Third Party Technical Guidelines

Configuration Guide

Release: Cross-Release
NICE Engage 7.4
Advanced Process Automation

Document Revision: A4
Distribution Status: Published
Publication Date: September 2024

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.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of NICE or in Affiliate and is protected by United States and international copyright laws. Permission is granted to use, view and photocopy (or print) materials from this document only in connection with the products to which this document relates and subject to the terms of license applicable to such products. Any other use, copying, distribution, retransmission or modification of the information in this document without the express prior written permission of NICE or an Affiliate is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

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.

All contents of this document are: Copyright © 2024 NICE Ltd. All rights reserved.

For assistance, contact your local supplier or nearest NICE Customer Service Center: www.nice.com/company/global-locations

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

NICE values diversity and inclusion. Our documentation aims to use language free of bias based on race, color, age, sex, sexual orientation, disabilities, religion, national origin, or any other characteristic protected by applicable law.

CONTENTS

1: Introduction 9

Scope of this Guide 9

Document Revision History 10

2: Microsoft Software Service Packs Certified by NICE 13

3: Microsoft Client Operating Systems: Windows 10 32-bit or 64-bit 23

General Information: Localization 23

Windows 10 Client Applications Compatibility 23

Using the Silent Installation to Install Client Applications 24

Reporter Viewer 24

NICE BSF Toolkit 25

Manually Installing NICE Client Applications 25

4: Microsoft Client Operating Systems: Windows 11 64-bit 27

General Information: Localization 27

Windows 11 Client Applications Compatibility 27

Using the Silent Installation to Install Client Applications 28

Reporter Viewer 28

NICE BSF Toolkit 29

Manually Installing NICE Client Applications 29

5: Web Browsers 31

6: Microsoft Edge with IE Mode 33

Compatibility of NICE Web Applications with Microsoft Edge in IE Mode 33

Client Application Compatibility 34
Enabling IE Mode for Microsoft Edge 34
Configuring IE Mode in Microsoft Edge Simplified Procedure 35
Configuring IE Mode in Microsoft Edge over Domain Controller GPO 39

7: Google Chrome with the IE Tab Extension **51**

Compatibility of NICE Web Applications with the IE Tab Extension in Google Chrome 32/64-bit 52
General Description and Conclusions 52
Conclusions 53
Client Application Compatibility 53
Adding the IE Tab to Google Chrome 54
NICE Web Applications Known Issues with the IE Tab in Google Chrome 61

8: Microsoft .NET Framework **63**

NICE Support for Microsoft .NET Framework 63
Overview 63
Microsoft .NET Framework Server-Side Support 63
Microsoft .NET Framework Client-Side Support 64
Microsoft .NET Framework 4.8 Requirements 65
Microsoft .NET 6.0 Requirements 66

9: Microsoft SQL Server **67**

SQL Server 2016 67
SQL Server 2019 67

10: Additional Third Party Components **69**

Apache Tomcat 69
ActiveMQ Artemis 69
RabbitMQ 70
SAP Products 70
SIP Stack 70

Java 11 Azul 72
Java 17 Azul 73

11: Microsoft Kerberos Configuration Manager 75

12: Microsoft Security Bulletins 85
KBs Delivered by Microsoft and NICE Certification Policy 85

13: Federal Information Processing Standards (FIPS) 87
Configuring Windows for FIPS 87
FIPS Verification Flow 88
Spell Check Limitation 89

14: Microsoft Daylight Savings Time Updates 91

15: Antivirus: General Antivirus Configuration Guidelines 93
Overview 93
Antivirus Real Time Scan 93
Daily Scan 93
Weekly Scan 94
Folders and Files Exclusion 94
Disabling Firewalls 97
Live Updates 97
CPU Priority 97
Additional Configurations 97
Additional Recommendations 97

16: Antivirus: Antivirus Software Configuration 99
Configuring Symantec Endpoint Protection 99
Disabling Heuristic Scanning 99
Configuring SONAR 100

Configuring LiveUpdate 101
Excluding Folders and Files 102
Configuring the CPU Priority 103
Configuring Trend Micro OfficeScan 103
Configuring Scheduled Updating of the OfficeScan Server 104
Configuring Automatic Update 105
Excluding Folders and Files 105
Configuring the CPU Usage 106
Configuring Sophos 107
Configuring Scheduled Updating 107
Excluding Folders and Extensions 107
Disabling Buffer Overflow Protection 108
Configuring Scheduled Scanning 108

17: Antivirus: General Antivirus **111**
Antivirus Certifications for NICE Products 111
General Instructions 111
General Limitations 111
Trellix ePO 112
Trellix 112
Trellix ENS Certification 112
SEP 113
SEP Limitations 115
Trend Micro 117
Sophos 117
Microsoft Defender Antivirus 117
Antivirus Matrixes for NICE Products 118
NICE Engage 7.x Antivirus Support 118

18: Remote Connection to Customers **121**

19: NICE Third Party Software Certification Policy **123**
NICE Products 123

Compatibility Validation Policy **125**
Compatibility Validation Process **127**
Compatibility Validation by Professional Services 128
Compatibility Validation Guidelines **129**
Antivirus Software 129
Microsoft Windows Operating System 130
Microsoft Service Packs 130
Microsoft .NET Framework 130
Microsoft SQL Server 130
Microsoft SQL Server Service Packs 131
Web Browsers 131
Microsoft Security Patches 131
Microsoft Security Advisory Patches 132
Microsoft Daylight Saving (DST) Updates 132
Patch Management Tools 132
Remote Support Tools 133
Server Hardening **133**
Compatibility Matrix **134**

20: Vulnerability Scanner Guidelines **137**

Nessus Vulnerability Scanner **138**
Advanced Interaction Recorder 138
Interactions Center 138

21: SQL Backup **139**

SQL Backup Guidelines **139**
Overview 139
Schedule 139
Backup Files Location 140
Implementation Guidelines 140
Backup Tools 140
Database Configuration Guidelines **140**

[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 serves as general guidelines and applies to all existing NICE Engage 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.

Scope of this Guide

Software Version

This guide is updated for:

- NICE Engage Platform 7.4.
- Advanced Process Automation

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*
Setting up a client computer to work with ASPX	*Workstation Setup*
Configuring XBAP	*Workstation Setup*
Microsoft Daylight Savings Time configurations	*Maintenance*

Document Revision History

Revision	Date	Software Version	Description
A4	September 2024	Engage 7.4.4	Updated Microsoft Software Service Packs Certified by NICE on page 13
A3	July 2024	Engage 7.4 (Playback Portal 7.5)	■ Updated Additional Third Party Components on page 69. ■ Updated Microsoft .NET Framework on page 63
A2	May 2024	Engage 7.4	Updated Microsoft Software Service Packs Certified by NICE on page 13
A1	March 2024	Engage 7.4	Updated: ■ Microsoft .NET Framework on page 63 ■ Microsoft Software Service Packs Certified by NICE on page 13

Revision	Date	Software Version	Description
A0	December 2023	Engage 7.4	Rebranded for Engage 7.4. Delta from Engage 7.3 includes: ■ Removed Windows 7, 8, 8.1 support from Engage 7.4 in the following: ■ Microsoft Edge with IE Mode on page 33 ■ Microsoft Client Operating Systems: Windows 10 32-bit or 64-bit on page 23 ■ Microsoft Client Operating Systems: Windows 11 64-bit on page 27 ■ Microsoft Kerberos Configuration Manager on page 75 ■ Microsoft Security Bulletins on page 85 ■ NICE Third Party Software Certification Policy on page 123 ■ Removed Internet Explorer support from Engage 7.4 in the following: ■ Web Browsers on page 31 ■ Section Microsoft Edge with IE Mode on page 33 ■ Section NICE Third Party Software Certification Policy on page 123 ■ Google Chrome with the IE Tab Extension on page 51 ■ Microsoft Kerberos Configuration Manager on page 75 ■ Updated ActiveMQ Artemis on page 69 ■ Updated Folders and Files Exclusion on page 94

Revision	Date	Software Version	Description
			▪ Updated Microsoft .NET Framework on page 63 (Playback Portal 7.4 Requirements added) ▪ Updated Microsoft Software Service Packs Certified by NICE on page 13 ▪ Updated Additional Third Party Components on page 69

2

Microsoft Software Service Packs Certified by NICE

This section lists the Microsoft Software Service Packs certified by NICE. These service pack versions are part of the site readiness tests in the SRT, in addition to the minimum hardware and software requirements that are in the *Certified Servers*.

Product	NICE Engage Platform
Release	NICE Engage Platform 7.x
Synopsis	Provides information regarding the latest Microsoft Software Service Packs certified by NICE.

Below are two tables that list the latest Microsoft Software Service Packs certified by NICE for servers and client machines.

Windows Server and SQL Server Service Packs

Microsoft Software	Service Pack	NICE Release	Comment
Windows 2016 Datacenter 64-bit		NICE Engage Platform 7.x	
Windows 2016 Standard 64-bit		NICE Engage Platform 7.x	

2: Microsoft Software Service Packs Certified by NICE

Microsoft Software	Service Pack	NICE Release	Comment
Windows 2016 Datacenter 64-bit	Supported Creator Updates: Version 1709	NICE Engage Platform 7.x	
Windows 2016 Standard 64-bit	Supported Creator Updates: Version 1709	NICE Engage Platform 7.x	
Windows 2019 Standard 64-bit		NICE Engage Platform 7.x	
Windows 2019 Datacenter 64-bit		NICE Engage Platform 7.x	
SQL Server 2016 Enterprise Edition 64-bit	SP2	NICE Engage Platform 7.x NICE Sentinel 7.x Playback Portal 6.8	
SQL Server 2016 Standard 64-bit	SP2	NICE Engage Platform 7.x NICE Sentinel 7.x Playback Portal 6.8	
SQL Server 2016 Enterprise Edition 64-bit	SP2 CU11	NICE Engage Platform 7.x NICE Sentinel 7.x Playback Portal 6.8	
SQL Server 2016 Standard 64-bit	SP2 CU11	NICE Engage Platform 7.x NICE Sentinel 7.x Playback Portal 6.8	

2: Microsoft Software Service Packs Certified by NICE

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2016 Enterprise Edition 64-bit	SP2 CU11 (KB 4527378)	NICE Engage Platform 7.x NICE Sentinel 7.x Playback Portal 6.8	CU Release Date: September 12, 2019 NICE Certification Date: January 20, 2020
SQL Server 2016 Enterprise Edition 64-bit	SP2 CU12 (KB 4536648)	NICE Engage Platform 7.x NICE Sentinel 7.x Playback Portal 6.8	CU Release Date: February 25, 2020 NICE Certification Date: March 17, 2020
SQL Server 2016 Enterprise Edition 64-bit	SP2 CU13 (KB 4549825)	NICE Engage Platform 7.x NICE Sentinel 7.x Playback Portal 6.8	CU Release Date: May 28, 2020 NICE Certification Date: August 7, 2020
SQL Server 2016 Enterprise Edition 64-bit	SP2 CU14 (KB4564903)	NICE Engage Platform 7.x NICE Sentinel 7.x Playback Portal 6.8	CU Release Date: August 6, 2020 NICE Certification Date: August 28, 2020
SQL Server 2016 Enterprise Edition 64-bit	SP2 CU15 (KB4577775)	NICE Engage Platform 7.x NICE Sentinel 7.x Playback Portal 6.8	CU Release Date: September 28, 2020 NICE Certification Date: October 8, 2020
SQL Server 2016 Enterprise Edition 64-bit	SP2 CU16 (KB5000645)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: February 11, 2021 NICE Certification Date: March 29, 2021
SQL Server 2016 Enterprise Edition 64-bit	SP2 CU17 (KB5001092)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: March 29, 2021 NICE Certification Date: April 23, 2021

2: Microsoft Software Service Packs Certified by NICE

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2016 Enterprise Edition 64-bit	SP3 (KB5003279)	NICE Engage Platform 7.x NICE Sentinel 7.x	SP Release Date: September 15, 2021 NICE Certification Date: January 22, 2022
SQL Server 2016 Standard 64-bit	SP3 (KB5003279)	NICE Engage Platform 7.x NICE Sentinel 7.x	SP Release Date: September 15, 2021 NICE Certification Date: January 22, 2022
SQL Server 2019 Standard 64-bit	CU13 (KB5005679)	NICE Engage Platform 7.x	CU Release Date: October 5, 2021 NICE Certification Date: January 22, 2022
SQL Server 2019 Enterprise Edition 64-bit	CU13 (KB5005679)	NICE Engage Platform 7.x	CU Release Date: October 5, 2021 NICE Certification Date: January 22, 2022
SQL Server 2019 Standard 64-bit	CU14 (KB 5007182)	NICE Engage Platform 7.x	CU Release Date: November 22, 2021 NICE Certification Date: January 22, 2022
SQL Server 2019 Enterprise Edition 64-bit	CU14 (KB 5007182)	NICE Engage Platform 7.x	CU Release Date: November 22, 2021 NICE Certification Date: January 22, 2022

2: Microsoft Software Service Packs Certified by NICE

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2019 Standard 64-bit	CU16 (KB5011644)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: April 18, 2022 NICE Certification Date: August 18, 2022
SQL Server 2019 Enterprise Edition 64-bit	CU16 (KB5011644)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: April 18, 2022 NICE Certification Date: August 18, 2022
SQL Server 2019 Standard 64-bit	CU18 (KB5017593)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: September 28, 2022 NICE Certification Date: November 8, 2022
SQL Server 2019 Enterprise Edition 64- bit	CU18 (KB5017593)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: September 28, 2022 NICE Certification Date: November 8, 2022
SQL Server 2019 Standard 64- bit	CU19 (KB5023049)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: February 16, 2023 NICE Certification Date: March 14, 2023

2: Microsoft Software Service Packs Certified by NICE

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2019 Enterprise Edition 64- bit	CU19 (KB5023049)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: February 16, 2023 NICE Certification Date: March 14, 2023
SQL Server 2019 Standard 64-bit	CU20 (KB5024276)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: April 13, 2023 NICE Certification Date: June 1, 2023
SQL Server 2019 Enterprise Edition 64- bit	CU20 (KB5024276)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: April 13, 2023 NICE Certification Date: June 1, 2023
SQL Server 2019 Standard 64-bit	CU21 (KB5025808)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: June 15, 2023 NICE Certification Date: July 18, 2023
SQL Server 2019 Enterprise Edition 64- bit	CU21 (KB5025808)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: June 15, 2023 NICE Certification Date: July 18, 2023
SQL Server 2019 Standard 64-bit	CU22 (KB5027702)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: August 15, 2023 NICE Certification Date: September 26, 2023

2: Microsoft Software Service Packs Certified by NICE

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2019 Enterprise Edition 64- bit	CU22 (KB5027702)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: August 15, 2023 NICE Certification Date: September 26, 2023
SQL Server 2019 Standard 64-bit	CU23 (KB5030333)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: October 12, 2023 NICE Certification Date: October 30, 2023
SQL Server 2019 Enterprise Edition 64- bit	CU23 (KB5030333)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: October 12, 2023 NICE Certification Date: October 30, 2023
SQL Server 2019 Standard 64-bit	CU24 (KB5031908)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: December 14, 2023 NICE Certification Date: March 15, 2024
SQL Server 2019 Enterprise Edition 64-bit	CU24 (KB5031908)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: December 14, 2023 NICE Certification Date: March 15, 2024
SQL Server 2019 Standard 64-bit	CU25 (KB5033688)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: February 15, 2024 NICE Certification Date: March 15, 2024

2: Microsoft Software Service Packs Certified by NICE

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2019 Enterprise Edition 64-bit	CU25 (KB5033688)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: February 15, 2024 NICE Certification Date: March 15, 2024
SQL Server 2019 Standard 64-bit	CU26 (KB5035123)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: April 11, 2024 NICE Certification Date: May 14, 2024
SQL Server 2019 Enterprise Edition 64-bit	CU26 (KB5035123)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: April 11, 2024 NICE Certification Date: May 14, 2024
SQL Server 2019 Standard 64-bit	CU27 (KB5037331)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: June 14, 2024 NICE Certification Date: September 2, 2024
SQL Server 2019 Enterprise Edition 64-bit	CU27 (KB5037331)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: June 14, 2024 NICE Certification Date: September 2, 2024
SQL Server 2019 Standard 64-bit	CU28 (KB5039747)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: August 1, 2024 NICE Certification Date: September 2, 2024

2: Microsoft Software Service Packs Certified by NICE

Microsoft Software	Service Pack	NICE Release	Comment
SQL Server 2019 Enterprise Edition 64-bit	CU28 (KB5039747)	NICE Engage Platform 7.x NICE Sentinel 7.x	CU Release Date: August 1, 2024 NICE Certification Date: September 2, 2024

Windows Client Software Service Packs

Microsoft Software	SP/Creator Update	NICE Release	Comment
Windows 10	Supported Creator Updates: Version 1511 Version 1703 Version 1709 Version 1803 Version 1809 Version 1903 Version 1909 Version 2004 Version 20H2 Version 21H1 Version 21H2 Version 22H2	NICE Engage Platform 7.x	
Windows 11	Supported Creator Updates: Version 21H2 Version 22H2 Version 23H2	NICE Engage Platform 7.x	

[This page intentionally left blank]

3

Microsoft Client Operating Systems: Windows 10 32-bit or 64-bit

NICE Engage Platform Release 7.x supports Windows 10. This section provides information on Microsoft Windows 10 Operating system, both in the 32-bit and 64-bit versions.

In addition to the operating systems that are highlighted in this section, NICE Engage Platform was also certified for Windows 11.

General Information: Localization

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

Windows 10 Client Applications Compatibility

From NICE Engage 7.x, Microsoft Windows 10 Pro Edition and Windows 10 Enterprise Edition are compatible with NICE client applications, in both 32-bit and 64-bit configurations.

	Windows 10 Pro		Windows 10 Enterprise	
Application	**32-bit**	**64-bit**	**32-bit**	**64-bit**
ScreenAgent	Approved	Approved	Approved	Approved
Record on Demand/Stop on Demand	Approved	Approved	Approved	Approved

	Windows 10 Pro		Windows 10 Enterprise	
Application	**32-bit**	**64-bit**	**32-bit**	**64-bit**
Standalone NICE Player and NICE Player Codec Pack	Approved	Approved	Approved	Approved
Reporter Viewer	Approved	Approved	Approved	Approved
Survey Manager	Not approved	Not approved	Not approved	Not approved
VRA	Not approved	Not approved	Not approved	Not approved
BSF Tool Kit	Approved	Approved	Approved	Approved
NICE Sentinel Remote Client	Approved	Approved	Approved	Approved
NDM/SRT/RHT	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 on the facing page
- Record on Demand on the facing page
- NICE BSF Toolkit 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
```

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.

4

Microsoft Client Operating Systems: Windows 11 64-bit

NICE Engage Platform Release 7.x supports Windows 11. This section provides information on Microsoft Windows 11 Operating system 64-bit version.

In addition to the operating systems that are highlighted in this section, NICE Engage Platform was also certified for Windows 10.

General Information: Localization

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

Windows 11 Client Applications Compatibility

From NICE Engage 7.x, Microsoft Windows 11 Pro Edition and Windows 11 Enterprise Edition are compatible with NICE client applications.

Important! Before using Windows 11 Pro or Enterprise Editions with supported browsers, configure the required browser. See Enabling IE Mode for Microsoft Edge on page 34 or Adding the IE Tab to Google Chrome on page 54.

Application	Windows 11 Pro 64-bit	Windows 11 Enterprise 64-bit
ScreenAgent	Approved	Approved

Application	Windows 11 Pro 64-bit	Windows 11 Enterprise 64-bit
IntelliAgent (ConnectAPI)	Approved	Approved
Record on Demand/Stop on Demand	Approved	Approved
Standalone NICE Player and NICE Player Codec Pack	Approved	Approved
Reporter Viewer	Approved	Approved
BSF Tool Kit	Approved	Approved
NICE Sentinel Remote Client	Approved	Approved
NDM/SRT/RHT	Approved	Approved
High Availability Manager	Approved	Approved
NICE Web Applications	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 11:

- Reporter Viewer
- NICE Player and NICE Player Codec Pack on the facing page
- Record on Demand on the facing page
- NICE BSF Toolkit 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
```

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 11 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 11:

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

Web Browsers

Important! Microsoft announced that Internet Explorer 11 (IE11) desktop application **retired** on June 15, 2022. For more information, see Internet Explorer 11 desktop app retirement FAQ. NICE Engage Platform is fully compatible with Microsoft Edge and Google Chrome browsers.

To continue working in your NICE environment, follow one of these options:

- Use the Microsoft Edge browser in IE mode. This is the official Microsoft alternative to IE11. Microsoft have stated that they are committed to supporting this solution until at least 2029.

  For more details, see The future of Internet Explorer on Windows 10 is in Microsoft Edge.

  To configure Microsoft Edge with IE Mode for Engage, see Microsoft Edge with IE Mode on page 33.

- Use the Google Chrome browser with IE Tab. IE Tab is a certified extension to Chrome from Blackfish Software that fully supports IE11.

  For more details, see IE Tab - Run Internet Explorer Inside Chrome.

  To configure Google Chrome with the IE Tab Extension for Engage, see Google Chrome with the IE Tab Extension on page 51.

[This page intentionally left blank]

6

Microsoft Edge with IE Mode

This section describes compatibility of the Microsoft Edge browser in IE Mode with NICE Web Applications.

Compatibility of NICE Web Applications with Microsoft Edge in IE Mode

Browser	Support Policy
Microsoft Edge	Latest supported public version IE Mode

Product	NICE Engage Platform, NICE Sentinel, NICE Advanced Process Automation, NICE Playback Portal, Compliance Center
Release	NICE Engage Platform 7.x Compliance Center 8.9 and above NICE Sentinel: ▪ NICE Sentinel Server ▪ NICE Sentinel Remote Client

Synopsis	Windows 11 Pro 64-bit Windows 11 Enterprise 64-bit Windows 10 Pro 32/64-bit Windows 10 Enterprise 32/64-bit Windows Server 2016 Datacenter 64-bit Windows Server 2016 Standard 64-bit Windows Server 2019 Datacenter 64-bit Windows Server 2019 Standard 64-bit

Client Application Compatibility

The following table shows the NICE Engage Platform 7.x client applications compatible with IE Mode in Microsoft Edge.

Application	Latest Supported Public IE Mode Version
NICE Web Applications	Approved
RTA	Approved
Reporter	Approved
NICE Sentinel Remote Client	Approved
NICE Playback Portal	Approved
Compliance Assurance	Approved
Policy Manager	Approved
Fraudster Exposure	Approved
Authentication spotlight	Approved

Enabling IE Mode for Microsoft Edge

This section describes how to use Edge in IE Mode to access NICE Web Applications. This is necessary because Edge does not support ActiveX controls, Browser Helper Objects, VBScript, or other legacy technology. To access the NICE Web Applications that use this technology, you can configure Edge to automatically load these sites in IE Mode.

Before you configure Edge with IE Mode, make sure that all your workstations have the latest version of Edge.

To enable IE Mode in Edge, perform *one* of the following procedures:

a. Configuring IE Mode in Microsoft Edge Simplified Procedure below

b. Configuring IE Mode in Microsoft Edge over Domain Controller GPO on page 39

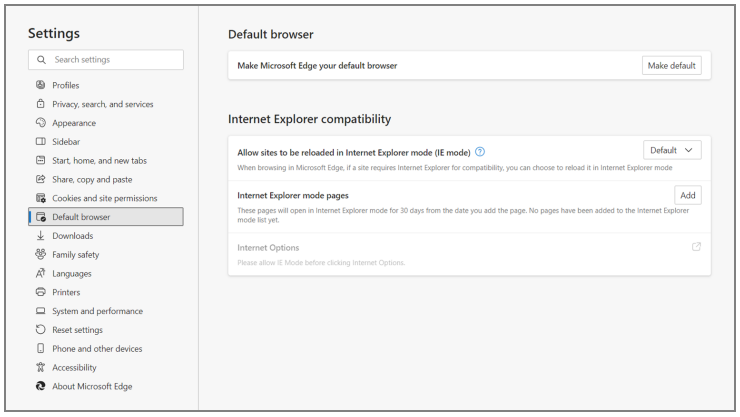
Configuring IE Mode in Microsoft Edge Simplified Procedure

1. Open Microsoft Edge.

2. Do one of the following:

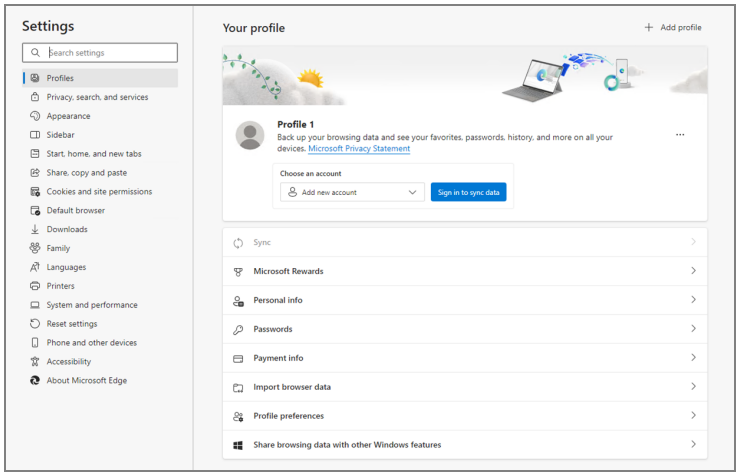
   a. In the address bar, enter **edge://settings/defaultbrowser**.

