National Utilization Management Integration (NUMI)

Server Setup Guide

Release 1.1.15.9

Department of Veterans Affairs

June 2020

Revision History

Date	Description	Author
04/22/2009	Submitted to Medora Team for	Rob Fatzinger
07/14/2009	Updated to reflect “Release 1.1”	Suzanne Van Order
08/28/2009	Updated document name to	Suzanne Van Order
08/01/2011	Updated per issues found in AITC	Dan Michaelis,Wai
08/02/2011	Updated section 9.9 per AITC	Doug Lincoln
08/04/2011	Refined CERME instructions in section 6 per AITC Windows SA	Doug Lincoln
08/24/2011	Refined MDWS instructions in section 6.12-6.15 per AITC	Doug Lincoln
10/13/2011	Updated CERME instructions in	Tim Blanchard
04/10/2012	Draft preliminary update for	Dave Curl
07/03/2012	Added figures to section 6.13; Added captions to figures throughout; replaced example in section 6.12, step #10; added new section 6.14; updated cover and footers to “Release 14” per VA PM	Eric Dahlenburg
01/03/2013	Added section 6.12; updated section 6.13 with new Fig. 19, corrected Section 6.14, Windows Event Log and updated SSL setup and config; updated 6.19 per Operational feedback; added Appendix F NUMI Exchange	Eric Dahlenburg
03/25/2013	Modified section 6.15 for NUMI event folder, modified section 6.19	Dave Curl
3/29/2013	Removed original highlighting and updated per customer feedback: changed Section 2.2 Web Server (Server 2) to reference NUMI Exchange and MDWS; updated Section 3.1 Disk Space and Devices; updated Section 5.1 to reference test environments and removed Section 5.6, Installation During Off Peak Hours. Also reordered installation steps SQL and CERMe (now section 6.1 and 6.14) and added CERMe SSL	Dave Curl
5/13/2013	Corrected release referenced in section 1, removed content for Windows Server 2003 and IIS 6 setup, added content for Windows Server 2008 and IIS 7 setup, added content for MDWS 2.Xinstallation, re-organized document content.	D. Curl
5/24/2013	Made the following corrections per VA comments: Changed section 2.2.1 to specify SQL Server 2005, changed figures 37, 38, 39 to reflect MDWS1.2, added MDWS config information to section 6.11.3 (MDWS1.2) and 6.12.4 (MDWS2.x), added execution timeout setting for the synchronizer in section 6.18.1, step 4.	D. Curl
6/17/2013	Made the following corrections per VA comments: Changed section 2.2.1 to clarify restoring from a NUMI backup database and added replication comments, updated 3.1.3 with CPU capacity details, updated section 3.1.4 with disk space details;	D. Curl

Date	Description	Author
	changed section 5 to clarify restoring from a NUMI backup database, updated section 5.1 added synchronizer and user account information, removed original item 3, updated section 6.7 to specify version and recovery mode, updated section 6.8 removed Medora information, updated section 6.19 to add more script information.	
6/27/2013	Updated to version number to 14.1 changed sections 2.2.1 and 5. To include 14.0 and 14.1 database information.	D. Curl
7/2/2013	Changed example directory references to remove 14.0	D. Curl
8/2/2013	Removed references to CERMe 2012. Changed hard coded build name directory references to <install_dir>.	D. Curl
8/20/2013	Added version number for MDWS in section 2.2.2, added version number for CERME in section 2.2.3, added RAM to section 3.1.3, updated Figure 68, removed MDWS 1.2 section 6.11, renamed MDWS 2.x to MDWS 2.7.3.2 in section 6.12, renamed section 6.12 to 6.11	D. Curl
5/11/2015	Updated the version number from 14.1 to 14.2	Padma Subbaraman
11/12/2015	Updated the version number from 14.2 to 14.3	Padma Subbaraman
09/12/2016	Updating document for NUMI 14.4 and .NET version. Made the Windows version generic	Padma Subbaraman
9/20/2016	Updated install instructions for 15.0 and updated CERMe installation instructions and IIS and File service installation screenshots	Gopalakrishnan Unnikrishnan
2/3/2017	Added steps to encrypt the configuration files	Gopalakrishnan Unnikrishnan
3/1/2017	Updates for IAM SSO integration changes	Praveen Potturu
3/27/2017	Added CA WebAgent setup instructions	Praveen Potturu
5/25/2017	Reviewed document and revised	Gopalakrishnan Unnikrishnan Cheryl Jones
11/14/2017	Updated release version number (version 15.4) and CERME upgrade installation steps	Sunita Chundury
04/23/2018	Update release version number (15.5)	David Overstreet
10/1/2018	Updated release version number (15.6)	Sunita Chundury
02/19/2018	Updated release version number (15.7) and new Synchronizer installation instructions.	Jason Confer
08/28/2019	Updated release version number and added STS integration information (Section 13).	Jason Confer
2/1/2020	Updated release version number (15.9)	Daniel Henderson
5/28/2020	Updated CERMe RM and InterQual View version (19.0/2020)	Sunita Chundury

Table of Contents

1. Introduction 1
   1.1. Purpose 1
   1.2. Scope 1
   1.3. Target Audience 1
2. Deployment Overview 1
   2.1. National Deployment Request 1
   2.2. Installing NUMI on the Servers 1
      2.2.1. Database Server 1
      2.2.2. Web Server 2
      2.2.3. Application Server 2
3. Pre-Installation Instructions and Preparation 2
   3.1. Installation Process Requirements 2
      3.1.1. Minimum Software Version 2
      3.1.2. Resources Required 3
      3.1.3. CPU Capacity 3
      3.1.4. Disk Space 3
      3.1.5. Devices (Servers, etc.) 3
      3.1.6. VistA Rights Needed for NUMI Users 3
   3.2. Install Software in Test Environments 4
   3.3. Generate Pre-Installation Reports 4
   3.4. Coordinate Installation with Other Teams 4
   3.5. Install Sequence Information for Multiple Patches 4
   3.6. Logoff During Installation 4
   3.7. Average Amount of Time Required to Complete the Installation 4
4. Database Information 5
   4.1. Instructions for Installing Database Components 5
      4.1.1. Database Installation / Restoration Procedures 5
5. Installation Procedure for Server 2012 R2 5
   5.1. Patch the Operating System 5
6. SQL Server Setup (Windows Server 2012 R2) 6
   6.1. Role Setup 6

7. Web Server Setup (Windows Server 2012 R2) 6
7.1. Role Setup 6
7.2. ASP.NET 2.0 AJAX Extensions 1.0 Setup 9
7.3. MS Web Services Enhancements (WSE) 3.0 Setup 9
8. Application Server Setup (Windows Server 2012 R2) 9
8.1. Role Setup 9
8.2. Feature Delegation 11
8.3. Install MS ASP.Net 2.0 AJAX Extensions 1.0 12
8.4. Install MS Web Services Enhancements 3.0 16
9. Install SQL Server 19
9.1. Download all SQL Server Patches 20
9.2. Restore the Appropriate Databases for the NUMI Application 20
10. Installing NUMI Exchange on Server 2012 R2 20
10.1. Unzip/Install NUMI Exchange Distribution 20
10.2. NUMI Exchange Website Configuration 20
10.2.1. Application Pool Configuration 24
11. Installing NUMI on Server 2012 R2 27
11.1. Software Copy Instructions 27
11.2. NUMI Web Site Configuration 27
11.3. Application Pool Configuration 33
12. Install CA SiteMinder Web Agent for Single Sign On (SSO) on the Web server 37
12.1. Agent location 37
12.2. Agent installation 37
12.3. Agent configuration 41
12.3.1. Configuring for the first time 42
12.3.2. Reconfiguration configuration 48
13. Secure Token Service Integration for SSOi 54
13.1. Download Certificate Chain from appropriate endpoint 54
13.2. Export server cert to .pfx 59
13.3. NumiWebApp.config keys 61
14. Installing CERMe Software and Database from CERMe Installation CD

..... 61
14.1. Install CERMe on the Application Server 62
14.2. Install CERMe SSL Certificate 64
15. Setting up NUMI Section in the Windows Event Log 68
15.1. Validate XML Configuration File Settings 69
16. Perform Restart 71
17. Test NUMI Web Site Functionality 71
18. Installing NUMI Synchronizer on the DB Server 71
18.1. Installation Instructions 71
18.2. Uninstall: 74
18.3. Validate Installation: 74
18.4. Add Jobs to the SQL Server 74
19. Post-Installation Considerations 75
20. Acronyms and Descriptions 76
21. Numi Comparison Table 77

List of Tables

Table 1: CPRS Rights....4
Table 2: CPRS Access Tabs....4
Table 3: IAM Host Configuration Object....43
Table 4: SiteMinder Policy Server IP Address....44
Table 5: SSOLogoutUri values....70

List of Figures

Figure 1: SQL Server Role Services....6
Figure 2: NUMI Exchange Role Services....7
Figure 3: NUMI Exchange (IIS)....8
Figure 4: NUMI Role Services....9
Figure 5: NUMI Web Services IIS....10
Figure 6: IIS Feature Delegation....11
Figure 7: Feature Delegation Selection....12
Figure 8: MS ASP.Net 2.0 File Download-Security Warning Window....13
Figure 9: MS ASP.Net 2.0 Internet Explorer-Security Warning Window....13
Figure 10: MS ASP.NET 2.0 AJAX Extensions 1.0 Setup Wizard Window....14
Figure 11: MS ASP.NET 2.0 AJAX License Agreement Window....14
Figure 12: MS ASP.NET 2.0 AJAX Installation Window....15
Figure 13: MS ASP.NET 2.0 AJAX Completion window....16
Figure 14: MS WSE 3.0 File Download-Security Warning Window....16
Figure 15: MS WSE 3.0 Internet Explorer-Security Warning Window....17
Figure 16: MS WSE 3.0 InstallShield Wizard Welcome Window....17
Figure 17: MS WSE 3.0 License Agreement Window....18
Figure 18: MS WSE 3.0 InstallShield Wizard Window....18
Figure 19: MS WSE 3.0 Installation Window....19
Figure 20: MS WSE 3.0 Completion Window....19
Figure 21: Add NUMI Exchange Website....21
Figure 22: NUMI Exchange Website....21
Figure 23: NUMI Exchange Basic Settings....22
Figure 24: NUMI Advanced Settings....22
Figure 25: NUMI Exchange Bindings....23
Figure 26: NUMI Exchange Authentication Settings....23
Figure 27: NUMI Exchange SSL Settings....24
Figure 28: Application Pool Window....25
Figure 29: NUMI Exchange Application Pool Basic Settings....25
Figure 30: NUMI Exchange Pool Advanced Settings....26
Figure 31: Unblocking Restricted Files in Installation ZIP File....27
Figure 32: Add NUMI Website....28
Figure 33: NUMI Basic Settings....29
Figure 34: NUMI Advanced Settings....30
Figure 35: NUMI Bindings....31
Figure 36: NUMI Authentication Settings....31
Figure 37: NUMI SSL Settings....32
Figure 38: NUMI Compression Settings....33
Figure 39: Application Pool Window....34
Figure 40: NUMI Application Pool Basic Settings....35
Figure 41: NUMI Application Pool Advanced Settings....36

Figure 42: Security Warning 37
Figure 43: Preparing to install dialog 38
Figure 44: Web agent install wizard - Welcome screen 38
Figure 45: Web agent install wizard - License agreement screen 39
Figure 46: Web agent install wizard - Install location screen 39
Figure 47: Web agent install wizard - Review screen 40
Figure 48: Web agent install wizard - Agent configuration screen 40
Figure 49: Web agent install wizard - Install complete screen 41
Figure 50: Launch Web Agent Configuration Wizard 41
Figure 51: Web agent configuration wizard - Host registration 42
Figure 52: Web agent configuration wizard - Admin credentials 43
Figure 53: Web agent configuration wizard - Host name and configuration object 44
Figure 54: Web agent configuration wizard - Policy server IP Address 45
Figure 55: Web agent configuration wizard - FIPS mode setting 45
Figure 56: Web agent configuration wizard - Configuration file location 46
Figure 57: Web agent configuration wizard - Web server 46
Figure 58: Web agent configuration wizard - Agent configuration 47
Figure 59: Web agent configuration wizard - Sites selection 47
Figure 60: Web agent configuration wizard - Summary screen 48
Figure 61: Web agent configuration wizard - Completion screen 48
Figure 62: Web agent configuration wizard - Host registration 49
Figure 63: Web agent configuration wizard - Web server 49
Figure 64: Web agent configuration wizard - Agent configuration 50
Figure 65: Web agent configuration wizard - Sites selection 51
Figure 66: Web agent configuration wizard - Summary screen 51
Figure 67: Web agent configuration wizard - Previously configured sites 52
Figure 68: Web agent configuration wizard - Summary screen 53
Figure 69: Web agent configuration wizard - Completion screen 53
Figure 70: IIS Server Certificates 65
Figure 71: IIS Server Certificate Selection 66
Figure 72: IIS Certificate Details 66
Figure 73: keytool -keystore "C:\Certs\CERME.ks" –list 67
Figure 74: Creating a NUMI section in the Windows Event Log 69
Figure 75: Updating Settings in NUMI XML Configuration File 70

1. Introduction

This Server Setup Guide explains how to install National Utilization Management Integration (NUMI), Release 1.1.15.9.

1.1. Purpose

The purpose of this document is to explain the hardware and software requirements and tasks that must be performed before and after the installation process.

1.2. Scope

The scope of this document includes explanations of the appropriate steps to install the NUMI software, and the steps that are needed to be completed before and after the installation process is started.

1.3. Target Audience

This document is intended for the Information Technology Team and the individuals who install software in your organization.

2. Deployment Overview

The following process is followed to request permission to do a National Deployment.

2.1. National Deployment Request

The ProPath Release Management processes govern the request for a National Deployment. Refer to ProPath for guidance on requesting a release. This process must be complete before installation of services on the NUMI servers.

2.2. Installing NUMI on the Servers

The steps to install NUMI on the servers are described below. The middle tier of NUMI is the Veterans Information Systems Technology Architecture (VistA) Integration Adapter (VIA), which is a hosted service and is not part of the NUMI deployment. The primary NUMI application servers are located at the Austin Information Technology Center (AITC) facility in Austin, Texas. The application servers run on an Internet Information Services (IIS) Application Server. The NUMI application requires Microsoft (MS) ASP.NET 2.0 Ajax Extensions 1.0 and Web Services Enhancements 3.0 to enable the interactions with the Web Services.

2.2.1. Database Server

The NUMI database as it exists now is a manifestation of multiple changes over multiple releases. This installation document has as a pre-requisite the backup of an existing NUMI database. Therefore, to install a new NUMI database, it is necessary to restore a backup of an existing NUMI database.

Database Platform installation, and Database Restoration Procedures

1. Install Windows Server 2012 on the database server platform
2. Download and install any critical patches for the Operating System

3. Install the 64-bit MS Structured Query Language (SQL) Server 2012 application according to local "best practices"
   a. MS's Full Text Search is required for the NUMI installation
   b. Replication is necessary for the NUMI installation to use the alternate database reporting capability of NUMI
   c. Reporting Services is not necessary for installation on the NUMI database server
   d. NUMI's database will function properly in cluster, but clustering is not required for the NUMI application
4. Apply all appropriate patches (according to local best practices) to MS SQL Server 2012
5. Install / restore the database components according to the instructions in section 4.1 Instructions for Installing Database Components.

2.2.2. Web Server

To install NUMI Exchange software on the Web Server (Server 2):

1. Install Windows Server 2012 on the web server platform
2. Download and install any critical patches for the Operating System on all web servers
3. Install MS ASP.NET 2.0 Ajax Extensions 1.0
4. Install Web Services Enhancements 3.0
5. Install NUMI Exchange
6. Change the web.config file settings as needed

2.2.3. Application Server

To install NUMI application software on the Application Server (Server 3)

1. Install Windows Server 2012 on the application server platform
2. Download and install any critical patches for the Operating System on all application servers
3. Install the Care Enhance Review Management Enterprise (CERMe) 19.0 InterQual View 2020 application
4. Install the NUMI application
5. Change the web.config file settings as needed
6. Install the SiteMinder Web Agent and configure it for the NUMI application Web site

3. Pre-Installation Instructions and Preparation

The Pre-Installation Instructions and Preparation section explains the tasks that need to be performed before installing NUMI software. Before proceeding with the installation procedures, consult the list of requirements below.

3.1. Installation Process Requirements

An assumption is made that the person responsible for doing installations at your site has performed appropriate pre-installation planning.

3.1.1. Minimum Software Version

Operating System: Windows Server 2012 R2

Database: SQL Server 2012

3.1.2. Resources Required

Sys Admin, DBA

3.1.3. CPU Capacity

64GB RAM, 2.8ghz Xeon – Database Server

16GB RAM, 2.8 ghz Xeon – Application Server

8GB RAM, 2.8 ghz Xeon – Web Server

3.1.4. Disk Space

SAN – 900 gigabyte Application server – 100 GB Web Services server – 100 GB

Database – 800 GB (This includes space needed for the backups and data storage.)

3.1.5. Devices (Servers, etc.)

1 Database Server

2 Application Servers

2 Web Servers

1 Data Warehouse Server 1 SQL Reporting Server

3.1.6. VistA Rights Needed for NUMI Users

Each NUMI user must have Computerized Patient Record System (CPRS) access in their VistA menu structure, such as in their secondary menu tree. The VistA menu name is CPRSChart (or CPRS Graphical User Interface CHART). Table 1 and Table 2 identify the menus, options and settings these user accounts will need to have assigned.

It is also highly recommended that the VIAB WEB SERVICES OPTION be added to the System Command Options [XUCOMMAND] menu in each site's VistA system. If you do not add this to the Common Menu, you will need to add it to the secondary menu of each individual NUMI user.

Table 1: CPRS Rights

CPRS Rights
Primary Menu: XMUSER
Primary Menu: MailMan Menu
Secondary Menu: [OR CPRS GUI CHART]
Secondary Menu: CPRSChart Release 1.0.30.72
Keys Held
Patient Selection
Restrict? NO
OE/RR List

Table 2: CPRS Access Tabs

Name	Description	Effective Date	Expiration Date
RPT	Reports tab	Sept. 2, 2008	N/A

3.2. Install Software in Test Environments

The software will be installed in the Test environments before installing in Production.

3.3. Generate Pre-Installation Reports

Not applicable.

3.4. Coordinate Installation with Other Teams

The Installation Team will need to involve the Implementation/Architecture Team.

3.5. Install Sequence Information for Multiple Patches

Not applicable.

3.6. Logoff During Installation

End users do not need to be logged off during installation (during the act of copying files and installation executions to the server(s)). However, the users must be logged off for any updates to the software (running the executions and/or configuring the software and configuration files).

Logging off during software updates is no different from any other logoff that a user may do.

3.7. Average Amount of Time Required to Complete the Installation

The average amount of time required to complete the NUMI installation is 2 days.

4. Database Information

Refer to the NUMI Systems Management Guide for information about the structure and components of the NUMI database.

4.1. Instructions for Installing Database Components

The NUMI database as it exists now is a manifestation of multiple changes over multiple releases. This installation document has as a pre-requisite the backup of an existing NUMI database. Therefore, to install a new NUMI database, it is necessary to restore a backup of an existing NUMI database.

4.1.1. Database Installation / Restoration Procedures

1. Copy a backup of an existing NUMI database(s) of appropriate size and content to the new NUMI database server
   a. The application database (typically called NUMI) is necessary for proper function of the application
   b. The "auditing" database (typically called LogSyncDb) is necessary for proper functioning of the application and the synchronizer
   c. The CERMe database can be restored from an existing backup, or can be built from scratch from the CERMe installation media
      i. If the CERMe database is restored from an existing backup, verify that the application configuration files reference a database authenticated user that has DBO privilege on the CERMe database for proper functioning of the NUMI application
      ii. If the CERMe database is installed from media, follow the instructions provided by Change Healthcare for installation
   2. Restore the database backup to the existing server
   a. File paths will have to be altered according to local best practices
   b. User accounts may be, but are not required to be, restored with the database. NUMI requires the numi_user account to be setup.
   c. Database ownership may be altered so that the owning account for the NUMIdatabase complies with local best practices
   d. A database authenticated user for the application should be configured, and granted DBO privileges on the NUMI database
   3. Run the Install_XX.sql if it was provided with the build, where XX is the database version for the NUMI build. This will apply changes to the database necessary for the version of NUMI that is being installed
   4. Install the NUMI Synchronizer according to the instructions in section 17 Installing NUMI Synchronizer on the DB Server

5. Installation Procedure for Server 2012 R2

This section identifies the installation procedures that shall be followed.

5.1. Patch the Operating System

This applies to all servers.

1. Open up an instance of Internet Explorer.

2. Select menu item <Tools/Windows Update>.
3. Follow the instructions on MS's website. (**NOTE:** A restart of the servers may be necessary).

6. SQL Server Setup (Windows Server 2012 R2)

6.1. Role Setup

The role set-up in this section applies to the SQL database server. Use Server Manager to install the File Services with the role services shown in Figure 1: SQL Server Role Services.

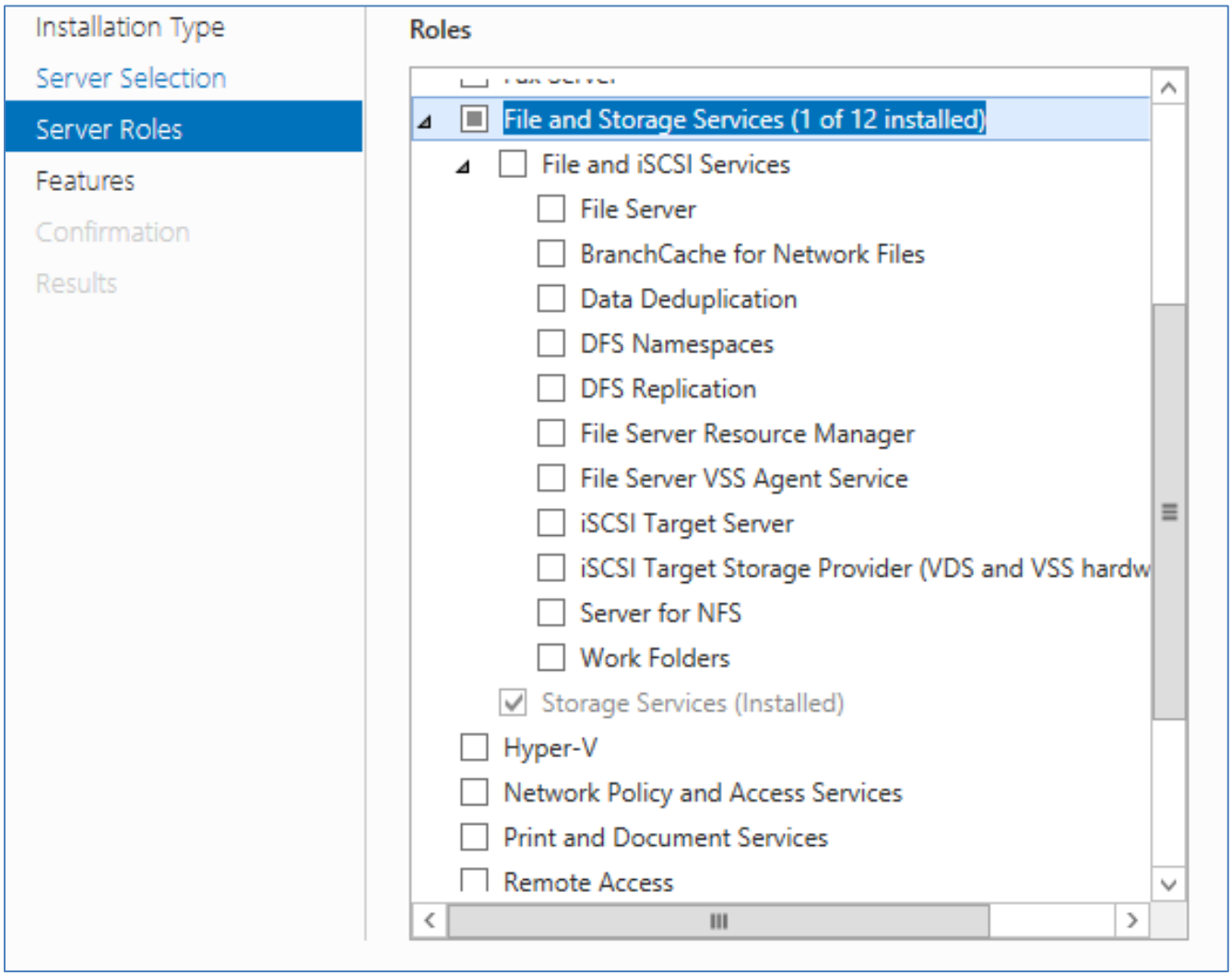


Figure 1: SQL Server Role Services

7. Web Server Setup (Windows Server 2012 R2)

7.1. Role Setup

The role setup in this section applies to the NUMI Exchange web server.

Use Server Manager to install the File Services and Web Server (IIS) roles with the role services shown in Figure 2: NUMI Exchange Role Services and Figure 3: NUMI Exchange (IIS).

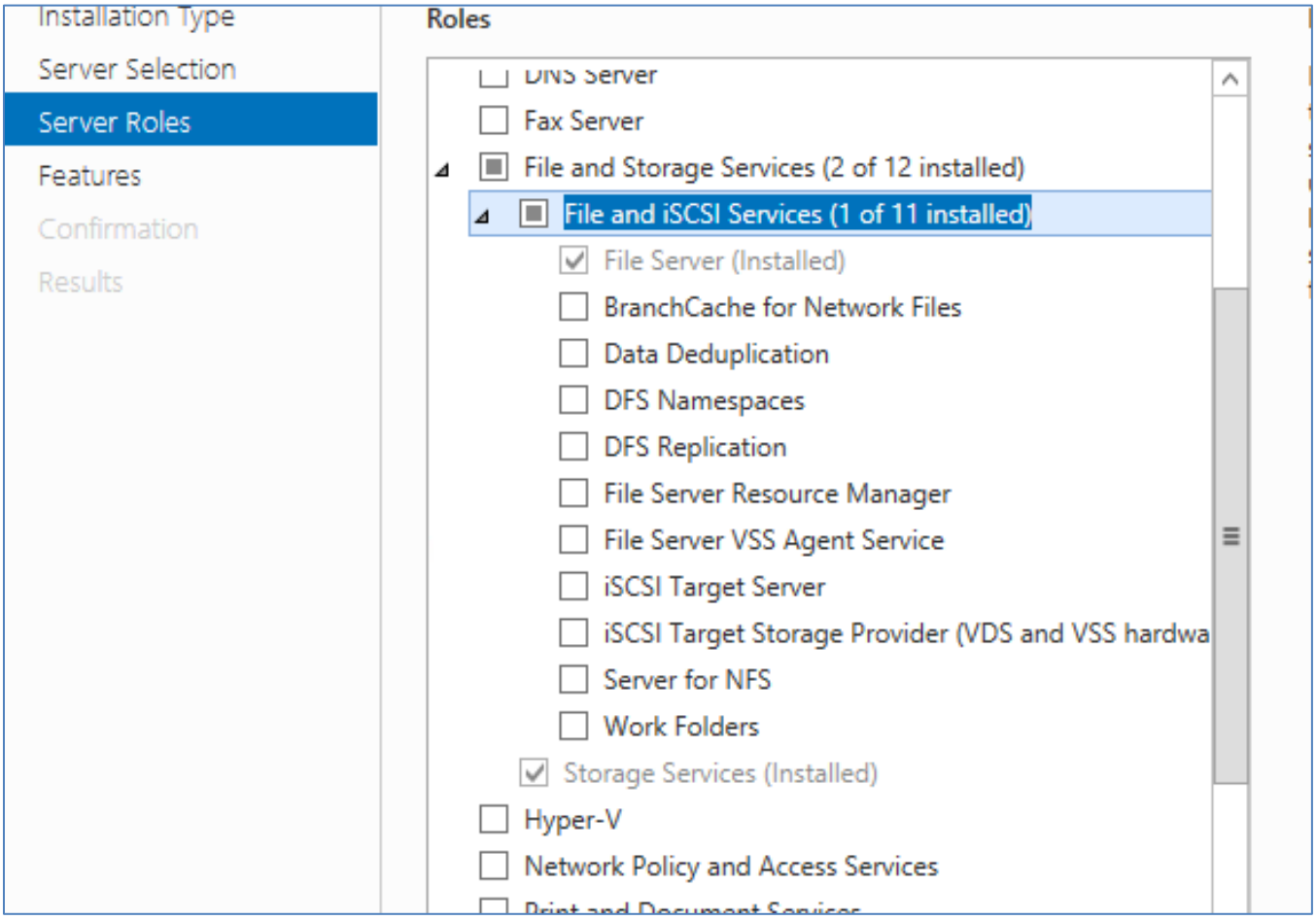


Figure 2: NUMI Exchange Role Services

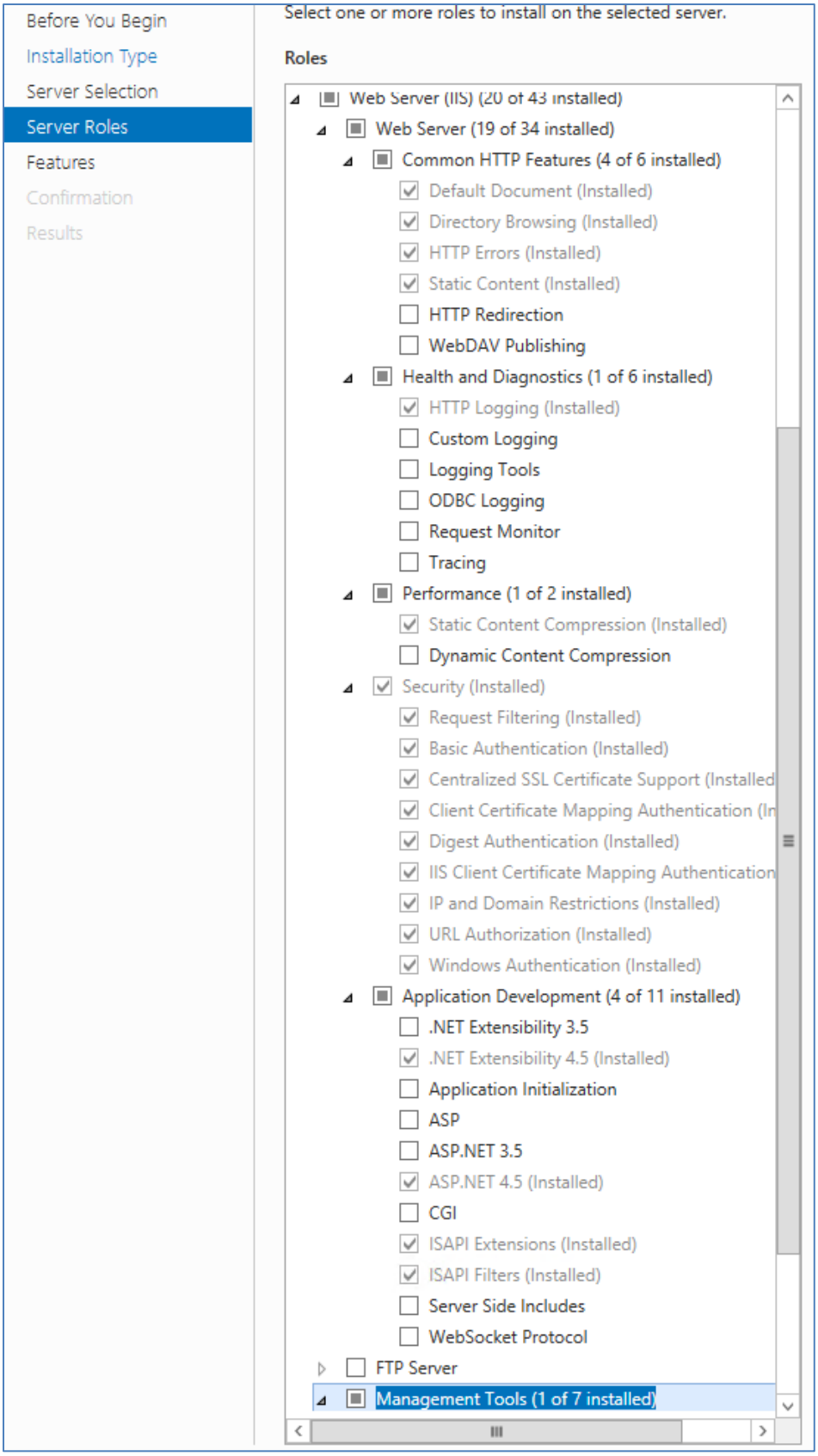


Figure 3: NUMI Exchange (IIS)

7.2. ASP.NET 2.0 AJAX Extensions 1.0 Setup

Install the ASP.NET 2.0 Ajax Extensions 1.0 as detailed in section 8.3, Install MS ASP.NET 2.0 Ajax Extensions 1.0.

