11-7: Modify Window
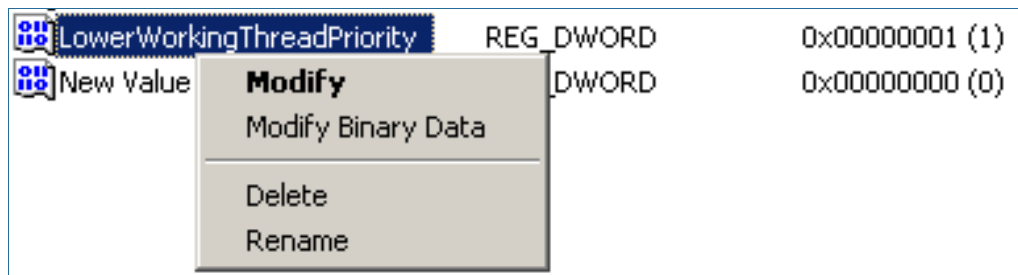
6. Right-click **LowerWorkingThreadPriority**, and select **Modify**. The Edit DWORD Value window appears.

Figure 11-8: Edit DWORD Value Window
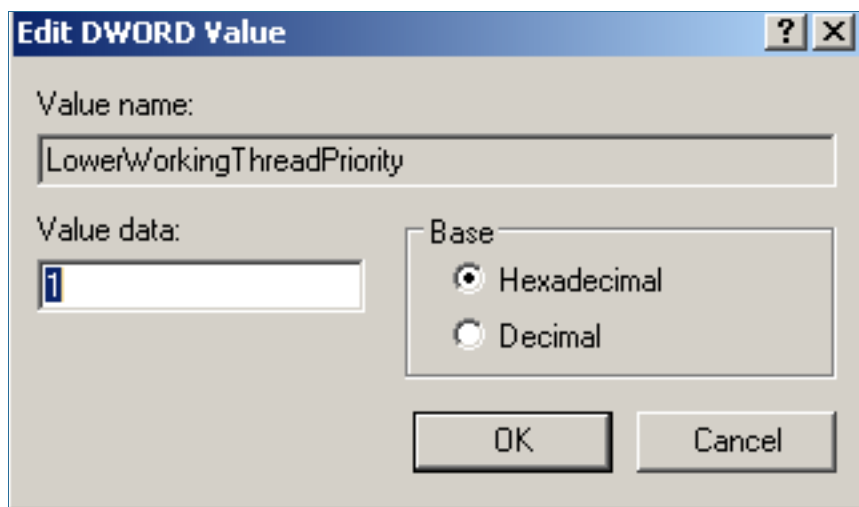
7. In the **Value data** field, enter **1**, and click **OK**.

8. Exit the registry.

9. Restart the McAfee Framework Service:

   a. Navigate to **Start** > **Run.**

   b. Enter **Services.msc.**

   c. Click **OK**.

The McAfee Framework Service window appears.