      The Settings window appears with **Default browser** selected.



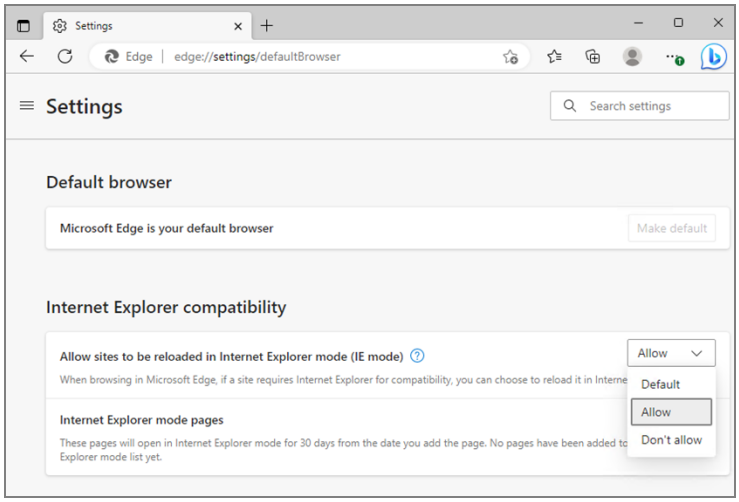
   b. Click the ellipsis menu button and select **Settings**.

      The Settings window appears.

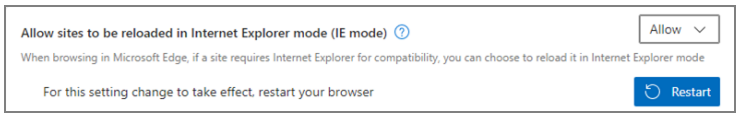


In the Settings window, select **Default browser**.

3. From the **Allow sites to be reloaded in Internet Explorer mode (IE mode)** dropdown menu, select **Allow**.

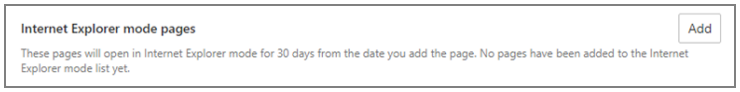


4. To apply the settings changes, click **Restart** in the **Allow sites to be reloaded in Internet Explorer mode (IE mode)** area.

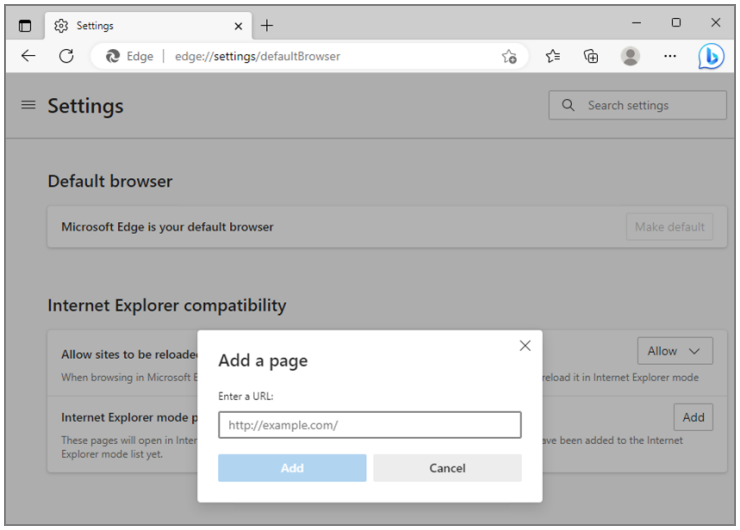


The browser restarts.

5. In the **Internet Explorer mode pages** area, click **Add** to add the NICE Engage URL.



The Add a page window appears.



6. In the URL field, enter the NICE Engage URL and click **Add**.

Important! The NICE Engage URL must have the following format: **https://<*Engage_FQDN*>/Nice**. Remember that the URL is case sensitive.

If the following NICE Engage components are used, enter the NICE Engage URLs below:

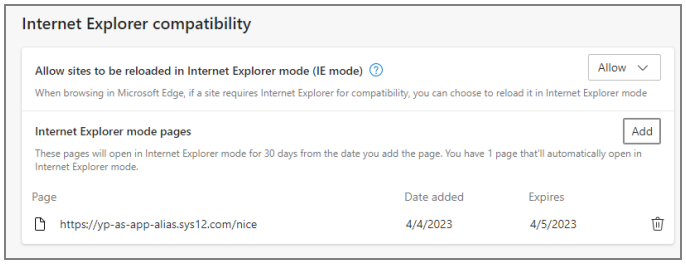
NICE Engage Components	NICE Engage URL
Policy Manager	https://yp-as-app-alias.sys12.com:63343/PolicyManager/index.html
Compliance Assurance	https://yp-as-app-alias.sys12.com:63343/compliance-assurance/index.html
Fraudster Exposure	https://yp-as-app-alias.sys12.com:63343/fraudster-exposure/index.html
Authentication Spotlight	https://bs-aa-app-acg.sys12.com:63343/Spotlight/index.html
Insight Amplifier	https://bs-aa-app-acg.sys12.com:63343/ccih-insight-amplifier-application/index.html

Show Tip

Port 63343 is used with secure communication (https), and port 63342 is used without secure communication (http).

The added URL appears in the **Internet Explorer mode pages** area.

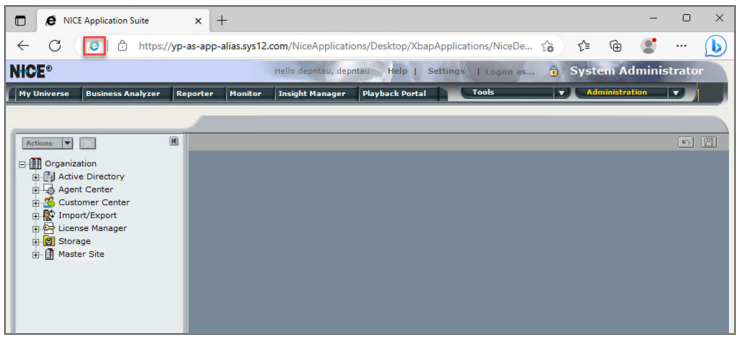
View image



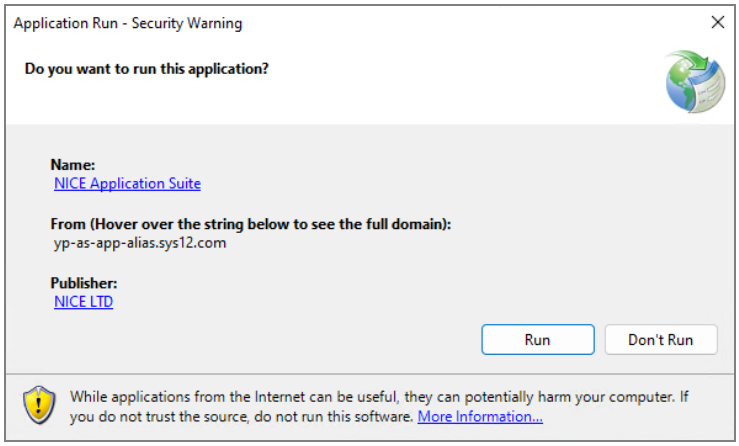
7. Verify that the NICE Engage URL is added to the Trusted sites, see *Adding NICE Engage URL to the Trusted sites* in the *Workstation Setup Configuration Guide*.

8. Open Microsoft Edge and log in to Engage.

   If the IE Mode configuration is working, the Internet Explorer favicon will appear on the left side of the navigation bar.



The Application Run - Security Warning window appears.



In the Application Run - Security Warning window, click **Run**, and log in to Engage.

Important! Using multiple browser types at the same time, on the same workstation, is not supported in Engage 7.x. For example, Microsoft Edge and Google Chrome cannot both be open and in use on the same workstation, at the same time.

Configuring IE Mode in Microsoft Edge over Domain Controller GPO

This procedure is optional and can be performed for configuring IE mode in Edge on all workstations placed in domain without the 30 day limitation from Microsoft.

You can use group policy objects to configure policy settings for Microsoft Edge. To configure Edge with group policy objects, you have to install administrative templates. Depending on your **Platform**, download the Microsoft Edge policy templates file from Download and configure Microsoft Edge for Business.

The policy template files add rules and settings for Microsoft Edge to the group policy in the domain controller for your domain or to the Policy Definition template folder on your individual computer, as described in:

- To Add the Administrative Template to the Domain Controller: below
- To Add the Administrative Template to an Individual Computer: on the next page

To Add the Administrative Template to the Domain Controller:

1. On a domain controller or workstation with RSAT, browse to the **PolicyDefinition** folder (also known as the Central Store) on any domain controller for your domain.

   For older versions of Windows Server, you may need to create the PolicyDefinition folder. For more information, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows.

2. Open **MicrosoftEdgePolicyTemplates**, and go to **windows > admx**.

3. Copy the **msedge.admx** file to the **PolicyDefinition** folder. (Example: %systemroot%\sysvol\domain\policies\PolicyDefinitions)

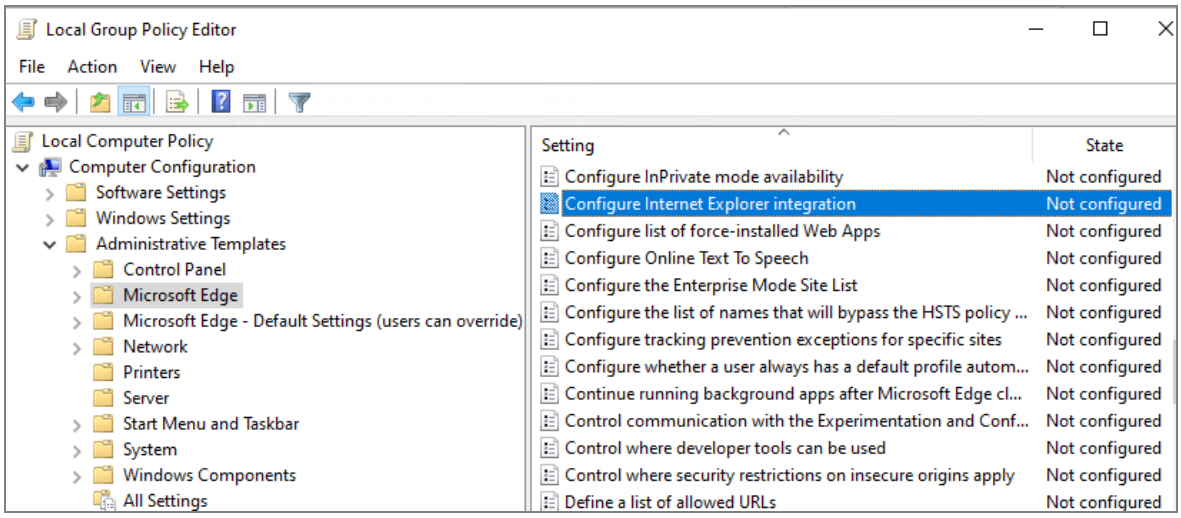
4. In the **admx** folder, open the appropriate language folder. For example, if you're in the U.S., open the en-US folder.

5. Copy the **msedge.adml** file to the matching language folder in the **Policy Definition** folder. Create the folder if it does not already exist. (Example: %systemroot%\sysvol\domain\policies\PolicyDefinitions\EN-US)

6. If your domain has more than one domain controller, the new **ADMX** files will be replicated to them at the next domain replication interval.

7. To confirm the files loaded correctly, open the **Local Group Policy Editor** from Windows Administrative Tools and expand **Computer Configuration** > **Administrative Templates** > **Microsoft Edge**. You should see one or more Microsoft Edge nodes as shown below.

View image



8. Continue with Configuring the Internet Explorer Integration Policy on the facing page.

To Add the Administrative Template to an Individual Computer:

1. On the target computer, open **MicrosoftEdgePolicyTemplates**, and go to **windows** > **admx**.

2. Copy the **msedge.admx** file to your Policy Definition template folder. (Example: C:\Windows\PolicyDefinitions)

3. In the **admx** folder, open the appropriate language folder. For example, if you're in the U.S., open the en-US folder.

4. Copy the **msedge.adml** file to the matching language folder in your **Policy Definition** folder. (Example: C:\Windows\PolicyDefinitions\en-US)

5. To confirm the files loaded correctly either open Local Group Policy Editor directly (Windows key + R and enter gpedit.msc) or open MMC and load the Local Group Policy Editor snap-in. If an error occurs, it's usually because the files are in an incorrect location.

6. Continue with Configuring the Internet Explorer Integration Policy below.

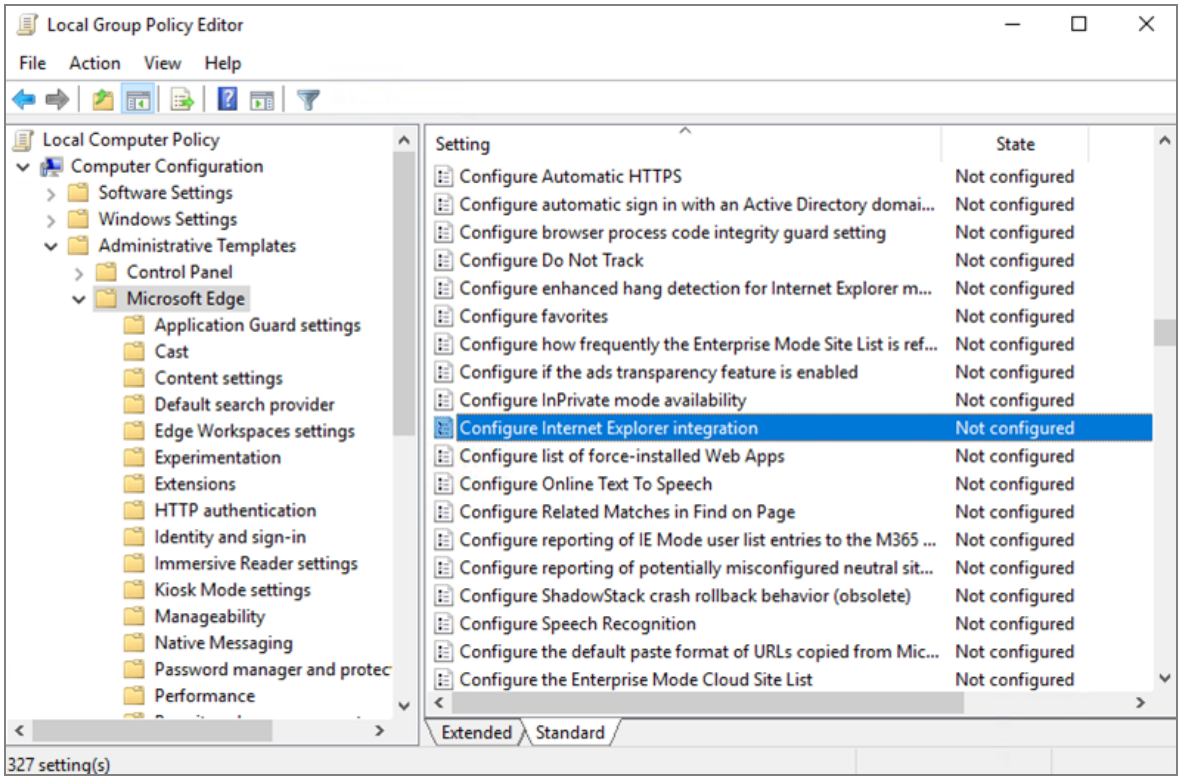
Configuring the Internet Explorer Integration Policy

To enable IE Mode in Edge you need to configure the **Internet Explorer integration** settings in the group policy.

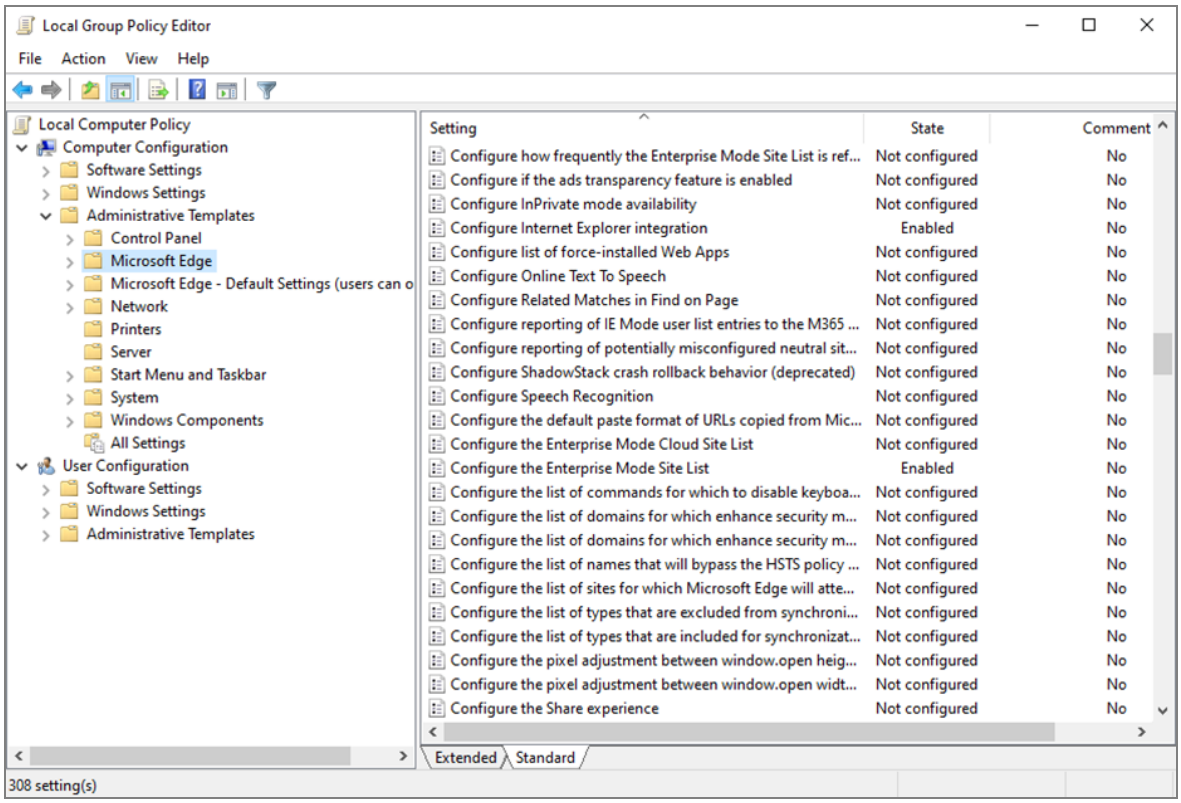
To configure the Internet Explorer integration policy:

1. In the **Local Group Policy Editor (gpedit.msc)**, under **Computer Configuration**, browse to **Administrative Templates** > **Microsoft Edge**.

View image

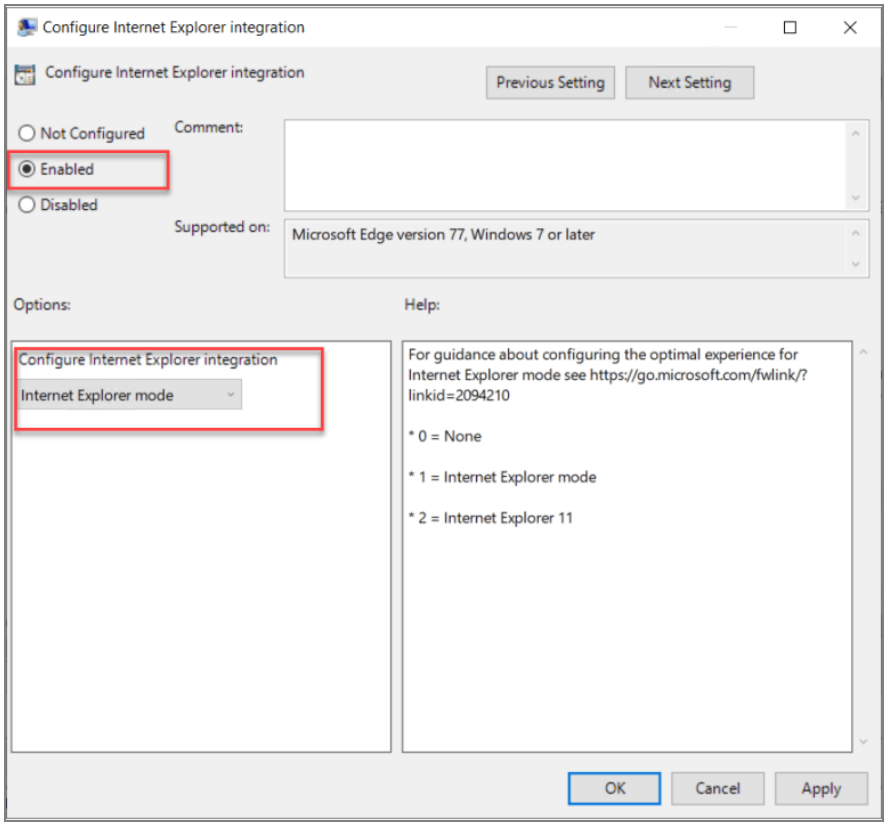


View image



2. Click **Configure Internet Explorer integration**. The Configure Internet Explorer integration window appears.

View image



3. Select the **Enabled** radio button, then, in the Options area select **Internet Explorer mode** from the dropdown menu.

4. Click **Apply**, then click **OK** to close the Configure Internet Explorer integration window.

5. Continue with Configuring the Enterprise Mode Site List below.

Configuring the Enterprise Mode Site List

To enable IE Mode in Edge, configure the Enterprise Mode Site List policy settings in the group policy. The Enterprise Mode Site List Manager helps create and manage XML files for IE Mode. An XML file can also be created manually.

This procedure will allow to use a web page without the 30 day limitation from Microsoft.

To configure the Enterprise Mode Site List:

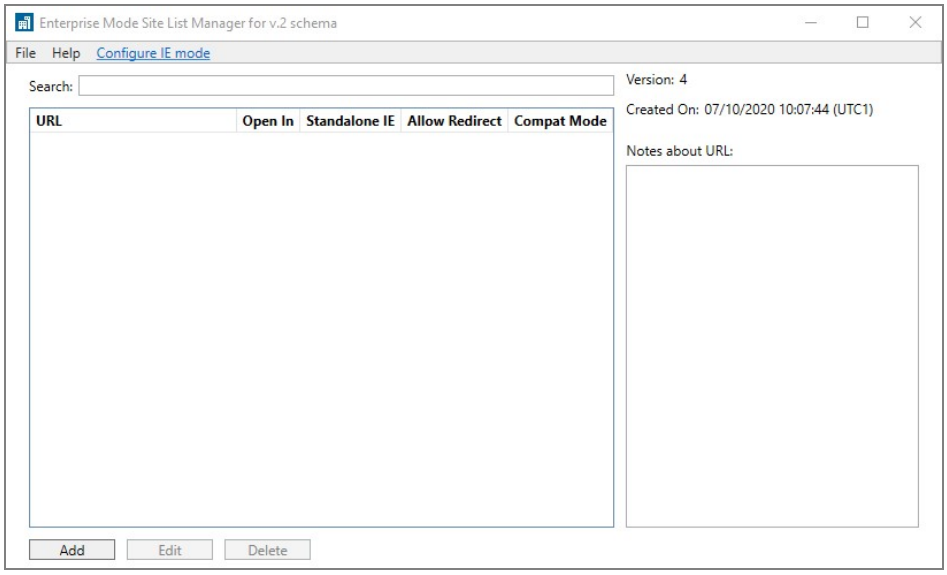
1. Download and install the Enterprise Mode Site List Manager (schema v.2): https://www.microsoft.com/en-us/download/details.aspx?id=49974.

