Third Party Technical Guidelines

Configuration Guide

Release:	Cross-Release NICE Engage Platform 6.x / NICE Interaction Management 4.1 Real-Time Solutions 4.9 NICE Perform 3.2 / 3.5
Document Revision:	D6
Distribution Status:	Published
Publication Date:	April 2017

PROPRIETARY AND CONFIDENTIAL INFORMATION

Information herein is proprietary information and trade secrets of NICE Ltd. and/or its affiliated companies (Affiliates). This document and the information herein is the exclusive property of NICE and its Affiliates and shall not be disclosed, in whole or in part, to any third party or utilized for any purpose other than the express purpose for which it has been provided.

IMPORTANT NOTICE

Subject always to any existing terms and conditions agreed between you and NICE or any Affiliate with respect to the products which are the subject matter of this document, neither NICE nor any of its Affiliates shall bear any responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any product supplied or any reliance placed on the content of this document. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any products supplied or the content of this document. Information in this document is subject to change without notice and does not represent a commitment on the part of NICE or any Affiliate.

Products supplied may be protected by one or more of the US patents listed at www.nice.com/Patents.

For the full list of trademarks of NICE and its Affiliates, visit www.nice.com/Nice-Trademarks. All other marks used are the property of their respective proprietors.

For assistance, contact your local supplier or nearest NICE 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

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

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

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

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

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

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

[This page intentionally left blank]

1

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 267.

This document serves as general guidelines and applies to all existing NICE Engage Platform/NICE Interaction Management 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*.

Document Revision History

Revision	Modification Date	Software Version	Description
D6	April 2017	NICE Engage Platform 6.6	■ Updated SQL 2014 requirements. See SQL Server 2014 on page 217. ■ Updated table for .NET Framework 4.6 support. See Overview on page 174.
D5	January 2017	NICE Engage Platform 6.6	■ Removed references to sunset NICE products. ■ Updated .NET Framework, Office Scan and Trend Micro versions ■ Updated remote connection guidelines. See Remote Connection to Customers on page 265. ■ Added KBs Delivered by Microsoft and NICE Certification Policy on page 220 ■ Added KB3182203 and KB3192321 to Microsoft Daylight Savings Time Updates on page 229. ■ Added support of .NET Framework 4.6.2 for NICE Engage Platform 6.x. ■ Removed the requirement to add NICE Web Application URL to the Compatibility View Settings List for NICE Engage Platform in Adding the NICE Web Application URL to the Compatibility View Settings List on page 158 and Internet Explorer 11 on page 160 ■ Added secured sites to FIPS limitation regarding spell check. See Spell Check Limitation on page 228.

Revision	Modification Date	Software Version	Description
D4	October 2016	NICE Engage Platform 6.5	■ Updated Microsoft Daylight Savings Time Updates on page 229 ■ Updated NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 in NICE Products and Antivirus Certification Matrices on page 244 ■ Updated table in Microsoft Software Service Packs Certified by NICE Systems on page 23
D3	September 2016	NICE Engage Platform 6.5	■ Updated Microsoft Software Service Packs Certified by NICE Systems on page 23 ■ Added NICE Interaction Management information to Client Applications Compatibility on page 117 ■ Updated Internet Explorer 8 on page 145
D2	August 2016	NICE Engage Platform 6.5	■ Updated Microsoft Software Service Packs Certified by NICE Systems on page 23 ■ Added NICE Interaction Management information to Client Applications Compatibility on page 117 ■ Updated Sophos version in NICE Products and Antivirus Certifications Matrix - NICE Engage Platform 6.x table in NICE Products and Antivirus Certification Matrices on page 244 ■ Added KBs to table in Microsoft Daylight Savings Time Updates on page 229

Revision	Modification Date	Software Version	Description
D1	July 2016	NICE Engage Platform 6.5	■ Updated supported NICE releases with Microsoft Service Packs. See Microsoft Software Service Packs Certified by NICE Systems on page 23. ■ Updated Engage client compatibility for Windows 10. See Client Applications Compatibility on page 117. ■ Updated virus certifications for NICE Interaction Management. See General Antivirus on page 234.
D0	June 2016	NICE Engage Platform 6.5	■ Added requirements for .NET Framework 4.6. See Microsoft .NET Framework 4.6 Requirements on page 185 ■ Corrected requirements for .NET Framework 4.5. See Microsoft .NET Framework 4.5 Requirements on page 182. ■ Added Windows 10 32-bit/64-bit on page 117. ■ Added Google Chrome with the IE Tab Extension on page 165.
C9	February 2016	NICE Engage Platform 6.4	■ Added new Microsoft Software service packs to Microsoft Software Service Packs Certified by NICE Systems on page 23 ■ Updated the Synopsis in Internet Explorer 11 on page 160 ■ Added Prerequisite Updates for Internet Explorer 11 on page 160 ■ Updated Conclusions on page 161 in Internet Explorer 11 on page 160 ■ Added new Microsoft DST Updates to Microsoft Daylight Savings Time Updates on page 229

Revision	Modification Date	Software Version	Description
C8	November 2015	NICE Engage Platform 6.4	- Updated Microsoft Server Operating Systems on page 35 - Updated product and release Information under the following: - Internet Explorer 8 on page 145 - Internet Explorer 9 on page 154 - Internet Explorer 10 on page 157 - Internet Explorer 11 on page 160 - Updated *Sentinel 6.3*, to *Sentinel 6.X* throughout the guide.
C7	August 2015	NICE Engage Platform 6.4 NICE Interactions Management 4.1	- Added NICE Sentinel to Microsoft Software Service Packs Certified by NICE Systems on page 23 - Updated antivirus information adding support for McAfee ePO 4.8. See: - Table 12-1: NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 - Table 12-2: NICE Products and Antivirus Certifications Matrix - NICE Engage Platform 6.x - Updated Service Pack information for Microsoft products in Microsoft Software Service Packs Certified by NICE Systems on page 23

Revision	Modification Date	Software Version	Description
C6	May 2015	NICE Engage Platform 6.3.5 NICE Interactions Management 4.1 NICE Real Time Solutions 4.9	- Updated for NICE Engage Platform 6.3. - Updated Anti-virus information - Added NICE Sentinel 2.5/4.1 to the following sections: - Internet Explorer on page 123 - Microsoft SQL Server on page 187 - Microsoft .NET Framework on page 173 - Removed XBAP information from guide. See the *Workstation Setup Guide*. - Updated registry path for .NET Framework, see Microsoft .NET Framework 4.5 Requirements on page 182 - Added the following chapters: - SQL Server 2012 on page 216 - SQL Server 2014 on page 217 - Added configuring Windows for FIPS. See Federal Information Processing Standards (FIPS) on page 225 - Updated the following Internet Explorer browsers, regarding Sentinel Release 6.3: - Internet Explorer 9 on page 154 - Internet Explorer 10 on page 157 - Internet Explorer 11 on page 160
C5	November 2014	4.1	Added section. Added a Before You Begin section.

Revision	Modification Date	Software Version	Description
C4	September 2014	6.3	Updated flowing topics: ▪ Microsoft Software Service Packs Certified by NICE Systems on page 23 ▪ Internet Explorer on page 123 ▪ Microsoft .NET Framework on page 173 ▪ Microsoft Daylight Savings Time Updates on page 229 ▪ NICE Products and Antivirus Certification Matrices on page 244 ▪ Updated ▪ Added the topic .
C3	September 2014	4.1.4x	▪ Updated NICE Products and Antivirus Certification Matrices on page 244(added separate table for NICE Interaction Management Release 4.1). ▪ Added
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 111. ▪ Updated the information for Internet Explorer 11 on page 160. ▪ Added about XBAP limitations. See Microsoft .NET Framework 4.0 and up with NICE Interaction Management 4.1.46 and Above on page 181. ▪ 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
C1	March 2014		Added Internet Explorer 11 support. See Internet Explorer 11 on page 160. Added an SEP limitaion. See SEP on page 236.
B9	January 2014		Fixed information regarding Microsoft Internet Explorer 10. See Internet Explorer 10 on page 157. Removed the Citrix section. The information is now in the Virtualization Guide.
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
B7	November 2013		■ Updated Microsoft Client Operating Systems: ■ Updated Reporter Viewer on page 103, and NICE ScreenAgent on page 104. ■ Added PO Client and NICE Insight to Impact Bridge on page 106 ■ Updated Manually Installing Client Applications on page 107 (updated the note that appears before the procedure). ■ Added section for Release 4.1.46 for XBAP. See Microsoft .NET Framework 4.5 Requirements on page 182 and Microsoft .NET Framework 4.0 and up with NICE Interaction Management 4.1.46 and Above on page 181.

Revision	Modification Date	Software Version	Description
B6	October 2013		■ Updated Internet Explorer 10 on page 157. Added the section Adding the NICE Web Application URL to the Compatibility View Settings List on page 158. ■ Added the appendix, Using Real-Time Solutions with App-V on page 271. ■ Added the appendix Using Real-Time Solutions with Citrix Streaming on page 275.
B5	July 2013		■ Updated Internet Explorer on page 123 (small correction in the **Contents**).
B4	July 2013		■ Updated Table 2-1: Microsoft Software Service Packs certified by NICE Systems ■ Added Internet Explorer 10 on page 157 ■ Updated Microsoft Daylight Savings Time Updates on page 229. ■ Updated General Limitations on page 235 ■ Updated NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 on page 245 (added: McAfee 8.8/8.8i and Sophos 10.2)
B3	March 2013		■ Added Microsoft .NET Framework 4.5 Requirements on page 182 ■ Updated NICE Web Applications Known Issues with Internet Explorer 8 on page 146 ■ Updated NICE Web Applications Known Issues with Internet Explorer 9 on page 155

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 123. - Updated IE8 General Description and Conclusions on page 145. - Updated IE9 General Description and Conclusions on page 154. - Added McAfee limitation on page 236. - Added TDM Logger 9.4 with Antivirus Certification in NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 on page 245. - Added Trend Micro OfficeScan 10.5 and Trend Micro OfficeScan 10.6 to NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 on page 245.

Revision	Modification Date	Software Version	Description
B1	July 2012		- Added information for avoiding false positives to SEP on page 236. - Added information to NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 on page 245. - Updated the table in Microsoft Daylight Savings Time Updates on page 229.
B0	January 2012		- Updated Windows 7 32-bit/64-bit on page 99.
A9	November 2011		- Added SP3 for SQL Server 2008 in Microsoft Software Service Packs Certified by NICE Systems on page 23. - Added information regarding machine and domain names with non-ASCII characters in Localization on page 86. - Added note regarding support for 32-bit version Internet Explorer in Internet Explorer on page 123.
A8	November 2011		- Added SP1 for SQL Server 2008 R2 in Microsoft Software Service Packs Certified by NICE Systems on page 23. - Updated ROD Client information in Windows 7 32-bit/64-bit on page 99 - Added Microsoft .NET Framework 4.0 Requirements on page 179 - Updated DST patch list in Microsoft Daylight Savings Time Updates on page 229. - Added McAfee ePO 4.6 in McAfee ePO on page 235, General Antivirus on page 234, and NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 on page 245. - Added Sophos exclusions in Sophos on page 244.

Revision	Modification Date	Software Version	Description
A7	September 2011		- Updated Table 2-1: Microsoft Software Service Packs certified by NICE Systems
A6	July 2011		- Updated Remote Connection to Customers for Microsoft Windows Server 2008. - Added support for Internet Explorer 6. See Internet Explorer 6 on page 125 - Added Sophos 9.7.
A5	June 2011		- Formatting changes. - Added EPO 4.5 to NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 on page 245
A4	May 2011		- Added NICE Interaction Management Release 4.1 compatibility. - Updated Compatibility with Microsoft Windows 7 for 32/64 bit. See Client Application Compatibility on page 99 - Added Internet Explorer compatibility. See Internet Explorer 9 on page 154 - Added Logger version 9.07 to anti-virus tables. - Added Sophos 9.5.
A3	March 2011		- Updated the section on Microsoft Windows 7. See Windows 7 32-bit/64-bit on page 99 - Added new section for Daylight Savings Time. See Microsoft Daylight Savings Time Updates on page 229

Revision	Modification Date	Software Version	Description
A2	February 2011		■ Updated Microsoft service packs support and requirements. See Microsoft Software Service Packs Certified by NICE Systems on page 23 ■ Added compatibility for Microsoft Windows 7 64-bit, and updated compatibility by NICE Perform release. See Windows 7 32-bit/64-bit on page 99 ■ Added new section for silent installations. See Using Silent Installation to Install Client Applications on page 102 ■ Updated procedures for installing client-side components on Microsoft Windows 7. See Manually Installing Client Applications on page 107
A1	November 2010		■ Updated SQL support. See Microsoft SQL Server on page 187 ■ Updated Antivirus. See Antivirus on page 233

Scope of this Guide

Software Version

This guide is updated for:

- NICE Engage Platform 6.6
- NICE Interaction Management 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*
Configuring XBAP	*Workstation Setup Guide*
Microsoft Daylight Savings Time configurations	*Maintenance Guide*

2

Microsoft Software Service Packs Certified by NICE Systems

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

Product	NICE Engage Platform NICE Interaction Management Version 8.9 SMB
Release	NICE Engage Platform 6.x NICE Interaction Management Release 4.1 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
Windows Server 2003 R2 Standard Edition 32-bit	SP2	■ NICE Version 8.9 ■ NICE Interaction Management Release 4.1 - supported only for upgrades	
Windows Server 2003 R2 Enterprise Edition 32-bit	SP2	■ NICE Version 8.9 ■ NICE Interaction Management Release 4.1 - supported only for upgrades	
Windows Server 2003 R2 Standard Edition 64-bit	SP2	■ NICE Interaction Management Release 4.1 - supported only for upgrades	DB Server Only

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

Microsoft Software	Service Pack	NICE Release	Comment
Windows Server 2003 R2 Enterprise Edition 64-bit	SP2	■ NICE Interaction Management Release 4.1 - supported only for upgrades	DB Server Only
Windows XP	SP2	■ NICE Version 8.9 ■ NICE Interaction Management Release 4.1	Client Side Only
Windows XP	SP3	■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x	Client Side Only
Windows Vista Business	SP2	NICE Perform ■ Release 3 SP4 ■ Release 3.1	Client Side Only

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

Microsoft Software	Service Pack	NICE Release	Comment
Windows Vista Enterprise Edition	SP2	■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x	Supported by: ■ Set Security ■ ROD ■ Reporter Viewer ■ ScreenAgent ■ Desktop Analysis Agent RTS ■ NICE Player Codec Pack ■ Nice Standalone Player ■ Survey Manager ■ Media Library
Windows 7	SP1	■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x	Supported Client Side Applications Only
Windows 8		■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x	
Windows 8.1		■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x	

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

Microsoft Software	Service Pack	NICE Release	Comment
Windows 10		■ NICE Engage Platform 6.4 and up	
Windows Server 2008 Standard Edition 32-bit	SP2	■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x, supported only for upgrades ■ NICE Perform eXpress Release 2.1	
Windows Server 2008 Enterprise Edition 32-bit	SP2	■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x, supported only for upgrades	
Windows Server 2008 Standard Edition 64-bit	SP2	■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x, supported only for upgrades	
Windows Server 2008 Enterprise Edition 64-bit	SP2	■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x, supported only for upgrades	
Windows Server 2008 R2 Enterprise Edition 64-bit		■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x, supported only for upgrades	

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

Microsoft Software	Service Pack	NICE Release	Comment
Windows Server 2008 R2 Standard Edition 64-bit		■ NICE Interaction Management Release 4.1 ■ NICE Engage Platform 6.x, supported only for upgrades	
Windows Server 2008 R2 Standard Edition 64-bit	SP1	■ NICE Interaction Management Release 4.1	
Windows Server 2008 R2 Enterprise Edition 64-bit	SP1	■ NICE Interaction Management Release 4.1	
Windows 2012 Datacenter 64-bit		■ NICE Engage Platform 6.x	
Windows 2012 Standard 64-bit		■ NICE Engage Platform 6.x	
Windows 2012 R2 Datacenter 64-bit		■ NICE Engage Platform 6.x	
Windows 2012 R2 Standard 64-bit		■ NICE Engage Platform 6.x	
SQL Server 2005 Standard Edition 32-bit	SP3	■ NICE Interaction Management Release 4.1 - supported only for upgrades	

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

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2005 Standard Edition 64-bit	SP3	■ NICE Interaction Management Release 4.1 - supported only for upgrades	
SQL Server 2005 Enterprise Edition 64-bit	SP3	■ NICE Interaction Management Release 4.1 - supported only for upgrades	
SQL Server 2005 Standard Edition 32-bit	SP4	■ NICE Interaction Management Release 4.1 - supported only for upgrades	
SQL Server 2005 Standard Edition 64-bit	SP4	■ NICE Interaction Management Release 4.1 - supported only for upgrades	
SQL Server 2005 Enterprise Edition 64-bit	SP4	■ NICE Interaction Management Release 4.1 - supported only for upgrades	
SQL Server 2005 Enterprise Edition 32-bit	SP4	NICE Perform ■ Release 3 SP4 ■ Release 3.1 ■ Release 3.2 ■ Release 3.5	
SQL Server 2008 Standard Edition 32-bit	SP1	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	

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

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

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

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2008 Standard Edition 32-bit	SP4	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 Standard Edition 64-bit	SP4	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 Enterprise Edition 64-bit	SP4	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 R2 Standard Edition 32-bit	SP1	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 R2 Standard Edition 64 -bit	SP1	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 R2 Enterprise Edition 64-bit	SP1	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 R2 Standard Edition 32-bit	SP2	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 R2 Standard Edition 64-bit	SP2	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	

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

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2008 R2 Enterprise Edition 64-bit	SP2	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 R2 Standard Edition 32-bit	SP3	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 R2 Standard Edition 64-bit	SP3	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2008 R2 Enterprise Edition 64-bit	SP3	■ NICE Interaction Management Release 4.1 ■ NICE Sentinel 4.1	
SQL Server 2012 Enterprise Edition 64-bit	SP1	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.X	
SQL Server 2012 Standard 64-bit	SP1	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.X	
SQL Server 2012 Enterprise Edition 64-bit	SP2	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.X	
SQL Server 2012 Standard 64-bit	SP2	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.X	
SQL Server 2012 Standard 64-bit	SP3	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.X	
SQL Server 2012 Enterprise Edition 64-bit	SP3	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.X	

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

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2014 Enterprise Edition 64-bit		■ NICE Engage Platform 6.X	
SQL Server 2014 Standard 64-bit		■ NICE Engage Platform 6.X	
SQL Server 2014 Enterprise Edition 64-bit	SP1	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.X	
SQL Server 2014 Standard 64-bit	SP1	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.X	
SQL Server 2014 Enterprise Edition 64-bit	SP2	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.5	
SQL Server 2014 Standard 64-bit	SP2	■ NICE Engage Platform 6.X ■ NICE Sentinel 6.5	

[This page intentionally left blank]

3

Microsoft Server Operating Systems

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

Contents

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 40)
	NICE Perform RII (from SP4)	OK (See Limitations on page 40)
	NICE Perform 9.09	OK
	NICE Perform R3	OK (See Limitations on page 40)
	NICE Perform R3.1	OK

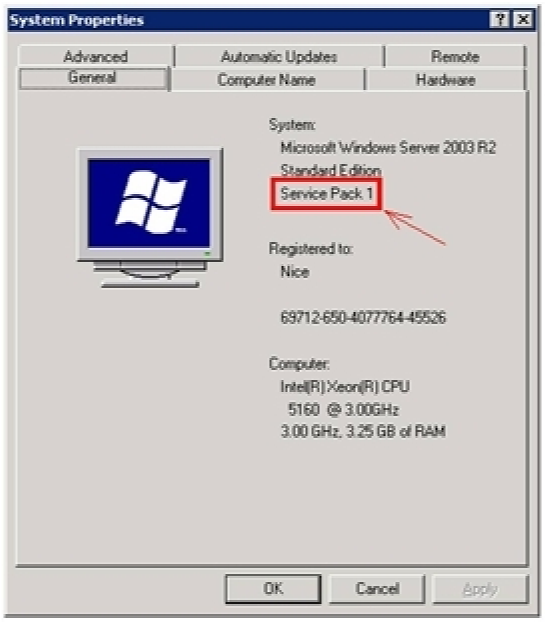
No.	Release Version	Status
	NICE Perform R3.2	OK
	NICE Perform R3.5	OK
	NICE Interaction Management R4.1	For upgrades only

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



System:
Microsoft Windows Server 2003 R2
Standard Edition
Service Pack 1

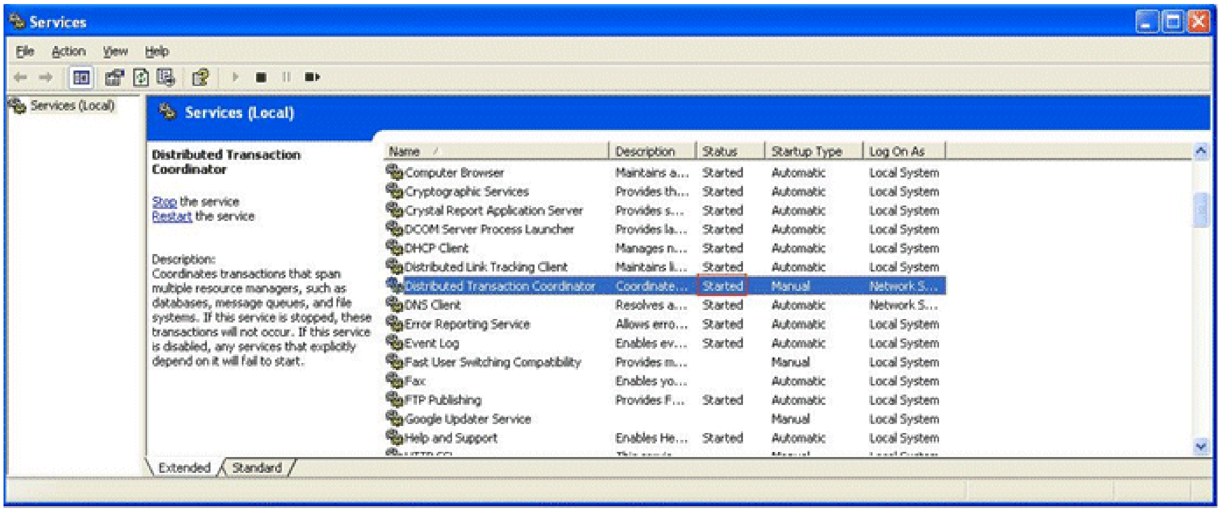
Registered to:
Nice

69712-650-4077764-45526

Computer:
Intel(R) Xeon(R) CPU
5160 @ 3.00GHz
3.00 GHz, 3.25 GB of RAM

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



Distributed Transaction Coordinator

Stop the service
Restart the service

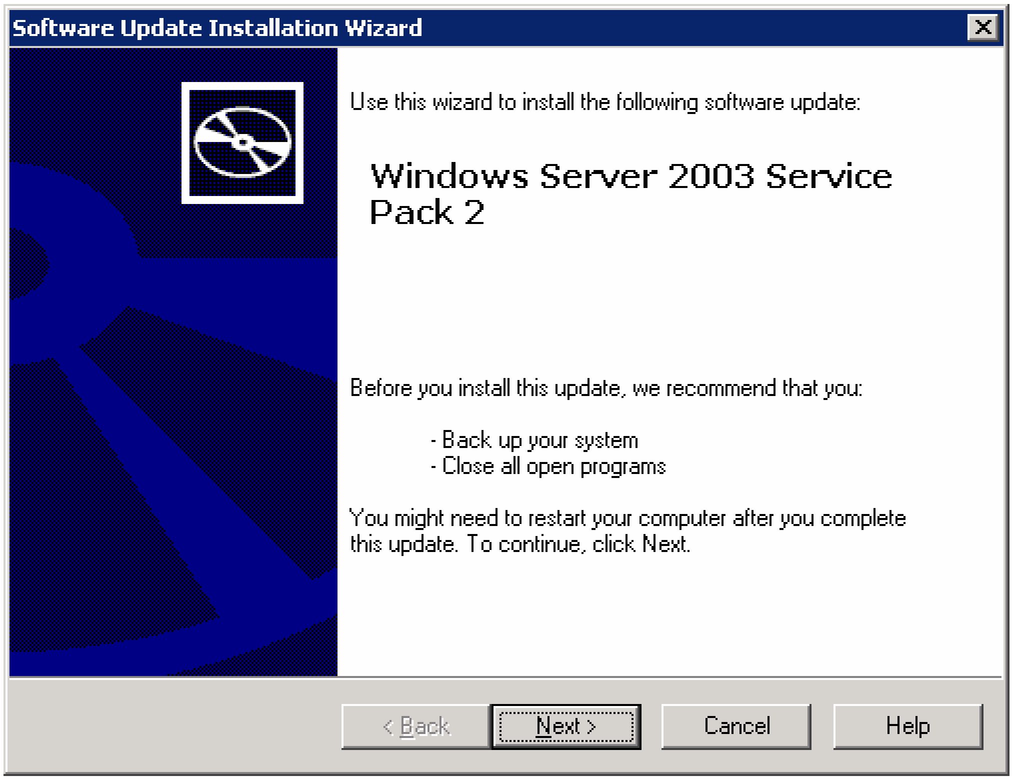
Description:
Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
Computer Browser	Maintains a...	Started	Automatic	Local System
Cryptographic Services	Provides th...	Started	Automatic	Local System
Crystal Report Application Server	Provides s...	Started	Automatic	Local System
DCOM Server Process Launcher	Provides la...	Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...	Started	Manual	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Service	Allows erro...	Started	Automatic	Local System
Event Log	Enables ev...	Started	Automatic	Local System
Fast User Switching Compatibility	Provides m...		Manual	Local System
Fax	Enables yo...		Automatic	Local System
FTP Publishing	Provides F...	Started	Automatic	Local System
Google Updater Service			Manual	Local System
Help and Support	Enables He...	Started	Automatic	Local System

To install Microsoft Windows Server 2003 SP2:

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

   Figure 3-3: Software Update Installation Wizard Window



Use this wizard to install the following software update:

Windows Server 2003 Service Pack 2

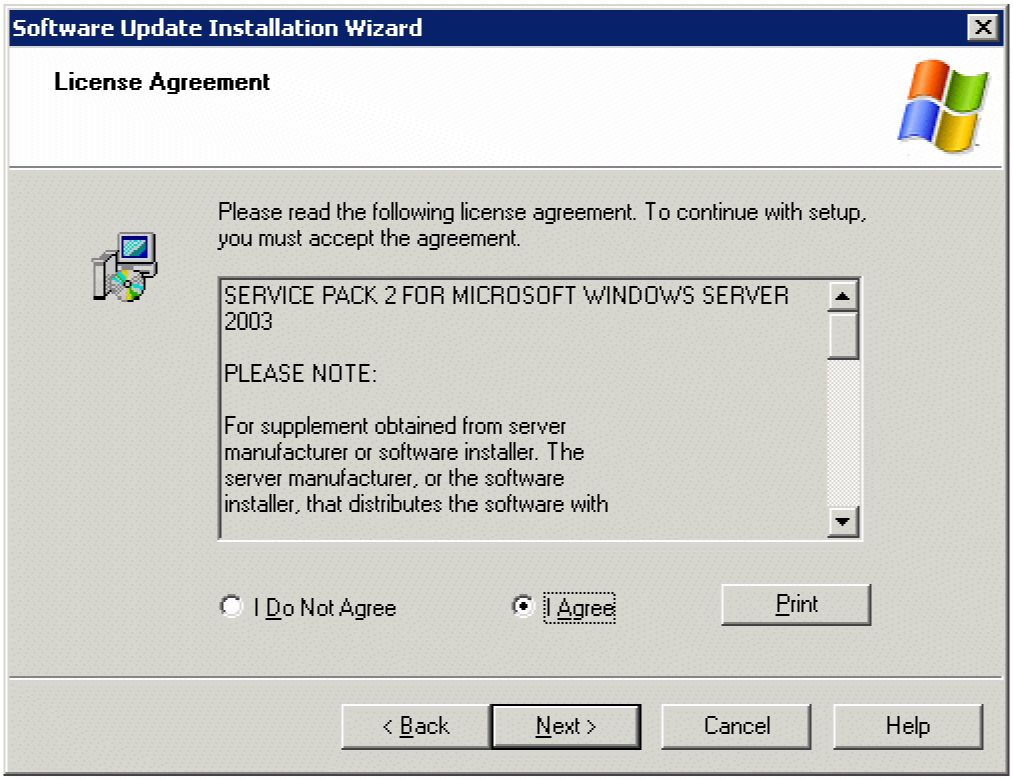
Before you install this update, we recommend that you:

- Back up your system
- Close all open programs

You might need to restart your computer after you complete this update. To continue, click Next.

2. Click **Next**.

Figure 3-4: License Agreement



Please read the following license agreement. To continue with setup, you must accept the agreement.

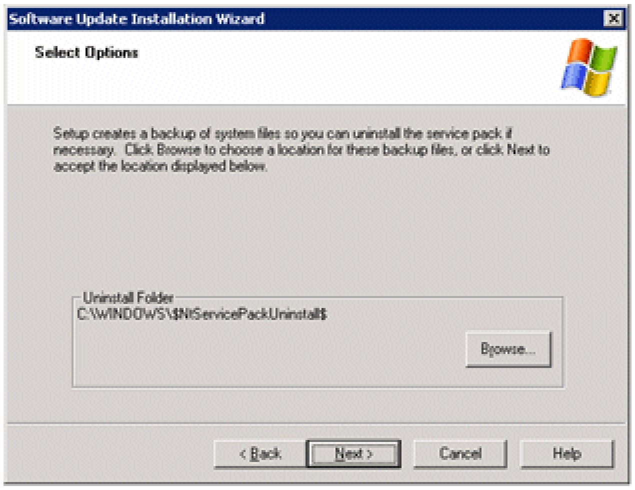
SERVICE PACK 2 FOR MICROSOFT WINDOWS SERVER 2003

PLEASE NOTE:

For supplement obtained from server manufacturer or software installer. The server manufacturer, or the software installer, that distributes the software with

3. Select **I agree,** and click **Next**.

Figure 3-5: Select Options Window

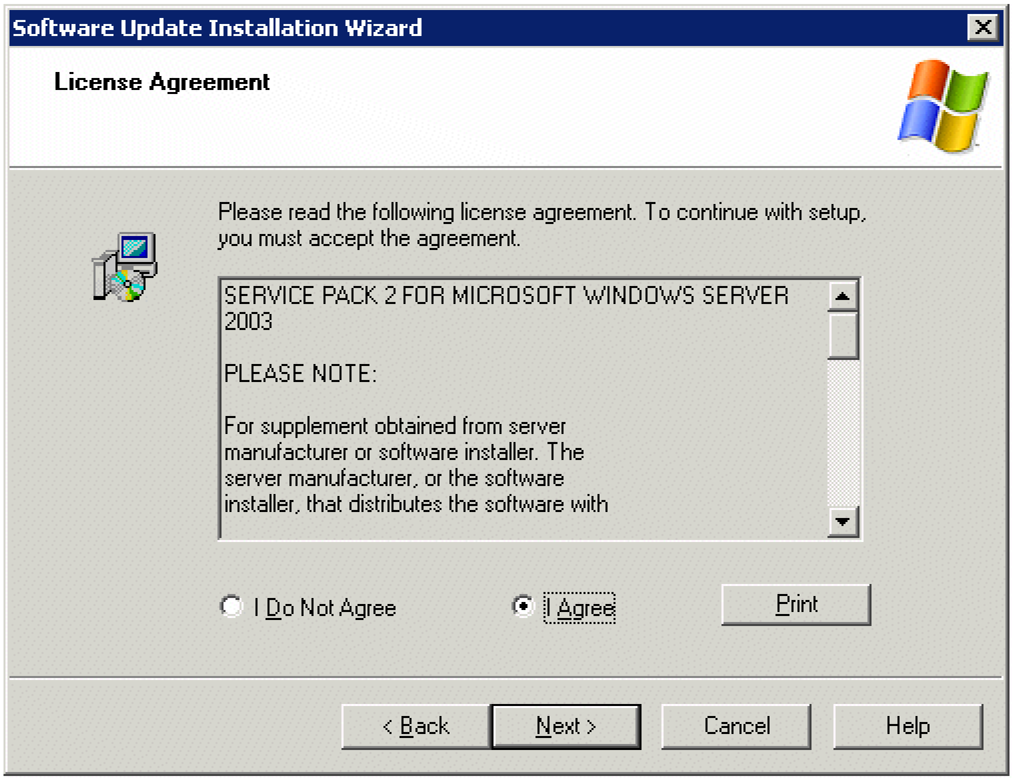


Setup creates a backup of system files so you can uninstall the service pack if necessary. Click Browse to choose a location for these backup files, or click Next to accept the location displayed below.

Uninstall Folder
C:\WINDOWS\$NtServicePackUninstall$

4. Click **Next**.

Figure 3-6: License Agreement Window



Please read the following license agreement. To continue with setup, you must accept the agreement.

SERVICE PACK 2 FOR MICROSOFT WINDOWS SERVER 2003

PLEASE NOTE:

For supplement obtained from server manufacturer or software installer. The server manufacturer, or the software installer, that distributes the software with

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 facing 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.

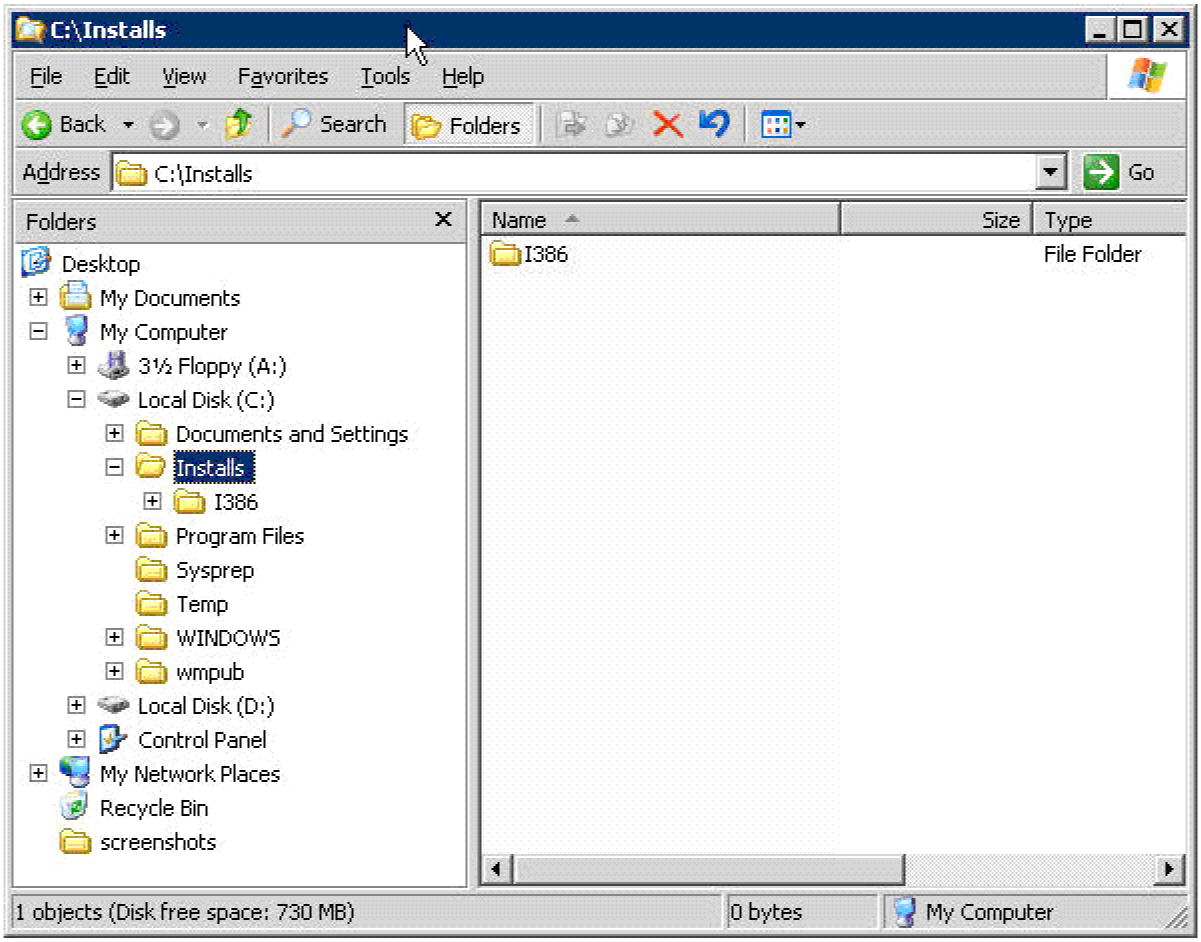
Moving Unused Files - NiceLog Loggers

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



Name	Size	Type
I386		File Folder

1 objects (Disk free space: 730 MB) | 0 bytes | My Computer

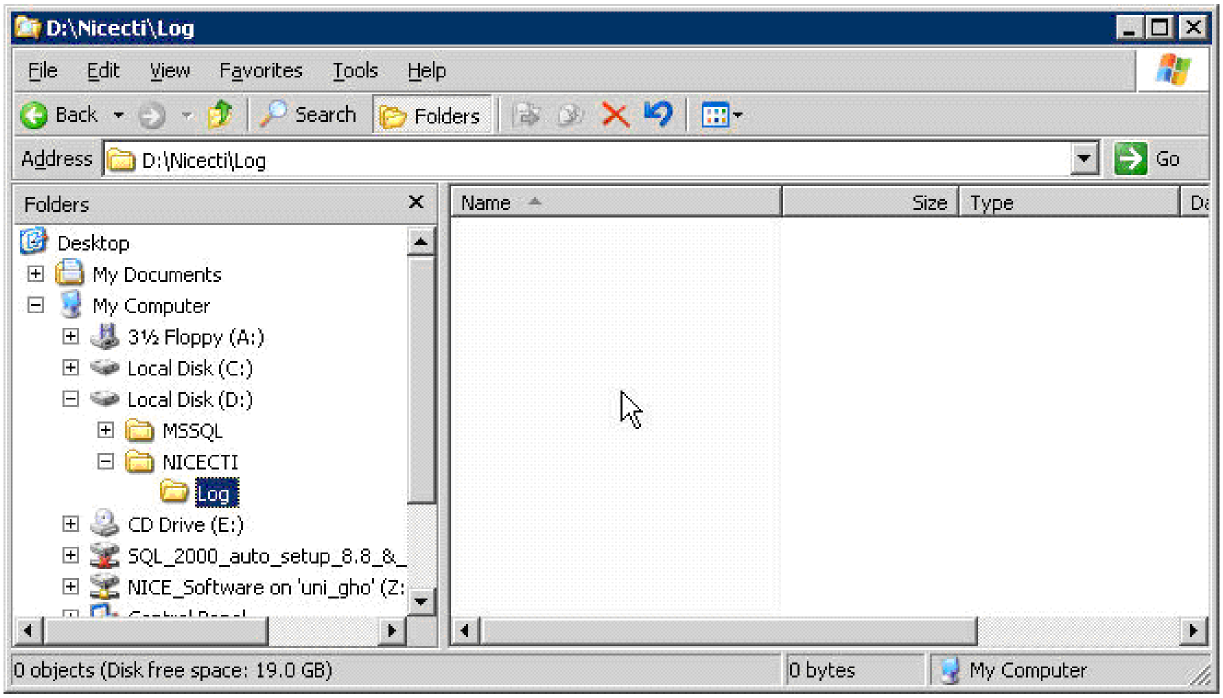
Moving Log Files - NiceCLS Servers

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



Address D:\Nicecti\Log

0 objects (Disk free space: 19.0 GB)

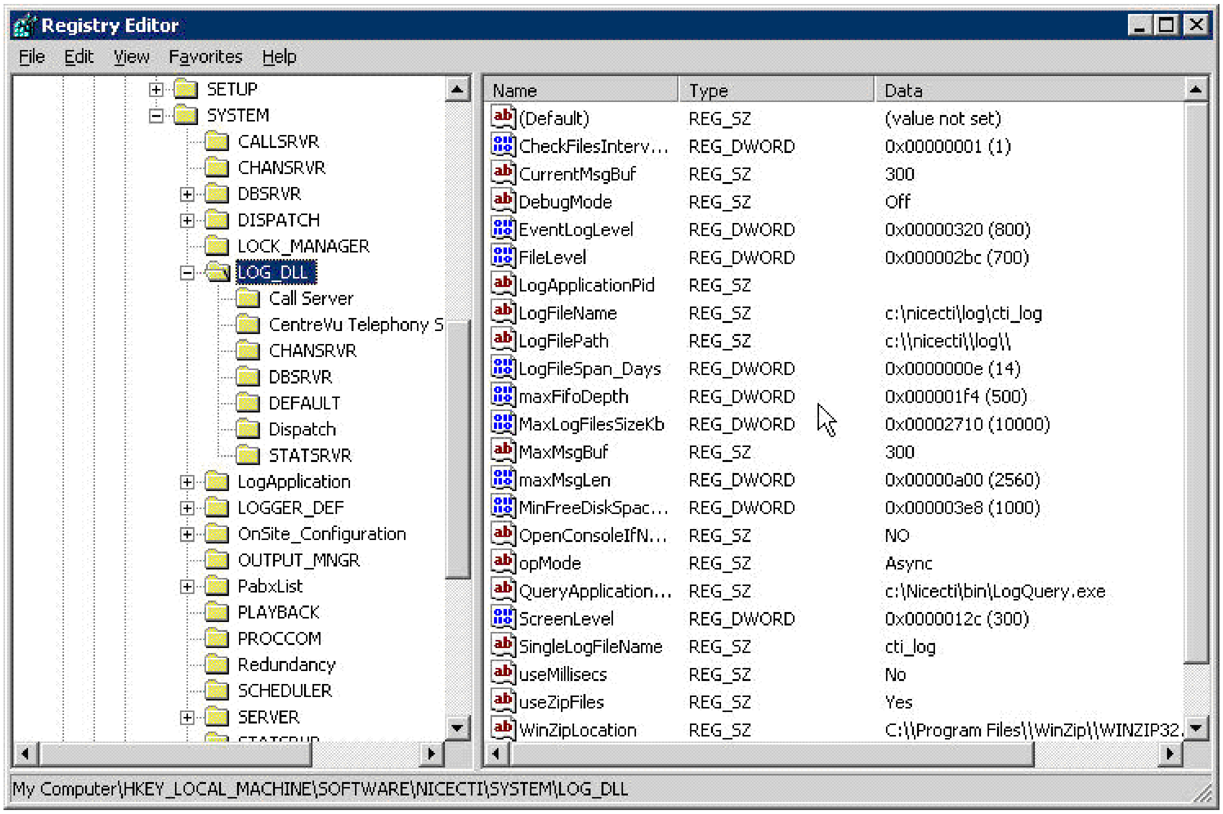
0 bytes

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

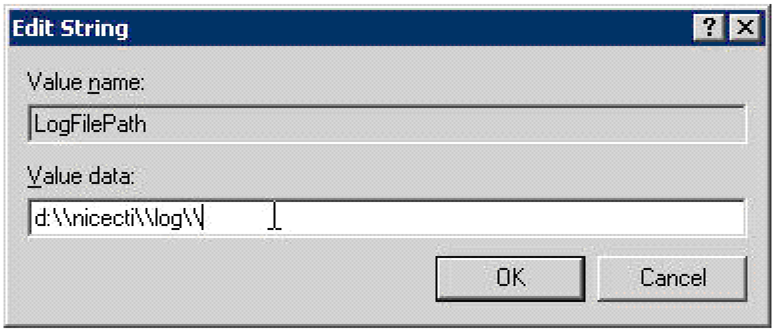


Name	Type	Data
(Default)	REG_SZ	(value not set)
CheckFilesInterv...	REG_DWORD	0x00000001 (1)
CurrentMsgBuf	REG_SZ	300
DebugMode	REG_SZ	Off
EventLogLevel	REG_DWORD	0x00000320 (800)
FileLevel	REG_DWORD	0x000002bc (700)
LogApplicationPid	REG_SZ	
LogFileName	REG_SZ	c:\nicecti\log\cti_log
LogFilePath	REG_SZ	c:\\nicecti\\log\\
LogFileSpan_Days	REG_DWORD	0x0000000e (14)
maxFifoDepth	REG_DWORD	0x000001f4 (500)
MaxLogFilesSizeKb	REG_DWORD	0x00002710 (10000)
MaxMsgBuf	REG_SZ	300
maxMsgLen	REG_DWORD	0x00000a00 (2560)
MinFreeDiskSpac...	REG_DWORD	0x000003e8 (1000)
OpenConsoleIfN...	REG_SZ	NO
opMode	REG_SZ	Async
QueryApplication...	REG_SZ	c:\Nicecti\bin\LogQuery.exe
ScreenLevel	REG_DWORD	0x0000012c (300)
SingleLogFileName	REG_SZ	cti_log
useMillisecs	REG_SZ	No
useZipFiles	REG_SZ	Yes
WinZipLocation	REG_SZ	C:\\Program Files\\WinZip\\WINZIP32.

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\NICECTI\SYSTEM\LOG_DLL

4. Set the value of LogFilePath as shown below:

Figure 3-10: LogFilePath



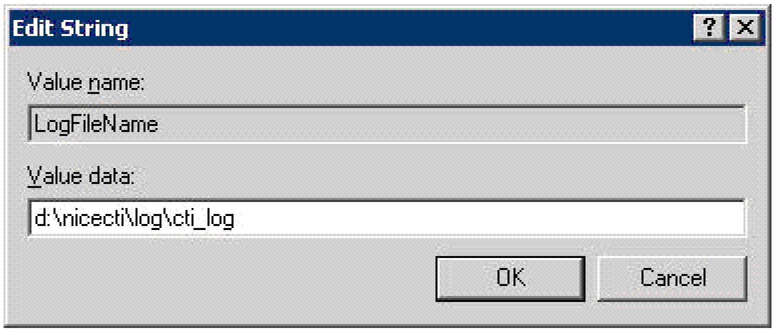
Value name: LogFilePath

Value data: d:\\nicecti\\log\\

5. Click **OK**.

6. Set the value of LogFileName as shown below:

Figure 3-11: LogFileName



Value name: LogFileName

Value data: d:\nicecti\log\cti_log

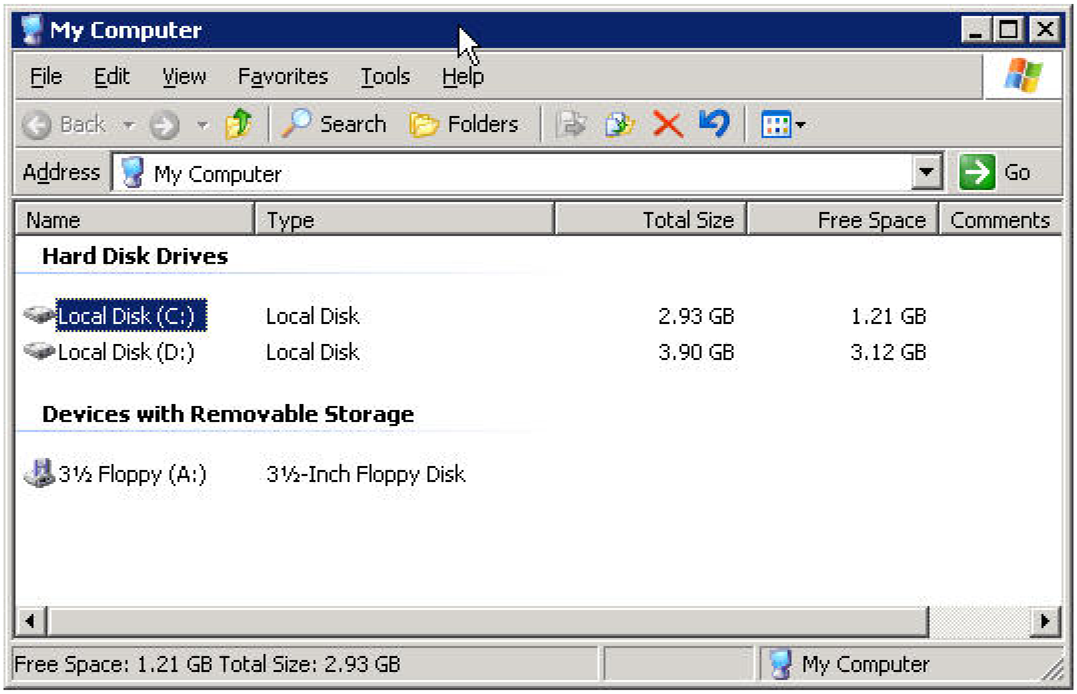
7. Click **OK**.