7.3. MS Web Services Enhancements (WSE) 3.0 Setup

Install MS WSE 3.0 as detailed in section 8.4 Install MS Web Services Enhancements 3.0.

8. Application Server Setup (Windows Server 2012 R2)

8.1. Role Setup

The role setup in this section applies to the NUMI app servers. Use Server Manager to install the File Services and Web Server (IIS) roles with the role services shown in Figure 4: NUMI Role Services and Figure 5: NUMI Web Services IIS.

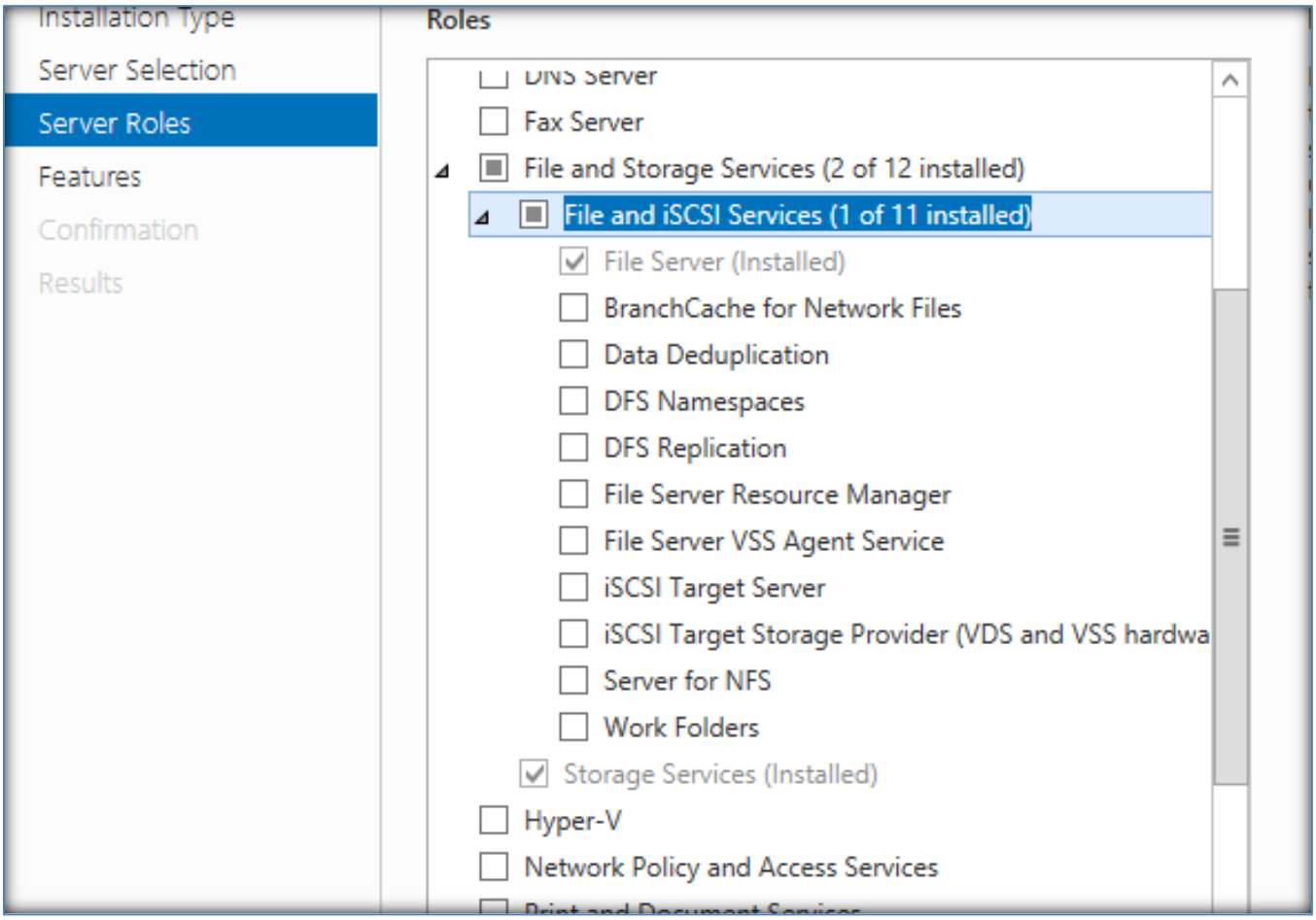


Figure 4: NUMI Role Services

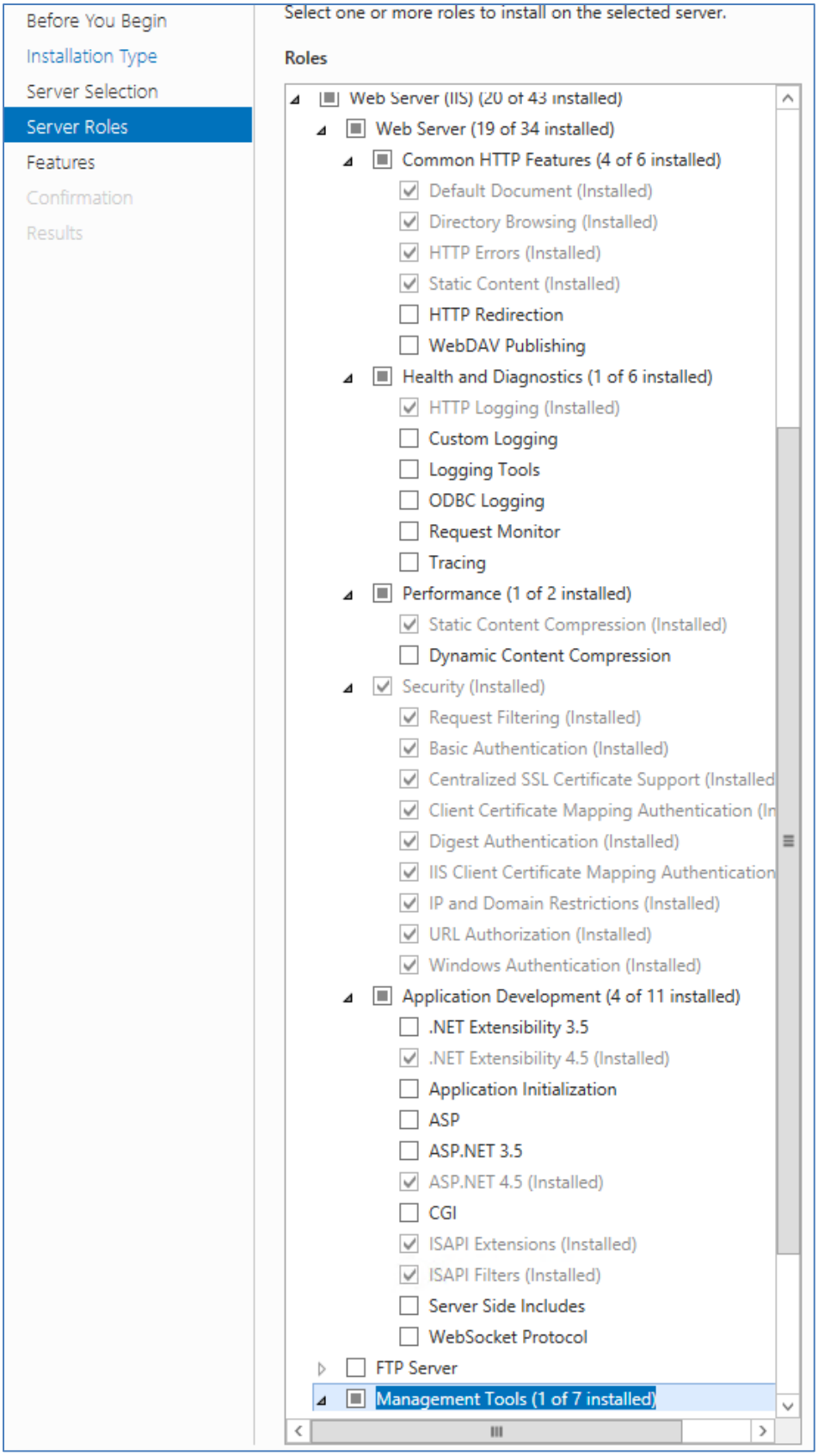


Figure 5: NUMI Web Services IIS

8.2. Feature Delegation

Select the main node in IIS, with the server name. Then double click on “Feature Delegation” item. Change the “Feature Delegation” settings for the server, as shown in Figure 6: IIS Feature Delegation.

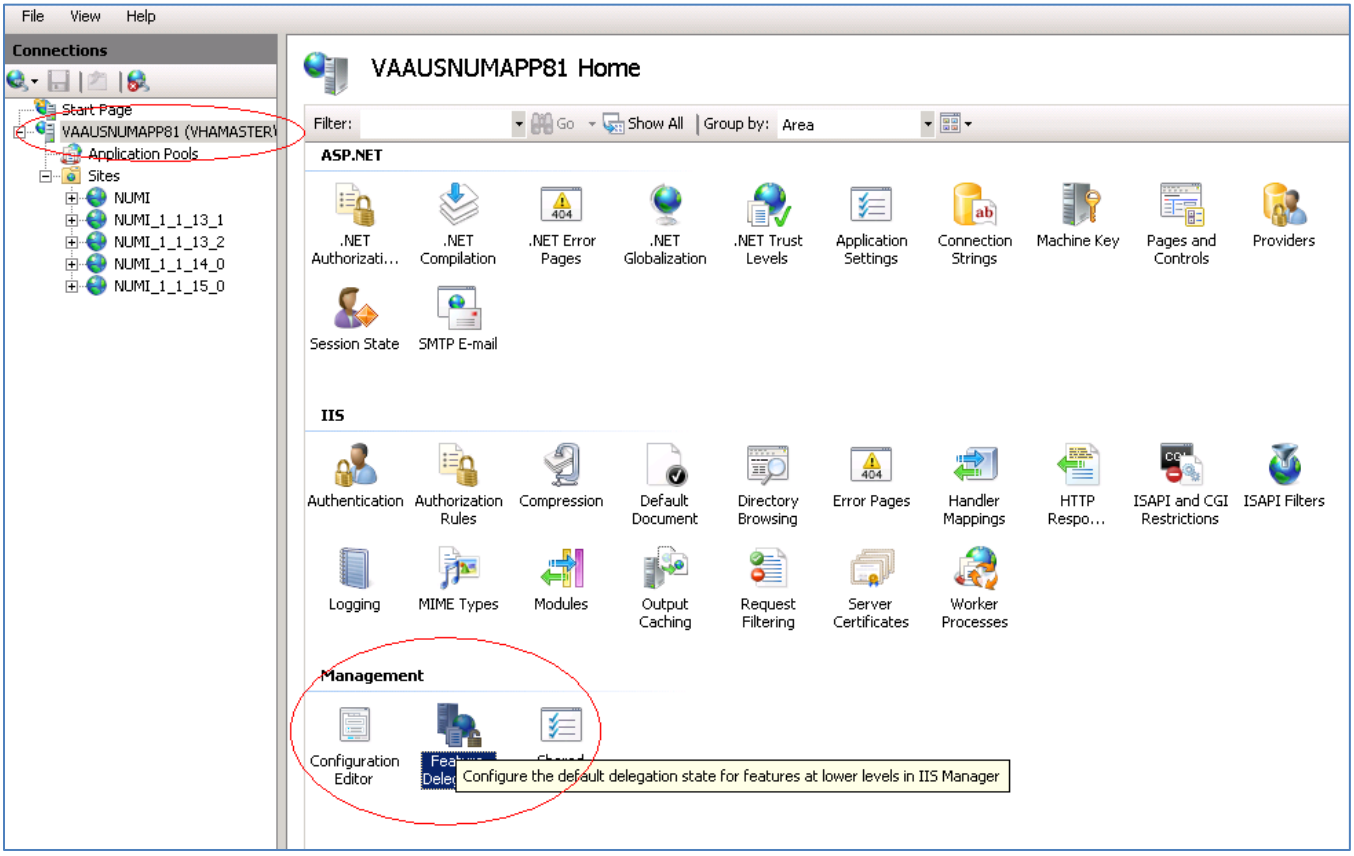


Figure 6: IIS Feature Delegation

Make sure all authentication rules are set to Read/Write as shown in Figure 7: Feature Delegation Selection.

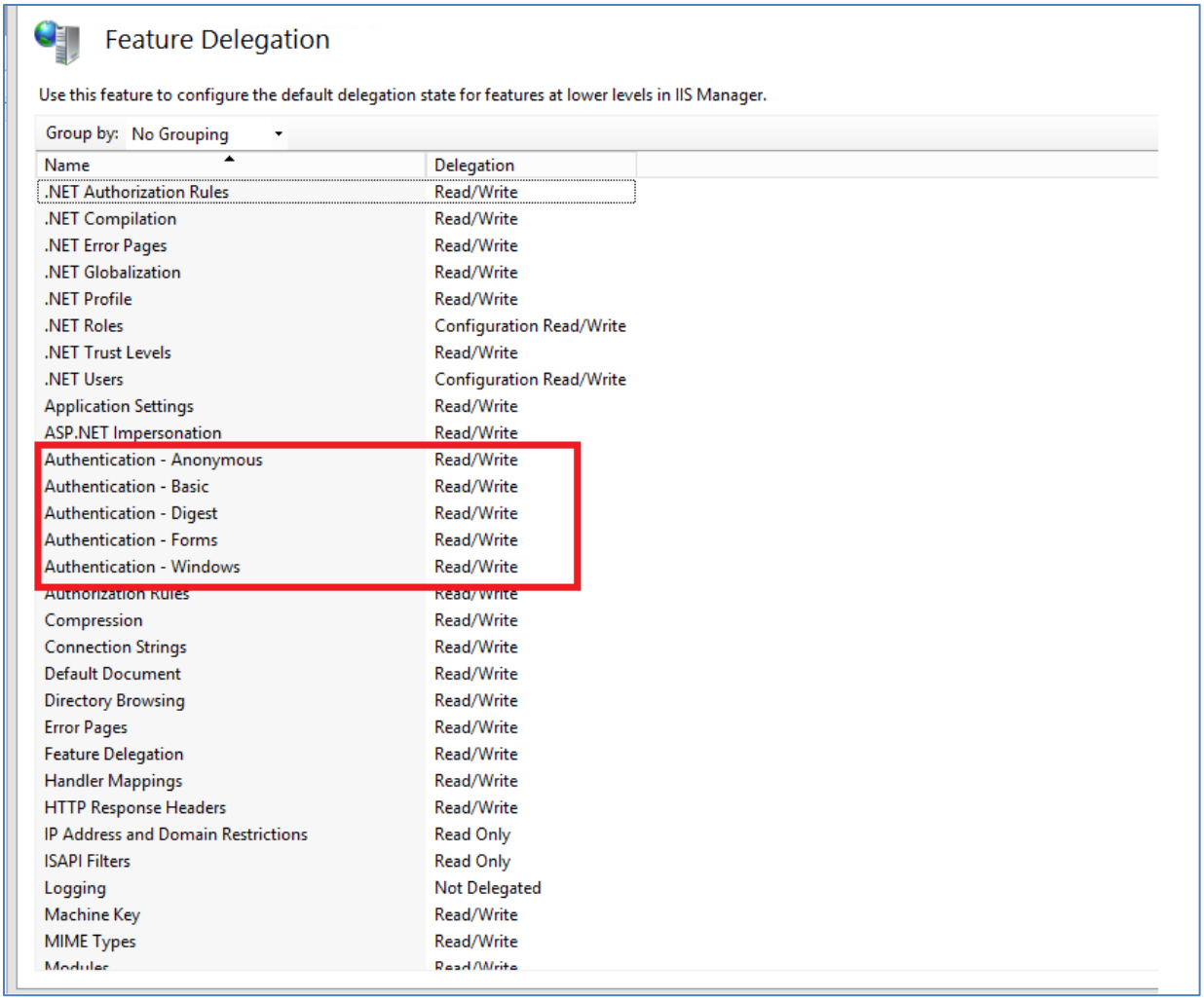


Figure 7: Feature Delegation Selection

8.3. Install MS ASP.Net 2.0 AJAX Extensions 1.0

Installing MS ASP.NET 2.0 Ajax Extensions 1.0 applies to the web servers only.

1. Download the MS ASP.NET 2.0 Ajax Extensions 1.0 from MS's website.
    2. Run the ASPAJAXExtSetup.msi by double-clicking it.
    3. When the File Download – Security Warning window displays, click the <Run> button (shown in Figure 8: MS ASP.Net 2.0 File Download-Security Warning Window).

Figure 8: MS ASP.Net 2.0 File Download-Security Warning Window

4. When the Internet Explorer – Security Warning window displays, click the <Run> button (shown in Figure 9: MS ASP.Net 2.0 Internet Explorer-Security Warning Window).

Figure 9: MS ASP.Net 2.0 Internet Explorer-Security Warning Window

5. When the MS ASP.NET 2.0 AJAX Extensions 1.0 Setup window displays, click the <Next> button (shown in Figure 10: MS ASP.NET 2.0 AJAX Extensions 1.0 Setup Wizard Window).

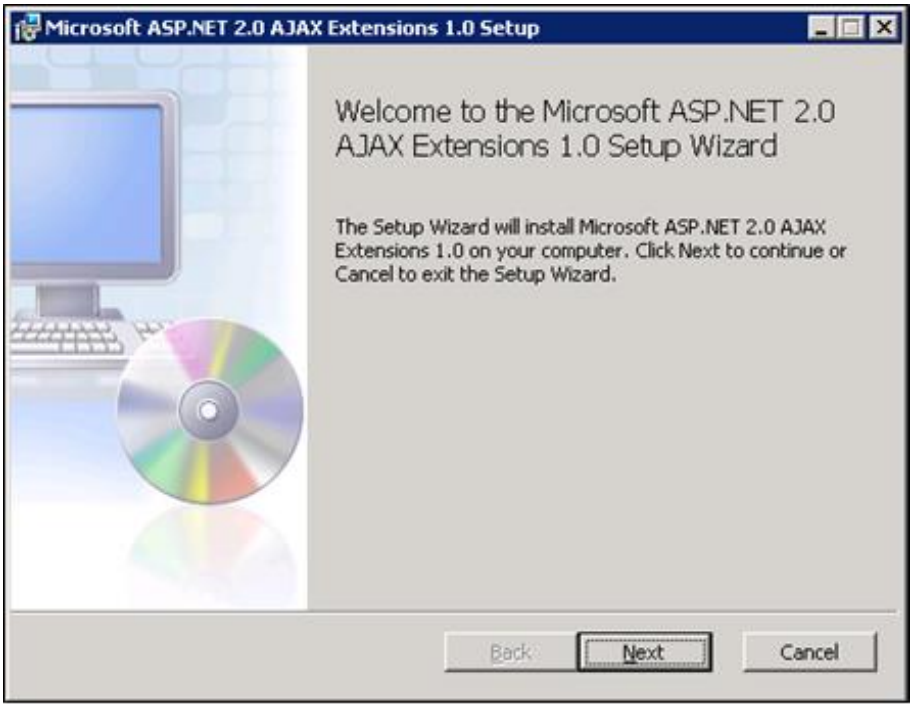


Figure 10: MS ASP.NET 2.0 AJAX Extensions 1.0 Setup Wizard Window

Click the "I accept the terms in the License Agreement" checkbox, as illustrated in Figure 11: MS ASP.NET 2.0 AJAX License Agreement Window.

1. Click the <Next> button.

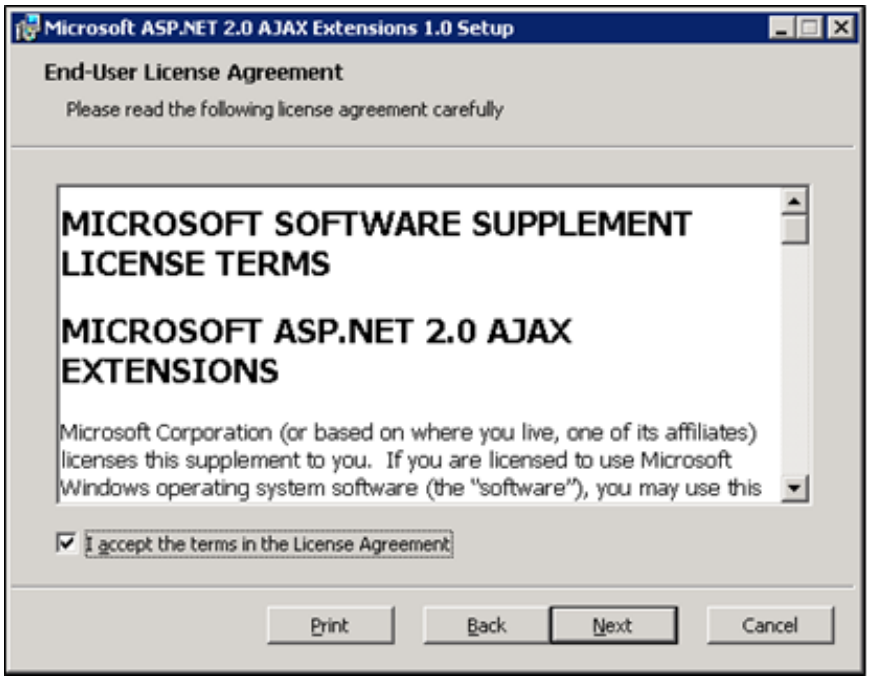


Figure 11: MS ASP.NET 2.0 AJAX License Agreement Window

2. Click the <Install> button (shown in Figure 12: MS ASP.NET 2.0 AJAX Installation Window).

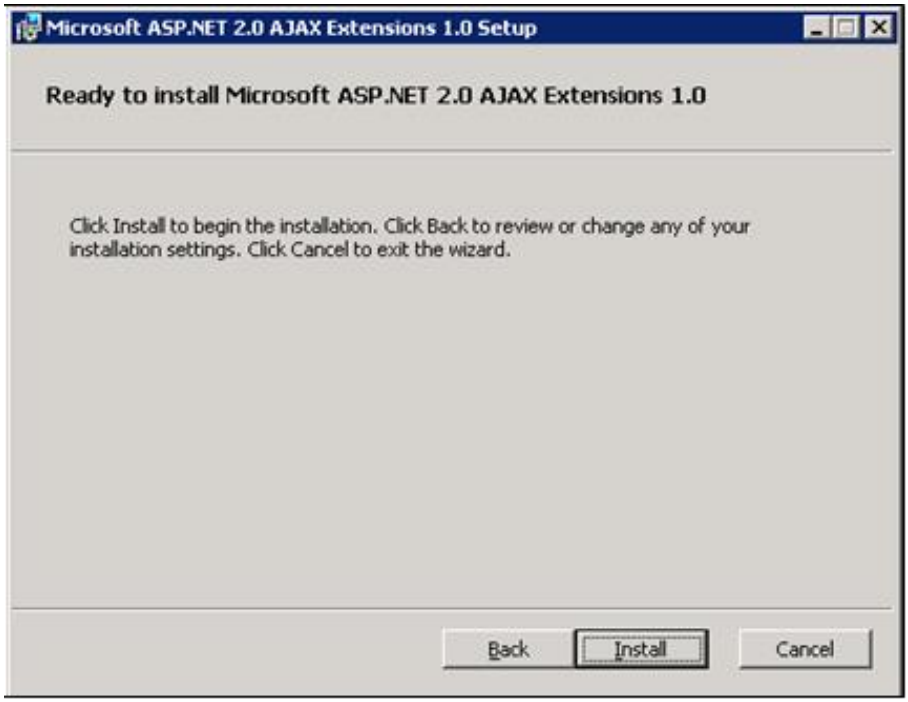


Figure 12: MS ASP.NET 2.0 AJAX Installation Window

3. The installation is complete. Select the <Finish> button by clicking on it to exit the installation wizard, as depicted in Figure 13: MS ASP.NET 2.0 AJAX Completion window.

If you do not wish to view the release notes, un-check the “Display MS ASP.NET 2.0 AJAX Extensions 1.0 Release Notes” checkbox.

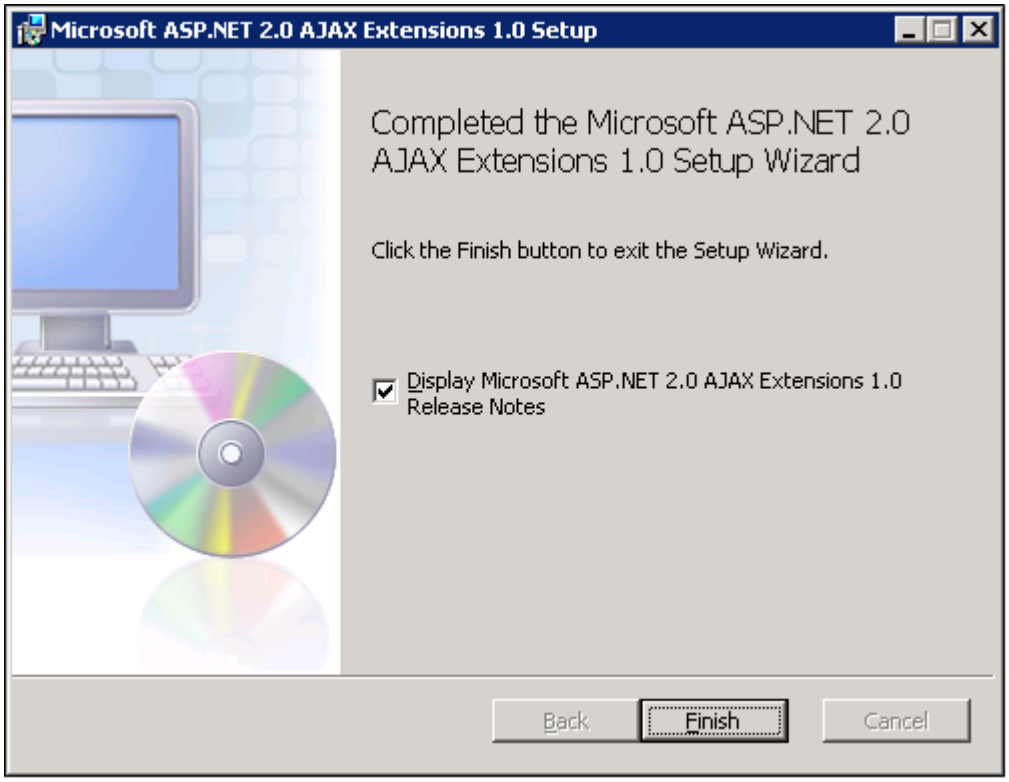


Figure 13: MS ASP.NET 2.0 AJAX Completion window

8.4. Install MS Web Services Enhancements 3.0

Installing MS Web Services Enhancements 3.0 applies to the web servers only.

1. Download the MS Web Services Enhancements 3.0 from MS's website.
    2. Run the MS WSE 3.0.msi by double-clicking it.
    3. When the File Download – Security Warning window displays, click the <Run> button (shown in Figure 14: MS WSE 3.0 File Download-Security Warning Window).

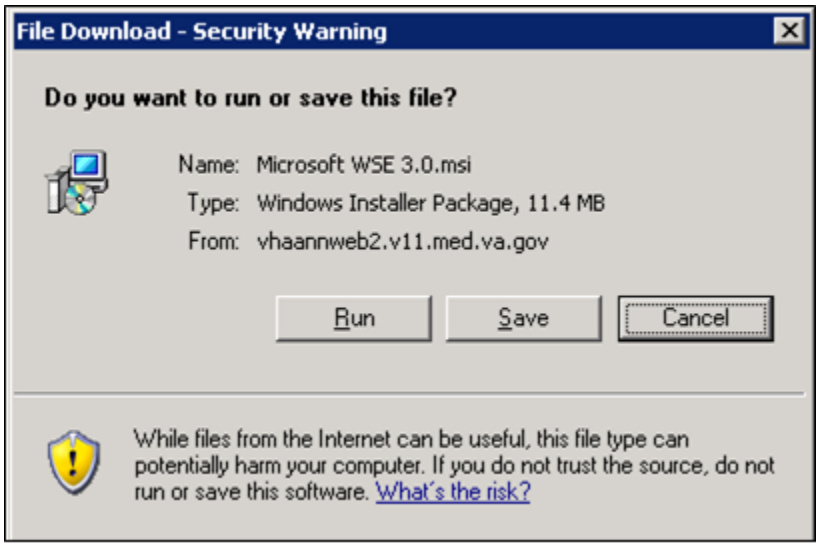


Figure 14: MS WSE 3.0 File Download-Security Warning Window

4. When the Internet Explorer – Security Warning window displays, click the <Run> button (shown in Figure 15: MS WSE 3.0 Internet Explorer-Security Warning Window).

Figure 15: MS WSE 3.0 Internet Explorer-Security Warning Window

5. When the MS WSE 3.0 – InstallShield Wizard window displays, click the <Next> button (shown in Figure 16: MS WSE 3.0 InstallShield Wizard Welcome Window).

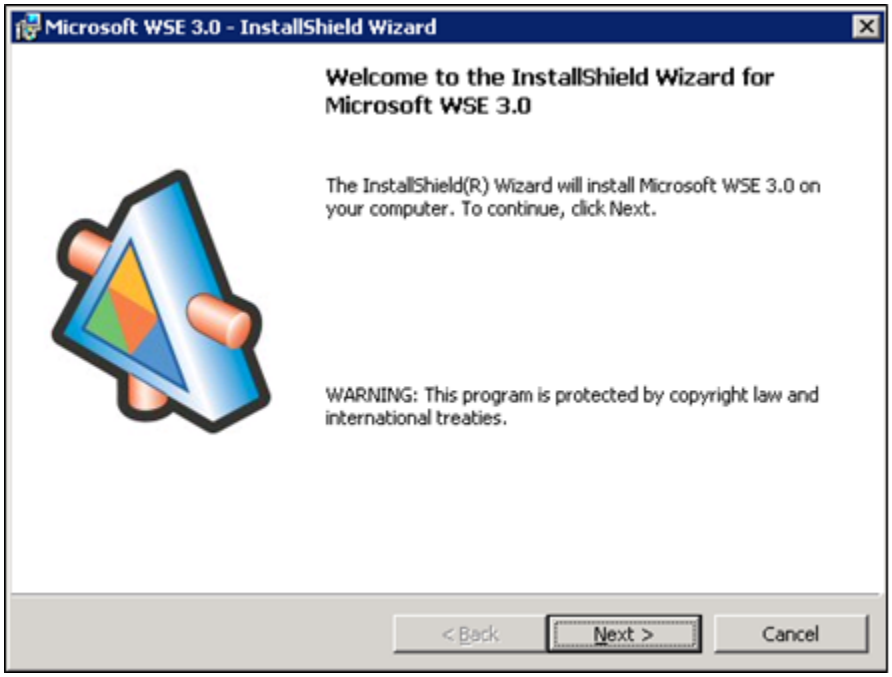


Figure 16: MS WSE 3.0 InstallShield Wizard Welcome Window

6. Click the "I accept the terms in the license agreement" checkbox, as illustrated in Figure 17: MS WSE 3.0 License Agreement Window.
7. Click the <Next> button.