2. Open the **Enterprise Mode Site List Manager** application

.

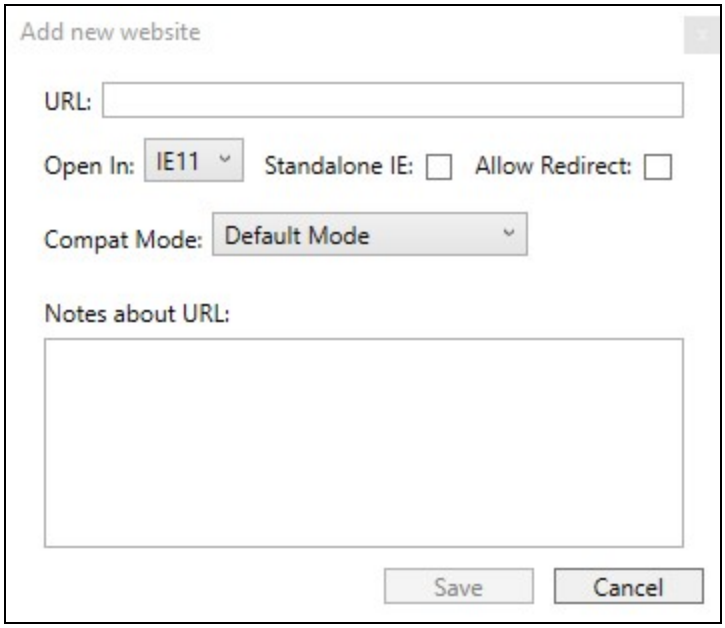
   The Enterprise Mode Site List Manager for v.2 schema window appears.

   View image



3. Click **Add**. The Add new website window appears.

   View image



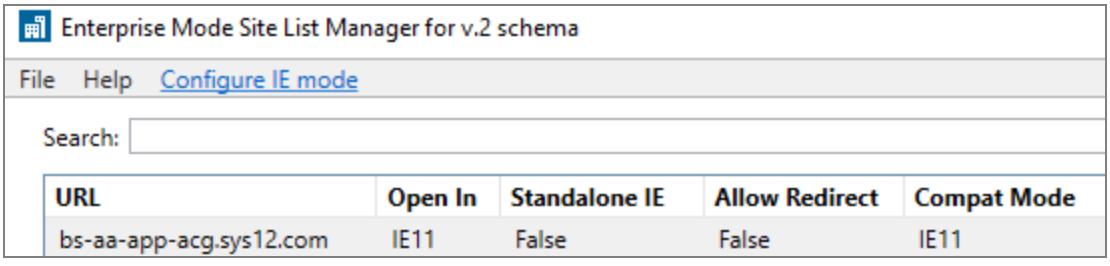
4. Enter the following information:
   a. In the **URL** field, enter your Engage FQDN without http or https. The Enterprise Mode Site List Manager tool automatically attempts to run both versions during the validation of the URL. If you are in an AD FS environment, you need to add the FQDN of the Federation Service name.

   b. From the **Open In** dropdown menu, select **IE11**.

   c. Ensure the **Standalone IE** check box and the **Allow Redirect** check box are unchecked.

   d. Click **Save**. The Enterprise Mode Site List Manager window appears with the list of sites you selected to open in IE Mode.

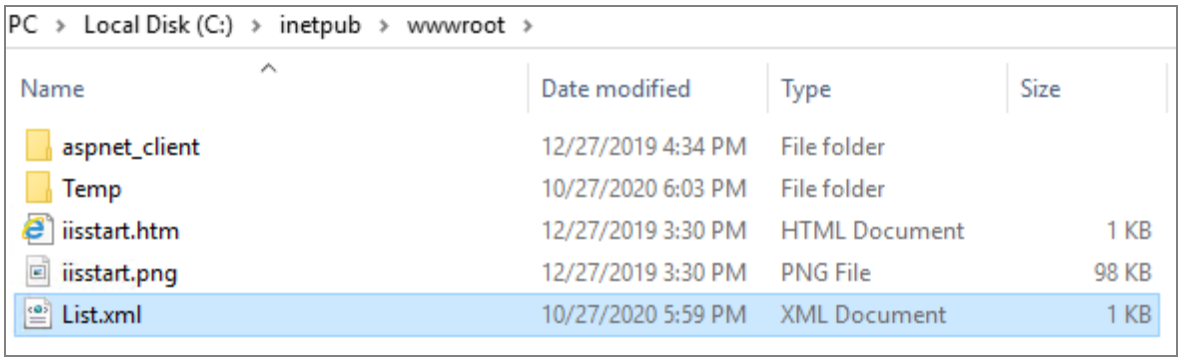
View image



5. Select **File**, then select **Save to XML**.

6. Copy the xml file to the **Application server** in the folder **C:\inetpub\wwwroot.**

View image



Example:

```
<site-list version="1">
<created-by>
<tool>EMIESiteListManager</tool>
<version>12.0.0.0</version>
<date-created>05/16/2023 13:05:20</date-created>
</created-by>
<site url="yp-as-app-alias.sys12.com">
<compat-mode>Default</compat-mode>
<open-in>IE11</open-in>
</site>
</site-list>
```

7. Continue with Configuring the Enterprise Mode Site List Policy below.

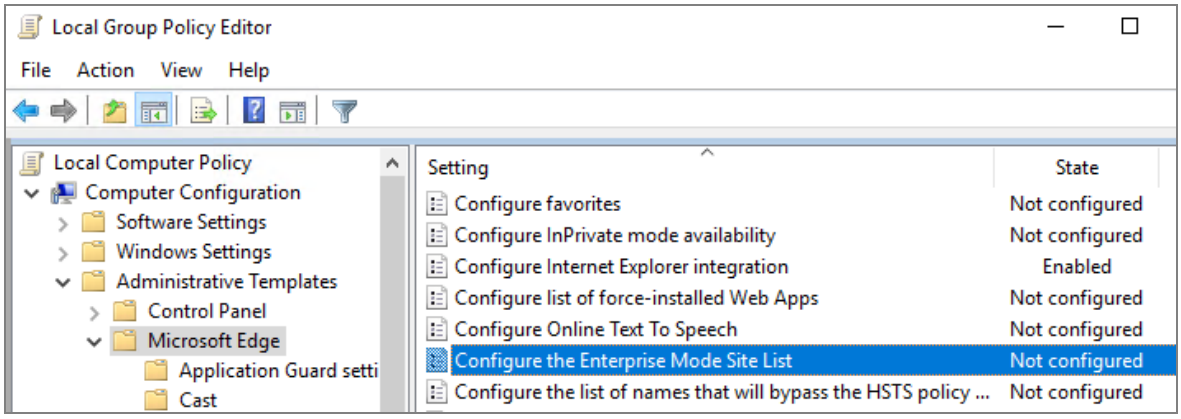
Configuring the Enterprise Mode Site List Policy

To enable IE Mode in Edge you need to configure the Enterprise Mode Site List policy settings in the group policy.

To configure the Enterprise Mode Site List Policy:

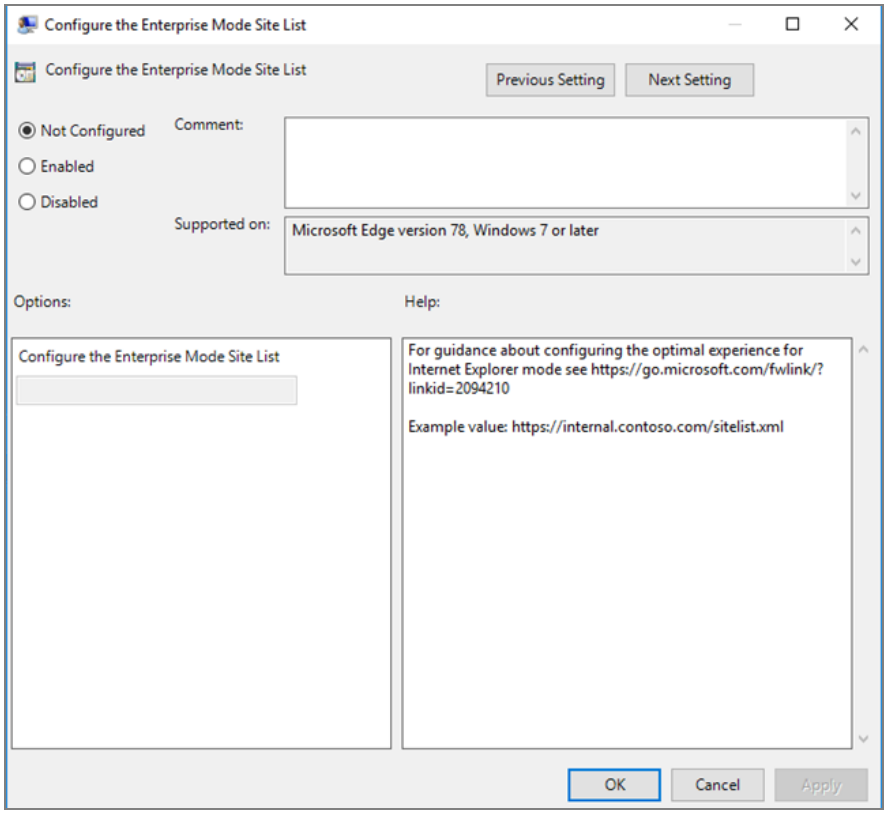
1. In the **Local Group Policy Editor (gpedit.msc)**, under **Computer Configuration**, browse to **Administrative Templates** > **Microsoft Edge**.

View image



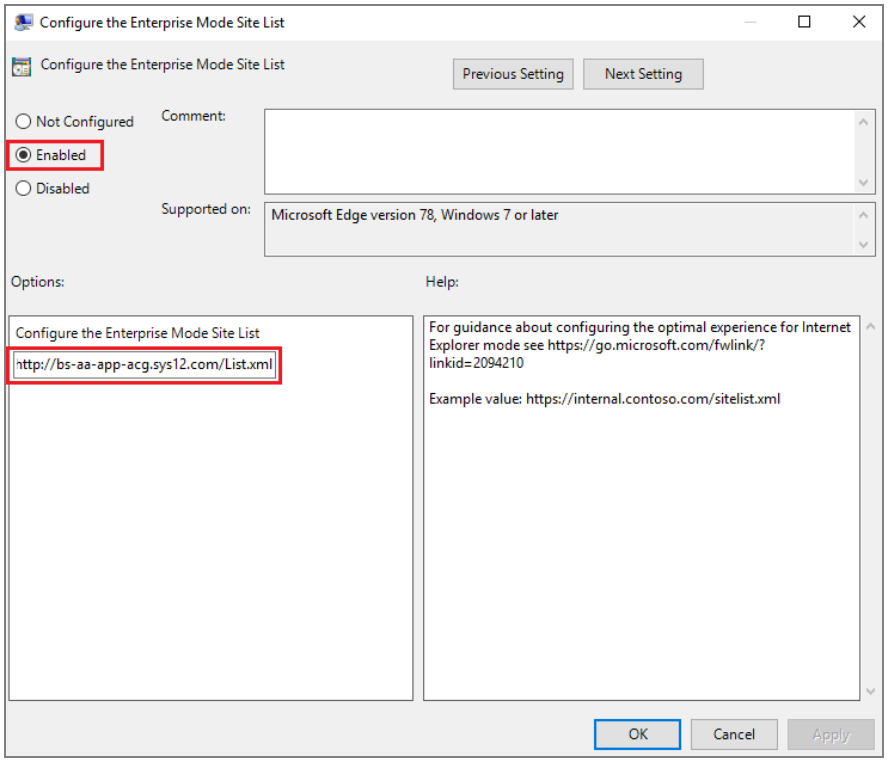
2. Click **Configure the Enterprise Mode Site List**. The Configure the Enterprise Mode Site List window appears.

View image



3. Select the **Enabled** radio button, then in the Options area enter the location of your site list.

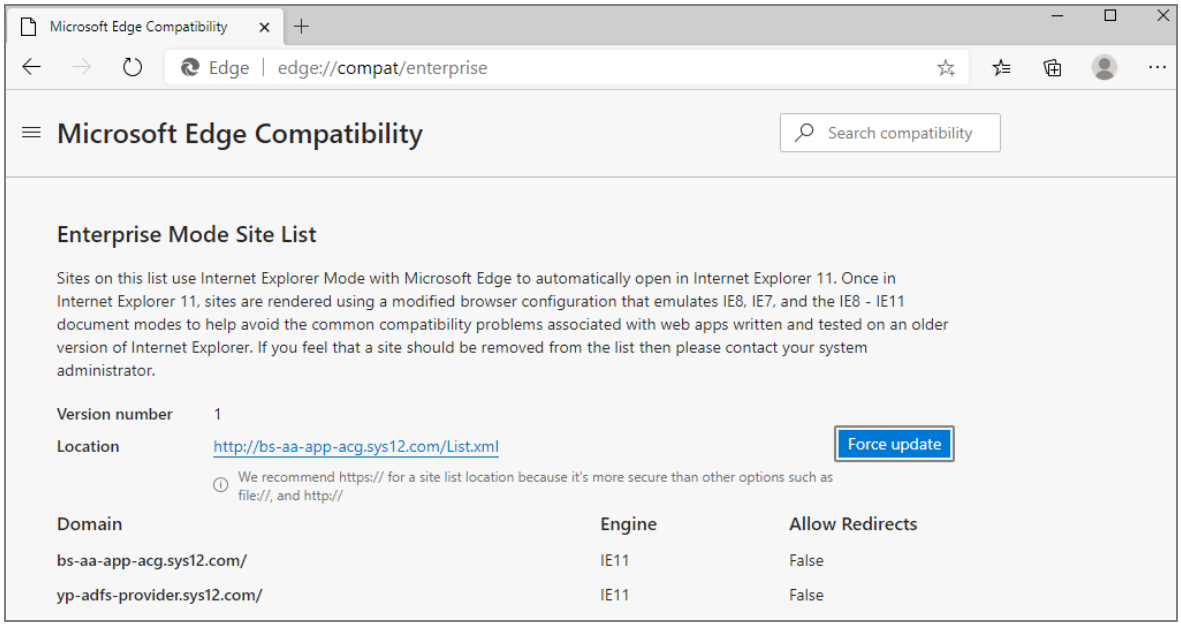
View image



4. Click **Apply**, then click **OK** to close the Configure the Enterprise Mode Site List window.

5. Open Microsoft Edge, in the address bar, enter **edge://compat/enterprise**, and check if the Enterprise Mode Site List is updated.

View image


Microsoft Edge Compatibility
Edge | edge://compat/enterprise
Microsoft Edge Compatibility
Search compatibility
Enterprise Mode Site List
Sites on this list use Internet Explorer Mode with Microsoft Edge to automatically open in Internet Explorer 11. Once in Internet Explorer 11, sites are rendered using a modified browser configuration that emulates IE8, IE7, and the IE8 - IE11 document modes to help avoid the common compatibility problems associated with web apps written and tested on an older version of Internet Explorer. If you feel that a site should be removed from the list then please contact your system administrator.
Version number 1
Location http://bs-aa-app-acg.sys12.com/List.xml
Force update
We recommend https:// for a site list location because it's more secure than other options such as file://, and http://
Domain
Engine
Allow Redirects
bs-aa-app-acg.sys12.com/ IE11 False
yp-adfs-provider.sys12.com/ IE11 False

[This page intentionally left blank]

7

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.

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

Browser	Support Policy
Google Chrome	Latest supported public version IE-Tab

Product	NICE Engage Platform, NICE Sentinel, NICE Advanced Process Automation, NICE Playback Portal, Compliance Center
Release	NICE Engage Platform 7.x NICE Sentinel: ▪ NICE Sentinel Server ▪ NICE Sentinel Remote Client
Synopsis	Windows 11 Pro 64-bit Windows 11 Enterprise 64-bit Windows 10 Pro 32/64-bit Windows 10 Enterprise 32/64-bit Windows Server 2016 Datacenter 64-bit Windows Server 2016 Standard 64-bit Windows Server 2019 Datacenter 64-bit Windows Server 2019 Standard 64-bit

General Description and Conclusions

General tests were performed using the IE Tab extension in Google Chrome with Engage Platform 7.x

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 10, or Windows 11 client systems.

Client Application Compatibility

The following table shows the NICE Engage Platform 7.x client applications compatible with Microsoft Edge in IE Mode.

Application	Latest Supported Public IE Mode Version
NICE Web Applications	Approved
RTA	Approved
Reporter	Approved
NICE Sentinel Remote Client	Approved
NICE Playback Portal	Approved
Compliance Assurance	Approved
Policy Manager	Approved
Fraudster Exposure	Approved
Authentication spotlight	Approved

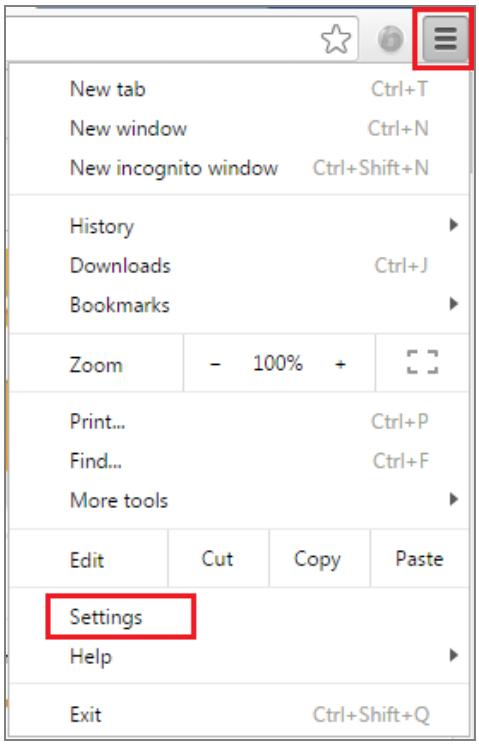
Adding the IE Tab to Google Chrome

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

To add the IE Tab

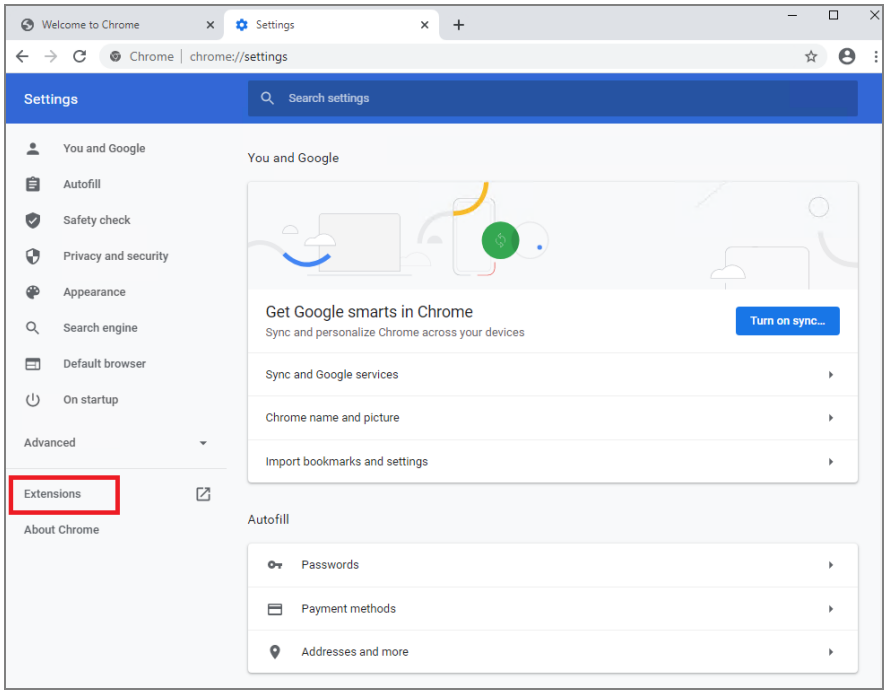
1. Install and start Google Chrome.
2. Click the **Customize and Control** button and select **Settings**.

   View image



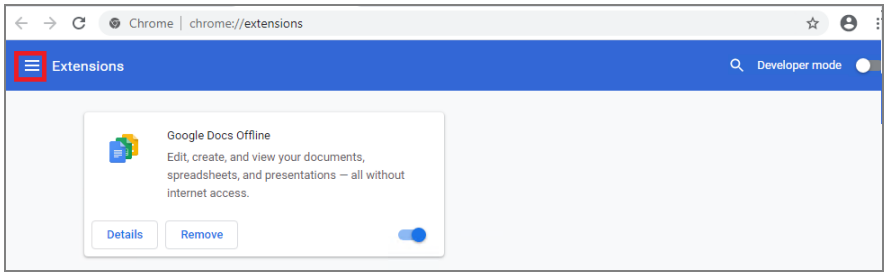
3. In the **Settings** window, open the **Extensions** tab.

   View image



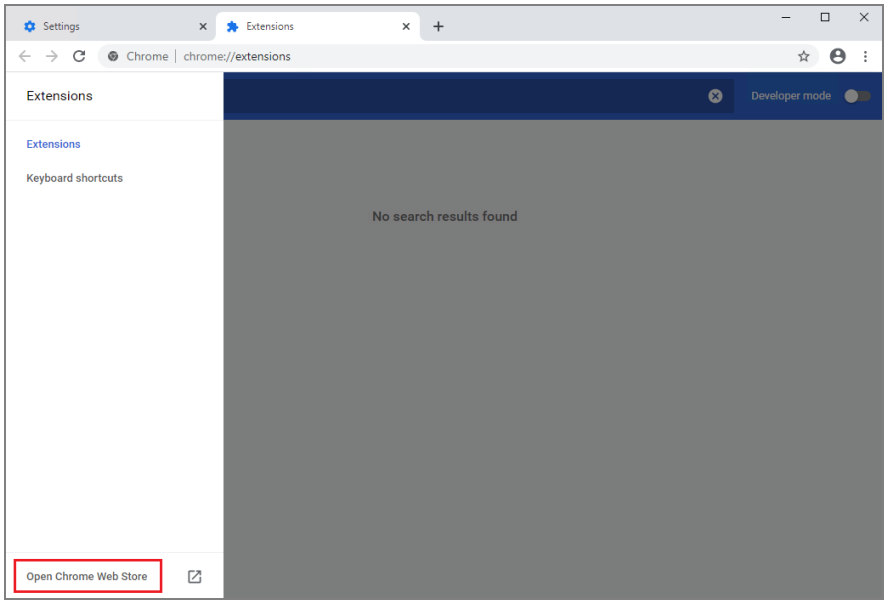
4. Click the **Main menu** icon.

View image



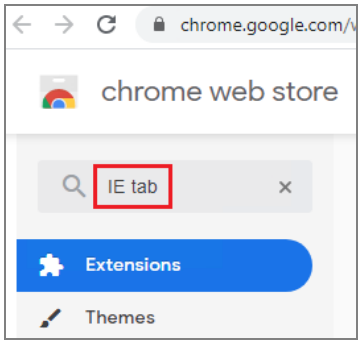
5. Click the **Open Chrome Web Store** tab.

View image



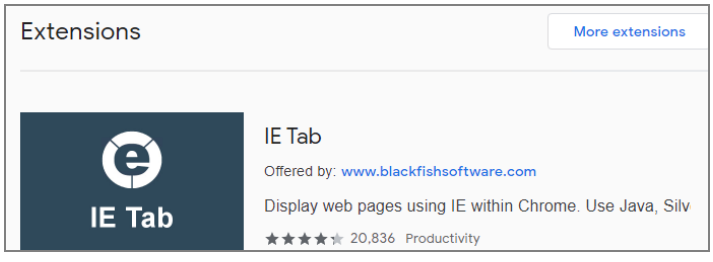
6. In the **Search** field, type in "IE Tab" and press **Enter**.