Figure 11-9: McAfee Framework Service Window
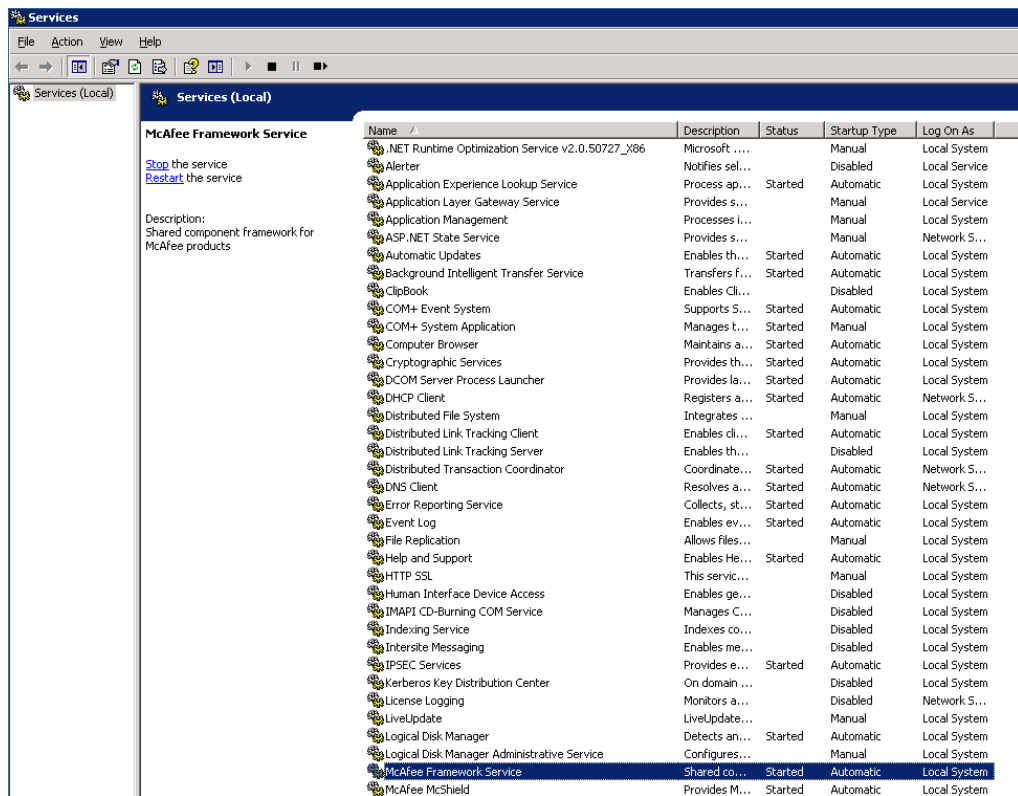
There is no need to restart the logger in the above process.

For more information, see *https://kc.mcafee.com/corporate/index?page=content&id=KB53690&pmv=print.*

12

Remote Desktop Connection

This chapter includes Remote Desktop Connection related issues.

Contents

PcAnywhere

Symantec pcAnywhere 11 Compatibility

Product	Symantec pcAnywhere 11 compatability
Release	
Synopsis	

Symantec pcAnywhere 11 compatibility is determined by the operating system running on the machine. To ensure proper system functionality, you must install the appropriate Symantec pcAnywhere 11 subversion on each NICE server installed at the site.

The following table lists the pcAnywhere subversions that must be installed on NICE servers.

> **Important!**
>
> Ensure that you install the correct subversion on your NICE machine!

Table 12-1:
PC Anywhere Subsessions Installed on NICE Servers

	pcAnywhere 11.0.0 (build 730)	pcAnywhere 11.0.1 (build 764)
Windows 2000 Pro	Yes	No
Windows 2000 Server	Yes	No
Windows 2003 Standard/Appliance Edition	No	Yes
WinXP Pro	No	Yes

NICE Products Certified to Work with pcAnywhere 12

Product	NICE Products Certified to Work with pcAnywhere 12
Release	Version 8.9 and NICE Perform
Synopsis	This section contains lists of the NICE products that are certified to work with pcAnywhere 12.

General Description

The NICE products that are certified to work with pcAnywhere 12 (remote solution) are listed below.

Version 8.9 Products

The following Version 8.9 products are certified to work with pcAnywhere 12.

Table 12-2:
Version 8.9 Products

NICE Component	Operating System
NiceLog Logger	Windows Server 2003 SP1
NiceUniverse Web Applications	Windows Server 2003 SE SP1
NiceCLS	Windows Server 2003 SE SP1
NICE Storage Center	Windows Server 2003 SE SP1
NiceScreen Logger	Windows Server 2003 SE SP1
SNMP Manager	Windows Server 2003 SE SP1

NICE Perform Products

The following NICE Perform products are certified to work with pcAnywhere 12.