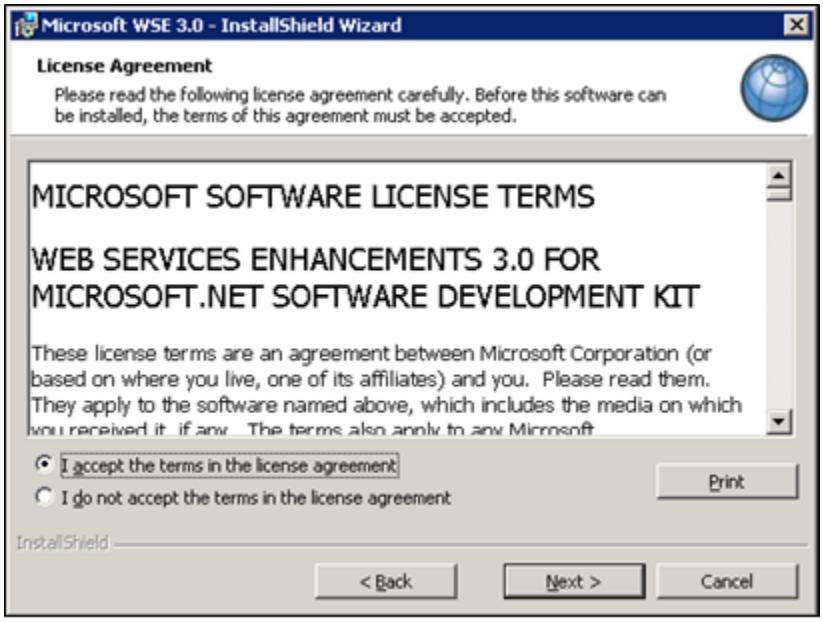


Figure 17: MS WSE 3.0 License Agreement Window

8. Click the <Administrator> radio button, as illustrated in Figure 18: MS WSE 3.0 InstallShield Wizard Window.
   9. Click the <Next> button.

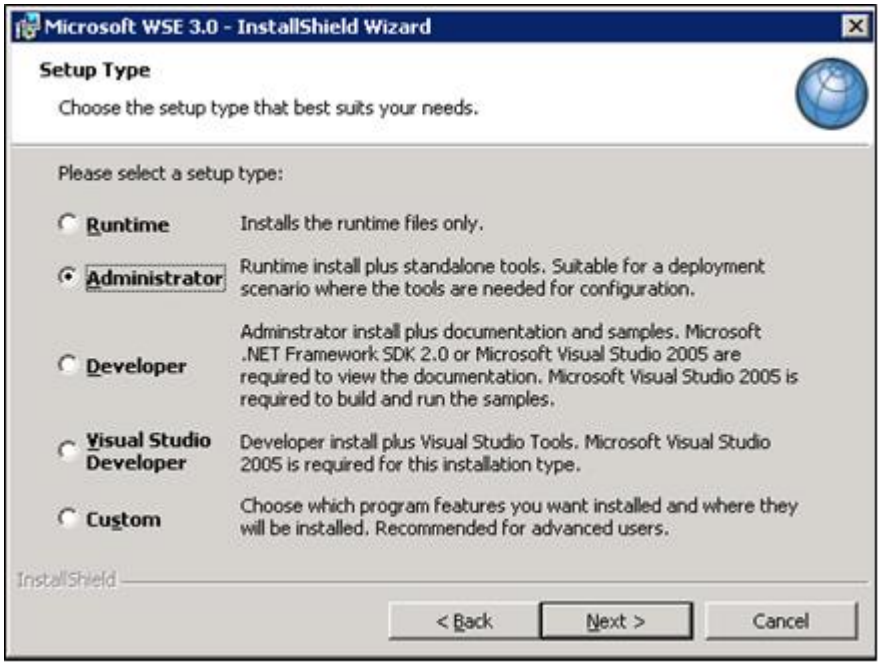


Figure 18: MS WSE 3.0 InstallShield Wizard Window

10. Click the <Install> button (shown in Figure 19: MS WSE 3.0 Installation Window).

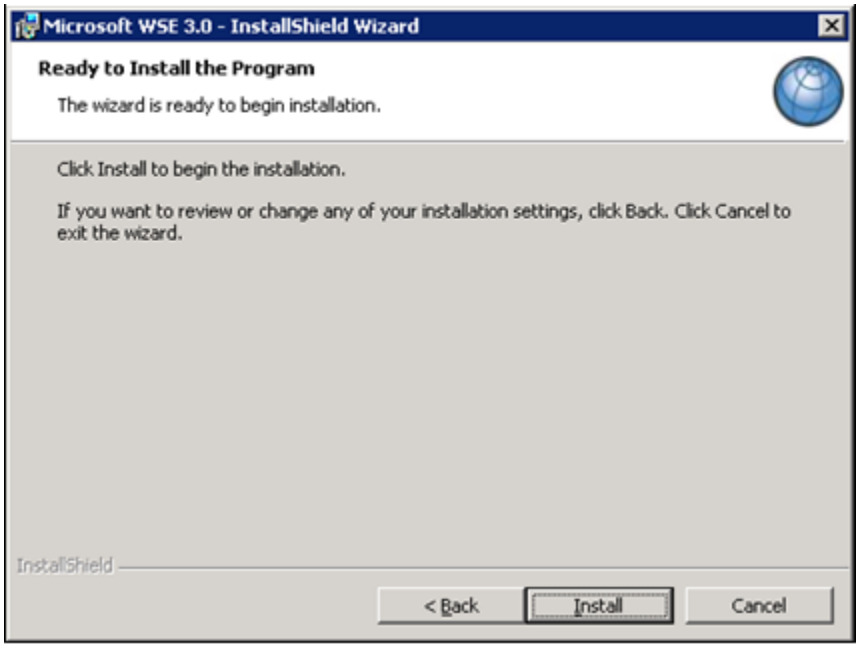


Figure 19: MS WSE 3.0 Installation Window

11. Click the <Finish> button (shown in Figure 20: MS WSE 3.0 Completion Window).

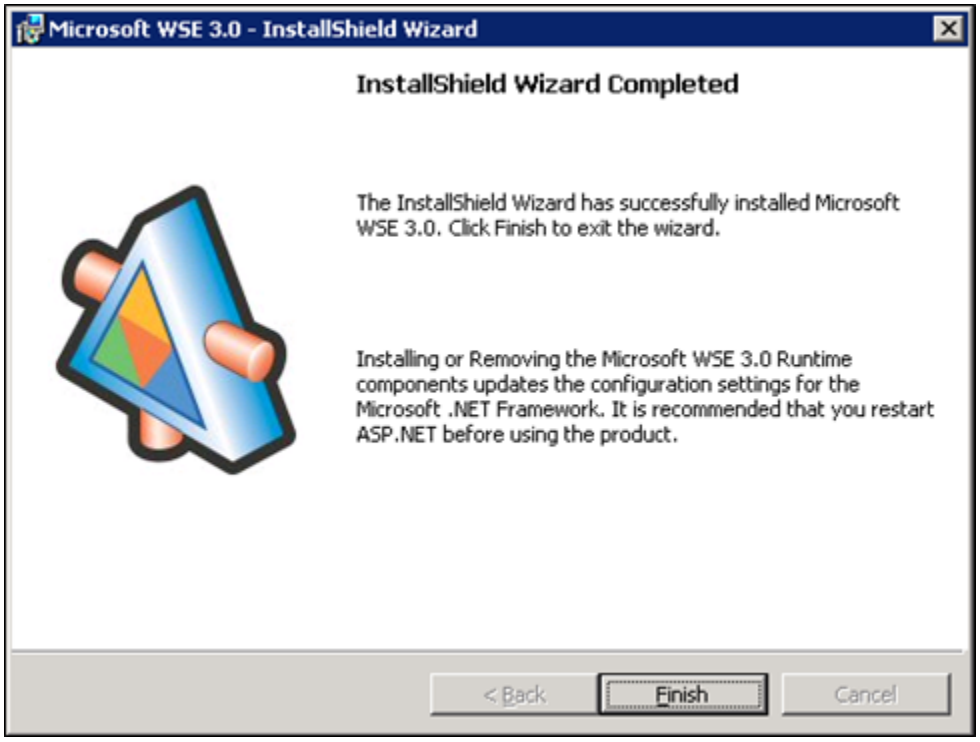


Figure 20: MS WSE 3.0 Completion Window

9. Install SQL Server

Install the MS SQL Server 2012 Database Server software only on the database server, applying both MS installation instructions and local best practices.

Additional service packs or patches may be installed subsequent to application testing, and in accordance with local best practices.

All production NUMI databases should be run in Simple Recovery mode, to enable replication to function, and to maximize the recoverability of the databases. In non-production environments, any recovery mode is acceptable, and simple recovery mode is encouraged for development and QA testing environments due to ease of administration.

9.1. Download all SQL Server Patches

Downloading all SQL Server Patches applies to the database server only.

9.2. Restore the Appropriate Databases for the NUMI Application

Restoring the Appropriate Databases for the NUMI Application applies to the database server only.

Follow the instructions in section 4 Instructions for Installing Database Components.

10. Installing NUMI Exchange on Server 2012 R2

Before doing this, you must make a backup copy of the web.config file (if this is an upgrade). Settings may need to be extracted from this in the future.

10.1. Unzip/Install NUMI Exchange Distribution

1. Using Windows Explorer, create the NumiExchange folder on the D drive, if available; otherwise create on the C drive. E.g., D:\NumiExchange
2. Unzip the NUMI Exchange files into the NumiExchange folder created above.
3. Update the application settings in the NUMI Exchange web.config file, located in the directory created above. Typically, this would involve updating the database connection string.

10.2. NUMI Exchange Website Configuration

Using IIS Manager, add a new website and select the Secure Socket Layer (SSL) certificate as shown in Figure 21: Add NUMI Exchange Website.

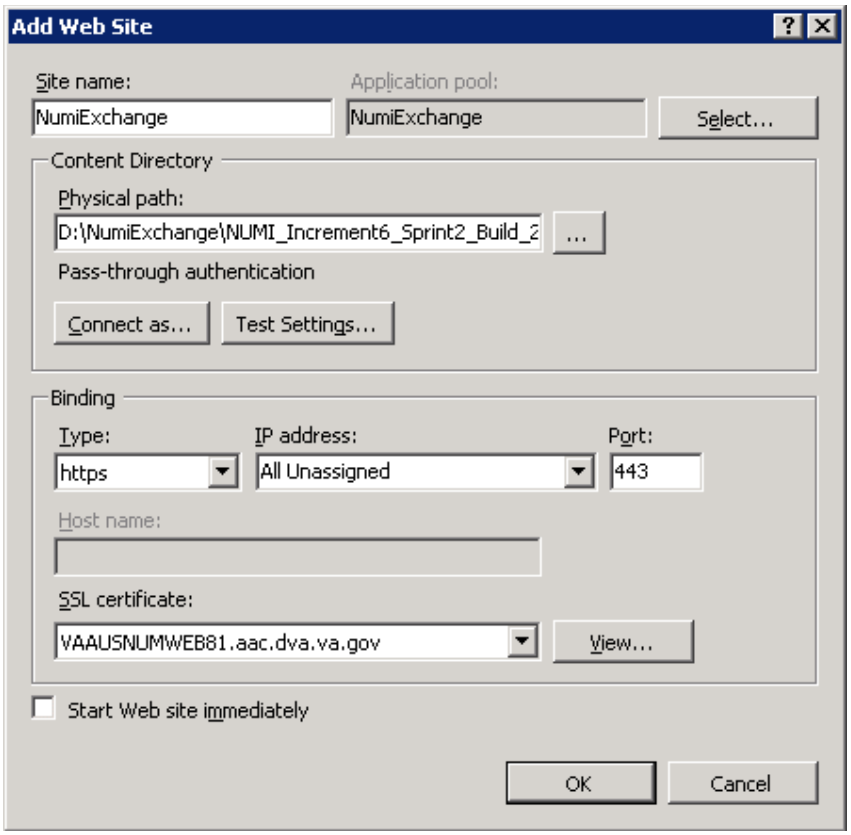


Figure 21: Add NUMI Exchange Website

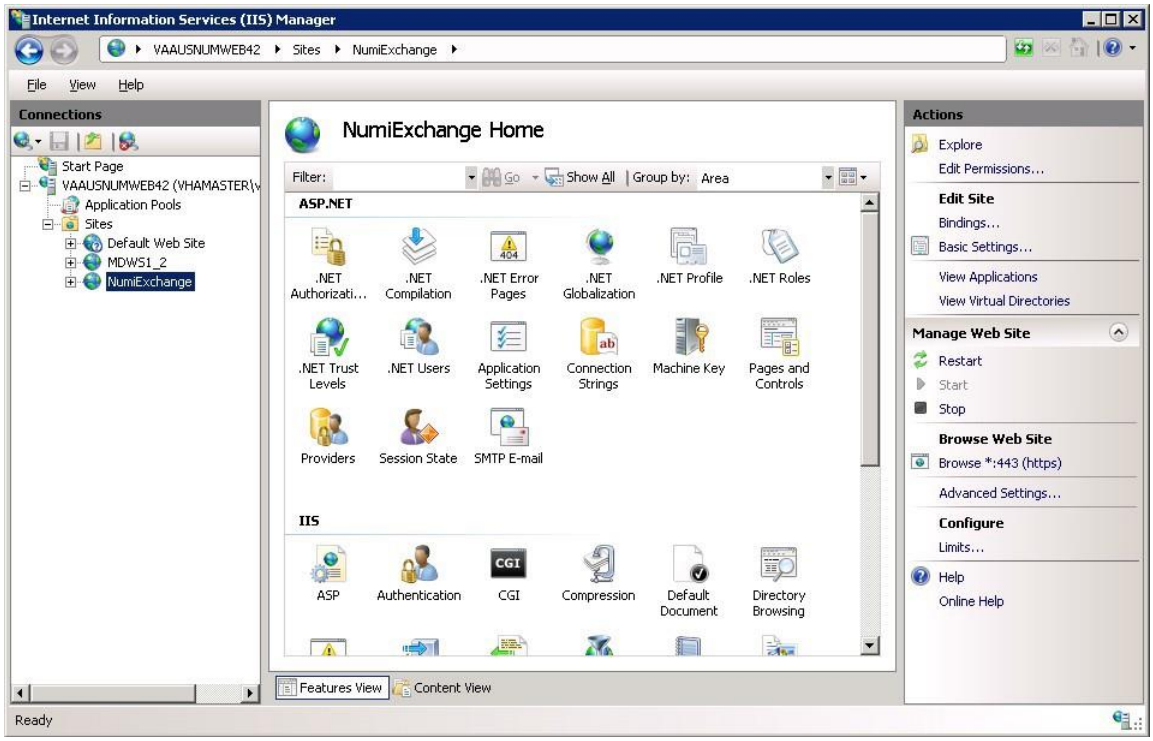


Figure 22: NUMI Exchange Website

The NUMI website basic and advanced settings are shown in Figure 23: NUMI Exchange Basic Settings and Figure 24: NUMI Advanced Settings.

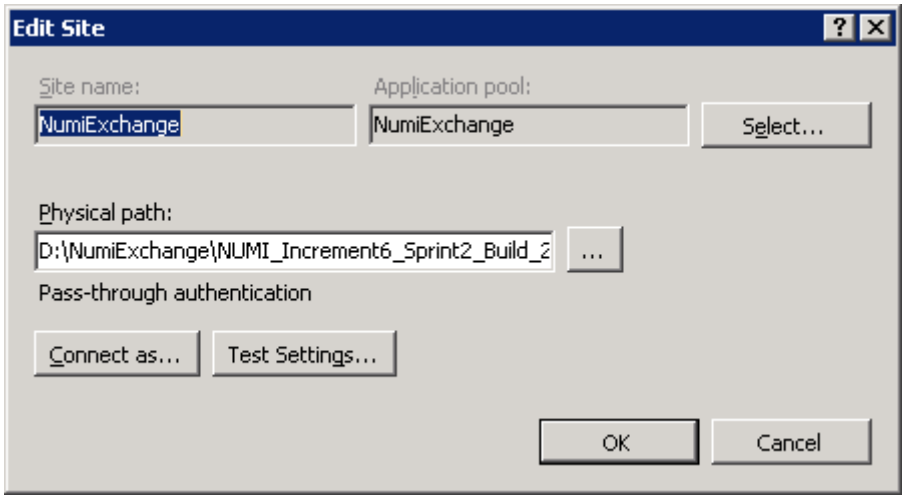


Figure 23: NUMI Exchange Basic Settings

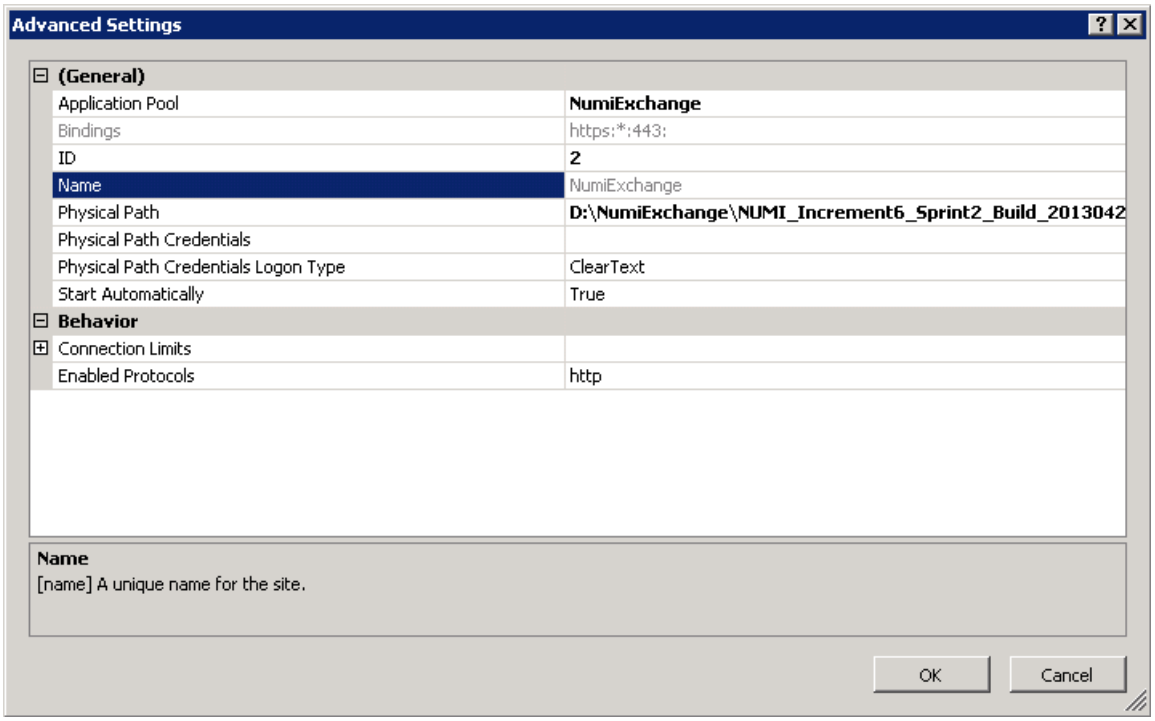


Figure 24: NUMI Advanced Settings

The NUMI Exchange web site bindings are shown in Figure 25: NUMI Exchange Bindings.

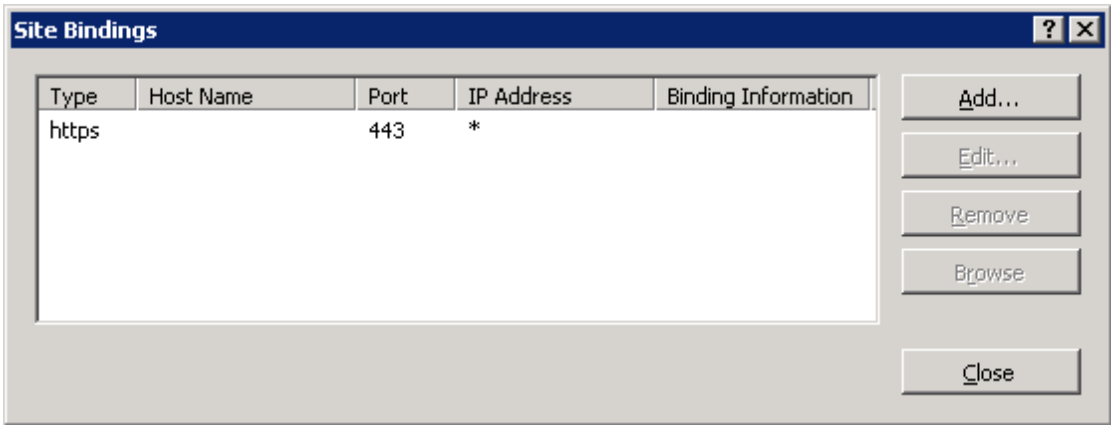


Figure 25: NUMI Exchange Bindings

The NUMI Exchange web site authentication settings are shown in Figure 26: NUMI Exchange Authentication Settings.

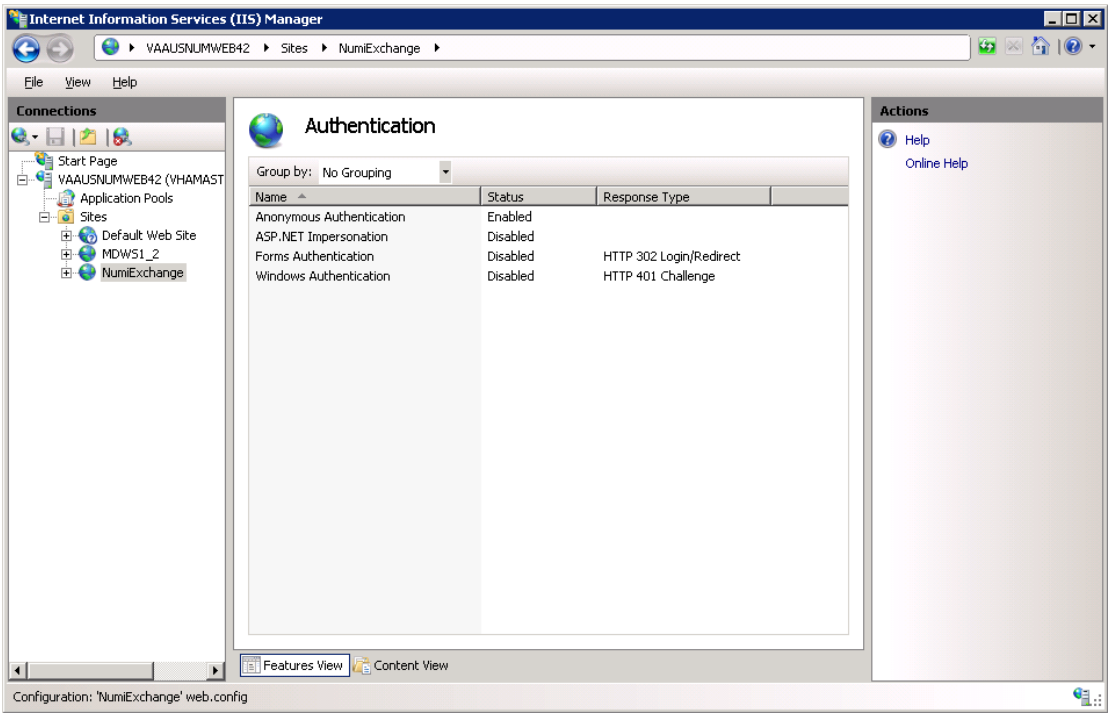


Figure 26: NUMI Exchange Authentication Settings

The NUMI Exchange website SSL settings are shown in Figure 27: NUMI Exchange SSL Settings.

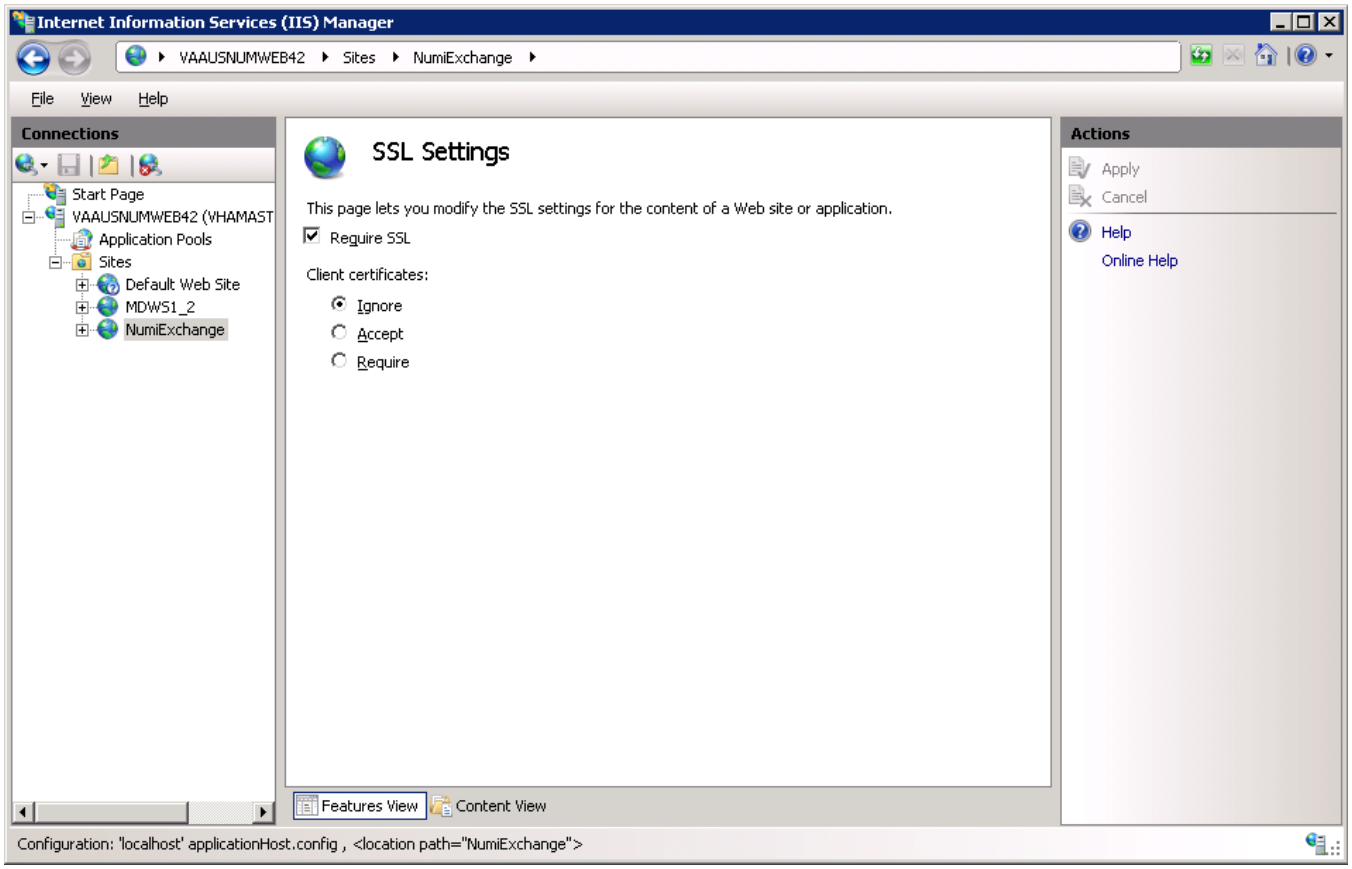


Figure 27: NUMI Exchange SSL Settings

10.2.1. Application Pool Configuration

The NUMI Exchange application pool setup is shown in Figure 28: Application Pool Window.

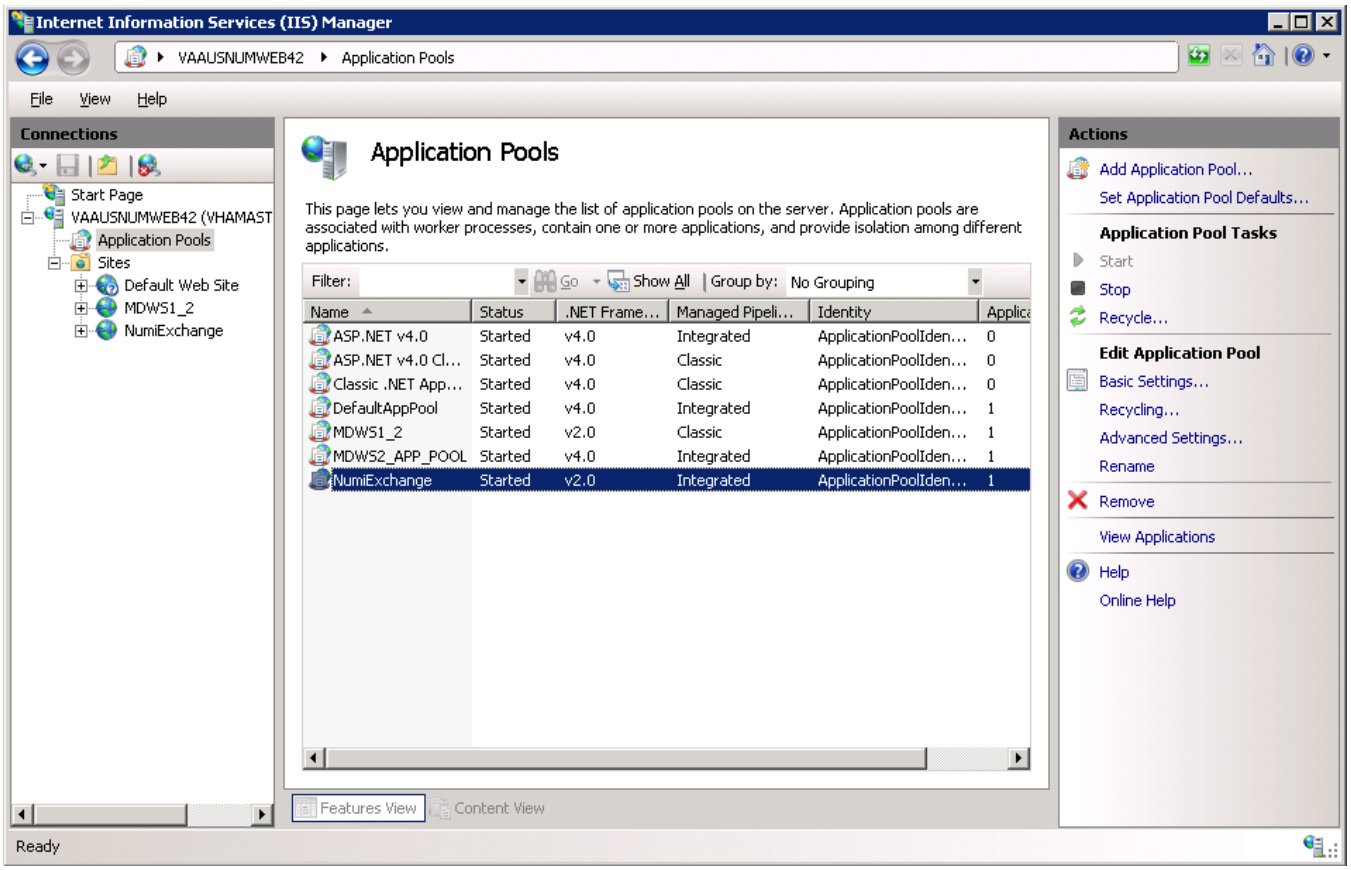


Figure 28: Application Pool Window

The NUMI Exchange application pool basic settings are shown in Figure 29: NUMI Exchange Application Pool Basic Settings.