View image



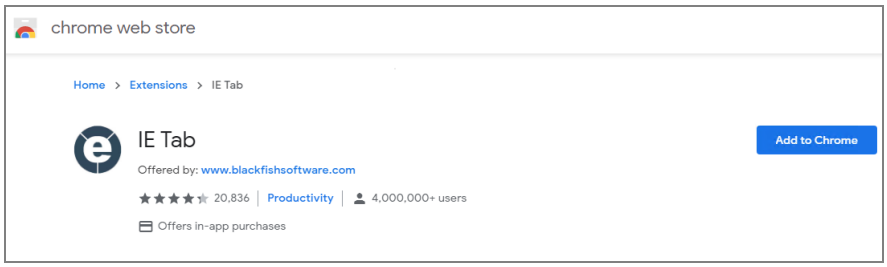
7. In the **Search** results, find the **IE Tab extension** and click to open.

View image



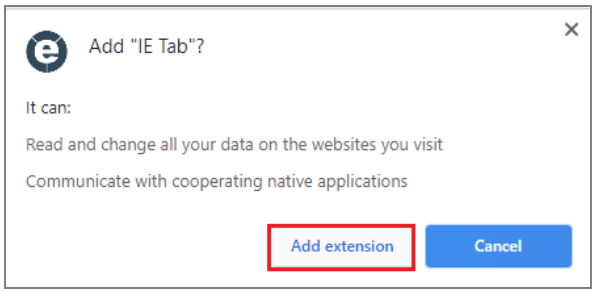
8. Click the **Add to Chrome** button.

View image



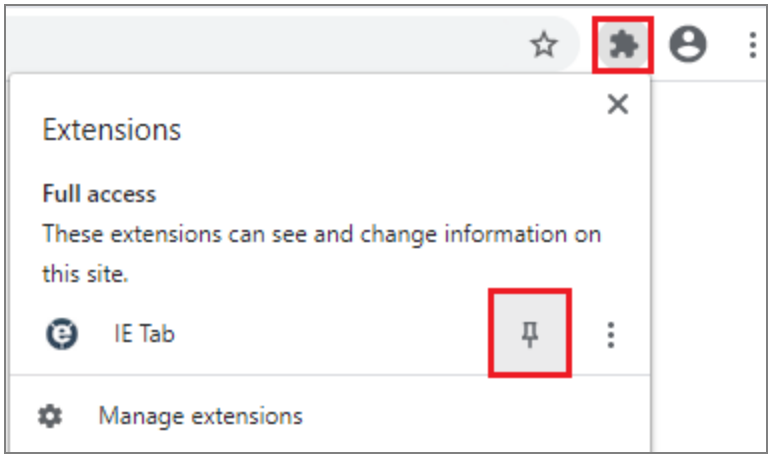
9. In the dialog box that appears, click **Add extension**.

View image



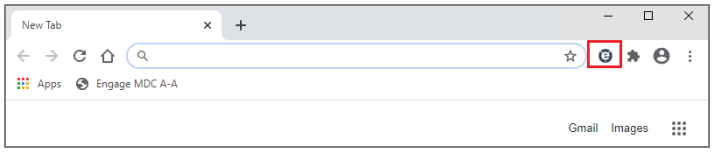
10. Click the **Extensions** icon, select **Pin extension**, then click the **IE Tab** button.

View image



The **IE Tab** button is added to the Tool bar.

View image

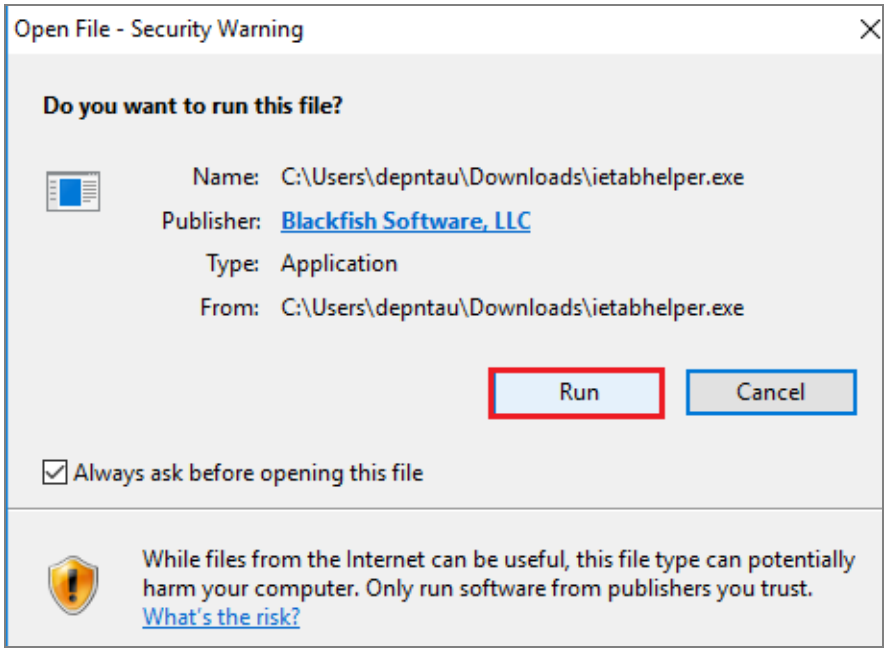


11. The **ietabhelper.exe** file is automatically downloaded.

    View image

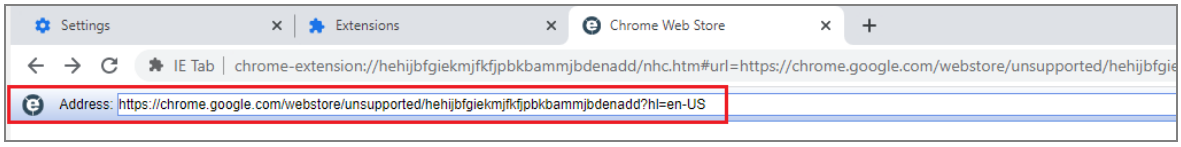
12. Open the **ietabhelper.exe** file and click **Run**.

    View image

13. The IE address bar is added to Google Chrome.

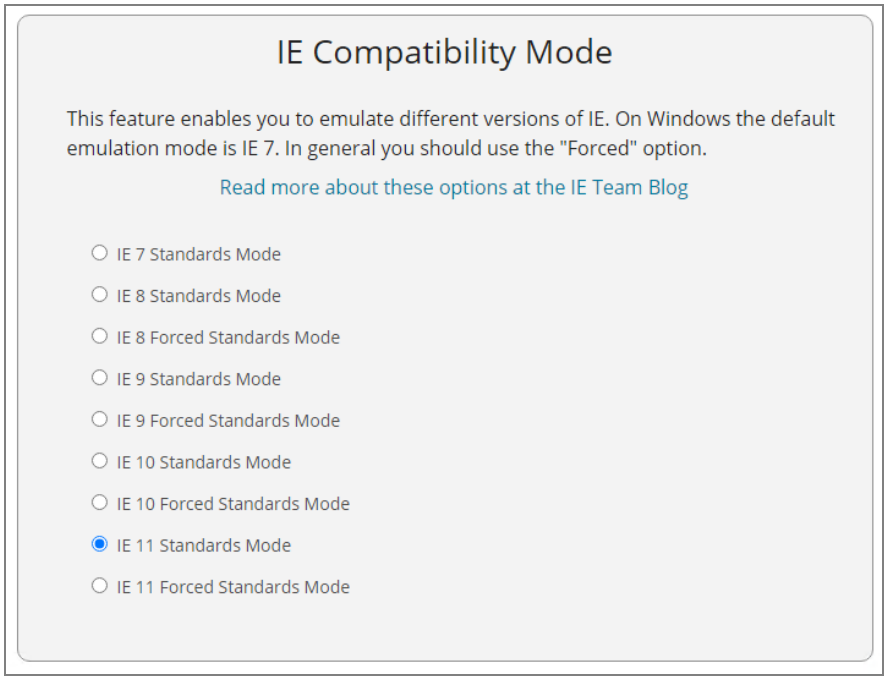
    View image

14. Click the Settings button ( ).

    The **IE Tab Options and Settings** window opens. Scroll down to the **IE Compatibility Mode** area and select **IE 11 Standard Mode**.

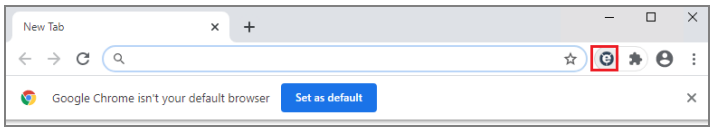
    View image



15. Verify that the NICE Engage URL is added to the Trusted sites, see *Adding NICE Engage URL to the Trusted sites* in the *Workstation Setup Configuration Guide*.

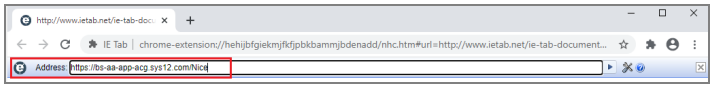
16. Open Google Chrome and click the **IE Tab** button that appears to the right of the address bar on the tool bar.

View image



17. In the address bar enter the Engage URL (https://ENGAGE_FQDN/Nice).

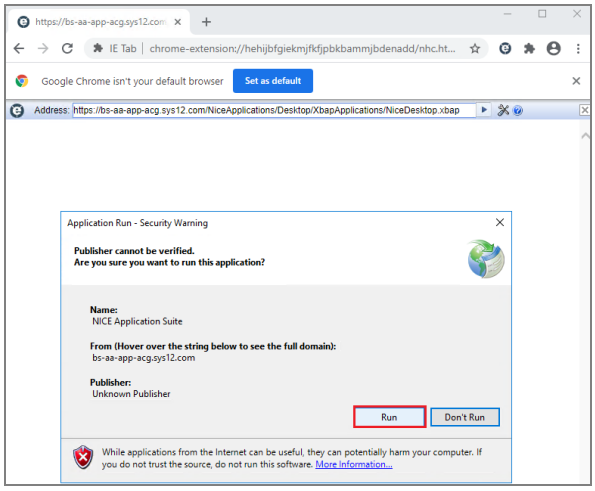
View image



18. Log in to Engage.

19. In the **Application Run - Security Warning** window click **Run**.

View image


IE Tab
chrome-extension://hehijbfgiekmjfkfjpbkbammjbdenadd/nhc.ht...
Google Chrome isn't your default browser
Set as default
Address: https://bs-aa-app-acg.sys12.com/NiceApplications/Desktop/XbapApplications/NiceDesktop.xbap
Application Run - Security Warning
Publisher cannot be verified.
Are you sure you want to run this application?
Name:
NICE Application Suite
From (Hover over the string below to see the full domain):
bs-aa-app-acg.sys12.com
Publisher:
Unknown Publisher
Run
Don't Run
While applications from the Internet can be useful, they can potentially harm your computer. If you do not trust the source, do not run this software. More Information...

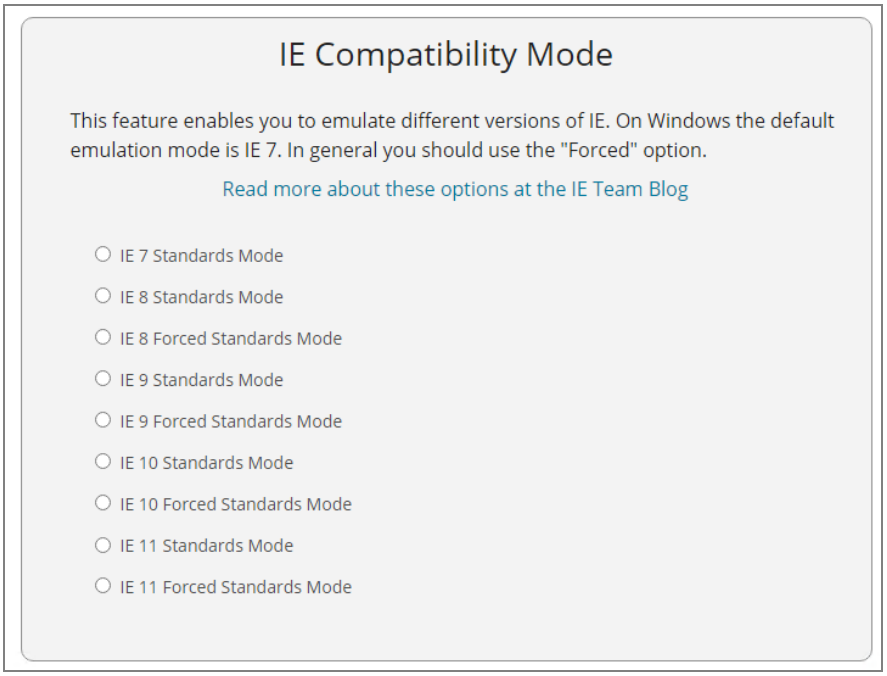
NICE Web Applications Known Issues with the IE Tab in Google Chrome

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.

View image



Using multiple browser types at the same time, on the same workstation, is not supported in Engage 7.x. *For example*, Microsoft Edge and Google Chrome can't both be open and in use on the same workstation, at the same time.

[This page intentionally left blank]

8

Microsoft .NET Framework

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

NICE Support for Microsoft .NET Framework

Product	.NET Framework Support
Release	NICE Engage Platform 7.3 and above, NICE Sentinel 7.3 and above, NICE Playback Portal 7.4, NICE Playback Portal 7.5.
Synopsis	This section describes support for Microsoft .NET Framework (versions 4.0, 4.5.2, 4.6/4.6.1, 4.7/4.7.1/4.7.2, 4.8 and 6.0) by NICE products, for NICE Engage Platform 7.3 and above, NICE Sentinel 7.3 and above, NICE Playback Portal 7.4, NICE Playback Portal 7.5.

Overview

This section provides information regarding NICE products support for Microsoft .NET Framework (versions 4.0, 4.5.2, 4.6/4.6.1, 4.7/4.7.1/4.7.2, 4.8, 6.0).

Microsoft .NET Framework Server-Side Support

The following table lists the NICE release versions and indicates which version supports Microsoft .NET Framework (versions 4.0, 4.5.2, 4.6/4.6.1, 4.7/4.7.1/4.7.2, 4.8, 6.0).

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

Release Version	Status
NICE Engage Platform 7.3 and above	.NET 4.0 is approved .NET 4.5 is approved .NET 4.5.1 is approved .NET 4.5.2 is approved .NET 4.6./4.6.1/4.6.2 Framework is approved .NET 4.7/4.7.1/4.7.2 is approved *(For Compliance Center only)* .NET 4.8 is required on the Applications Server .NET 4.8 is required .NET 6.x side-by-side with .NET 4.x is approved See the *Certified Servers Guide* for more details about requirements.
NICE Sentinel 7.3 and above	.NET 4.5 is approved .NET 4.5.1/4.5.2 is approved .NET 4.6/4.6.1 is approved .NET 4.7/4.7.1/4.7.2 is approved .NET 4.8 is required
NICE Playback Portal 7.4	.NET 4.8 is required .NET 6.0 is required
NICE Playback Portal 7.5	.NET 4.8 is required .NET 6.0 is required

Microsoft .NET Framework Client-Side Support

The following table lists the NICE release versions and indicates which version supports Microsoft .NET Framework (Versions 4.0, 4.5, 4.5.1, 4.5.2, 4.6/4.6.1, 4.7/4.7.1/4.7.2, and 4.8).

Release Version	Status
NICE Engage Platform 7.3 and above	.NET 4.0 is approved .NET 4.5 is approved .NET 4.5.1 is approved .NET 4.5.2 is approved .NET 4.6./4.6.1/4.6.2 Framework is approved .NET 4.7/4.7.1/4.7.2 is approved .NET 4.8 is required .NET 6.x side-by-side with .NET 4.x is approved See the *Certified Servers Guide* for more details about requirements.
NICE Sentinel 7.3 and above	.NET 4.5 is approved .NET 4.5.1/4.5.2 is approved .NET 4.6/4.6.1 is approved .NET 4.7/4.7.1/4.7.2 is approved .NET 4.8 is required

Microsoft .NET Framework 4.8 Requirements

NICE Engage Platform 7.3 and above requires Microsoft .NET Framework version 4.8. .NET Framework version 4.8 must be installed on all servers and clients in the site. See *Certified Servers* for a complete list.

Ensuring the Correct XBAP Version on the workstation

In order for .NET Framework 4.8 to work optimally with XBAP, the newest version of XBAP must be installed. If updating a previous version of NICE Engage Platform to Release 7.x, 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.

Microsoft .NET 6.0 Requirements

NICE Playback Portal 7.4 and NICE Playback Portal 7.5 require Microsoft .NET 6.0.

ASP.NET Core Runtime 6.0.x – Hosted bundle must be installed on Engage Application server or Playback Portal Stream Server depending on the Playback Portal scale.

For more information, see *Certified Servers Guide*.

9

Microsoft SQL Server

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

SQL Server 2016

Product	NICE Engage Platform
Release	NICE Engage Platform 7.x NICE Sentinel 7.x

SQL 2016 Standard/Enterprise was certified for the Database Server and Data Mart. Only clean installation is supported. There is no migration/upgrade from previous SQL versions.

For more information see:

- *Requirements and Best Practices for Microsoft SQL Server*
- *Requirements and Best Practices for Microsoft SQL Server*

SQL Server 2019

Product	NICE Engage Platform
Release	NICE Engage Platform 7.2 and up NICE Sentinel 7.2 and up

SQL 2019 Standard/Enterprise/Developer edition was certified for the Database server, the Data Mart server, the Seamless Key Database server and the SQL Server Analysis services.

Important! SQL Server Developer edition includes all the functionality of the Enterprise edition. However, SQL Server Developer edition is licensed only for applying as a test system, not as a production server.

For more information see:

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

10

Additional Third Party Components

This section outlines the additional third party components and their supported versions used by NICE Engage Platform.

Apache Tomcat

NICE Engage Platform uses Apache Tomcat to implement Java Servlet and run the Java-based applications.

Apache Tomcat Version	NICE Engage Platform Release
Apache Tomcat 9.0.80	NICE Engage Release 7.4

ActiveMQ Artemis

ActiveMQ Artemis is a next generation ActiveMQ messaging broker.

NICE supports these ActiveMQ Artemis versions.

ActiveMQ Artemis Version	NICE Release Version	NICE Engage Components
ActiveMQ Artemis 2.31	NICE Engage Release 7.4	▪ NICE RTA Message Queue
ActiveMQ Artemis 2.30	NICE Engage Release 7.4	▪ Monitoring
ActiveMQ Artemis 2.27.1	Compliance Center Release 9.2	Compliance Center

RabbitMQ

RabbitMQ is a message broker. NICE supports the following version of RabbitMQ.

RabbitMQ Version	NICE Release Version	NICE Engage Components
3.12.5	Compliance Center 9.2, Compliance Center 9.3	Compliance Center
3.12.5	Playback Portal 7.4, Playback Portal 7.5	Playback Portal

To change passwords for RabbitMQ users, see *Compliance Center Deployment Guide* or *Playback Portal Installation Deployment Guide*.

SAP Products

SAP products are used by NICE Engage Platform in the NICE Reporter application to generate and view reports. Crystal Report deployment includes Oracle JAVA instance.

Below are the supported SAP versions:

NICE Engage Platform Release	NICE Reporter Viewer (Online /Offline)	NICE Reporter Server	NICE Reporter Server and Client Workstations
NICE Engage Release 7.4	09.27.78.01	SAP Crystal Reports Server 2020 SP2, OEM Edition 14.3.2.4073	SAP BO BI Platform .NET SDK 4.3 SP2 14.3.2.4073

SIP Stack

NICE Engage Platform uses the Softil SIP Stack version 7.6.4.

The SIP Stack is upgraded in these components:

- AIR
- VRSP
- Screen Agent
- Stream Server

- Monitor Application

Java 11 Azul

NICE Engage Platform requires Java 11 Azul for some NICE and third party components.

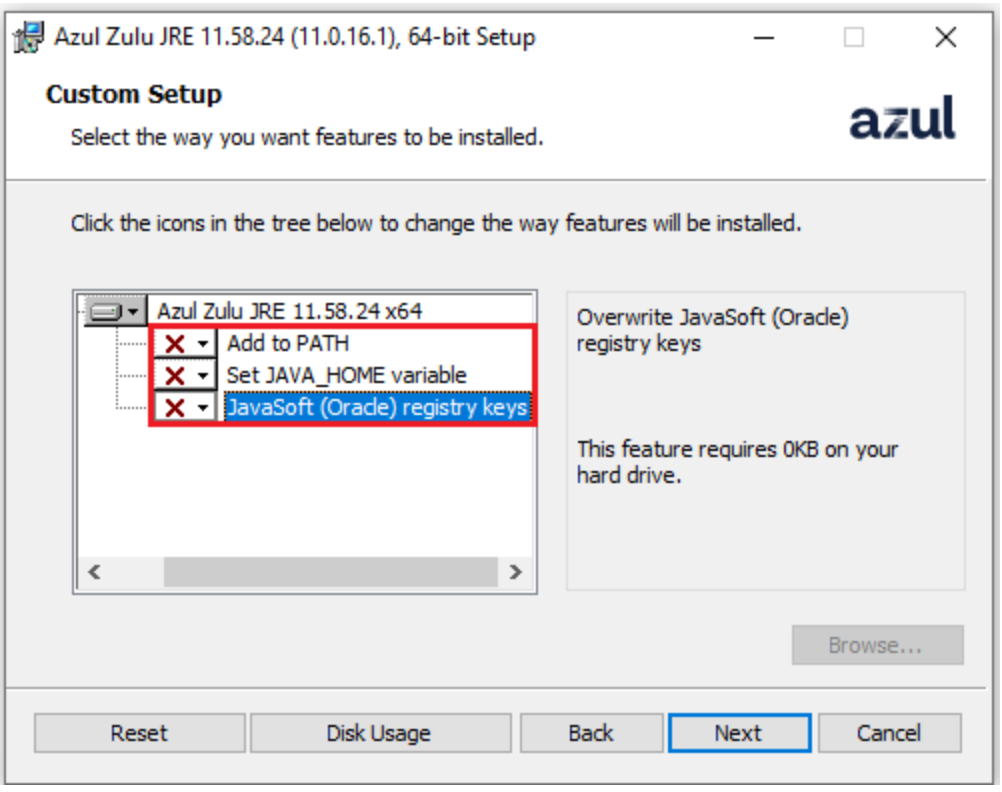
> **Important!** Java 11 Azul must be installed **only** by NICE Professional Service Engineers, NICE Technical Support Engineers, and Certified Business Partners.

To install or update Java 11 Azul

1. From NICE Software Download Center (SDC), download the **Java Azul** package.
2. Extract the **zulu11.xx.xx-xx-jre11.xx.xx-win_x64.msi** file, where <*xx*> is the latest version.
3. Double-click the .msi file to run the Setup Wizard and follow the instructions in the wizard.

   NOTE: In the **Custom Setup** window, the following features are not required:
   - Set JAVA_HOME variable
   - JavaSoft (Oracle) registry keys

   View image



4. Complete the installation.

Java 17 Azul

NICE Engage Platform requires Java 17 Azul for some NICE and third party components.

> **Important!** Java 17 Azul must be installed **only** by NICE Professional Service Engineers, NICE Technical Support Engineers, and Certified Business Partners.

To install or update Java 17 Azul

1. From NICE Software Download Center (SDC), download the **Java Azul** package.

   NOTE: A basic MSI installer for Java 17 Azul can be found in the Policy Manager CC – BE zip package, located in the **Java_package** folder.