Table 12-3:
NICE Perform Products

NICE Component	Operating System
Voice Logger	Windows Server 2003 SE SP1
CLS	Windows Server 2003 SE SP1
NICE Storage Center	Windows Server 2003 SE SP1
NiceScreen Logger	Windows Server 2003 SE SP1
Media Library	Windows Server 2003 SE SP1
Audio Analysis	Windows Server 2003 SE SP1
Applications Server	Windows Server 2003 SE SP1
Database Server	Windows Server 2003 SE SP1

Microsoft Remote Desktop Connection

Remote Connection Certifications for NICE Products

Product	NICE Products
Release	
Synopsis	This section lists remote connection software certified with NICE products.

NICE Products and Relevant Remote Connection Certifications

The following tables provide lists of NICE products and the relevant remote connection certifications for these products.

Table 12-4:
Remote Connection Certifications for NICE Products

NICE Products	Version	PC Anywhere 11.5*	PC Anywhere 12.0	Remote Desktop Protocol 6.0/6.1/ 7.0/7.1**	VNC Server 4.0
TDM Logger	9.01	Yes	Yes	Yes	Yes
	9.06	Yes	Yes	Yes	No
VoIP Logger	9.10	No	No	Yes	No
NiceCLS	8.93	Yes	Yes	Yes	Yes
NiceCall Focus III	8.90	Yes	Yes	Yes	No
NiceScreen Logger	8.9	Yes	Yes	Yes	Yes
NICE Storage Center	8.9	Yes	Yes	Yes	Yes
Web Applications	8.9	Yes	Yes	Yes	Yes
SNMP Manager	8.9	Yes	Yes	Yes	Yes

> **NOTE:** All NICE Products run on Microsoft Windows Server 2003/2008 (see the relevant Certified Servers Guide), except NiceCall Focus III (NCF III), which runs on Microsoft Windows XP Professional SP2.

Table 12-5:
NICE Products - NICE Perform Releases I, II, 9.09, 3, and 3.1

NICE Products	Version	PC Anywhere 11.5*	PC Anywhere 12.0	PC Anywhere 12.1****	Remote Desktop Protocol 6.0/6.1/7.0/7.1**	VNC Server 4.0 ***
TDM Logger	9.01	Yes	Yes	Yes	Yes	No
	9.06	Yes	Yes	Yes	Yes	No
VoIP Logger	9.12	Yes	Yes	Yes	Yes	No
NICE Interactions Center		Yes	Yes	Yes	Yes	No
NiceScreen Logger		Yes	Yes	Yes	Yes	No
Playback Server		Yes	Yes	Yes	Yes	No
SNMP Manager (NMS)		Yes	Yes	Yes	Yes	No
NICE Storage Center		Yes	Yes	Yes	Yes	No
Media Library		Yes	Yes	Yes	Yes	No
Application Server		Yes	Yes	Yes	Yes	No
Audio Analysis Server		Yes	Yes	Yes	Yes	No
ScreenSense Server		Yes	Yes	Yes	Yes	No
Reporter		Yes	Yes	Yes	Yes	No

NICE Products	Version	PC Anywhere 11.5*	PC Anywhere 12.0	PC Anywhere 12.1****	Remote Desktop Protocol 6.0/6.1/7.0/7.1**	VNC Server 4.0 ***
Database Server		Yes	Yes	Yes	Yes	No

* To verify compliance of older versions of PCAnywhere, see PcAnywhere on page 1.

** Microsoft Windows Remote Desktop Protocol (RDP) - Console Mode (use Console/Admin switch:

RDP 6.0: **Console** switch

RDP 6.1 and higher: **Admin** switch

*** Virtual Network Computing (VNC) support in NICE Perform is commitment-based.

> **NOTE:** All NICE Products run on Microsoft Windows Server 2003/2008 (see the relevant Certified Servers Guide).