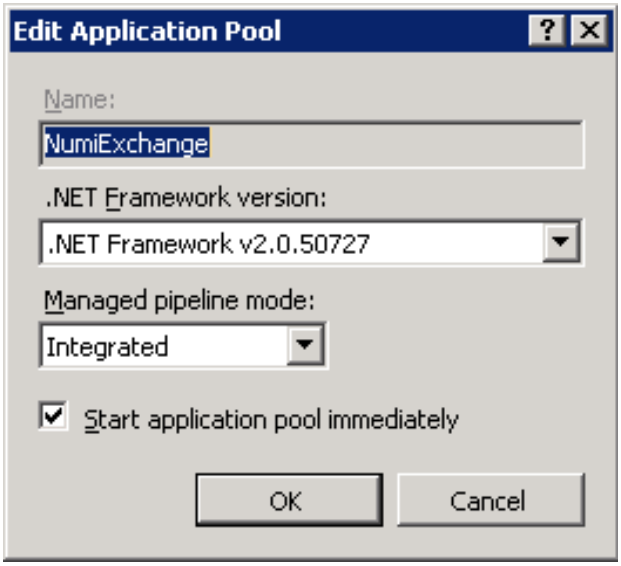


Figure 29: NUMI Exchange Application Pool Basic Settings

The NUMI Exchange application pool advanced settings are shown in Figure 30: NUMI Exchange Pool Advanced Settings.

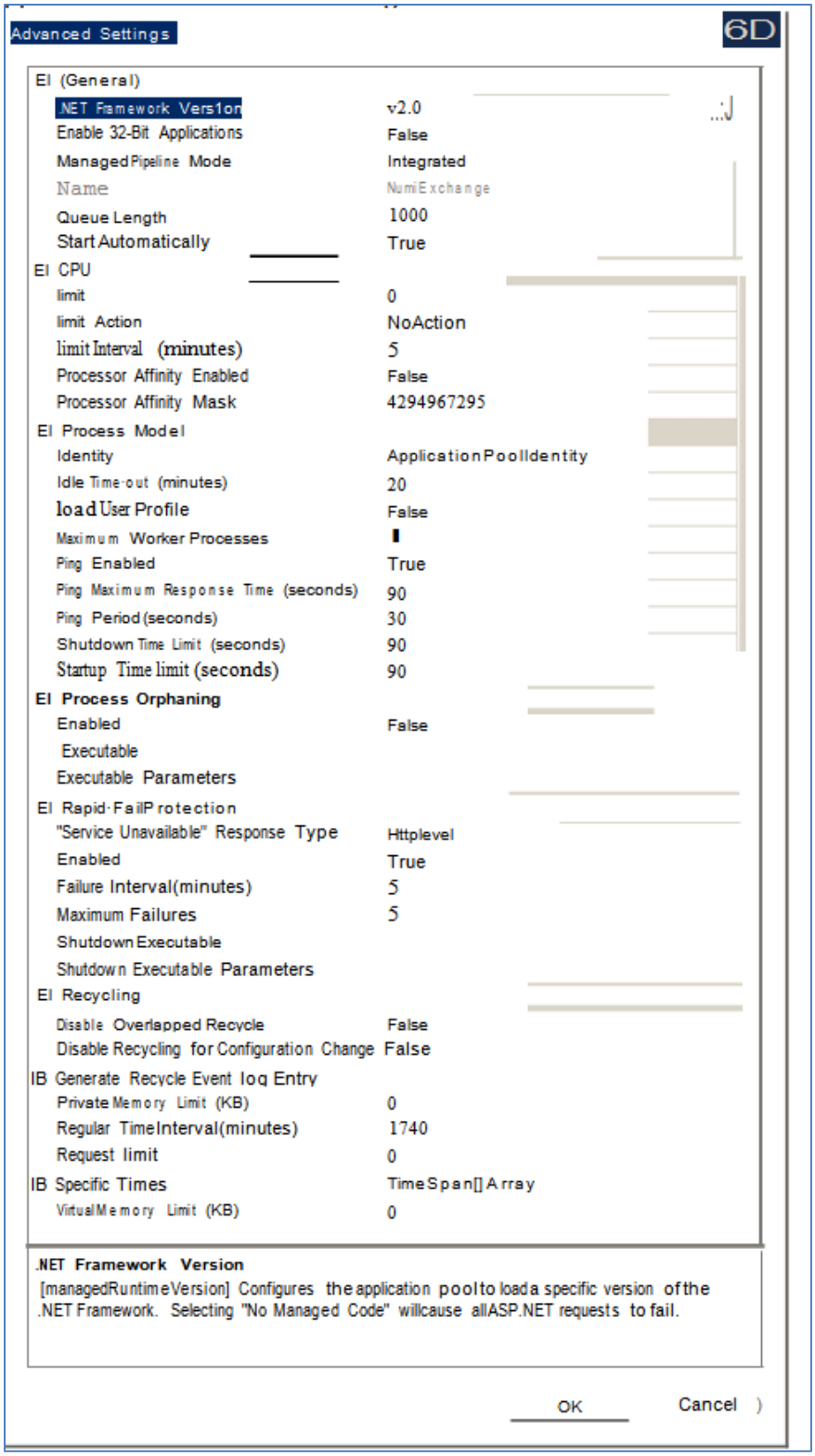


Figure 30: NUMI Exchange Pool Advanced Settings

11. Installing NUMI on Server 2012 R2

11.1. Software Copy Instructions

Right click on the zip file, select the “Unblock” if active, and select O.K. Some security schemes will block certain files from being unpacked, typically the Java files under the “web” directory. Setting the file to Unblock eliminates this problem.

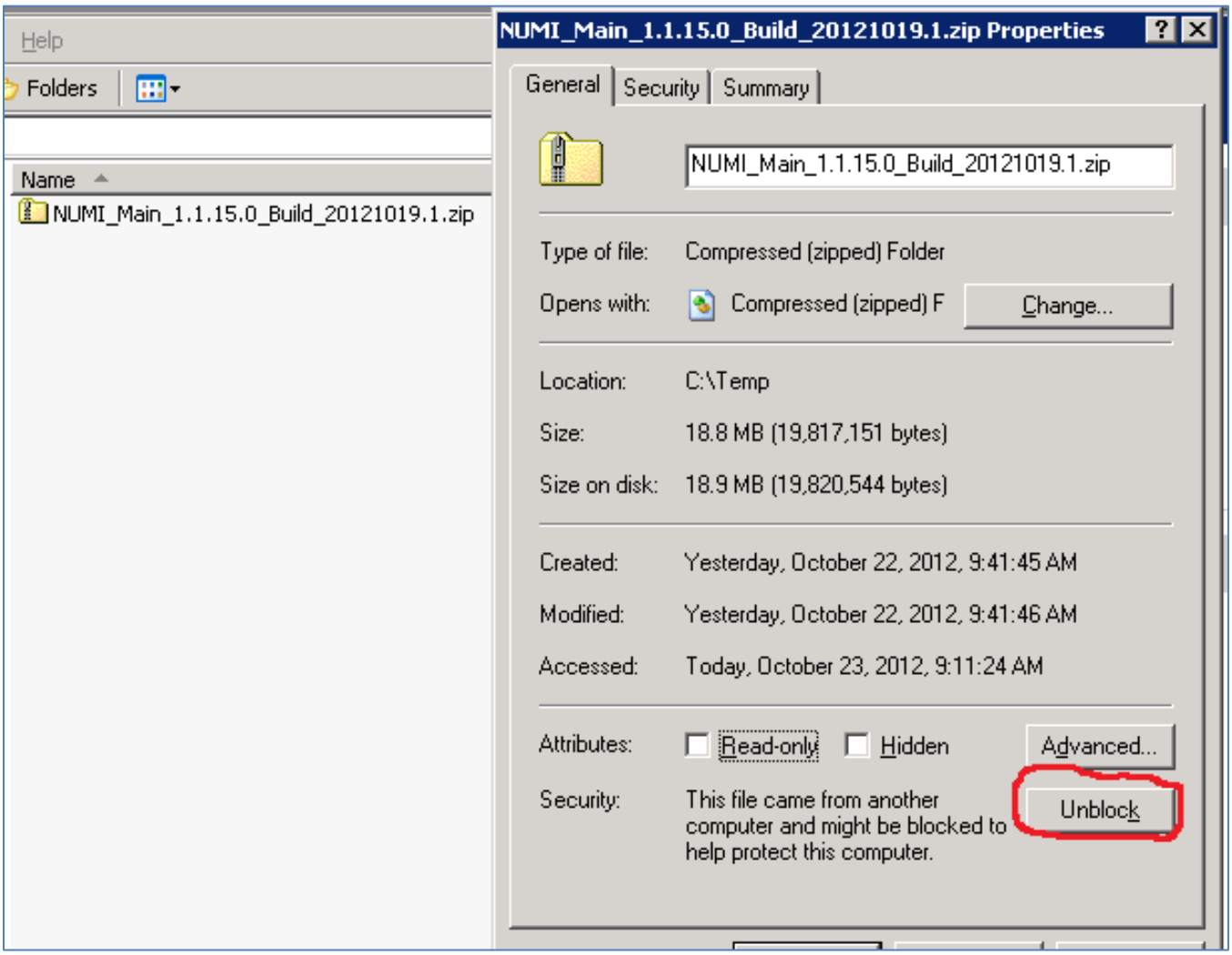


Figure 31: Unblocking Restricted Files in Installation ZIP File

It is recommended that NUMI be installed in the D:\NUMI folder. Using Windows Explorer, create a NUMI folder in D drive, if available, otherwise create in C drive. E.g., D:\NUMI.

Unzip the NumiWebApp folder from the NUMI distribution zip file into the D:\NUMI folder. Rename the NumiWebApp folder using the build name of the distribution zip file.

11.2. NUMI Web Site Configuration

Using IIS Manager, add a new web site as shown in Figure 32: Add NUMI Website.

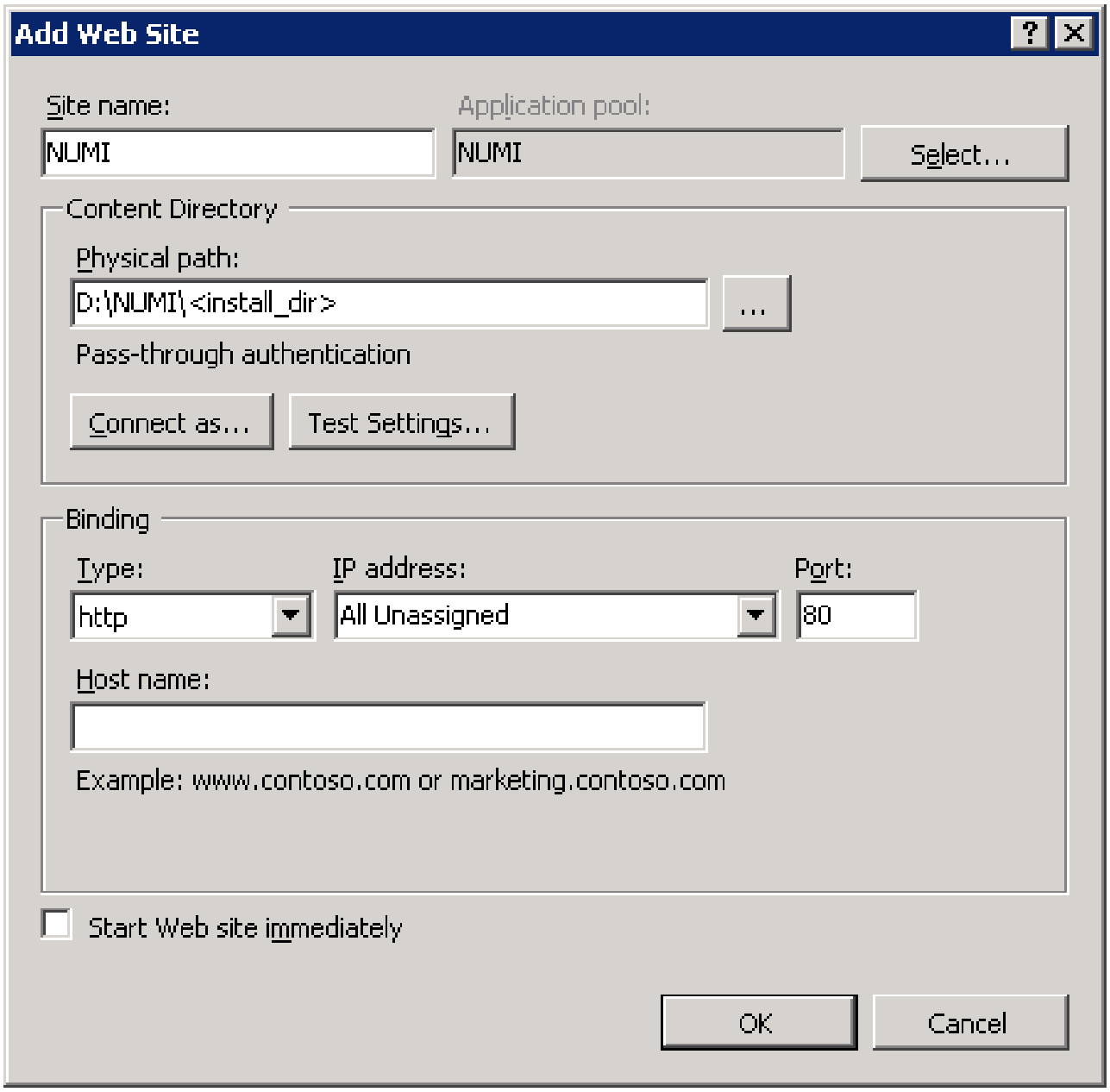


Figure 32: Add NUMI Website

The NUMI web site basic and advanced settings are shown in Figure 33: NUMI Basic Settings and Figure 34: NUMI Advanced Settings.

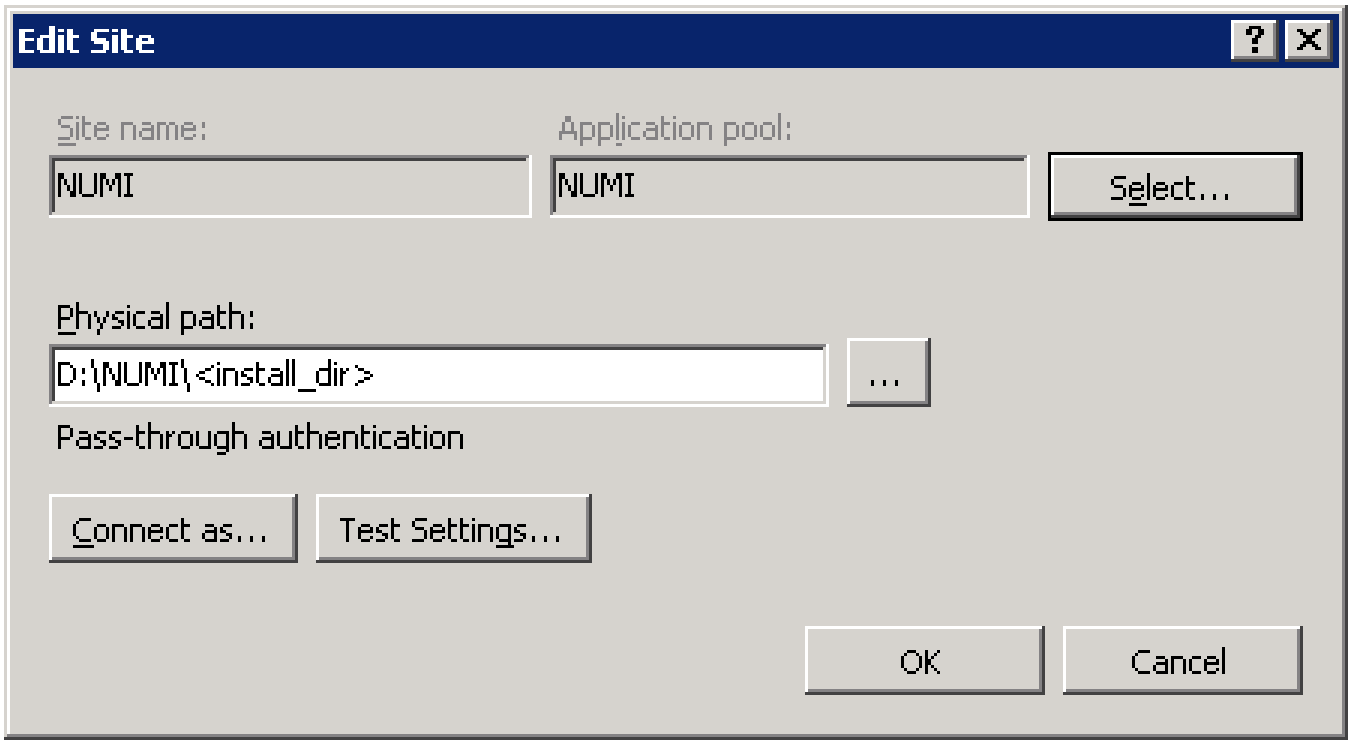


Figure 33: NUMI Basic Settings

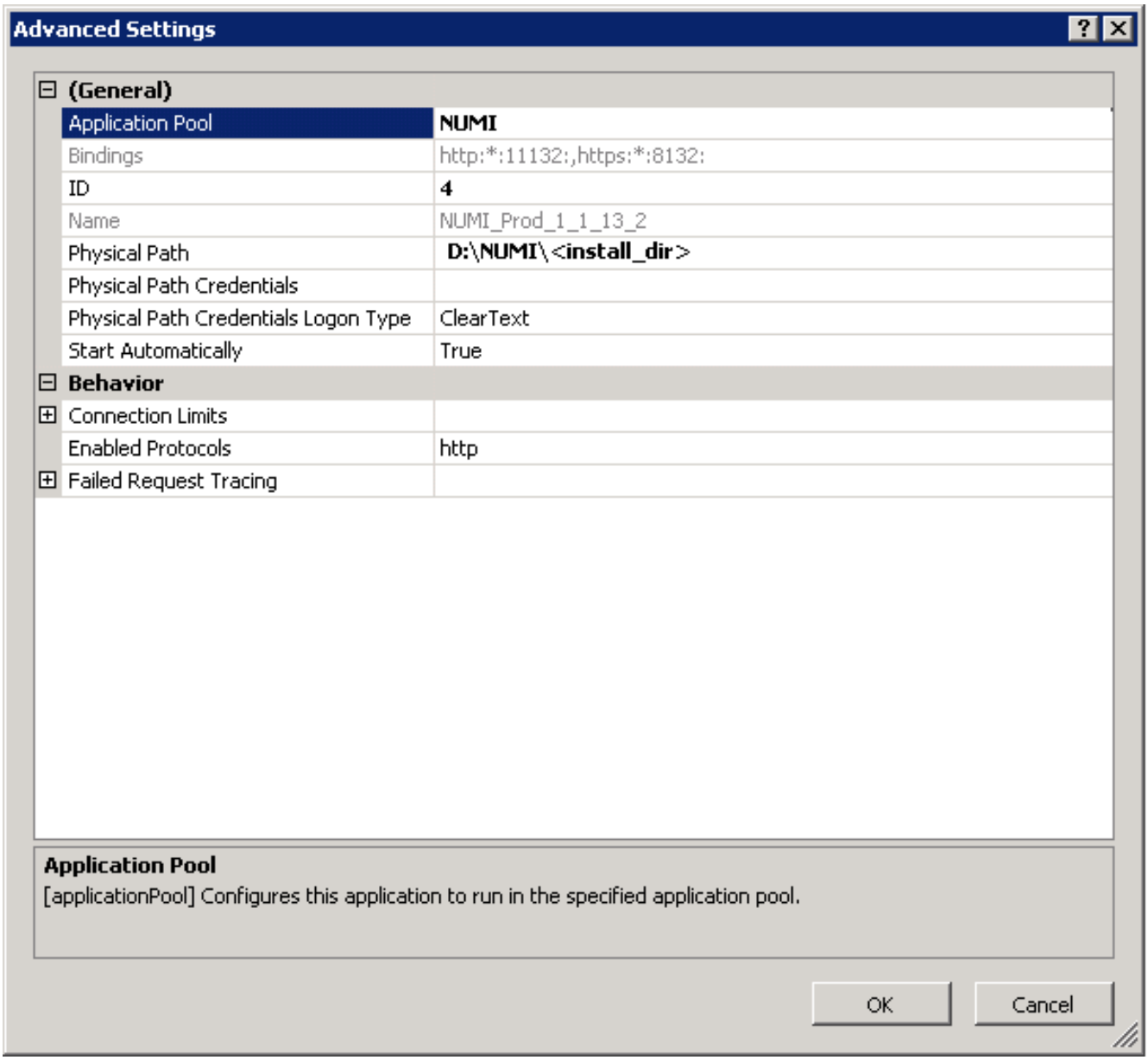


Figure 34: NUMI Advanced Settings

The NUMI web site bindings are shown in Figure 35: NUMI Bindings.

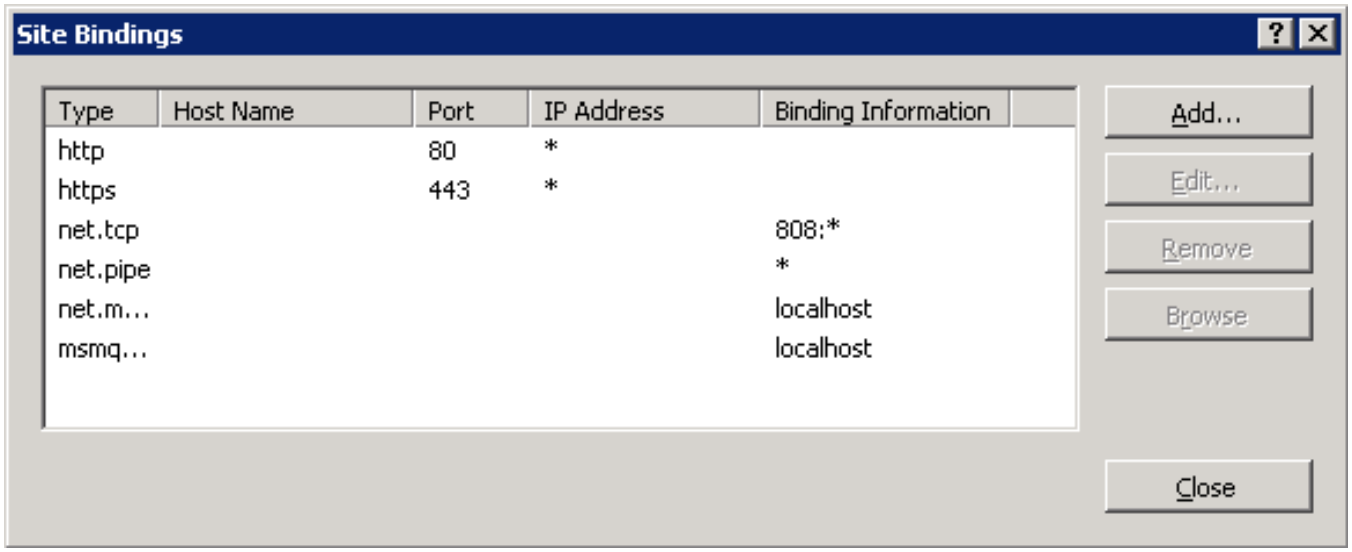


Figure 35: NUMI Bindings

The NUMI web site authentication settings are shown in Figure 36: NUMI Authentication Settings. Make sure Forms Authentication is the only one enabled.

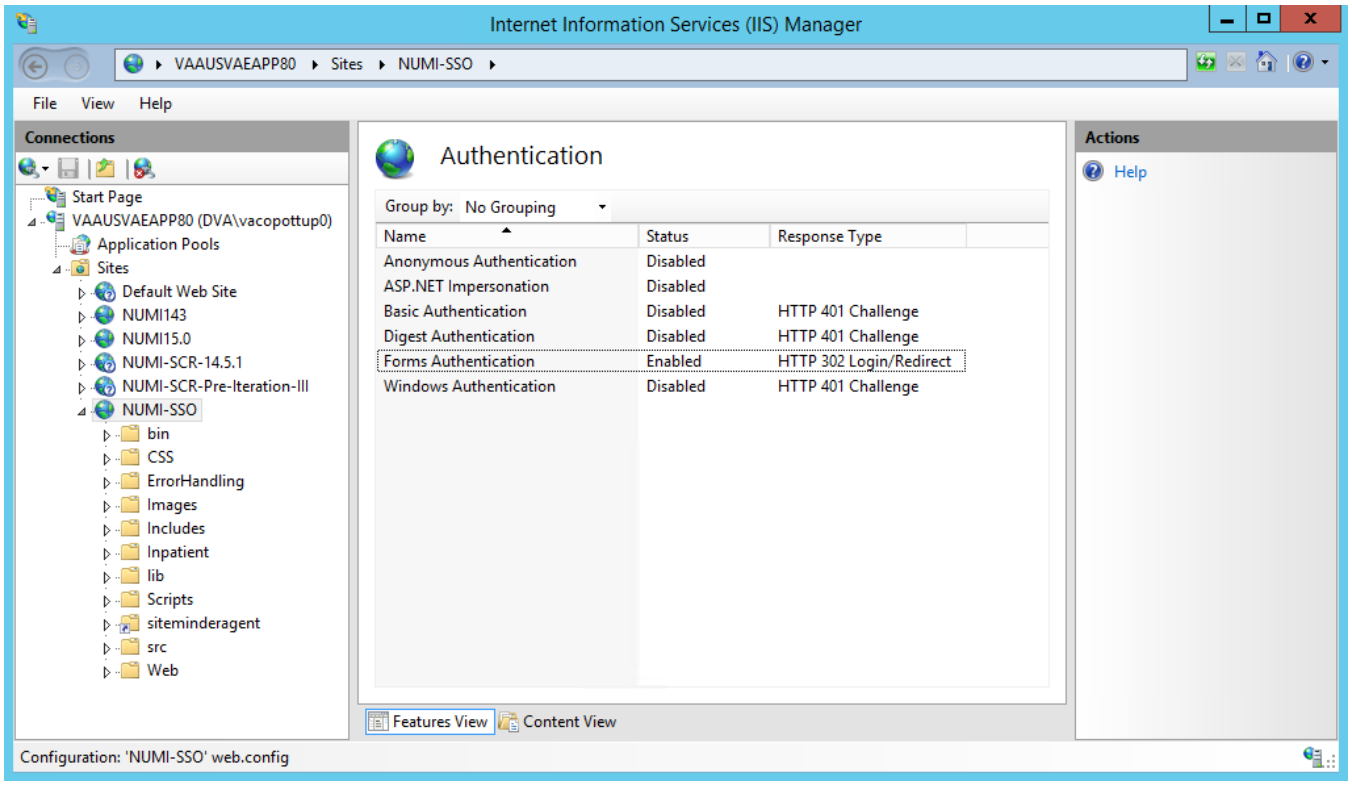


Figure 36: NUMI Authentication Settings

The NUMI website SSL settings are shown in Figure 37: NUMI SSL Settings.

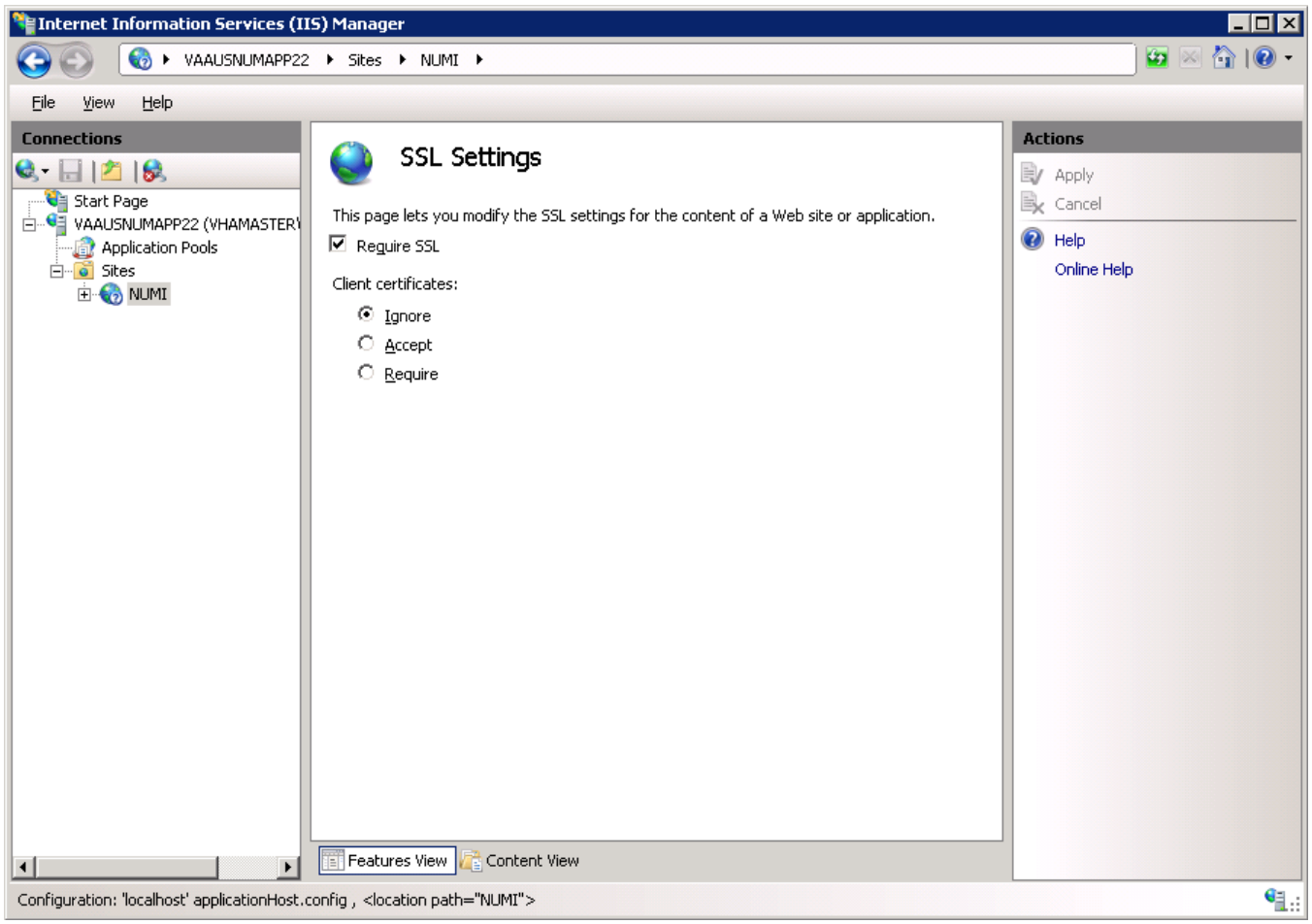


Figure 37: NUMI SSL Settings

The NUMI web site compression settings are shown in Figure 38: NUMI Compression Settings.