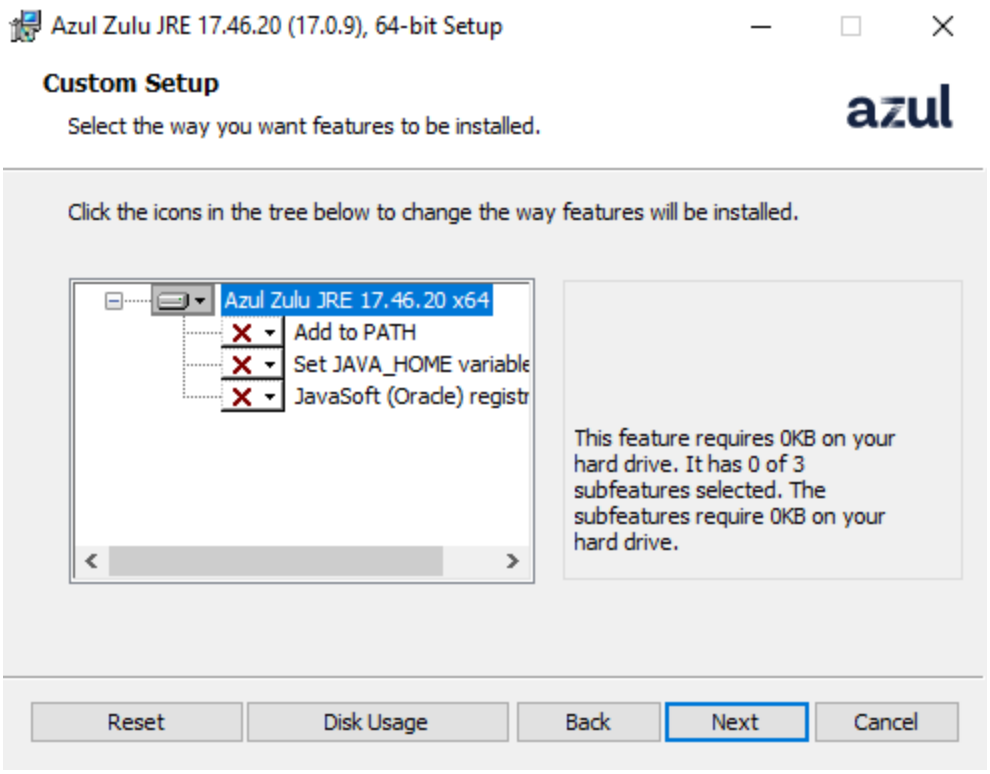
2. Extract the **zulu17.xx.xx-xx-jre17.xx.xx-win_x64.msi** file, where <*xx*> is the latest version.

3. Double-click the .msi file to run the Setup Wizard and follow the instructions in the wizard.

   NOTE: In the **Custom Setup** window, the following features are not required:

   - Add to PATH
   - Set JAVA_HOME variable
   - JavaSoft (Oracle) registry keys

View image



4. Complete the installation.

11

Microsoft Kerberos Configuration Manager

Microsoft Kerberos Configuration Manager for SQL Server is a diagnostic tool for troubleshooting Kerberos-related connectivity issues with SQL Server.

The tool performs these functions:

- Gathers information about the operating system and Microsoft SQL Server instances installed on a server.
- Generates reports about all SPN and delegation configurations on the server.
- Identifies potential issues in SPNs and delegations.
- Repairs potential SPN issues.

The tool requires .NET framework 4.0 or higher.

Supported Operating Systems

Microsoft Kerberos Configuration Manager for SQL Server supports these operating systems:

- Windows 10
- Windows Server 2016/2019

To configure Kerberos using Microsoft Kerberos Configuration Manager for SQL Server:

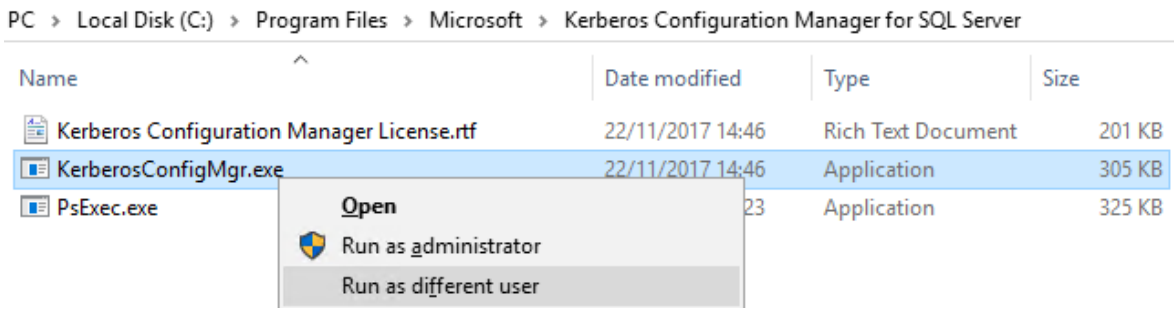
1. Download Microsoft Kerberos Configuration Manager for SQL Server from the Microsoft website.

2. After the installation is complete, go to **...ProgramFiles\Microsoft\Kerberos Configuration Manager for SQL Server**.

3. Right-click **KerberosConfigMgr.exe**, and click **Run as different user**.

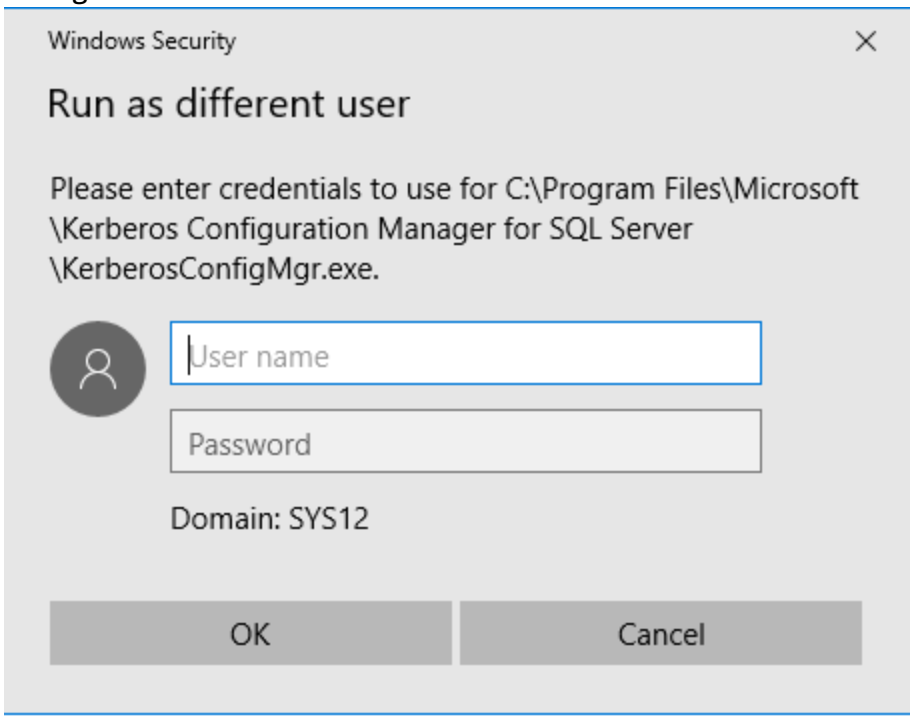
   View image

11: Microsoft Kerberos Configuration Manager



The Run as different user window appears.

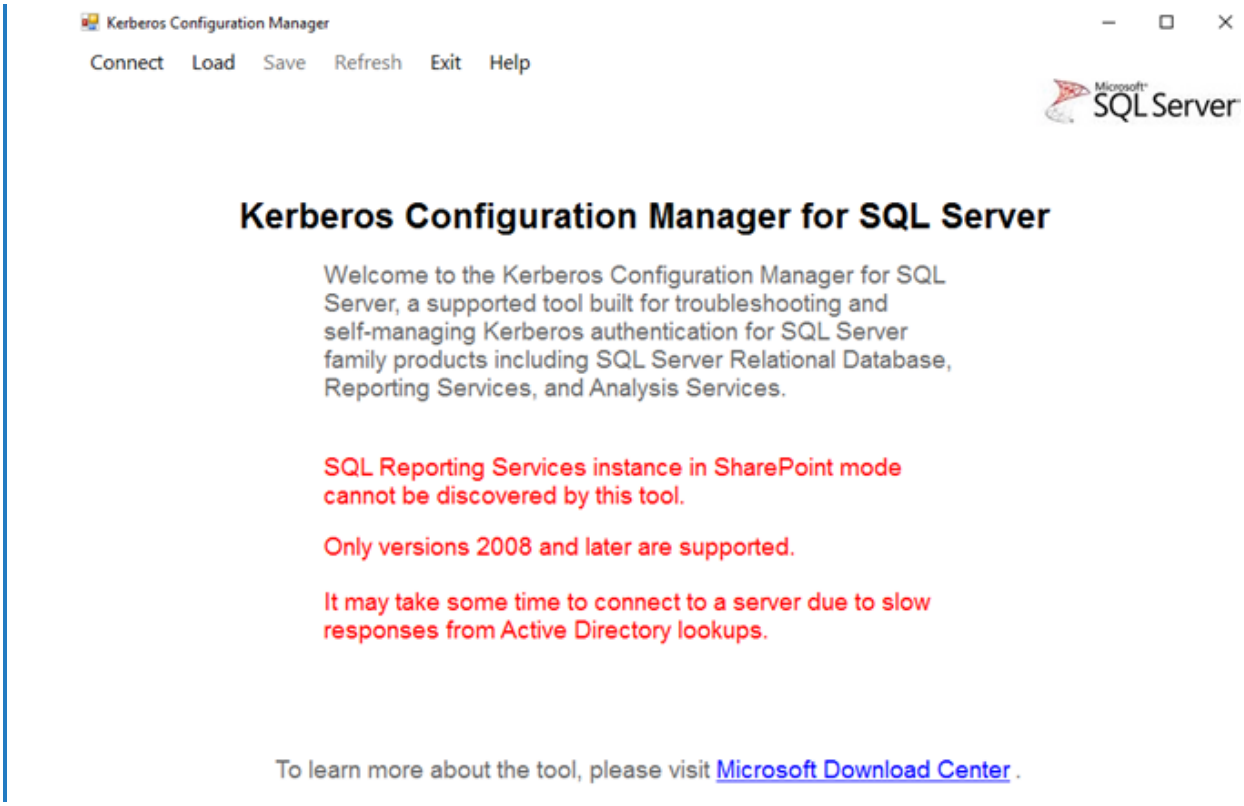
View image



4. Enter the user name and password of the user with privileges to fix the SPN on the server, and click **OK**. The main Kerberos Configuration Manager for SQL Server appears.

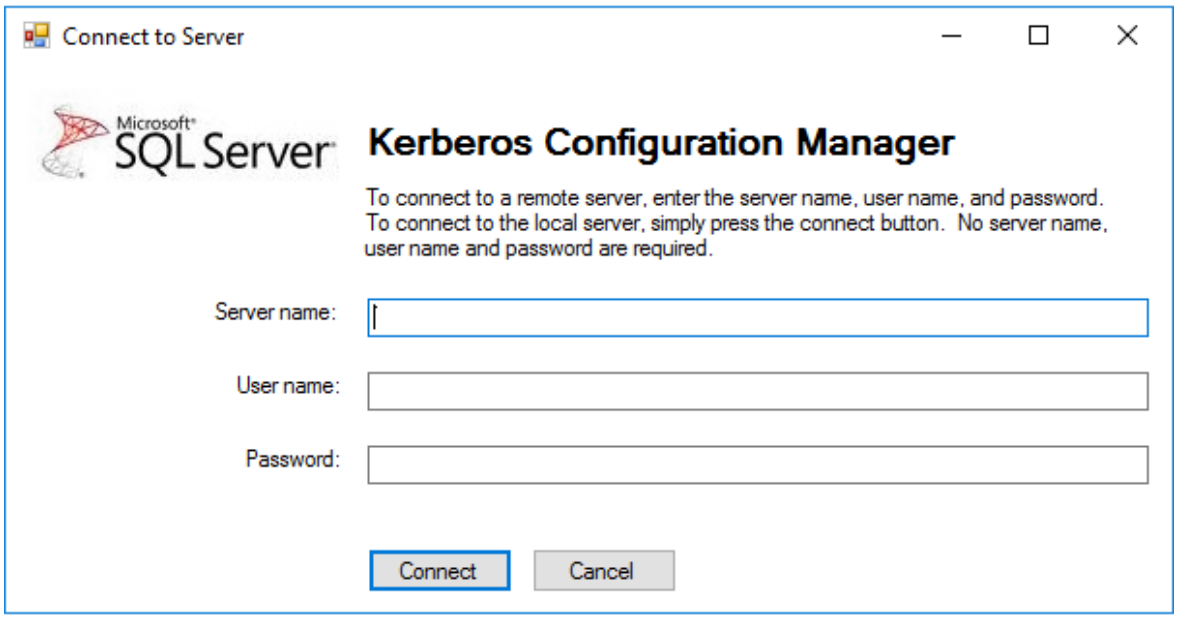
View image

11: Microsoft Kerberos Configuration Manager



5. Click **Connect**. The Connect to Server window appears.

View image



11: Microsoft Kerberos Configuration Manager

6. In the Connect to Server window:

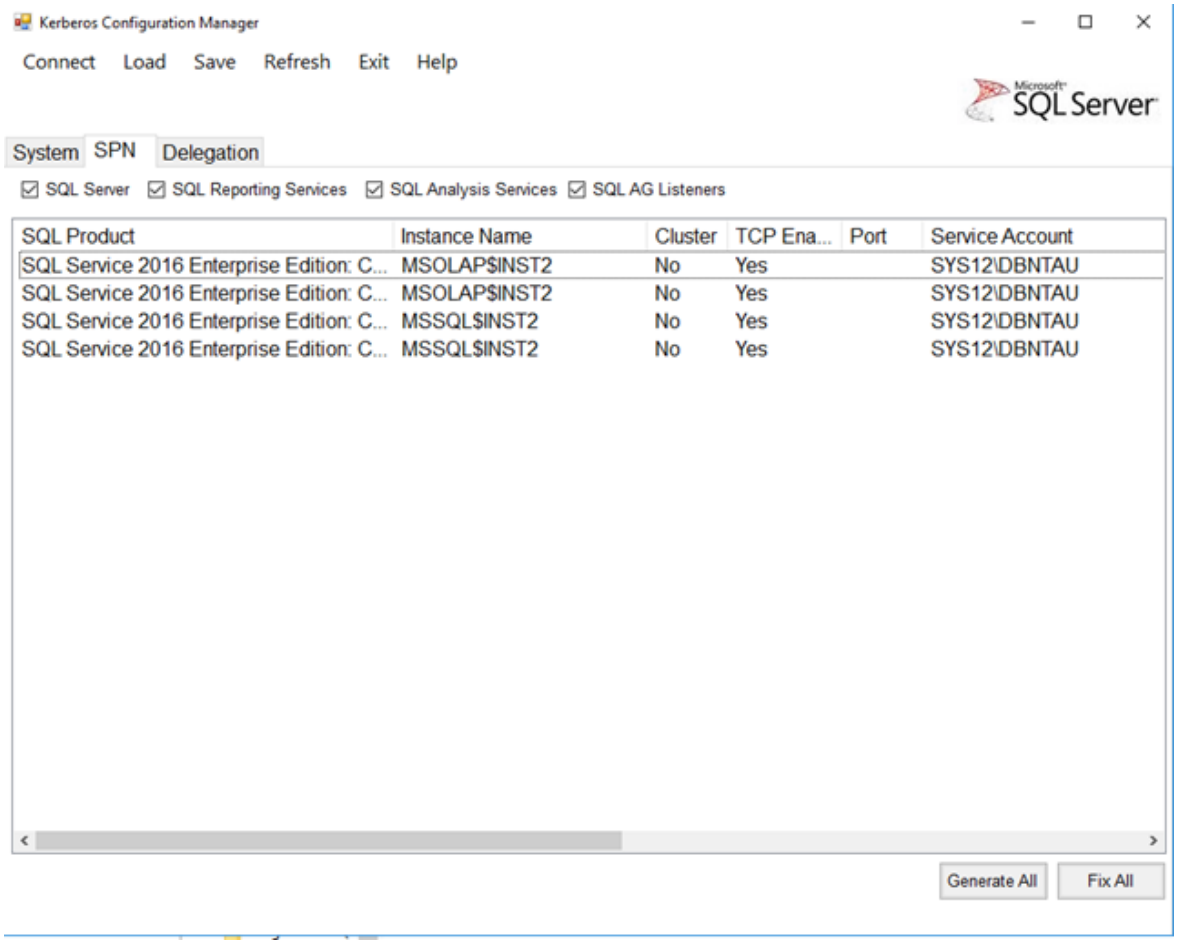
   a. For a remote instance, enter the **Server name** for the Windows Authentication server, **User name** and **Password** .

      For a local instance, keep all of the fields empty.

   b. Click **Connect**.

7. After connecting to the instance, click the **SPN** tab, and select the relevant check boxes to filter the results.

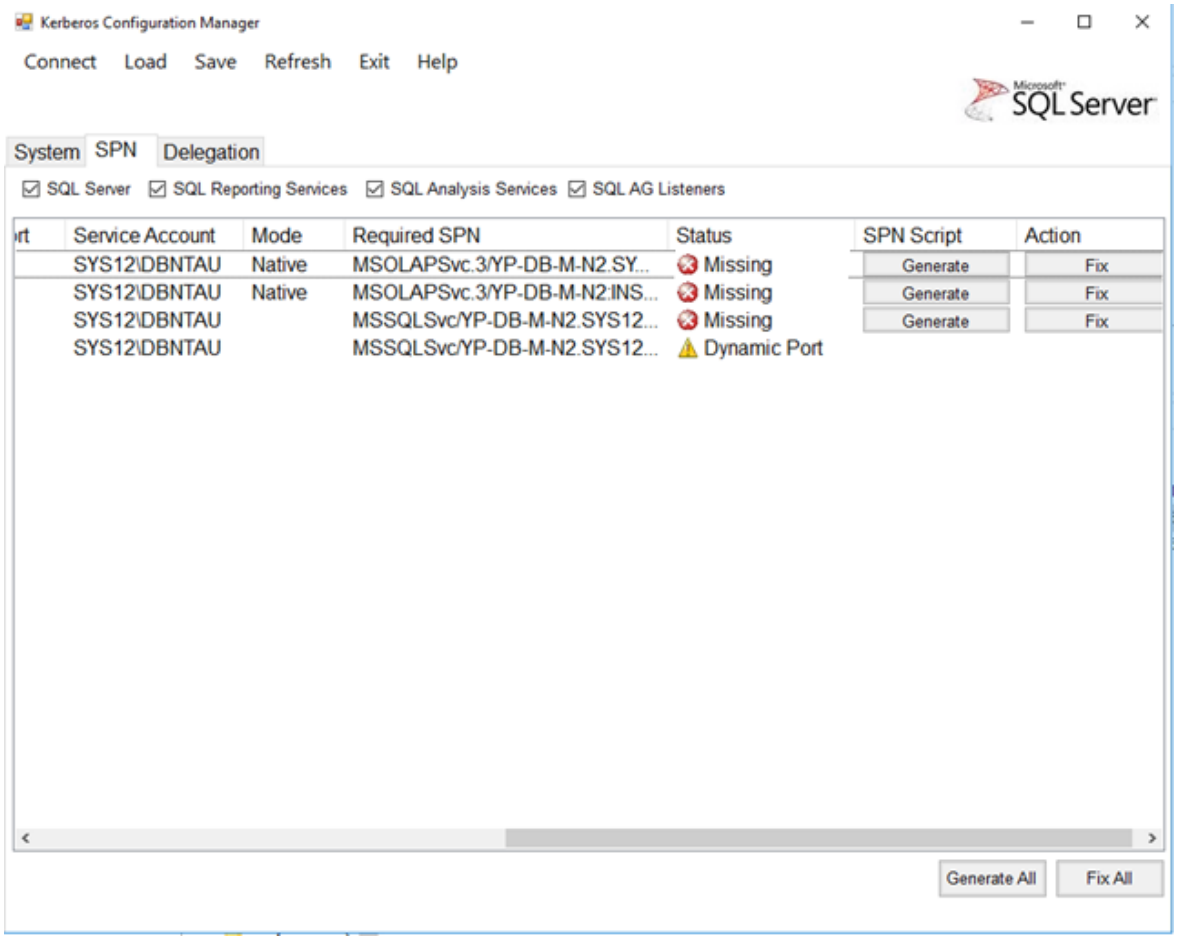
   View image



8. Check the status of the registered SPNs. If the status of any of the SPNs is **Missing**, click Fix for specific SPNs or **Fix All** to fix all of the ones that are missing.

   View image

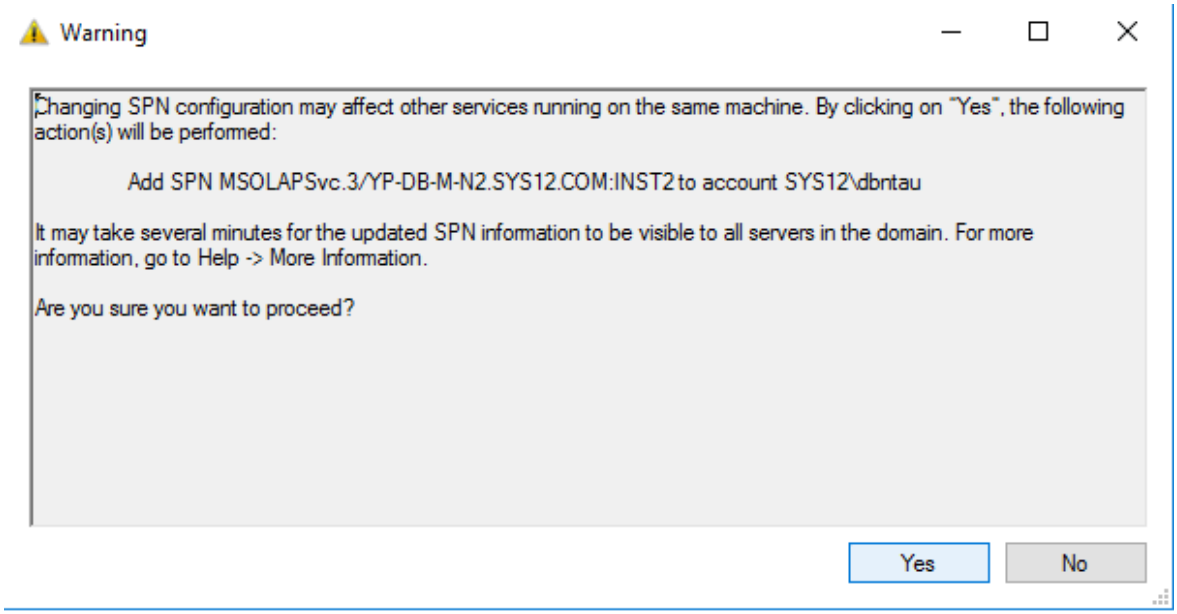
11: Microsoft Kerberos Configuration Manager



A warning appears.

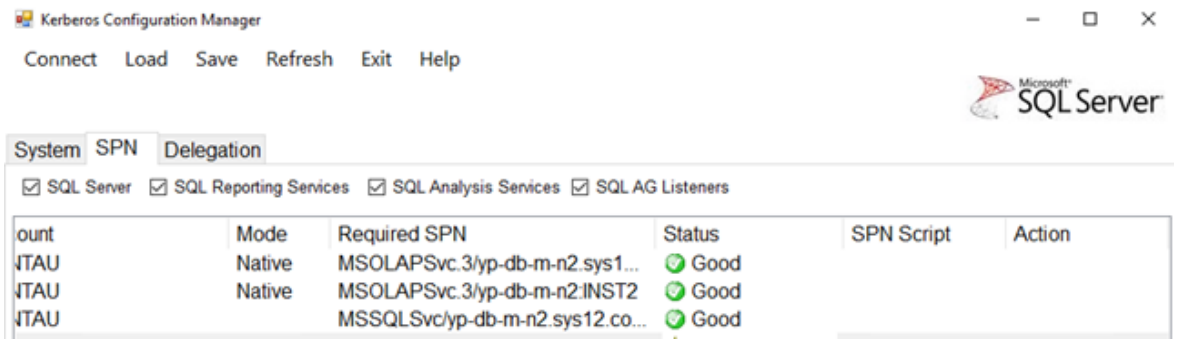
View image

11: Microsoft Kerberos Configuration Manager



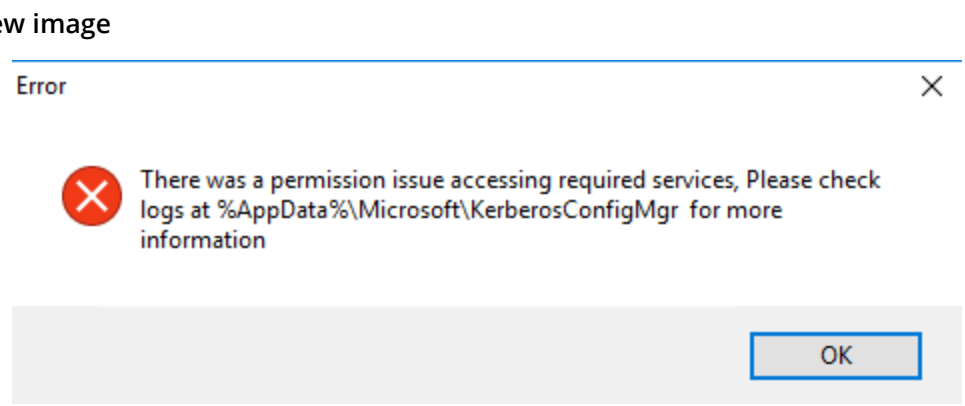
9. Click **Yes** to start fixing the SPN.
   - If the SPN is fixed, the status converts to **Good, and the procedure is complete**

View image



   - If you receive a permissions error as shown below, continue to Step 10.