Enabling Remote Connection on Microsoft Windows Server 2003

◆ **To enable Remote Connection in Microsoft Windows Server 2003:**

1. Start the **Terminal Services** service.

2. Right-click **My Computer,** and select **Properties**.

3. Click the **Remote** tab.

Figure 12-1: System Properties - Remote Tab (2003)
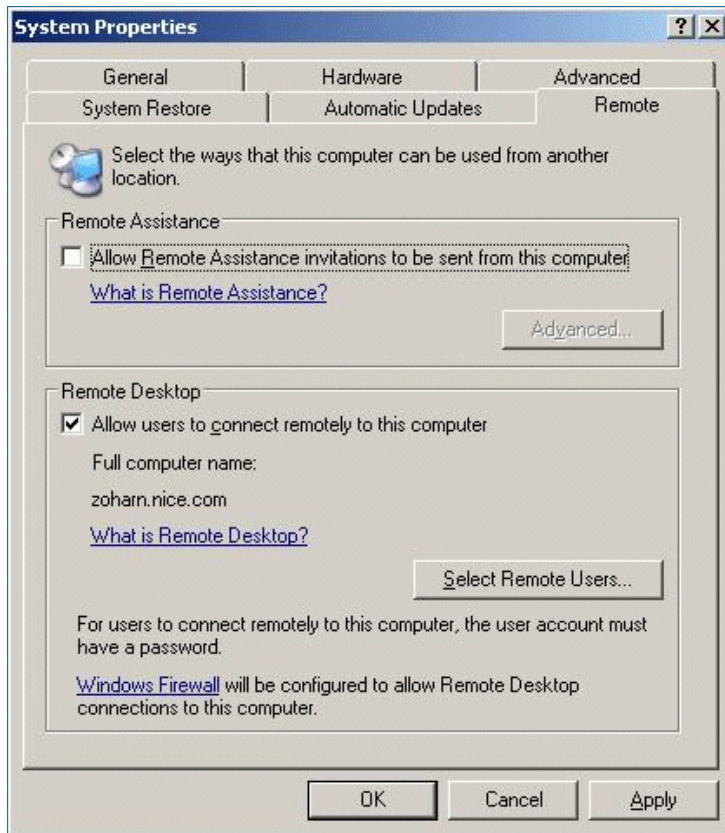
4. Select **Allow users to connect remotely to this computer**.

5. Click **OK**.

Enabling Remote Connection on Microsoft Windows Server 2008

◆ **To enable Remote Connection Microsoft Windows Server 2008:**

1. Start the **Terminal Services** service.

> 📝 **NOTE:** In Microsoft Windows Server 2008 R2, **Terminal Services** are called **Remote Desktop Services**.

2. Right-click **Computer,** and select **Properties.**

Figure 12-2: System Window (2008)

3. Click **Remote Settings**.

Figure 12-3: System Properties Window - Remote Tab (2008)