Running the Disk Cleanup Wizard

To run the Disk Cleanup wizard:

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

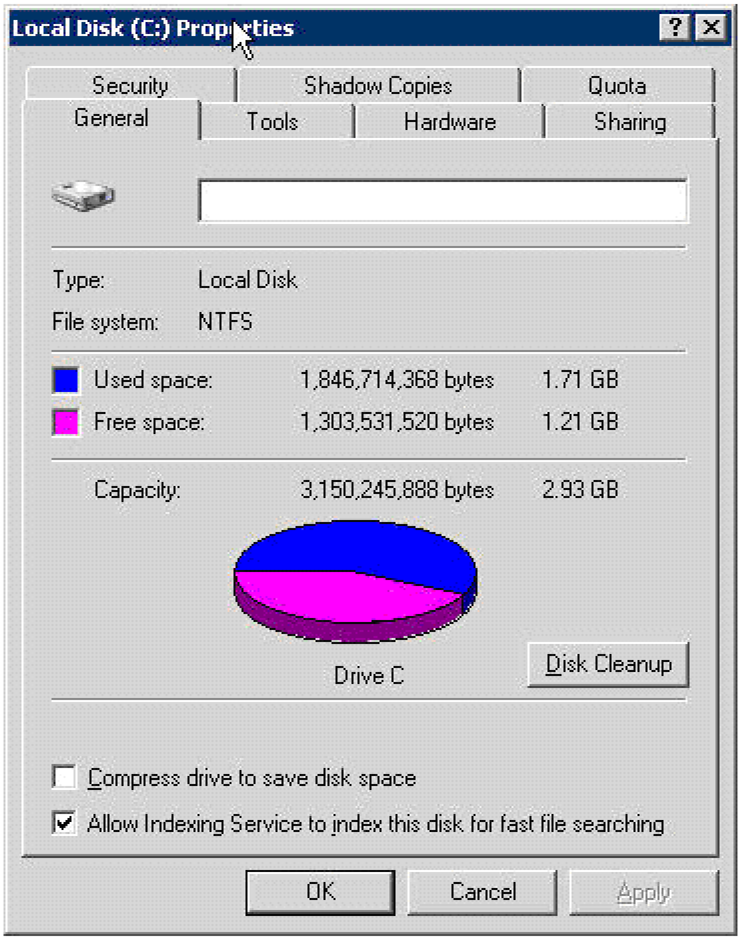


Address: My Computer

Name	Type	Total Size	Free Space	Comments
Hard Disk Drives				
Local Disk (C:)	Local Disk	2.93 GB	1.21 GB	
Local Disk (D:)	Local Disk	3.90 GB	3.12 GB	
Devices with Removable Storage				
3½ Floppy (A:)	3½-Inch Floppy Disk			

Free Space: 1.21 GB Total Size: 2.93 GB | My Computer

Figure 3-13: Local Disk (C): Properties Window



Type: Local Disk

File system: NTFS

🟦 Used space: 1,846,714,368 bytes 1.71 GB

🟪 Free space: 1,303,531,520 bytes 1.21 GB

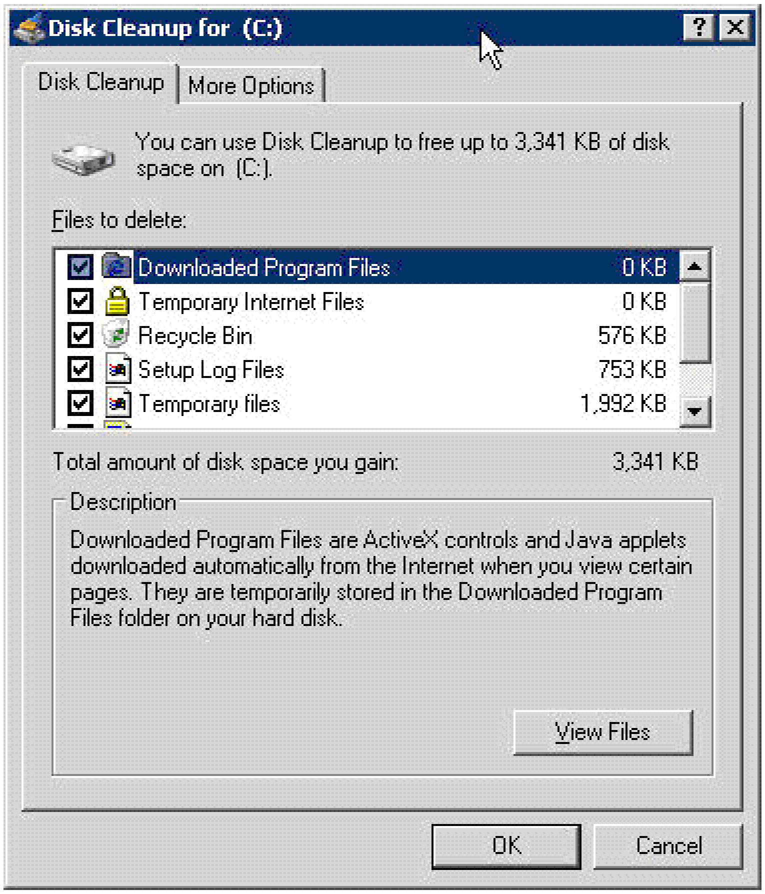
Capacity: 3,150,245,888 bytes 2.93 GB

□ Compress drive to save disk space

☑ Allow Indexing Service to index this disk for fast file searching

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



You can use Disk Cleanup to free up to 3,341 KB of disk space on (C:).

Files to delete:

☑	Downloaded Program Files	0 KB
☑	Temporary Internet Files	0 KB
☑	Recycle Bin	576 KB
☑	Setup Log Files	753 KB
☑	Temporary files	1,992 KB

Total amount of disk space you gain: 3,341 KB

Description

Downloaded Program Files are ActiveX controls and Java applets downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.

4. Click **OK**. Disk Cleanup will clean all the selected files.

Copying the Service Pack 1 Installation File

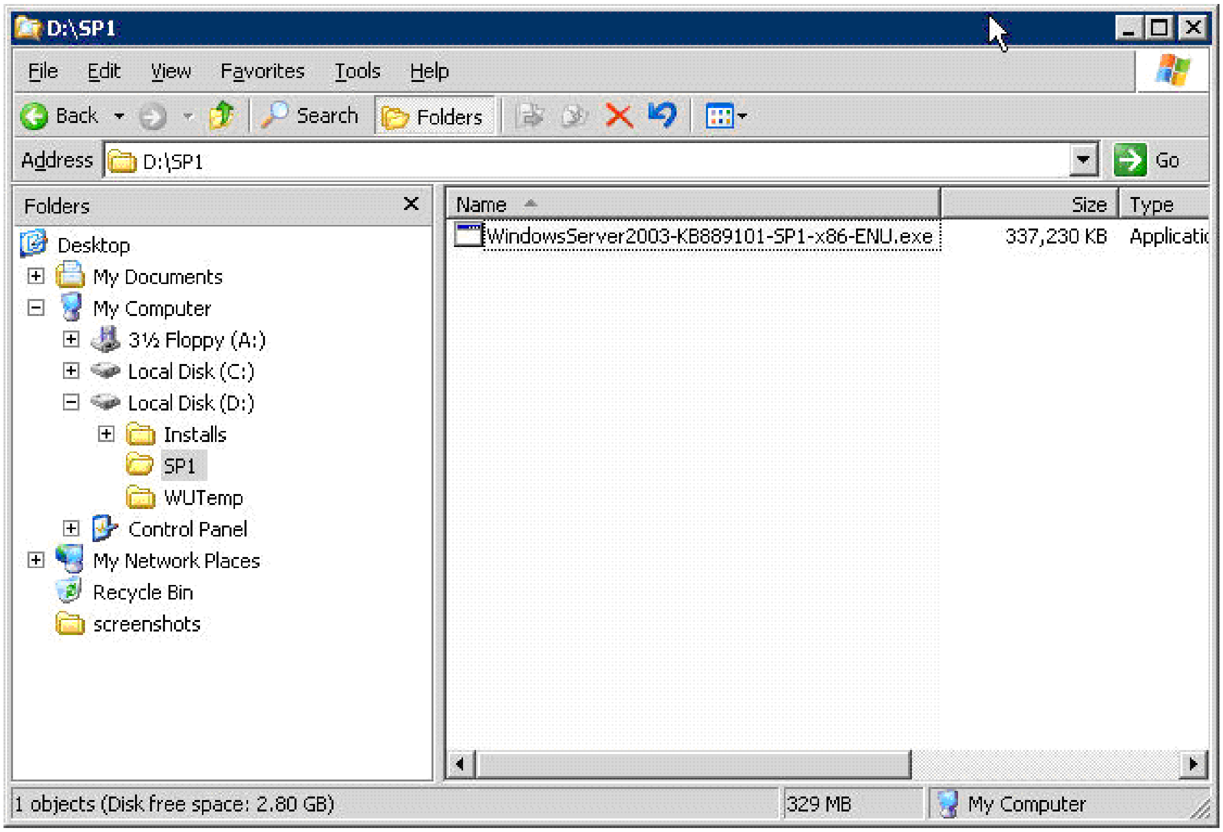
IMPORTANT

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.

Figure 3-15: :\SP1 Folder

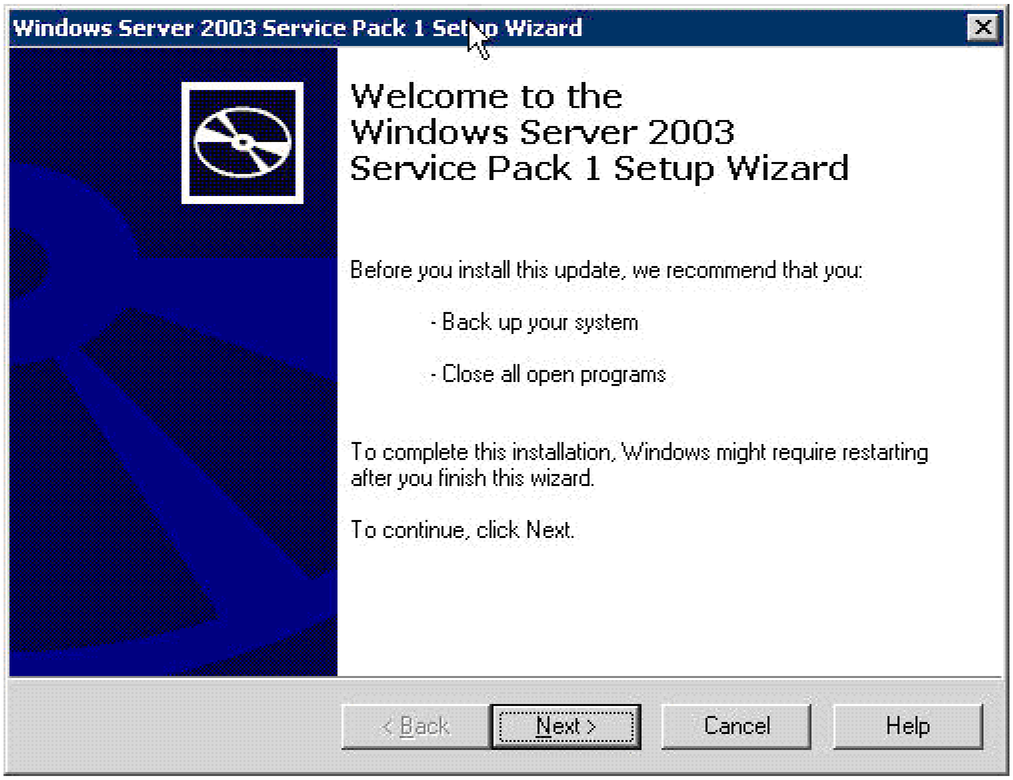


Running the Microsoft Windows Server 2003 Service Pack 1 Setup

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



Windows Server 2003 Service Pack 1 Setup Wizard

Welcome to the Windows Server 2003 Service Pack 1 Setup Wizard

Before you install this update, we recommend that you:

- Back up your system

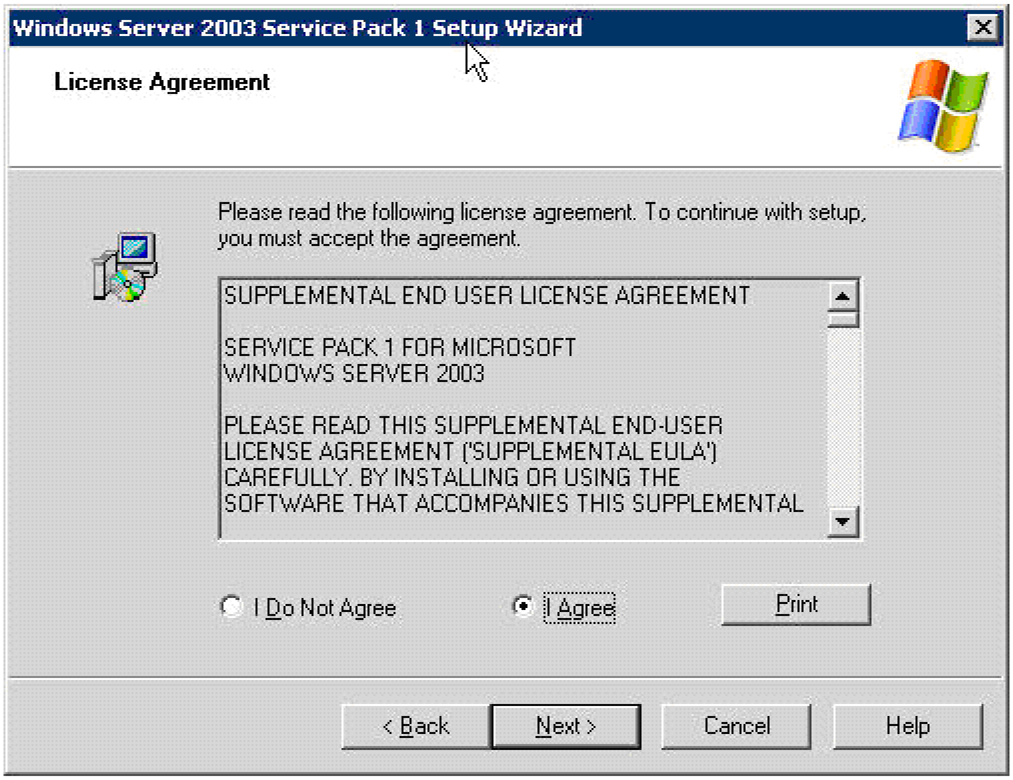
- Close all open programs

To complete this installation, Windows might require restarting after you finish this wizard.

To continue, click Next.

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

Figure 3-17: Windows Server 2003 Service Pack 1 Setup Wizard - License Agreement



Windows Server 2003 Service Pack 1 Setup Wizard

License Agreement

Please read the following license agreement. To continue with setup, you must accept the agreement.

SUPPLEMENTAL END USER LICENSE AGREEMENT

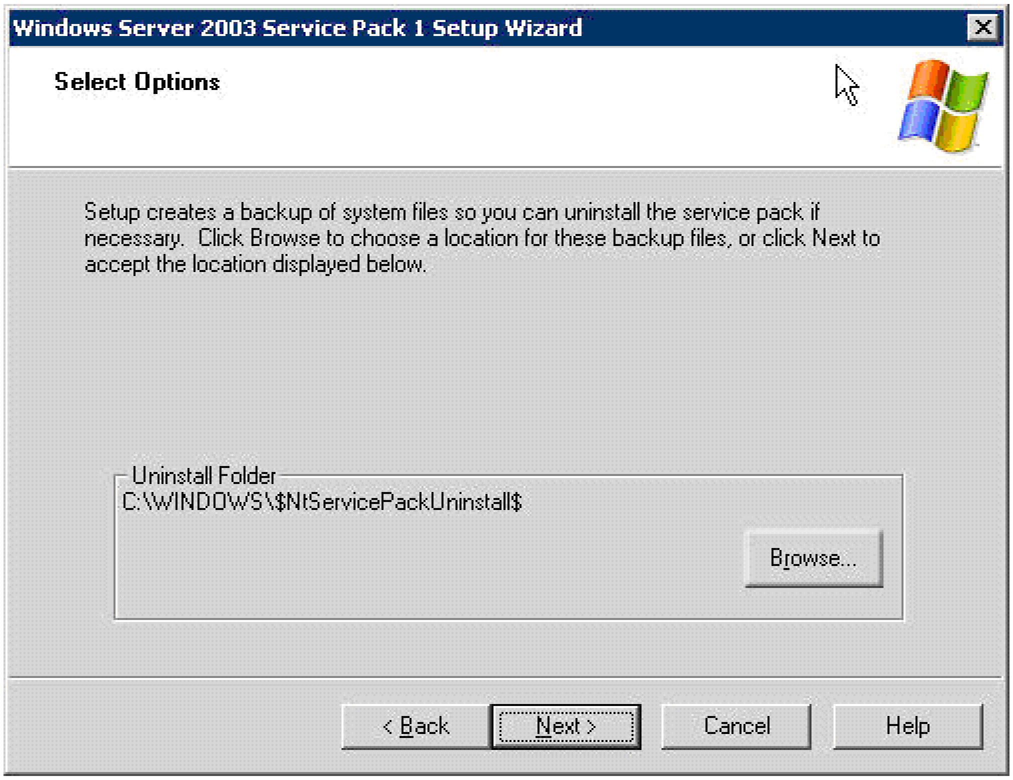
SERVICE PACK 1 FOR MICROSOFT
WINDOWS SERVER 2003

PLEASE READ THIS SUPPLEMENTAL END-USER LICENSE AGREEMENT ('SUPPLEMENTAL EULA') CAREFULLY. BY INSTALLING OR USING THE SOFTWARE THAT ACCOMPANIES THIS SUPPLEMENTAL

○ I Do Not Agree ● I Agree

3. Select **I Agree** and click **Next**. The Windows Select Options window appears.

Figure 3-18: Select Options Window



Windows Server 2003 Service Pack 1 Setup Wizard

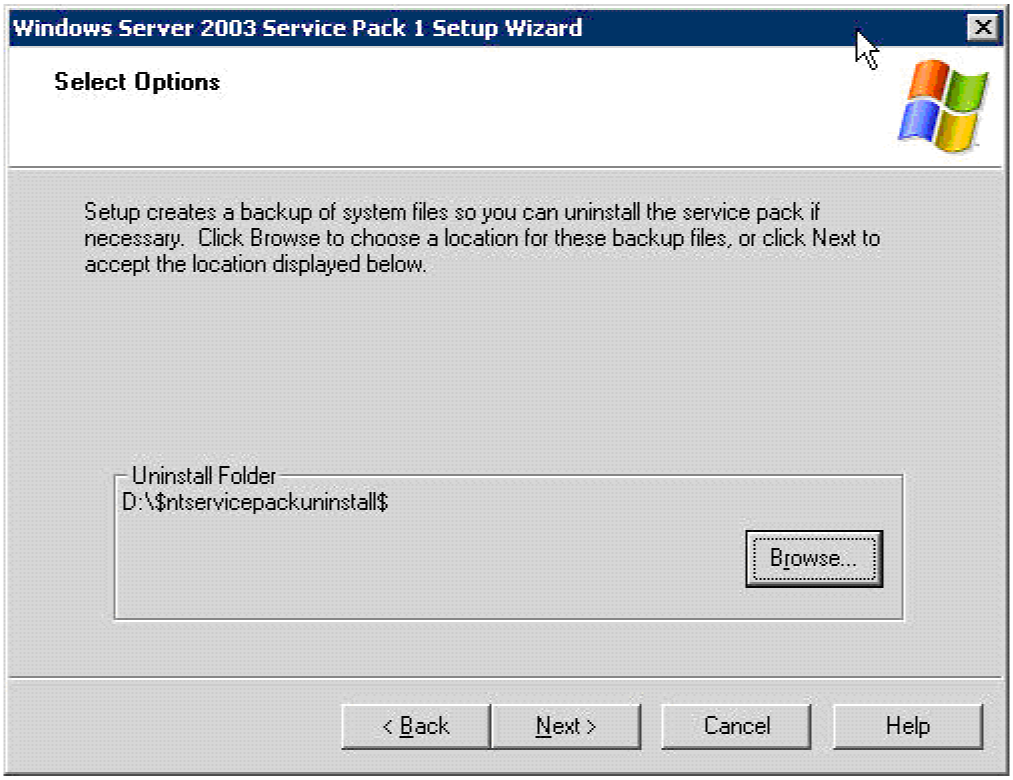
Select Options

Setup creates a backup of system files so you can uninstall the service pack if necessary. Click Browse to choose a location for these backup files, or click Next to accept the location displayed below.

Uninstall Folder
C:\WINDOWS\$NtServicePackUninstall$

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



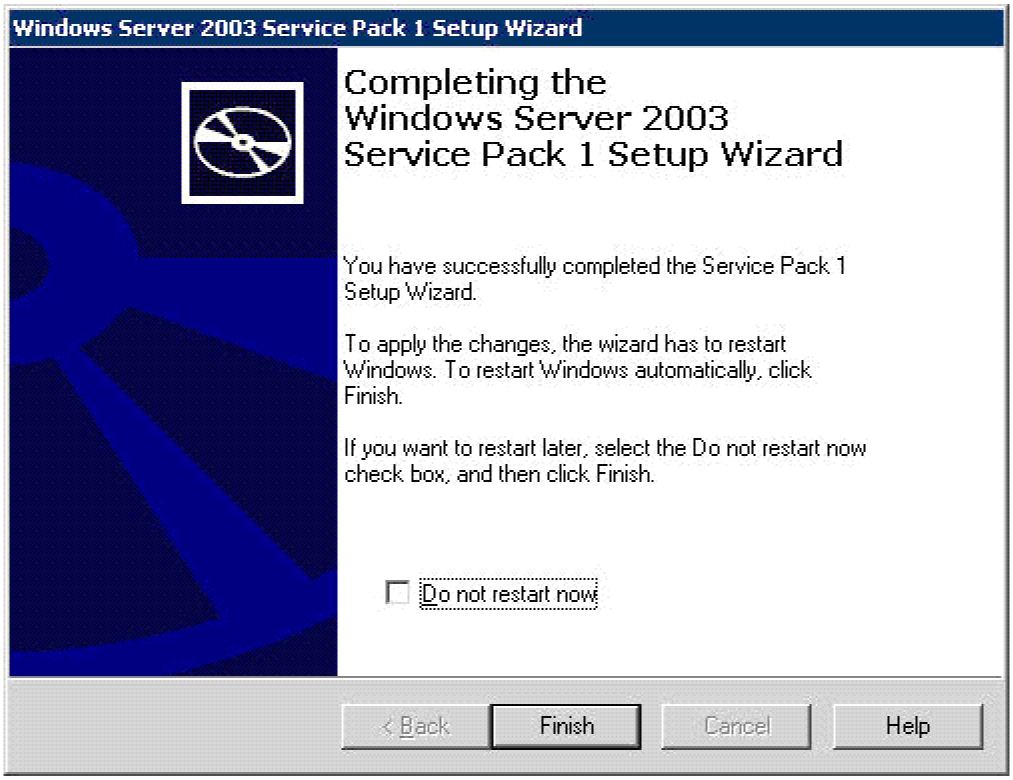
Setup creates a backup of system files so you can uninstall the service pack if necessary. Click Browse to choose a location for these backup files, or click Next to accept the location displayed below.

Uninstall Folder
D:\$ntservicepackuninstall$

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



Windows Server 2003 Service Pack 1 Setup Wizard

Completing the Windows Server 2003 Service Pack 1 Setup Wizard

You have successfully completed the Service Pack 1 Setup Wizard.

To apply the changes, the wizard has to restart Windows. To restart Windows automatically, click Finish.

If you want to restart later, select the Do not restart now check box, and then click Finish.

□ Do not restart now

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 on the facing page.
- Adding Applications to the Exceptions List on page 58.
- Activating the Windows Firewall on page 59.

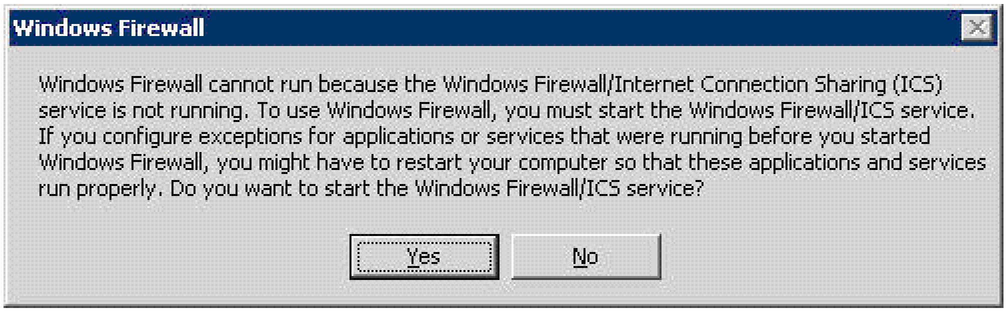
Enabling the Windows Firewall Service

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



Windows Firewall

Windows Firewall cannot run because the Windows Firewall/Internet Connection Sharing (ICS) service is not running. To use Windows Firewall, you must start the Windows Firewall/ICS service. If you configure exceptions for applications or services that were running before you started Windows Firewall, you might have to restart your computer so that these applications and services run properly. Do you want to start the Windows Firewall/ICS service?

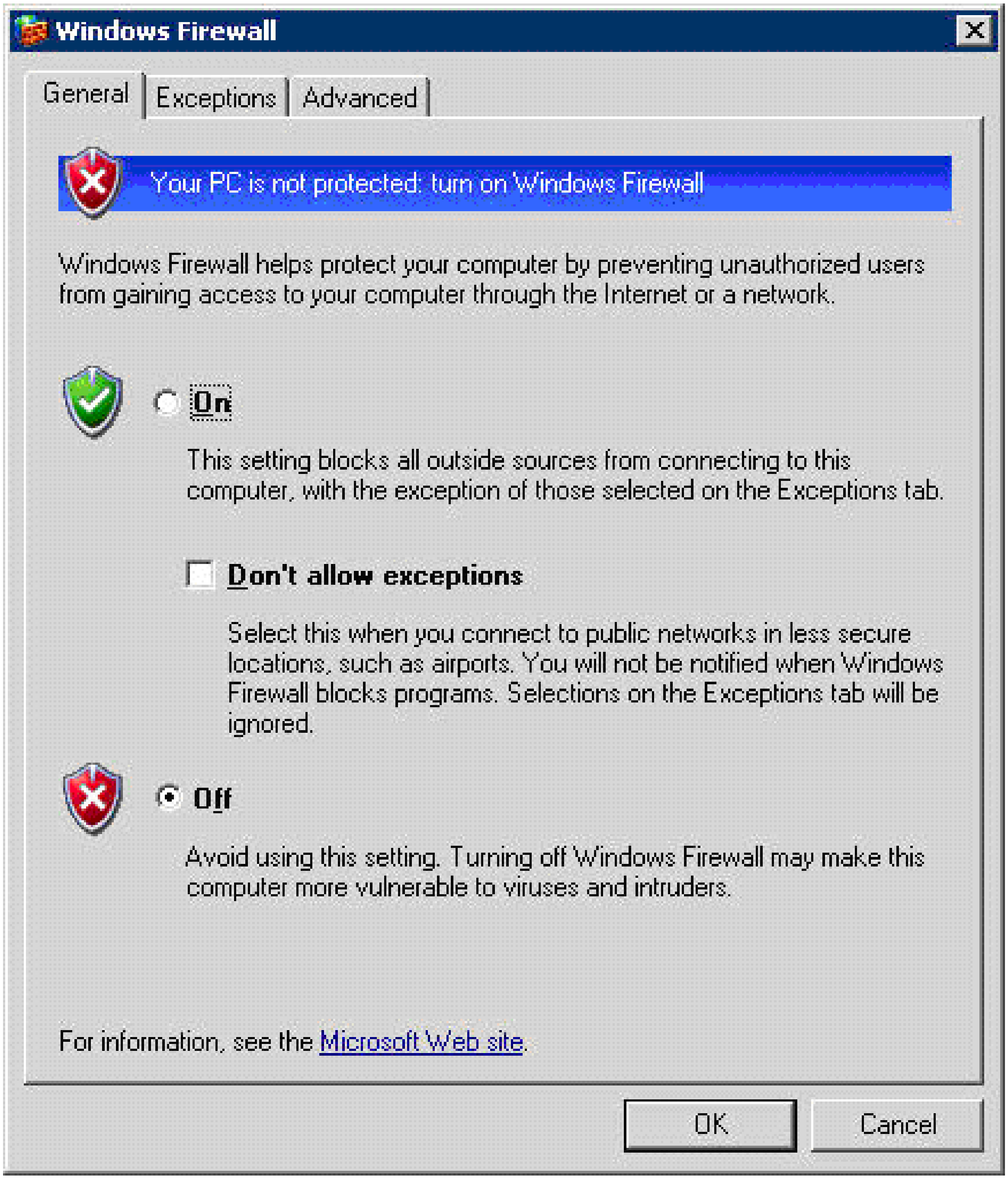
2. Click **Yes** and close the Windows Firewall application. The Windows Firewall service is now enabled, however, the Windows Firewall is not active yet.

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



Your PC is not protected: turn on Windows Firewall

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

○ On

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

● Off

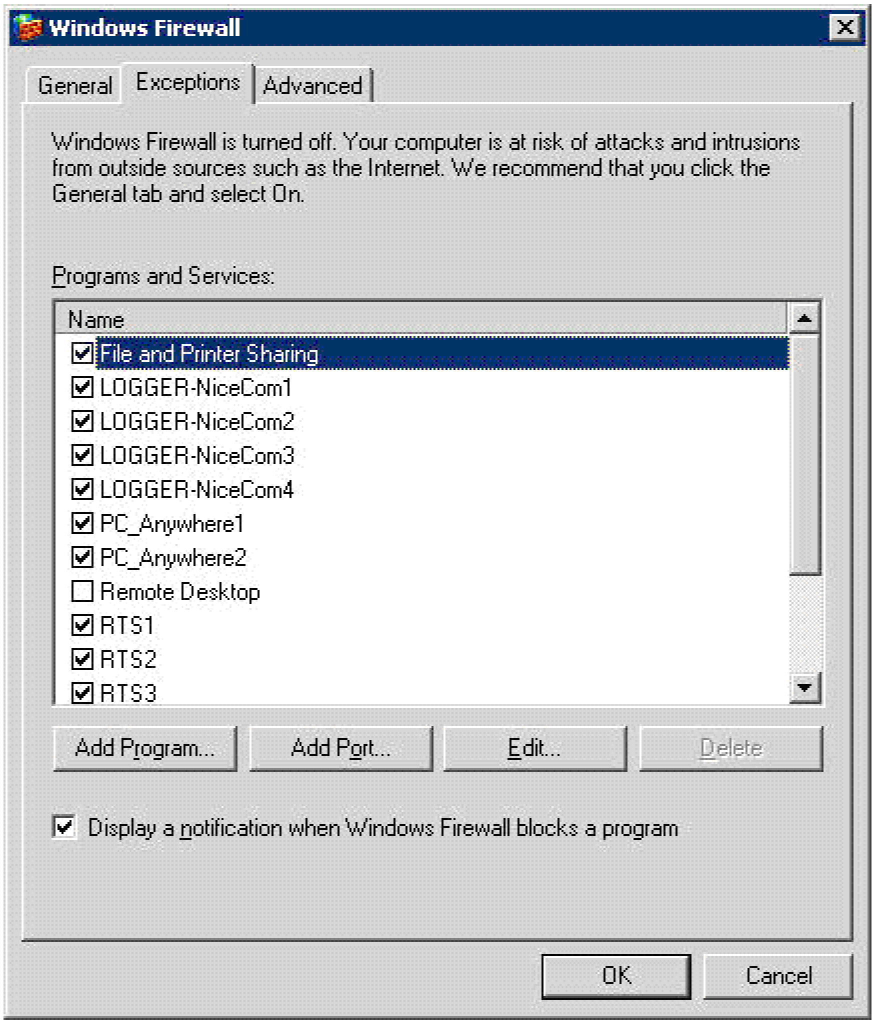
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

For information, see the Microsoft Web site.

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



Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.

Programs and Services:

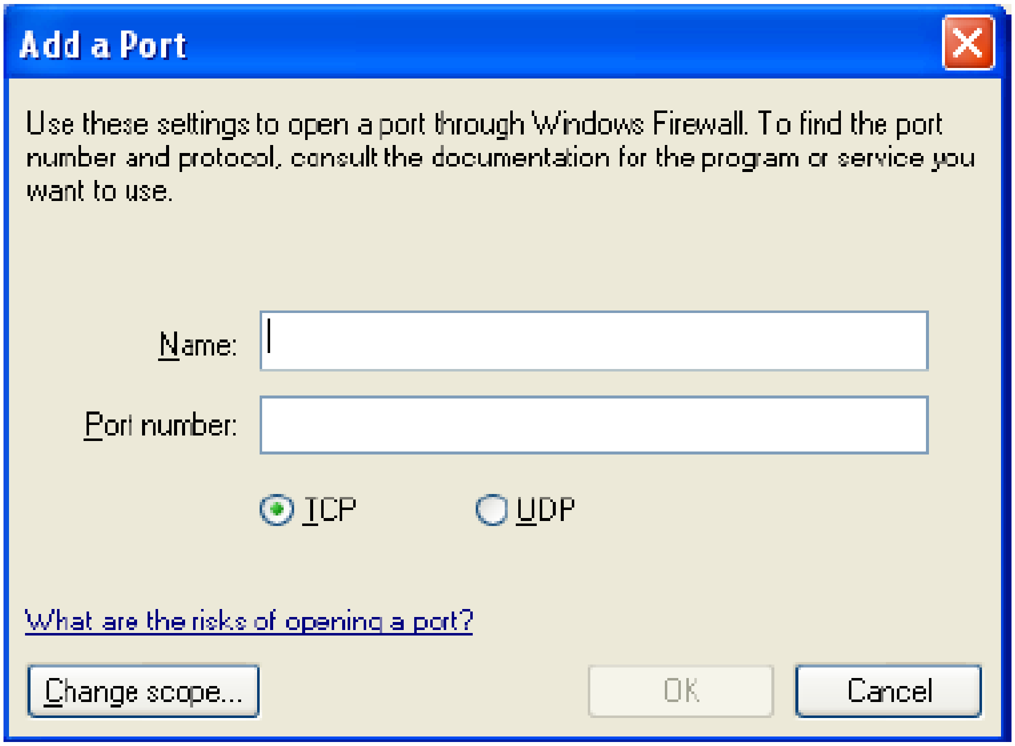
Name
☑ File and Printer Sharing
☑ LOGGER-NiceCom1
☑ LOGGER-NiceCom2
☑ LOGGER-NiceCom3
☑ LOGGER-NiceCom4
☑ PC_Anywhere1
☑ PC_Anywhere2
□ Remote Desktop
☑ RTS1
☑ RTS2
☑ RTS3

☑ Display a notification when Windows Firewall blocks a program

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



Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name:

Port number:

● TCP ○ UDP

4. Referring to Network Usage by NICE Systems on page 60, add the port and click **OK**. Repeat this step for all NICE ports.

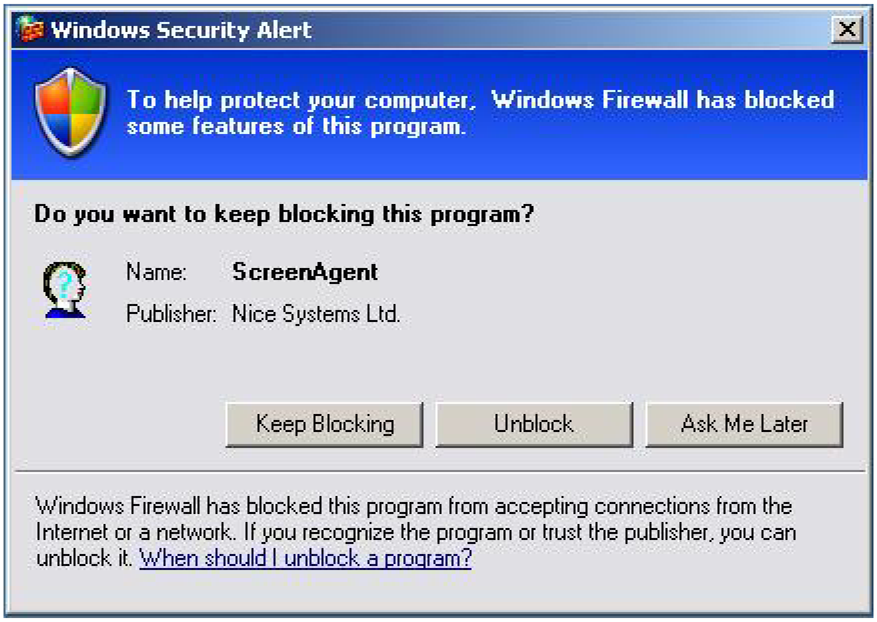
Adding Applications to the Exceptions List

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)



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: ScreenAgent

Publisher: Nice Systems Ltd.

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

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

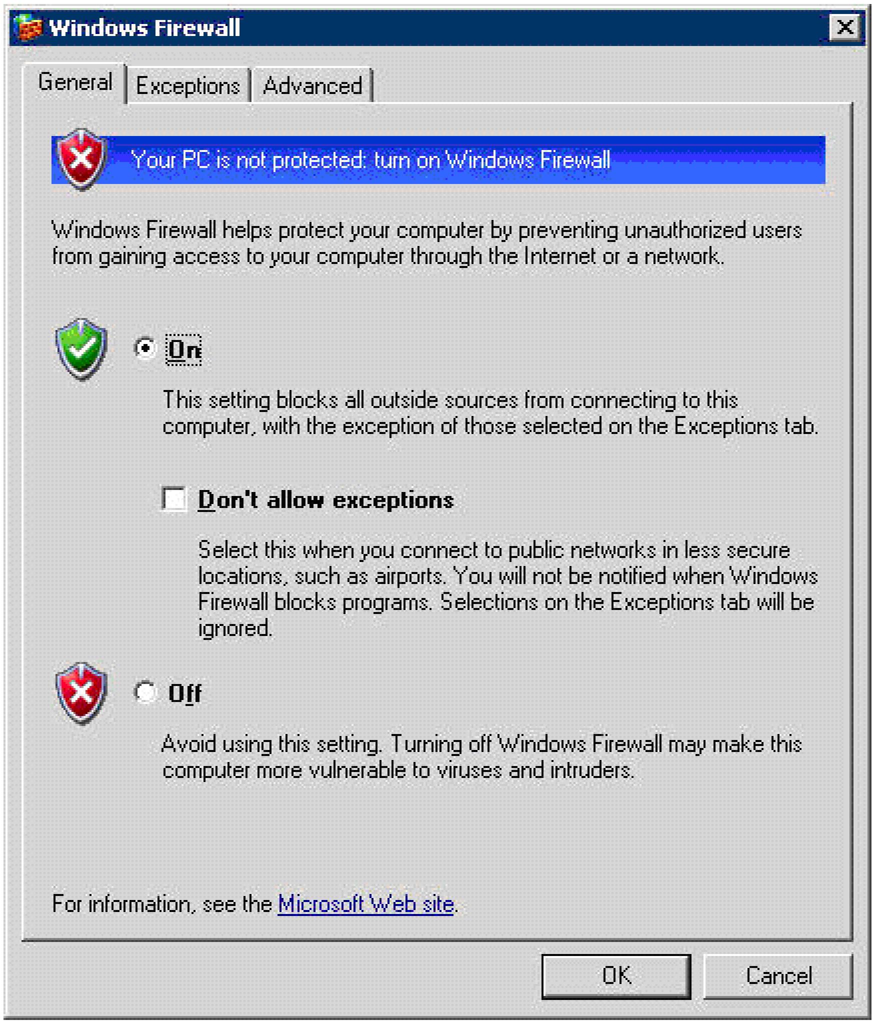
Activating the Windows Firewall

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



Your PC is not protected: turn on Windows Firewall

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ Off

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

For information, see the Microsoft Web site.

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	

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

Port in 9.0	Used By	Comments
62071	Audit Trail	
62072	Rule Manager	
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	
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

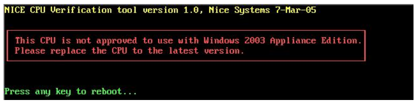
From April 2005, an Image CD (Ghost) will be shipped with each NICE High Density Logger, NICE Interaction Capture Unit or Nicelog version 8.9 ISA, instead of Microsoft Windows Server 2003 installation CDs.

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



```
NICE CPU Verification tool version 1.0, Nice Systems 7-Mar-05

 This CPU is not approved to use with Windows 2003 Appliance Edition.
 Please replace the CPU to the latest version.

Press any key to reboot...
```

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 next page.
- Installing the Image CD (Ghost) from a Workstation on page 76.

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

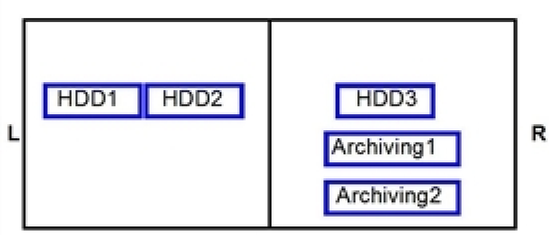
Platform	Preloaded HDD
NICE High Density Logger v9.0	36GB or 72GB SCSI HDD
NICE Interaction Capture Unit	250GB IDE HDD
NiceLog Logger ISA 8.9	36GB or 72GB SCSI HDD

- 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.

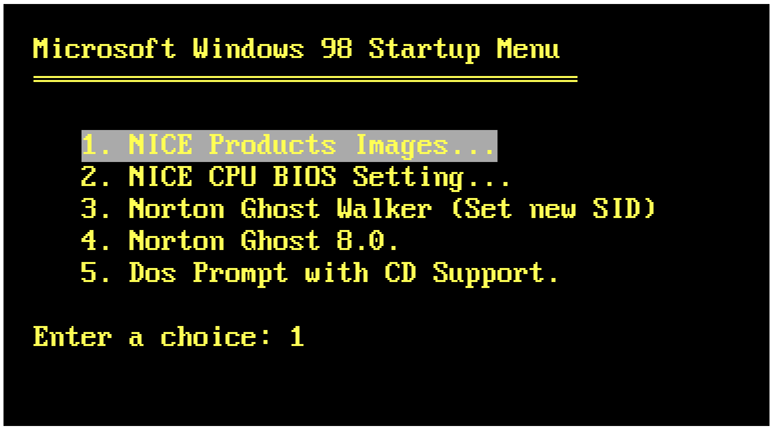
Installing the Image CD (Ghost) from a Logger DVD Device

> **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



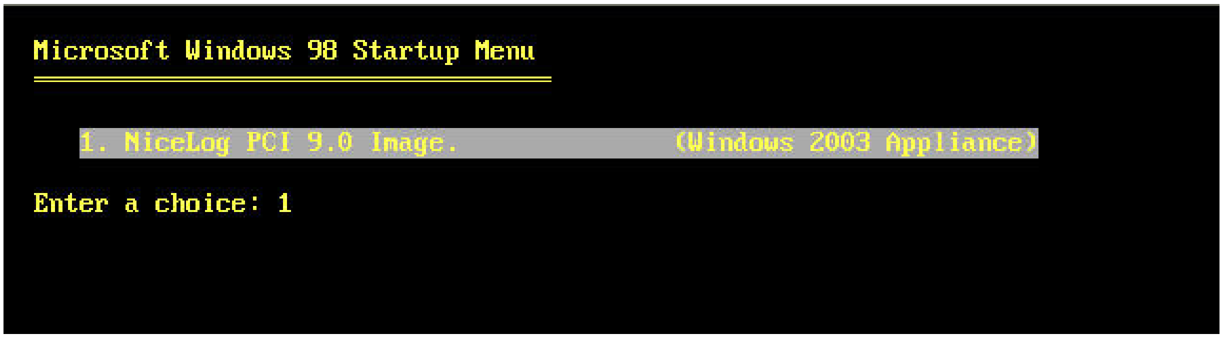
```
Microsoft Windows 98 Startup Menu
=================================

    1. NICE Products Images...
    2. NICE CPU BIOS Setting...
    3. Norton Ghost Walker (Set new SID)
    4. Norton Ghost 8.0.
    5. Dos Prompt with CD Support.

Enter a choice: 1
```

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



```
Microsoft Windows 98 Startup Menu
=================================

    1. NiceLog PCI 9.0 Image.              (Windows 2003 Appliance)

Enter a choice: 1
```

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)].

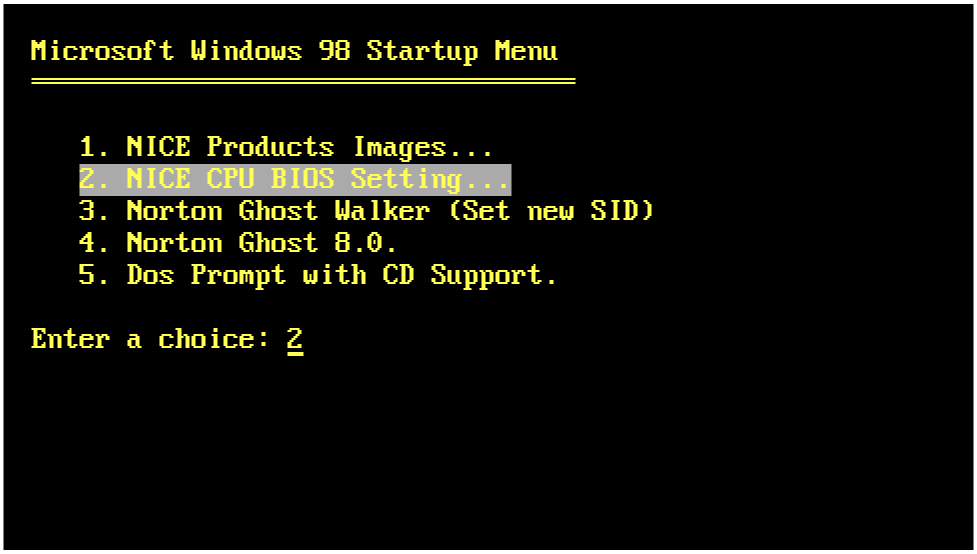
8. Select **OK** with the arrow buttons and press **Enter**.