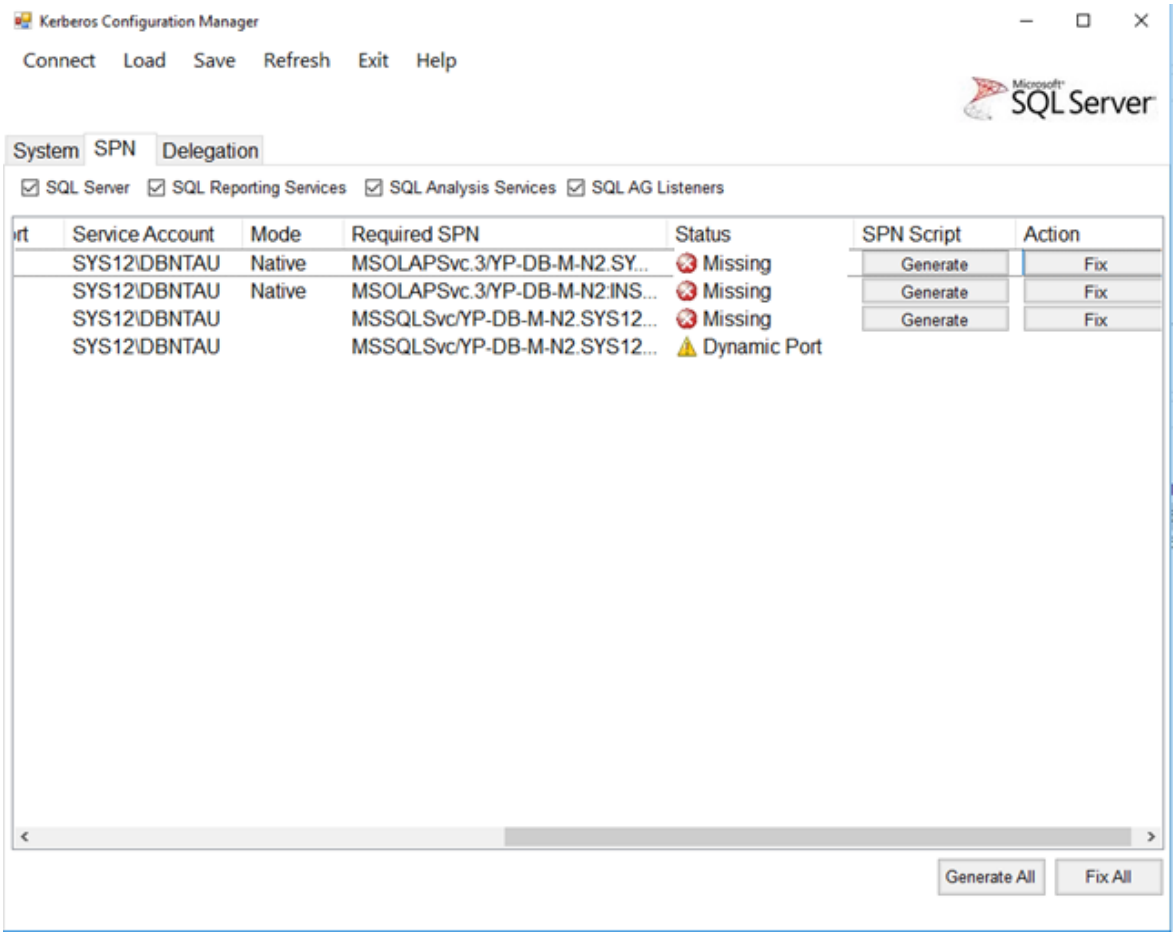
View image



11: Microsoft Kerberos Configuration Manager

10. ***This step should only be performed if you receive a permissions error.*** Create a script, and run it as a user with privileges to fix the SPN on the server.
    a. Go to the **SPN** tab, and click **Generate** to generate a script for specific SPNs or **Generate All** to generate scripts for all of the SPNs that are missing.

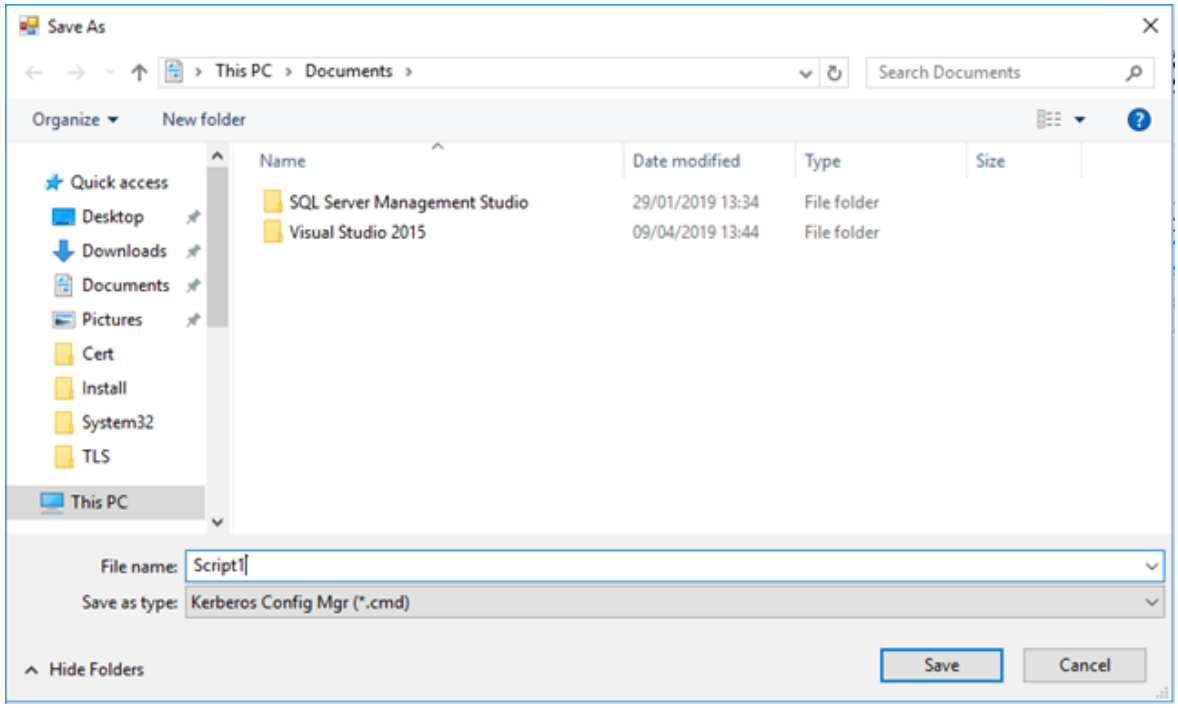
View image



    b. Save the script in your desired location.

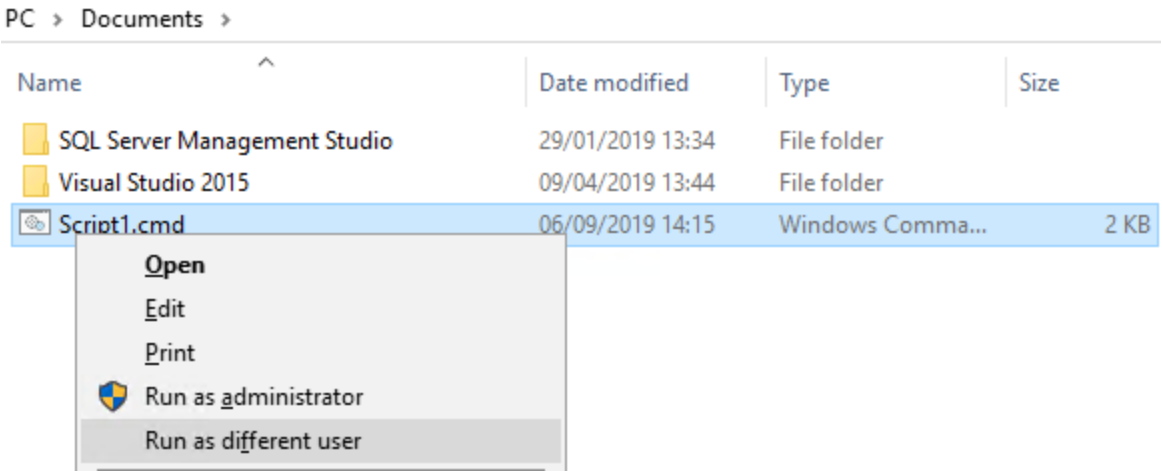
View image

11: Microsoft Kerberos Configuration Manager



c. Right-click the file with the script, and click **Run as different user**.

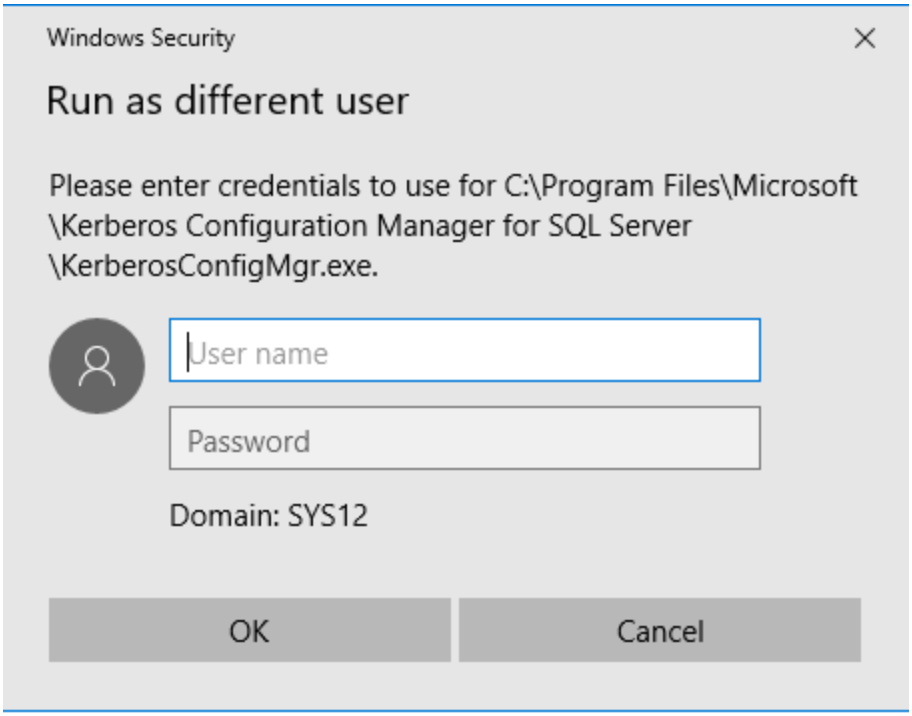
View image



The Run as different user window appears.

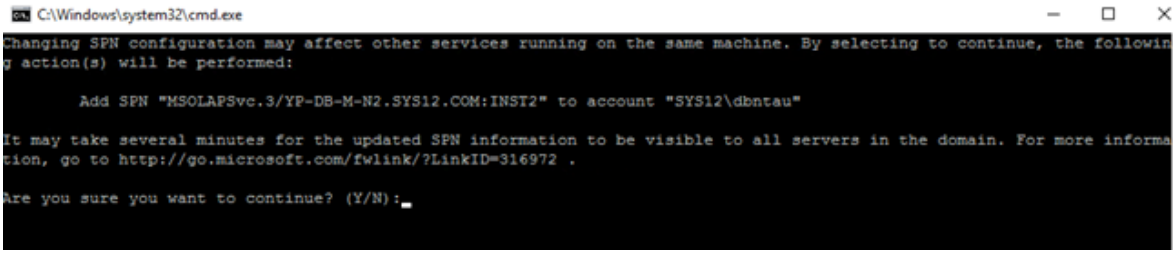
View image

11: Microsoft Kerberos Configuration Manager



d. Enter the user name and password of the user with privileges to fix the SPN on the server, and click **OK**. The cmd.exe will open.

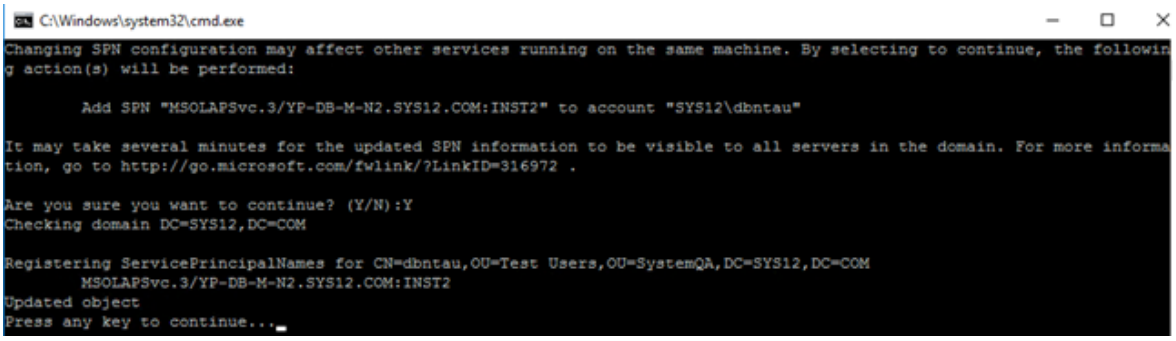
View image



e. For the question **Are you sure you want to continue?**, enter **Y** to fix the SPN.

View image

11: Microsoft Kerberos Configuration Manager



12

Microsoft Security Bulletins

This section describes Microsoft security bulletins.

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 Server 2016, Windows Server 2019 (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

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	

13

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

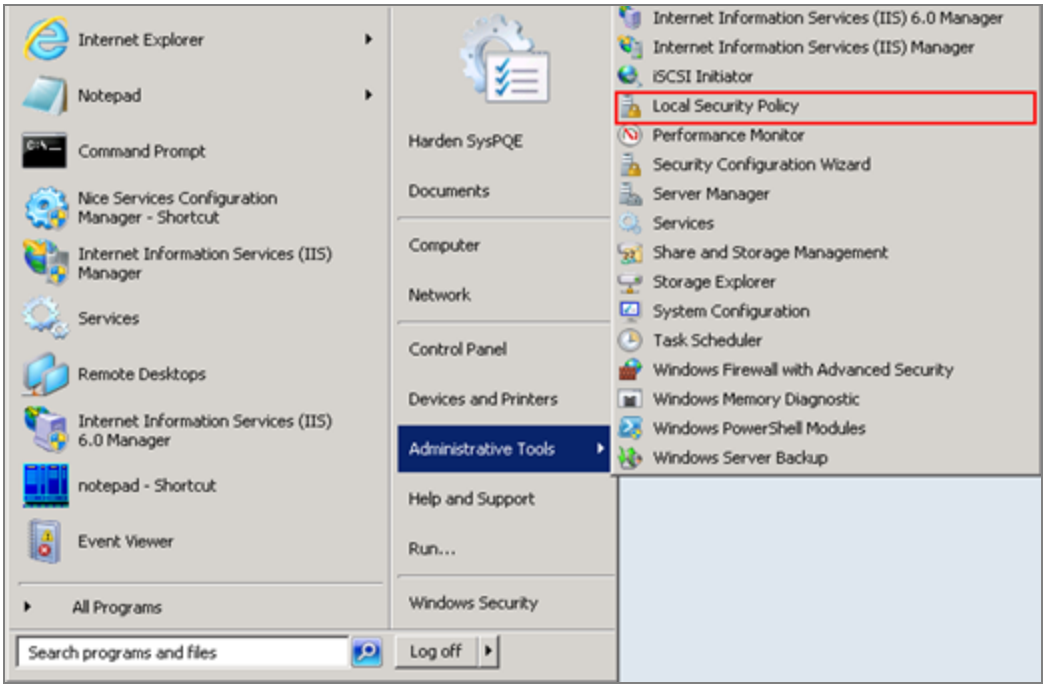
The FIPS mode can be applied on the server or client machine in one of two ways:

- 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:

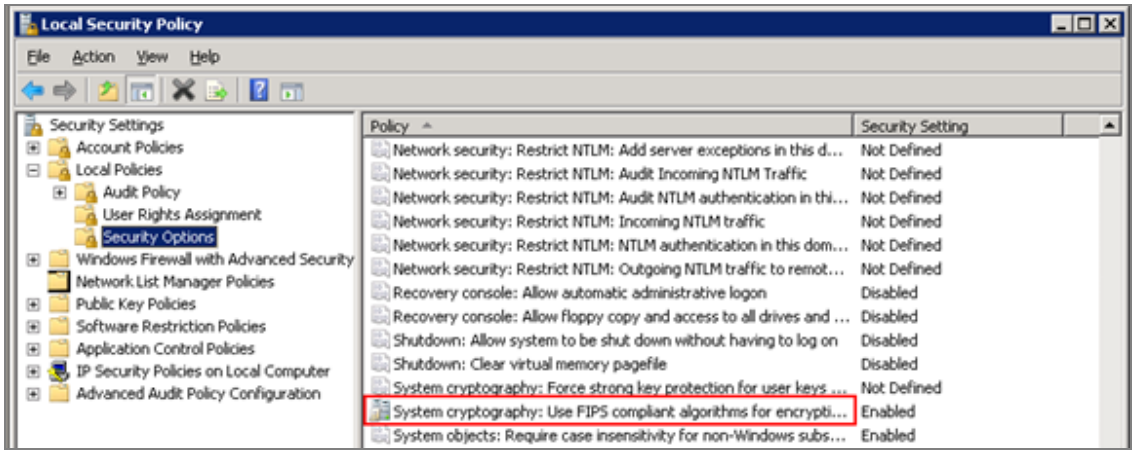
1. Open the Local Security Policy by selecting **Start -> Administrative tools->Local Security Policy**. Run the Local Security Policy under a user that has privileges to edit the local policy.

   View image



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).

View image



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

FIPS Verification Flow

As part of the Engage Media Encryption solution, we use the AesCryptoServiceProvider class in the Media Encryption Framework (MEF) component. The AesCryptoServiceProvider class is a FIPS 140-2 compliant wrapper of the Microsoft Crypto API, used in Engage for:

- Encryption keys and VI generation
- Data encryption
- Data decryption

NICE Engage Platform 7.x installed on Windows Server 2016 and Windows Server 2019 uses the Enhanced Cryptographic Provider library (RSAENH.DLL), a FIPS 140-2 compliant cryptographic module. The Enhanced Cryptographic Provider library is responsible for verifying that encryption algorithms are FIPS compliant when AesCryptoServiceProvider class is used.

In Windows Server 2019, each call to the Enhanced Cryptographic Provider library routs an API call into the FIPS-certified CNG libraries (or in recent Windows releases to the Kernel Mode Cryptographic Primitives Library) that check and indicate if the specific call is FIPS compliant.

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.

[This page intentionally left blank]

14

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*.

Supported in:	Microsoft DST Updates
NICE Engage Platform 7.x	KB 951072, KB 955839, KB 970653, KB 976098, KB 981793, KB 2158563, KB 2443685, KB 2570791, KB 2633952, KB 2756822, KB 2779562, KB 2863058, KB 2974661, KB 2984350, KB 2967990, KB 2981580, KB 2998527, KB 3011843, KB 3013410, KB 3049874, KB 3062741, KB 3062740, KB 3077715, KB 3093503, KB 3112148, KB 3148851, KB 3153731, KB 3162835, KB 3148851, KB 3153731, KB 3162835, KB 3177723, KB 3182203, KB 3192321, KB 3203884, KB 4015193, KB 4012864, KB 4023136, KB 4020322, KB 4486459, KB 4501226, KB 4507704, KB 4519108, KB 4484172, KB 4557900

[This page intentionally left blank]

15

Antivirus: General Antivirus Configuration Guidelines

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

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

Overview

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

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

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

Antivirus Real Time Scan

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

NICE does not recommend using real time scanning due to numerous risks including, but not limited to:

- Recording loss
- Playback performance degradation
- Impact on archiving queue, possibly leading to archiving failures

Daily Scan

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

Weekly Scan

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

Folders and Files Exclusion

Exclude the folders and files in the tables below from your scheduled antivirus scans (Read & Write), since they are used for NICE system operations.

All the paths in the tables below are the default installation paths. If you used a different path in your installation, you must use the same path for the excluded files.

NICE Engage Platform

NICE Components	Default Path	Files
Advanced Interaction Recorder		
▪ Package and binaries folder	D:\Program Files\NICE systems\	
▪ Log files folder	NiceLogLocation: D:\Program Files\NICE systems\Logs	
▪ Metadata Management folder	D:\Program Files\NICE systems\	*.s3db*
▪ Advanced Interaction Recorder Storage	E:\Recorder_Storage	*.nmf
▪ Archiving Folders	User defined path: <Archiving directory>	*.nmf

NICE Components	Default Path	Files
Applications Server	D:\Program files\NICE Systems	*.exe *.dll *.config *.log
ConnectAPI	D:\Program Files\NICE Systems	*.exe *.dll *.config *.log
CTI / VRSP	D:\Program files\NICE Systems\CTI	
Database Server	E:\<SQL Data Files>	*.mdf
	F:\<SQL Log Files>	*.ldf
Data Mart	E:\<SQL Data Files>	*.mdf
	F:\<SQL Log Files>	*.ldf
SeamlessKey Database	F:\<SQL Data Files>	*.ndf *.mdf
	E:\<SQL Log Files>	*.ldf
Interactions Center	D:\Program Files\NICE Systems\Interactions Center\Bin	
	D:\Program Files\NICE Systems\Interactions Center\Data	
	D:\Program Files\NICE Systems\Interactions Center\Log	

NICE Components	Default Path	Files
NICE Sentinel	D:\<SQL Data Files>	*.mdf
	D:\<SQL Log Files>	*.ldf
	D:\Program files\NICE Systems\NICE Sentinel	*.exe *dll *.config *.log
Playback Portal Server (7.x)	D:\Program files\NICE Systems\PBP\NICE Playback Portal Server	
Playback Portal Database (7.x)	H:\<SQL Data Files>	*.mdf
	G:\<SQL Log Files>	*.ldf
Real-Time Authentication		
▪ Enrollment Engine	D:\Program files\NICE Systems\	*.nmf
▪ Authentication Engine	D:\Program files\NICE Systems	*.nmf
	C:\windows\system32\MSMQ	*.*
Storage Center **NOTE:** There is no Storage Center in NICE Engage 7.x clean installation. However, Storage Center can be found if there was an upgrade to 7.x.	E:\<SC_Archive_Directory>	*.nmf

Client-side Component	Default Path	Files
ScreenAgent	C:\Program Files (x86)\NICE Systems\ScreenAgent	

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

- The path of the \mscs folder on the quorum drive, for example, the Q:\mscs folder.
- The %Systemroot%\Cluster folder.

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

Disabling Firewalls

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

To disable firewalls:

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

Live Updates

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

Low network traffic refers to customer network and not to NICE Engage Platform system.

CPU Priority

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

Additional Configurations

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

  If you choose to enable this option, you might experience performance issues in your system.
- **Heuristic scanning** should be disabled in case of performance issues.

Additional Recommendations

In order to maintain performance of your machines during scans, see Microsoft Virus Scanning recommendations.

This information is provided for reference purposes only.

16

Antivirus: Antivirus Software Configuration

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.
- These guidelines are provided for NICE server performance. Customers should make their own risk analysis while implementing these guidelines.