4. In the Remote tab, select **Allow connections from computers running any version of Remote Desktop (less secure)**.
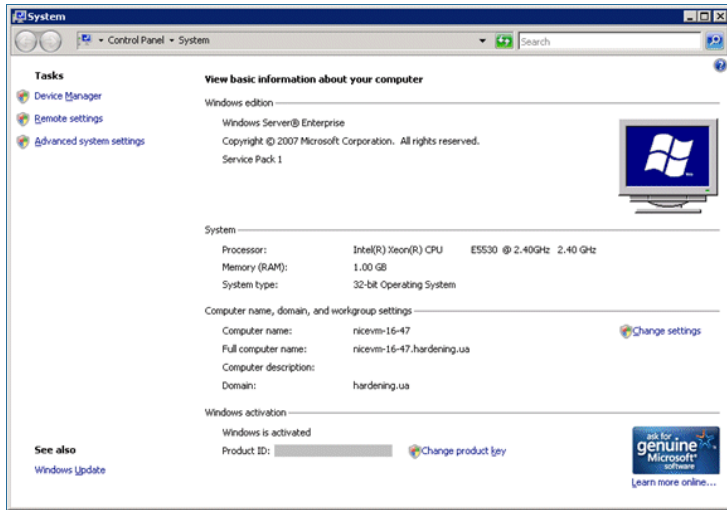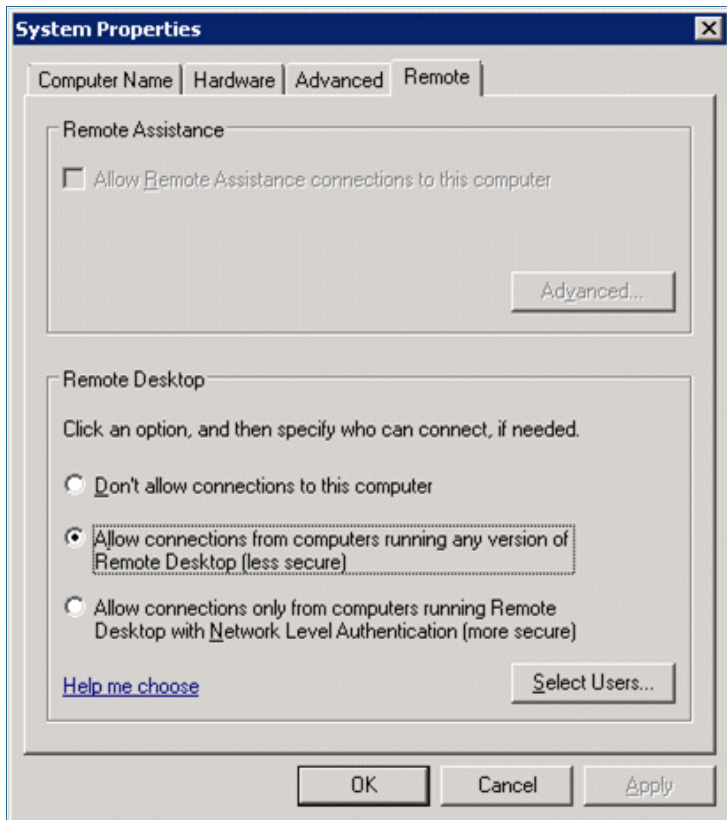
5. Click **OK**.

Remote Desktop Recommendations

■ To access the logger through VPN, access the server that connects to the logger on the LAN.

■ Close any RDP session when done (click ![x button]), or use the traditional logoff function.

■ In environments where the network between the RDP client to server is not stable, or when working with VPN that may disconnect due to inactivity timeout, do not leave an RDP session open when not needed.

■ Access the logger with **Console** Mode. If the network disconnects during the RDP session, close the session and reconnect again. Verify that there is no problem with IPCapture; if there is a problem, restart IPCapture.

Remote Desktop Limitations

> **NOTE:** The Console Mode for Microsoft Windows Remote Desktop Protocol has different switch names, depending on the RDP version:
>
> ■ RDP 6.0: **Console** switch
>
> ■ RDP 6.1 and higher: **Admin** switch

The following limitations apply to remote desktop:

■ Only **Console** mode is supported.

■ When you use remote desktop in **Console** mode, only one user can connect to the server at any one time. Once a user connects to the server, all other open sessions to that server are closed.

■ Once a user connects to the server, no one else can view the session. However, when working with PCAnywhere, the user can see the actions performed by the installer or technician.

Ports Used in the Remote Connection

The following table lists the ports that must be opened when working under Microsoft Windows Server 2003 with the Firewall enabled.

Table 12-6:
List of Ports

Service	TCP	UDP	Comment
PCA	22	22	

Service	TCP	UDP	Comment
PCA	5631		PCAnywheredata
PCA	5632	5632	PCAnywherestat
PCA	65301		
VNC	5900		
RDP	3389		
PCA - PCAnywhere			
RDP - Remote Desktop Protocol			
VNC - Virtual Network Computing			

RDP (Remote Desktop Protocol) Delay Solution

Product	RDP (Remote Desktop Protocol)
Release	
Synopsis	This section provides information regarding an RDP (Remote Desktop Protocol) delay issue and its solution.