➡ 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.**

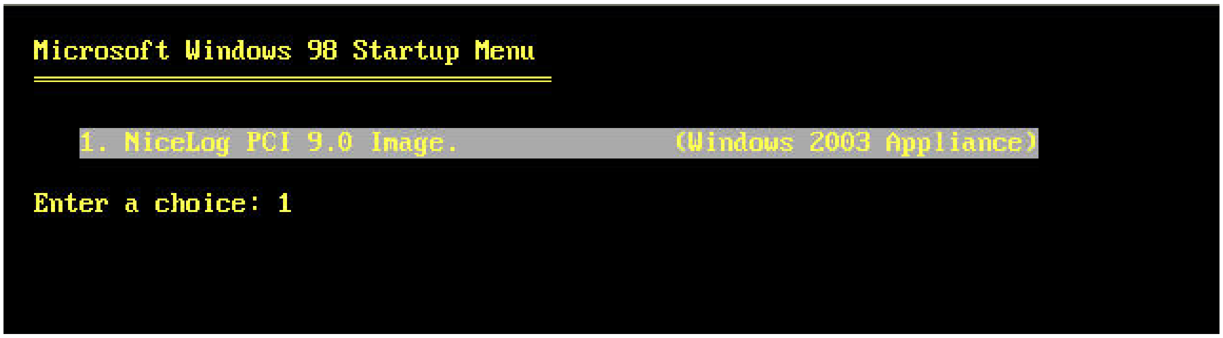
Figure 3-30: Microsoft Windows 98 Startup Menu



```
Microsoft Windows 98 Startup Menu
═════════════════════════════════

   1. NICE Products Images...
   2. NICE CPU BIOS Setting...
   3. Norton Ghost Walker (Set new SID)
   4. Norton Ghost 8.0.
   5. Dos Prompt with CD Support.

Enter a choice: 2
```

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



```
Microsoft Windows 98 Startup Menu
═════════════════════════════════

   1. NiceLog PCI 9.0 Image.              (Windows 2003 Appliance)

Enter a choice: 1
```

NICE S/W Installation

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

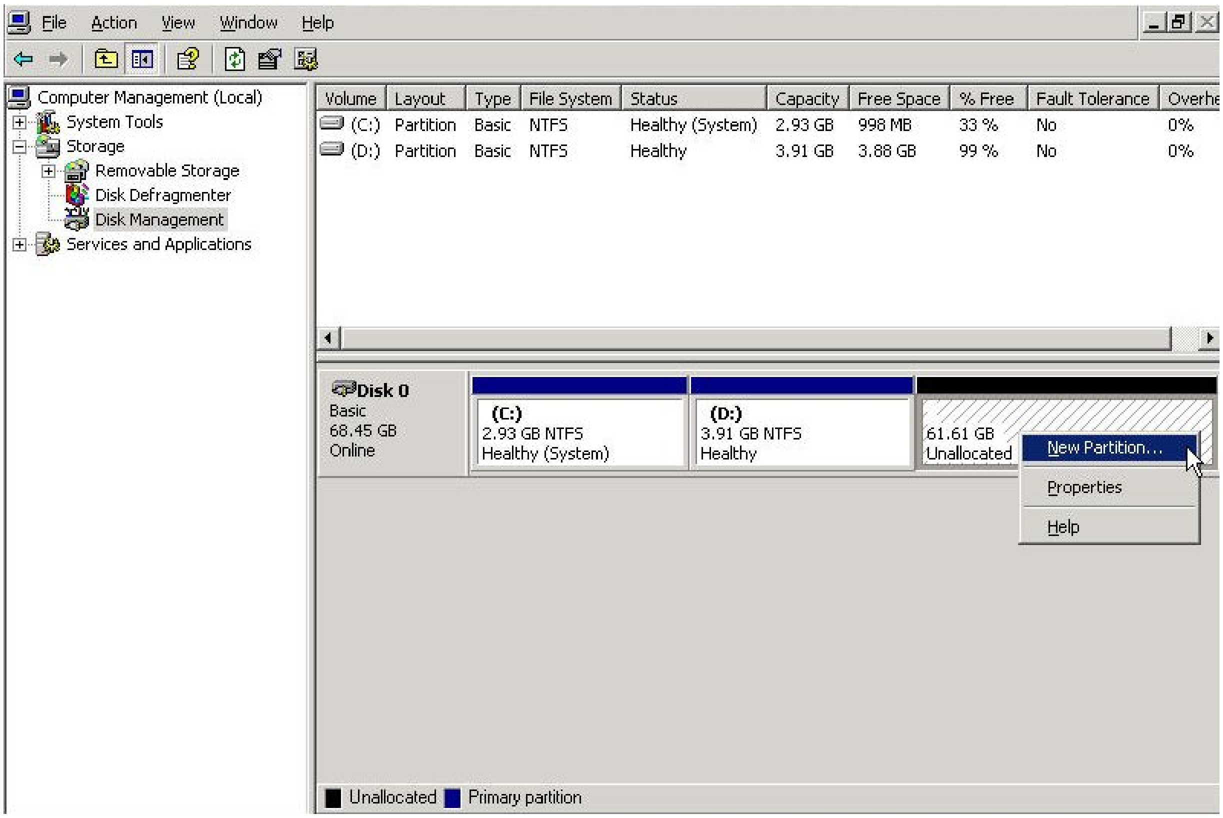
You must create the **E** partition on the HDD accordingly.

➡ 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.

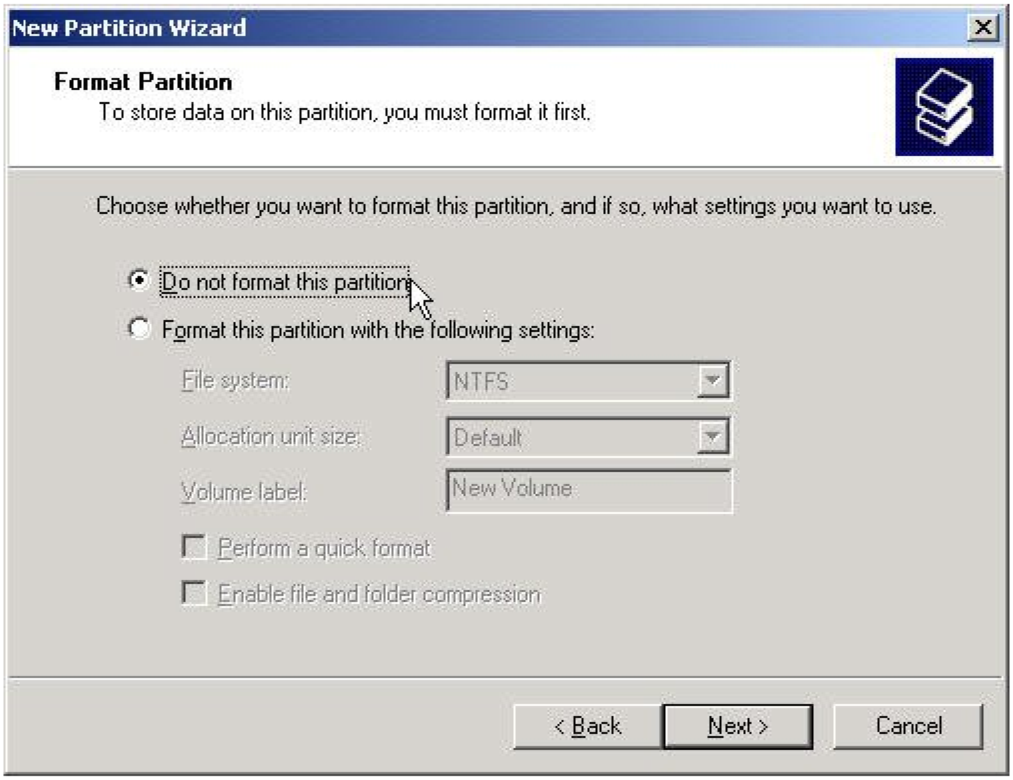
Figure 3-32: Disk Management



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhe
(C:)	Partition	Basic	NTFS	Healthy (System)	2.93 GB	998 MB	33 %	No	0%
(D:)	Partition	Basic	NTFS	Healthy	3.91 GB	3.88 GB	99 %	No	0%

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



New Partition Wizard

Format Partition

To store data on this partition, you must format it first.

Choose whether you want to format this partition, and if so, what settings you want to use.

● Do not format this partition

○ Format this partition with the following settings:

File system: NTFS

Allocation unit size: Default

Volume label: New Volume

□ Perform a quick format

□ Enable file and folder compression

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.

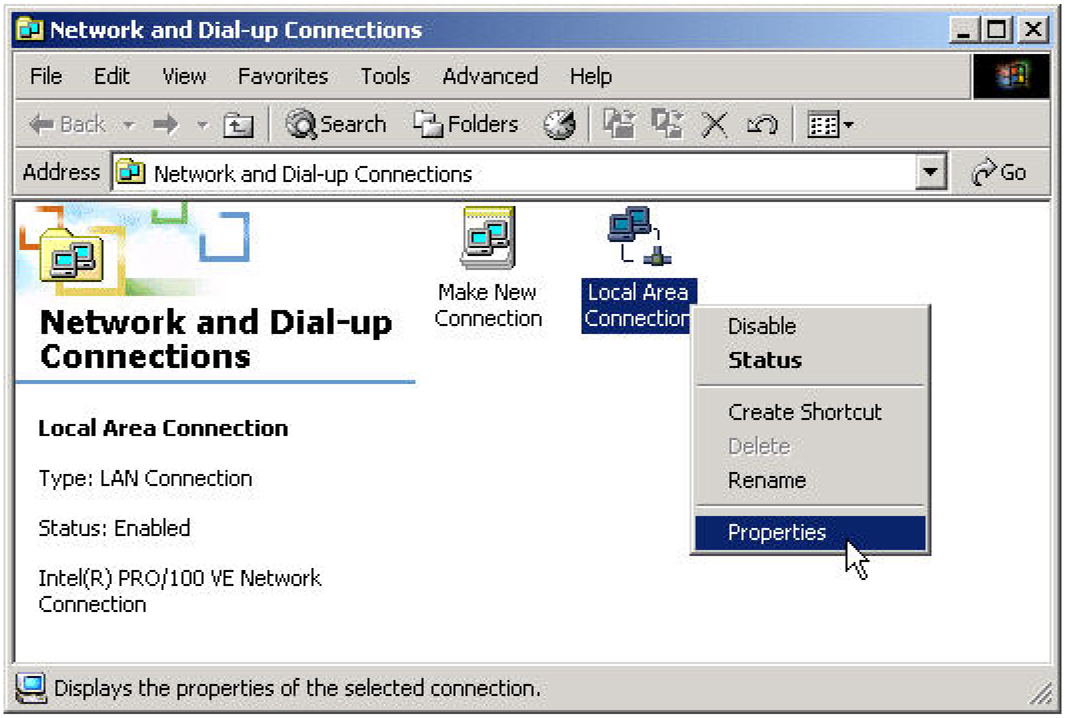
Installing the Image CD (Ghost) from a Workstation

> **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


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network and Dial-up Connections
Go
Network and Dial-up Connections
Make New Connection
Local Area Connection
Disable
Status
Create Shortcut
Delete
Rename
Properties

Local Area Connection

Type: LAN Connection

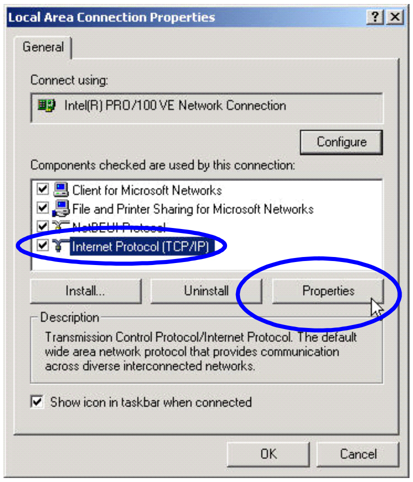
Status: Enabled

Intel(R) PRO/100 VE Network Connection

Displays the properties of the selected connection.

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



Connect using:

Intel(R) PRO/100 VE Network Connection

Components checked are used by this connection:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ NetBEUI Protocol
- ☑ Internet Protocol (TCP/IP)

Description

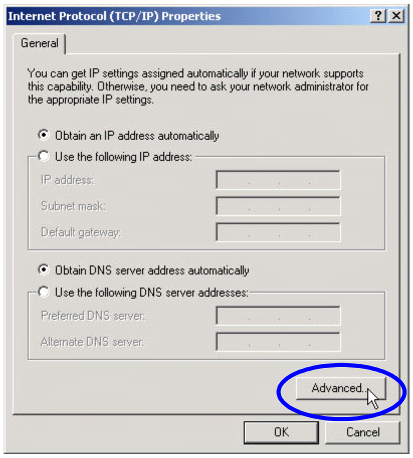
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

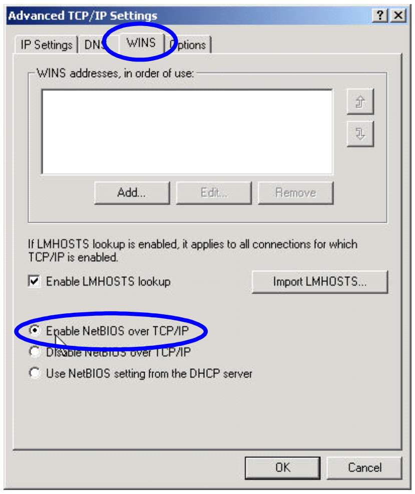
○ Use the following IP address:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

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



If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

● Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

○ Use NetBIOS setting from the DHCP server

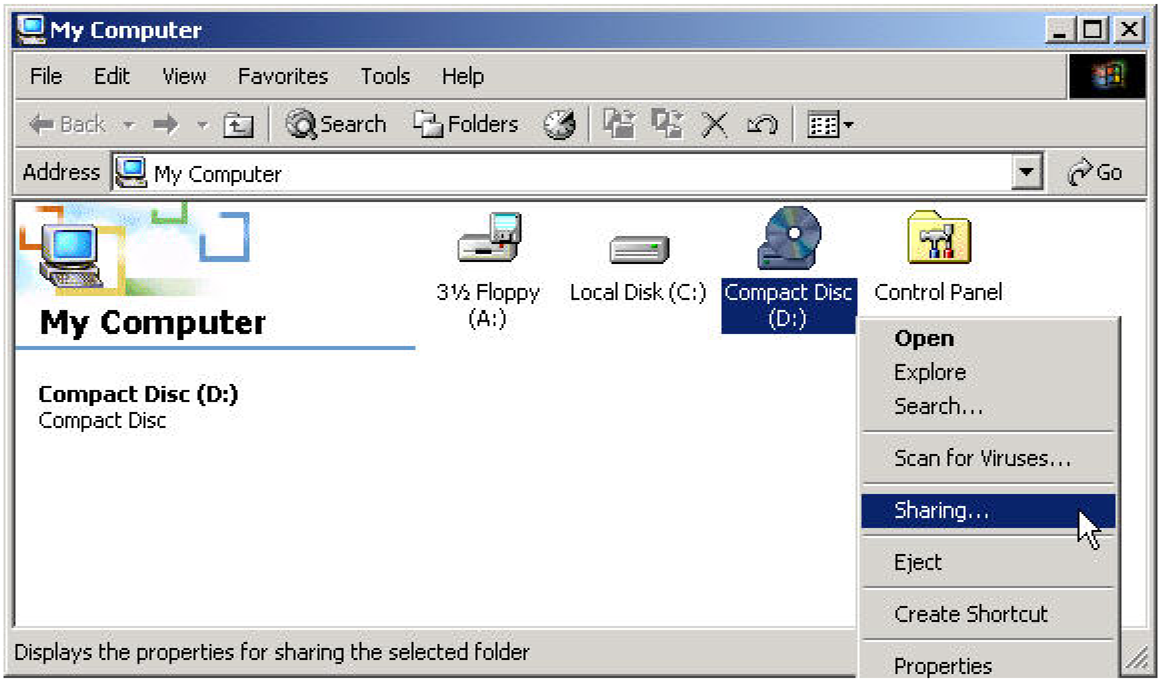
6. Close all open dialogs.

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...

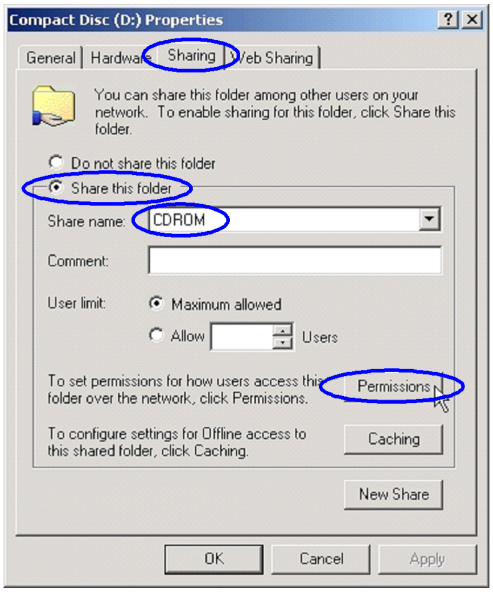


3. Click the **Sharing** tab, and select **Share this folder**.

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



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: CDROM

Comment:

User limit: ● Maximum allowed

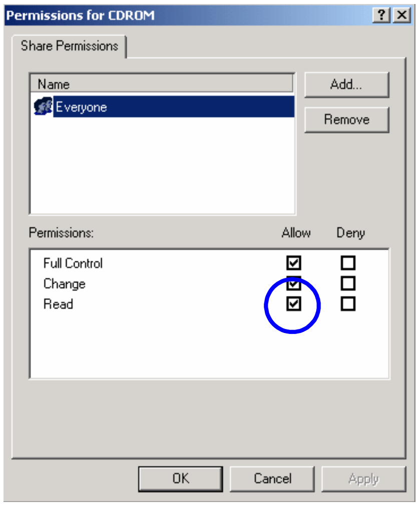
○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

6. From the **Permissions for CDROM** window, ensure that the **Everyone** group is defined with a **Read** permission.

Figure 3-40: Share Permissions Window



Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

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)

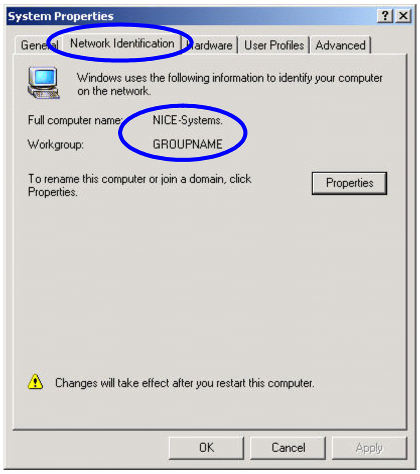
- Domain / Workgroup name (Up to 15 characters)___________________________(2)

  (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



Windows uses the following information to identify your computer on the network.

Full computer name: NICE-Systems.

Workgroup: GROUPNAME

To rename this computer or join a domain, click Properties.

Changes will take effect after you restart this computer.

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)

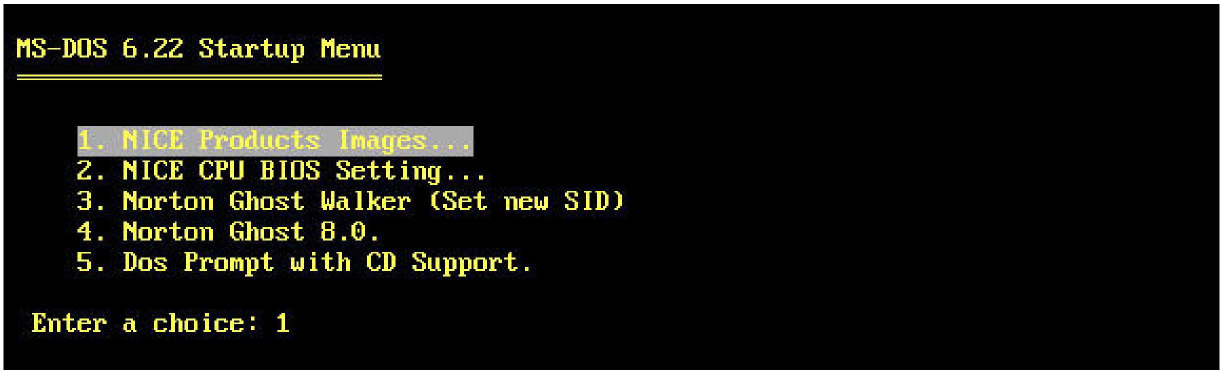
3. **Reboot** the Logger.

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.

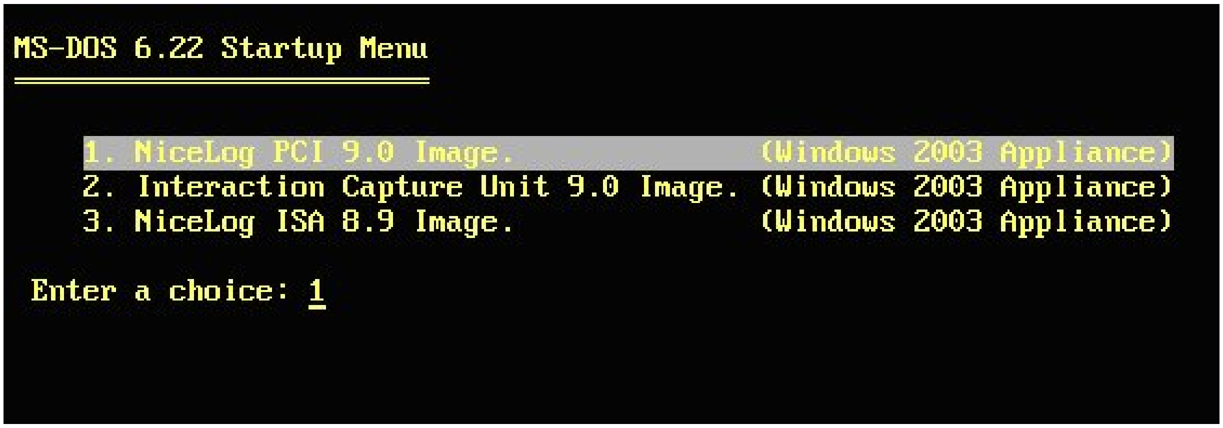
Figure 3-42: MS-DOS 6.22 Startup Menu



```
MS-DOS 6.22 Startup Menu
========================

    1. NICE Products Images...
    2. NICE CPU BIOS Setting...
    3. Norton Ghost Walker (Set new SID)
    4. Norton Ghost 8.0.
    5. Dos Prompt with CD Support.

 Enter a choice: 1
```

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



```
MS-DOS 6.22 Startup Menu
========================

    1. NiceLog PCI 9.0 Image.                 (Windows 2003 Appliance)
    2. Interaction Capture Unit 9.0 Image.  (Windows 2003 Appliance)
    3. NiceLog ISA 8.9 Image.                 (Windows 2003 Appliance)

 Enter a choice: 1
```

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 the previous page.

   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**.

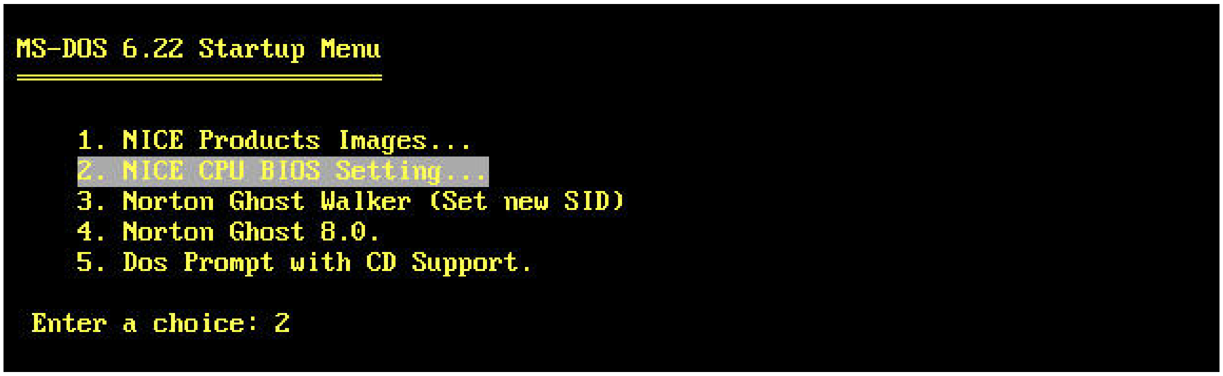
9. At the end of the installation a **Network Installation Done** notification appears.

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**.

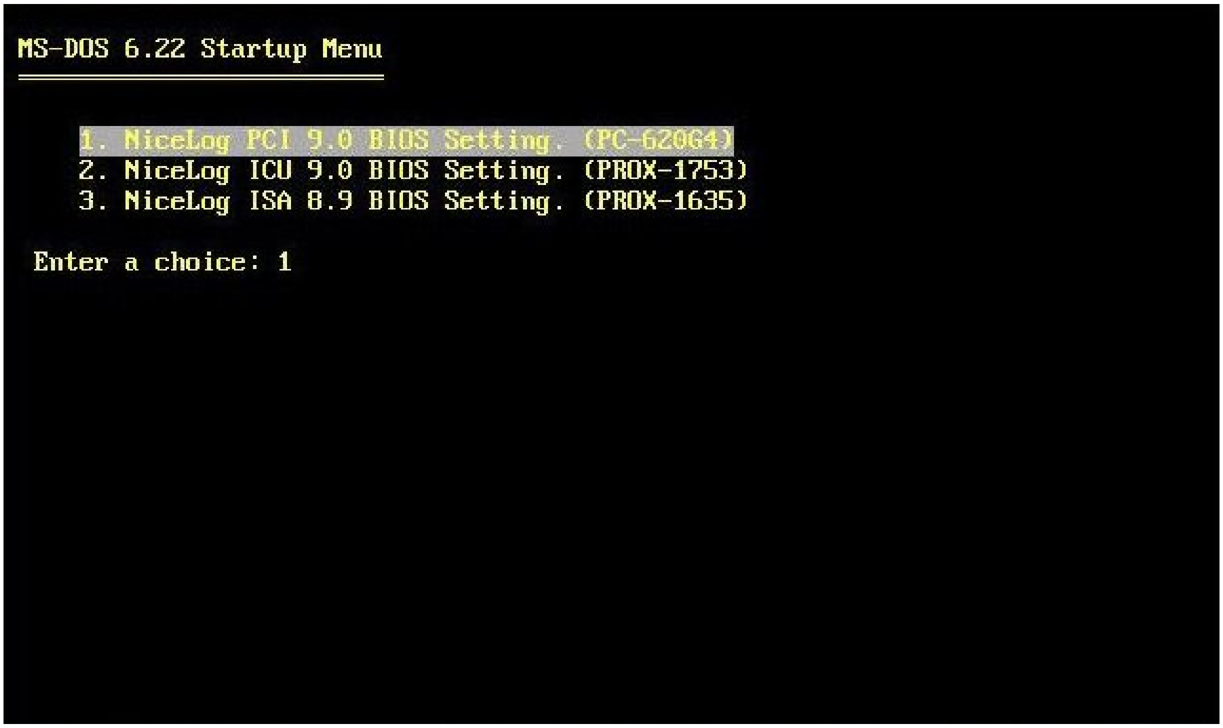
Figure 3-44: MS-DOS 6.22 Startup Menu



```
MS-DOS 6.22 Startup Menu
========================

    1. NICE Products Images...
    2. NICE CPU BIOS Setting...
    3. Norton Ghost Walker (Set new SID)
    4. Norton Ghost 8.0.
    5. Dos Prompt with CD Support.

 Enter a choice: 2
```

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 74.

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.

4

Microsoft Client Operating Systems

This section 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 Engage Platform 6.x, NICE Interaction Management 4.1, 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 NICE Perform Release 3.1, NICE Interaction Management 4.1 and on NICE Engage Platform 6.x, 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 Firewall Unblocked	Manually Add to Firewall Exceptions Tab	Internet Explorer	Comments
NICE ScreenAgent Version 8.8	NICE ScreenAgent See Firewall Unblock Example on page 91.	-		
NICE Perform ScreenAgent	NICE ScreenAgent See Firewall Unblock Example on page 91.	-		

Table 4-1: Security-Tuning List (continued)

NICE Component	Security-Tuning Firewall Unblocked	Manually Add to Firewall Exceptions Tab	Internet Explorer	Comments
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 the facing page.	NICE Administrator See Adding NICE Administrator to the Exceptions List on page 94.		
NICE Client/Server Applications Version 8.9	NICE Supervision Media Library Printer Server NICE RTS See Firewall Unblock Example on the facing page.	NICE Administrator See Adding NICE Administrator to the Exceptions List on page 94.		
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 96.		

Table 4-1: Security-Tuning List (continued)

NICE Component	Security-Tuning Firewall Unblocked	Manually Add to Firewall Exceptions Tab	Internet Explorer	Comments
NICE Web Applications Version 8.8			Install Crystal Smart Viewer for ActiveX. See Crystal Smart Viewer for ActiveX Guideline on the next 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.

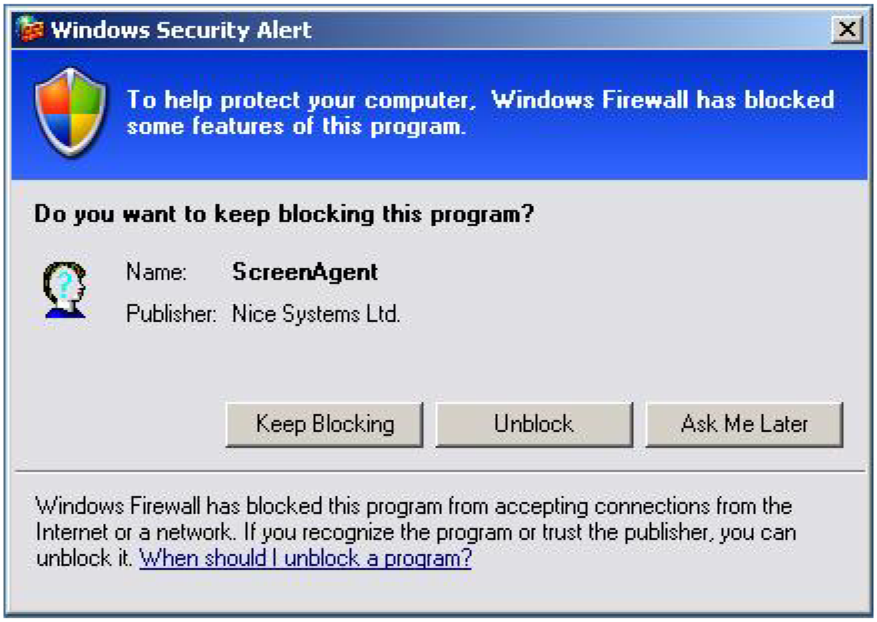
Security-Tuning Your System

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



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: ScreenAgent

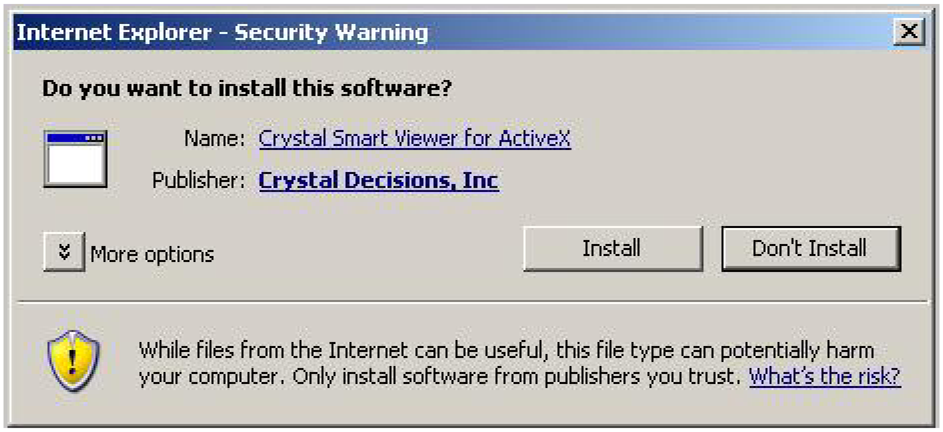
Publisher: Nice Systems Ltd.

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

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



Internet Explorer - Security Warning

Do you want to install this software?

Name: Crystal Smart Viewer for ActiveX

Publisher: Crystal Decisions, Inc

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

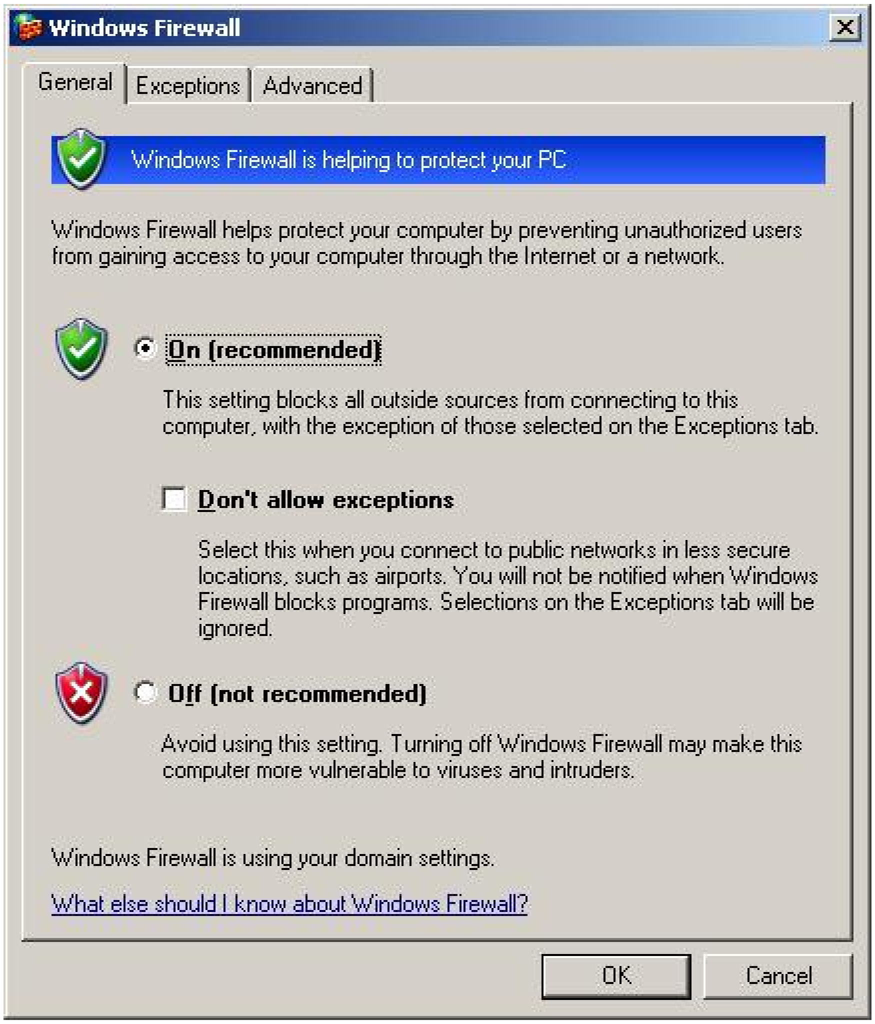
Manually Adding Programs to the Firewall Exceptions List

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



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

☐ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

Windows Firewall is using your domain settings.

What else should I know about Windows Firewall?

2. Ensure that **On (recommended)** is selected.

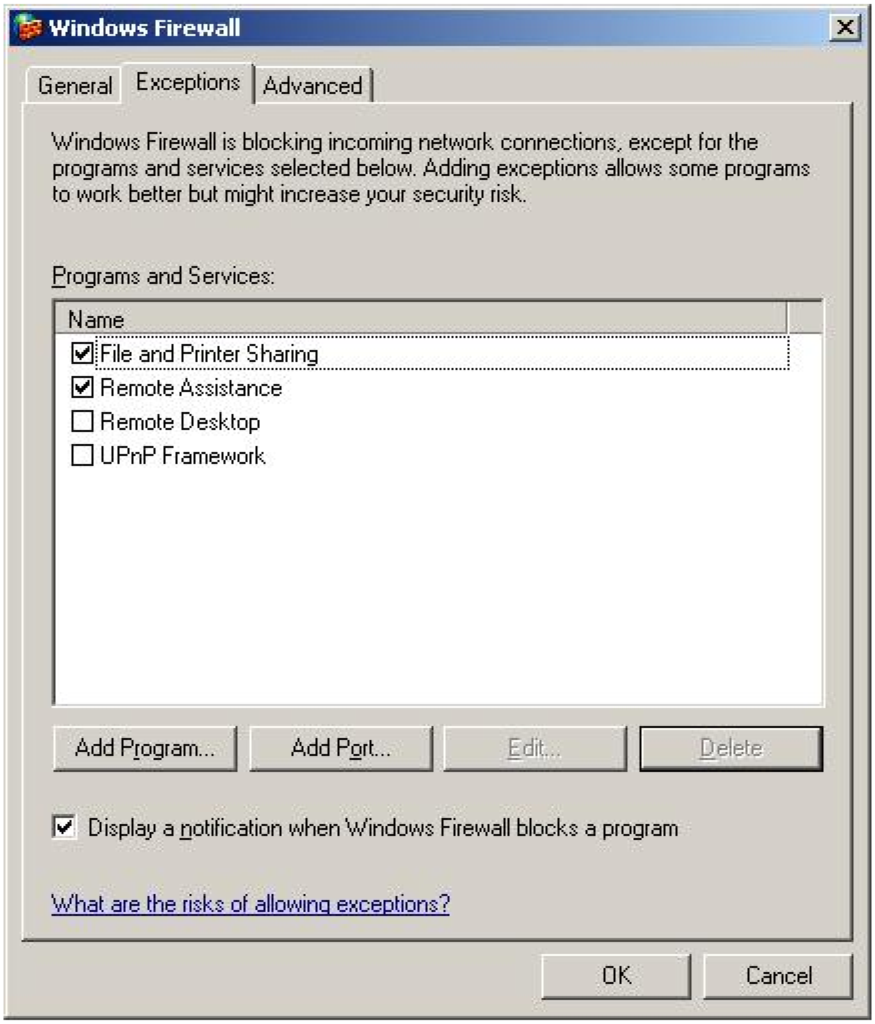
Adding NICE Administrator to the Exceptions List

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



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name
☑ File and Printer Sharing
☑ Remote Assistance
☐ Remote Desktop
☐ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

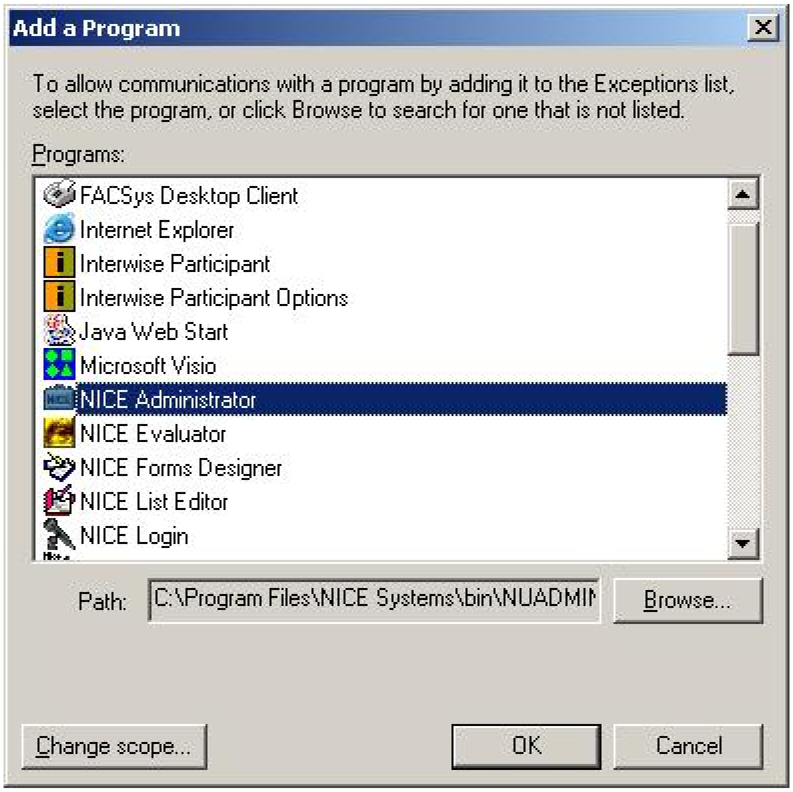
NOTE: Ensure that Display a notification when Windows Firewall blocks a program is selected.

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

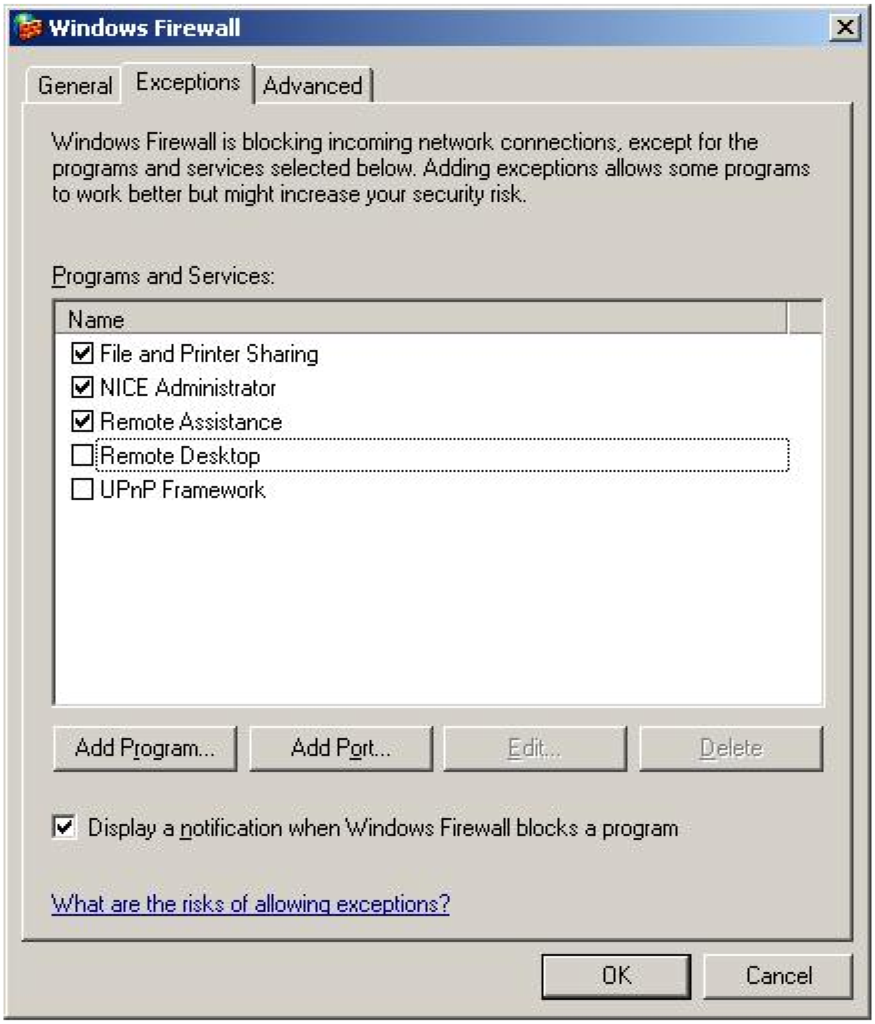
   Add a Program

   To allow communications with a program by adding it to the Exceptions list, select the program, or click Browse to search for one that is not listed.

   Path: C:\Program Files\NICE Systems\bin\NUADMIN

4. Click **OK**. NICE Administrator now appears in the **Exceptions** tab.

Figure 4-6: Windows Firewall - Exceptions Tab



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name
☑ File and Printer Sharing
☑ NICE Administrator
☑ Remote Assistance
□ Remote Desktop
□ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

5. In the **Exceptions** tab, click **OK**.

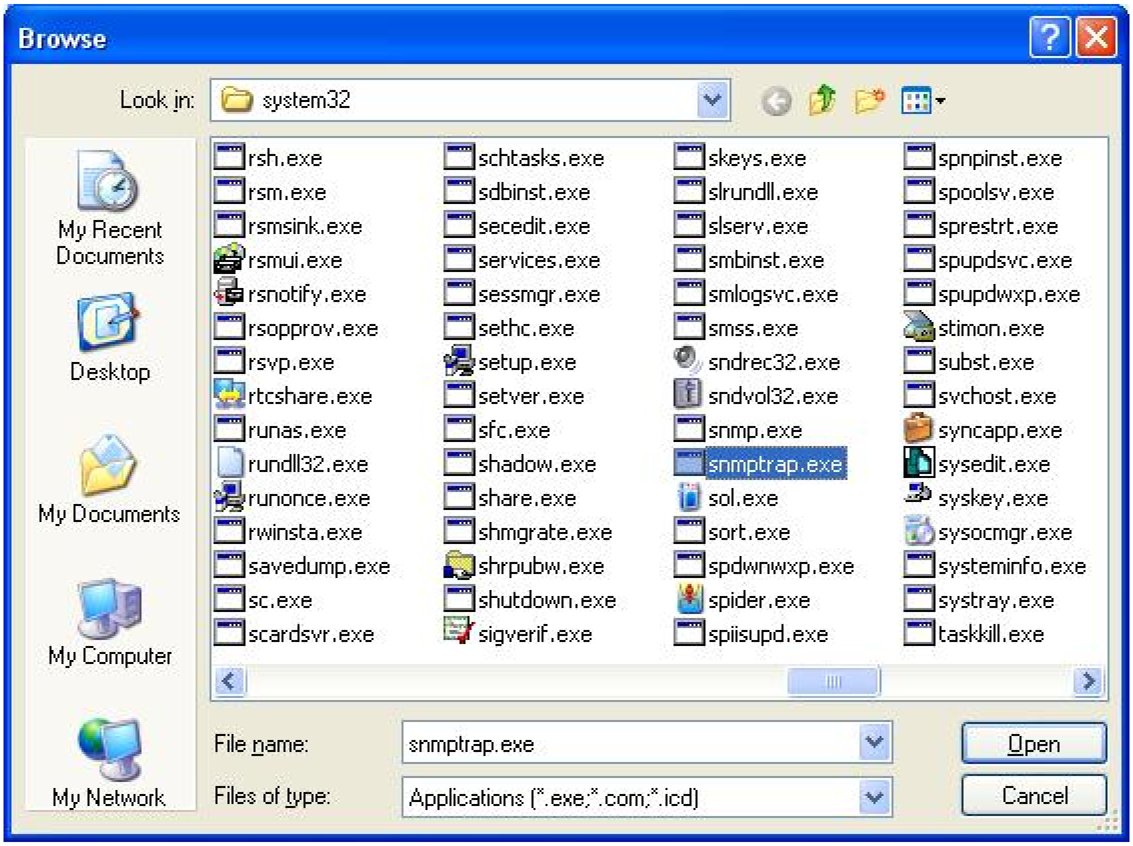
Adding snmptrap.exe to the Exceptions List

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



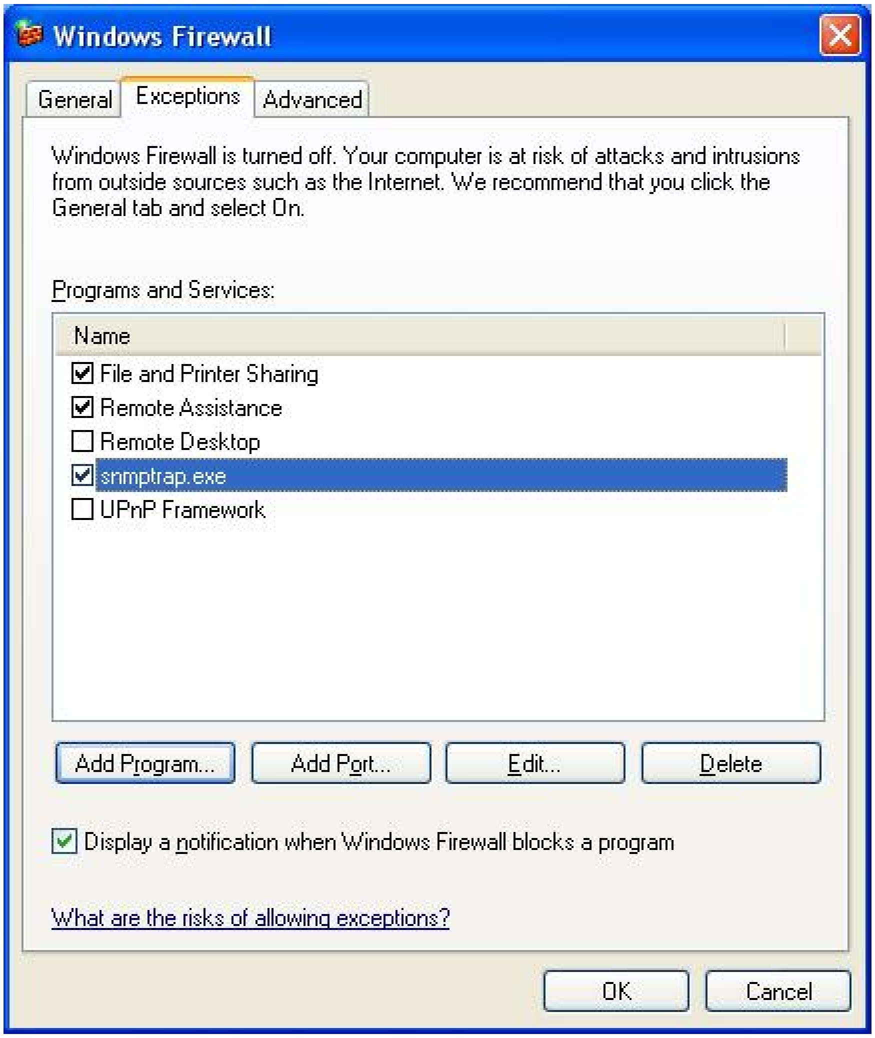
Look in: system32

File name: snmptrap.exe

Files of type: Applications (*.exe;*.com;*.icd)

3. Click **Open**. snmptramp.exe is now added to the Exceptions list.

Figure 4-8: Windows Firewall - Exceptions Tab



Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.