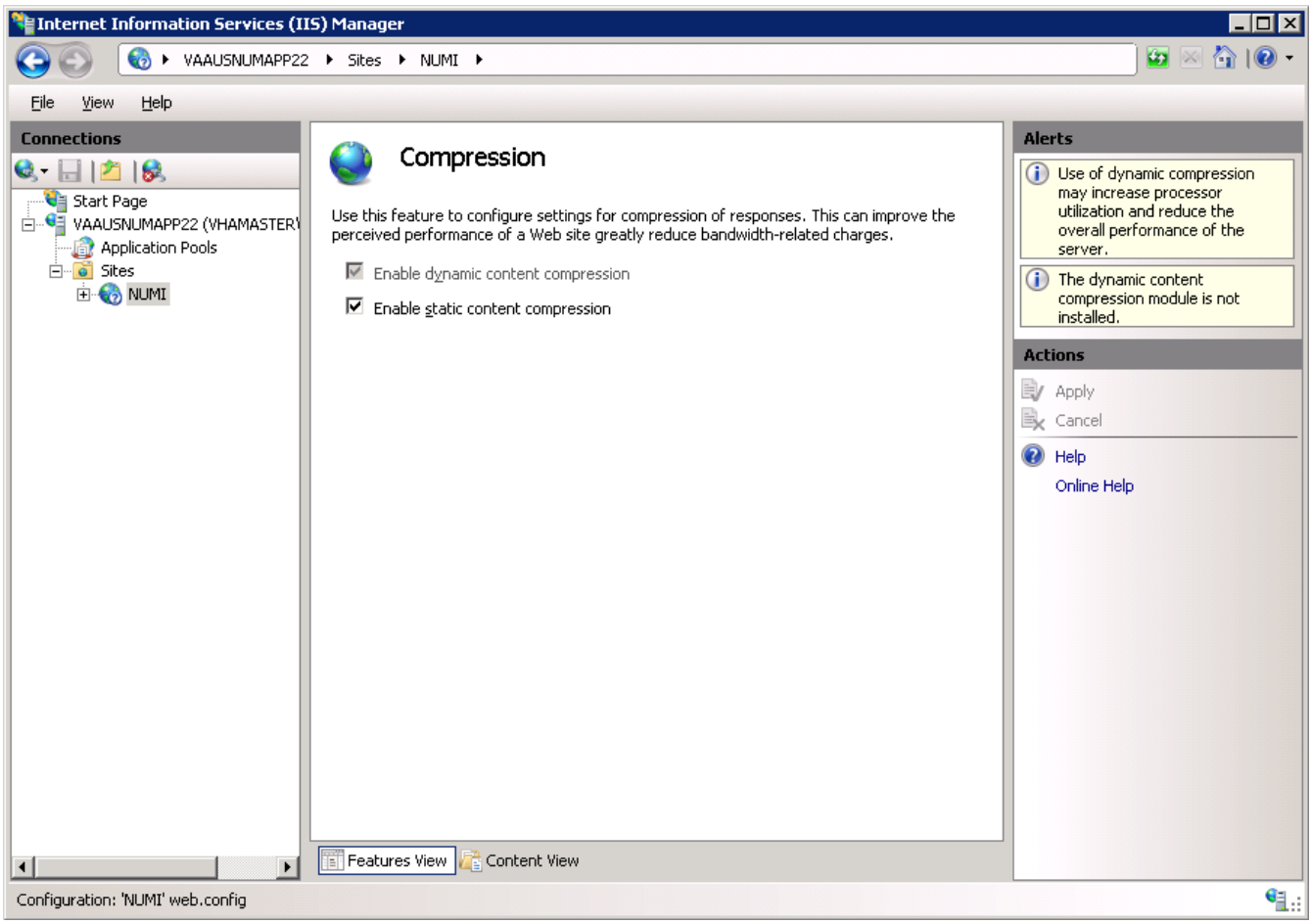


Figure 38: NUMI Compression Settings

11.3. Application Pool Configuration

The NUMI application pool setup is shown in Figure 39: Application Pool Window.

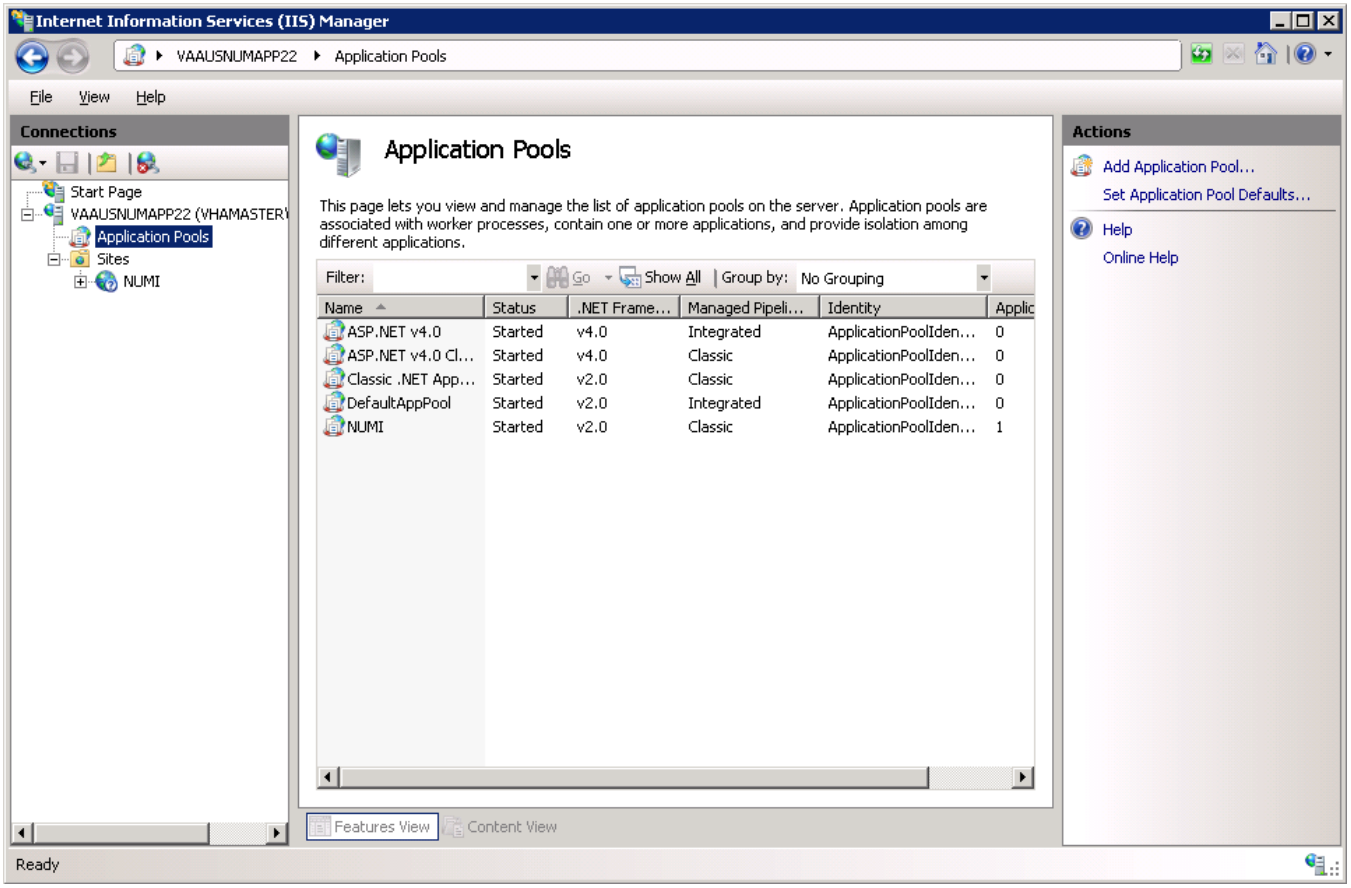


Figure 39: Application Pool Window

The NUMI application pool basic settings are shown in Figure 40: NUMI Application Pool Basic Settings.

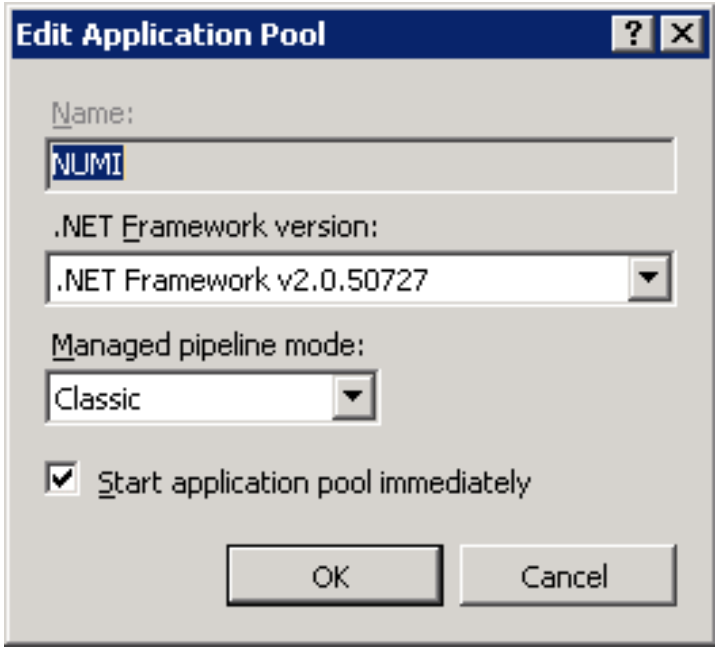


Figure 40: NUMI Application Pool Basic Settings

The NUMI application pool advanced settings are shown in Figure 41: NUMI Application Pool Advanced Settings.

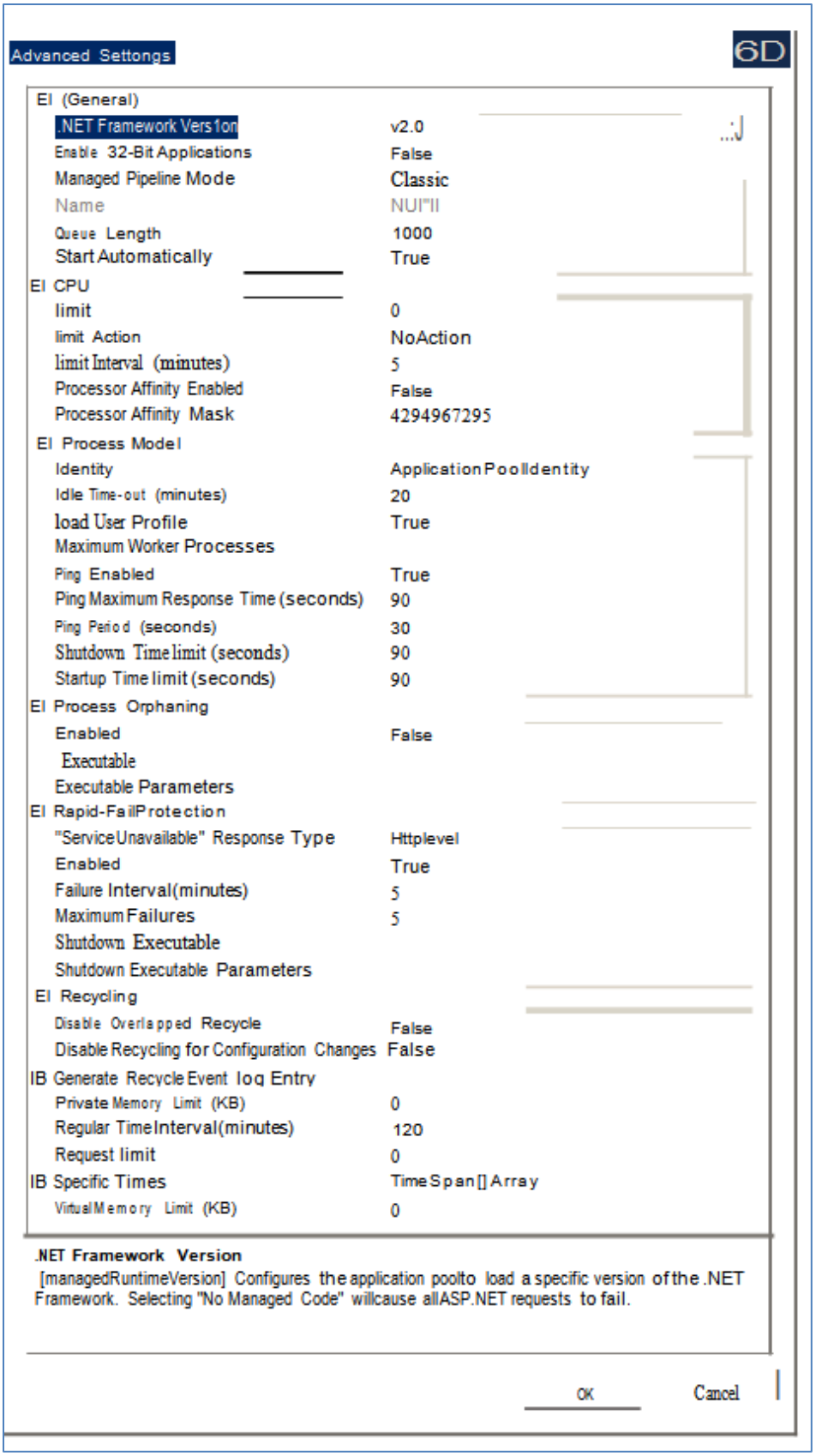


Figure 41: NUMI Application Pool Advanced Settings

12. Install CA SiteMinder Web Agent for Single Sign On (SSO) on the Web server

The CA SiteMinder Web Agent needs to be installed and configured on the WebServer where the NUMI web application will be setup. The VA Identity and Access Management (IAM) Team provides the software and instructions to install the CA SiteMinder Web Agent.

12.1. Agent location

The current version of software can be found below:
\\vaausfpciamsh61.vha.med.va.gov\Partners Share\CA SiteMinder WebAgents\Windows\Current

Copy the 32-bit or 64-bit version of the zip file as appropriate based on the OS in the server and extracts it. You will get a file with name 'ca-wa-12.51-cr08-win32.exe' in case of 32-bit and 'ca-wa-12.51-cr08-win64-64.exe' in case of 64-bit.

12.2. Agent installation

Follow the instructions below to install the software on the application server:

1. Run the exe file you obtained after extracting the zip file. If you get a dialog as shown in Figure 42 click on '`Run`' button.

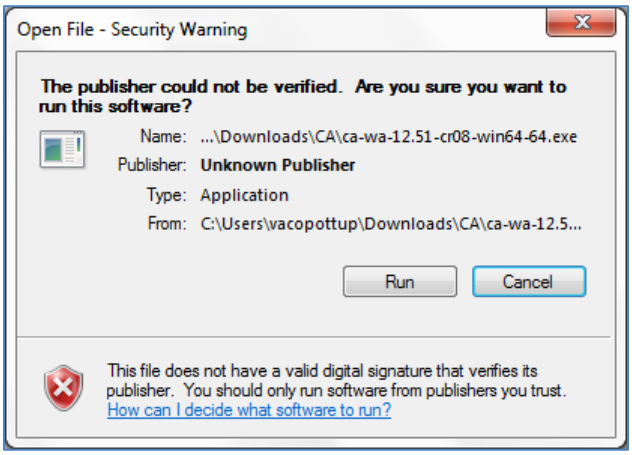


Figure 42: Security Warning

2. Wait for the dialog shown in Figure 43 to close. It may take little longer for the next dialog to show up.

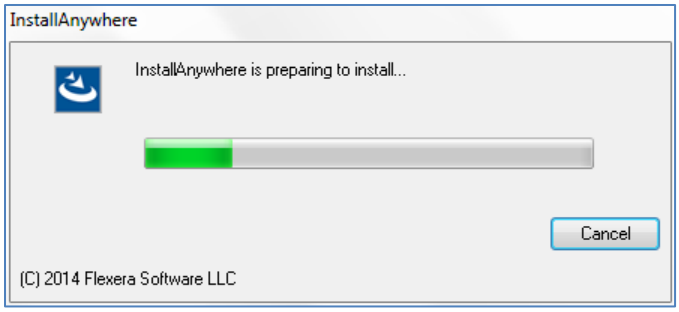


Figure 43: Preparing to install dialog

3. Click on '`Next`' in the dialog shown in Figure 44.

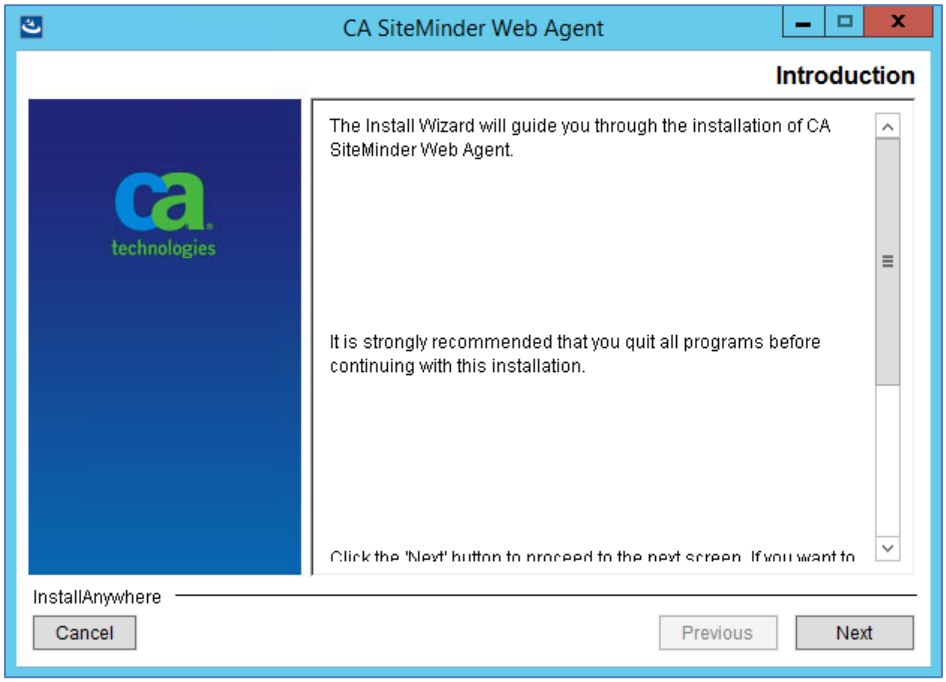


Figure 44: Web agent install wizard - Welcome screen

4. Scroll through to the bottom of the license agreement, accept it and click '`Next`' button (as shown in Figure 45).

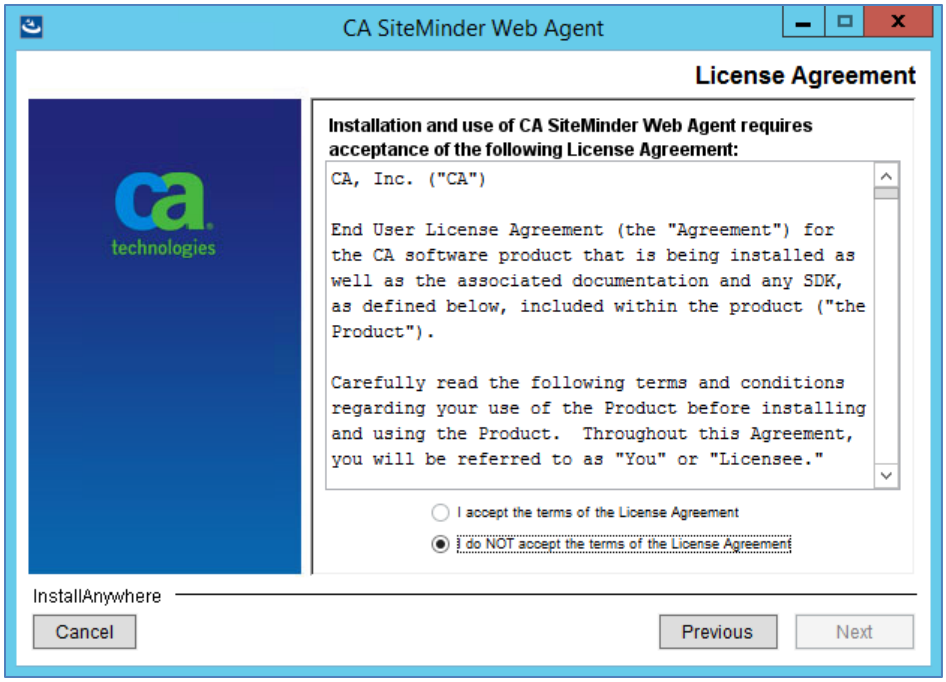


Figure 45: Web agent install wizard - License agreement screen

5. Leave the default location of installation (as shown in Figure 46) and click '`Next`'.

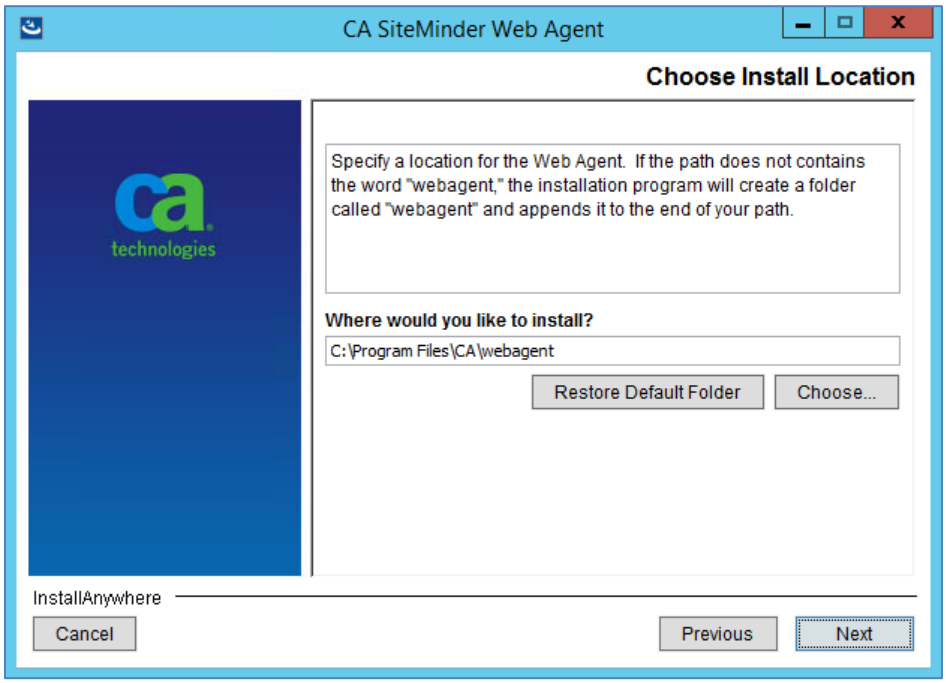


Figure 46: Web agent install wizard - Install location screen

6. Review the summary screen and click on '`Install`' button (as shown in Figure 47).

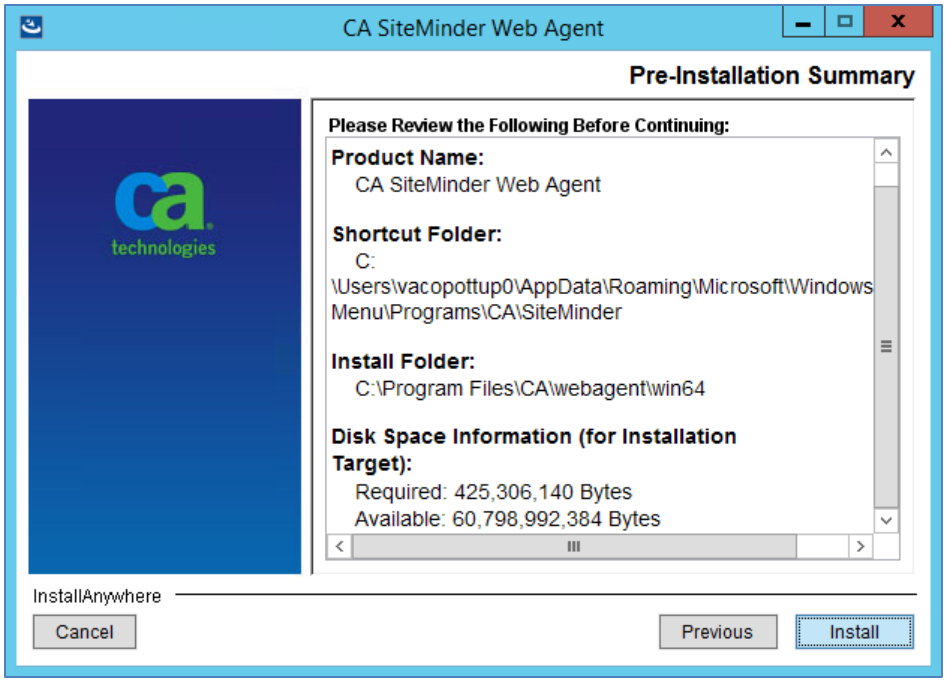


Figure 47: Web agent install wizard - Review screen

7. Select '`No. I would like to configure the Agent later`' option in the agent configuration screen as shown in Figure 48 and click '`Next`'.

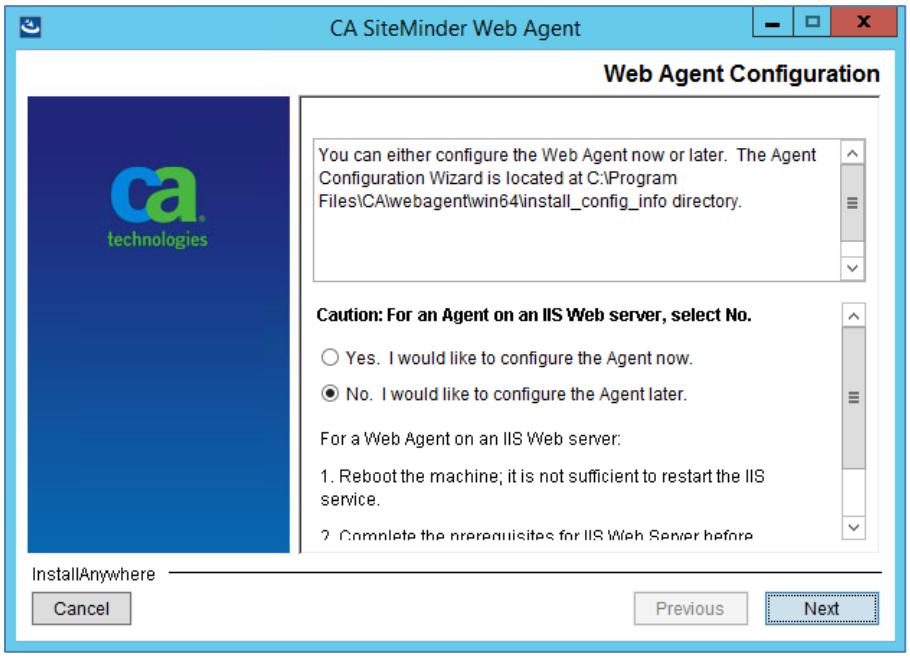


Figure 48: Web agent install wizard - Agent configuration screen

8. Select one of the options in the Install Complete screen as shown in Figure 49 and click on '`Done`' button. A restart is required to continue with the agent configuration steps described in the next section. If you selected '`No`' you would need to wait until the server is restarted to continue with next steps.

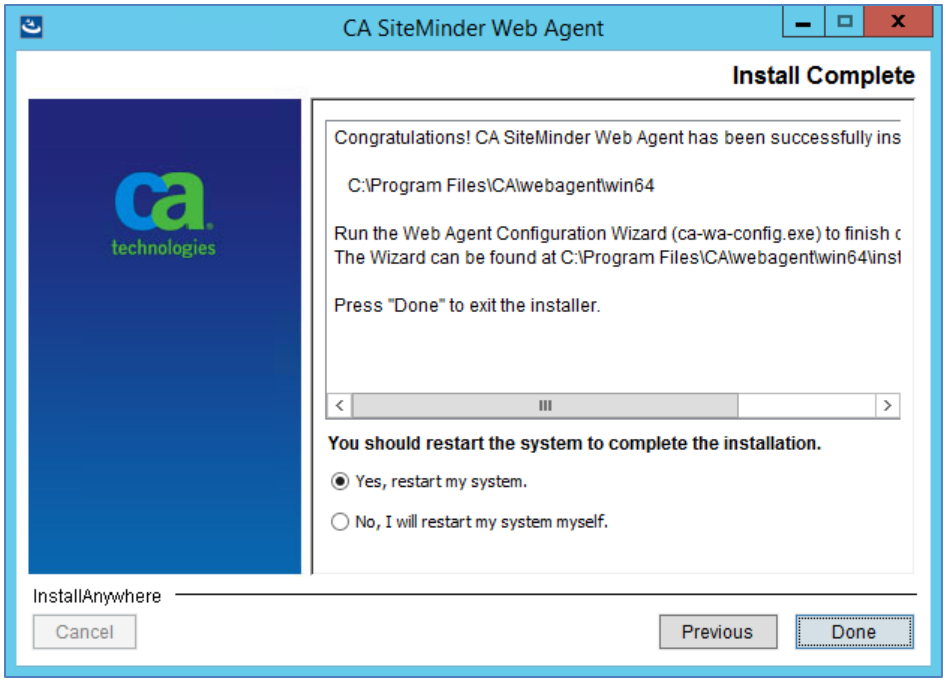


Figure 49: Web agent install wizard - Install complete screen

12.3. Agent configuration

The next steps require you to launch the agent configuration wizard from the start menu. The Figure 50 shows the one that would need to be launched.

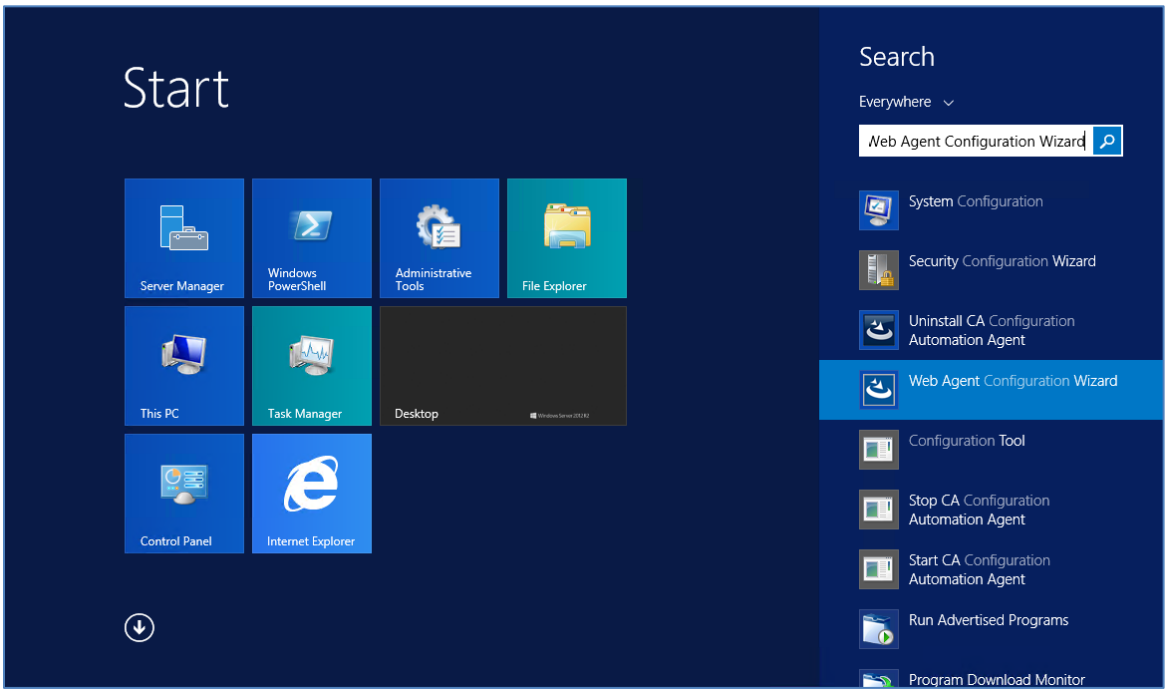


Figure 50: Launch Web Agent Configuration Wizard

If you were configuring the agent for the first time on this specific server, you would need to register the host with the IAM server. In that case, follow the instructions in Section 12.3.1.