Symptoms

When connecting to a machine using RDP (Remote Desktop Protocol), a serious delay could occur both on the client side (console "freeze") and on the server side (processes hang). As a result, crucial processes (for example, IP Capture process on the VoIP Logger) will face unexpected situations due to not receiving the necessary resources.

Cause

There are several different parameters and system configurations that could cause such delays. Some are related to the network configuration and others to the RDP version installed on either the client or the server.

1. The order of Network Providers in the registry could be incorrect. The key to be selected is **HKEY_ LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Ord er.** The default order is "RDPNP,LanmanWorkstation,WebClient". Note that in Vista clients (prior to SP1) there is a bug and the order is not as stated above (when installing Vista SP1 from a clean installation this bug is fixed). RDPNP should be the first provider in the list (before the LanmanWorkstation).

2. In RDP version 6.0, a network query is launched during the connection attempt (which does not happen in RDP version 5.x). If a WINS server is configured on the client, and this server does not respond, the query will time out. As a result, the server waits for a response from the client and this causes the symptoms as described above.

Solution

In general, the Remote Desktop Connection could affect both the client and the server, causing delays and process starvation.

Verify the following to solve the delays:

1. The registry key stated above **(HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Ord er)** is set to the default order ("RDPNP,LanmanWorkstation,WebClient").

2. If using RDP version 6.0 make sure all network configurations (for example, WINS servers) are available.

Remote Desktop- Remote Connection Console Mode for NICE 8.90

Product	Remote Desktop
Release	
Synopsis	This section displays the procedures for Remote Desktop- Remote Connection.

This section specifies the support and approval of Remote Connection – Remote Desktop Console mode on NICE 8.90 systems.

Environment

NICE System Components

Table 12-7:
Supported Products

NICE Product	OS	Version
Voice Loggers	Windows 2003 (Enterprise, Appliance) SP1	ISA 8.91 SP1 PCI 9.01 SP7
Web Applications (Universe)	Windows 2003 SE SP1	8.80 SP6

NICE Product	OS	Version
CLS	Windows 2003 SE SP1	8.90 SP4
Storage Center	Windows 2003 SE SP1	8.90 SP2
Screen Logger	Windows 2003 SE SP1	8.80 SP3
SNMP Manager	Windows 2003 SE SP1	2.02 SP5
Client (Screen Agent and Desktop Applications)	Windows 2000 Pro SP4	

Installation Instructions

Remote Desktop Solution

❖ **To install Remote Desktop Solution:**

1. Install the NICE servers and clients.

2. Remove other remote connection SW (if exist).

3. Enable Remote connection by starting the Terminal Services service, and enabling the remote option on My Computer > Properties > Remote tab):