Programs and Services:

Name

☑ File and Printer Sharing
☑ Remote Assistance
☐ Remote Desktop
☑ snmptrap.exe
☐ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

4. Click **OK**.

Windows 7 32-bit/64-bit

Client Application 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/NICE Interaction Management Release 4.1/NICE Engage Platform client applications with Microsoft Windows 7 for Releases 3.1, 3.2, and 3.5:

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	NICE Perform 3.1		NICE Perform 3.2		NICE Perform 3.5		NIM 4.1 /NICE Engage Platform 6.x	
	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
Reporter Viewer	Approved (*)	Not Supported	Approved	Approved	Approved	Approved	Approved	Approved
NICE Applications (including Set Security)	Approved (*)	Approved (*)	Approved	Approved	Approved	Approved	Approved	Approved

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

Application	NICE Perform 3.1		NICE Perform 3.2		NICE Perform 3.5		NIM 4.1 /NICE Engage Platform 6.x	
	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
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

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

Application	NICE Perform 3.1		NICE Perform 3.2		NICE Perform 3.5		NIM 4.1 /NICE Engage Platform 6.x	
	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
Desktop Analytics (using PO Client)	N/A	N/A	N/A	N/A	Approved	NICE Approval	Approved	NICE Approval
RTS	Approved	Approved	Approved	Approved	Approved	Approved	Approved	Approved

Using Silent Installation to Install 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/NICE Engage Platform 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 on the facing page.
- ScreenSense Agent on the facing page.
- NICE Player and NICE Player Codec Pack on the facing page.
- Reporter Viewer on the facing page.
- NICE ScreenAgent on page 104.

- Record on Demand on page 106.
- PO Client on page 106
- NICE Insight to Impact Bridge on page 106
- Nice BSF Toolkit on page 106

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 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/NICE Engage Platform Release 6.x

Enter in the command line:

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

or

```
msiexec /i "ReporterViewer.msi" /qn
```

For NICE Interaction Management only, after installation of the **ReporterViewer.msi**, install the SAP Business Object BI platform which is located in the following folder:

C:\Program Files (x86)\Nice Systems\Reporter Viewer\32bitCA\32bit

In a silent installation BI platform, enter the command line:

```
setup.exe –r response.ini /q
```

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 4.1/NICE Engage Platform 6.x

➡ 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 "
```

Nice BSF Toolkit

For NICE Interaction Management/NICE Engage Platform, in the Command line, enter the following:

```
msiexec /i "NICE BSF Toolkit.msi" /qn
```

Manually Installing Client Applications

NOTE:
The procedures listed below are applicable to all NICE Perform Release 3.x/NICE Interaction Management 4.1/NICE Engage Platform 6.x 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 99. After installation is finished the UAC should be turned on.
- In NICE Interaction Management Release 4.1/NICE Engage Platform 6.x, UAC can be turned on during the installation of the client-side applications.

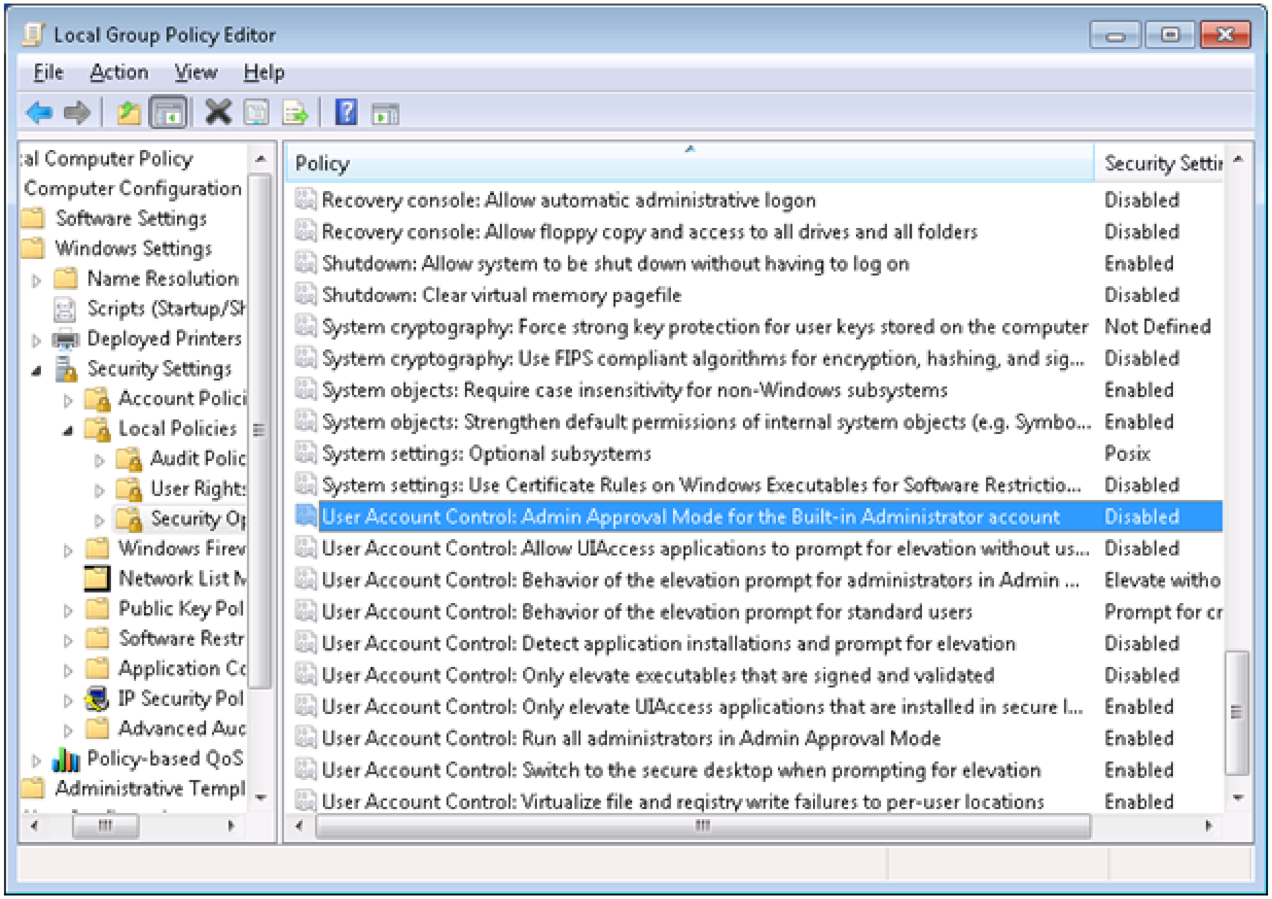
➡ To install client-side applications on workstations with Microsoft Windows 7:

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 99 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**.

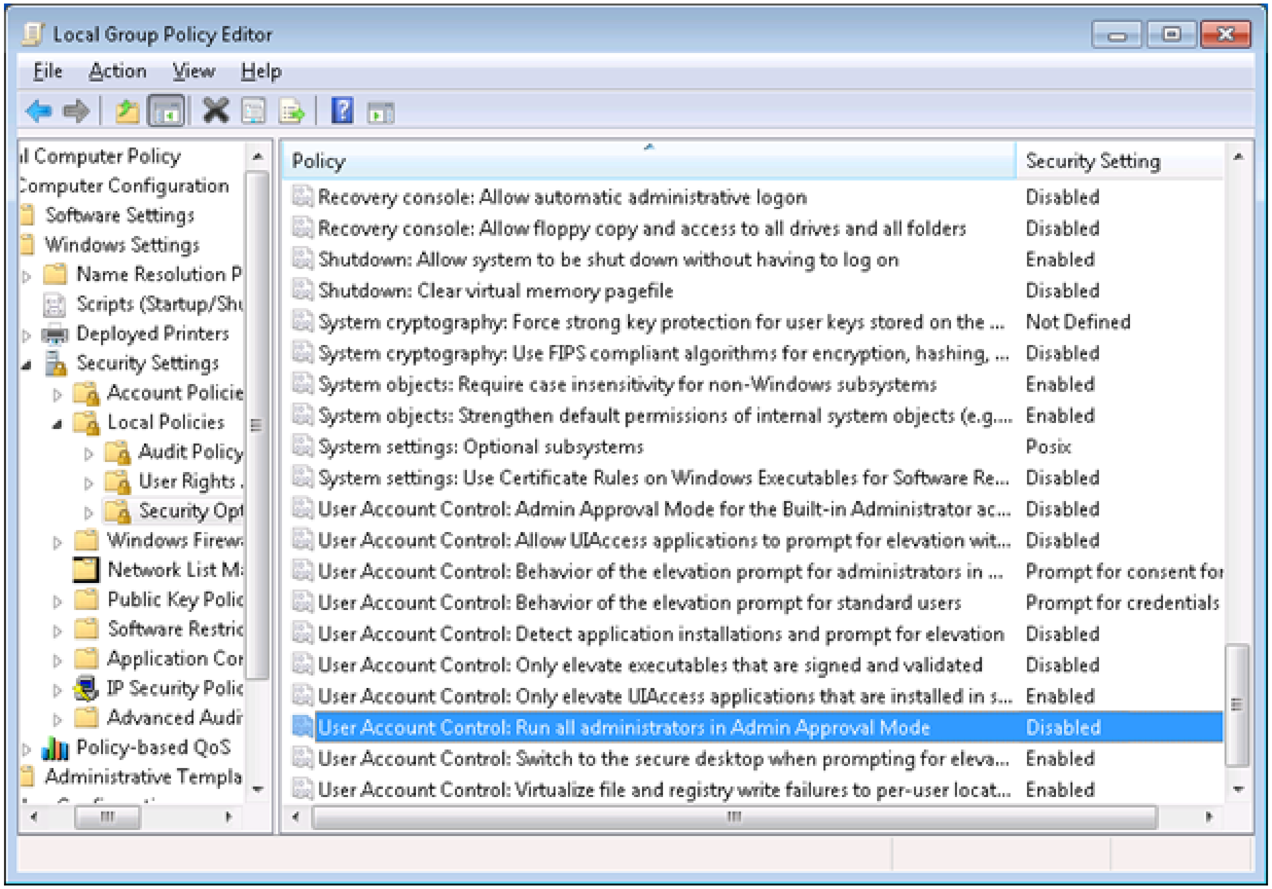
Figure 4-9: Local Group Policy Editor Window



Policy	Security Settir
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and sig...	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbo...	Enabled
System settings: Optional subsystems	Posix
System settings: Use Certificate Rules on Windows Executables for Software Restrictio...	Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without us...	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin ...	Elevate witho
User Account Control: Behavior of the elevation prompt for standard users	Prompt for cr
User Account Control: Detect application installations and prompt for elevation	Disabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure l...	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

- 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



Policy	Security Setting
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the ...	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, ...	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g....	Enabled
System settings: Optional subsystems	Posix
System settings: Use Certificate Rules on Windows Executables for Software Re...	Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator ac...	Disabled
User Account Control: Allow UIAccess applications to prompt for elevation wit...	Disabled
User Account Control: Behavior of the elevation prompt for administrators in ...	Prompt for consent for
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials
User Account Control: Detect application installations and prompt for elevation	Disabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in s...	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Disabled
User Account Control: Switch to the secure desktop when prompting for eleva...	Enabled
User Account Control: Virtualize file and registry write failures to per-user locat...	Enabled

5. Run the installation wizard.

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

Client Applications Compatibility

NICE Interaction Management 4.1.47 and later and NICE Engage Platform 6.x 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 and NICE Engage Platform 6.x 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

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

Application	Windows 8 32-bit	Windows 8 64-bit	Windows 8.1 32-bit	Windows 8.1 64-bit
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

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

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 Client Applications

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

- Set Security Application on the next page
- NICE Player and NICE Player Codec Pack on the next page
- NICE Screen Agent on the next page

- Record on Demand on the facing page

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 Client Applications

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

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

➡ To manually install NICE 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.

Windows 10 32-bit/64-bit

This section provides information on Microsoft Windows 10 Operating system, both in the 32-bit and 64-bit versions.

Client Applications Compatibility

NICE Engage Platform supports the following editions of Microsoft Windows 10, in both 32-bit and 64-bit configurations:

- Microsoft Windows 10 Professional Edition
- Microsoft Windows 10 Enterprise Edition

The following table shows the compatibility of client applications with NICE Engage Platform 6.4 and up with Microsoft Windows 10:

Table 4-4: Compatibility with Microsoft Windows 10 32-bit and 64-bit for NICE Engage Platform

	Windows 10 Professional		Windows 10 Enterprise	
Application	32-bit	64-bit	32-bit	64-bit
Screen Agent	Approved	Approved	Approved	Approved
Record on Demand/Stop on Demand	Approved	Approved	Approved	Approved
Standalone NICE Player and NICE Player Codec Pack	Approved	Approved	Approved	Approved

Table 4-4: Compatibility with Microsoft Windows 10 32-bit and 64-bit for NICE Engage Platform (continued)

	Windows 10 Professional		Windows 10 Enterprise	
Application	32-bit	64-bit	32-bit	64-bit
Reporter Viewer	Approved	Approved	Approved	Approved
QM Apps	Approved	Approved	Approved	Approved
Survey Manager	Not approved	Not approved	Not approved	Not approved
VRA	Not approved	Not approved	Not approved	Not approved
Media Library	Not approved	Not approved	Not approved	Not approved
BSF Tool Kit	Approved	Approved	Approved	Approved
NICE Sentinel Remote Client	Approved	Approved	Approved	Approved

Table 4-4: Compatibility with Microsoft Windows 10 32-bit and 64-bit for NICE Engage Platform (continued)

	Windows 10 Professional		Windows 10 Enterprise	
Application	32-bit	64-bit	32-bit	64-bit
Real-Time Designer	Approved	Approved	Approved	Approved
Real-Time Client	Approved	Approved	Approved	Approved
NDM/SRT/RHT	Approved	Approved	Approved	Approved
Engage Search	Approved	Approved	Approved	Approved
Analytics Apps	Approved	Approved	Approved	Approved
High Availability Manager	Not approved	Not approved	Not approved	Not approved
NICE Web Applications	Approved	Approved	Approved	Approved

Using the Silent Installation to Install Client Applications

Use the following commands to install NICE Engage Platform client-side applications with the silent installation on workstations running Microsoft Windows 10:

- Reporter Viewer
- NICE Player and NICE Player Codec Pack below
- Record on Demand on the facing page
- NICE BSF Toolkit on the facing page
- RTI Client on the facing page
- NICE Insight to Impact Bridge on the facing page

Reporter Viewer

To install the Reporter Viewer Application:

1. In the command-line prompt, enter the following command:

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

   or

```
msiexec /i "ReporterViewer.msi" /qn
```

2. After installing the Reporter Viewer, install the SAP Business Object BI platform located in the following folder:

   C:\Program Files (x86)\Nice Systems\Reporter Viewer\32bitCA\32bit

   In a silent installation BI platform, enter the following command:

```
setup.exe -r response.ini /q
```

NICE Player and NICE Player Codec Pack

To install the NICE Player and NICE Player Codec Pack:

- In the command-line prompt, enter the following command:

  msiexec /i "Nice Player.msi" /qn

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

Record on Demand

To install the Record on Demand:

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

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

  Where ***nnn*** is the Host Name.

NICE BSF Toolkit

To install the NICE BSF Toolkit:

In the command-line prompt, enter the following command:

```
msiexec /i "NICE BSF Toolkit.msi" /qn
```

RTI Client

To install the RTI Client:

In the command-line prompt, enter the following command:

```
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

To install the NICE Insight to Impact Bridge

In the command-line prompt, enter the following command:

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

Manually Installing NICE Client Applications

> **NOTE:** The procedures listed below are applicable to all NICE Engage Platform client-side components on workstations running Microsoft Windows 10 operating system.
>
> In NICE Engage Platform systems, UAC can be turned on while installing client-side applications.

➡ **To manually install NICE client-side applications on workstations with Microsoft Windows 10:**

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 section 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.

Using XBAP with Internet Explorer

- 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/NICE Engage Platform 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 Engage Platform 6.x 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 more information on setting up XBAP, see the *Workstation Setup Guide*

Contents

5: Internet Explorer

Internet Explorer 6

Compatibility of NICE Web Applications with Internet Explorer 6

Product	NICE Interaction Management, NiceUniverse Web Application, NICE Sentinel, NICE Real-Time Solution
Release	NICE Interaction Management R4.1 NICE Sentinel: - NICE Sentinel Server: R2.1, R2.5, R4.1 - NICE Sentinel Remote Client: R2.1, R2.5, R4.1 NICE Real-Time Solution 4.9.x
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 Interaction Management Release 4.1
- NICE Sentinel
  - Release 2.1
  - Release 2.5
  - Release 4.1
  - Release 6.3

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	NiceUniverse Web Application, NICE Sentinel, NICE Real-Time Solution
Release	NICE Interaction Management R4.1 NICE Sentinel: ■ NICE Sentinel Server: R2.1, R2.5, R4.1, R6.X ■ NICE Sentinel Remote Client: R2.1, R2.5, R4.1 NICE Real-Time Solution 4.9.x
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 Interaction Management Release 4.1
- NICE Sentinel
  - Release 2.1
  - Release 2.5
  - Release 4.1
  - Release 6.X

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 136

Table 5-2:
Operating Systems

Operating System	IPC 9.09	NP R3.2	NP R3.5	NIM 4.1	NICE Sentinel R2.1/2.5	NICE Sentinel R4.1
Windows Vista Business						
Windows Vista Enterprise		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
Windows XP	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

Table 5-3: Known Issues (continued)

Issue	Description	Release
		- 2 - NICE Perform R3 - Release IPC 9

Table 5-3: Known Issues (continued)

Issue	Description	Release
		▪ .09 ▪ Universe Web Applications Ver

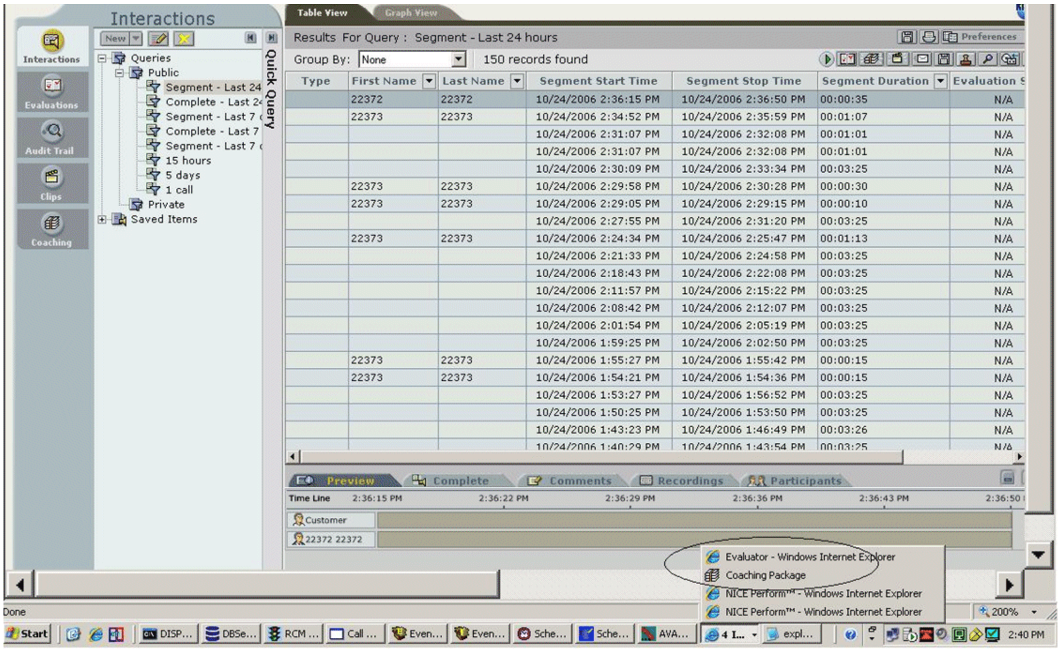
Table 5-3: Known Issues (continued)

Issue	Description	Release
		■ sion 8.9

Table 5-3: Known Issues (continued)

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 R1 ■ NICE Perform R2

Table 5-3: Known Issues (continued)

Issue	Description	Release
		- NICE Perform R3 (Contact Center)

Results For Query : Segment - Last 24 hours

Group By: None 150 records found

Type	First Name	Last Name	Segment Start Time	Segment Stop Time	Segment Duration	Evaluation S
	22372	22372	10/24/2006 2:36:15 PM	10/24/2006 2:36:50 PM	00:00:35	N/A
	22373	22373	10/24/2006 2:34:52 PM	10/24/2006 2:35:59 PM	00:01:07	N/A
			10/24/2006 2:31:07 PM	10/24/2006 2:32:08 PM	00:01:01	N/A
			10/24/2006 2:31:07 PM	10/24/2006 2:32:08 PM	00:01:01	N/A
			10/24/2006 2:30:09 PM	10/24/2006 2:33:34 PM	00:03:25	N/A
	22373	22373	10/24/2006 2:29:58 PM	10/24/2006 2:30:28 PM	00:00:30	N/A
	22373	22373	10/24/2006 2:29:05 PM	10/24/2006 2:29:15 PM	00:00:10	N/A
			10/24/2006 2:27:55 PM	10/24/2006 2:31:20 PM	00:03:25	N/A
	22373	22373	10/24/2006 2:24:34 PM	10/24/2006 2:25:47 PM	00:01:13	N/A
			10/24/2006 2:21:33 PM	10/24/2006 2:24:58 PM	00:03:25	N/A
			10/24/2006 2:18:43 PM	10/24/2006 2:22:08 PM	00:03:25	N/A
			10/24/2006 2:11:57 PM	10/24/2006 2:15:22 PM	00:03:25	N/A
			10/24/2006 2:08:42 PM	10/24/2006 2:12:07 PM	00:03:25	N/A
			10/24/2006 2:01:54 PM	10/24/2006 2:05:19 PM	00:03:25	N/A
			10/24/2006 1:59:25 PM	10/24/2006 2:02:50 PM	00:03:25	N/A
	22373	22373	10/24/2006 1:55:27 PM	10/24/2006 1:55:42 PM	00:00:15	N/A
	22373	22373	10/24/2006 1:54:21 PM	10/24/2006 1:54:36 PM	00:00:15	N/A
			10/24/2006 1:53:27 PM	10/24/2006 1:56:52 PM	00:03:25	N/A
			10/24/2006 1:50:25 PM	10/24/2006 1:53:50 PM	00:03:25	N/A
			10/24/2006 1:43:23 PM	10/24/2006 1:46:49 PM	00:03:26	N/A
			10/24/2006 1:40:29 PM	10/24/2006 1:43:54 PM	00:03:25	N/A

Time Line 2:36:15 PM 2:36:22 PM 2:36:29 PM 2:36:36 PM 2:36:43 PM 2:36:50

Customer

22372 22372

Evaluator - Windows Internet Explorer
Coaching Package
NICE Perform™ - Windows Internet Explorer
NICE Perform™ - Windows Internet Explorer

Done

Table 5-3: Known Issues (continued)

Issue	Description	Release
		■ 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
	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 facing 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 145.

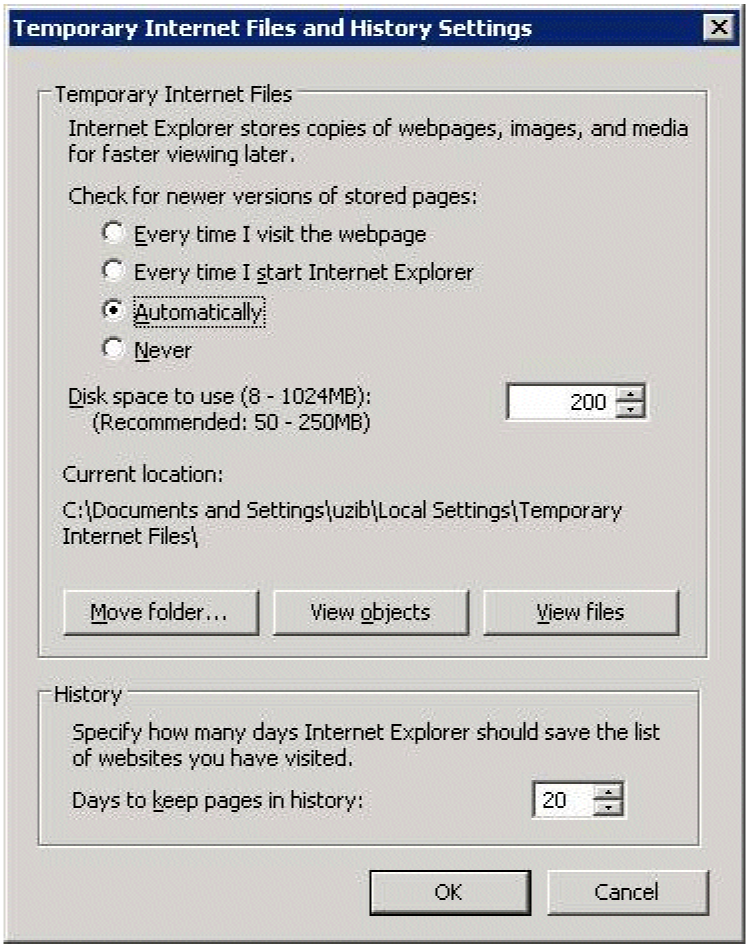
Changing the Cache Size

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



Temporary Internet Files and History Settings

Temporary Internet Files

Internet Explorer stores copies of webpages, images, and media for faster viewing later.

Check for newer versions of stored pages:

○ Every time I visit the webpage

○ Every time I start Internet Explorer

● Automatically

○ Never

Disk space to use (8 - 1024MB):
(Recommended: 50 - 250MB) 200

Current location:

C:\Documents and Settings\uzib\Local Settings\Temporary Internet Files\

History

Specify how many days Internet Explorer should save the list of websites you have visited.

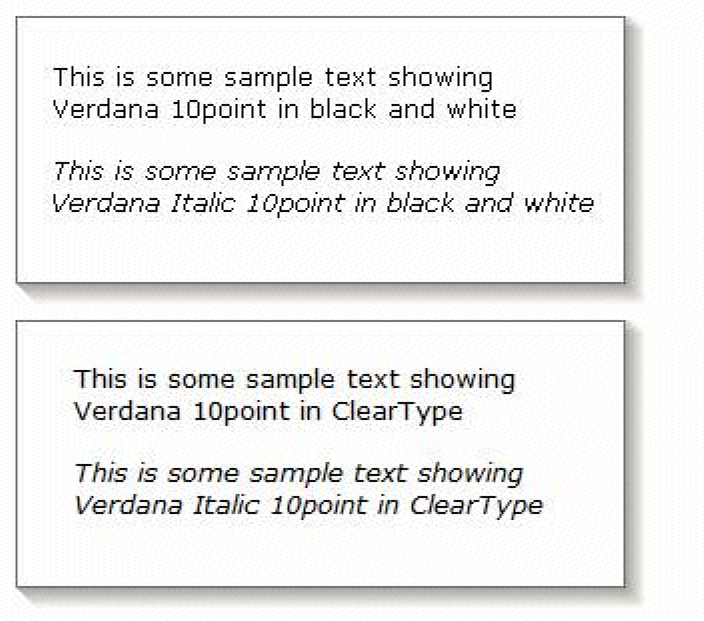
Days to keep pages in history: 20

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



This is some sample text showing Verdana 10point in black and white

This is some sample text showing Verdana Italic 10point in black and white

This is some sample text showing Verdana 10point in ClearType

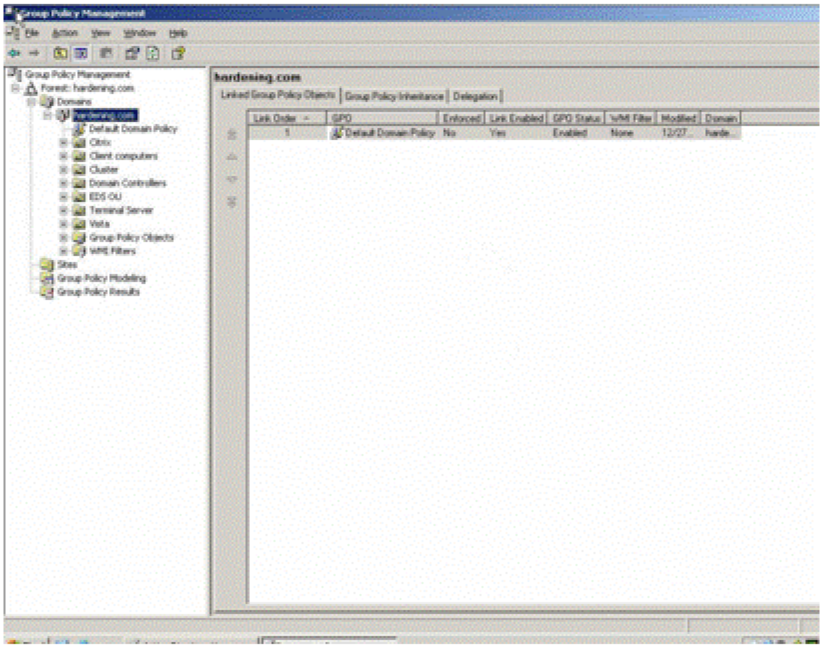
This is some sample text showing Verdana Italic 10point in ClearType

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.

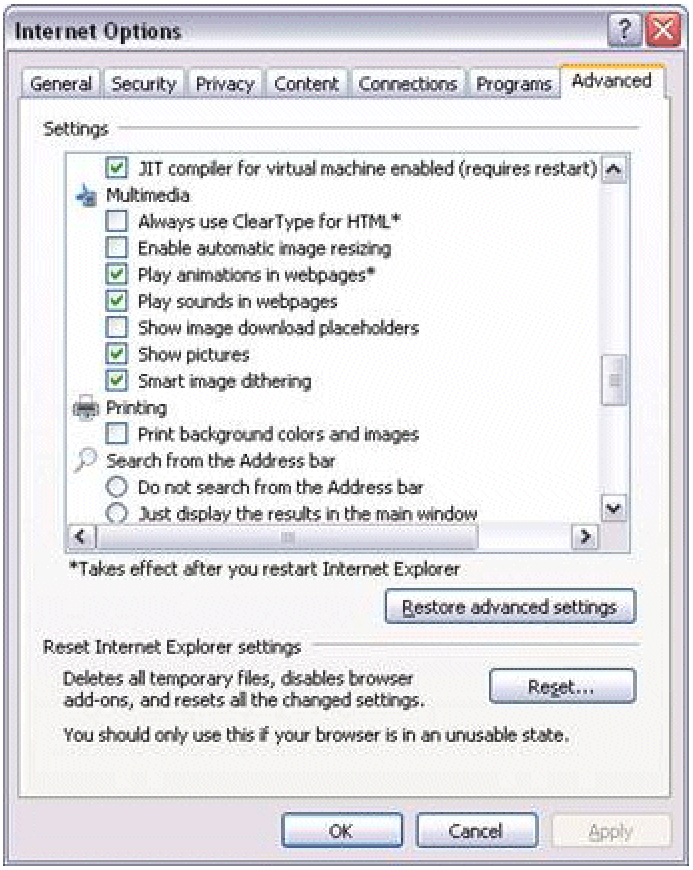
Figure 5-3: Internet Explorer Window



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Default Domain Policy	No	Yes	Enabled	None	12/27...	harde...

2. Click **Tools**, select **Internet Option**, and click **Advanced**. The following window appears.

Figure 5-4: Internet Options - Advanced Tab



☑ JIT compiler for virtual machine enabled (requires restart)

Multimedia

☐ Always use ClearType for HTML*

☐ Enable automatic image resizing

☑ Play animations in webpages*

☑ Play sounds in webpages

☐ Show image download placeholders

☑ Show pictures

☑ Smart image dithering

Printing

☐ Print background colors and images

Search from the Address bar

○ Do not search from the Address bar

○ Just display the results in the main window

*Takes effect after you restart Internet Explorer

Deletes all temporary files, disables browser add-ons, and resets all the changed settings.

You should only use this if your browser is in an unusable state.

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

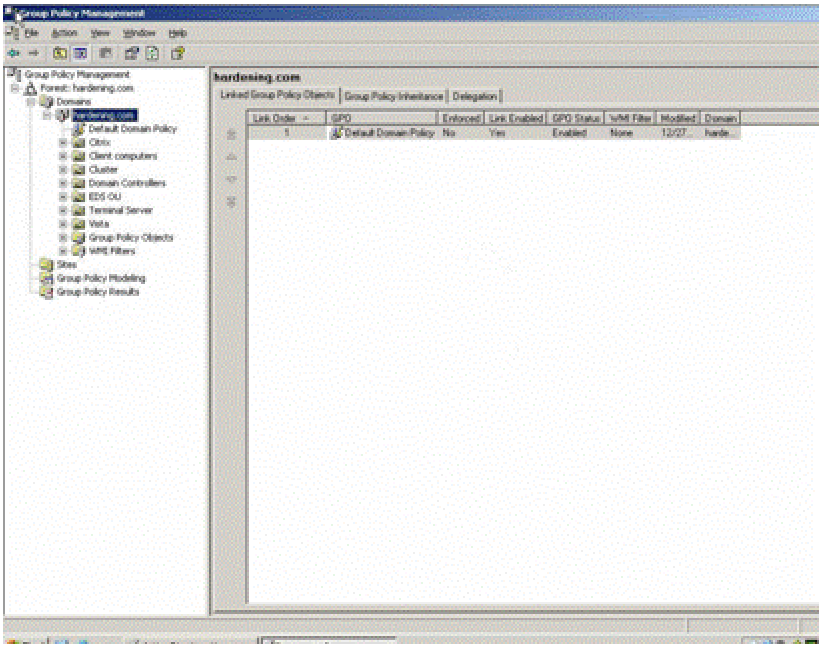
Perform the following procedure to manually add the application server to the trusted site list.

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



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Default Domain Policy	No	Yes	Enabled	None	12/27...	harde...

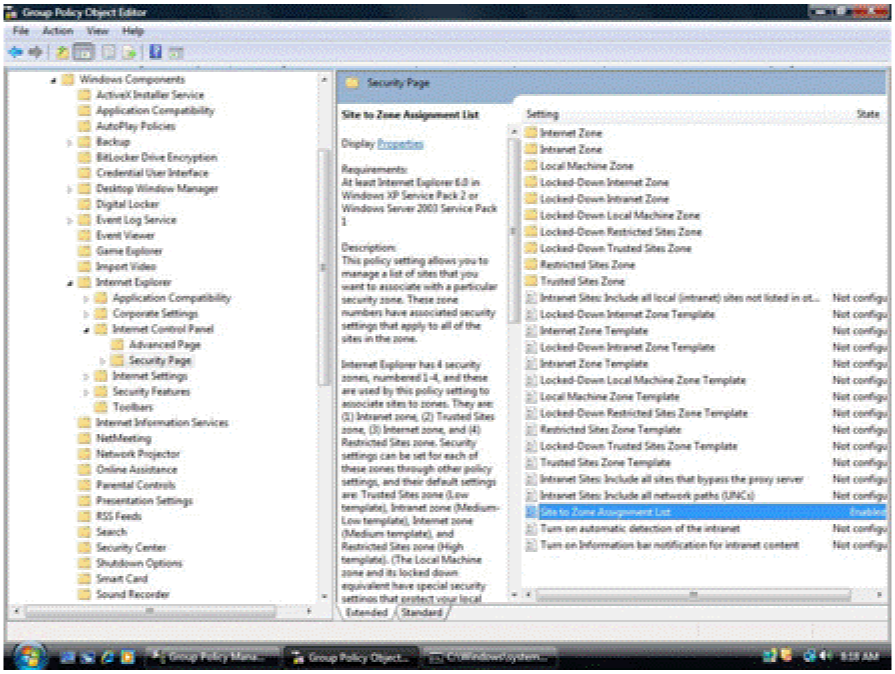
2. Right-click the **GPO** you created when you created the User Account Control and click **Edit**.

> **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



Site to Zone Assignment List

Display Properties

Requirements:
At least Internet Explorer 6.0 in Windows XP Service Pack 2 or Windows Server 2003 Service Pack 1

Description:
This policy setting allows you to manage a list of sites that you want to associate with a particular security zone. These zone numbers have associated security settings that apply to all of the sites in the zone.

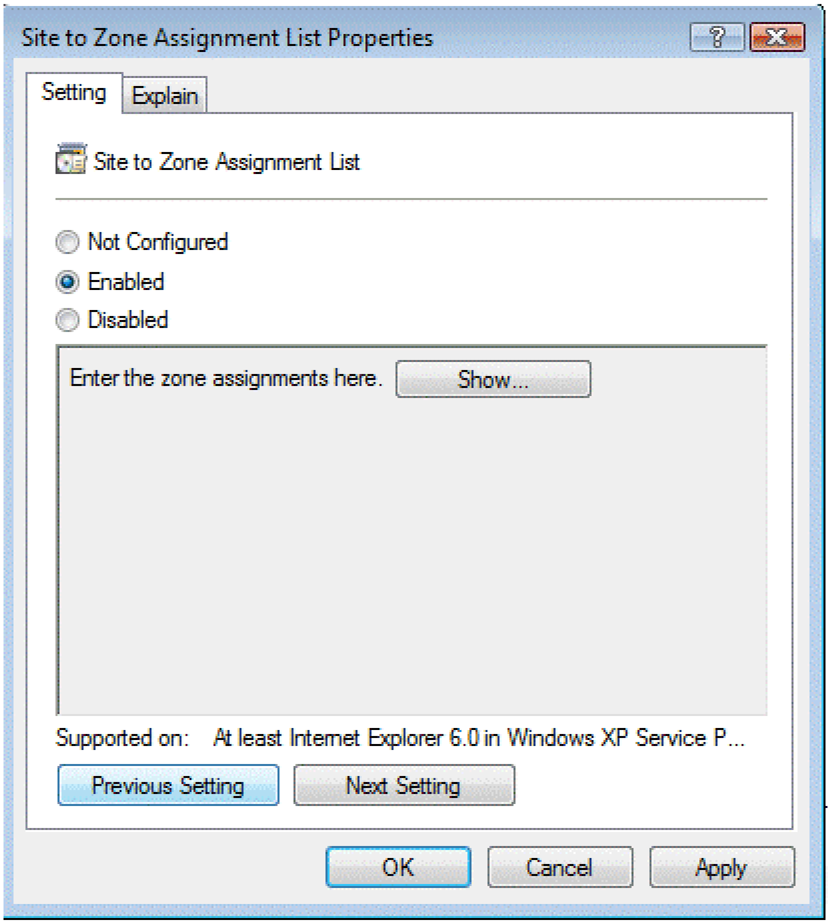
Internet Explorer has 4 security zones, numbered 1-4, and these are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zone, (3) Internet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings are: Trusted Sites zone (Low template), Intranet zone (Medium-Low template), Internet zone (Medium template), and Restricted Sites zone (High template). (The Local Machine zone and its locked down equivalent have special security settings that protect your local

Setting	State
Internet Zone	
Intranet Zone	
Local Machine Zone	
Locked-Down Internet Zone	
Locked-Down Intranet Zone	
Locked-Down Local Machine Zone	
Locked-Down Restricted Sites Zone	
Locked-Down Trusted Sites Zone	
Restricted Sites Zone	
Trusted Sites Zone	
Intranet Sites: Include all local (intranet) sites not listed in ot...	Not configu
Locked-Down Internet Zone Template	Not configu
Internet Zone Template	Not configu
Locked-Down Intranet Zone Template	Not configu
Intranet Zone Template	Not configu
Locked-Down Local Machine Zone Template	Not configu
Local Machine Zone Template	Not configu
Locked-Down Restricted Sites Zone Template	Not configu
Restricted Sites Zone Template	Not configu
Locked-Down Trusted Sites Zone Template	Not configu
Trusted Sites Zone Template	Not configu
Intranet Sites: Include all sites that bypass the proxy server	Not configu
Intranet Sites: Include all network paths (UNCs)	Not configu
Site to Zone Assignment List	Enabled
Turn on automatic detection of the intranet	Not configu
Turn on Information bar notification for intranet content	Not configu

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


Site to Zone Assignment List Properties

Site to Zone Assignment List

○ Not Configured
● Enabled
○ Disabled

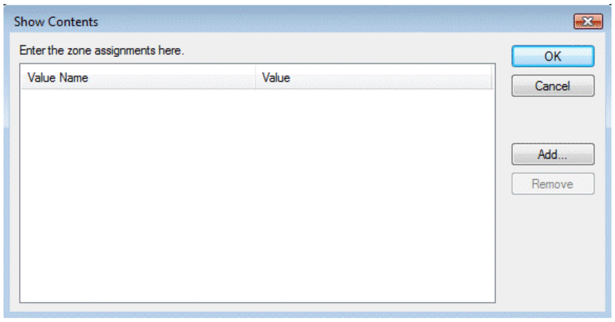
Enter the zone assignments here.

Supported on: At least Internet Explorer 6.0 in Windows XP Service P...

5. Select **Enabled** and click **Show.**

The Show Contents window appears.

Figure 5-8: Show Contents Window


Show Contents

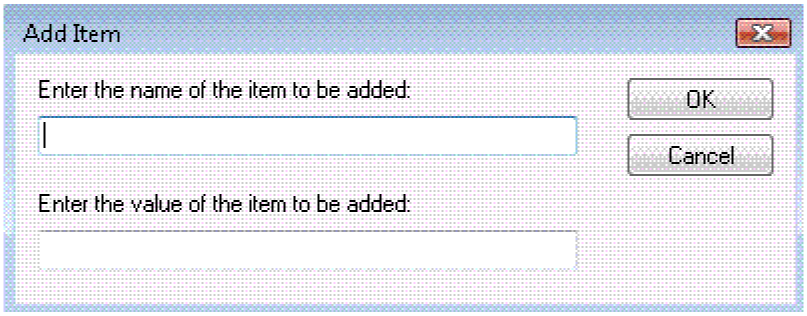
Enter the zone assignments here.

Value Name	Value

6. Click **Add.**

The Add Item window appears.

Figure 5-9: Add Item Window


Add Item
Enter the name of the item to be added:
Enter the value of the item to be added:
OK
Cancel

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 Engage Platform, NICE Interaction Management, NICE Perform, NiceUniverse Web Application, NICE Sentinel, NICE Real-Time Solution
Release	NICE Interaction Management R4.1 NICE Engage Platform R6.x **NOTE:** NICE Engage Platform 6.x environments with Engage Search, require Internet Explorer 10 or above. NICE Perform: R3 SP3/SP4, R3.1, R3.2, R3.5 NICE Sentinel: ■ NICE Sentinel Server: R2.1, R2.5, R4.1 ■ NICE Sentinel Remote Client: R2.1, R2.5, R4.1 NICE Real-Time Solution 4.9.x
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 Perform

  - Release 3.1
  - Release 3.2
  - Release 3.5
- NICE Interaction Management Release 4.1
- NICE Engage Platform 6.x
- NICE Sentinel
  - Release 2.1
  - Release 2.5
  - Release 4.1
  - Release 6.X

Conclusions

The NICE Engage Platform/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 Web Applications Known Issues with Internet Explorer 8 below.

NICE Web Applications Known Issues with Internet Explorer 8

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

NICE Web Applications

Issue 1

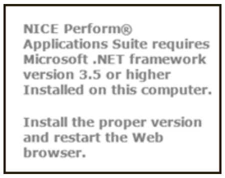
The NICE Web application URL must be added to the Trusted Site list. See Manually Adding NICE Web Applications to the Trusted Site List on the facing page.

Issue 2

NICE 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 Web Applications URL to the Local Intranet Site List on page 152.

Issue 4

To correctly display the NICE Web Application, the default documentation mode in Internet Explorer 8 should be Quirks mode. If a different mode is used, the application screen appears.

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 Web Applications to the Trusted Site List below.

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 151.

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 Web Applications to the Trusted Site List

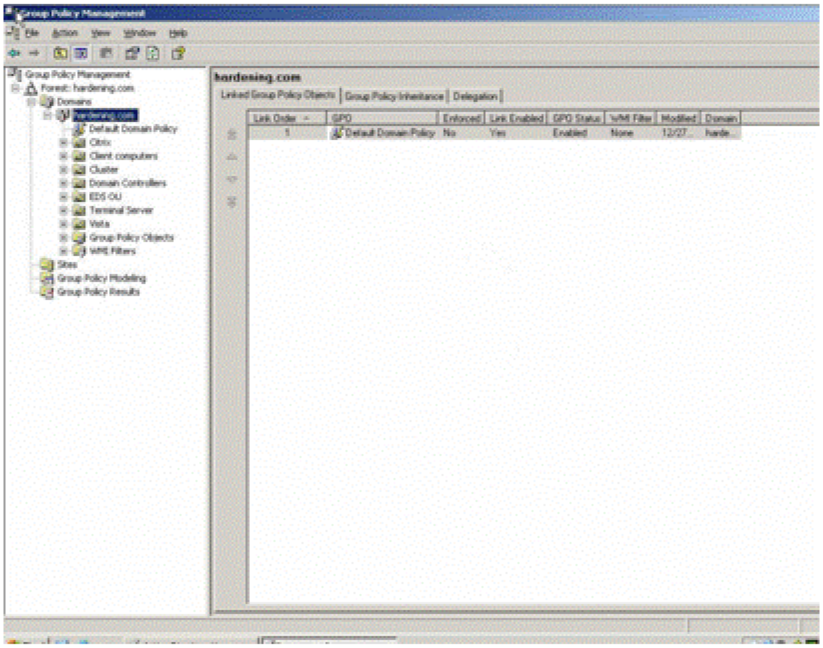
Perform the following procedure to manually add the Applications server to the trusted site list.

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 Web Applications 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

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Default Domain Policy	No	Yes	Enabled	None	12/27...	harde...