Configuring Symantec Endpoint Protection

If you are using Symantec Endpoint Protection, do the following:

- Disable Heuristic Scanning
- Configure SONAR
- Configure LiveUpdate
- Exclude the required folders and files from virus scanning
- Configure the CPU priority

Disabling Heuristic Scanning

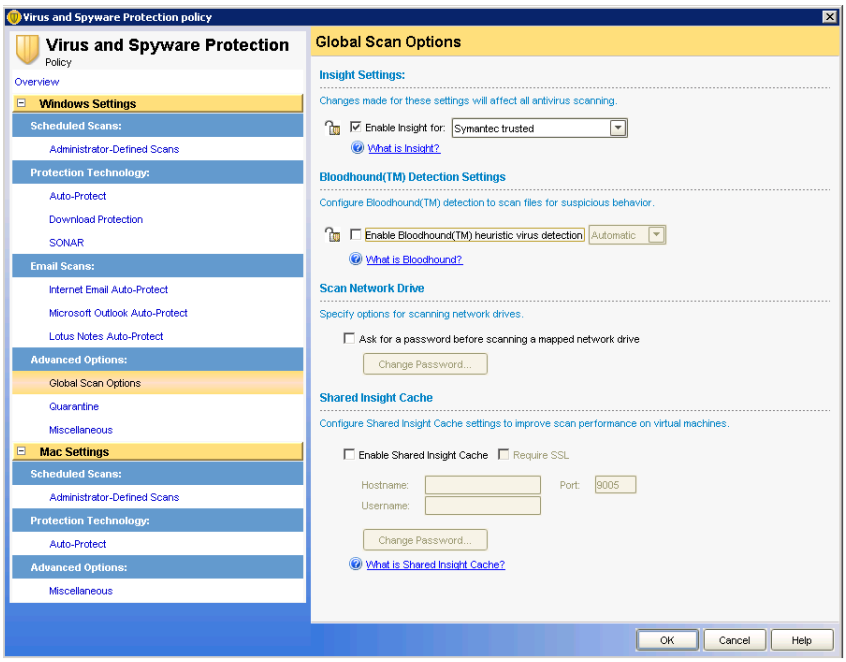
To disable heuristic scanning with Symantec Endpoint Protection:

1. Log on to Symantec Endpoint Protection Manager.
2. In the left-hand column, click the **Policies** tab.
3. In the **Policies** pane, click **Virus and Spyware Protection**.

4. In the **Virus and Spyware Protection Policies** pane, click the appropriate policy that you use from the list.

5. In the Virus and Spyware Protection Policy window, under **Windows Settings**, click **Global Scan Options**.

View image



6. Clear the **Enable Bloodhound(TM) heuristic virus detection** checkbox.

7. Click **OK**.

Configuring SONAR

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

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

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

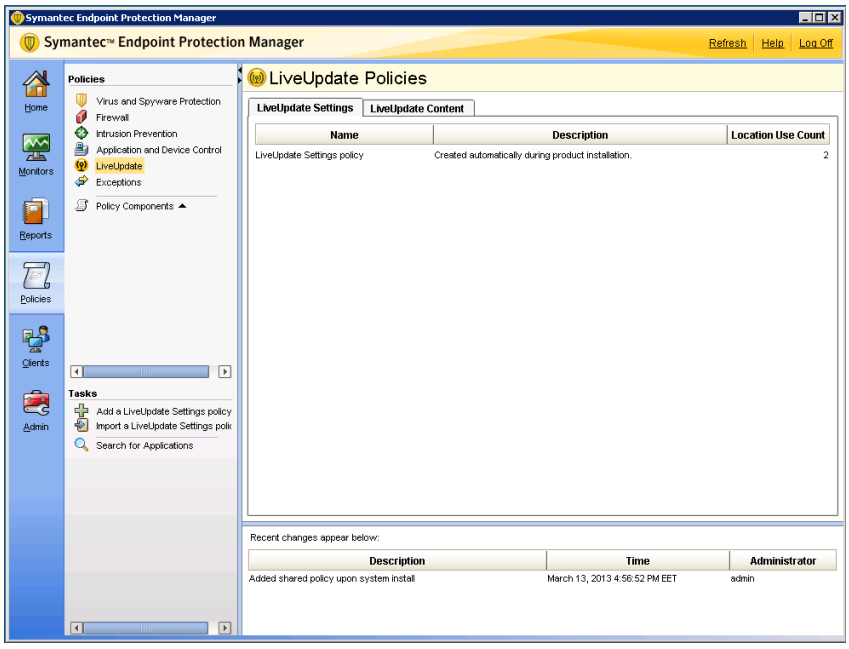
If your system requires SONAR to be enabled, configure all exclusions using the guidelines in the Folders and Files Exclusion on page 94 section.

Configuring LiveUpdate

To configure live update with Symantec Endpoint Protection:

1. Log on to Symantec Endpoint Protection Manager.
2. In the Symantec Endpoint Protection Manager, in the left-hand column, click the **Policies** tab.
3. In the **Policies** pane, click **LiveUpdate**.

   View image



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

   View image

5. Edit the policy as required.

6. In the left-hand pane, expand the **Schedule** section and set an appropriate time for running LiveUpdate.

7. Click **OK**.

Excluding Folders and Files

Exclude the folders and files specified in Folders and Files Exclusion on page 94 from your scheduled antivirus scans (Read & Write), since they are used for NICE system operations.

To exclude folders and files

1. Log on to Symantec Endpoint Protection Manager.

2. In the Symantec Endpoint Protection Manager, in the left-hand column, click the **Policies** tab.

3. Select **Extensions**.
4. Add an Exceptions policy:
    a. Go to **Exceptions Policy** > **Exceptions** > **Add** > **Windows Exceptions** > **Folder/Extensions**.
    b. Specify a folder/extension.
    c. Click **OK** and then **Yes**.
    d. Select a specific group, where to apply the policy.
    e. Click **Assign** and then **Yes**.

Configuring the CPU Priority

To configure the CPU priority

1. Log on to Symantec Endpoint Protection Manager.
2. In the Symantec Endpoint Protection Manager, in the left-hand column, click the **Policies** tab.
3. Select **Virus and Spyware Protection**.
4. Select an appropriate policy from the policies list.
5. Go to Windows **Settings** > **Administrator-Defined Scans**.
6. Select an appropriate scheduled scan.
7. Go to **Edit** > **Scan Detail** > **Advanced Scanning Option** > **Tuning**.
8. Select **Best Application Performance**.

Configuring Trend Micro OfficeScan

If you are using Trend Micro OfficeScan, do this:

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

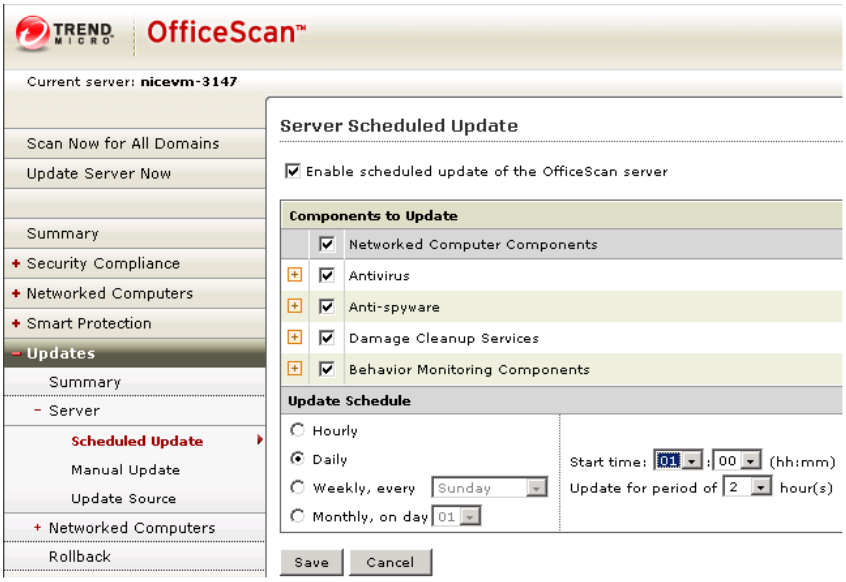
- Exclude the required folders and files from virus scanning
- Configure the CPU usage

Configuring Scheduled Updating of the OfficeScan Server

To configure scheduled updates of the OfficeScan server:

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

   View image



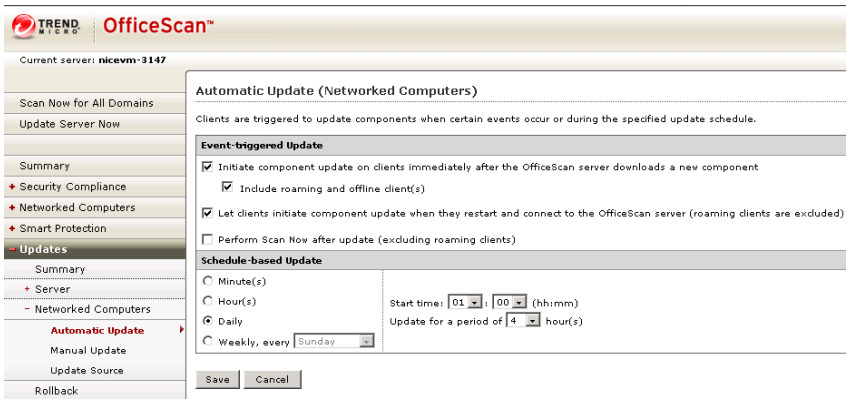
3. Select **Enable scheduled update of the OfficeScan server**.
4. In the **Components to Update** section, select the applicable components.
5. In the **Update Schedule** section, select **Daily** (highly recommended) and set the applicable parameters.
6. Click **Save**.

Configuring Automatic Update

To configure automatic update of OfficeScan clients:

1. Log on to the OfficeScan Management console.
2. In the right-hand pane, go to **Updates** > **Networked Computers** > **Automatic Update**.

View image



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

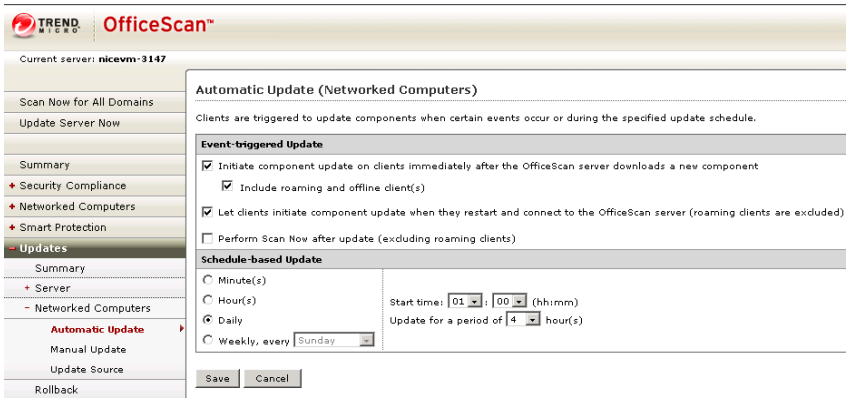
Excluding Folders and Files

Exclude the folders and files specified in Folders and Files Exclusion on page 94 from your scheduled antivirus scans (Read & Write), since they are used for NICE system operations.

To exclude folders and files:

1. Log on to the OfficeScan Management console.
2. In the right-hand pane, select **Scan Now for All Domains**.

View image



3. Go to **Server or servers > Settings >Scan Settings > Select Scan Methods**.

4. Define what folders and files to exclude.

5. Click **Save**.

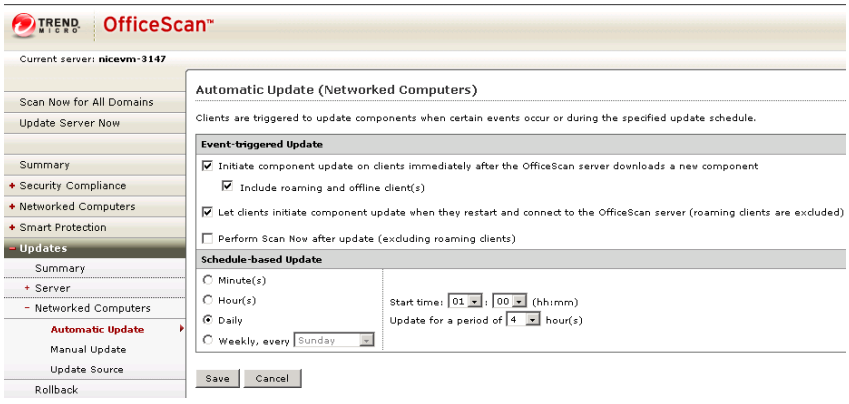
Configuring the CPU Usage

To configure the CPU usage

1. Log on to the OfficeScan Management console.

2. In the right-hand pane, select **Scan Now for All Domains**.

View image



3. Go to **Server or servers > Settings >Scan Settings > Select Scan Methods**.

4. Define the CPU usage level.

5. Click **Save**.

Configuring Sophos

If you are using Sophos, do the following:

- Configure scheduled updating
- Exclude the required folders and files from virus scanning
- Disable buffer overflow protection
- Configure scheduled scanning

Configuring Scheduled Updating

To configure scheduled updating

6. Open the Sophos Enterprise Console.
7. In the main window, go to **Polices** > **Updating**.
8. Create a new policy (or use the default one), right click it and select **View/Edit Policy**.
9. On the **Primary Server** tab, click **Advanced** and select a bandwidth use.
10. On the **Schedule** tab, enter an appropriate time.
11. Click **OK**.

Excluding Folders and Extensions

Exclude the folders and extensions specified in Folders and Files Exclusion on page 94 from your scheduled antivirus scans (Read & Write), since they are used for NICE system operations.

To exclude folders and extensions

1. Open the Sophos Enterprise Console.
2. In the main window, go to **Polices** > **Antivirus and HIPS**.
3. Create a new policy (or use the default one), right click it and select **View/Edit Policy**.
4. Click the **Extensions and Exclusions** button.

   For Extensions:

f. On the **Extensions** tab, click the **Exclude** button.

g. Click **Add**.

h. Add an extension and click **OK**.

For Folders:

a. On the **Windows Extensions** tab, click **Add**.

b. Select and item type drive or folder and specify location.

Disabling Buffer Overflow Protection

To disable buffer overflow protection

1. Open the Sophos Enterprise Console.
2. In the main window, go to **Polices** > **Antivirus and HIPS**.
3. Create a new policy (or use the default one), right-click it and select **View/Edit Policy**.
4. Select **On-access scanning** and click **Configure**.
5. Disable **Detect buffer overflows**.
6. Click **OK**.

Configuring Scheduled Scanning

To configure scheduled scanning

1. Open the Sophos Enterprise Console.
2. In the main window, go to **Polices** > **Updating**.
3. Create a new policy (or use the default one), right click it and select **View/Edit Policy**.
4. Under **Scheduling Scanning**, click **Add**.
5. Specifying scanning parameters.
6. Click **OK**.

[This page intentionally left blank]

17

Antivirus: General Antivirus

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*- 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.

Trellix ePO

- Trellix ePO 5.10 works with ENS
- Make sure that when using ePO for Microsoft patches update, the configured policy matches the NICE policy concerning Microsoft Windows updates and Service packs.

Trellix

- Make sure to **clear** the option to install the Trellix 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 ENS to 10%.
- The ENS 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 Trellix ePO 3.5 and ENS Certification for NICE 8.80.

Trellix ENS Certification

The Trellix Endpoint Security (ENS) solution is a fully integrated security solution that protects servers and endpoints against a variety of threats, such as malware, suspicious communications, unsafe websites, and downloaded files. The solution consists of these modules:

- Threat Prevention
- Firewall
- Web Control
- Adaptive Threat Protection

NICE Engage Platform Release 7.x and up are Trellix ENS Threat Prevention 10.7 certified. The Threat Prevention module checks for viruses, spyware, unwanted programs, and other threats by scanning items automatically upon access or on-demand.

Trellix ENS Threat Prevention 10.7 is part of the base certification for NICE Engage Platform Release 7.x and up (see Antivirus Matrixes for NICE Products on page 118). The Firewall, Web Control and Adaptive Threat Protection modules are not a part of base certification process.

The Trellix ENS Threat Prevention certification process was conducted under these conditions:

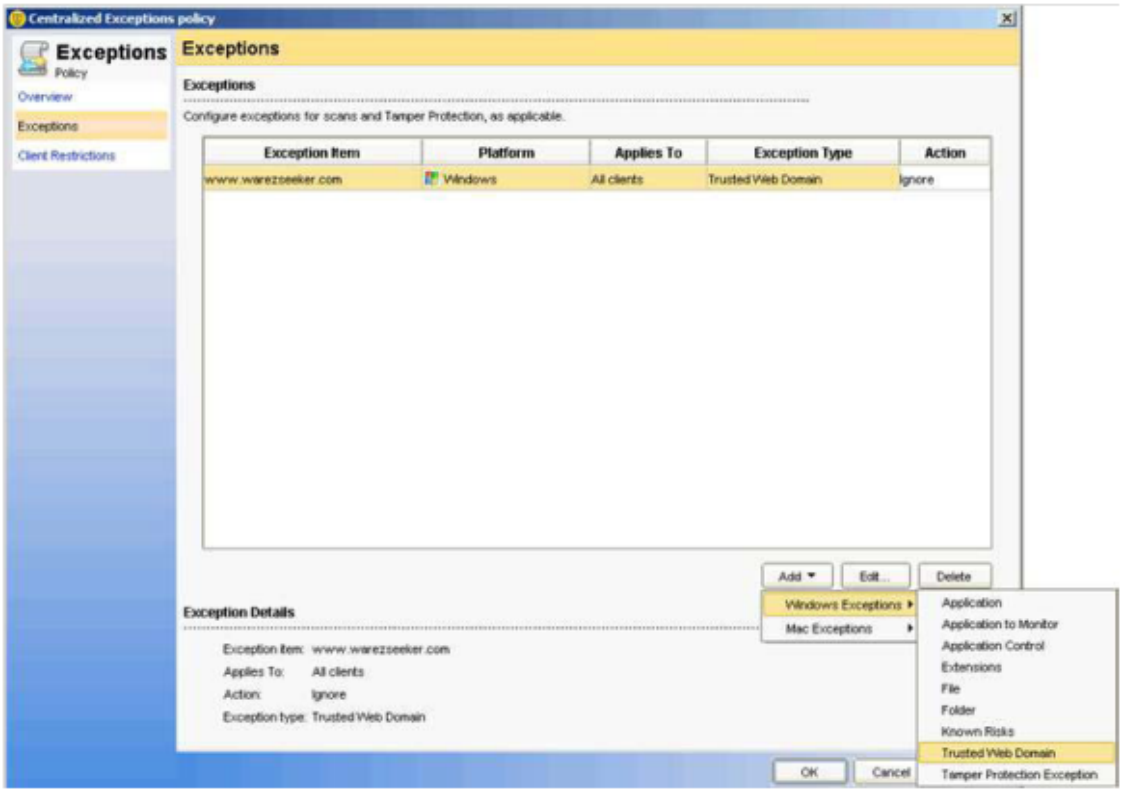
- Trellix ENS Threat Prevention ran with these protection features or technologies, which were configured with the default Trellix policy:
  - Access Protection
  - Exploit Prevention (buffer overflow)
  - On-Access Scan
  - On-Demand Scan
- NICE binaries were excluded (see Folders and Files Exclusion on page 94). NICE binary exclusion is supported by path and file names/types but not by MD5 hash or Signer.
- Full Scan and Live Update tasks were configured for idle time.

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* (**Symantec Endpoint Protection and Endpoint Security**).

  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.

  View image



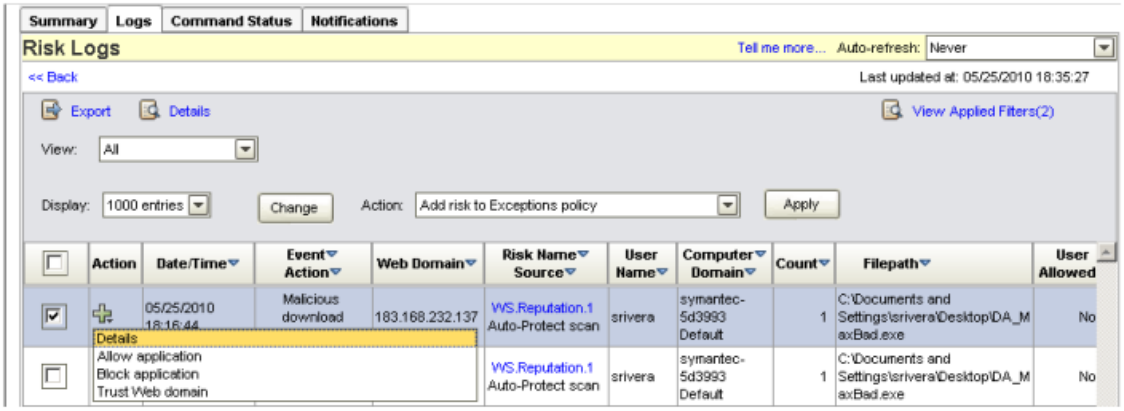
NOTE: You can select **Trusted Web Domain**, to add a Web domain to the exceptions policy.

- 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.

View image



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

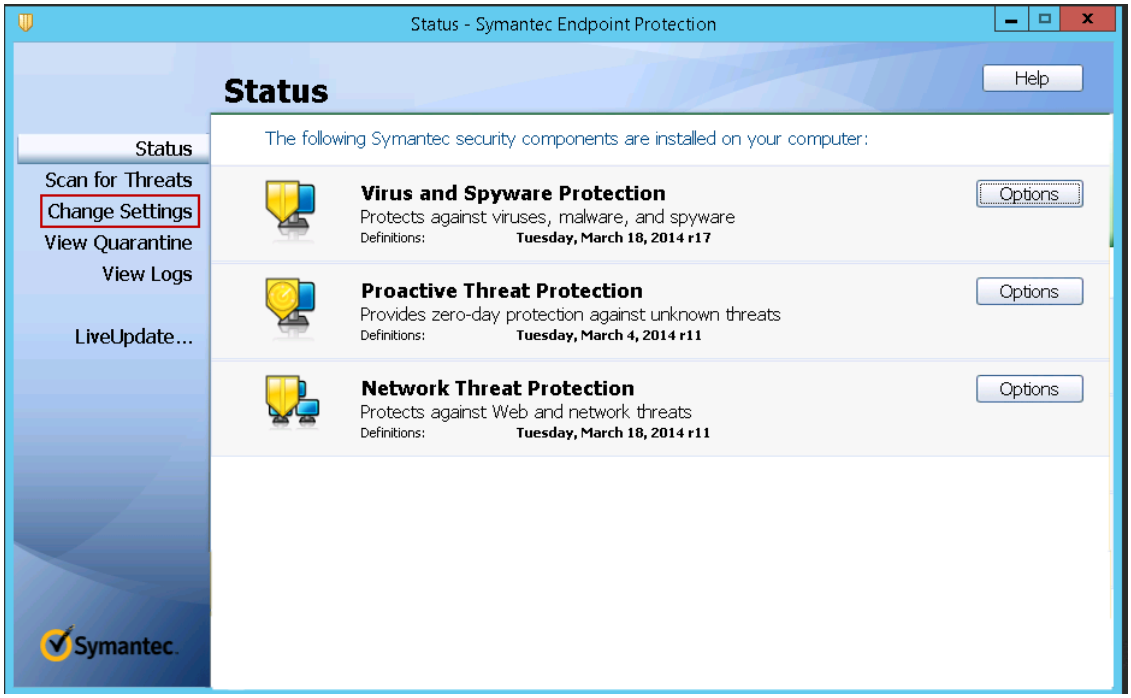
SEP Limitations

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:

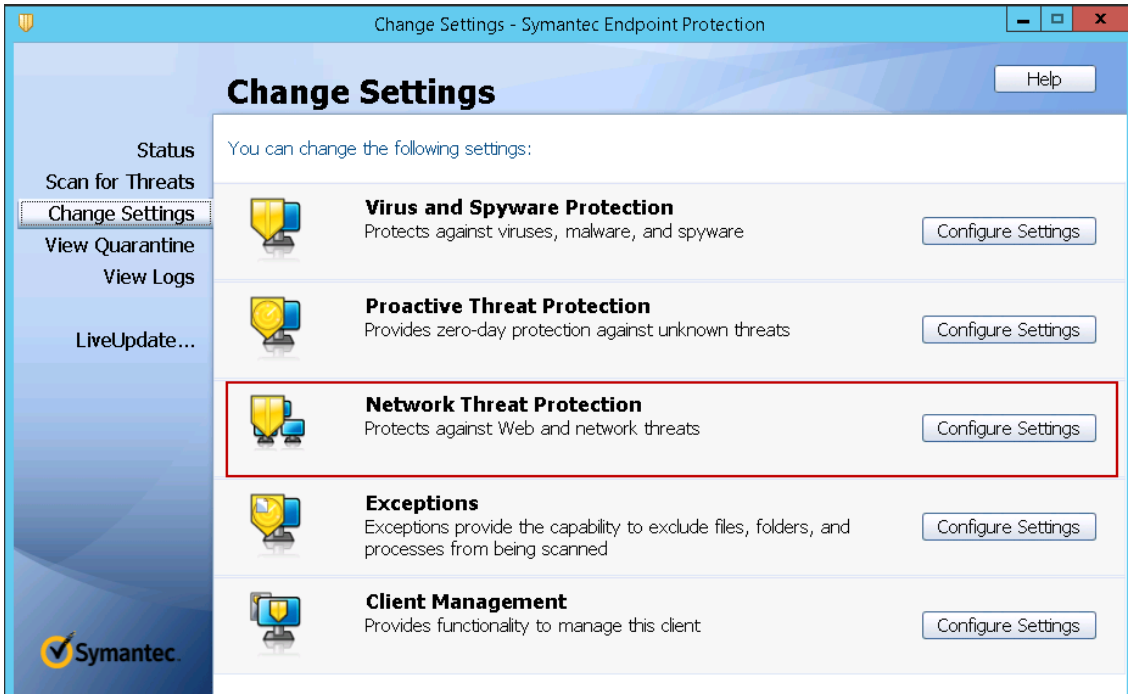
1. Open Symantec Endpoint Protection (SEP).