Figure 12-4: System Properties - Remote Tab
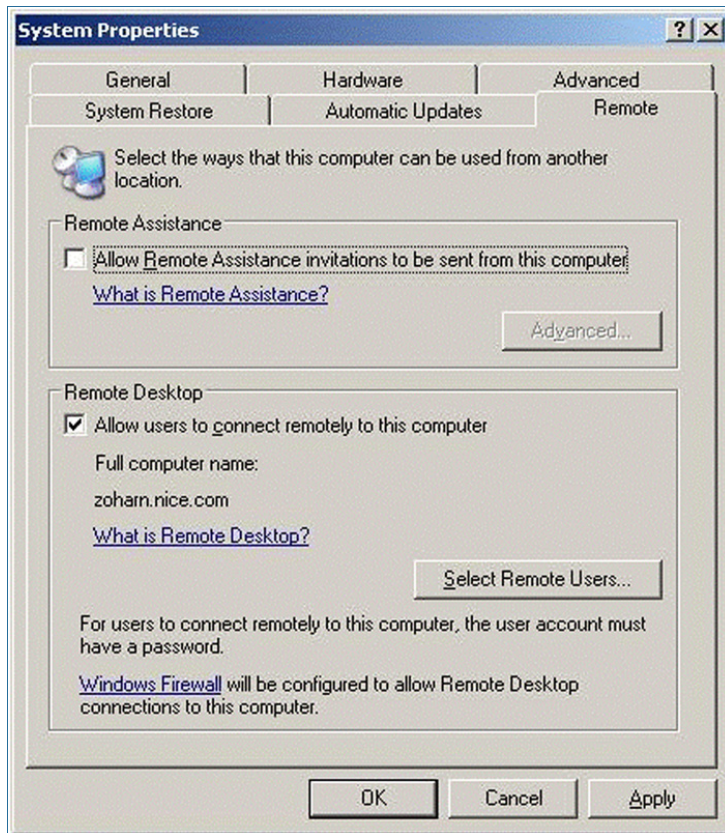
4. Synchronize all the servers time using NTP (optional).

5. Set up a dial-up connection using MODEM (connected external server part of sites network area).

Limitations

▪ Using remote desktop in console mode means that only one user can connect to the server at any onetime. Once a user connects to the server, any other open sessions to that server will be closed.

▪ Once a user connects to the server, no one else can see the session (unlike PCAnywhere in which the user can see that actions performed by the installer/technician).

[This page intentionally left blank]

A

Discontinued Technical Notes

This appendix lists the Technical Notes that were discontinued and whose information is now included in this document.

Contents

List of Discontinued Technical Notes

Table A-1:
List of Discontinued Technical Notes

Technical Note Number	Technical Note Title
TN0509	NICE Software Components Running on Windows XP Machines
TN0513	McAfee ePO 3.5 – Configuration Guide For Nice Products
TN0528	Windows Server 2003 Appliance Notes
TN0538	Windows Server 2003 Service Pack 1 Integration with NICE Servers
TN0539	Anti Virus
TN0549	Symantec pcAnywhere 11 compatibility
TN0552	SQL Server 2000 SP4
TN0555	Anti Virus Certifications for NICE Products
TN0564	Anti Virus Certifications for NICE Products III
TN0569	Windows 2000 Update Rollup 1 for Service Pack 4
TN0577	McAfee VirusScan products
TN0578	Norton Anti-Virus products
TN0616	ScreenAgent Configuration in Citrix Published Application Environment
TN0628	How to configure Voice and Screen best performance on Citrix
TN0640	McAfee ePO 3.5 and McAfee Antivirus 8.0 Certification for NICE 8.80
TN0642	Remote Desktop - Remote Connection Console Mode
TN0651	DBM Error on Loggers due to MS Security Patch KB921883
TN0656	PC Anywhere 12 certification in 8.90 NICE systems
TN0672	Compatibility of NICE Web Applications with Internet Explorer 7

Technical Note Number	Technical Note Title
TN0676	Fixing MSDTC in a Multi Site Environment
TN0680	NICE Support for Microsoft .NET Framework 2.0.
TN0688	NICE Support for Microsoft .NET Framework 2.0.-Playback Organizer
TN0698	NICE products certified to work with pcAnywhere 12
TN0701	Remote Connection Certifications for NICE Products
TN0705	MS SQL Server for NICE Perform Release 3
TN0719	Windows Server 2003 Service Pack 2 (SP2) Support
TN0736	.Net 3.0 Support
TN0776	RDP (Remote Desktop Protocol) - Delay Solution
TN0790	Incompatibility Citrix hotfix
TN0806	NICE Product Support for MS Windows XP Service Pack 3
TN0815	Resolving Citrix Connection Issues Related to ScreenSense
TN0820	.NET Framework Support for NP 3.1
TN0838	Interactions Center workaround for .NET 3.5
TN0867	Compatibility of NICE Web Applications with Internet Explorer 8
TN0889	Installing NICE Perform 3.2 on Windows 7
TN0890	Installing NICE Perform 3.1 on Windows 7
TN0897	Microsoft Software Service Packs Certified by NICE Systems

[This page intentionally left blank]

B

Using Real-Time Solutions with App-V

This appendix lists the limitations and rules for working with Real-Time Solutions in an App-V environment.