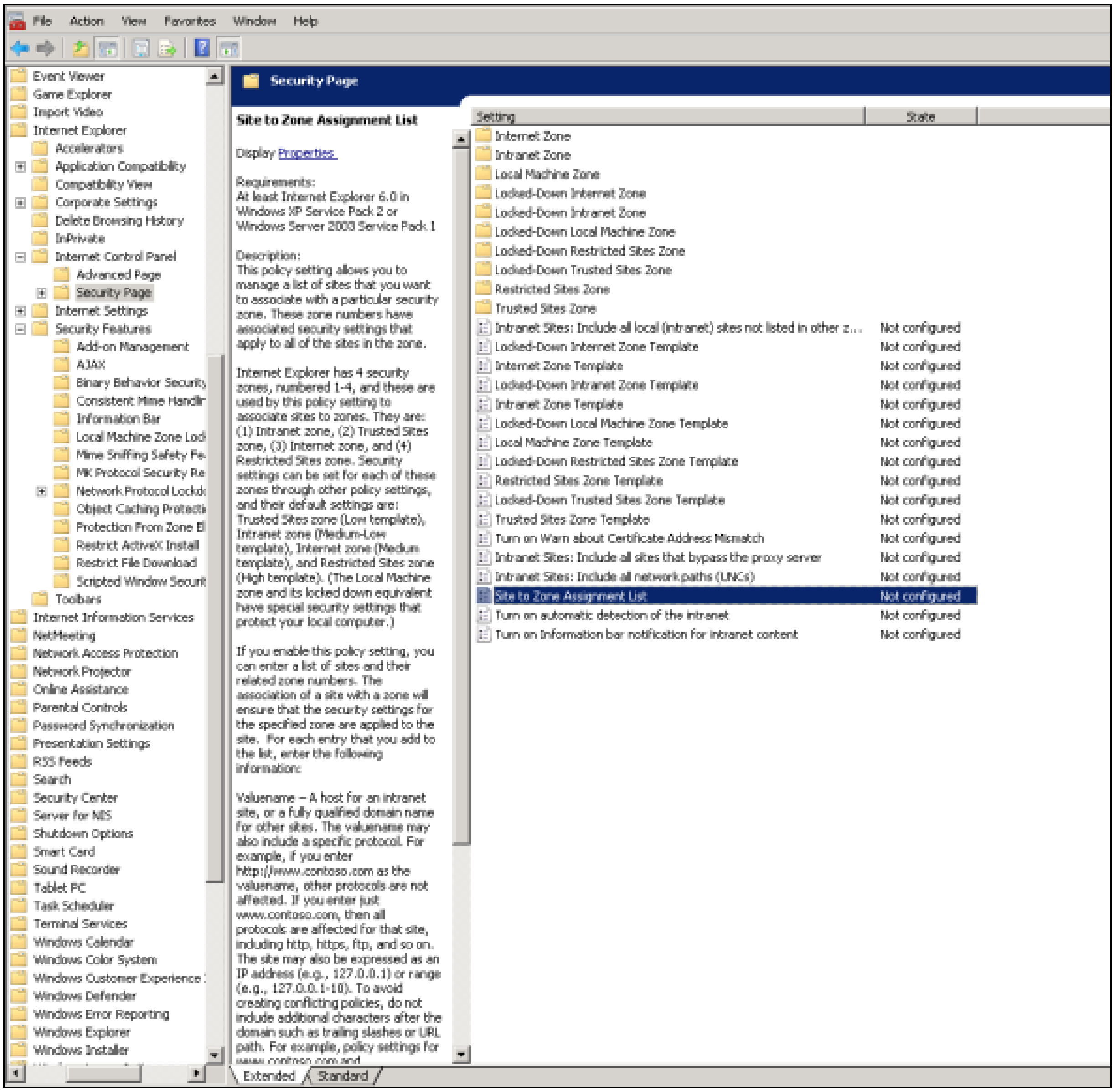
2. Right-click the **GPO** you created when you created the User Account Control and click **Edit.**

   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 section: 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



Site to Zone Assignment List

Display Properties

Requirements:
At least Internet Explorer 6.0 in Windows XP Service Pack 2 or Windows Server 2003 Service Pack 1

Description:
This policy setting allows you to manage a list of sites that you want to associate with a particular security zone. These zone numbers have associated security settings that apply to all of the sites in the zone.

Internet Explorer has 4 security zones, numbered 1-4, and these are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zone, (3) Internet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings are: Trusted Sites zone (Low template), Intranet zone (Medium-Low template), Internet zone (Medium template), and Restricted Sites zone (High template). (The Local Machine zone and its locked down equivalent have special security settings that protect your local computer.)

If you enable this policy setting, you can enter a list of sites and their related zone numbers. The association of a site with a zone will ensure that the security settings for the specified zone are applied to the site. For each entry that you add to the list, enter the following information:

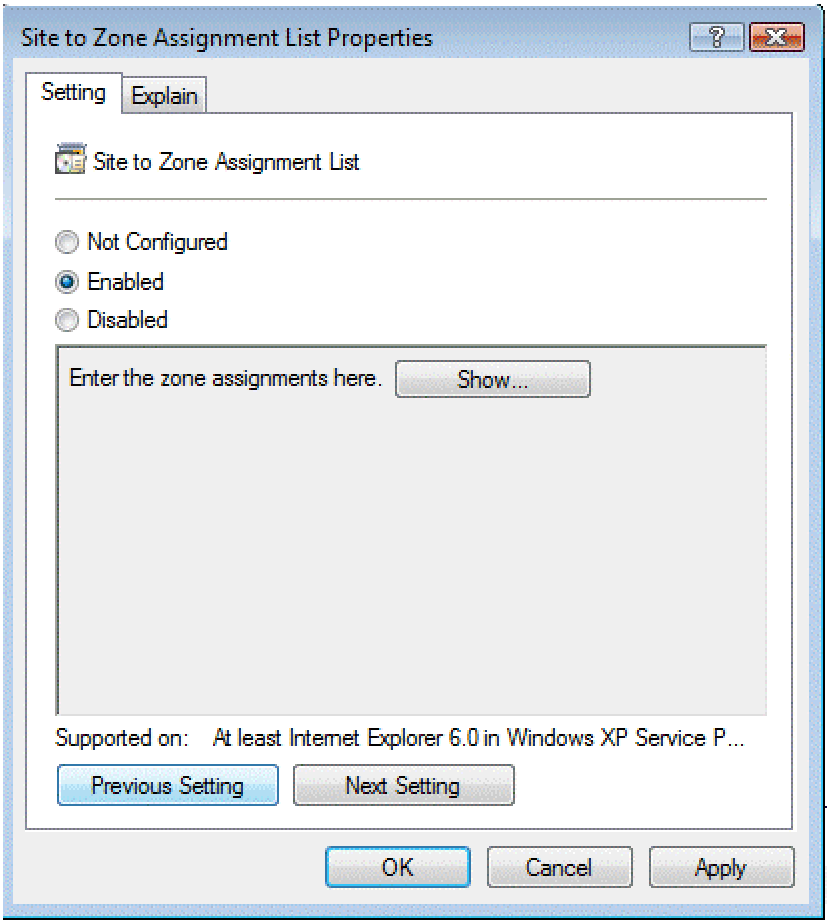
Valuename – A host for an intranet site, or a fully qualified domain name for other sites. The valuename may also include a specific protocol. For example, if you enter http://www.contoso.com as the valuename, other protocols are not affected. If you enter just www.contoso.com, then all protocols are affected for that site, including http, https, ftp, and so on. The site may also be expressed as an IP address (e.g., 127.0.0.1) or range (e.g., 127.0.0.1-10). To avoid creating conflicting policies, do not include additional characters after the domain such as trailing slashes or URL path. For example, policy settings for www.contoso.com and

Setting	State
Internet Zone	
Intranet Zone	
Local Machine Zone	
Locked-Down Internet Zone	
Locked-Down Intranet Zone	
Locked-Down Local Machine Zone	
Locked-Down Restricted Sites Zone	
Locked-Down Trusted Sites Zone	
Restricted Sites Zone	
Trusted Sites Zone	
Intranet Sites: Include all local (intranet) sites not listed in other z...	Not configured
Locked-Down Internet Zone Template	Not configured
Internet Zone Template	Not configured
Locked-Down Intranet Zone Template	Not configured
Intranet Zone Template	Not configured
Locked-Down Local Machine Zone Template	Not configured
Local Machine Zone Template	Not configured
Locked-Down Restricted Sites Zone Template	Not configured
Restricted Sites Zone Template	Not configured
Locked-Down Trusted Sites Zone Template	Not configured
Trusted Sites Zone Template	Not configured
Turn on Warn about Certificate Address Mismatch	Not configured
Intranet Sites: Include all sites that bypass the proxy server	Not configured
Intranet Sites: Include all network paths (UNCs)	Not configured
Site to Zone Assignment List	Not configured
Turn on automatic detection of the intranet	Not configured
Turn on Information bar notification for intranet content	Not configured

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



Site to Zone Assignment List Properties

Site to Zone Assignment List

○ Not Configured
● Enabled
○ Disabled

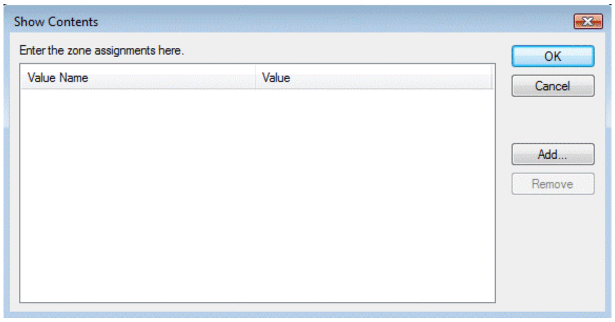
Enter the zone assignments here.

Supported on: At least Internet Explorer 6.0 in Windows XP Service P...

5. Select **Enabled** and click **Show.**

   The Show Contents window appears.

   Figure 5-13: Show Contents Window



Show Contents

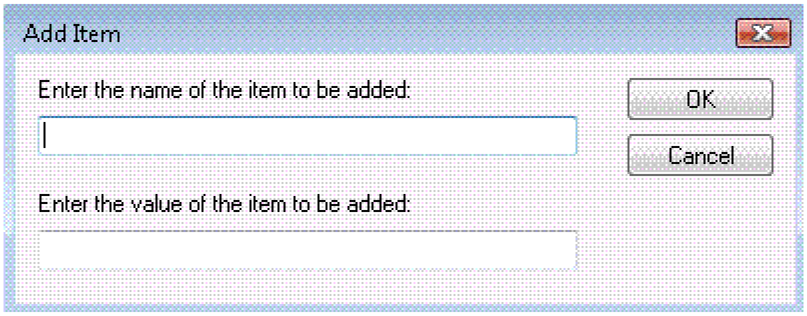
Enter the zone assignments here.

Value Name	Value

6. Click **Add.**

The Add Item window appears.

Figure 5-14: Add Item Window


Add Item
Enter the name of the item to be added:
Enter the value of the item to be added:
OK
Cancel

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*.

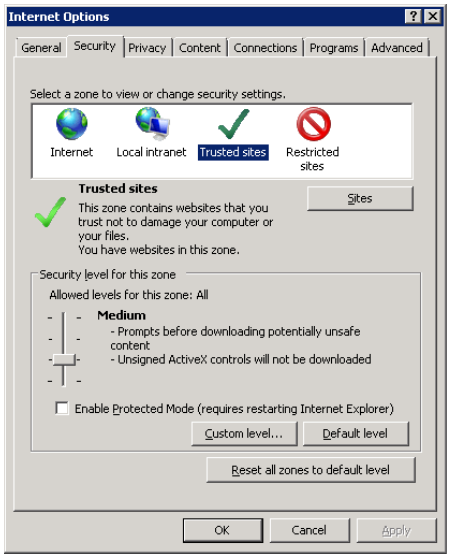
To disable *Protected Mode*:

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



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

You have websites in this zone.

Security level for this zone

Allowed levels for this zone: All

Medium

- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☐ Enable Protected Mode (requires restarting Internet Explorer)

3. Click the **Security** tab. In the Security level for this zone area, make sure that **Enable Protected Mode** is not selected.

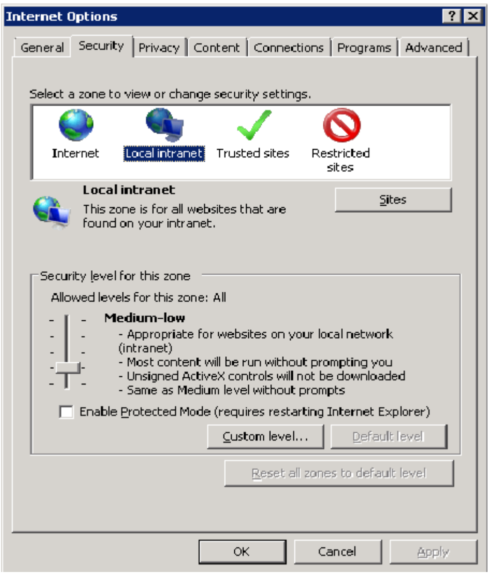
4. Click **OK**.

Adding the NICE Web Applications 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



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

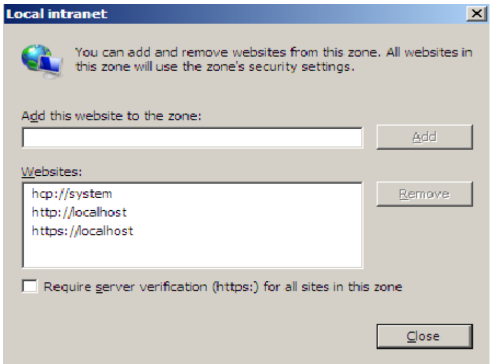
□ Enable Protected Mode (requires restarting Internet Explorer)

3. Click **Local Internet**.

4. Click **Sites**.

   The Local Intranet window appears.

Figure 5-17: Local Intranet Window



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Websites:

hcp://system
http://localhost
https://localhost

□ Require server verification (https:) for all sites in this zone

5. Enter the NICE 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 Engage Platform, NICE Interaction Management, NICE Sentinel, NICE Real-Time Solution
Release	NICE Interaction Management R4.1 NICE Engage Platform R6.x **NOTE:** NICE Engage Platform 6.x environments with Engage Search, require Internet Explorer 10 or above. NICE Sentinel: - NICE Sentinel Server: R2.1, R2.5, R4.1, R6.X - NICE Sentinel Remote Client: R4.1, R6.X. **NOTE:** Internet Explorer works with Sentinel Remote Client only when using compatibility mode (Compatibility mode is the Microsoft Internet Explorer default mode). For more information, see the *Sentinel Installation and Configuration Guide*. Real-Time Solution 4.9.x
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 Interaction Management Release 4.1

- NICE Engage Platform 6.x
- NICE Sentinel
    - Release 2.1
    - Release 2.5
    - Release 4.1
    - Release 6.X

Conclusions

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

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

See NICE Web Applications Known Issues with Internet Explorer 9 below.

NICE Web Applications Known Issues with Internet Explorer 9

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

Issue 1

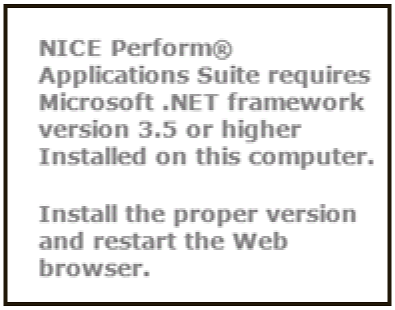
The NICE Engage Platform/NICE Interaction Management Web application URL must be added to the Trusted Site list. See Manually Adding NICE Web Applications to the Trusted Site List on page 147.

Issue 2

NICE Engage Platform/NICE Interaction Management 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 Engage Platform/NICE Interaction Management 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 Web Applications URL to the Local Intranet Site List on page 152.

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 151.

Issue 5

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

Internet Explorer 10

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

Product	NICE Engage Platform, NICE Interaction Management, NICE Sentinel, NICE Real-Time Solutions, Engage Search
Release	NICE Interaction Management 4.1 NICE Engage Platform 6.3 and above NICE Sentinel: ■ NICE Sentinel Server: R2.1, R2.5, R4.1, R6.X ■ NICE Sentinel Remote Client: R4.1, R6.X. **NOTE:** Internet Explorer works with Sentinel Remote Client only when using compatibility mode (Compatibility mode is the Microsoft Internet Explorer default mode). For more information, see the *Sentinel Installation and Configuration Guide*. NICE Real-Time Solution 4.9.6
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 Engage Platform 6.x andNICE Interaction Management Release 4.1.

Conclusions

The NICE Engage Platform/NICE Interaction Management Applications Suites are compatible with all tested operating systems with the following limitations:

- You should only run one NICE Web Applications Suite per browser.

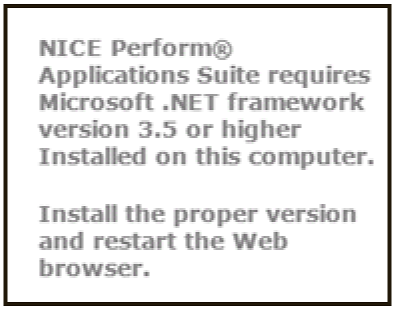
See NICE Web Applications Known Issues with Internet Explorer 10 on the next page.

NICE Web Applications 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. 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 Web Applications URL to the Local Intranet Site List on page 152.

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

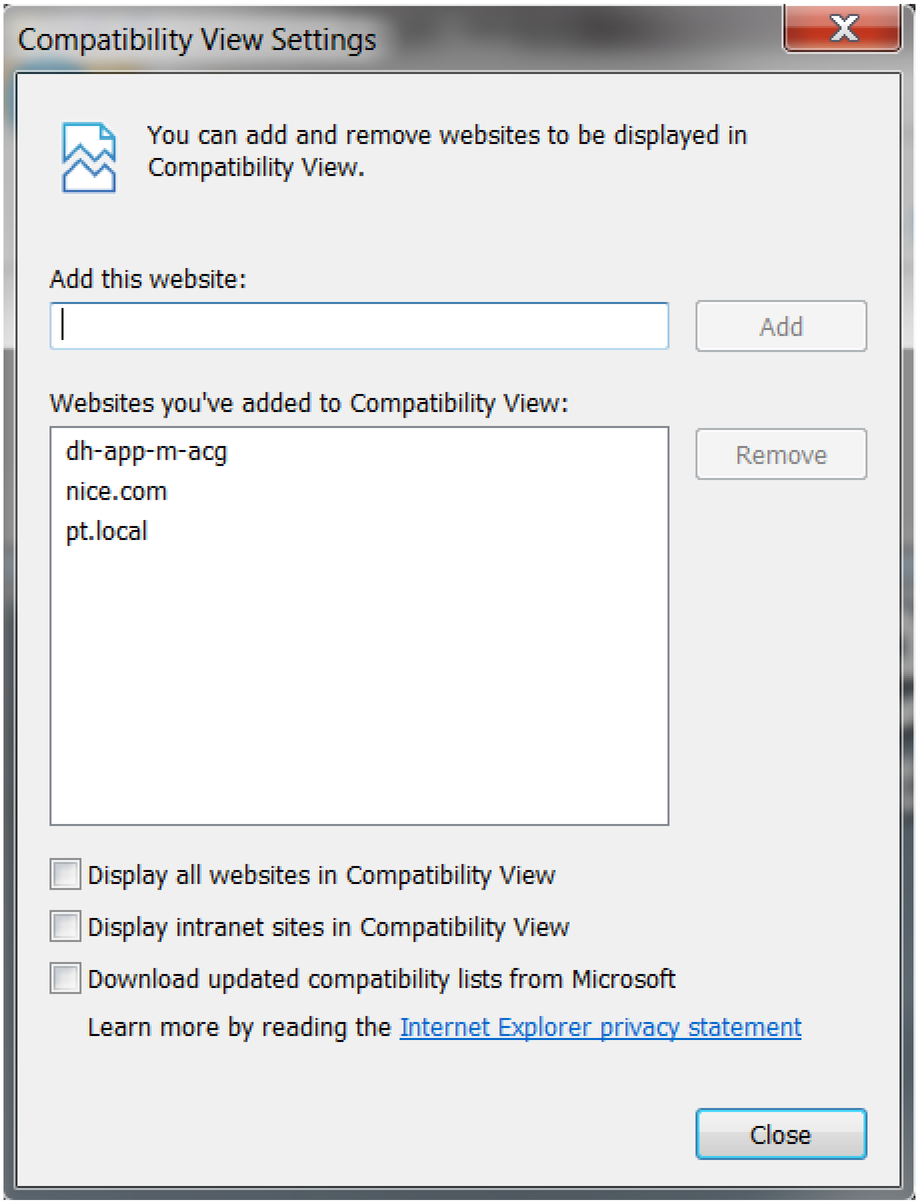
To ensure that NICE Interaction Management works properly when using Microsoft Internet Explorer 10, you should make sure to add the URL from the application server to the Windows Compatibility View settings.

Starting from NICE Engage Platform 6.x, Web Applications do not require working in the Compatibility mode.

To add the NICE Web 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



Compatibility View Settings

You can add and remove websites to be displayed in Compatibility View.

Add this website:

Websites you've added to Compatibility View:

dh-app-m-acg
nice.com
pt.local

□ Display all websites in Compatibility View

□ Display intranet sites in Compatibility View

□ Download updated compatibility lists from Microsoft

Learn more by reading the Internet Explorer privacy statement

2. Type the Application Server URL for the instance of NICE Engage Platform/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 Engage Platform, NICE Interaction Management, NICE Sentinel, NICE Real-Time Solutions, Engage Search
Release	NICE Interaction Management R4.1 NICE Engage Platform R6.3 and above NICE Sentinel: - NICE Sentinel Server: R2.1, R2.5, R4.1, R6.3 - NICE Sentinel Remote Client: R4.1, R6.X. **NOTE:** Internet Explorer works with Sentinel Remote Client only when using compatibility mode (Compatibility mode is the Microsoft Internet Explorer default mode). For more information, see the *Sentinel Installation and Configuration Guide*. NICE Real-Time Solutions 4.9.6
Synopsis	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 Windows Server 2012 R2 Standard 64-bit Windows Server 2012 R2 Datacenter 64-bit

Prerequisite Updates for Internet Explorer 11

During the installation of Internet Explorer 11 for Windows 7 SP1 or Windows Server 2008 R2 SP1, prerequisite components are installed as well. If the prerequisite components cannot be installed, the installation stops. In this case, install the following prerequisite updates manually:

- KB2729094
- KB2731771
- KB2533623

- KB2670838
- KB2786081
- KB2834140

General Description and Conclusions

General tests were performed using Internet Explorer 11 (IE11) with NICE Interaction Management Release 4.1 and NICE Engage Platform 6.x.

Conclusions

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

- Run only one NICE Engage Platform/NICE Interaction Management Applications Suite per browser.
- Use XBAP with the Windows 8.1 and Windows 7 client systems only.
- For Internet Explorer 11 on Windows 8.1 and Windows 7, you must have NICE Engage Platform/NICE Interaction Management Release 4.1.46 or above.

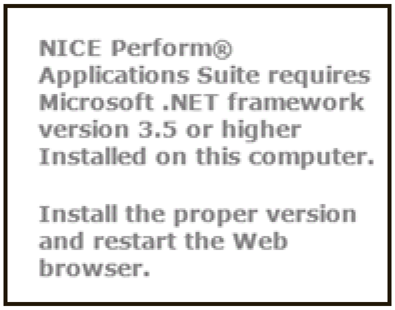
See NICE Web Applications Known Issues with Internet Explorer 11 below.

NICE Web Applications 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 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 Web Application URL to the Compatibility View Settings List on the next page

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

NOTE: Relevant for NICE Interaction Management only.

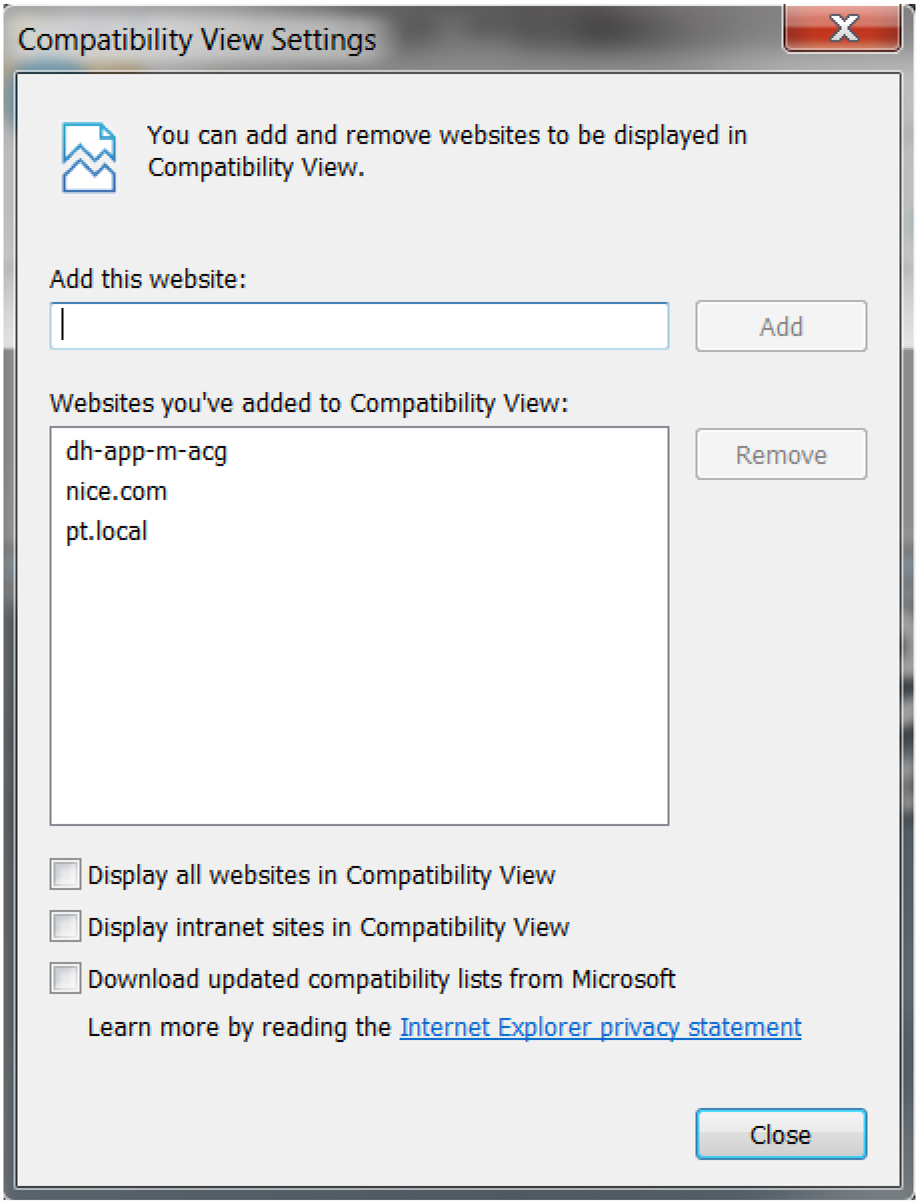
To ensure that NICE Interaction Management works properly when using Microsoft Internet Explorer 11, you should make sure to add the URL from the application server to the Windows Compatibility View settings.

Starting from NICE Engage Platform 6.x, Web Applications do not require working in the Compatibility mode.

➡ To add the NICE 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



Compatibility View Settings

You can add and remove websites to be displayed in Compatibility View.

Add this website:

Websites you've added to Compatibility View:

dh-app-m-acg
nice.com
pt.local

□ Display all websites in Compatibility View

□ Display intranet sites in Compatibility View

□ Download updated compatibility lists from Microsoft

Learn more by reading the Internet Explorer privacy statement

2. In the Add this website field, enter the Application Server URL for the instance of NICE Engage Platform/NICE Interaction Management that you are using. For example, **dh-app-m-acg**.

3. Click **Add**.

[This page intentionally left blank]

Google Chrome with the IE Tab Extension

This section describes compatibility of the Google Chrome browser with the IE Tab Extension with NICE Web Applications.

Contents

Compatibility of NICE Web Applications with the IE Tab Extension in Google Chrome 32/64-bit

Product	NICE Engage Platform, NICE Sentinel, NICE Real-Time Solutions, Engage Search
Release	NICE Engage Platform 6.5 NICE Sentinel: ■ NICE Sentinel Server 6.5 ■ NICE Sentinel Remote Client 6.5.
Synopsis	Windows 10 Pro 32/64-bit Windows 10 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 2012 R2 Standard 64-bit Windows Server 2012 R2 Datacenter 64-bit
IE-Tab extension inGoogle Chrome	IE-Tab 9.5 Google Chrome 49

General Description and Conclusions

General tests were performed using the IE Tab extension in Google Chrome with Engage Platform 6.5.

Conclusions

The NICE Engage Platform is compatible with all tested operating systems with the following limitations:

- You should run only one NICE Engage Platform Applications Suite per browser.
- You should only use the XBAP technology with the Windows 8.1, Windows 10 client systems.

Client Application Compatibility

The following table shows the NICE Engage Platform 6.5 client applications compatible with the IE-Tab extension in Google Chrome.

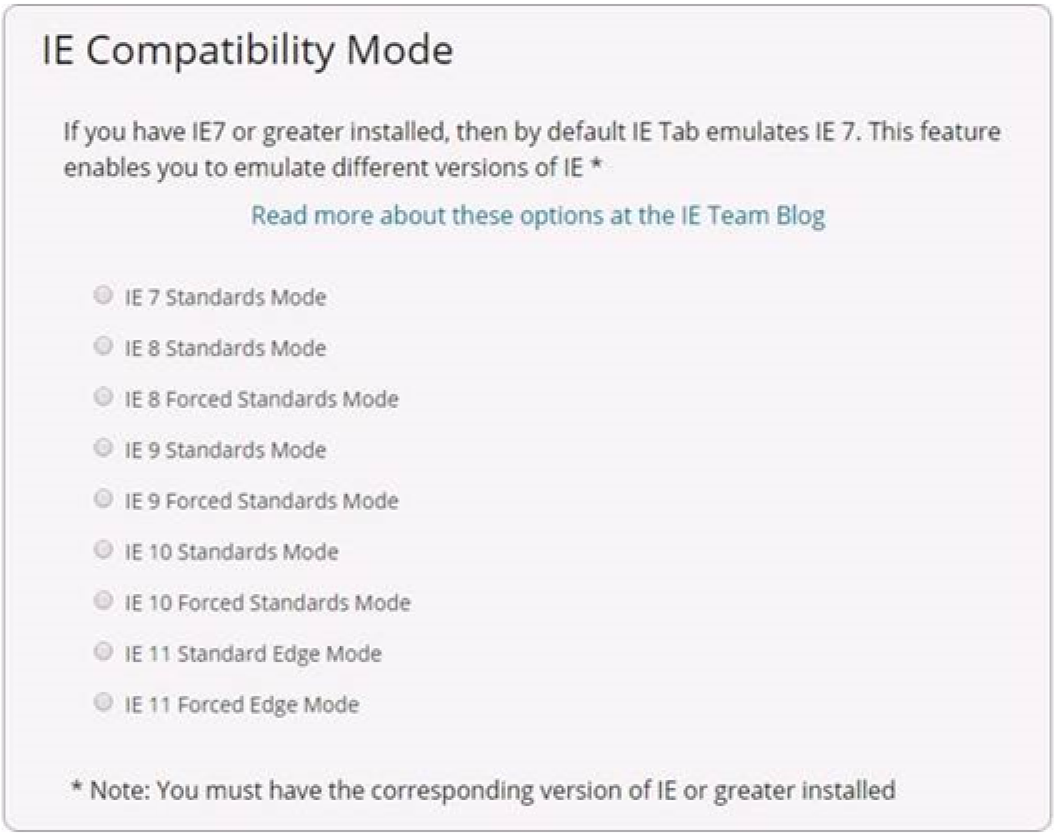
Application	IE Tab (Version 9.5.2.1) Extension in Google Chrome (Version 49.0.2623.112)
Analytics Apps	Approved
NICE Web Applications	Approved
QM Apps	Approved
RTA	Approved
Engage Search	Approved
Reporter	Approved
NICE Sentinel Remote Client	Approved

NICE Web Applications Known Issues with the IE Tab in Google Chrome

Sentinel Web Client doesn’t support Compatibility Mode. However, for IE-Tab it is turned on by default.

To disable the Compatibility Mode:

1. Right-click the IE Tab button and select **Options**.
2. Open the **IE Compatibility Mode** window and select the Internet Explorer version you want Google Chrome to emulate.



IE Compatibility Mode

If you have IE7 or greater installed, then by default IE Tab emulates IE 7. This feature enables you to emulate different versions of IE *

Read more about these options at the IE Team Blog

○ IE 7 Standards Mode

○ IE 8 Standards Mode

○ IE 8 Forced Standards Mode

○ IE 9 Standards Mode

○ IE 9 Forced Standards Mode

○ IE 10 Standards Mode

○ IE 10 Forced Standards Mode

○ IE 11 Standard Edge Mode

○ IE 11 Forced Edge Mode

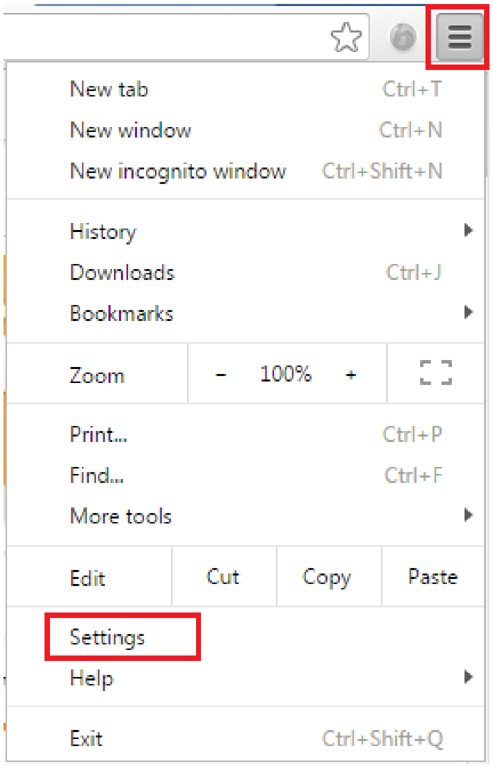
* Note: You must have the corresponding version of IE or greater installed

Adding the IE Tab to Google Chrome

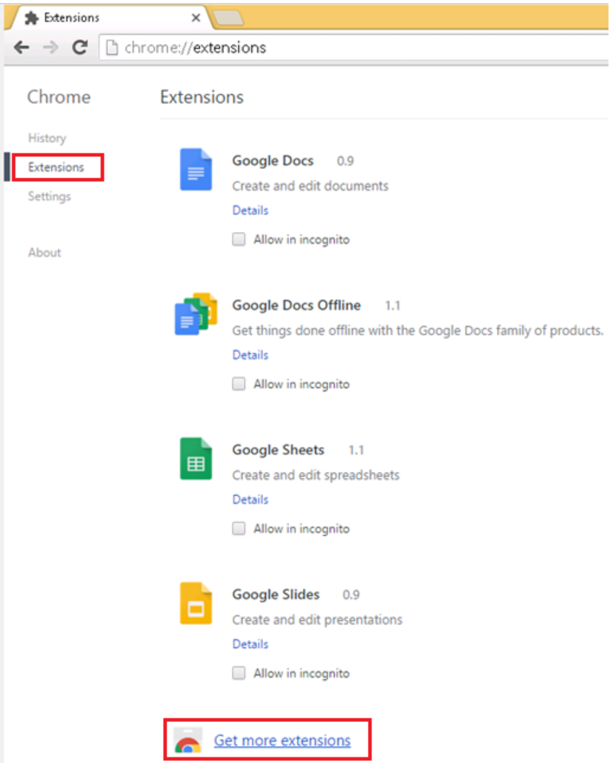
The IE Tab is an extension that allows you to emulate Internet Explorer, while working in Google Chrome.

To add the IE Tab

1. Install and start Google Chrome.
2. Click the **Customize and Control** button and select **Settings**.



3. In the **Settings** window, open the **Extensions** tab and click **Get more extensions**.



Extensions

chrome://extensions

Chrome

History

Extensions

Settings

About

Extensions

Google Docs 0.9
Create and edit documents
Details
□ Allow in incognito

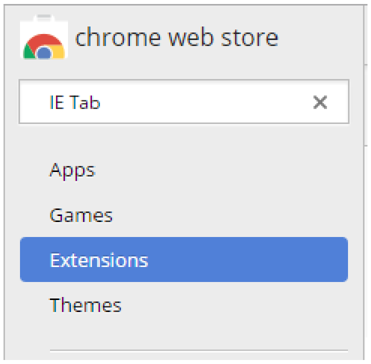
Google Docs Offline 1.1
Get things done offline with the Google Docs family of products.
Details
□ Allow in incognito

Google Sheets 1.1
Create and edit spreadsheets
Details
□ Allow in incognito

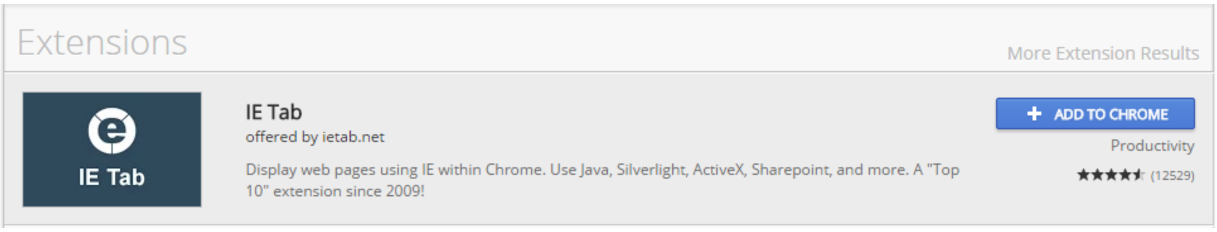
Google Slides 0.9
Create and edit presentations
Details
□ Allow in incognito

Get more extensions

4. In the **Search** field, type in "IE Tab" and press **Enter**.



5. In the Search results, find the IE Tab extension and click **Add to Chrome**.



Extensions

More Extension Results

IE Tab

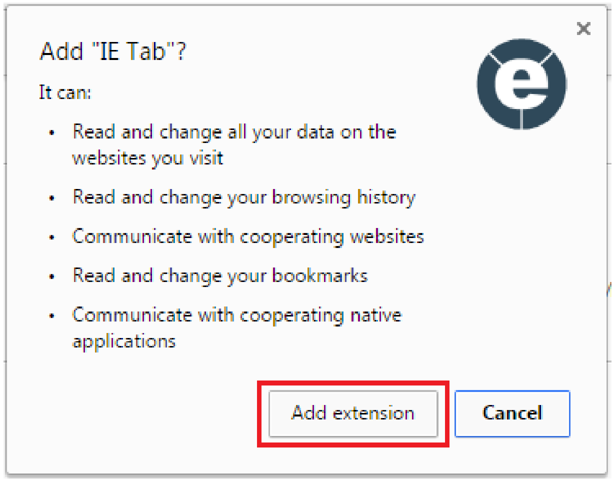
IE Tab
offered by ietab.net
Display web pages using IE within Chrome. Use Java, Silverlight, ActiveX, Sharepoint, and more. A "Top 10" extension since 2009!

+ ADD TO CHROME

Productivity

★★★★★ (12529)

6. In the menu that appears, click **Add extension**.

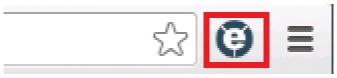


Add "IE Tab"?

It can:

- Read and change all your data on the websites you visit
- Read and change your browsing history
- Communicate with cooperating websites
- Read and change your bookmarks
- Communicate with cooperating native applications

After the IE Tab extension is successfully installed, the **IE Tab** button is added to the **Tool** bar.

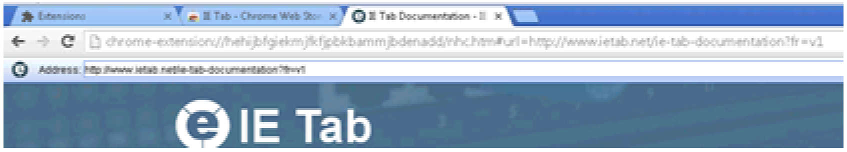


7. Click the **IE Tab** button.

   The **ietabhelper.exe** file is automatically dowloaded.

8. Open the **ietabhelper.exe** file and click **Run**.

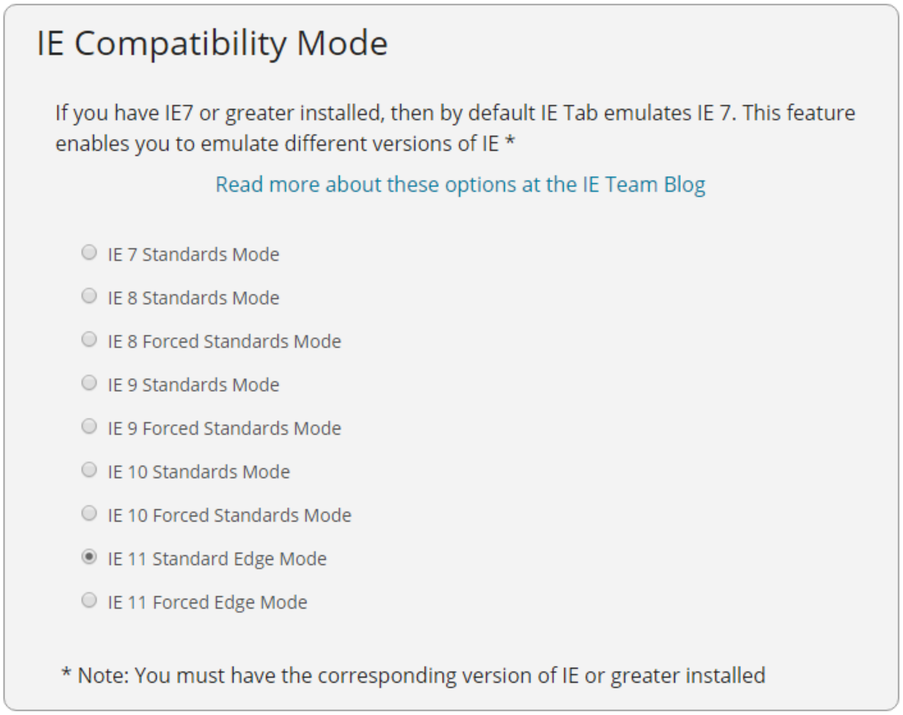
   The IE address bar is added to Google Chrome:



Extensions
IE Tab - Chrome Web Stor
IE Tab Documentation - IE
chrome-extension://hehijbfgiekmjfkfjpbkbammjbdenadd/nhc.htm#url=http://www.ietab.net/ie-tab-documentation?fr=v1
Address: http://www.ietab.net/ie-tab-documentation?fr=v1
IE Tab

9. Click the Settings button (⚒).

   The **IE Tab Options and Settings** window opens.



IE Compatibility Mode

If you have IE7 or greater installed, then by default IE Tab emulates IE 7. This feature enables you to emulate different versions of IE *

Read more about these options at the IE Team Blog

○ IE 7 Standards Mode
○ IE 8 Standards Mode
○ IE 8 Forced Standards Mode
○ IE 9 Standards Mode
○ IE 9 Forced Standards Mode
○ IE 10 Standards Mode
○ IE 10 Forced Standards Mode
● IE 11 Standard Edge Mode
○ IE 11 Forced Edge Mode

* Note: You must have the corresponding version of IE or greater installed

10. Scroll down to the **IE Compatibility Mode** area and select **IE 11 Standard Edge Mode**.

7

Microsoft .NET Framework

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

Contents

NICE Support for Microsoft .NET Framework

Product	.NET Framework Support
Release	NICE Interaction Management 4.1, NICE Engage Platform 6.x, NICE Sentinel 2.5, 4.1 and 6.x
Synopsis	This section describes support for Microsoft .NET Framework (versions 1.1, 2.0, 3.0, 3.5, 4.0, 4.5.2 and 4.6/4.6.1/4.6.2) by NICE products, from V8.9 system through NICE Interaction Management 4.1, NICE Engage Platform6.x, NICE Sentinel 2.5, 4.1 and 6.x. 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, 3.5, 4.0, 4.5.2 and 4.6/4.6.1).

NICE Logger Requirements

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

- Logger PCI 9.01 Service Pack 8 and above
- Logger PCI 9.03 Service Pack 3 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, 4.0, 4.5.2 and 4.6/4.6.1)

Table 7-1:
NICE Release Versions support Microsoft .NET Framework - Server-Side

Release Version	Status
	Approved for all environments, except Playback Organizer version 2.

Table 7-1: NICE Release Versions support Microsoft .NET Framework - Server-Side (continued)

Release Version	Status
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 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 Service Pack 1 is approved. .NET 4.0 is approved. .NET 4.5 is approved. .NET 4.5.1/4.5.2 is approved*. .NET 4.6/4.6.1/4.6.2 is approved.
NICE Engage Platform 6.x	.NET 3.5 Service Pack 1 is required. .NET 4.0 is required. .NET 4.5 is approved*. .NET 4.5.1 is approved*. .NET 4.5.2 is approved*. (Engage 6.4 and below) .NET Framework 4.6./4.6.1/4.6.2 is approved. (Engage 6.5 and above) .NET 4.6./4.6.1/4.6.2 Framework is required.
NICE Sentinel 2.5	.NET 3.5 is required. .NET 3.5 Service Pack 1 is required. .NET 4.0 is required.
NICE Sentinel 4.1	.NET 3.5 is required. .NET 3.5 Service Pack 1 is required. .NET 4.0 is required. .NET 4.5 is approved*

Table 7-1: NICE Release Versions support Microsoft .NET Framework - Server-Side (continued)

Release Version	Status
NICE Sentinel 6.x	.NET 3.5 Service Pack 1 is required. .NET 4.5 is required. .NET 4.5.1/4.5.2 is approved .NET 4.6/4.6.1 is approved.

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, 4.0, 4.5, 4.5.1, 4.5.2 and 4.6/4.6.1).

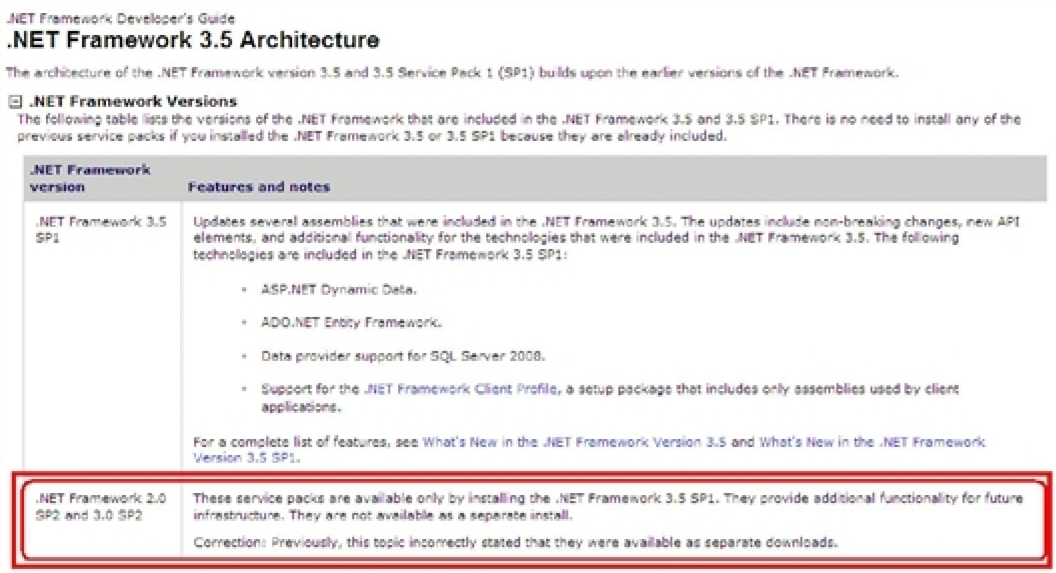
Table 7-2:
NICE Release Versions support Microsoft .NET Framework - Client-Side

Release Version	Status
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 Service Pack 1 is approved. .NET 4.0 is approved. .NET 4.5 is approved. .NET 4.5.1/4.5.2 is approved*. .NET 4.6/4.6.1/4.6.2 is approved.

Table 7-2: NICE Release Versions support Microsoft .NET Framework - Client-Side (continued)

Release Version	Status
NICE Engage Platform 6.x	.NET 3.5 Service Pack 1 is required. .NET 4.0 is required. .NET 4.5 is approved*. .NET 4.5.1 is approved*. .NET 4.5.2 is approved*. (Engage 6.4 and below) .NET Framework 4.6./4.6.1/4.6.2 is approved. (Engage 6.5 and above) .NET 4.6./4.6.1/4.6.2 Framework is required.
NICE Sentinel 2.5	.NET 2.0 is required. .NET 3.5 is required. .NET 3.5 Service Pack 1 is approved. .NET 4.0 is approved.
NICE Sentinel 4.1	.NET 3.5 is required. .NET 3.5 Service Pack 1 is approved. .NET 4.0 is approved. .NET 4.5 is approved*
NICE Sentinel 6.x	.NET 3.5 Service Pack 1 is required. .NET 4.5 is required. .NET 4.5.1/4.5.2 is approved. .NET 4.6/4.6.1 is approved.

Figure 7-1: .NET Framework Developer’s Guide



.NET Framework Developer's Guide

.NET Framework 3.5 Architecture

The architecture of the .NET Framework version 3.5 and 3.5 Service Pack 1 (SP1) builds upon the earlier versions of the .NET Framework.