View image



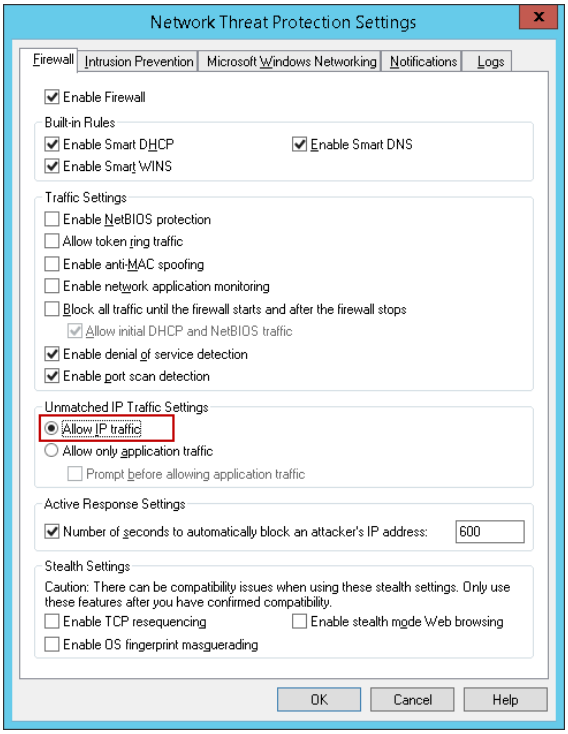
2. In the left column, click **Change Settings**. The Change Settings area appears on the right.

View image



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

View image



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 Engage Platform 7.x 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.

Microsoft Defender Antivirus

Microsoft Defender Antivirus is an anti-malware component of Microsoft Windows. It is built into Microsoft Windows and works with Microsoft Defender for Endpoint to provide protection on devices and in the cloud.

Microsoft Defender Antivirus is the major component of the next-generation protection in Microsoft Defender for Endpoint. This protection combines machine learning, big-data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices (or endpoints) in your organization.

- Supported operating systems:
  - Windows 10 or up
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server version 1803 or up.
- Versions: from 1.371.120.0 and up.

Antivirus Matrixes for NICE Products

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

NICE Engage 7.x Antivirus Support

NICE Products	SEP 14	Trellix ePO 5.10	Trellix ENS 10.7	Trend Micro Apex One 2019 SP1	Sophos 10.8	Microsoft Defender Antivirus*
Interactions Server	Y	Y	Y	Y	Y	Y
Playback Server / Telephony Services Server	Y	Y	Y	Y	Y	Y

NICE Products	SEP 14	Trellix ePO 5.10	ENS 10.7	Trend Micro Apex One 2019 SP1	Sophos 10.8	Microsoft Defender Antivirus*
Storage Center **NOTE:** There is no Storage Center in NICE Engage 7.x clean installation. However, Storage Center can be found if there was an upgrade to 7.x.	Y	Y	Y	Y	Y	Y
Application Server	Y	Y	Y	Y	Y	Y
Reporter	Y	Y	Y	Y	Y	Y
Database Server	Y	Y	Y	Y	Y	Y
Sentinel	Y	Y	Y	Y	Y	Y
RTA - Enrollment Engine	Y	Y	Y	Y	Y	Y
Advanced Interaction Recorder	Y	Y	Y	Y	Y	Y
NPP	Y	Y	Y	Y	Y	Y
NPP Extractor	Y	Y	Y	Y	Y	Y
MS Teams	Y	Y	Y	Y	Y	Y

NICE Products	SEP 14	Trellix ePO 5.10	ENS 10.7	Trend Micro Apex One 2019 SP1	Sophos 10.8	Microsoft Defender Antivirus*
KVS	Y	Y	Y	Y	Y	Y

* In some cases SEP can detect NICE's binaries as a potential security risk.

* Microsoft Defender Antivirus installed on top of Windows OS versions is supported by Engage.

18

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. 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.

2. Microsoft Teams - The customer or NICE can set up the Teams meeting.

3. 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.

[This page intentionally left blank]

19

NICE Third Party Software Certification Policy

This internal policy outlines the procedures to be carried out by the NICE System QA team in relation to validation of security related software compatibility with NICE products.

These conducts and procedures aim to:

- Assure customers of NICE products that the systems and components of NICE are compatible with third party software that are likely to be installed in NICE servers and on client desktops.
- Provide clear guidelines regarding compatibility validation and certification processes for the Professional Services group.
- Allow consistent and efficient work by the System QA team.
- Reduce time and money spent by NICE on a global level, and ensure efficient use of its resources.

This commitment involves delicate balances and trade-offs. Therefore, compatibility validation is limited only to commonly accepted third party software, which directly affects the system's overall security and serviceability.

This policy states general technical guidelines and shall not be construed in a manner which shall impose any type of legal undertaking on NICE. In particular, NICE does not warrant the compatibility of validated third party software with the NICE products, or that the validated security related software will operate error-free, or in an uninterrupted fashion.

NICE Products

For clarity, the tables below list the components that require compatibility validation for the latest versions of NICE Engage Platform. The validation includes all testing required to ensure that the normal functionality of the components and of the entire system is not affected by the introduction of the additional third party software. The compatibility validation testing is related to the specific version of the third-party software. Validation of a specific version of the third-party software shall not guarantee the compatibility of any subsequent version of the third-party software.

The compatibility validation for **NICE Engage Platform Release 7.x** with the latest service pack and updates includes the following components:

NO.	Component	Operating System	Version
1.	AIR	Windows Server 2016, Windows Server 2019*	
2.	Applications Server	Windows Server 2016, Windows Server 2019*	
3.	Database Server	Windows Server 2016* Windows Server 2019*	
4.	Playback Portal Stream Server	Windows Server 2016, Windows Server 2019*	
5.	Interactions Center Server	Windows Server 2016, Windows Server 2019*	
6.	NICE Sentinel Server	Windows Server 2016, Windows Server 2019*	
7.	NICE Stream Server	Windows Server 2016, Windows Server 2019*	
8.	Storage Center Server **NOTE:** There is no Storage Center in NICE Engage 7.x clean installation. However, Storage Center can be found if there was an upgrade to 7.x.	Windows Server 2016, Windows Server 2019*	
9.	Telephony Services Server	Windows Server 2016, Windows Server 2019*	

NO.	Component	Operating System	Version
10.	Voice Biometrics Server	Windows Server 2016, Windows Server 2019*	
11.	Playback Portal Database Server	Windows Server 2016, Windows Server 2019*	
* See appropriate Certified Server Guide			

NO.	Component	Operating System	Version
1.	BSF Toolkit	Windows 10, Windows 11*	
2.	ScreenAgent	Windows 10, Windows 11*	
3.	NICE Player	Windows 10, Windows 11*	
4.	ROD/SOD Desktop Application	Windows 10, Windows 11*	
5.	Reporter Viewer	Windows 10, Windows 11*	
6.	Survey Manager	Windows 10, Windows 11*	
7.	Sentinel Client	Windows 10, Windows 11*	
8.	VoIP Recording Agent (VRA)	Windows 10, Windows 11*	
* See appropriate Certified Server Guide			

Compatibility Validation Policy

All of the NICE products listed in NICE Products on page 123 are validated for compatibility with the following software:

- Commonly used antivirus software (see list on page 129)
- New versions of Microsoft Windows Operating System (only under product management direction)

- Microsoft .NET Framework - new versions and service packs
- New versions of Microsoft SQL Server (only under product management direction)
- Microsoft SQL Server service packs
- Supported web browsers - new versions and service packs
- Microsoft Windows security patches and service packs
- Microsoft Windows security advisory patches
- Microsoft Windows Daylight Saving Time (DST) updates
- Commonly used third party software:
  - Patch management tools (see list on page 129)
  - Remote support tools (see list on page 129)
- Customer's hardening guidelines (only under commitment)

The list of NICE products and their components is regularly updated (on a quarterly basis or on demand) according to the NICE Sunset Policy (refer to the most recent Marketing Note - *NICE Sunset Dates*) and the introduction of new NICE products/components and product/component versions.

When a product version meets its End-of-Mainstream Software Support Date, it is no longer validated for any of the above mentioned software, except for Microsoft security patches, security Advisory patches, Daylight Saving Time updates and service packs, as well as web browser updates, for which validation for compatibility will continue until the product version's End-of-Extended Software Support Date is met.

NOTE:

- End-of-Mainstream Software Support Date - The final date when NICE will cease to provide code fixes and changes for a product version.
- End-of-Extended Software Support Date - The final date when NICE will cease to provide critical code fixes and changes for a product version. Requests for third-party software certifications may require an upgrade to a newer minor/major release.

Validation of the above mentioned software ceases when Microsoft no longer supports the respective operating system required to run this product version (for example, when Microsoft ceases to release patches and service packs for the operating system in question).

> **Show example**
>
> The end of support date for Windows 2003 is July 14, 2015. The end of support date for Windows XP SP2 is April 4, 2014.

A compatibility matrix of NICE products/components and product/component versions vs. Microsoft or third party software and software versions is maintained and tested by the System QA team.

When a new NICE product/component or a new version of a product/component is introduced, it is added to the compatibility matrix. See Compatibility Matrix on page 134.

Based on agreement with Product Management, an older version of a product/component or a third party software may be omitted from the compatibility matrix, in the following cases:

- A version is no longer commonly used by NICE customers. For example, an older version of an antivirus software (two or more years older), will be omitted from the compatibility matrix since antivirus software is usually replaced once a year with a newer version, and most customers switch to the newer version shortly after its release.
- Both Product Management and R&D view the newer version of a NICE product/component as an evolutionary (rather than revolutionary) step in the development of the product/component and the testing of the newer version fully ensures, in high probability, the compatibility of older versions. Hence, the older version is omitted from the compatibility matrix.

Compatibility Validation Process

The System QA team develops and publishes comprehensive test procedures for each type of compatibility validation.

The System QA team is in constant contact with local third party software vendors who are included in the compatibility matrix, and proactively checks for new updates at least once a month. The System QA team maintains an internal list of planned validations, listing details of vendors' software release dates, and the appropriate NICE validation target dates stipulated in this policy.

In addition, the System QA team can be assigned to validate the compatibility of third party software that is not included in the compatibility matrix, if requested by Product Management, and subject to a commitment. The System QA team will be asked to provide a timetable dating from ARO (After Receipt of Order), and include this one-time validation in its list of planned validations. In this case, the System QA team will not be required to proactively track and validate future software version compatibility.

The System QA team notifies the EIS Technical Writing group of expected new compatibility validations, and regularly informs the Technical Writing group of validation status changes. The Technical Writing group publishes and maintains this information in the Documentation Hub. This information includes the following validation details:

- Vendor name
- Third party software name

- Software version
- Software release date – which can also be a future date
- Validation completion target date
- Validation status. The following status options are applicable: Pending software release, Pending validation, Under validation, Validated.
- Last status update
- Comments. The comments may include a link to a relevant technical note.

Upon the completion of the compatibility validation, and no later than 10 business days thereafter
(5 business days in case of validation of Microsoft high risk security patches, see Microsoft Security Patches on page 17), the System QA team updates the *Third Party Technical Guidelines*, specifying the newly validated software. This update may also include validated third party software limitations and recommended installation guidelines for NICE products. Before appearing in the *Third Party Technical Guidelines*, these updates are sent to Product Management for approval.

Compatibility Validation by Professional Services

The System QA team develops and publishes comprehensive test procedures (ATP) adequate for compatibility validation of third part software categories not included in the compatibility matrix, as listed below:

- Antivirus and endpoint protection
- Intrusion detection and prevention
- File integrity
- Log collection
- Backup agent
- Monitoring agent
- Remote access
- Patch management and distribution
- SOE and customer certified OS build

Third party software not included in the compatibility matrix is validated for compatibility according and subject to the following process:

1. A Commitment Request is filed by the Solution Engineer responsible for the project, providing the full details of the project.

2. Product Management evaluates the commitment and forwards it to the System QA team if required. A detailed test plan (ATP) is provided based on the type of software.

3. Product Management assigns the commitment to the regional Professional Services team, who provide a timetable dating from ARO, and a cost estimate.

4. When off-site staging is required, the regional Professional Services team takes responsibility for execution.

5. The Professional Services team runs the ATP on-site, to validate the software compatibility on NICE servers.

6. The completed ATP is re-submitted to the System QA team for approval. If additional or repeated testing is required, the System QA team instructs Professional Services accordingly.

7. The System QA team supports the software for the validated version only. Future versions of the software are not proactively tracked or validated by the System QA team or Professional Services.

8. the System QA team makes a reasonable effort, time and money-wise, to diagnose and solve problems if the arise. If no reasonable solution is diagnosed and/or found, NICE is not held responsible, and the software is removed from NICE servers.

9. Once verified, a Verification Statement is be published by the Services Manager, describing the environment in which the verification is applicable. Any change to the environment (including software upgrades), voids the verification.

Compatibility Validation Guidelines

These are the guidelines by which all of the NICE products are validated for compatibility with the following software:

Antivirus Software

The System QA team regularly validates the most commonly used antivirus software. As agreed with Product Management, this list currently includes:

- Symantec AntiVirus Corporate Edition
- Trellix ePO and ENS
- Trend Micro OfficeScan
- Sophos Endpoint Security and Control

Usually, customers replace antivirus software versions soon after the release of a new version by the vendor. Therefore, the System QA team is required to test and validate only the last two most recent *major releases* of the above mentioned antivirus software packages. Minor releases are supported when major releases have been certified. For the complete antivirus compatibility matrix, see the Antivirus: General Antivirus on page 111 section.

Other antivirus software packages may be validated on demand, based on commitment.

The System QA team is in constant contact with the local antivirus software vendors, and proactively checks for new updates at least once every quarter.

Validation of a new antivirus software version will take place no later than **45 business days** after its general availability.

Microsoft Windows Operating System

The System QA team validates NICE products for compatibility with a new *major version* of Microsoft Windows Operating System (OS) within **60 business days** following the Microsoft official release. This refers to Windows editions planned to be in use by NICE products, servers, and clients, under Product Management direction.

Compatibility validation of a new version of Windows OS includes validation of the most recent available version of a web browser.

Microsoft Service Packs

The System QA team validates NICE products for compatibility with Microsoft service packs within **30 business days** following the Microsoft official release.

Microsoft .NET Framework

The System QA team validates NICE products for compatibility with Microsoft .NET Framework new versions and service packs within **30 business days** following the Microsoft official release.

The System QA team compatibility validation ensures that the normal functioning of NICE applications is not effected by the new .NET Framework software if installed simultaneously on the same desktop with the .NET Framework version utilized by NICE applications. This requires validation on all operating systems supported by NICE applications.

Microsoft SQL Server

The System QA team validates NICE products for compatibility with a new *major version* of Microsoft SQL Server within **60 business days** following the Microsoft official release. This refers to SQL Server editions planned to be used by NICE products under Product Management direction.

Microsoft SQL Server Service Packs

The System QA team validates NICE products for compatibility with Microsoft SQL Server service packs within **30 business days** following the Microsoft official release. This includes service packs for all supported SQL Server editions used by NICE products.

Web Browsers

The System QA team validates NICE products for compatibility with web browsers. Other Internet browsers are currently not supported.

Compatibility validation of web browser service packs follows the same validation guidelines for Windows service packs (see Microsoft Service Packs on the previous page).

The System QA team validates NICE products with a new *major version* of the web browser within **30 business days** following the Microsoft official release.

Compatibility validation of a new version of Windows Operating System (OS) includes validation of the most recent available version of the web browser.

Microsoft Security Patches

Microsoft classifies its security patches as follows:

1. Critical
2. Important
3. Moderate
4. Low

NICE considers Critical and Important security patches as High Risk patches, and Moderate and Low security patches as Low Risk patches.

According to NICE policy, High Risk patches are validated by the System QA team in an expedited manner within **5 business days**.

Low Risk patches are validated together with high risk patches. For example, if at a given time, moderate and/or low patches are released with at least one critical or important patch, all patches will be validated. Otherwise, the low risk patch validation is postponed until the next release of high risk patches.

The System QA team is registered on the Microsoft site for alerts of security patches releases. Upon a Microsoft patch release, the System QA team notifies Product Management, Customer Services and the Technical Writing group, listing patches that are relevant to NICE, and their expected validation date.

No later than **72 hours** after a high risk patch release, the Documentation Hub is updated to inform NICE customers and partners of the expected patch compatibility (content is published in Engage Security Bulletins).

Information about validated bulletins is published using Excel format. The Excel file will be updated periodically with new security bulletins. The new bulletins are added to the same aggregated Excel file.

The Excel file includes bulletins in 3 categories:

1. Bulletins which are certified by NICE: Bulletins that were tested by NICE and approved for installation.

2. Bulletins which are not relevant for NICE: Bulletins. Bulletins that appear under this section affect Microsoft components that should not be installed on NICE servers, and as a result, should NOT be installed. Sample Microsoft components: Domain Controller, DNS server, Microsoft Office.

3. Bulletins which are not certified by NICE: Bulletins that were tested by NICE and were not approved for installation.

Microsoft Security Advisory Patches

Microsoft Security Advisory Patches are a supplement to Microsoft Security bulletins, and address security changes that may not require a security patch, but that may still affect overall security.

NICE considers the Microsoft Security Advisory Patches as Low Risk patches.

According to NICE policy, Low Risk patches are validated by the System QA team , together with the next High Risk patch release (seeMicrosoft Security Patches on the previous page).

Microsoft Daylight Saving (DST) Updates

Daylight Saving Time (DST) updates move local time forward one hour ahead of standard time in the spring and set it back one hour in the fall. Microsoft has established an annual update schedule for DST updates, with provisions for semi-annual cumulative updates if necessary.

According to NICE policy, DST updates are validated by the System QA team within **45 business days** following the Microsoft official release.

Patch Management Tools

Many NICE customers use patch management tools. Patch management tools allow automatic deployment of Microsoft patches to enterprise servers, including NICE servers, and to client desktops.

In many cases, the deployment of a security patch or service pack requires restarting the machine. The System QA team will test and validate that such reboots forced by the patch management agents can be properly handled by NICE servers and agents. In particular, NICE servers and agents must recommence their normal work immediately following a machine restart after a forced reboot.

Most of the patch management tools allow the setting of rules, as to what is to be installed, when and where. It is imperative that these settings do not contradict the NICE policy for Microsoft security patches and service packs, as stated in MN1145. The System QA team will test and publish recommendations regarding the proper configuration of the patch management tool in order to conform with the NICE policy.

Given the variety of tools available and lack of consistent requirements by the market, and since the NICE solution is based on Microsoft Windows technology, the System QA team will validate, by default, the following Microsoft patch management tool(s):

- Microsoft Systems Management Server (latest version).
- System Center Configuration Manager (latest version).

Other tools might be added to the list of compatible patch management tools upon demand, based on commitment or Product Management request.

Validation of a new patch management software *major version* takes place no later than **45 business days** after its general availability.

Remote Support Tools

NICE is required to support remote support tools, in addition to Symantec pcAnywhere (PCA).

Remote support tools validated by NICE must be able to provide remote support for all NICE products over VPN, with full screen view, using encrypted session and strong authentication.

By default, the System QA team validates the following remote support tool(s), in addition to pcAnywhere:

- Microsoft Remote Desktop

Other tools might be added to the list of compatible remote support tools upon demand, based on commitment or Product Management request.

Validation of a new remote support software *major version* takes place no later than **45 business days** after its general availability.

Server Hardening

The System QA team publishes an updated Hardening Guide for Windows 2016 and Windows 2019, for every new release of NICE Engage Platform.

The hardening process is based on the Center for Internet Security (CIS) Standard.

The NICE Hardening Guide accurately describes the minimal set of services, protocols, user rights assignments, permissions to system resources, and communication ports required to allow normal functioning of the NICE system.

In certain scenarios, if a customer cannot make the necessary analysis based on the information provided by NICE, the customer might ask NICE to validate their hardening procedures based on the customers' IT department security policies. Such a validation could require special staging of a testing environment. This validation could be performed by the System QA team and/or NICE Professional Services in the local region, based on commitment and Product Management approval.

Compatibility Matrix

The following table summarizes the response times required for different types of compatibility validation.

Validation Type	Maximum Validation Response Time	Comment
Antivirus	45 business days	Major versions of leading vendors only (see list on page 129)
Web Browsers	30 business days	Major versions only
.NET Framework	30 business days	New versions and service packs
Patch Management	45 business days	Major versions of Microsoft tools only (see page 129)
Remote Support	45 business days	Major versions of selected tools only (see page 129)
Security patch – High-risk	5 business days	Preliminary notification on Documentation Hub within 72 hours of patch release
Security patch – Low-risk	With (next) high risk security patch	
Security Advisory patch	With (next) high risk security patch	

Validation Type	Maximum Validation Response Time	Comment
Daylight Savings Time update	45 business days	
SQL Server	60 business days	Major versions – under Product Management direction
SQL Server Service Pack	30 business days	
Windows Operating System	60 business days	Major versions – under Product Management direction
Windows Service Pack	30 business days	

[This page intentionally left blank]

20

Vulnerability Scanner Guidelines

This section provides guidelines for configuring vulnerability scanner software running on NICE applications.

Nessus Vulnerability Scanner

Tenable Network Security Nessus is a security software application that allows you to perform vulnerability scanning of infrastructure with automatic scan analysis for remediation prioritization, configuration auditing and compliance checks.

Follow the below guidelines to improve your system performance and prevent recording loss, when running Nessus scans.

Advanced Interaction Recorder

A full Nessus scan with a full-range port scan interrupts recording. To prevent recording loss, use these options:

- Instead of a full-range port scan, run a filtered-range port scan with the Service Discovery function.

  A filtered-range port scan excludes ports used by NICE components on each server type. See the Ports List document for ports to be excluded.
- Run full Nessus scans only when the system is idle, and no recordings are made.

Interactions Center

A full Nessus scan with a full-range port scan and the Service Discovery function interrupts recording. To prevent recording loss, use these options:

- Run a full-range port scan without Service Discovery.
- Run full Nessus scans only when the system is idle, and no recordings are made.

21

SQL Backup

This section provides guidelines for backing up NICE Engage Platform SQL databases.

SQL Backup Guidelines

Overview

Customers can implement their own database backup policies for NICE Engage Platform database.

NOTE:

- Each backup schedule provides a different level of recovery. Customers should match recovery levels according to their needs.
- The customer is responsible for database backup operations. They should ensure that there is enough free space for the database and backups.
- Customers MUST NOT restore the SQL database from the backup to production system without first consulting with NICE Customer Services.
- Backup software should be used when the size of any of the NICE server databases are approximately 1TB and larger. SQL Backup jobs should not be used in such a scenario.

Schedule

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

Below is a sample backup schedule:

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

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

Backup Files Location

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

Implementation Guidelines

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

Disable the following SQL Jobs on the Database server:

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

Disable the following SQL Jobs on the Data Mart server:

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

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

Backup Tools

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

Database Configuration Guidelines

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

- SQL Server log backups are essential.
- In the **Full Recovery Model**, all transactions are logged in the transactional log until they are backed up. Therefore, log backups must be created on a regular basis. Hourly backup is recommended.

- Transactional log disk space monitoring is essential. If the transactional log is not purged due to backup failure, new transactions and/or calls will not be added to the database.