Otherwise, skip to Section 12.3.2. Launch the Web Agent Configuration Wizard as described in Figure 50 and continue with the steps in that section.

After you complete any of these configuration steps, you would need to reset IIS by running the following command at admin command prompt:

```
iisreset
```

NOTE: You may need to use different values for various options in the below steps if IAM team has provided different values.

12.3.1. Configuring for the first time

NOTE: The steps below are if you want to register the server with IAM. This can only be done once. If for any reason you need to reconfigure the whole server, you would need to contact the IAM Team to get the current server registration deleted before you can re-run these steps.

1. Select '`Yes, I would like to do Host Registration now`' and click '`Next`' in the dialog as shown in Figure 51.

Figure 51: Web agent configuration wizard - Host registration

2. Enter the following details in the Admin Registration screen (Figure 52), ensure '`Enable Shared Secret Rollover`' is unchecked and click '`Next`' button.
   Admin User Name: threg
   Admin Password: <will be provided>

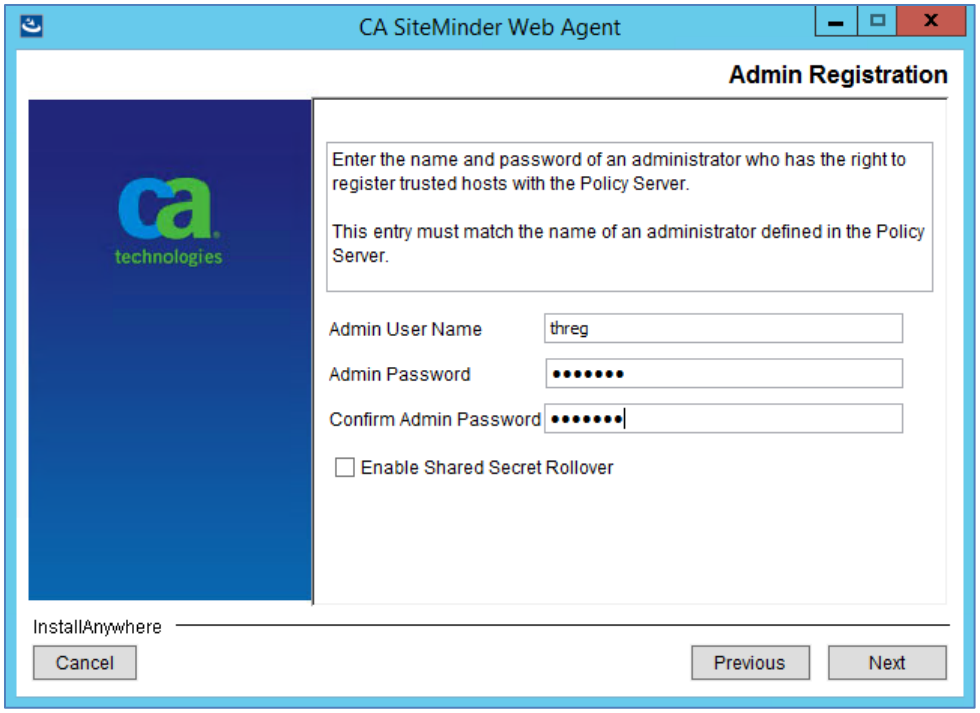


Figure 52: Web agent configuration wizard - Admin credentials

3. Enter the FQDN of the server you are currently configuring in the '`Trusted Host Name`' box and one of values from Table 3 based on which IAM environment you are trying to connect to for '`Host Configuration Object`' in the next dialog as shown in Figure 53.

Table 3: IAM Host Configuration Object

Environment	Host Configuration Object
DEV	DEVHCO
SQA	SQAHCO
Preprod	Preprod_ext
PROD	PROD_external_HCO

Figure 53: Web agent configuration wizard - Host name and configuration object

4. Add the three IP Address of Policy Server one at a time in the '`IP Address`' box from Table 4 based on the IAM environment you are trying to connect to and click '`Next`' in the dialog as shown in the Figure 54.

Table 4: SiteMinder Policy Server IP Address

Environment	SiteMinder Policy Server IP Address
DEV	10.227.211.211
	10.227.211.212
	10.227.211.213
SQA	10.227.238.46
	10.227.238.47
	10.227.238.48
Preprod	10.244.91.18
	10.244.91.20
	10.244.91.21
PROD	10.244.90.18
	10.244.90.20
	10.244.90.21

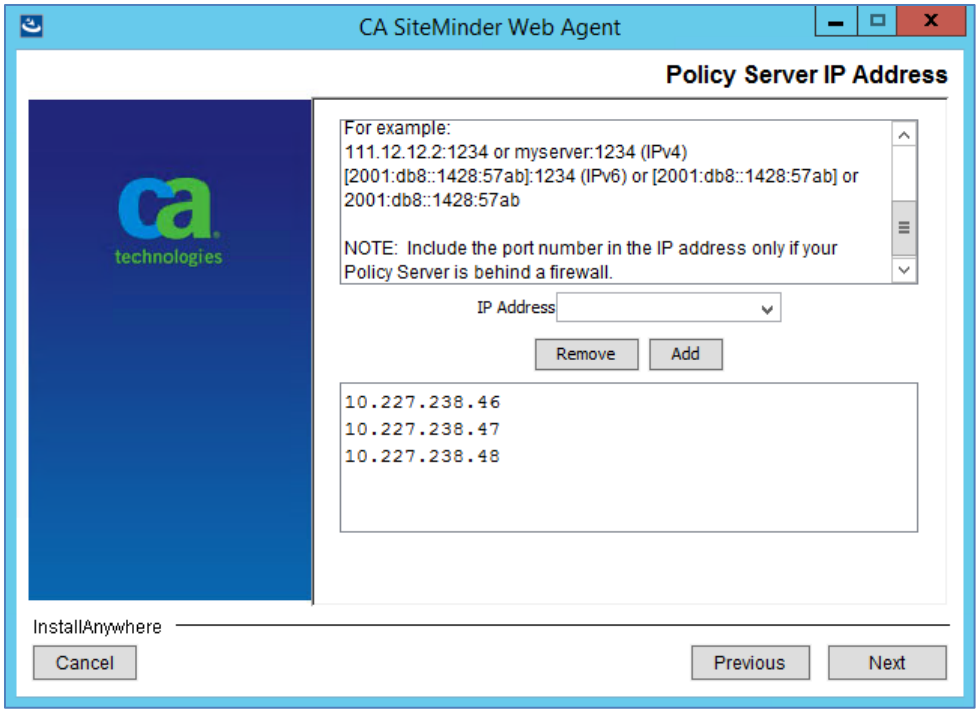


Figure 54: Web agent configuration wizard - Policy server IP Address

5. Select '`FIPS Only Mode`' in the next screen as shown in Figure 55 and click '`Next`'.

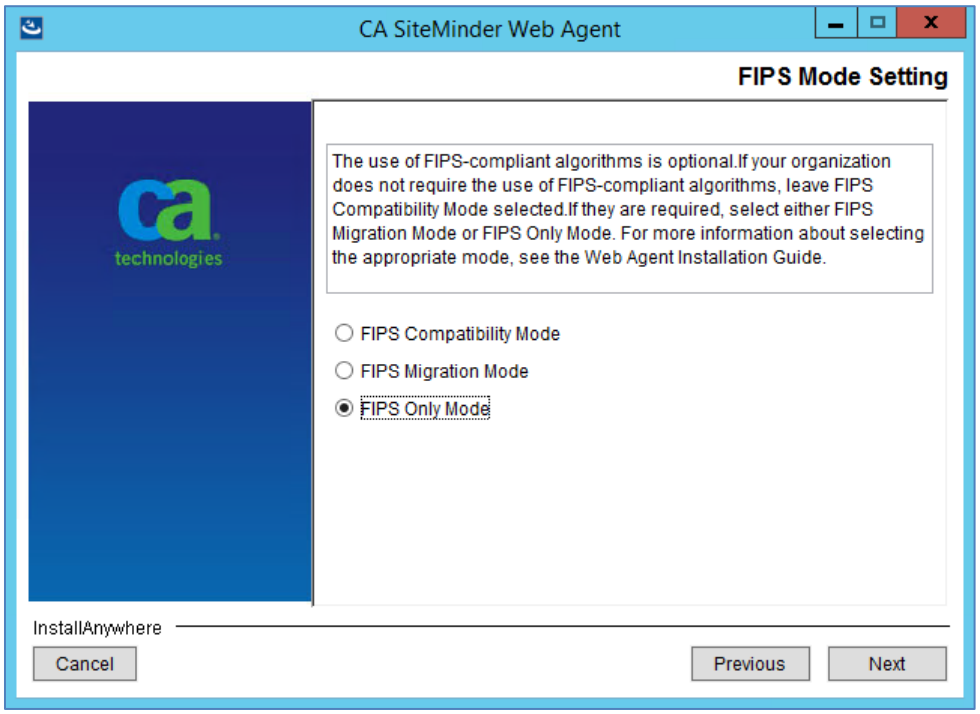


Figure 55: Web agent configuration wizard - FIPS mode setting

6. Leave everything default in the next screen as shown in Figure 56 and click '`Next`'

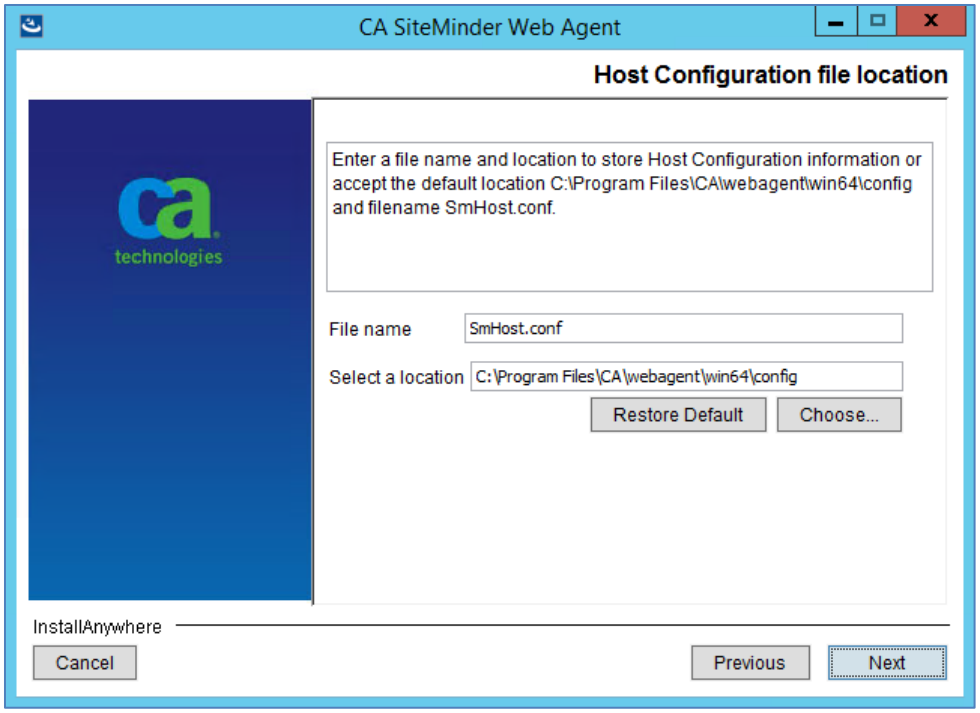


Figure 56: Web agent configuration wizard - Configuration file location

7. Select the web server on which NUMI was installed and click '`Next`'. Usually only one will be listed in this dialog as shown in Figure 57.

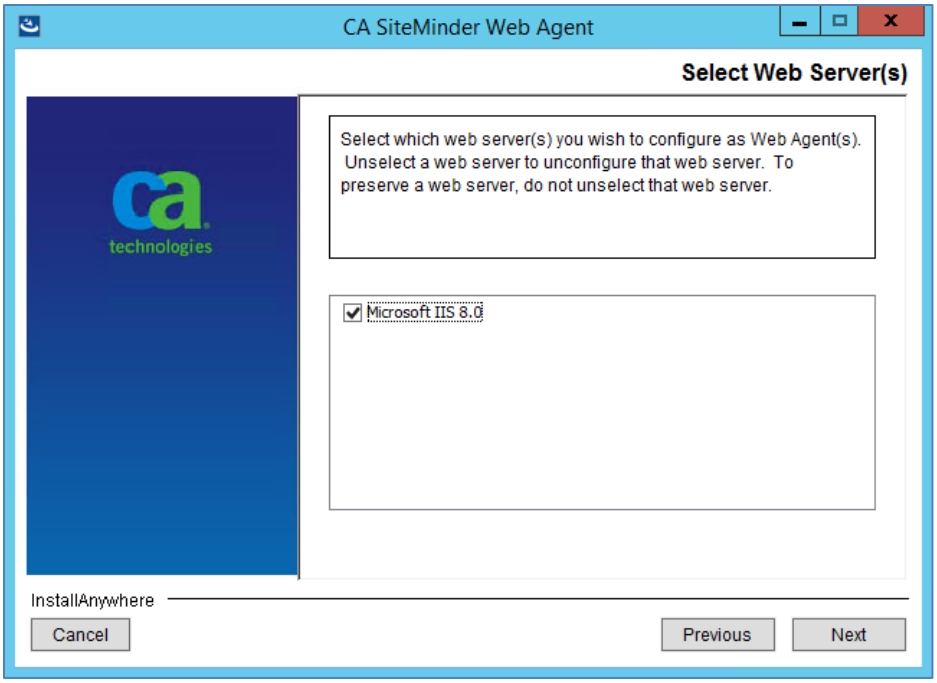


Figure 57: Web agent configuration wizard - Web server

8. Enter 'NUMIAgentConfig' in '`Default Agent Configuration Object,`' check '`Enable Agent`' and uncheck '`Manage Application Pools`' in the next screen as shown in Figure 58 and click '`Next`'.

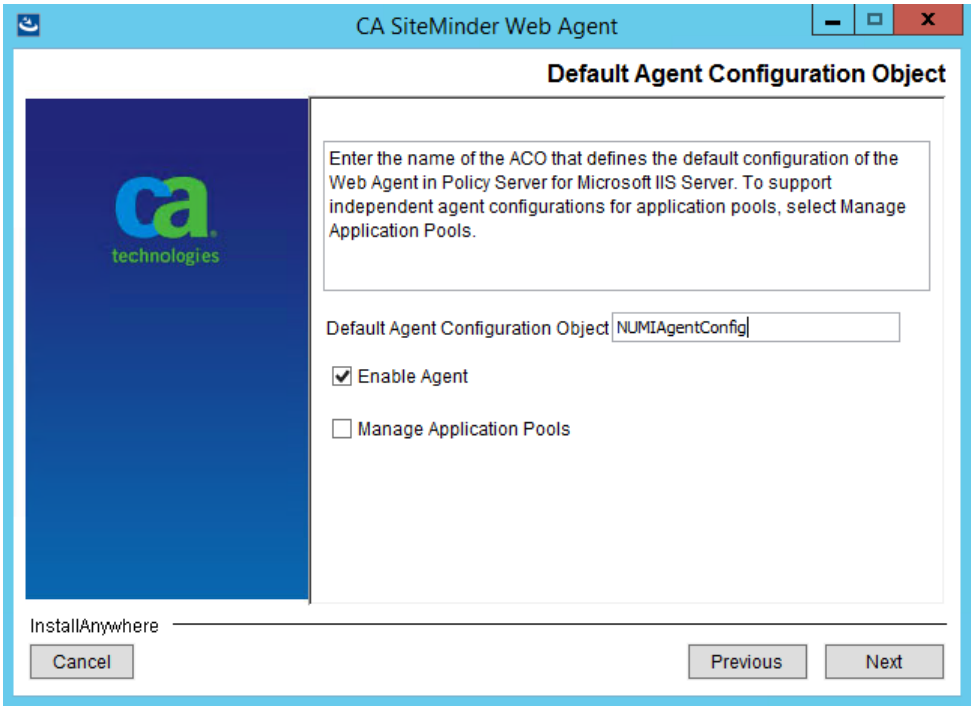


Figure 58: Web agent configuration wizard - Agent configuration

9. Select the NUMI website and any other sites where you want to enable SSO on and click '`Next`'.

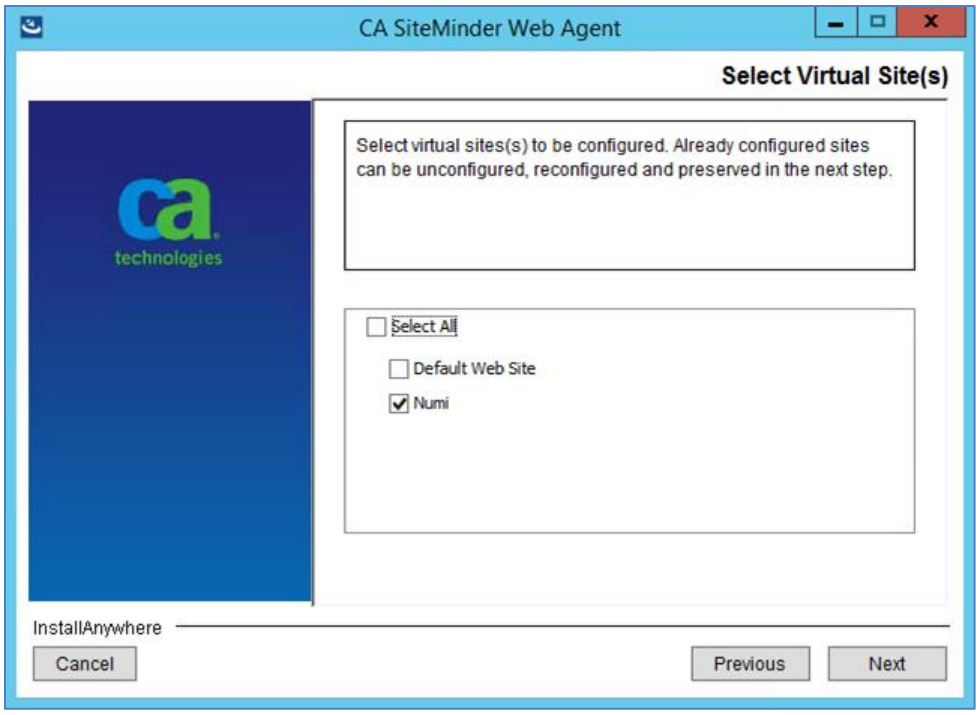


Figure 59: Web agent configuration wizard - Sites selection

10. Review the options you selected in the summary screen as shown in Figure 60 and click on '`Install`' button.

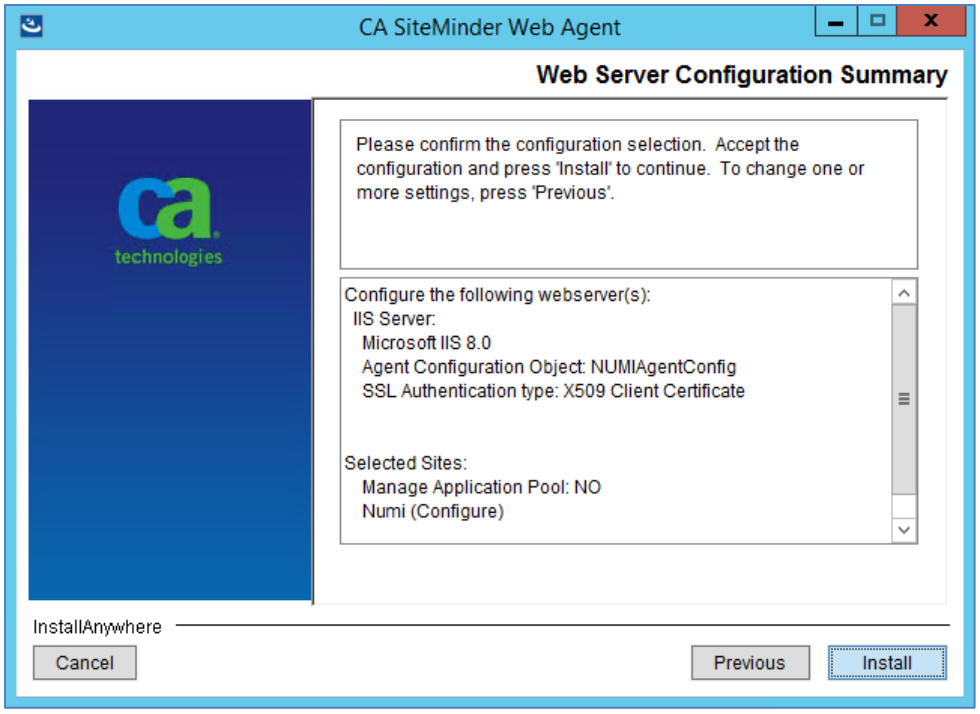


Figure 60: Web agent configuration wizard - Summary screen

11. Click on '`Done`' when you see the completion screen as shown in Figure 61.

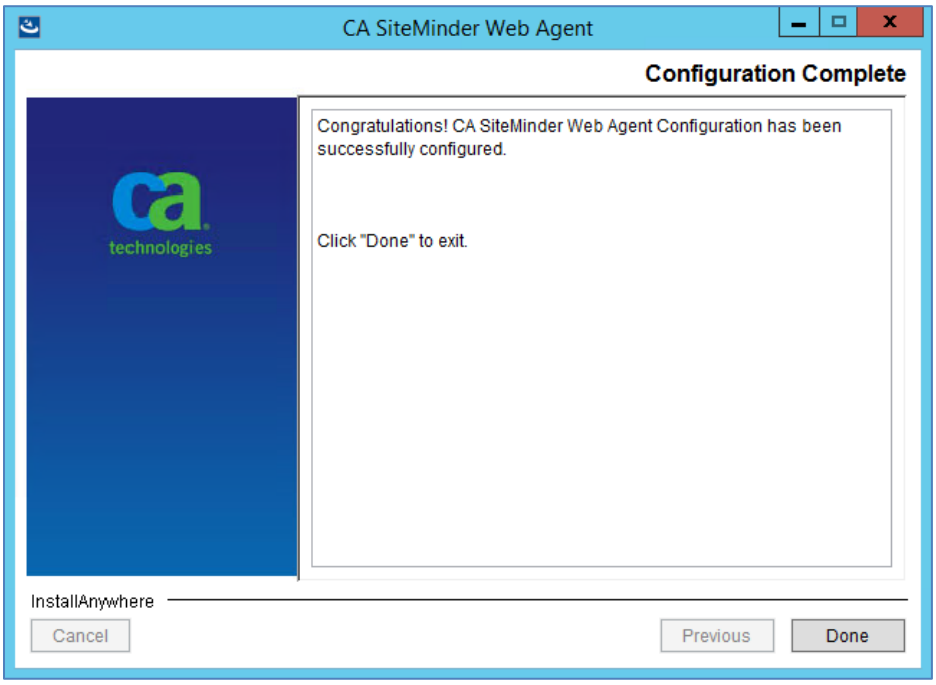


Figure 61: Web agent configuration wizard - Completion screen

12.3.2. Reconfiguration configuration

NOTE: The steps below are if you want to reconfigure one or more websites in IIS due to say re-deployment. The server should have already been registered with IAM using the steps in Section 12.3.1.

1. Select '`No, I would like to do Host Registration later`' and click '`Next`' in the dialog as shown in Figure 62.

Figure 62: Web agent configuration wizard - Host registration

2. Select the web server on which NUMI was installed and click '`Next`'. Usually only one will be listed in this dialog as shown in Figure 63.

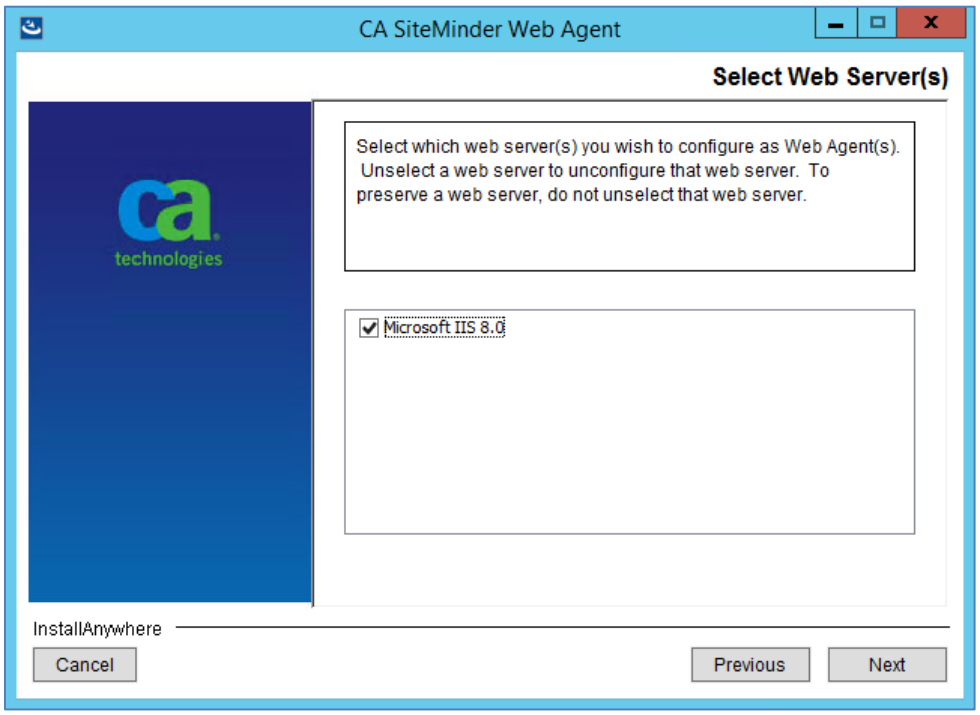


Figure 63: Web agent configuration wizard - Web server

3. Enter 'NUMIAgentConfig' in '`Default Agent Configuration Object`' if not already entered, check '`Enable Agent`' and uncheck '`Manage Application Pools`' in the next screen as shown in Figure 64 and click '`Next`'.

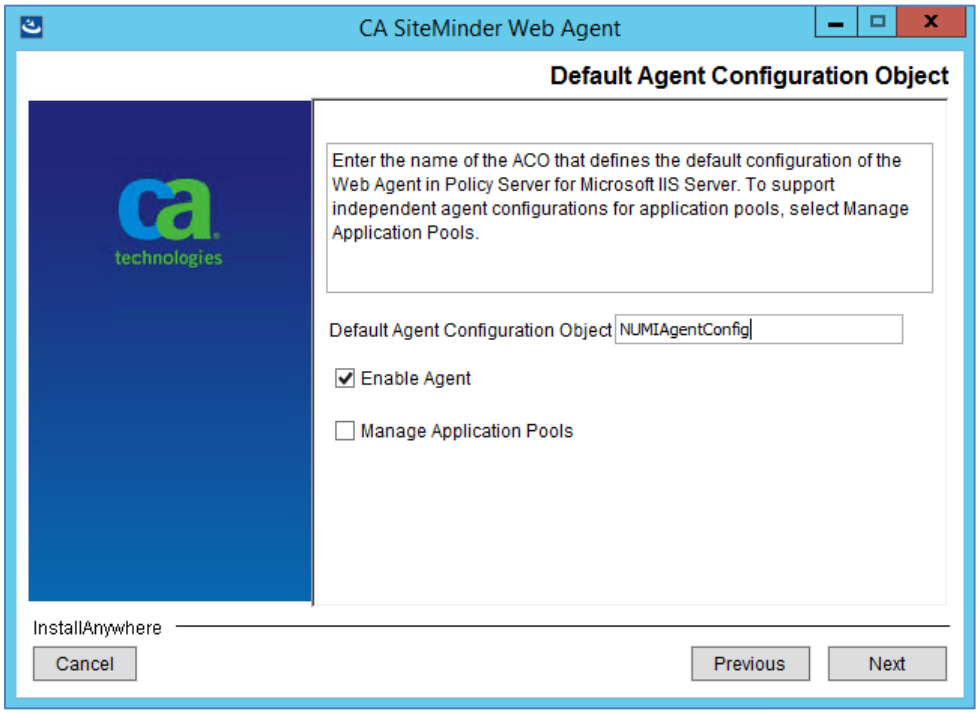


Figure 64: Web agent configuration wizard - Agent configuration

4. Select the NUMI website and any other sites where you want to enable SSO on and click '`Next`'. The sites that were previously configured will remain selected and cannot be changed (unconfigured) as shown in Figure 65.

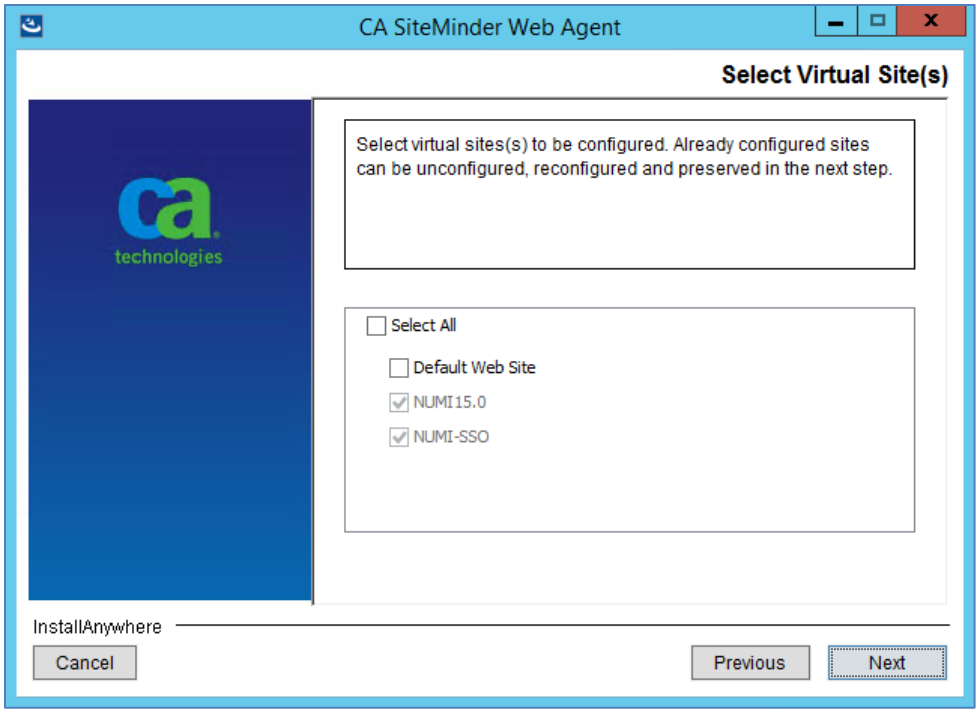


Figure 65: Web agent configuration wizard - Sites selection

5. Review the options you selected in the summary screen as shown in Figure 66 and click on '`Install`' button.

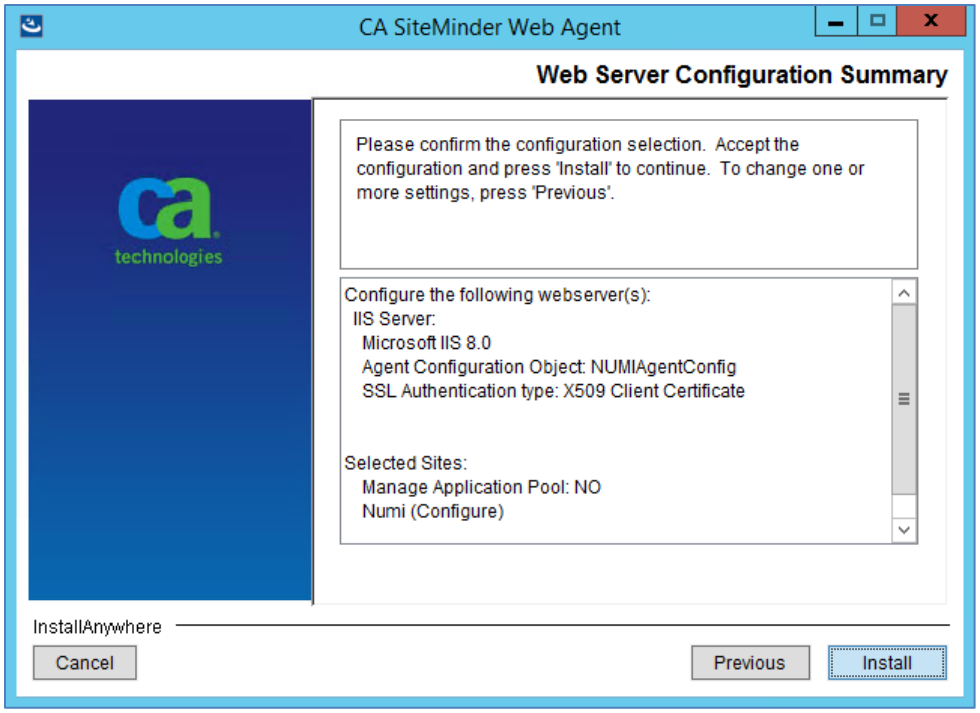


Figure 66: Web agent configuration wizard - Summary screen

6. In the screen shown in Figure 67, select appropriate option for the site you are trying to reconfigure and click '`Next`'.