⊟ .NET Framework Versions

The following table lists the versions of the .NET Framework that are included in the .NET Framework 3.5 and 3.5 SP1. There is no need to install any of the previous service packs if you installed the .NET Framework 3.5 or 3.5 SP1 because they are already included.

.NET Framework version	Features and notes
.NET Framework 3.5 SP1	Updates several assemblies that were included in the .NET Framework 3.5. The updates include non-breaking changes, new API elements, and additional functionality for the technologies that were included in the .NET Framework 3.5. The following technologies are included in the .NET Framework 3.5 SP1: • ASP.NET Dynamic Data. • ADO.NET Entity Framework. • Data provider support for SQL Server 2008. • Support for the .NET Framework Client Profile, a setup package that includes only assemblies used by client applications. For a complete list of features, see What's New in the .NET Framework Version 3.5 and What's New in the .NET Framework Version 3.5 SP1.
.NET Framework 2.0 SP2 and 3.0 SP2	These service packs are available only by installing the .NET Framework 3.5 SP1. They provide additional functionality for future infrastructure. They are not available as a separate install. Correction: Previously, this topic incorrectly stated that they were available as separate downloads.

Microsoft .NET Framework 4.0 Requirements

> **NOTE:** Only relevant for NICE Interaction Management 4.1/NICE Engage Platform 6.x and NICE Sentinel 2.5/NICE Sentinel 4.1.

Microsoft .NET Framework 4.0 is now required for all NICE Interaction Management 4.1 /NICE Engage Platform 6.x sites and NICE Sentinel 2.5/Sentinel 4.1. 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.

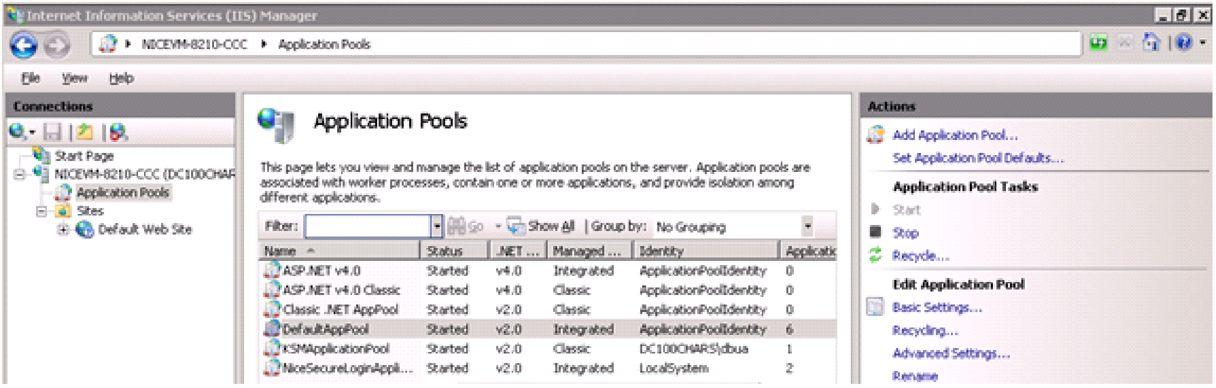
If IIS is installed after Microsoft .NET Framework 4, change the Application Pool to .NET2 as described below.

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 7-2: Internet Information Services (IIS) Manager Window



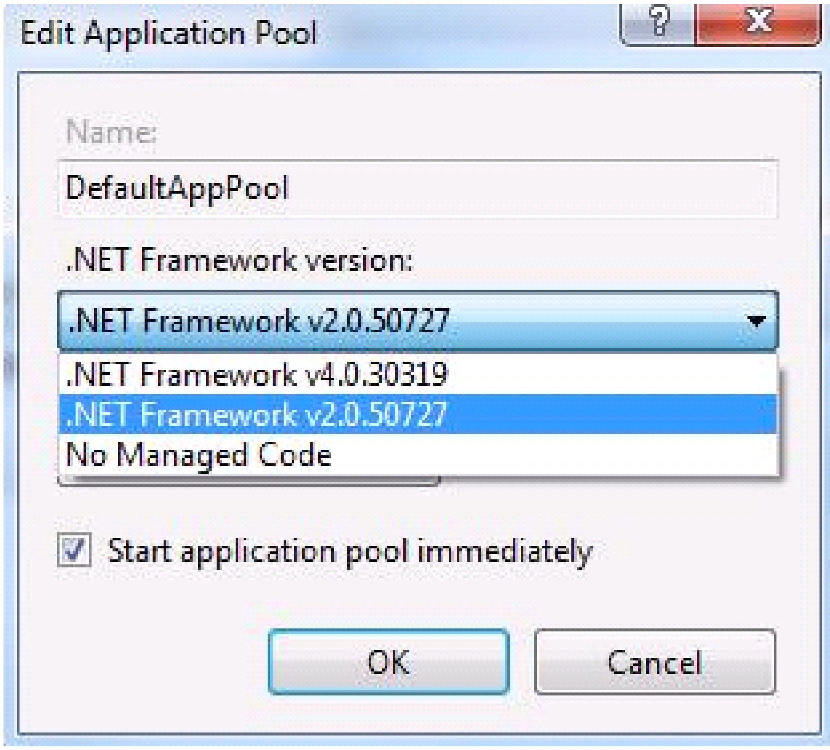
Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET ...	Managed ...	Identity	Applicatio
ASP.NET v4.0	Started	v4.0	Integrated	ApplicationPoolIdentity	0
ASP.NET v4.0 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	0
Classic .NET AppPool	Started	v2.0	Classic	ApplicationPoolIdentity	0
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIdentity	6
KSMApplicationPool	Started	v2.0	Classic	DC100CHARS\dbua	1
NiceSecureLoginAppli...	Started	v2.0	Integrated	LocalSystem	2

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 7-3: Edit Application Pool Window



Edit Application Pool

Name: DefaultAppPool

.NET Framework version: .NET Framework v2.0.50727

☑ Start application pool immediately

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 4.0 and up with NICE Interaction Management 4.1.46 and Above

NOTE: Relevant for NICE Interaction Management 4.1.46 and NICE Engage Platform 6.x.

If your client machine has the Microsoft .NET Framework version 4.0 and up, when you sign in to NICE Interaction Management/NICE Engage Platform, 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/NICE Engage Platform in compatibility mode, see Adding the NICE Web Application URL to the Compatibility View Settings List on page 158.
- If you changed your system configuration to work with .NET Version 4.5/4.5.1/4.5.2 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/NICE Engage Platform.
- 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/NICE Engage Platform 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 Engage Platform 6.x 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*.

Microsoft .NET Framework 4.5 Requirements

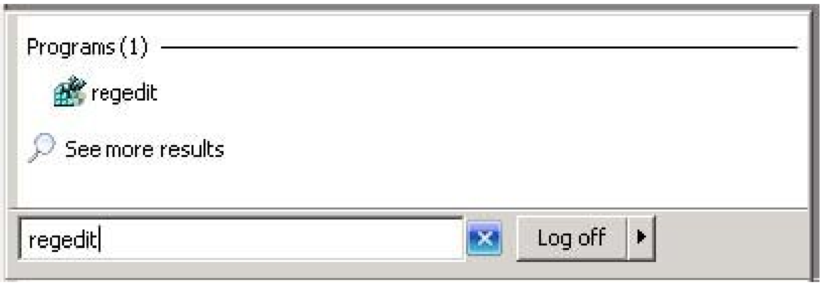
NICE Interaction Management 4.1 and NICE Engage Platform 6.x support Microsoft .NET Framework version 4.5/4.5.1/4.5.2.

Login Issues

Due to login issues, it is required to add the EnableIEHosting registry key to all machines where .NET 4.5 is installed. For more details, see the Microsoft article Application Compatibility in the .NET Framework 4.5. See the *Certified Servers Guide* for a list of the machines where it is required to add the registry key.

➡ To fix login issues:

1. Click **Start**>**Search**, and in the search field, type **Regedit**.
   Figure 7-4: Regedit Search Results



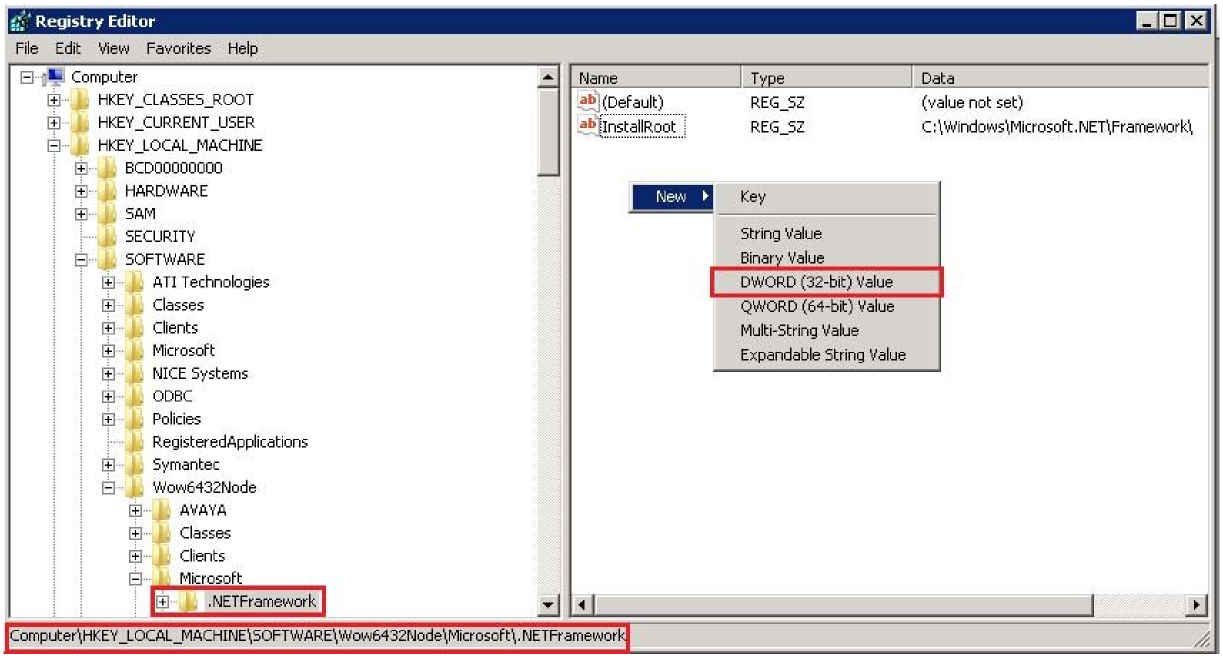
2. Right-click the **Regedit** icon and select **Run as Administrator** from the menu.
3. Enter the correct user credentials for working with registries.
4. Follow the link mentioned above to find the required registry folder.

NOTE: The registry path is different for x86 and x64 Windows systems: ·

- **For x86 systems or for 32-bit processes on x64 systems:** Go to the HKLM/SOFTWARE/MICROSOFT/.NETFramework registry key and change the **EnableIEHosting** value to **1**.
- **For x64 systems or for 64-bit processes on x64 systems:** Go to the HKLM/SOFTWARE/Wow6432Node/.NETFramework registry key and change the **EnableIEHosting** value to **1**.

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

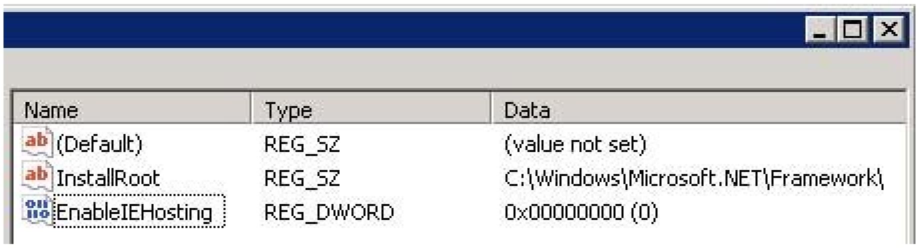
Figure 7-5: Creating a New DWORD Value Key in the .NET Framework Registry



Name	Type	Data
(Default)	REG_SZ	(value not set)
InstallRoot	REG_SZ	C:\Windows\Microsoft.NET\Framework\

6. Rename the new key as follows: **EnableIEHosting**

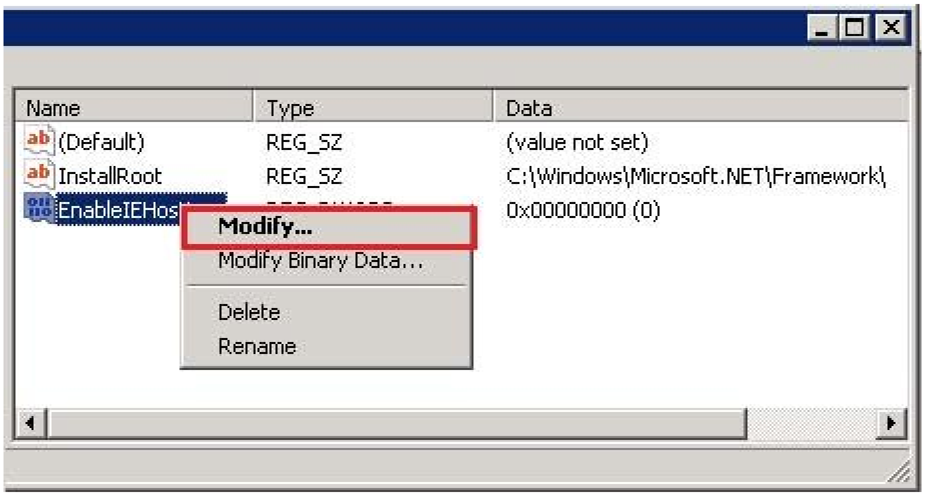
Figure 7-6: New EnableIEHosting DWORD



Name	Type	Data
(Default)	REG_SZ	(value not set)
InstallRoot	REG_SZ	C:\Windows\Microsoft.NET\Framework\
EnableIEHosting	REG_DWORD	0x00000000 (0)

7. Right-click the EnableIEHosting key and select **Modify** from the menu.

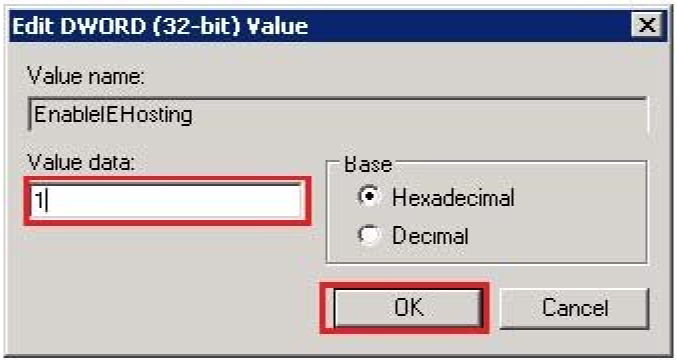
Figure 7-7: Modify New EnableIEHosting DWORD



Name	Type	Data
(Default)	REG_SZ	(value not set)
InstallRoot	REG_SZ	C:\Windows\Microsoft.NET\Framework\
EnableIEHos		0x00000000 (0)

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

Figure 7-8: DWORD Value



Edit DWORD (32-bit) Value

Value name: EnableIEHosting

Value data: 1

Base

● Hexadecimal

○ Decimal

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 4.6 Requirements

NICE Engage Platform 6.5 and up requires Microsoft .NET Framework version 4.6. .NET Framework version 4.6 must be installed on all servers and clients in the site. See *Certified Servers Guide* for a complete list.

Ensuring the Correct XBAP Version

In order for .NET Framework 4.6 to work optimally with XBAP, the newest version of XBAP must be installed. If updating a previous version of NICE Engage Platform to Release 6.5, it is required to delete the previously installed XBAP version. At the next login, the new version of XBAP will be installed automatically.

➡ To ensure the correct XBAP version:

- Navigate to **C:\Users\<username>\AppData\Local**, and delete the **Apps** folder.

  At the next login to NICE Engage Platform, the new version of XBAP will be installed automatically.

[This page intentionally left blank]

8

Microsoft SQL Server

This section 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®, NICE Sentinel
Release	NICE Perform Release 3 NICE Sentinel 2.1
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).

Table 8-2: SQL Server Licenses (continued)

SQL Server License	Price List Item	Description
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 194 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, NICE Sentinel
Release	NICE Perform Release 3.x NICE Interaction Management Release 4.1 NICE Sentinel 2.x NICE Sentinel 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 214.

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.

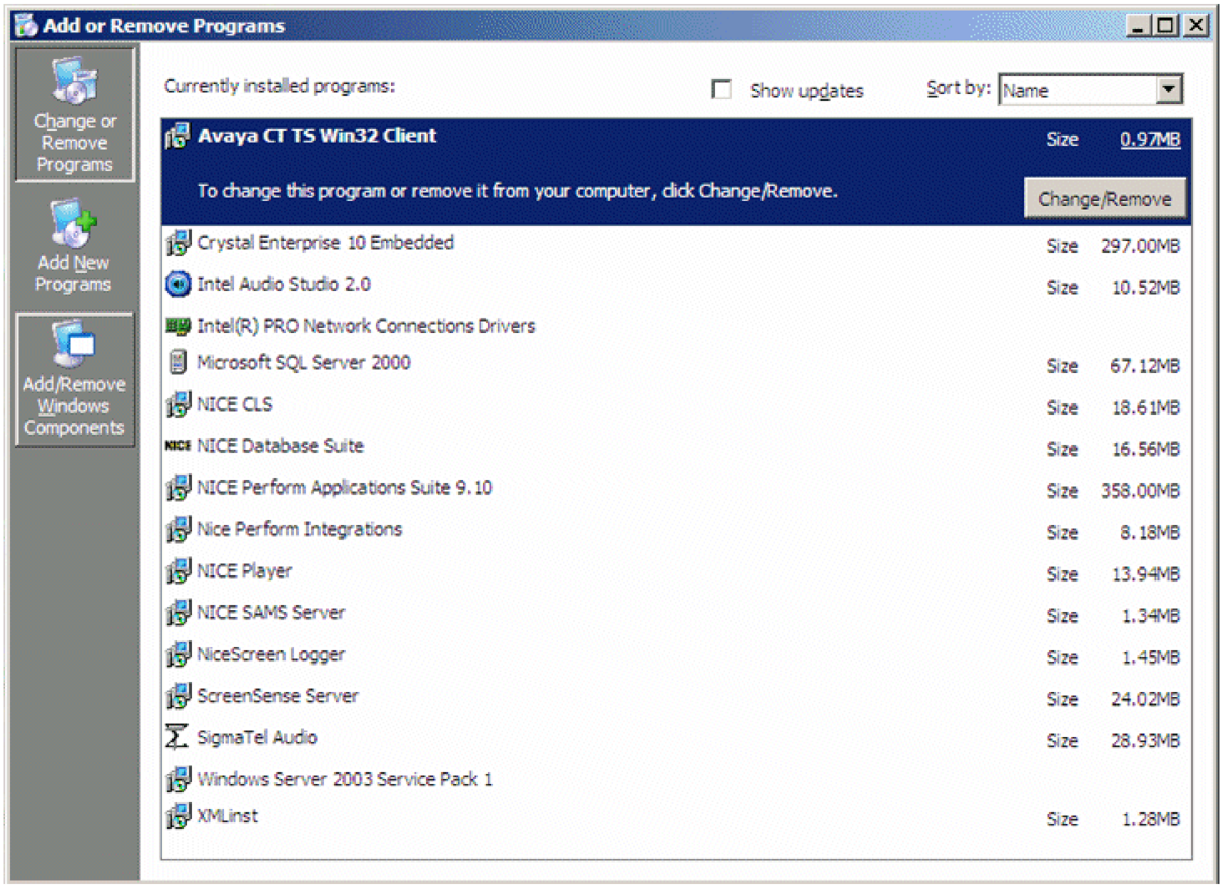
Removing the Network Distribute Transaction Coordinator (DTC) Access

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


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
□ Show updates
Sort by: Name
Change/Remove

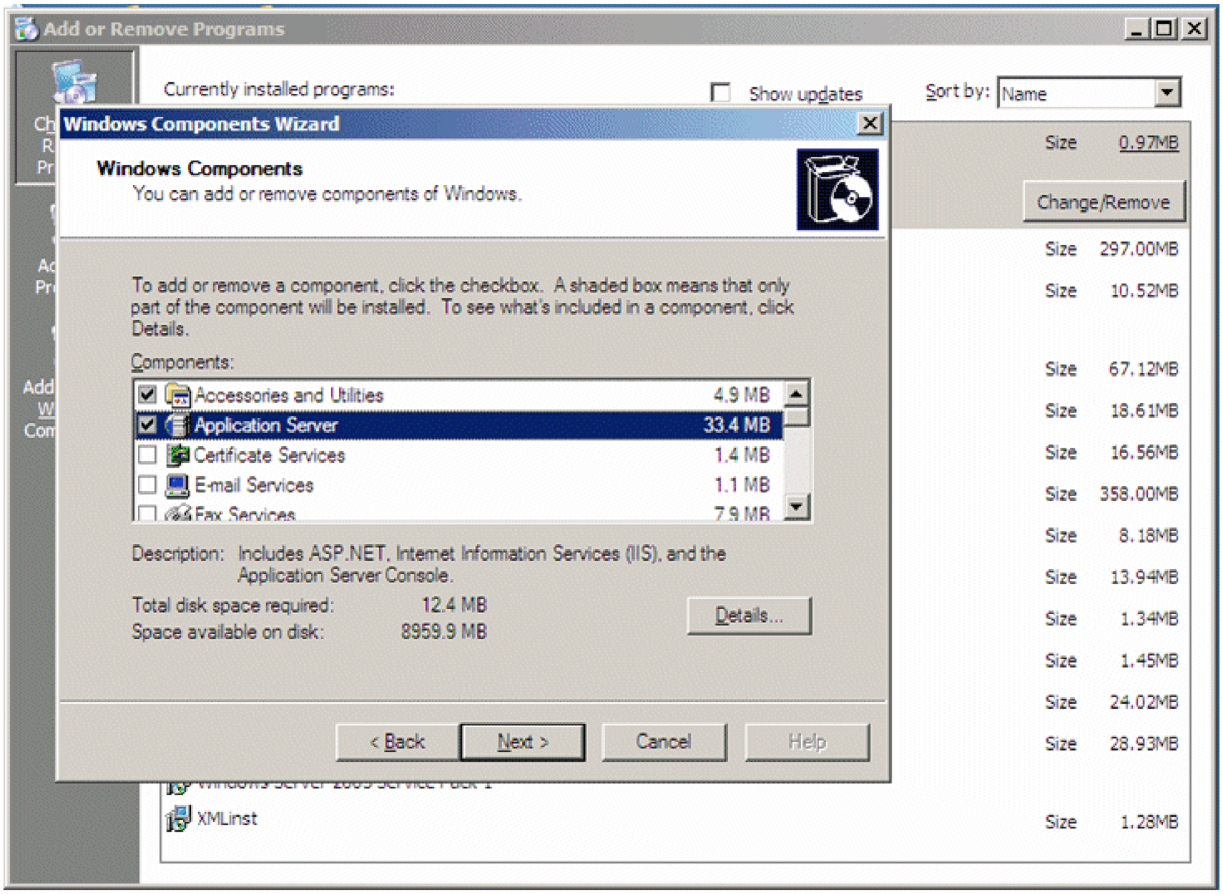
To change this program or remove it from your computer, click Change/Remove.

Avaya CT TS Win32 Client	Size	0.97MB
Crystal Enterprise 10 Embedded	Size	297.00MB
Intel Audio Studio 2.0	Size	10.52MB
Intel(R) PRO Network Connections Drivers		
Microsoft SQL Server 2000	Size	67.12MB
NICE CLS	Size	18.61MB
NICE Database Suite	Size	16.56MB
NICE Perform Applications Suite 9.10	Size	358.00MB
Nice Perform Integrations	Size	8.18MB
NICE Player	Size	13.94MB
NICE SAMS Server	Size	1.34MB
NiceScreen Logger	Size	1.45MB
ScreenSense Server	Size	24.02MB
SigmaTel Audio	Size	28.93MB
Windows Server 2003 Service Pack 1		
XMLinst	Size	1.28MB

2. Click **Add/Remove Windows Components**.

   The Windows Components Wizard starts.

Figure 8-2: Windows Component Wizard



Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ Accessories and Utilities	4.9 MB
☑ Application Server	33.4 MB
□ Certificate Services	1.4 MB
□ E-mail Services	1.1 MB
□ Fax Services	7.9 MB

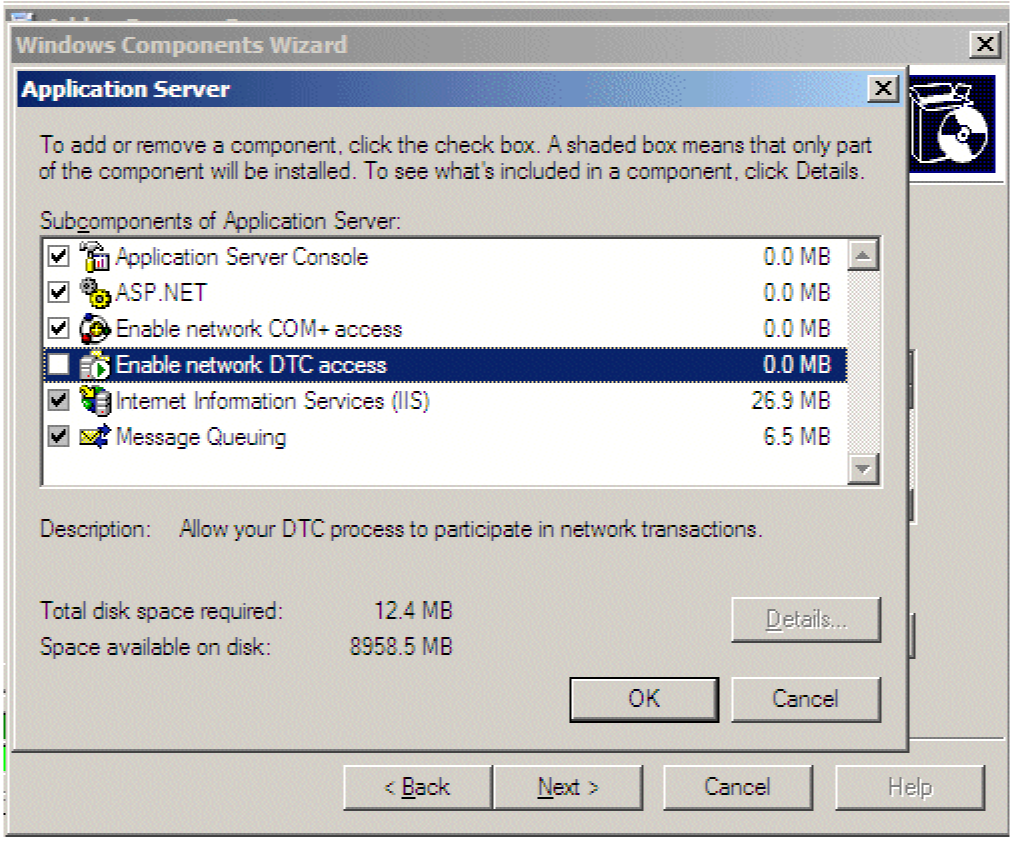
Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console.

Total disk space required: 12.4 MB

Space available on disk: 8959.9 MB

3. In the **Components** list, select **Applications Server**, and click **Details**. The Application Server window appears.

Figure 8-3: Application Server Window



Windows Components Wizard

Application Server

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Application Server:

☑	Application Server Console	0.0 MB
☑	ASP.NET	0.0 MB
☑	Enable network COM+ access	0.0 MB
□	Enable network DTC access	0.0 MB
☑	Internet Information Services (IIS)	26.9 MB
☑	Message Queuing	6.5 MB

Description: Allow your DTC process to participate in network transactions.

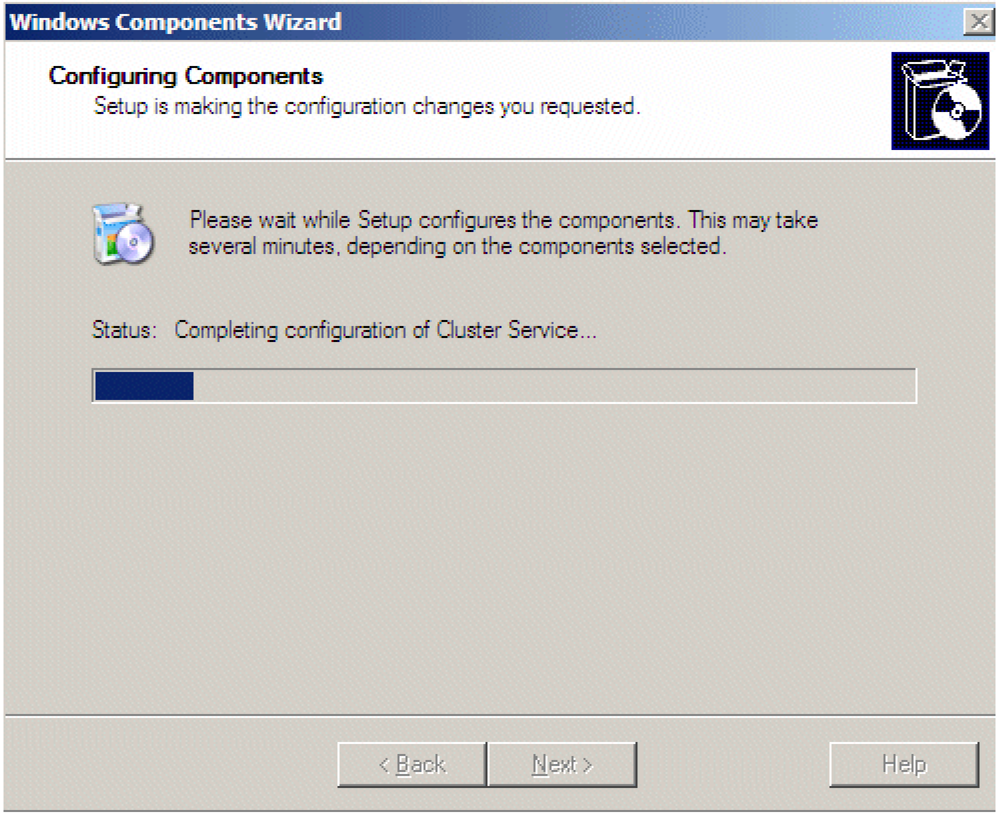
Total disk space required: 12.4 MB
Space available on disk: 8958.5 MB

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



Configuring Components

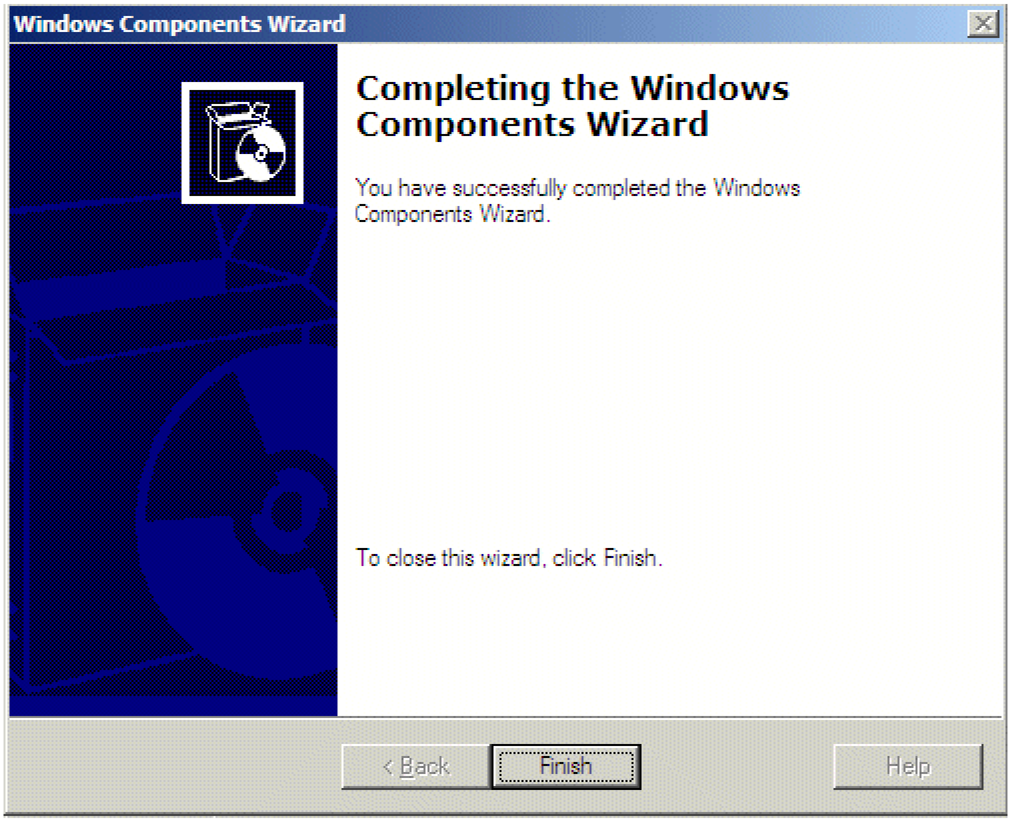
Setup is making the configuration changes you requested.

Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Status: Completing configuration of Cluster Service...

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



Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

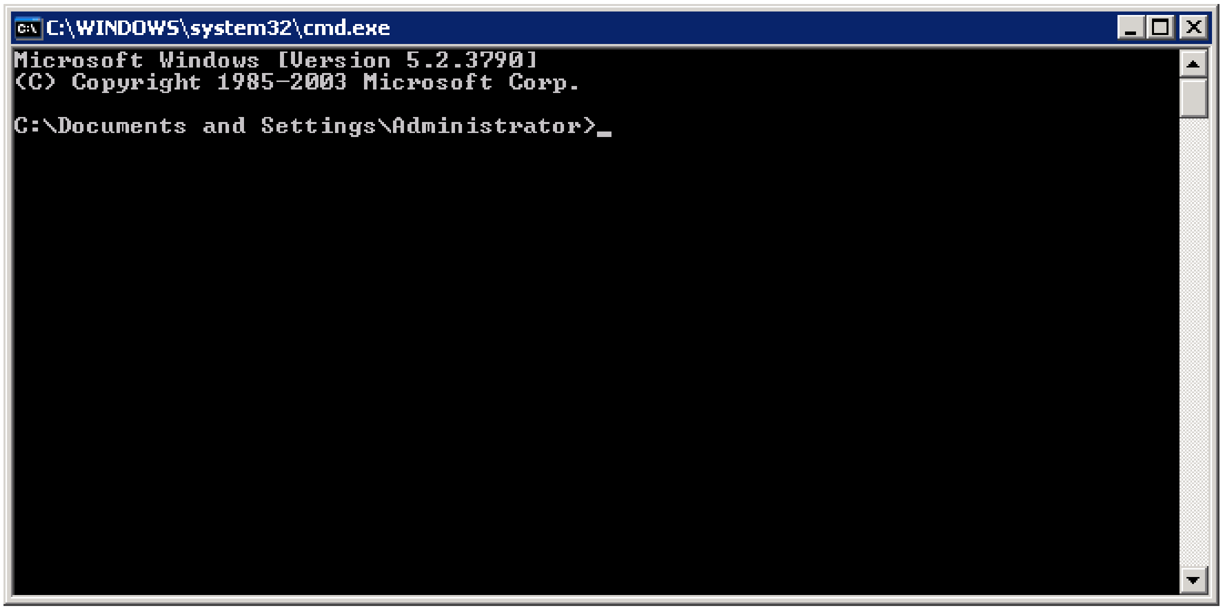
8. Click **Finish** to close the wizard.

Uninstalling the DTC

➡ To uninstall the DTC:

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

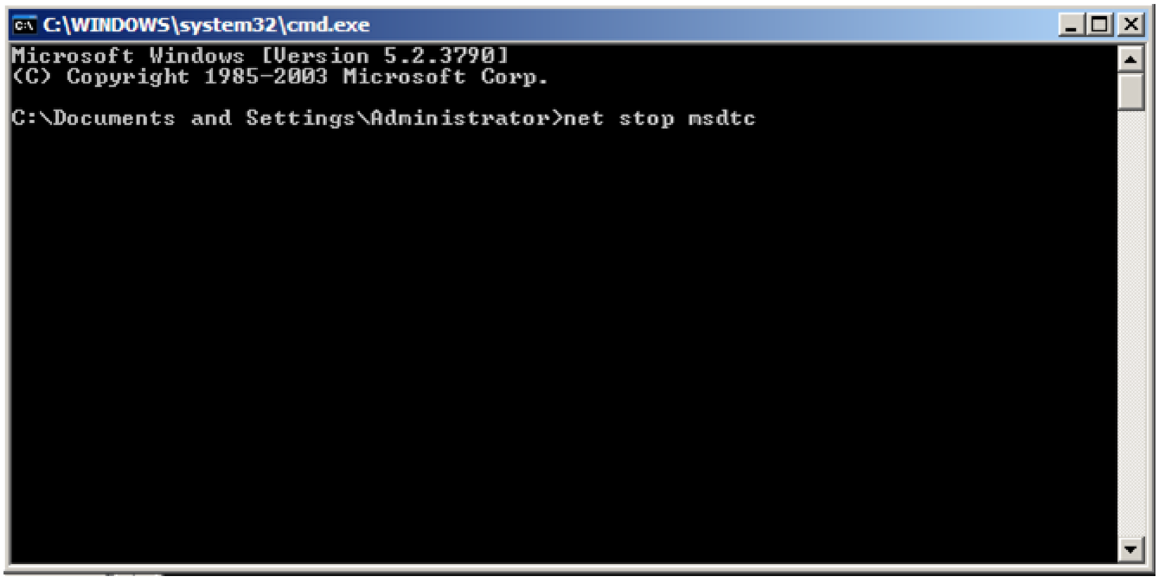
Figure 8-6: C:\WINDOWS\System32\cmd.exe



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>_
```

2. To stop the MSDTC, enter the following command: **net stop msdtc**.

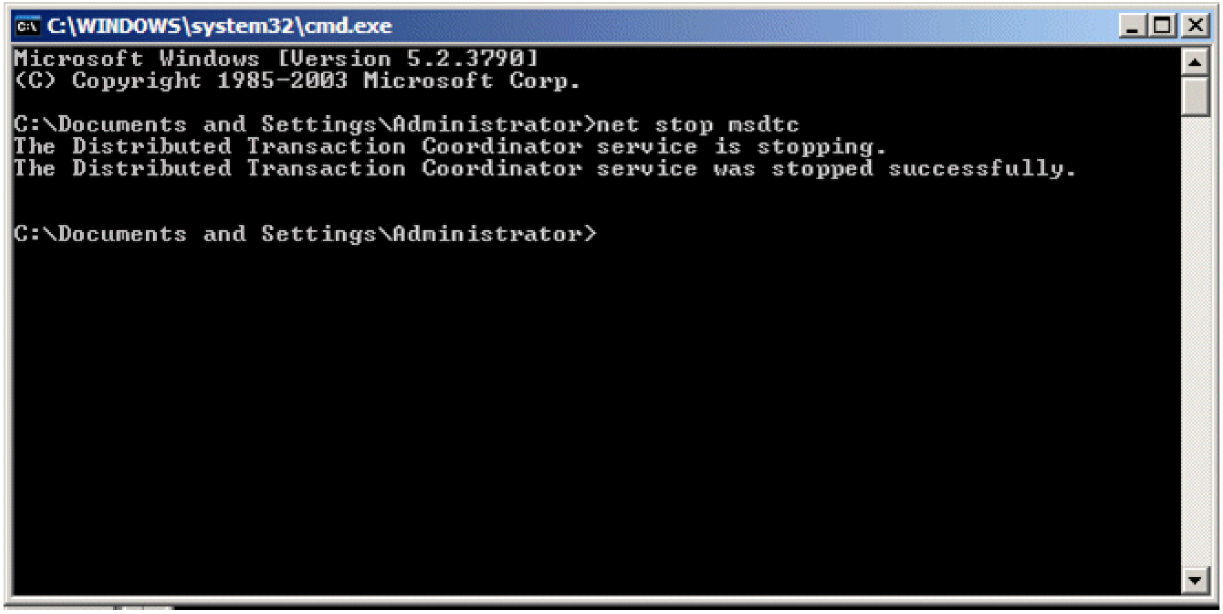
Figure 8-7: C:\WINDOWS\System32\cmd.exe



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net stop msdtc
```

The following window appears.

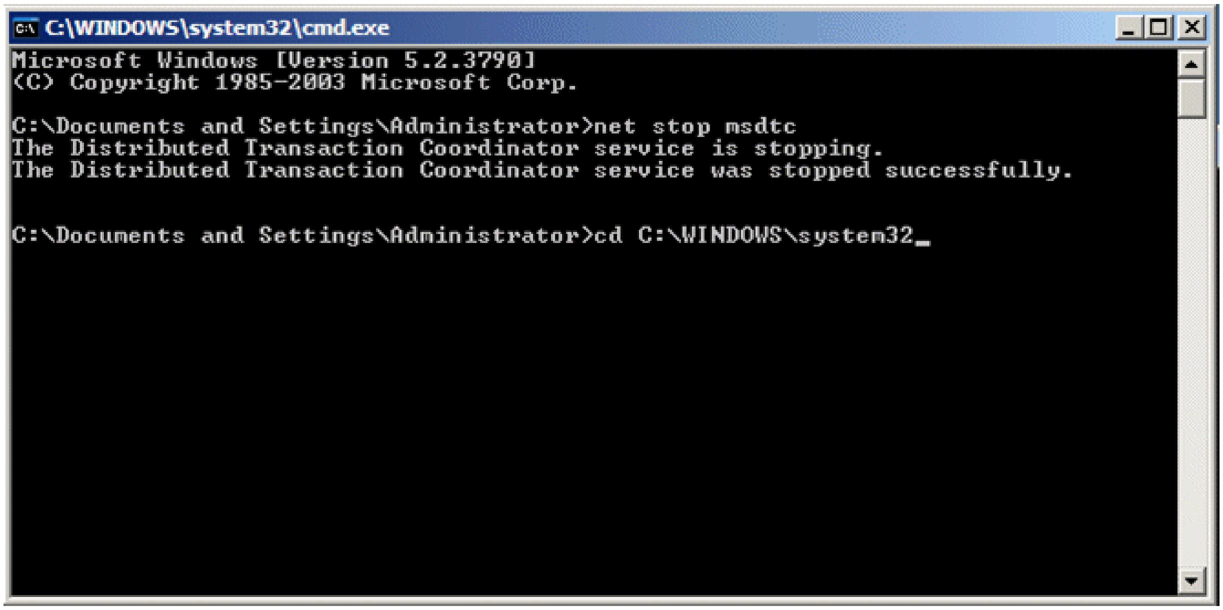
Figure 8-8: C:\WINDOWS\System32\cmd.exe



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net stop msdtc
The Distributed Transaction Coordinator service is stopping.
The Distributed Transaction Coordinator service was stopped successfully.


C:\Documents and Settings\Administrator>
```

3. Change the directory to c:\WINDOWS\system32

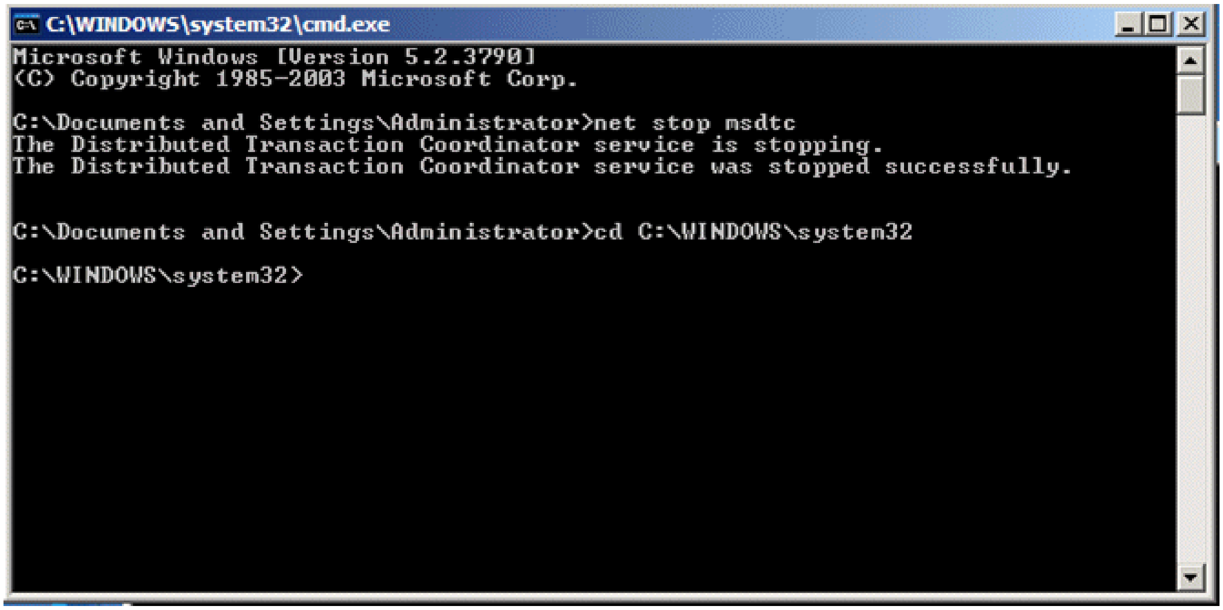
Figure 8-9: C:\WINDOWS\System32\cmd.exe



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net stop msdtc
The Distributed Transaction Coordinator service is stopping.
The Distributed Transaction Coordinator service was stopped successfully.


C:\Documents and Settings\Administrator>cd C:\WINDOWS\system32_
```

The following window appears.

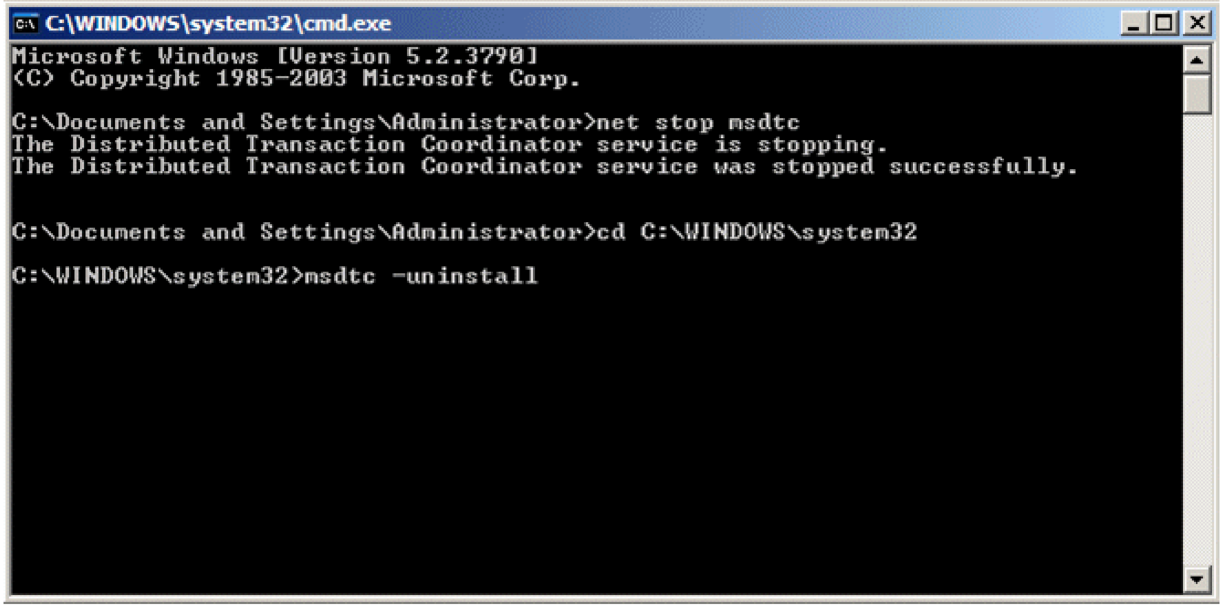
Figure 8-10: C:\WINDOWS\System32\cmd.exe



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net stop msdtc
The Distributed Transaction Coordinator service is stopping.
The Distributed Transaction Coordinator service was stopped successfully.