Contents

Working with the App-V System

The App-V Sequencer (Microsoft Application Virtualization Sequencer) is a wizard-based tool that administrators use to transform traditional applications into virtual applications. The Sequencer produces an application package that contains several files. These files include a sequenced application (.sft) file, one or more Open Software Description (.osd) application configuration files, one or more icon (.ico) files, a manifest xml file that can be used to distribute sequenced applications with electronic software delivery (ESD) systems, and a project (.sprj) file. The Sequencer can also generate a Windows Installer file (.msi) that can be deployed to clients configured for standalone operation. All files are stored in a shared content folder on the Management and/or Streaming Server and are used by the App-V Client to access and run sequenced applications.

The App-V Management Server (Microsoft Application Virtualization Streaming Server) has streaming capabilities that including active/package upgrade without Active Directory or SQL Server requirements. However, it does not have a publishing service, licensing, or metering capabilities. The publishing service of the App-V Management Server is used in conjunction with the App-V Streaming Server, so the Management Server configures the application but the Streaming Server delivers it (usually in branch offices).

App-V Limitations when Working With Real-Time Solutions

In App-V environments a bubble is an isolated environment streamed from the App-V server to the App-V client. On the client machine the application does not have to be installed.

When streaming the Real-Time Client to the App-V client, both clients must be in the same bubble as the application(s) you want to interact with.

If the Real-Time Client needs to interact with two App-V applications from separate bubbles, you must install the Real-Time Client on each bubble and interact using C2C (client to client) communication between the Real-Time Clients. In his case you must instal another Real-Time Client on the local computer and interact with the streamed clients using C2C.

[This page intentionally left blank]

Using Real-Time Solutions with Citrix Streaming

This appendix describes the limitations and rules for working with Real-Time Solutions with Citrix streaming.

Contents

Working with Citrix Streaming

A streamed application in Citrix resides in a separate memory space and environment and is delivered to the Citrix client without installing an application on the client side. The streamed application is located in a controlled isolated environment (sandbox).

To set a package for Citrix application streaming so that the Real-Time Client can capture other streamed applications both applications must run inside the same sandbox. The citrix profiles must be installed on a separate dedicated machine.

Citrix Streaming Limitations when Working With Real-Time Solutions

The Real-Time Client must be part of the same streaming package as the monitored applications. Another option is to use Inter-Isolation communication for Real-Time Client interaction with other streamed packages. You can install the Real-Time Client on the client computer to interact with one or more Citrix streamed applications.

Make sure of the following when setting up the Citrix Profiler:

▪ In the Support Legacy Offline Plug-ins page, select **Enable support for 6.0 Offline Plug-ins**.

▪ In the Select Install Page, select **Advanced Install**.

▪ In the Set up Inter-Isolation Communication page make sure to enter the path to the Profiler Package if you want to link between the profile package for the Real-Time client and other streamed applications.

▪ In the Select Install Method page, select **Run install program or command line script**.

▪ In the Choose Installer page, browse to or type in the path to the Process Optiization Client.msi.

When the Profiler is finished and the Citrix package is ready, make sure of the following:

▪ For a streamed Real-Time Client package, open the Target Properties configuration window and clear **Enable pre-launch analysis**.

▪ The remaining Target Properties rules should remain with their default values.

> **NOTE:** The Real-Time Client can interact with two streamed applications (each from a different server) only when it is installed locally.