'`Overwrite`' will overwrite the previously configured settings with the new one entered in the previous steps of this wizard. '`Preserve`' will not change any existing settings but will add missing settings back in to the site. If '`Unconfigure`' is selected it will remove and disable SSO for the selected site.

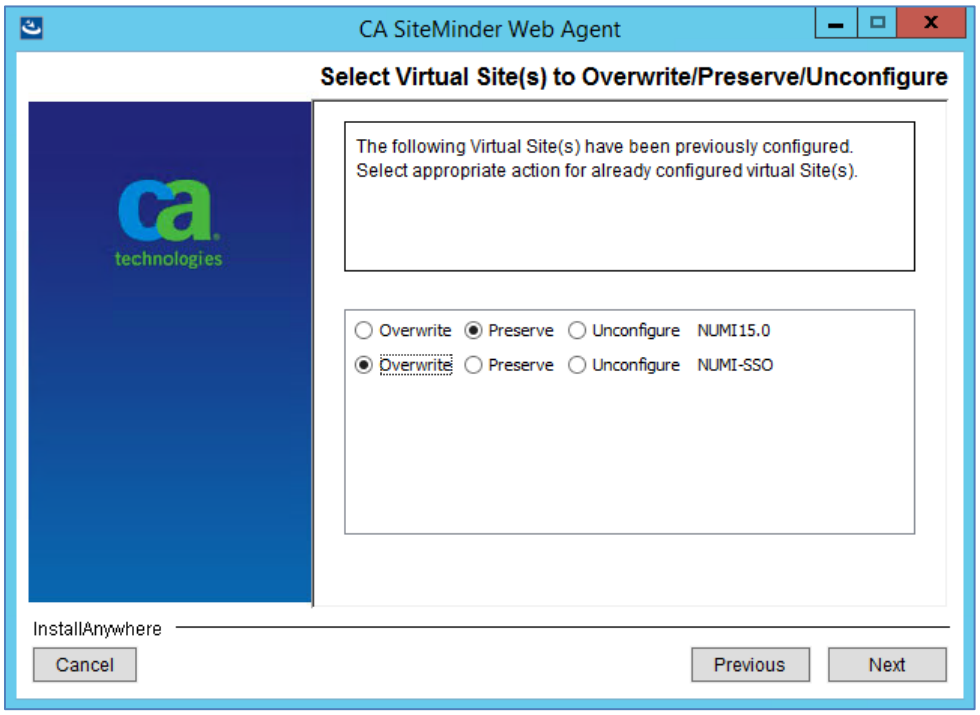


Figure 67: Web agent configuration wizard - Previously configured sites

7. Review the options you selected in the summary screen as shown in Figure 68 and click on '`Install`' button.

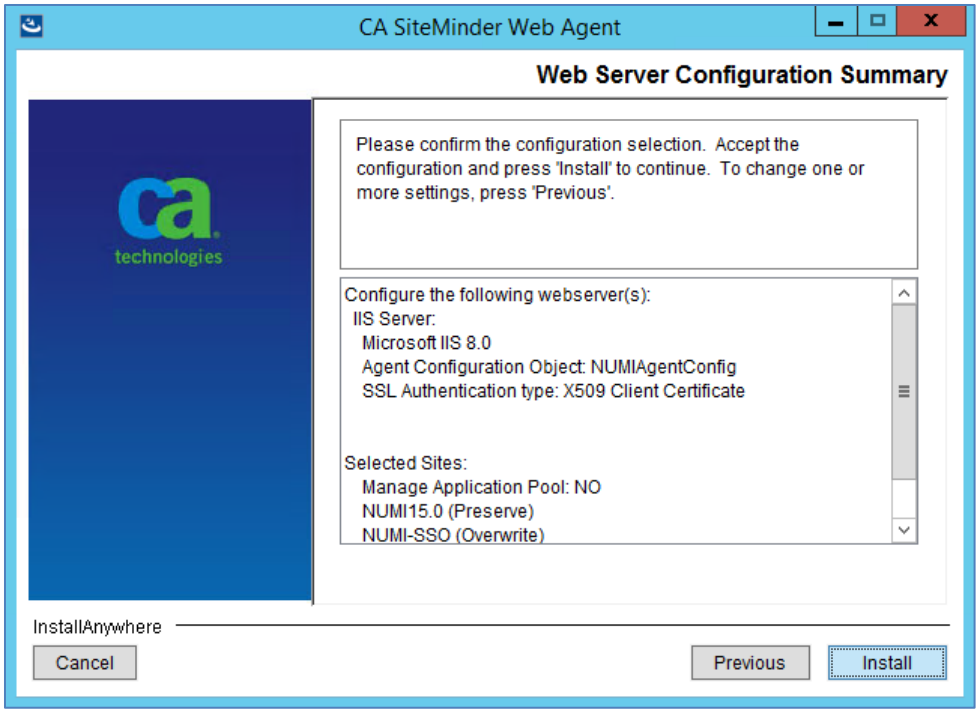


Figure 68: Web agent configuration wizard - Summary screen

8. Click on '`Done`' when you see the completion screen as shown in Figure 69.

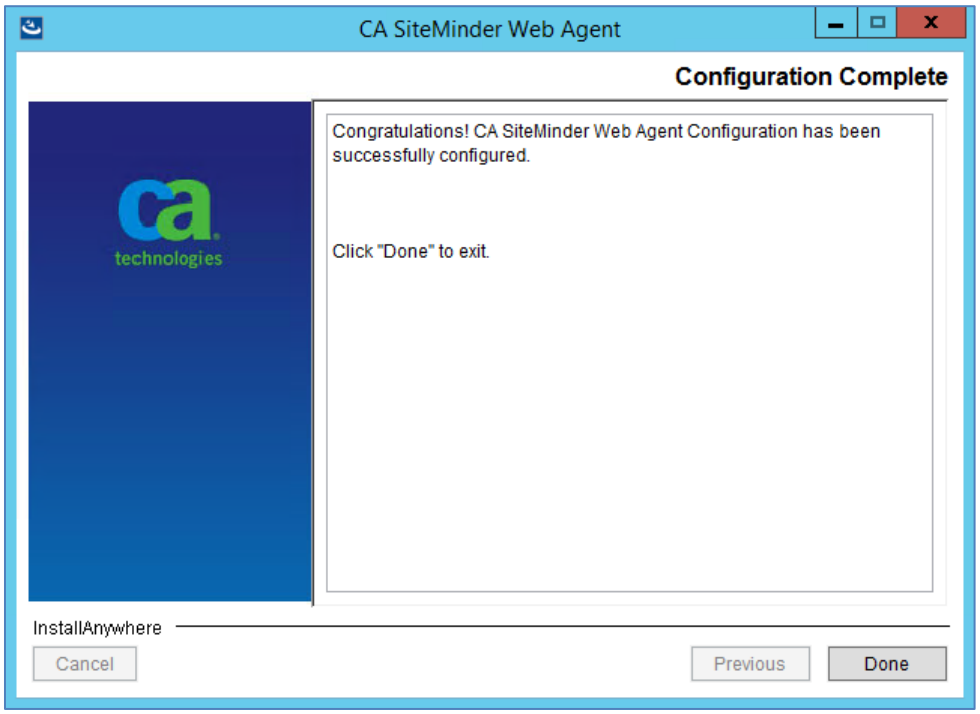


Figure 69: Web agent configuration wizard - Completion screen

13. Secure Token Service Integration for SSOi

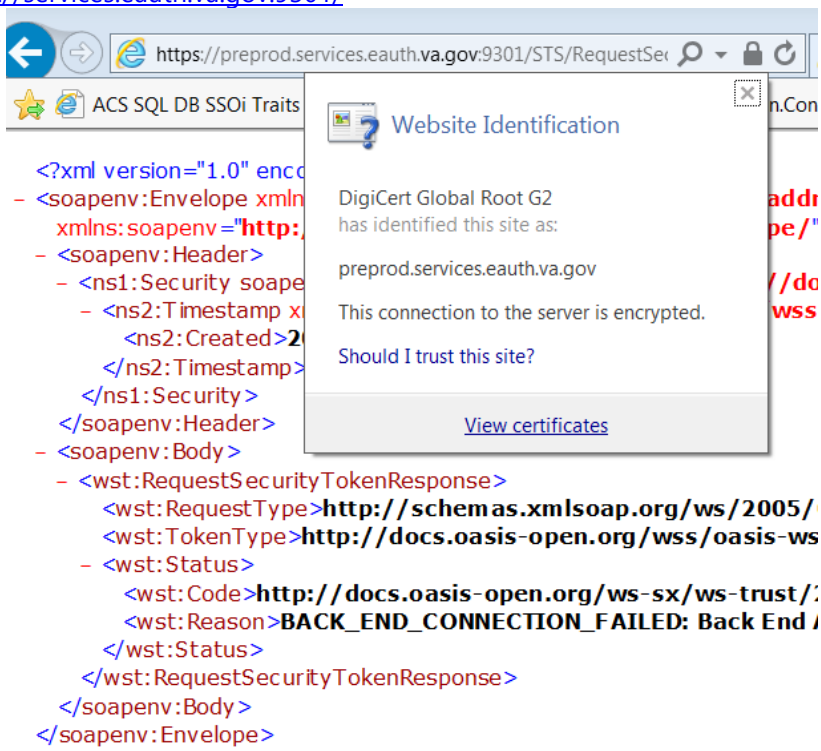
NUMI supports secure token service implementation through SSOi. Full details of the implementation can be found at SSOi Secure Token Service Playbook.

13.1. Download Certificate Chain from appropriate endpoint

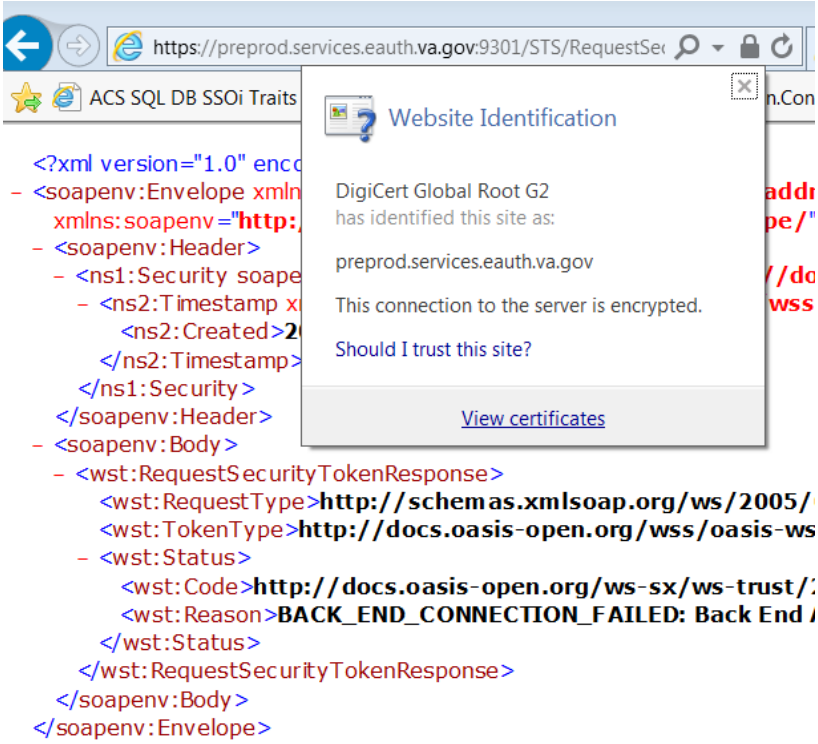
Downloading the chain can be done from any computer but installing the chain must be done as the local computer account of the server being set up.

- iDEV: https://int.services.eauth.va.gov:9301/STS/RequestSecurityToken
- SQA: https://sqa.services.eauth.va.gov:9301/STS/RequestSecurityToken
- PREPROD: https://preprod.services.eauth.va.gov:9301/STS/RequestSecurityToken
- PROD: https://services.eauth.va.gov:9301/STS/RequestSecurityToken

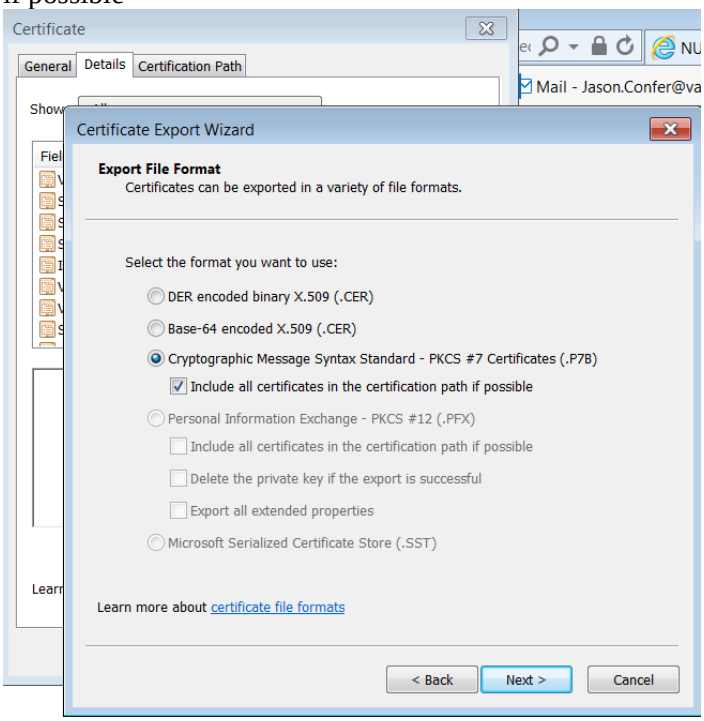
1. Install the full certification chain from the matching IAM environment(s). This can be obtained by visiting the link and clicking the lock icon and choosing "View Certificates".
   https://services.eauth.va.gov:9301/



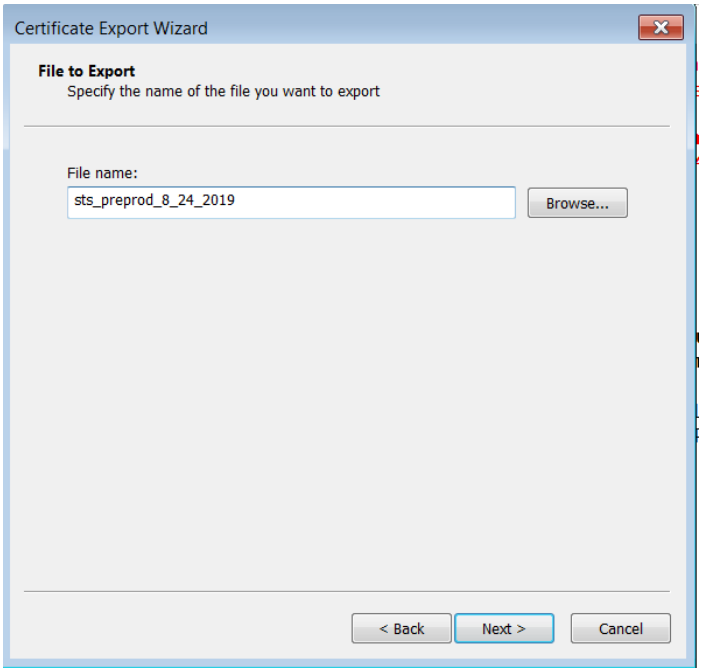
1. Install the full certification chain from the matching IAM environment(s). This can be obtained by visiting the link and clicking the lock icon and choosing "View Certificates".
   https://services.eauth.va.gov:9301/



2. Click on the Details tab and select “Copy to file”, choose PKCS and include all certificates in the path if possible

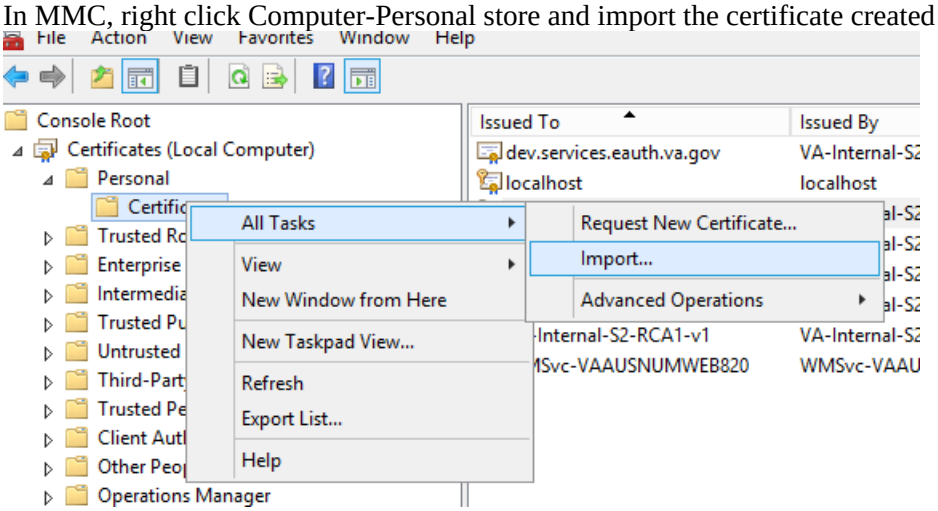


3. Save file as <endpointname_date>, click next then finish.

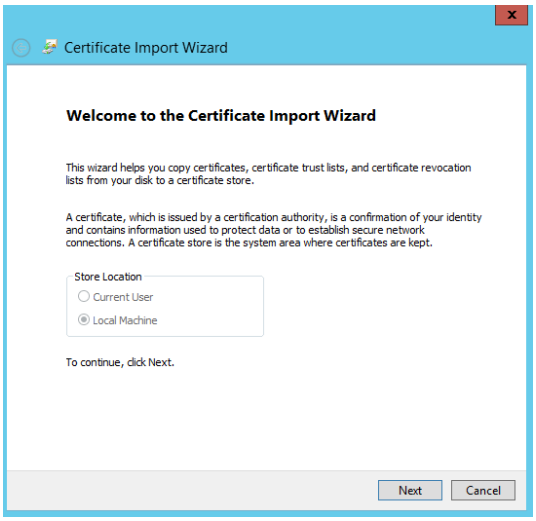


4. Optional – Reuse this file if another web server requires this STS endpoint's certificate.

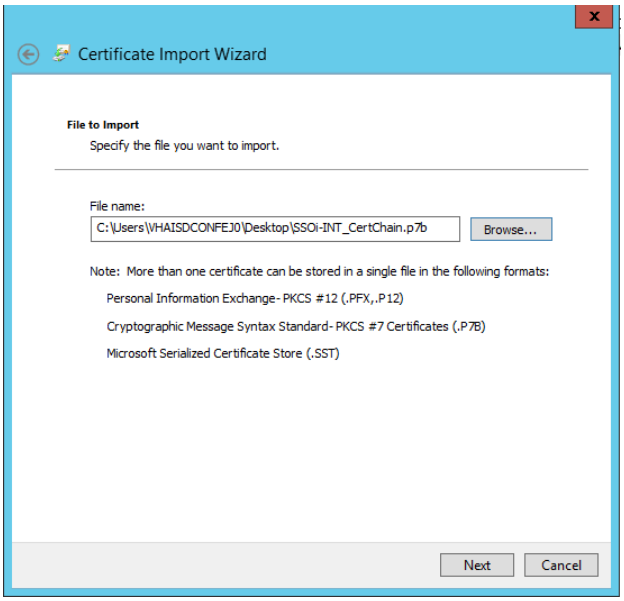
5. In MMC, right click Computer-Personal store and import the certificate created in Step 9.



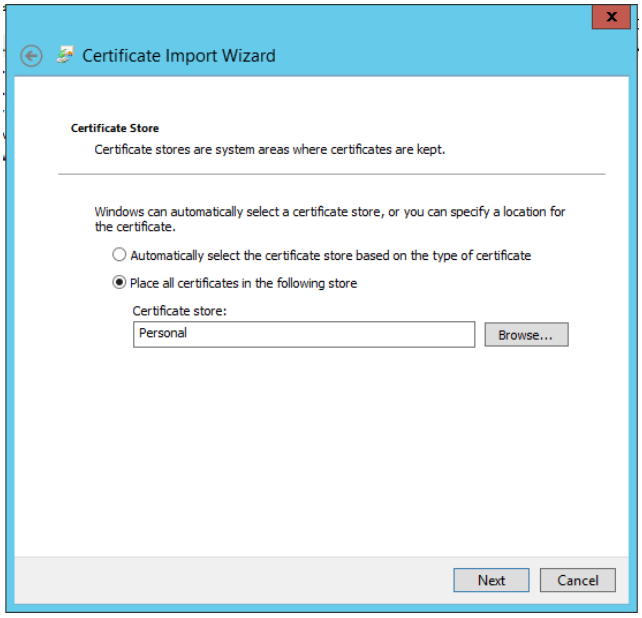
6. Import for local machine



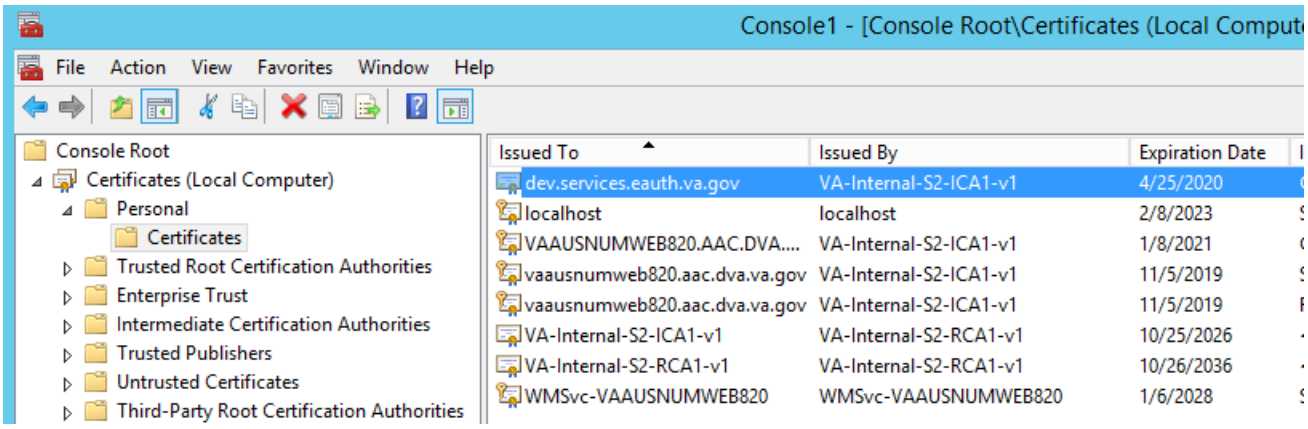
7. Browse to file created in step 10 and click Next



8. Place all certificates in the Personal store, click next and finish



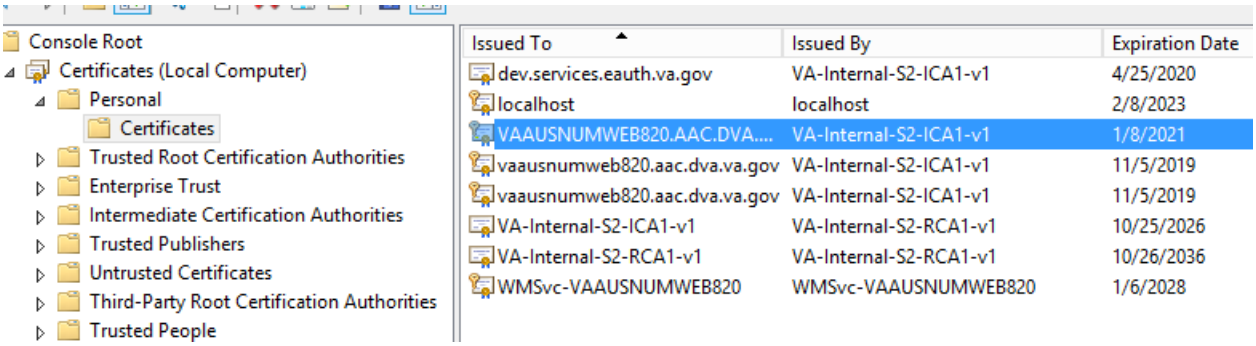
9. The imported certificate should now be in the store (refreshing may be required). It will follow the naming convention xxxx.services.eauth.va.gov



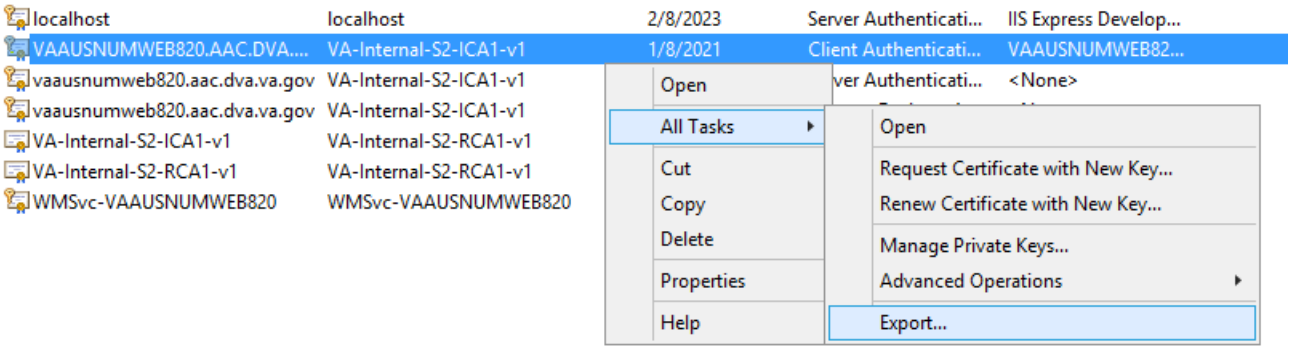
13.2. Export server cert to .pfx

This is a copy of the .cer installed locally to the computer/personal account. It should be the one served by IIS when you navigate to the website.

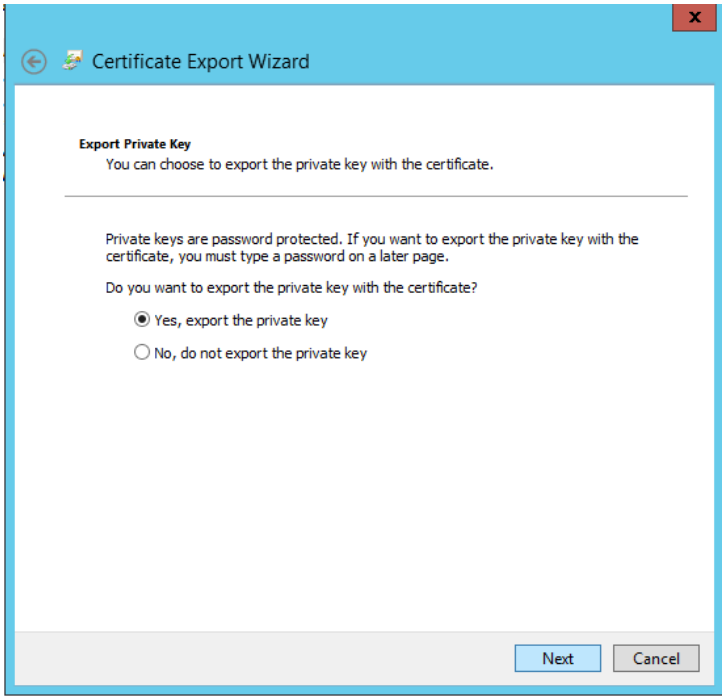
1. Load the Microsoft Management Console, Certificate Snap-in, for the local computer
2. Find the server cert in the personal folder



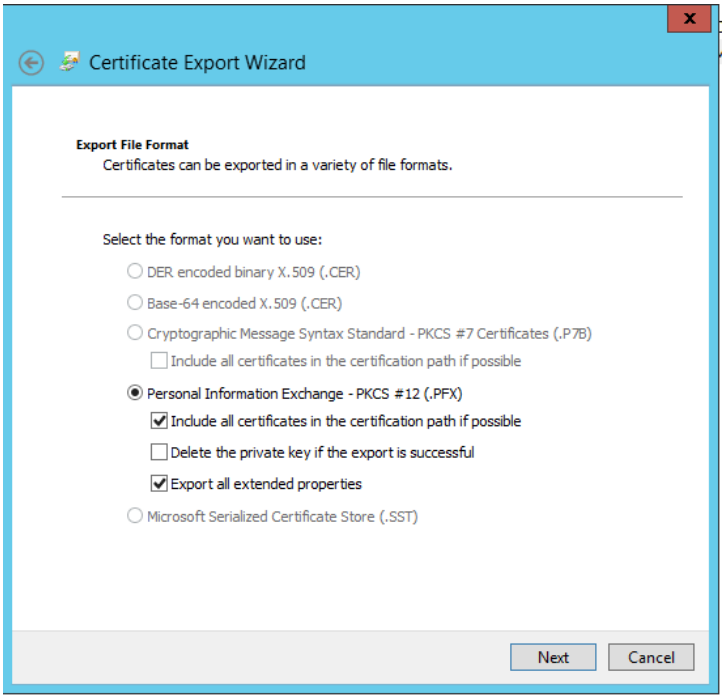
3. Right click and export the certificate



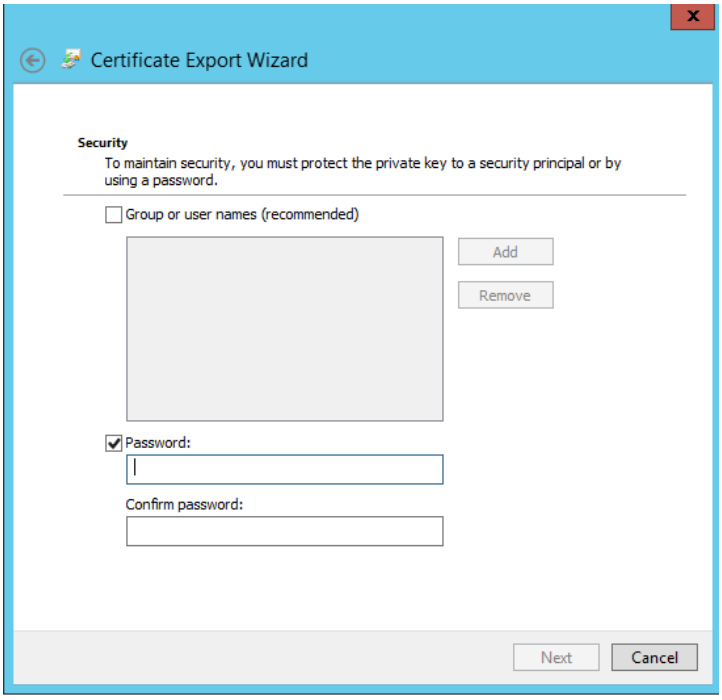
4. Select “Yes, export private key” and choose next



5. Select “Export all extended properties” and choose next



6. Select a strong password. This password will go into NumiWebApp.config later in this guide.



7. Select a filename for the exported certificate and save it as a .pfx. Select a folder not specific to a version of NUMI as this cert will be valid for future versions of the applications until expiration. For example, if the folder structure for website is NUMI/NUMI_15.9 select the /NUMI folder for the cert and not the specific /NUMI_15.9 folder. This file path will go into NumiWebApp.config later in this guide.