C:\Documents and Settings\Administrator>cd C:\WINDOWS\system32

C:\WINDOWS\system32>
```

4. Write command **msdtc -uninstall** to uninstall MSDTC, as shown in the following window.

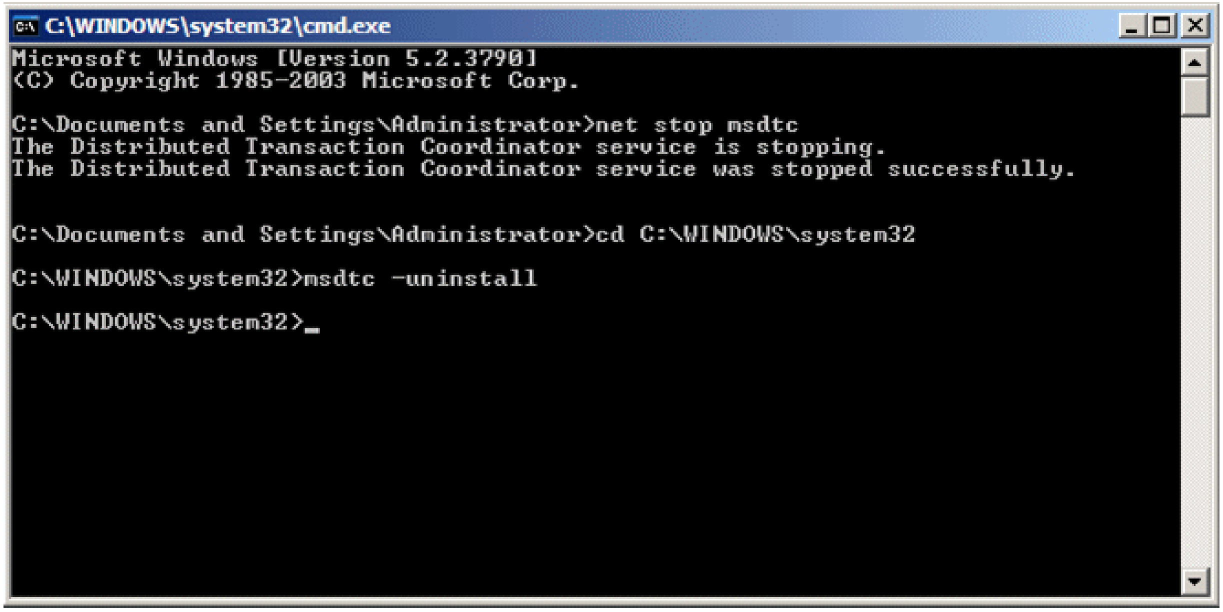
Figure 8-11: C:\WINDOWS\System32\cmd.exe



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net stop msdtc
The Distributed Transaction Coordinator service is stopping.
The Distributed Transaction Coordinator service was stopped successfully.


C:\Documents and Settings\Administrator>cd C:\WINDOWS\system32

C:\WINDOWS\system32>msdtc -uninstall
```

When the uninstall is completed, the following window appears.

Figure 8-12: C:\WINDOWS\System32\cmd.exe

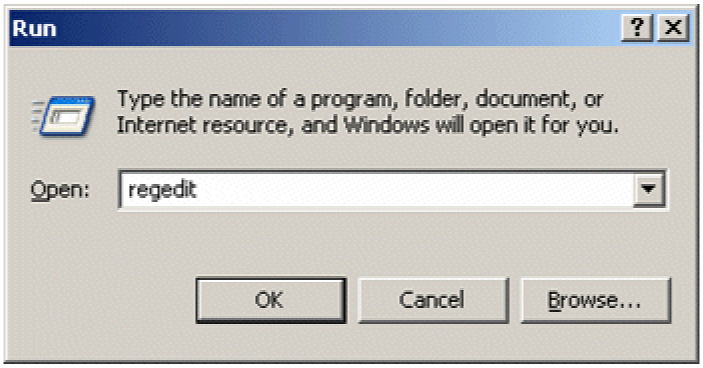


```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net stop msdtc
The Distributed Transaction Coordinator service is stopping.
The Distributed Transaction Coordinator service was stopped successfully.


C:\Documents and Settings\Administrator>cd C:\WINDOWS\system32

C:\WINDOWS\system32>msdtc -uninstall

C:\WINDOWS\system32>_
```

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

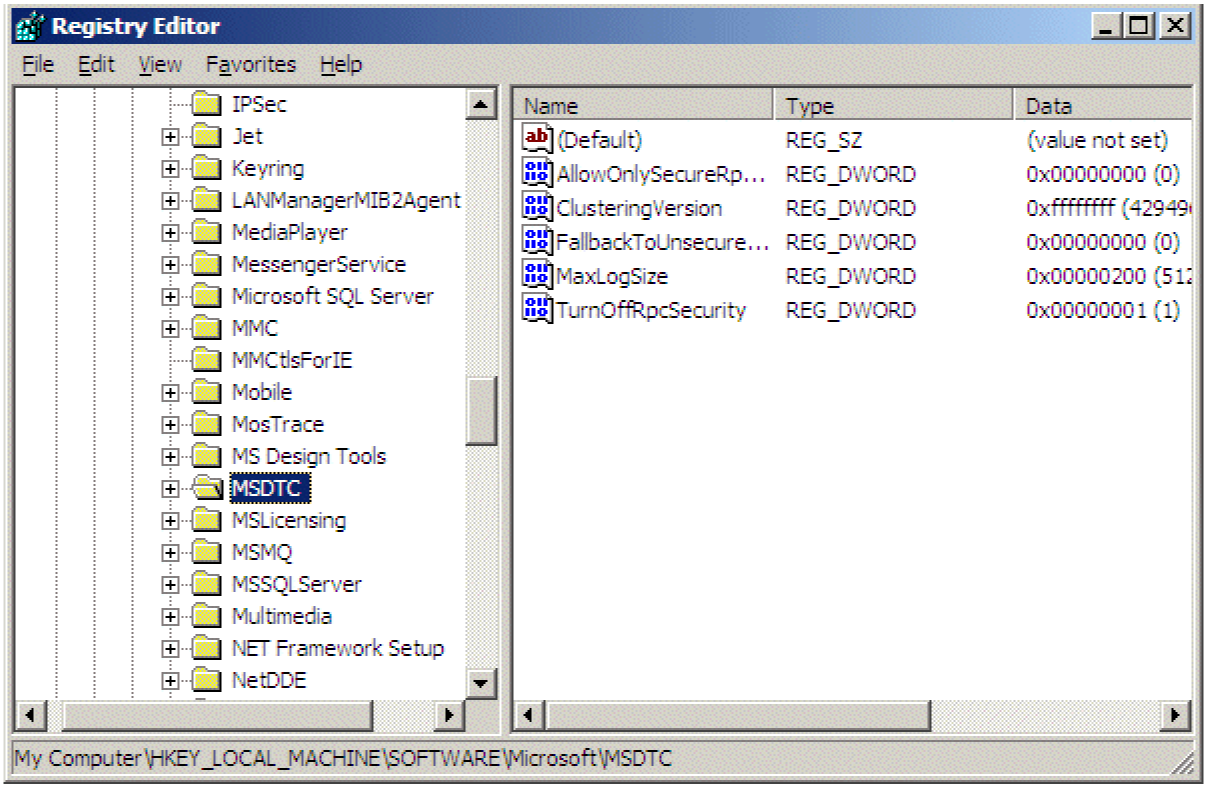


Run
?
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

Open: regedit

2. In the **Open** field, type **regedit** and click **OK**. The Registry Editor window appears.

Figure 8-14: The Registry Editor

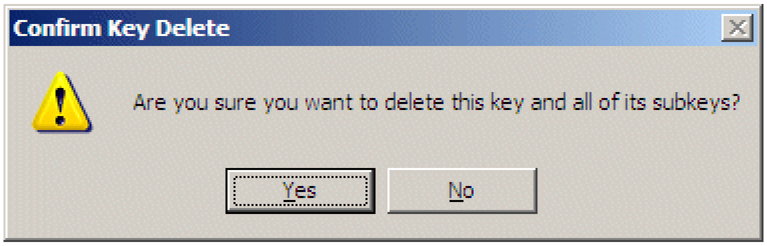


Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowOnlySecureRp...	REG_DWORD	0x00000000 (0)
ClusteringVersion	REG_DWORD	0xffffffff (42949
FallbackToUnsecure...	REG_DWORD	0x00000000 (0)
MaxLogSize	REG_DWORD	0x00000200 (512
TurnOffRpcSecurity	REG_DWORD	0x00000001 (1)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC

3. Right-click **MSDTC**, and select **Delete**. The following dialog box appears.

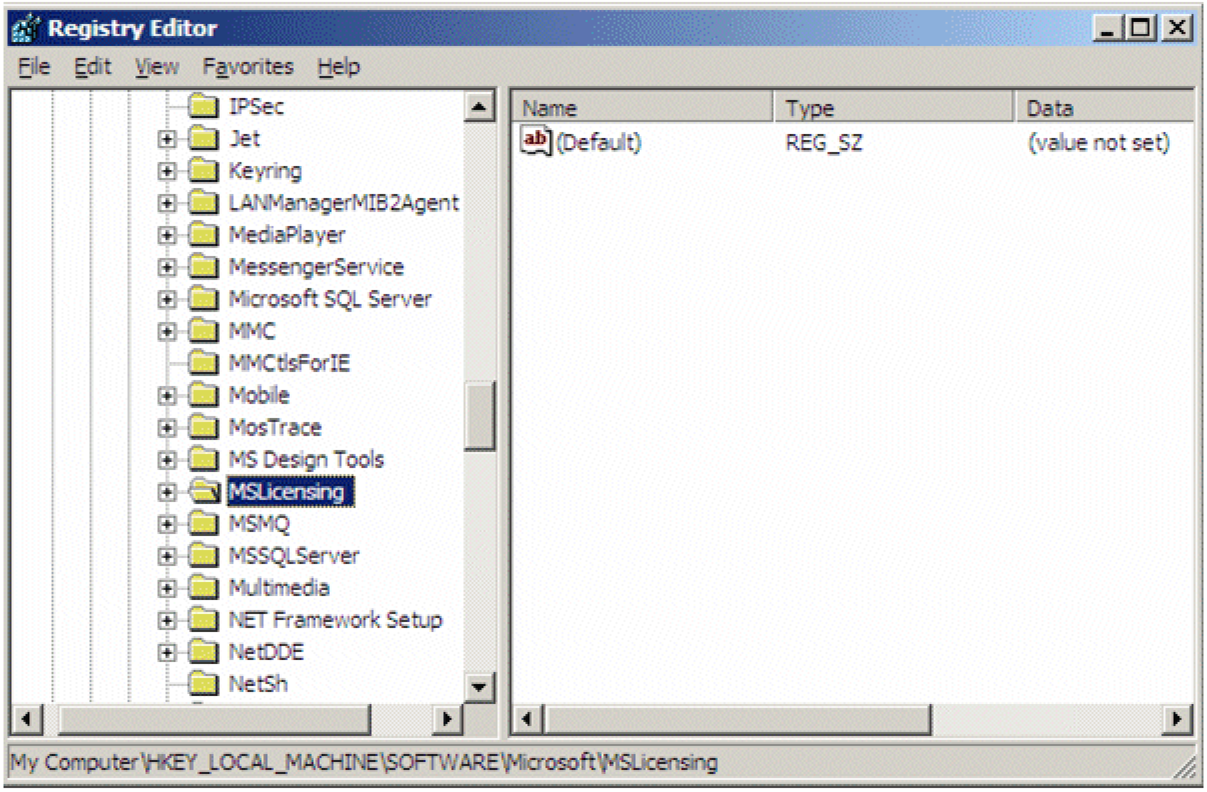
Figure 8-15: Confirm Key Delete Message



Are you sure you want to delete this key and all of its subkeys?

4. Click **Yes**. **MSDTC** is deleted from the Registry Editor.

Figure 8-16: Registry Editor



Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSLicensing

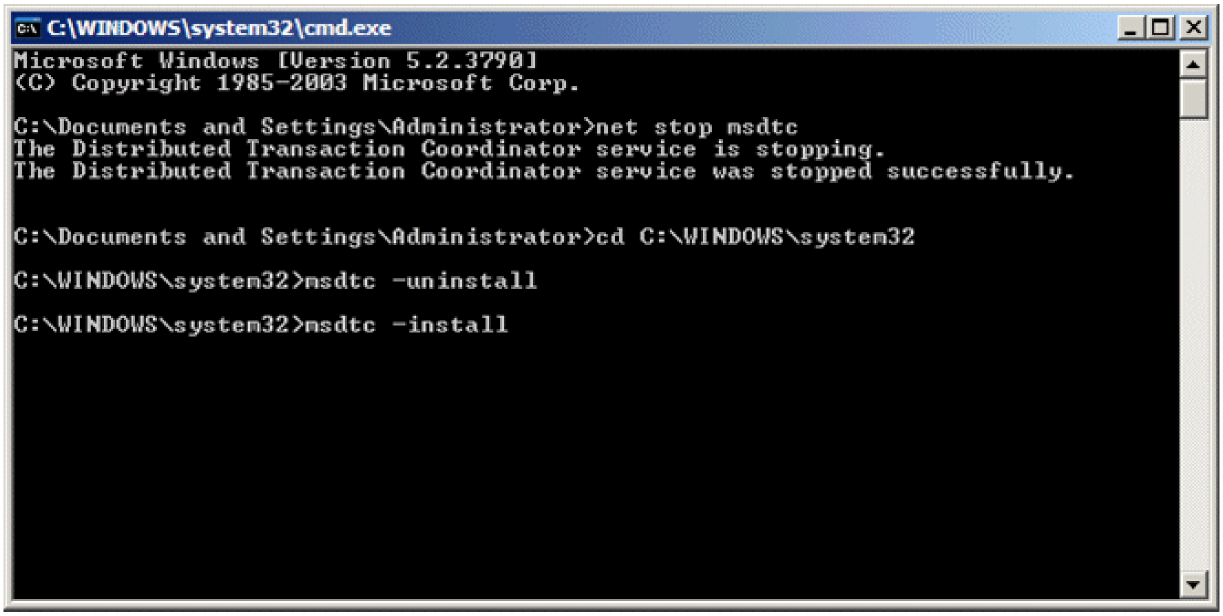
5. Close the Registry Editor.

Re-Installing the MSDTC

➡ To re-install the MSDTC:

1. In the command prompt window, type the command **msdtc -install.**

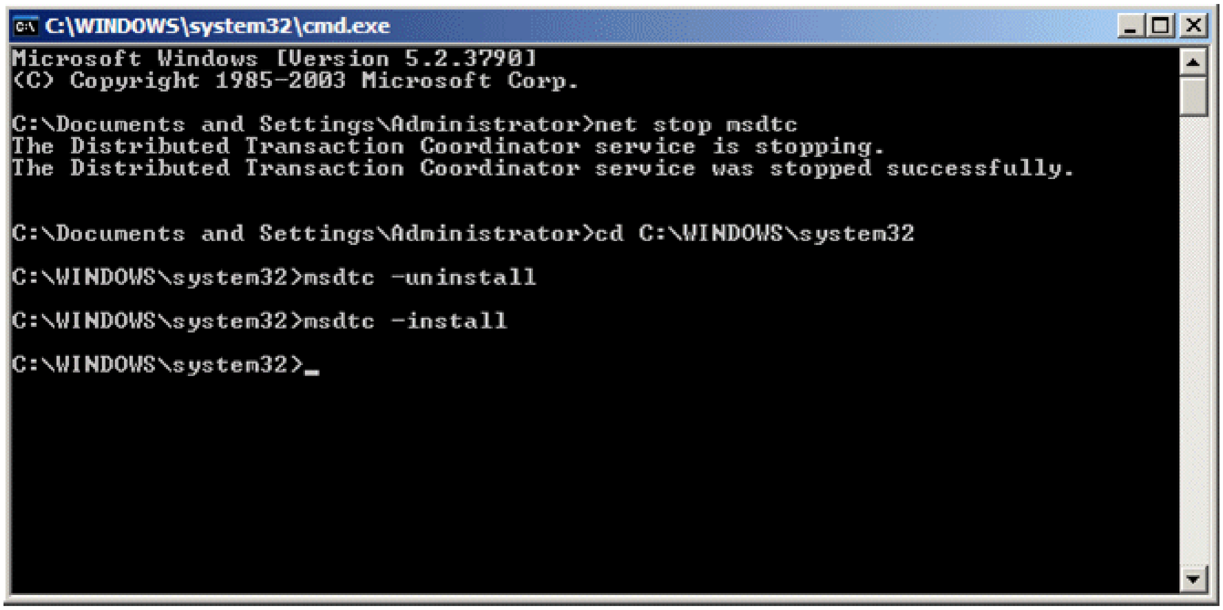
Figure 8-17: C:\WINDOWS\System32\cmd.exe



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net stop msdtc
The Distributed Transaction Coordinator service is stopping.
The Distributed Transaction Coordinator service was stopped successfully.


C:\Documents and Settings\Administrator>cd C:\WINDOWS\system32

C:\WINDOWS\system32>msdtc -uninstall

C:\WINDOWS\system32>msdtc -install
```

2. When the installation is completed, the following window appears.

Figure 8-18: C:\WINDOWS\System32\cmd.exe



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net stop msdtc
The Distributed Transaction Coordinator service is stopping.
The Distributed Transaction Coordinator service was stopped successfully.


C:\Documents and Settings\Administrator>cd C:\WINDOWS\system32

C:\WINDOWS\system32>msdtc -uninstall

C:\WINDOWS\system32>msdtc -install

C:\WINDOWS\system32>_
```

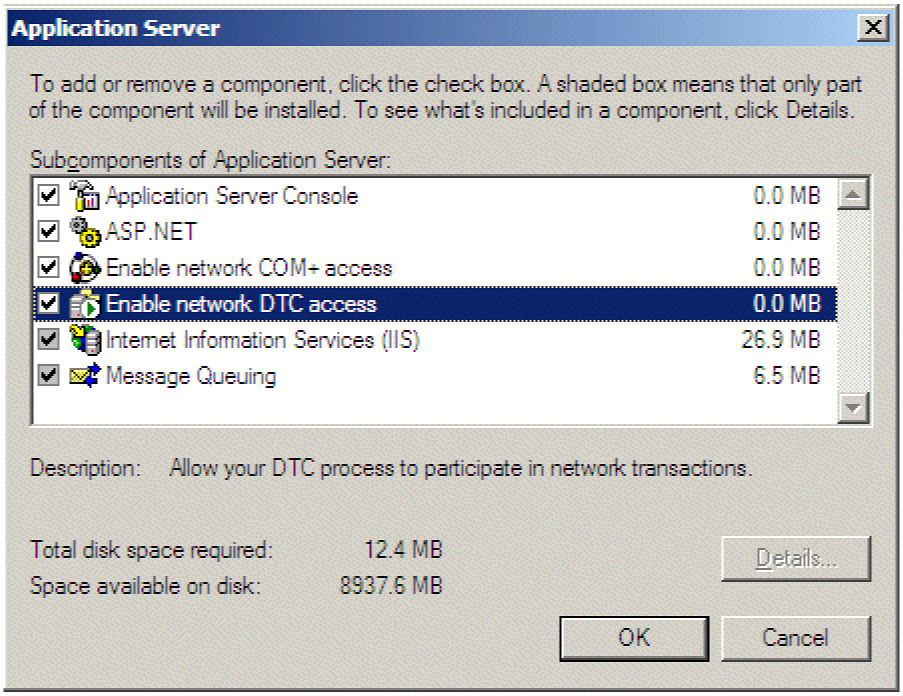
Re-Installing Network DTC Access

This procedure is very similar to the To remove network DTC access procedure. See Removing the Network Distribute Transaction Coordinator (DTC) Access on page 196

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



Application Server

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Application Server:

☑	Application Server Console	0.0 MB
☑	ASP.NET	0.0 MB
☑	Enable network COM+ access	0.0 MB
☑	Enable network DTC access	0.0 MB
☑	Internet Information Services (IIS)	26.9 MB
☑	Message Queuing	6.5 MB

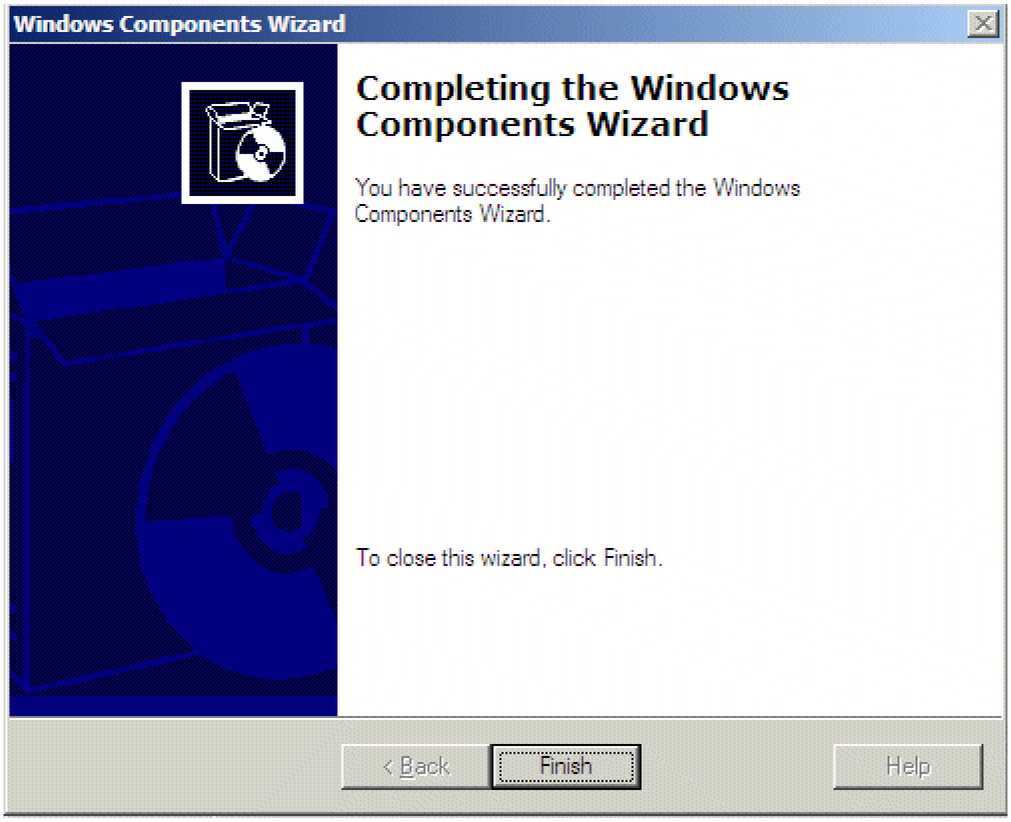
Description: Allow your DTC process to participate in network transactions.

Total disk space required: 12.4 MB

Space available on disk: 8937.6 MB

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



Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

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

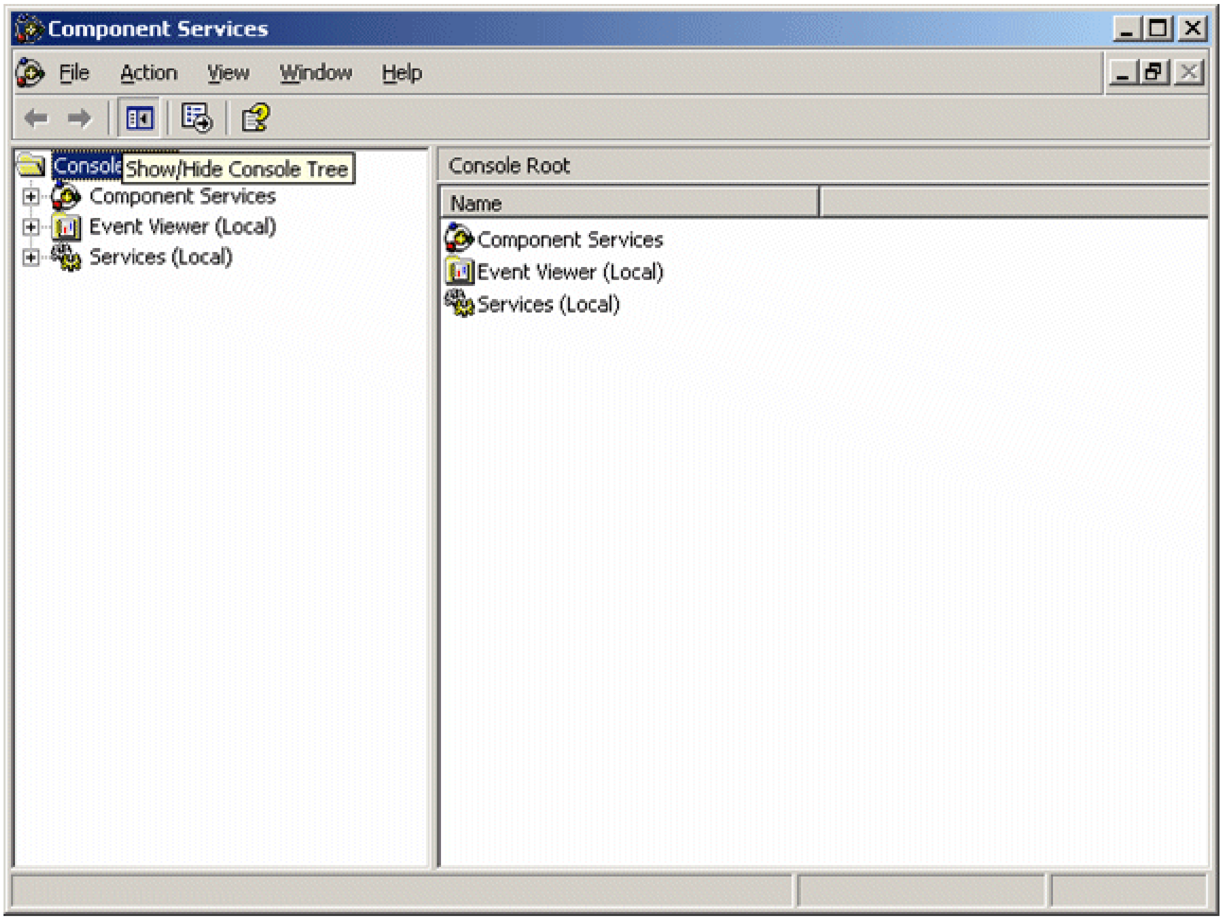
Restoring the Original Security Settings

Since MSTDC has been re-installed, the security definitions required by the NICE system must be reset.

➡ To restore the original security settings:

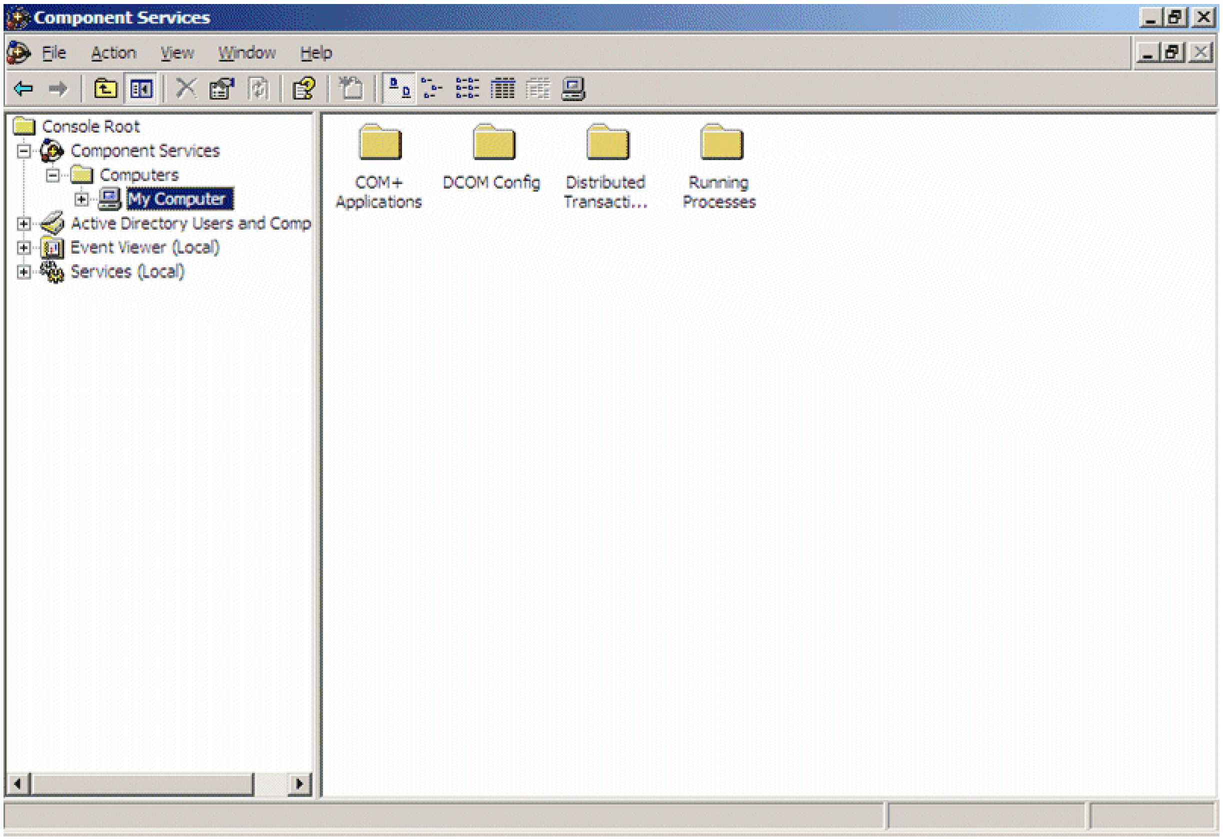
1. Select **Start**, and select **Settings** > **Control Panel** > **Administrative Tools** > **Component Services**. The Component Services window appears.

Figure 8-21: Component Services Window



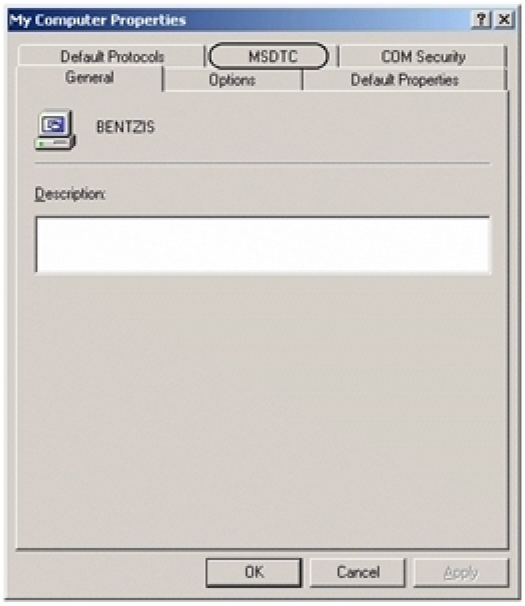
2. Expand **Computer Services**, and **Computers**. The following window appears:

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



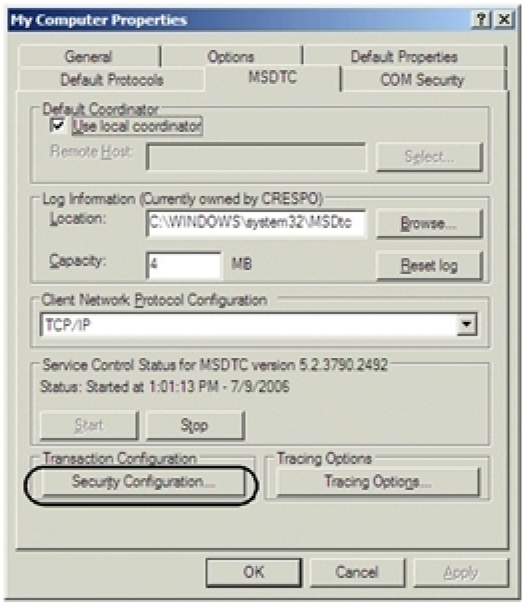
My Computer Properties

BENTZIS

Description:

4. Click the **MSDTC** tab. The following window appears.

Figure 8-24: My Computer Properties - MSDTC Tab



My Computer Properties

Default Coordinator

☑ Use local coordinator

Remote Host:

Log Information (Currently owned by CRESPO)

Location: C:\WINDOWS\system32\MSDtc

Capacity: 4 MB

Client Network Protocol Configuration

TCP/IP

Service Control Status for MSDTC version 5.2.3790.2492

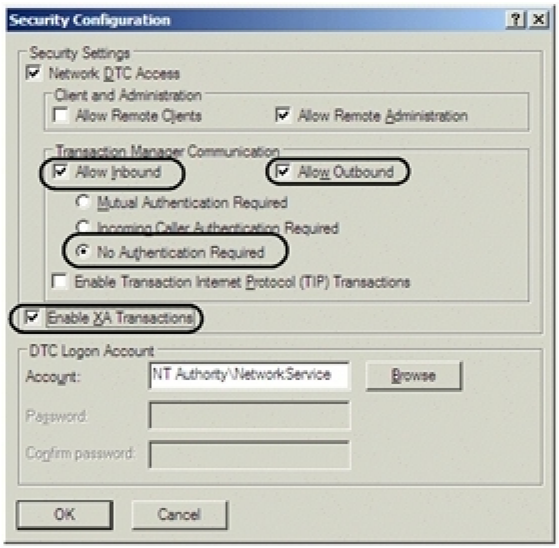
Status: Started at 1:01:13 PM - 7/9/2006

Transaction Configuration

Tracing Options

5. Click the **Security Configuration** button. The Security Configuration window appears.

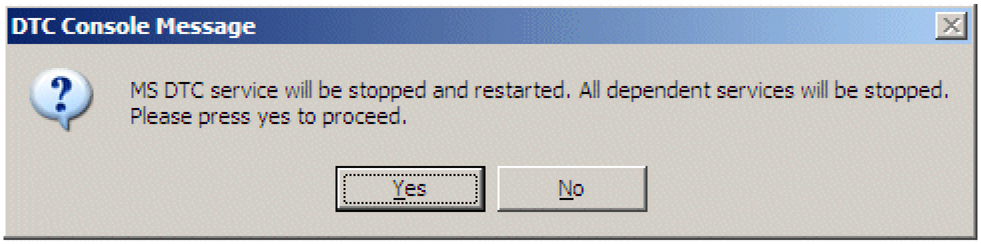
Figure 8-25: Security Configuration Window



Security Settings
☑ Network DTC Access
Client and Administration
□ Allow Remote Clients
☑ Allow Remote Administration
Transaction Manager Communication
☑ Allow Inbound
☑ Allow Outbound
○ Mutual Authentication Required
○ Incoming Caller Authentication Required
● No Authentication Required
□ Enable Transaction Internet Protocol (TIP) Transactions
☑ Enable XA Transactions
DTC Logon Account
Account: NT Authority\NetworkService
Password:
Confirm password:

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.

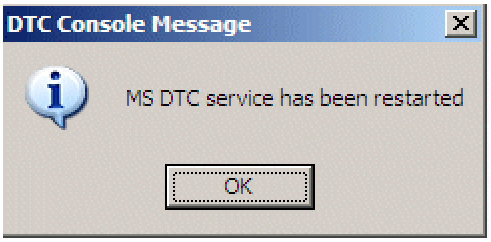
Figure 8-26: Console Message



MS DTC service will be stopped and restarted. All dependent services will be stopped. Please press yes to proceed.

9. Click **Yes**. The following message is issued:

Figure 8-27: DTC Console Message



DTC Console Message

MS DTC service has been restarted

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

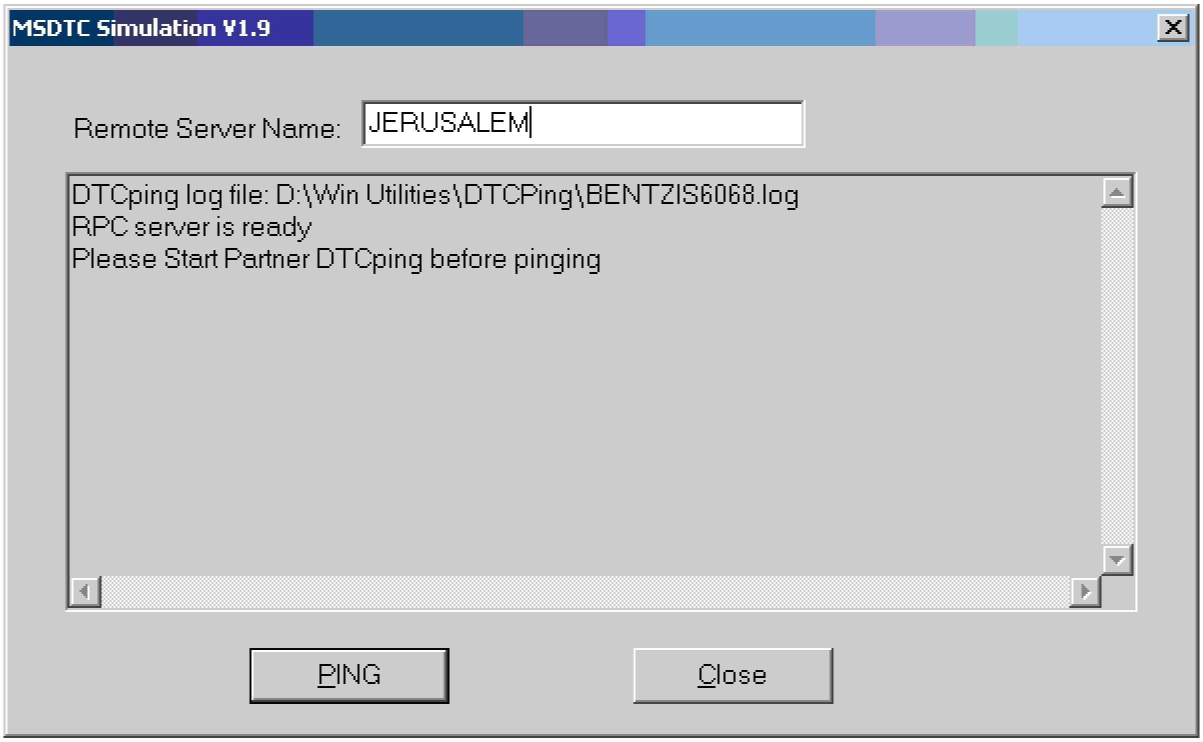
COMMIT

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



Remote Server Name: JERUSALEM

```
DTCping log file: D:\Win Utilities\DTCPing\BENTZIS6068.log
RPC server is ready
Please Start Partner DTCping before pinging
```

3. Click **PING**. The utility generates a log file with detailed information.

SQL Server 2012

Product	NICE Engage Platform, NICE Sentinel
Release	NICE Engage Platform 6.x Real-Time Solutions 4.9.6 NICE Sentinel 6.X

For more information see:

- *Requirements and Best Practices for Microsoft SQL Server*
- *Microsoft Cluster Installation for NICE Environments*

SQL Server 2014

Product	NICE Engage Platform
Release	NICE Engage Platform 6.x NICE Sentinel 6.X

For more information see:

- *Requirements and Best Practices for Microsoft SQL Server*
- *Microsoft Cluster Installation for NICE Environments*

[This page intentionally left blank]

9

Microsoft Security Bulletins

This section describes Microsoft security bulletins.

Contents

KBs Delivered by Microsoft and NICE Certification Policy

Microsoft launched a new policy in October 2016 where security and non-security packages are released in a cumulative rollup in addition to security update bulletins.

Security update bulletins are approved by NICE on a monthly basis.

Rollups released by Microsoft are not approved by NICE.

Package	Windows Vista SP2, Windows Server 2008 SP2 (with supported IE versions and .NET Framework)	Windows 7 SP1, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 (with supported IE versions)	Windows 10 (with supported IE versions and .NET Framework)	.NET Framework	SQL
Separate security KBs	KB delivered by Microsoft and certified by NICE				KB delivered by Microsoft and certified by NICE

One KB package with security only Includes KBs that are relevant and non-relevant to NICE		KB delivered by Microsoft and certified by NICE		KB delivered by Microsoft and certified by NICE	
Monthly rollup KB (includes security and non-security) Includes KBs that are relevant and non-relevant to NICE		KB delivered by Microsoft	KB delivered by Microsoft and certified by NICE	KB delivered by Microsoft	

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.

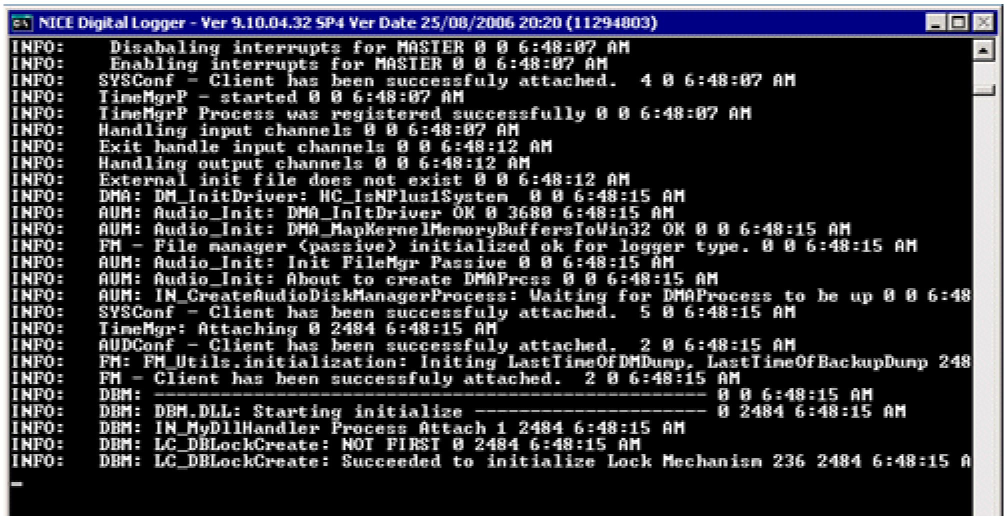
  This can affect all Loggers running on Microsoft Windows Server 2003 (HD, NCFIII, VoIP).
- The Microsoft patch is KB 921883 (MS 06-040).

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



NICE Digital Logger - Ver 9.10.04.32 SP4 Ver Date 25/08/2006 20:20 (11294803)

```
INFO:     Disabaling interrupts for MASTER 0 0 6:48:07 AM
INFO:     Enabling interrupts for MASTER 0 0 6:48:07 AM
INFO:    SYSConf - Client has been successfuly attached.  4 0 6:48:07 AM
INFO:    TimeMgrP - started 0 0 6:48:07 AM
INFO:    TimeMgrP Process was registered successfully 0 0 6:48:07 AM
INFO:    Handling input channels 0 0 6:48:07 AM
INFO:    Exit handle input channels 0 0 6:48:12 AM
INFO:    Handling output channels 0 0 6:48:12 AM
INFO:    External init file does not exist 0 0 6:48:12 AM
INFO:    DMA: DM_InitDriver: HC_IsNPlus1System  0 0 6:48:15 AM
INFO:    AUM: Audio_Init: DMA_InItDriver OK 0 3680 6:48:15 AM
INFO:    AUM: Audio_Init: DMA_MapKernelMemoryBuffersToWin32 OK 0 0 6:48:15 AM
INFO:    FM - File manager (passive) initialized ok for logger type. 0 0 6:48:15 AM
INFO:    AUM: Audio_Init: Init FileMgr Passive 0 0 6:48:15 AM
INFO:    AUM: Audio_Init: About to create DMAPrcss 0 0 6:48:15 AM
INFO:    AUM: IN_CreateAudioDiskManagerProcess: Waiting for DMAProcess to be up 0 0 6:48
INFO:    SYSConf - Client has been successfuly attached.  5 0 6:48:15 AM
INFO:    TimeMgr: Attaching 0 2484 6:48:15 AM
INFO:    AUDConf - Client has been successfuly attached.  2 0 6:48:15 AM
INFO:    FM: FM_Utils.initialization: Initing LastTimeOfDMDump, LastTimeOfBackupDump 248
INFO:    FM - Client has been successfuly attached.  2 0 6:48:15 AM
INFO:    DBM: -------------------------------------------------- 0 0 6:48:15 AM
INFO:    DBM: DBM.DLL: Starting initialize --------------------- 0 2484 6:48:15 AM
INFO:    DBM: IN_MyDllHandler Process Attach 1 2484 6:48:15 AM
INFO:    DBM: LC_DBLockCreate: NOT FIRST 0 2484 6:48:15 AM
INFO:    DBM: LC_DBLockCreate: Succeeded to initialize Lock Mechanism 236 2484 6:48:15 A
_
```

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

Federal Information Processing Standards (FIPS)

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the U.S. federal government for use in computer systems by non-military government agencies and government contractors. They were issued to establish requirements for various purposes such as ensuring computer security and interoperability.

The U.S. government developed a variety of FIPS specifications to standardize a number of topics including:

- Codes such as standards for encoding data (e,g,, country codes or codes to indicate weather conditions or emergency indications).
- Encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197).

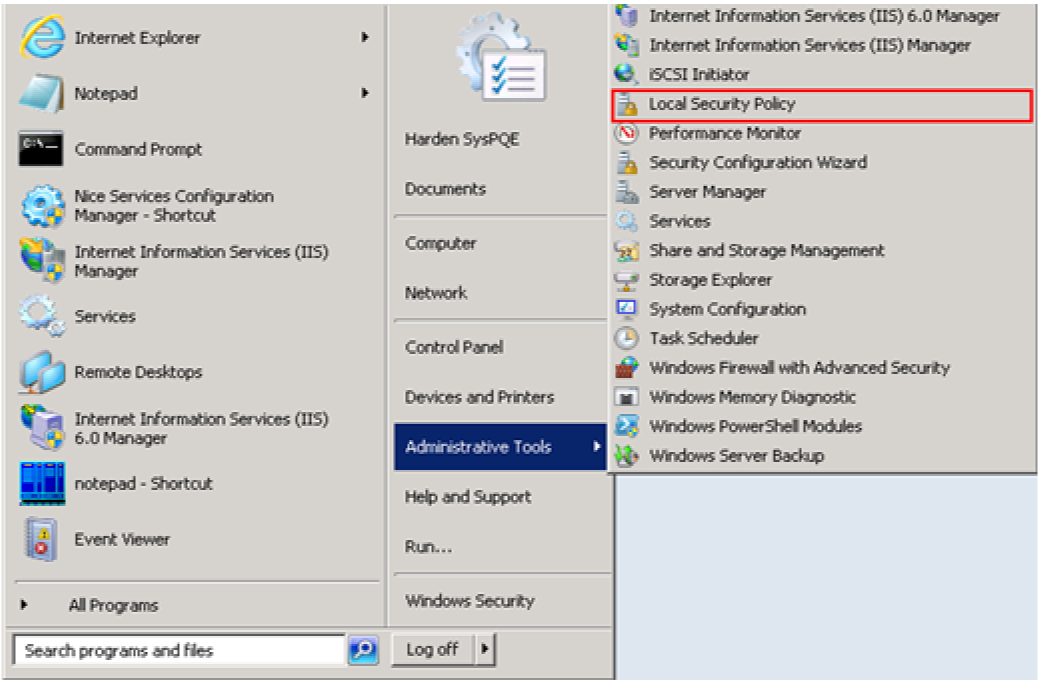
Configuring Windows for FIPS

The FIPS mode can be applied on the server or client machine in one of two ways:

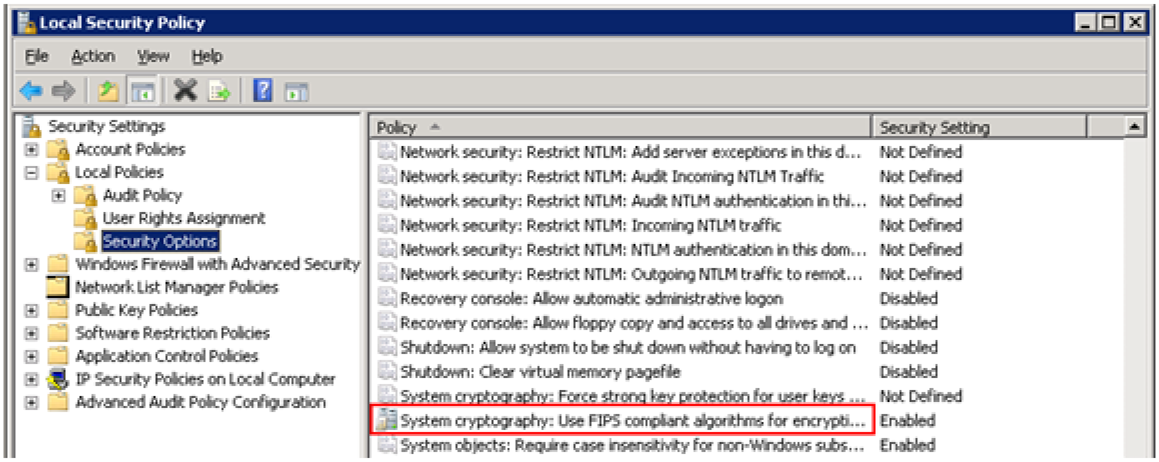
- It can be part of the domain policy.
- It can be manually configured on the server or client machine.

To manually apply FIPS mode on the machine:

1. Open the Local Security Policy by selecting **Start -> Administrative tools->Local Security Policy**. Run the Local Security Policy under a user that has privileges to edit the local policy.


Internet Explorer
Notepad
Command Prompt
Nice Services Configuration Manager - Shortcut
Internet Information Services (IIS) Manager
Services
Remote Desktops
Internet Information Services (IIS) 6.0 Manager
notepad - Shortcut
Event Viewer
All Programs
Search programs and files
Harden SysPQE
Documents
Computer
Network
Control Panel
Devices and Printers
Administrative Tools
Help and Support
Run...
Windows Security
Log off
Internet Information Services (IIS) 6.0 Manager
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Performance Monitor
Security Configuration Wizard
Server Manager
Services
Share and Storage Management
Storage Explorer
System Configuration
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell Modules
Windows Server Backup

2. In the open window, change the security settings. Navigate to **Security Settings->Local Polices->Security Options** and select **System Cryptography: Use FIPS compliant algorithms for encryption, hashing and signing** (disabled by default).



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Network security: Restrict NTLM: Add server exceptions in this d...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in thi...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this dom...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remot...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and ...	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys ...	Not Defined
System cryptography: Use FIPS compliant algorithms for encrypti...	Enabled
System objects: Require case insensitivity for non-Windows subs...	Enabled

3. Restart all of the servers and clients whose FIPS mode was activated.

Spell Check Limitation

For secured sites running Insight Manager, Form Designer, Lexicon Manager and Business Analyzer, spell check functionality is not available when FIPS is enabled on the system.

Users will receive the following error when activating the spell check:

Spell check is not available since FIPS (Federal Information Processing Standards) is enabled on this system.

11

Microsoft Daylight Savings Time Updates

This section provides the Microsoft Daylight Savings Time (DST) updates supported by NICE Systems.

For Microsoft Daylight Savings Time configurations, see the *Maintenance Guide*.

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 4.1	
KB 951072	NICE Engage Platform 6.x	
KB 955839		
KB 970653		
KB 976098		
KB 981793		
KB 2158563		

Microsoft DST Updates	Supported in:	Comments
KB 2443685		
KB 2570791		
KB 2633952		
KB 2756822		
KB 2779562		
KB 2863058		
KB 2974661		
KB 2984350		
KB 2967990		
KB 2981580		
KB 2998527		
KB3011843		
KB3013410		
KB3049874		
KB3062741		

Microsoft DST Updates	Supported in:	Comments
KB3062740		
KB3077715		
KB3093503		
KB3112148		
KB3148851		
KB3153731		
KB3162835		
KB3148851		
KB3153731		
KB3162835		
KB3177723		
KB3182203		
KB3192321		

[This page intentionally left blank]

12

Antivirus

This section includes installation instructions and limitations for Antivirus products on client computers and loggers.

> **NOTE:** The information in this section 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
- McAfee ePO 5.1 works with McAfee Antivirus 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.

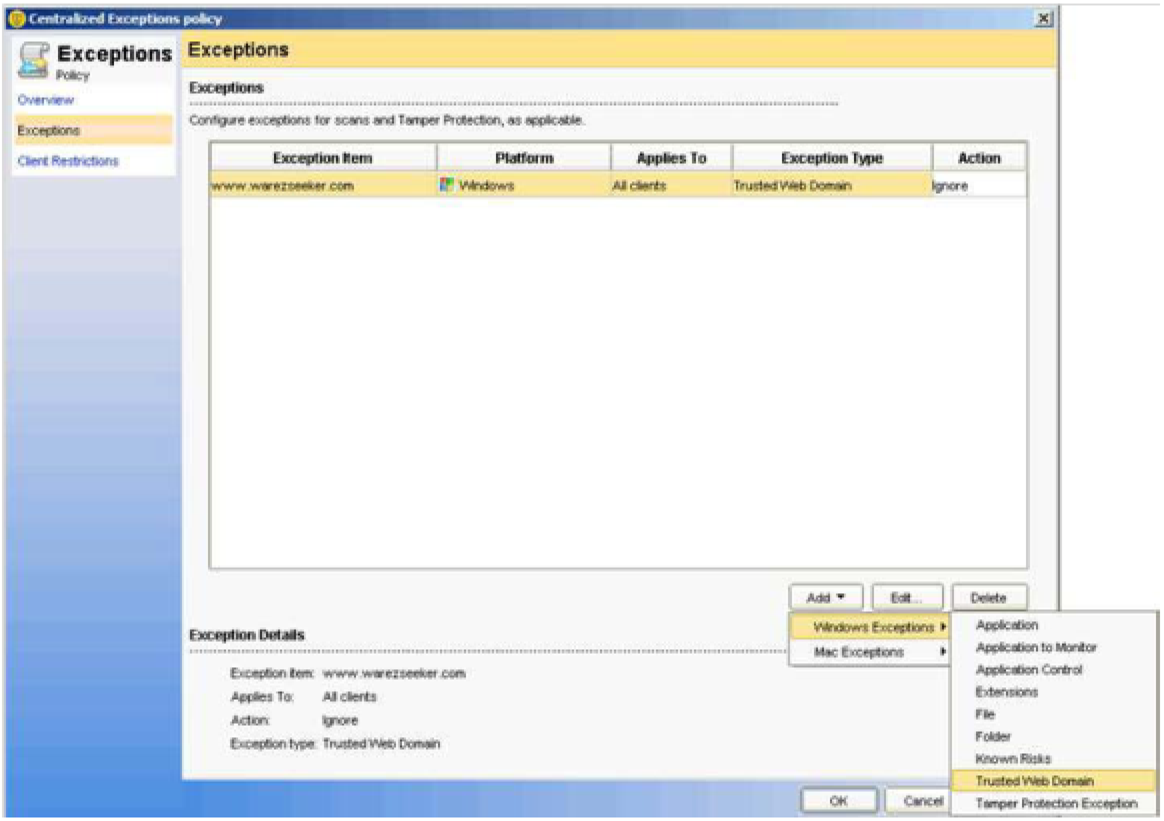
SEP

- NICE Products support Symantec Endpoint Protection.
- In some cases, SEP 12.1 and up 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 12-1: Exceptions Window



Exceptions

Exceptions

Configure exceptions for scans and Tamper Protection, as applicable.

Exception Item	Platform	Applies To	Exception Type	Action
www.warezseeker.com	Windows	All clients	Trusted Web Domain	Ignore

Exception Details

Exception Item: www.warezseeker.com
Applies To: All clients
Action: Ignore
Exception type: Trusted Web Domain

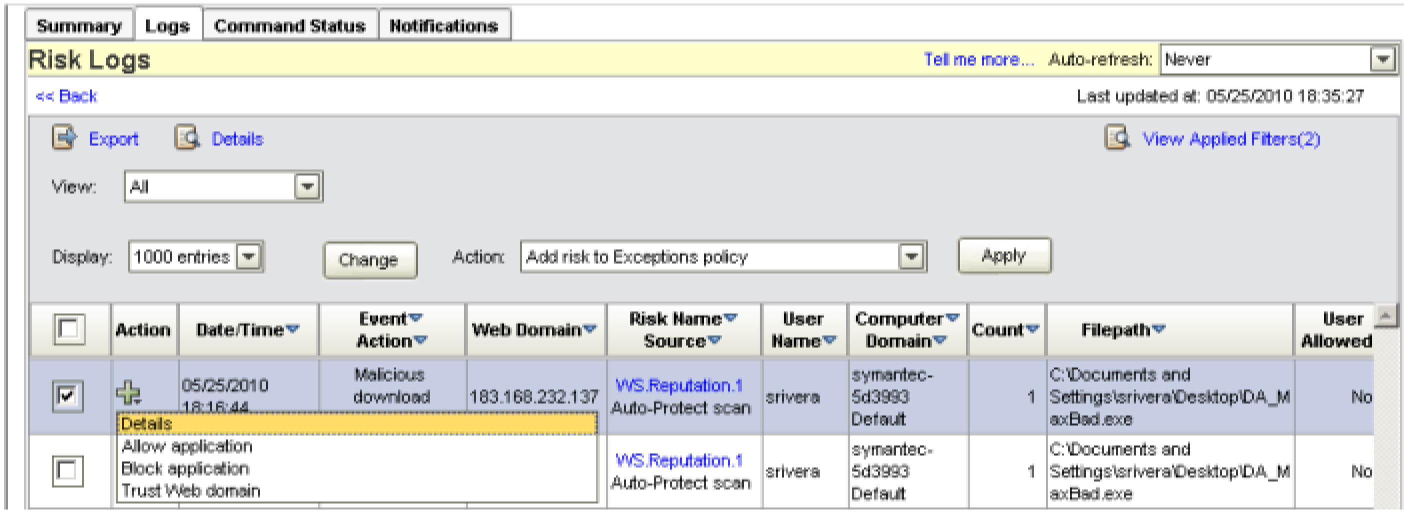
NOTE: You can select **Trusted Web Domain**, to add a Web domain to the exceptions policy.

- 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 12-2: Risk Logs Window



Risk Logs

Auto-refresh: Never

Last updated at: 05/25/2010 18:35:27

View: All

Display: 1000 entries

Action: Add risk to Exceptions policy

☐	Action	Date/Time	Event Action	Web Domain	Risk Name Source	User Name	Computer Domain	Count	Filepath	User Allowed
☑		05/25/2010 18:16:44	Malicious download	183.168.232.137	WS.Reputation.1 Auto-Protect scan	srivera	symantec-5d3993 Default	1	C:\Documents and Settings\srivera\Desktop\DA_MaxBad.exe	No
☐					WS.Reputation.1 Auto-Protect scan	srivera	symantec-5d3993 Default	1	C:\Documents and Settings\srivera\Desktop\DA_MaxBad.exe	No

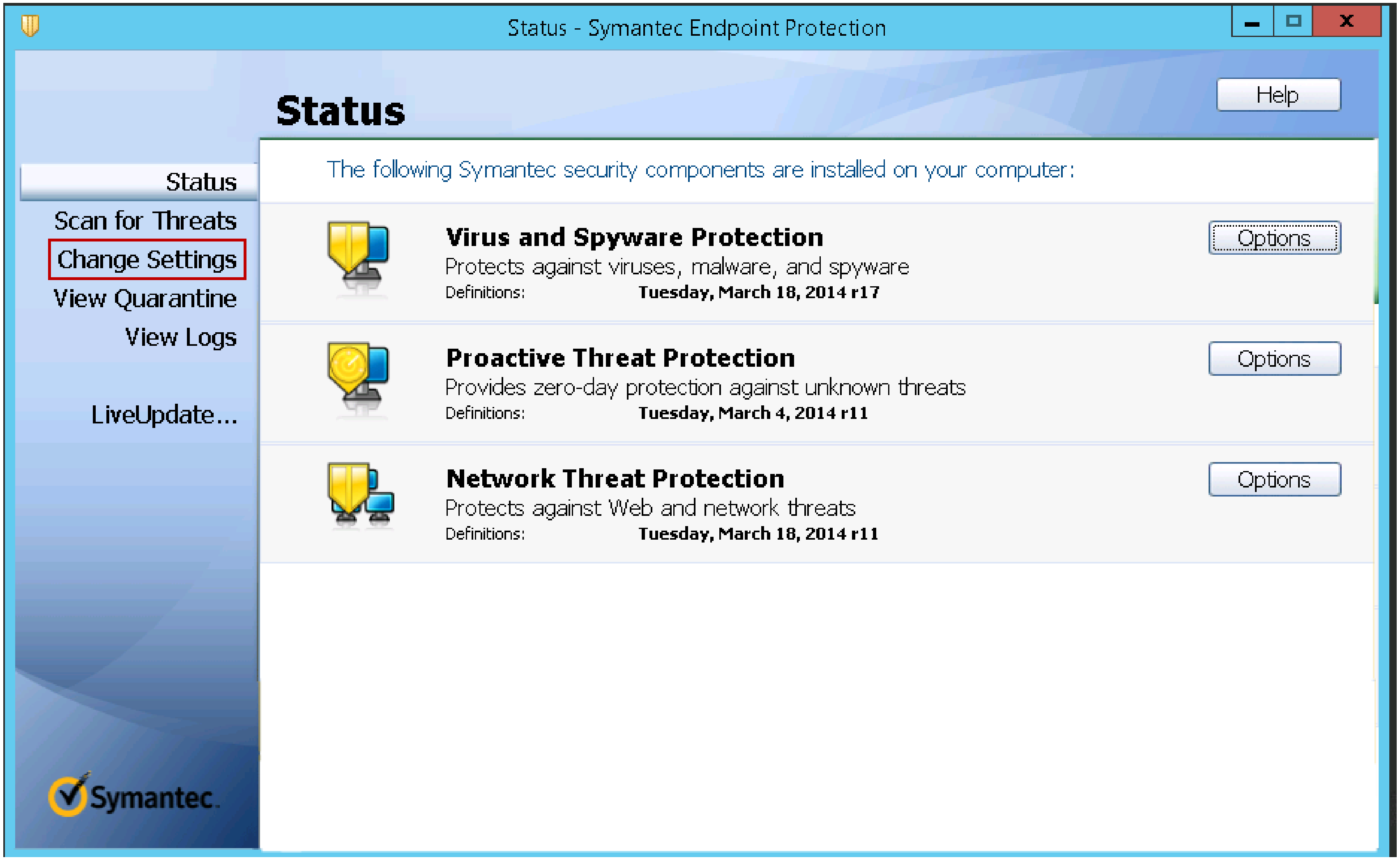
For more information, see the *Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide*.

SEP Limitations

Starting with SEP (Symantec Endpoint Protection) version 12.1.2 and up, 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).



Status

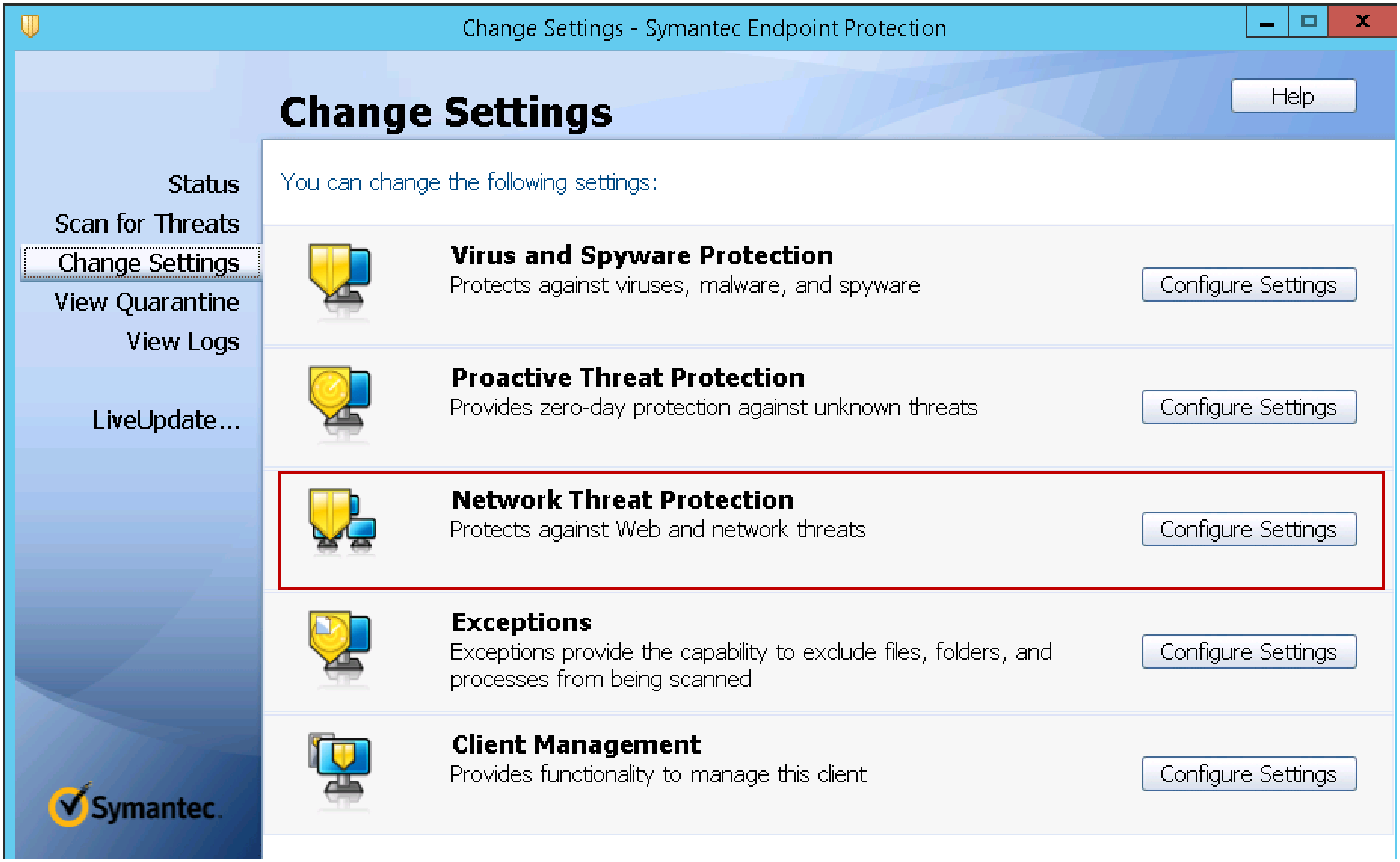
The following Symantec security components are installed on your computer:

Virus and Spyware Protection
Protects against viruses, malware, and spyware
Definitions: **Tuesday, March 18, 2014 r17**

Proactive Threat Protection
Provides zero-day protection against unknown threats
Definitions: **Tuesday, March 4, 2014 r11**

Network Threat Protection
Protects against Web and network threats
Definitions: **Tuesday, March 18, 2014 r11**

2. In the left column, click **Change Settings**. The Change Settings area appears on the right.



Change Settings

You can change the following settings:

Virus and Spyware Protection
Protects against viruses, malware, and spyware

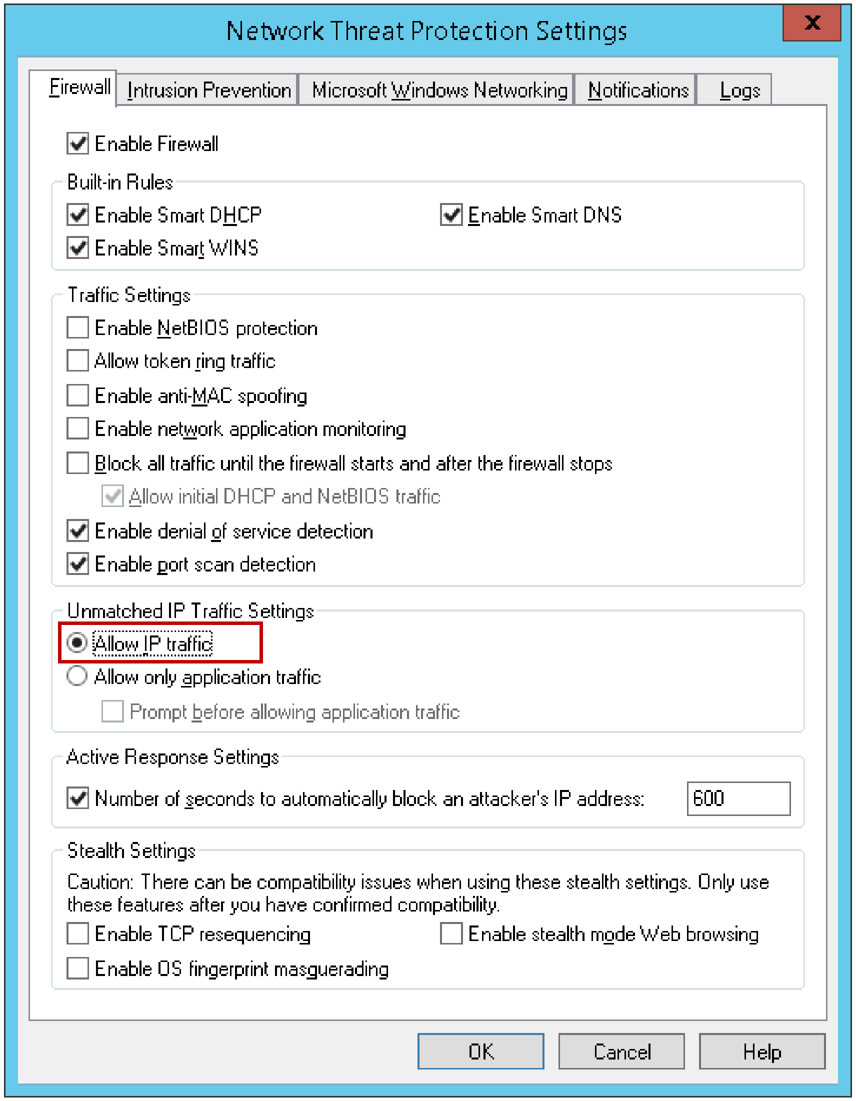
Proactive Threat Protection
Provides zero-day protection against unknown threats

Network Threat Protection
Protects against Web and network threats

Exceptions
Exceptions provide the capability to exclude files, folders, and processes from being scanned

Client Management
Provides functionality to manage this client

3. In the **Network Threat Protection** area, click **Configure Settings**. The Network Threat Protection Settings window appears.



Network Threat Protection Settings
Firewall
Intrusion Prevention
Microsoft Windows Networking
Notifications
Logs
OK
Cancel
Help

☑ Enable Firewall

Built-in Rules

☑ Enable Smart DHCP
☑ Enable Smart DNS
☑ Enable Smart WINS

Traffic Settings

□ Enable NetBIOS protection
□ Allow token ring traffic
□ Enable anti-MAC spoofing
□ Enable network application monitoring
□ Block all traffic until the firewall starts and after the firewall stops
☑ Allow initial DHCP and NetBIOS traffic
☑ Enable denial of service detection
☑ Enable port scan detection

Unmatched IP Traffic Settings

● Allow IP traffic
○ Allow only application traffic
□ Prompt before allowing application traffic

Active Response Settings

☑ Number of seconds to automatically block an attacker's IP address: 600

Stealth Settings

Caution: There can be compatibility issues when using these stealth settings. Only use these features after you have confirmed compatibility.

□ Enable TCP resequencing
□ Enable stealth mode Web browsing
□ Enable OS fingerprint masquerading

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 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

Note: Third-Party Software is approved per NICE product for all operating systems certified by NICE.

NOTE: Third-Party Software is approved per NICE product for all operating systems certified by NICE.

> **NOTE:** Third-Party Software is approved per NICE product for all operating systems certified by NICE.

Table 12-1:
NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1

NICE Products	SEP		McAfee			Trend Micro		Sophos	
	11.00	12.0 - 12.1.6	ePO 4.0/4.5/4.6	ePO 5.1 / 5.1.1/ 5.3.0	8.7/8.8	OfficeScan 10/10.5/10.6	OfficeScan 11/XG	9.5/9.7	10/10.2/10.3 - 10.3.15/10.6.3
TDM Logger	Y	Y	Y	Y	Y	Y	Y	Y	Y
VoIP Logger	Y	Y	Y	Y	Y	Y	Y	Y	Y
Interaction Server	Y	Y	Y	Y	Y	Y	Y	Y	Y
NiceScreen Logger	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
NMS	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 12-1: NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 (continued)

NICE Products	SEP		McAfee			Trend Micro		Sophos	
	11.00	12.0 - 12.1.6	ePO 4.0/4.5/4.6	ePO 5.1 / 5.1.1/ 5.3.0	8.7/8.8	OfficeScan 10/10.5/10.6	OfficeScan 11/XG	9.5/9.7	10/10.2/10.3 - 10.3.15/10.6.3
Storage Center	Y	Y	Y	Y	Y	Y	Y	Y	Y
Media Library	Y	Y	Y	Y	Y	Y	Y	Y	Y
Application Server	Y	Y	Y	Y	Y	Y	Y	Y	Y
Audio Analysis Server	Y	Y	Y	Y	Y	Y	Y	Y	Y
ScreenSense Server	Y	Y	Y	Y	Y	Y	Y	Y	Y
Reporter	Y	Y	Y	Y	Y	Y	Y	Y	Y
Database Server	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 12-1: NICE Products and Antivirus Certifications Matrix - NICE Interaction Management 4.1 (continued)

NICE Products	SEP		McAfee			Trend Micro		Sophos	
	11.00	12.0 - 12.1.6	ePO 4.0/4.5/4.6	ePO 5.1 / 5.1.1/ 5.3.0	8.7/8.8	OfficeScan 10/10.5/10.6	OfficeScan 11/XG	9.5/9.7	10/10.2/10.3 - 10.3.15/10.6.3
Sentinel	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.									

Table 12-2:
NICE Products and Antivirus Certifications Matrix - NICE Engage Platform 6.x

NICE Products	SEP			McAfee			Trend Micro		Sophos	
	11.00	12	12.1- 12.1.6	8.7	8.8	ePO 5.1/ 5.3.0	10.6	11/XG	10	10.3- 10.3.15/10.6.3
TDM Logger	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VoIP Logger	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 12-2: NICE Products and Antivirus Certifications Matrix - NICE Engage Platform 6.x (continued)

NICE Products	SEP			McAfee			Trend Micro		Sophos	
	11.00	12	12.1-12.1.6	8.7	8.8	ePO 5.1/ 5.3.0	10.6	11/XG	10	10.3-10.3.15/10.6.3
Interaction Server	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NiceScreen Logger	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
NMS	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Storage Center	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Media Library	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Application Server	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Audio Analysis Server	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 12-2: NICE Products and Antivirus Certifications Matrix - NICE Engage Platform 6.x (continued)

NICE Products	SEP			McAfee			Trend Micro		Sophos	
	11.00	12	12.1-12.1.6	8.7	8.8	ePO 5.1/ 5.3.0	10.6	11/XG	10	10.3-10.3.15/10.6.3
ScreenSense Server	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Reporter	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Database Server	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Sentinel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
RTA - Enrollment Engine	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
RTA - RTVA, Authentication Engine	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 12-2: NICE Products and Antivirus Certifications Matrix - NICE Engage Platform 6.x (continued)

NICE Products	SEP			McAfee			Trend Micro		Sophos	
	11.00	12	12.1-12.1.6	8.7	8.8	ePO 5.1/ 5.3.0	10.6	11/XG	10	10.3-10.3.15/10.6.3
RTA - Authentication and Fraud Engine (Nuance) audio folder	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
RTA - RTIM	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
RTA - ITIC	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Advanced Interaction Recorder	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 12-3:
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 12-4:
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

Table 12-4: EPO Tasks (continued)

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

Table 12-4: EPO Tasks (continued)

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

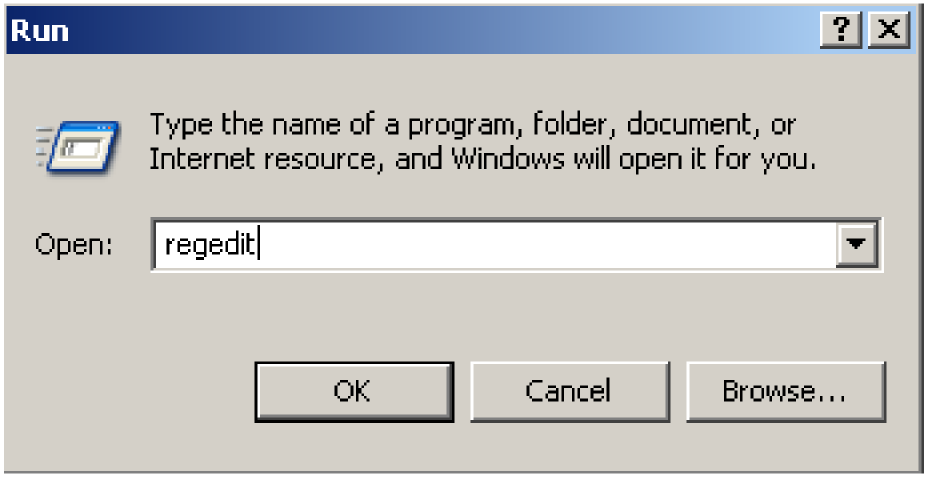
When updating the McAfee antivirus software, the logger capture card stops receiving interactions, resulting in a **Fatal** error message.

Solution

➡ To troubleshoot, do the following

1. Navigate to **Start**, and then select **Run**.
   The Run window appears.

   Figure 12-3: Run Window

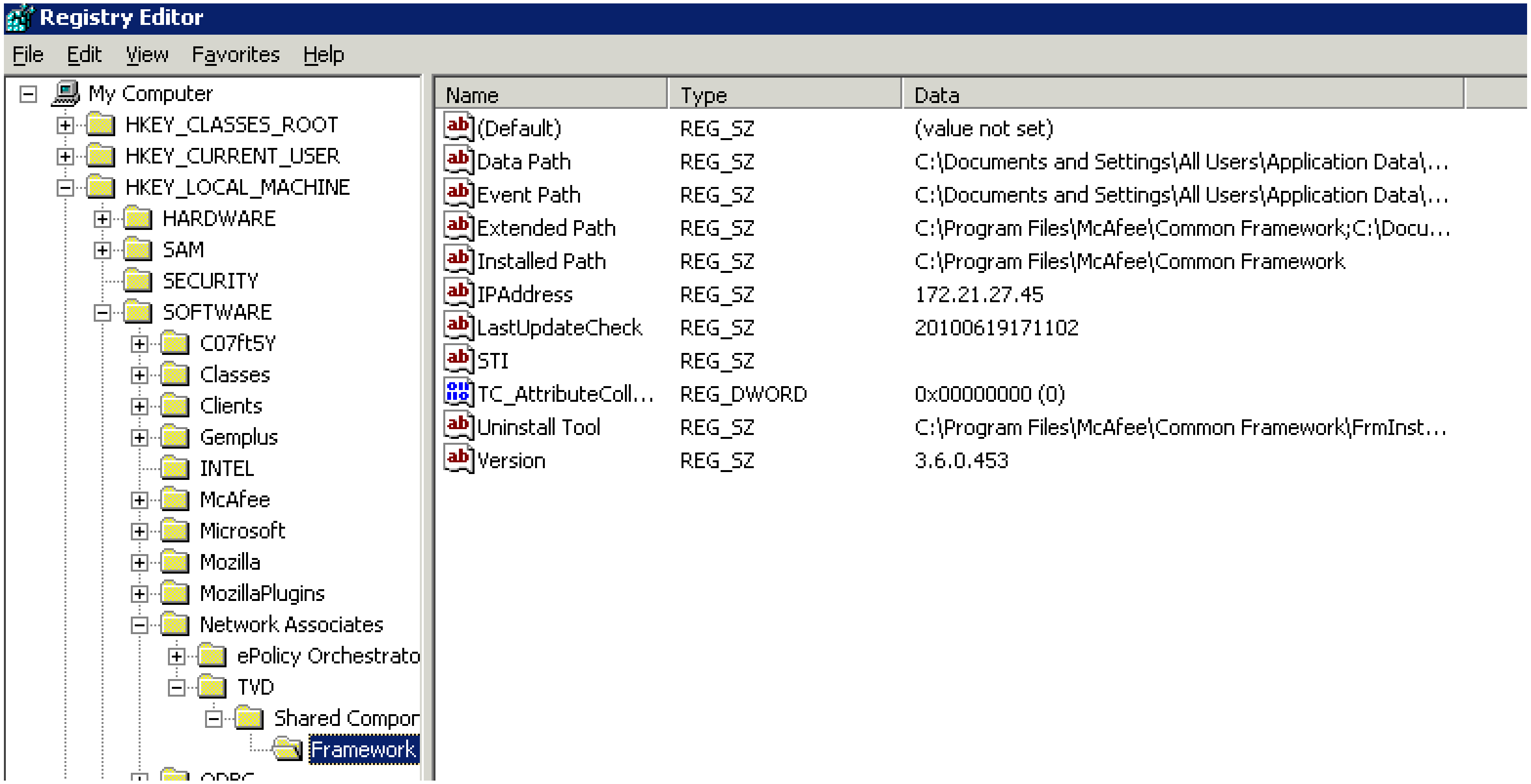
   Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

   Open: regedit

2. In the **Open** field, enter **regedit**, and click **OK**.

   The Registry Editor appears.

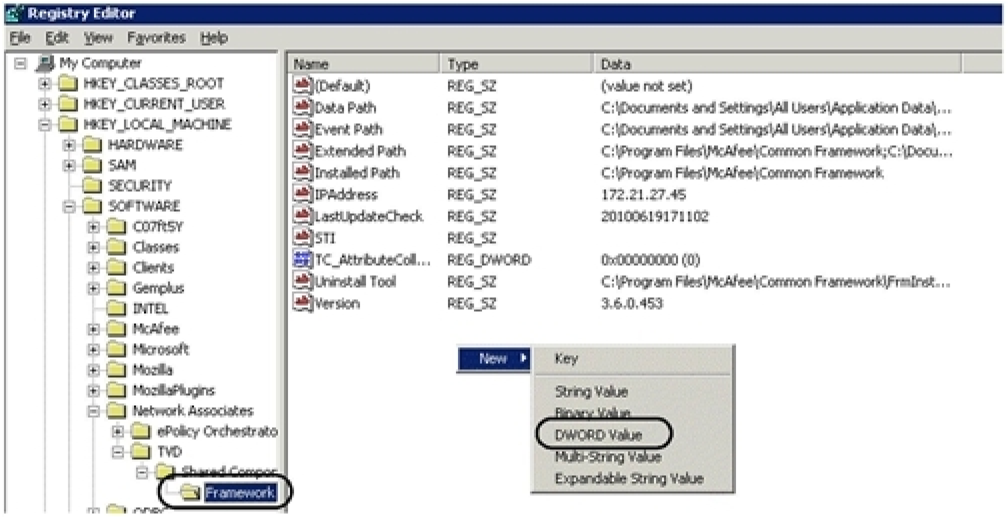
Figure 12-4: Registry Editor Window



Name	Type	Data
(Default)	REG_SZ	(value not set)
Data Path	REG_SZ	C:\Documents and Settings\All Users\Application Data\...
Event Path	REG_SZ	C:\Documents and Settings\All Users\Application Data\...
Extended Path	REG_SZ	C:\Program Files\McAfee\Common Framework;C:\Docu...
Installed Path	REG_SZ	C:\Program Files\McAfee\Common Framework
IPAddress	REG_SZ	172.21.27.45
LastUpdateCheck	REG_SZ	20100619171102
STI	REG_SZ	
TC_AttributeColl...	REG_DWORD	0x00000000 (0)
Uninstall Tool	REG_SZ	C:\Program Files\McAfee\Common Framework\FrmInst...
Version	REG_SZ	3.6.0.453

3. Navigate to HKEY_LOCAL_MACHINE > SOFTWARE > Network Associates > TVD > Shared Components > Framework.

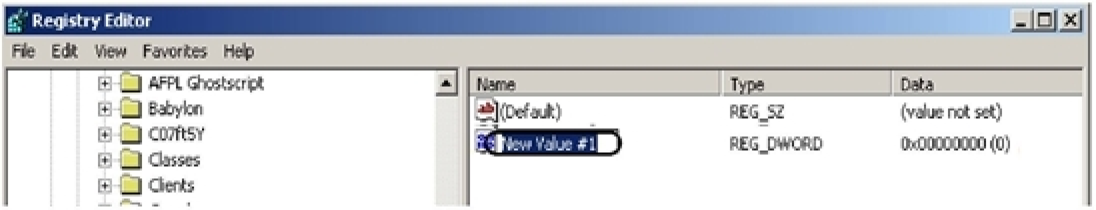
Figure 12-5: New Menu- DWORD Value



Name	Type	Data
(Default)	REG_SZ	(value not set)
Data Path	REG_SZ	C:\Documents and Settings\All Users\Application Data\...
Event Path	REG_SZ	C:\Documents and Settings\All Users\Application Data\...
Extended Path	REG_SZ	C:\Program Files\McAfee\Common Framework;C:\Docu...
Installed Path	REG_SZ	C:\Program Files\McAfee\Common Framework
IPAddress	REG_SZ	172.21.27.45
LastUpdateCheck	REG_SZ	20100619171102
STI	REG_SZ	
TC_AttributeColl...	REG_DWORD	0x00000000 (0)
Uninstall Tool	REG_SZ	C:\Program Files\McAfee\Common Framework\FrmInst...
Version	REG_SZ	3.6.0.453

4. In the right-hand pane, right-click in the empty space, and select **New** > **DWORD Value**. A new registry key appears.

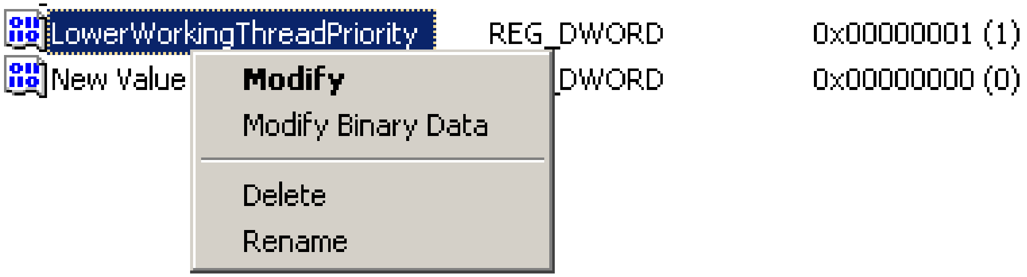
Figure 12-6: Registry Editor Window



Name	Type	Data
(Default)	REG_SZ	(value not set)
New Value #1	REG_DWORD	0x00000000 (0)

5. Change the name to **LowerWorkingThreadPriority**, and press **Enter**. The new file name **LowerWorkingThreadPriority** is reflected.

Figure 12-7: Modify Window

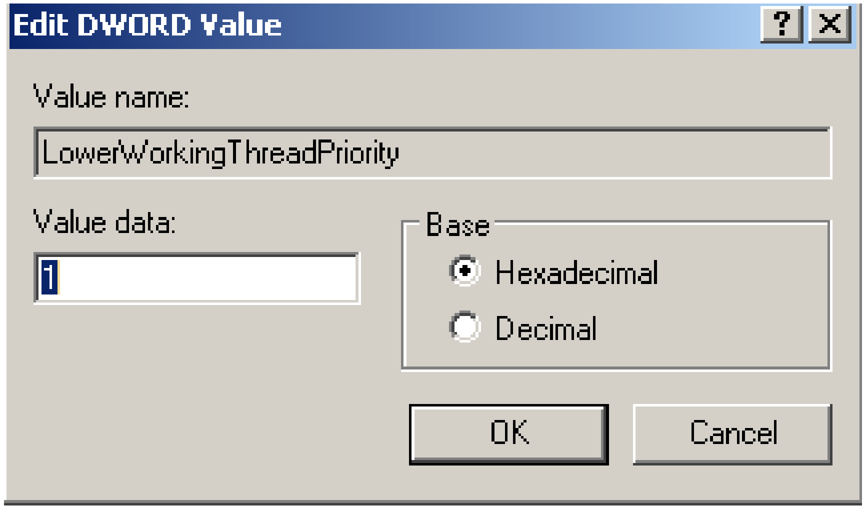


LowerWorkingThreadPriority REG_DWORD 0x00000001 (1)

New Value DWORD 0x00000000 (0)

6. Right-click **LowerWorkingThreadPriority**, and select **Modify**. The Edit DWORD Value window appears.

Figure 12-8: Edit DWORD Value Window



Edit DWORD Value

Value name: LowerWorkingThreadPriority

Value data: 1

Base

● Hexadecimal

○ Decimal

7. In the **Value data** field, enter **1**, and click **OK**.

8. Exit the registry.

9. Restart the McAfee Framework Service:

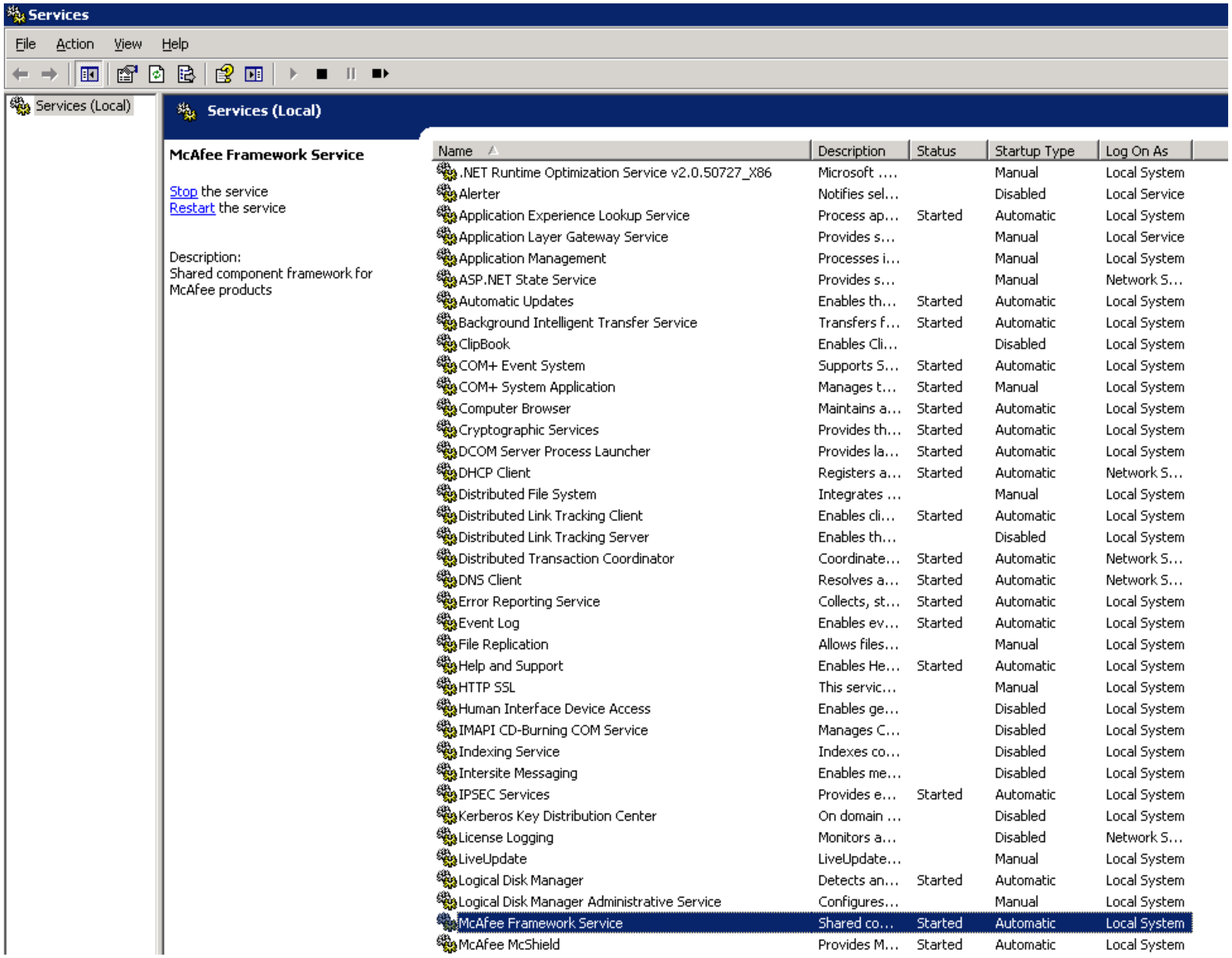
   a. Navigate to **Start** > **Run.**

   b. Enter **Services.msc.**

   c. Click **OK**.

   The McAfee Framework Service window appears.

Figure 12-9: McAfee Framework Service Window



McAfee Framework Service

Stop the service
Restart the service

Description:
Shared component framework for McAfee products

Name	Description	Status	Startup Type	Log On As
.NET Runtime Optimization Service v2.0.50727_X86	Microsoft		Manual	Local System
Alerter	Notifies sel...		Disabled	Local Service
Application Experience Lookup Service	Process ap...	Started	Automatic	Local System
Application Layer Gateway Service	Provides s...		Manual	Local Service
Application Management	Processes i...		Manual	Local System
ASP.NET State Service	Provides s...		Manual	Network S...
Automatic Updates	Enables th...	Started	Automatic	Local System
Background Intelligent Transfer Service	Transfers f...	Started	Automatic	Local System
ClipBook	Enables Cli...		Disabled	Local System
COM+ Event System	Supports S...	Started	Automatic	Local System
COM+ System Application	Manages t...	Started	Manual	Local System
Computer Browser	Maintains a...	Started	Automatic	Local System
Cryptographic Services	Provides th...	Started	Automatic	Local System
DCOM Server Process Launcher	Provides la...	Started	Automatic	Local System
DHCP Client	Registers a...	Started	Automatic	Network S...
Distributed File System	Integrates ...		Manual	Local System
Distributed Link Tracking Client	Enables cli...	Started	Automatic	Local System
Distributed Link Tracking Server	Enables th...		Disabled	Local System
Distributed Transaction Coordinator	Coordinate...	Started	Automatic	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Service	Collects, st...	Started	Automatic	Local System
Event Log	Enables ev...	Started	Automatic	Local System
File Replication	Allows files...		Manual	Local System
Help and Support	Enables He...	Started	Automatic	Local System
HTTP SSL	This servic...		Manual	Local System
Human Interface Device Access	Enables ge...		Disabled	Local System
IMAPI CD-Burning COM Service	Manages C...		Disabled	Local System
Indexing Service	Indexes co...		Disabled	Local System
Intersite Messaging	Enables me...		Disabled	Local System
IPSEC Services	Provides e...	Started	Automatic	Local System
Kerberos Key Distribution Center	On domain ...		Disabled	Local System
License Logging	Monitors a...		Disabled	Network S...
LiveUpdate	LiveUpdate...		Manual	Local System
Logical Disk Manager	Detects an...	Started	Automatic	Local System
Logical Disk Manager Administrative Service	Configures...		Manual	Local System
McAfee Framework Service	Shared co...	Started	Automatic	Local System
McAfee McShield	Provides M...	Started	Automatic	Local System

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*.

[This page intentionally left blank]

13

Remote Connection to Customers

This section includes requirements and recommendations for NICE to connect remotely to customers.

NICE Requirements

NICE needs a remote connection in place from the first days of the project. The connection needs to have both high bandwidth and low latency. In addition, it is highly recommended to use a dedicated machine for this connection.

NICE Recommendations

NICE suggests these methods to connect remotely, in order of preference. The customer needs to let the NICE Project Manager know of any site requirements:

1. Team Viewer - Based on availability. Team Viewer requires licensing.

2. VPN (on VSphere) - Setup can take from four to six weeks to arrange access through VPN on VSphere. This option enables a remote connection even when the customer is not present on the other side.

3. WebEx - In order to connect through WebEx, the customer must open the Webex connection on their side. Also, playback is not always possible through WebEx. This means that the customer needs to listen to the recording, or download the files locally to send them to NICE.

[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.

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

Table A-1: List of Discontinued Technical Notes (continued)

Technical Note Number	Technical Note Title
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
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

Table A-1: List of Discontinued Technical Notes (continued)

Technical Note Number	Technical Note Title
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]

C

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.