13.3. NumiWebApp.config keys

```
<!-- STS Service configuration -->
<add key="STSEndpoint" value="https://int.services.eauth.va.gov:9301/STS/RequestSecurityToken"/>
<add key="STSEnabled" value="true"/> <!-- Set "true" to enable STS service integration -->
<add key="STSCertificatePath" value="D:\\numi_web820.pfx"/>
<add key="STSCertificatePassword" value="numi123"/>
```

STSEnabled – anything but “true” will disable STS and revert to access/verify

14. Installing CERMe Software and Database from CERMe Installation CD

Refer to the RM Install Guide PDF file on the CERMe (COTS product) setup CD for detailed instructions on how to set up CERMe (DBA assistance may be required to setup the database, which must be done before application setup).

14.1. Install CERMe on the Application Server

NOTE: Change Healthcare provides version updates several times a year. The example below may not be the latest version

CERMe Review Manager (RM) 19.0 InterQual 2020 for NUMI 15.9 will be installed based on an existing installation of CERMe 18.1. The CERMe installation would be performed using a dump of the existing CERMe 18.1 database. Listed below are the steps to restore the database and install CERME:

1. Restore CERMe 18.1 data from the CERMe database dump obtained from the current CERMe pre-Prod/Production servers. Create database logins for orphaned users in the restored database. Write down the credentials for the new logins created. This will be required for the CERMe install.
   2. Navigate to the CERMe install image and double click the install.htm file in the root directory to open the setup welcome page. This will open the CERMe install page in Internet Explorer.
   3. Click on the Install Review Manager 19.0 / InterQual View 2020 link on the installation page. This will prompt to save or run the file, select Run. This will start the CERMe Install wizard.
   4. Accept the license agreement and click Next.
   5. On the License Information screen, enter the license information given above and click Next.
   6. On the Select Review Manager Enterprise screen, select “Review Manager Enterprise” and click Next.
   7. On the Installation Type screen, select “New Installation” and click Next.
   8. Select an installation directory.
   9. On the Choose Components screen, keep the default selection (i.e., all selected) and click Next.
   10. On the Database Information page, enter the following info and click Next.

- Database type: SQL Server
- Server Name: Name of the SQL database server
- Database: Name of the database to which the dump restored in step 1
- Port Number: SQL Server
- Instance: leave blank
- User ID: SQL Server user ID with access to the CERMe database restored above
- Password: Password for the SQL Server user used above

   11. On separate database to store report data screen, select No and click Next.
   12. On the Install Jetty window, select Yes to install Jetty.
   13. On the next screen, enter 8357 for Port Number.
   14. On the next screen, select the hardware architecture.
   15. Review the selections, and click Install to start the installation.
   16. Once the installation completes, go to the URL: http://<servername>:8357/rm/login.

   This is should open the CERMe login page.

   17. Now follow the steps below to update CERMe to CERMe 19.0.
   18. Stop the CERMe Service from the Windows Services.
   19. Create a backup of the CERMe Installation folder and the CERMe database.
   20. Make the changes to the file (below)on the CERMe Jetty Server:

File: <CERMe Install Folder>\Jetty\etc\webdefault.xml

Add the following element to <session-config> element.

```
<cookie-config>
<http-only>true</http-only>
```

```
</cookie-config>
```

Session Config element should look like the following after the change:

```
<session-config>
<session-timeout>30</session-timeout>
<cookie-config>
<http-only>true</http-only>
</cookie-config>
</session-config>
```

File: <CERMe Install Folder?\Jetty\etc\jetty-rewrite.xml

Add the following <Call> element to the end of the <New> element.

```
<Call name="addRule">
<Arg>
<New class="org.eclipse.jetty.rewrite.handler.HeaderPatternRule">
<Set name="pattern">/*</Set>
<Set name="name">Strict-Transport-Security</Set>
<Set name="value">max-age=31536000; includeSubDomains</Set>
</New>
</Arg>
</Call>
```

The file will look like the following after the change:

```
<Set name="handler">
<New id="Rewrite" class="org.eclipse.jetty.rewrite.handler.RewriteHandler">
<Set name="handler"><Ref refid="oldhandler"/></Set>
<Set name="rewriteRequestURI"><Property name="rewrite.rewriteRequestURI"
default="true"/></Set>
<Set name="rewritePathInfo"><Property name="rewrite.rewritePathInfo"
default="false"/></Set>
<Set name="originalPathAttribute"><Property name="rewrite.originalPathAttribute"
default="requestedPath"/></Set>
<Call name="addRule">
<Arg>
<New class="org.eclipse.jetty.rewrite.handler.HeaderPatternRule">
<Set name="pattern">/*</Set>
<Set name="name">Strict-Transport-Security</Set>
<Set name="value">max-age=31536000; includeSubDomains</Set>
</New>
</Arg>
</Call>
</New>
</Set>
```

File: <CERMe Install Folder>\Jetty\start.ini

Add the following new section to the bottom of the file:

```
# ==========================================================
# Enforce Strict Transport Security
# ----------------------------------------------------------
OPTIONS=rewrite
etc/jetty-rewrite.xml
```

File: <CERMe Install Folder>\Jetty\ReviewManager.xml

Add the content below to the end of the < Config > element

```
<IntegratedLogin Enabled="true" CookieName="unifiedkey"
UnifiedKey="8rzVNfLwjHWHvPctaen9dw=="
AuthenticationFailUrl="/iqm/html/rm_integrated_authentication_failed.htm"
GuidUserCid="IQ_1" Guid="A1B0B165-3C18-4561-935F-5FB81BD42128"
AuthenticateWS="false"/>
```

The modified file will look like the following:

```
…
<Path Prefix="/rm"/>
<Login Check="true"/>
<IntegratedLogin Enabled="true" CookieName="unifiedkey"
UnifiedKey="8rzVNfLwjHWHvPctaen9dw=="
AuthenticationFailUrl="/iqm/html/rm_integrated_authentication_failed.htm"
GuidUserCid="IQ_1" Guid="A1B0B165-3C18-4561-935F-5FB81BD42128"
AuthenticateWS="false"/>
</Config>
</ReviewManager>
```

21. Start CERMe Service from the Windows Services.
22. Go to CERMe URL: http://<server>:8443/rm/login Login with the credential provided, and go to the menu Help > About. It should show Version InterQual Review Manager™ 19 (Build 191).
23. This completes the installation of the CERMe RM 19.0 InterQual 2020.

14.2. Install CERMe SSL Certificate

NUMI will need SSL certificates for CERMe (for Jetty). NUMI uses the SSL certificate for the server that CERMe is running on. If the sever does not have a SSL certificate installed, follow the normal VA processes for obtaining SSL Certificates and install it.

1. Use IIS Manager to export the current certificate to a .pfx file. Select the server name in the Connections pane and double click on the Server Certificates in the IIS pane as shown in Figure 70.

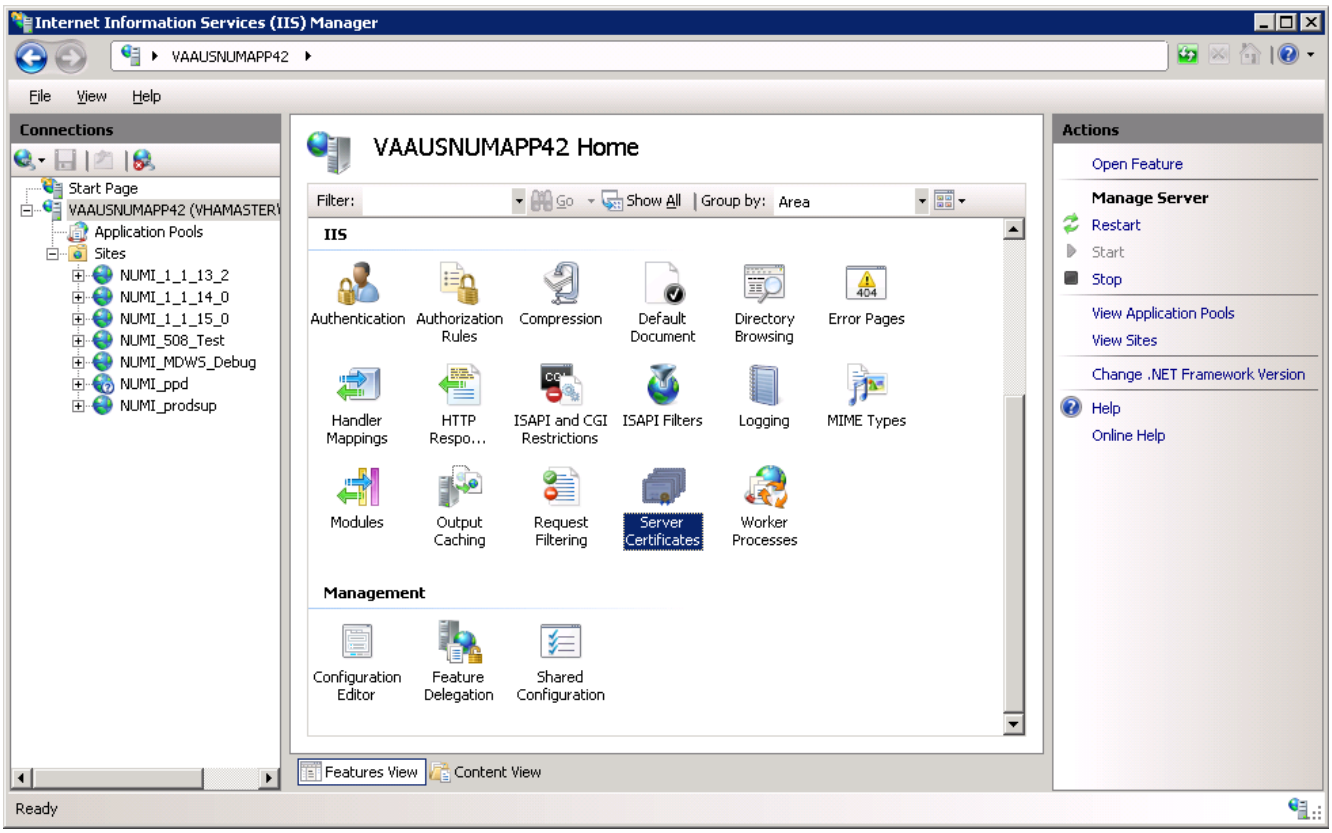


Figure 70: IIS Server Certificates

2. Select the certificate to export and click on the "Export…" link in the Actions pane, as shown in Figure 71.

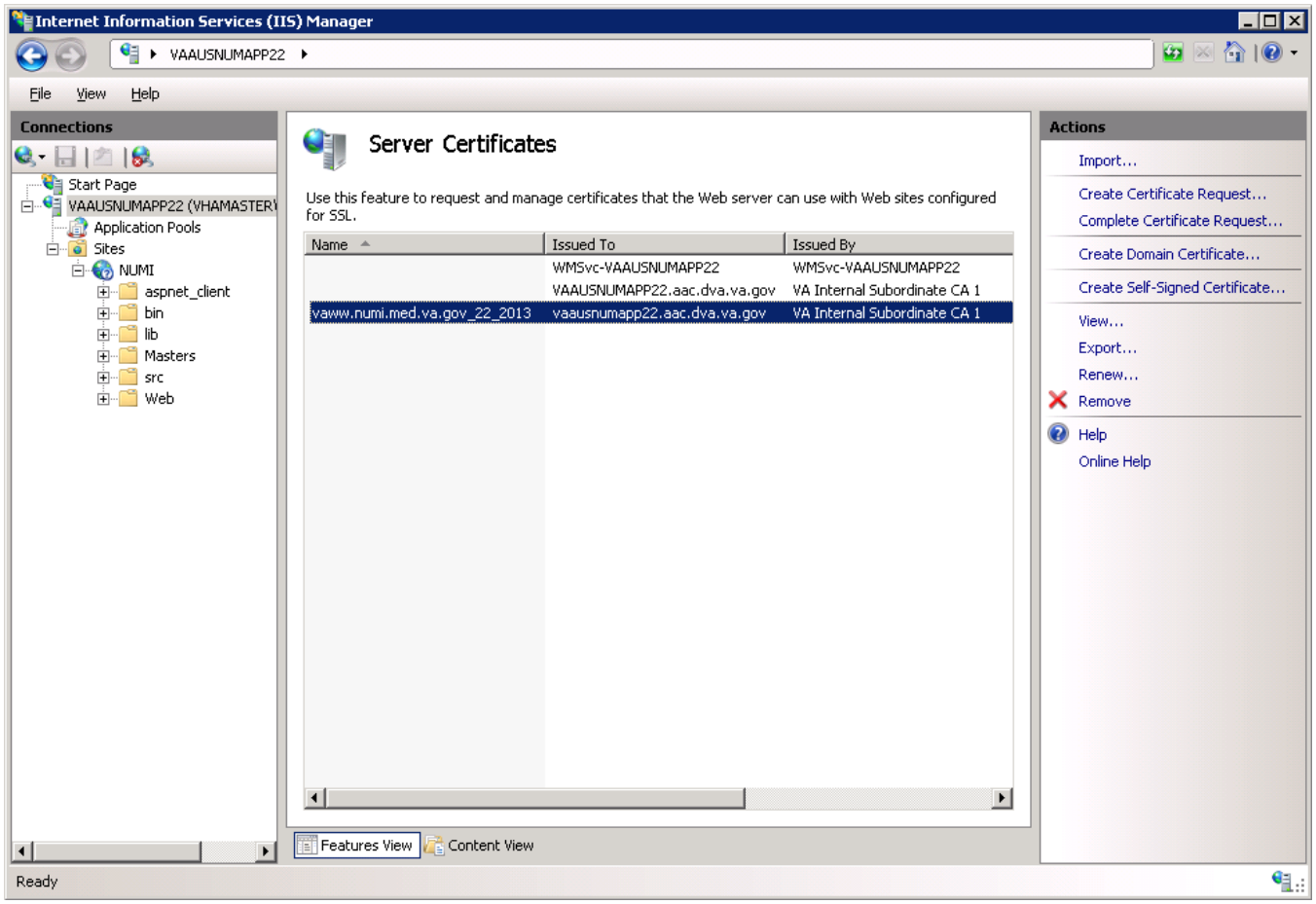


Figure 71: IIS Server Certificate Selection

3. Set the name of the .pfx file. Set the password, e.g., use numi (all lowercase) for the password, as shown in Figure 72. This password will be used in subsequent steps.

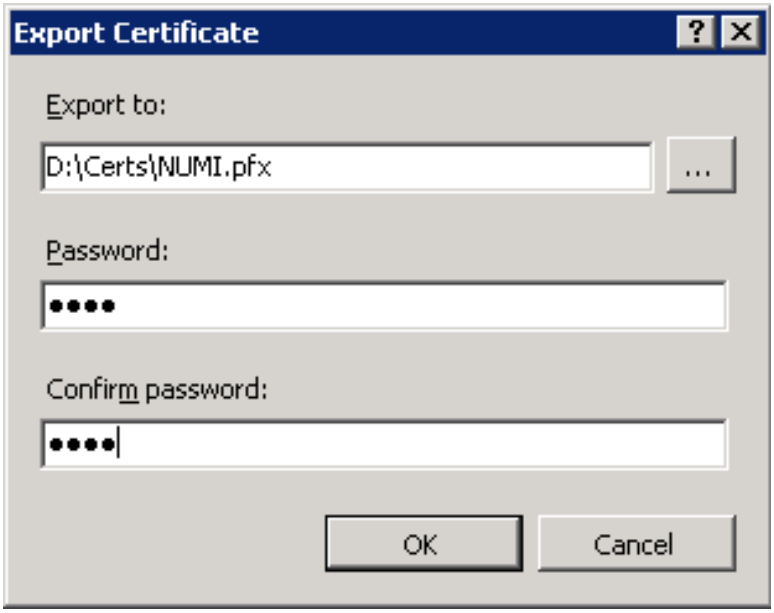


Figure 72: IIS Certificate Details

NOTE: For the following, the password can be whatever you choose, but please make a note of them, as they will be used later. For this example, D:\Certs\NUMI.pfx is the file name and the password, the one that you used to export the .pfx file, e.g., numi (all lowercase).

4. Open a command prompt window and change the current directory to the location of the keytool executable. In this example it would be:

```
D:\Program Files (x86)\Change Healthcare\CERME\Jre\bin\keytool.exe
```

5. Execute the following command:

```
keytool -importkeystore -srcstoretype PKCS12 -srckeystore "D:\Certs\NUMI.pfx" -
destkeystore "D:\Certs\CERME.ks"
```

NOTE: -srckeystore value will be the .pfx path and filename above, -destkeystore can be whatever you choose; again, passwords can be whatever you choose, but please make a note of them. The word "secret" is used as the keystore password in this example.

6. Execute the following command:

```
Keytool –list -keystore "D:\Certs\CERME.ks"
```

Make a note of the long, auto-generated alphanumeric value circled in red below. Recommended actions are to copy, paste the entire command prompt output to notepad to copy, and paste this value.

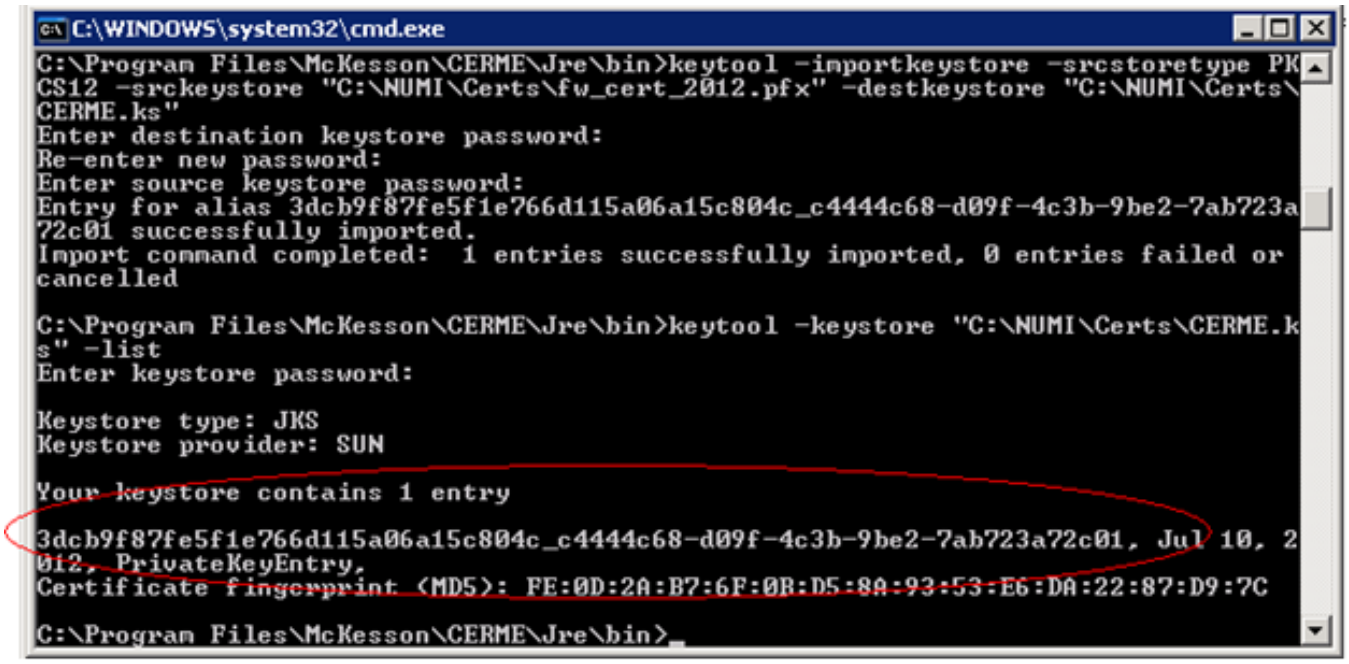


Figure 73: keytool -keystore "C:\Certs\CERME.ks" –list

7. Execute the following command:

```
keytool -changealias -keystore "D:\Certs\CERME.ks" -destalias numi –alias
<alphanumeric value>
```

NOTE: Replace <alphanumeric value> with the value noted and circled from the step above. The keystore password is the password specified when creating the keystore above, secret in our example. The key password is the password specified when creating the pfx file, numi in our example.

8. Execute the following command:

```
keytool -keypasswd -keystore "D:\Certs\CERME.ks" -alias numi
```

NOTE: With this command, we are changing the key password to “reallysecret” for this example.

9. Next, copy the keystore, (D:\Certs\CERME.ks), to the Jetty\etc directory. For this example, it would be here: D:\Program Files (x86)\Change Healthcare\CERME\Jetty\etc.
10. Modify <Jetty-home>\start.ini. Uncomment the relevant lines in the SSL Context and HTTPS Connector sections of start.ini file (as shown in the example below).

```
#=========================================================
# SSL Context
# Create the keystore and trust store for use by
# HTTPS and SPDY
#-------------------------------------------------------------------
jetty.keystore=etc/keystore
jetty.keystore.password=(your password)
jetty.keymanager.password=(your password)
jetty.truststore=etc/keystore
jetty.truststore.password=(your password)
jetty.secure.port=(your SSL port number)
etc/jetty-ssl.xml
#=========================================================
# HTTPS Connector
# Must be used with jetty-ssl.xml
#---------------------------------------------------------
jetty.https.port=(your SSL port number)
etc/jetty-https.xml
```

11. Open the windows services management console, (START->RUN->services.msc->OK), and restart the CERMe service. It will take about 20 to 30 seconds for the service to restart completely but you should be able to browse directly to the secure CERMe. Use whatever URL is used to access NUMI, e.g., https://vaww.prod.temp.numi.med.va.gov/web/home.aspx
12. Replace the “/web/home.aspx” portion with CERMe’ s secure port, (8443 by default), e.g., https://vaww.prod.temp.numi.med.va.gov:8443/

The CERMe website should be displayed and you should not have been warned of the security certificate problem.

15. Setting up NUMI Section in the Windows Event Log

1. Change Directory - Go to command prompt (run as Administrator) and change current directory to Framework v2.0 bit folder e.g., C:\WINDOWS\MS.NET\Framework\v4.5.x
2. Install Command - Type InstallUtil.exe /I < source folder full path >\bin\NumiWebApp.dll under Framework v4.5 folder and press enter.

```
e.g., InstallUtil.exe /i D:\NUMI\<install_dir>\bin\NumiWebApp.dll
```

3. This should create a NUMI section in the Windows Event log.

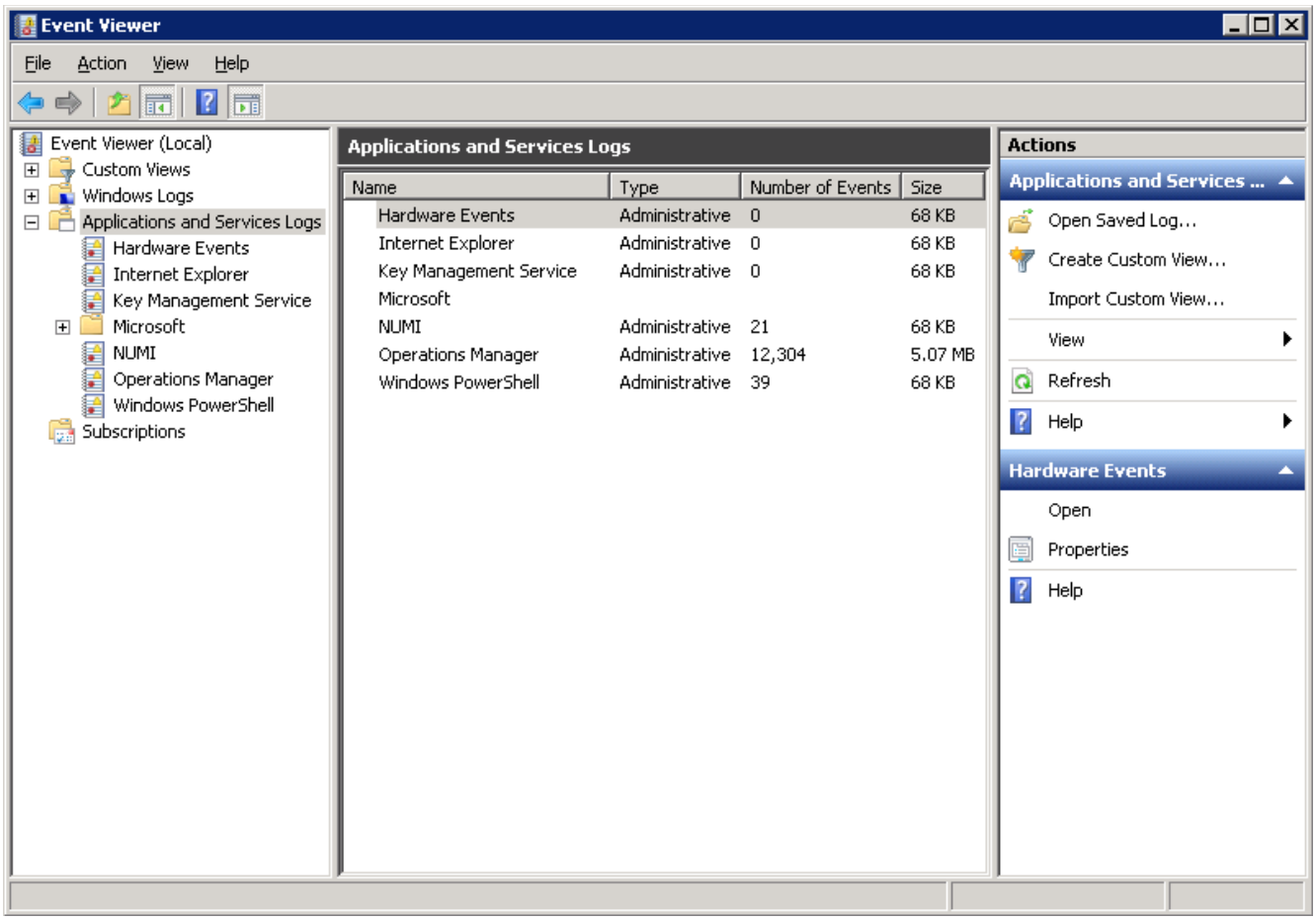


Figure 74: Creating a NUMI section in the Windows Event Log

4. NUMI Event Folder Properties

a. Go to NUMI Properties by right mouse.
b. Click on General Tab under NUMI Properties dialog box window. Check/Click on Overwrite events as needed.
c. Press <Apply> button (if needed) and Press <OK> button.
d. Verify Event View, if any error logs occurred during the installation.

15.1. Validate XML Configuration File Settings

Verify that all XML configuration file settings are correct. Validate NUMI XML Configuration File Settings.

1. Edit the application settings in the web.config file in the NUMI folder. E.g., D:\NUMI\<install_dir>\web.config

Settings to update:

```
<!-- change this setting to point to the appropriate config file for the
deployment. -->
<appSettings
configSource="src\\main\\resources\\xml\\deployment\\numiwebapp.config"/>
<connectionStrings/>
```

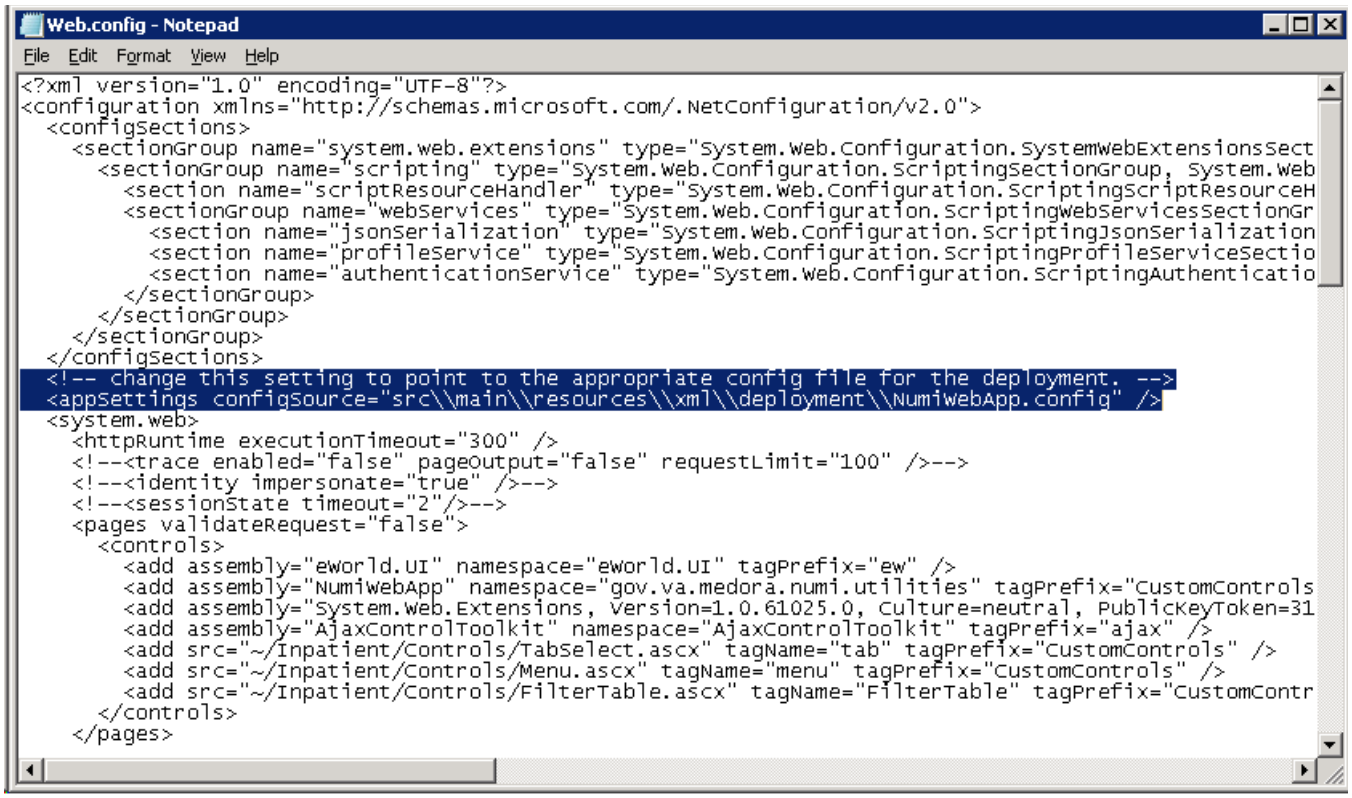


Figure 75: Updating Settings in NUMI XML Configuration File

2. Edit the application settings in the config file indicated in the previous entry. Make sure to enter the VIA configuration properties listed below and the NUMI database server names, and the NUMI database password as indicated.

D:\NUMI\<install_dir>\src\main\resources\xml\deployment\numiweb app.config Settings to update:

```
<!-- VIA Service configuration -->
<add key="VIAServiceURL" value="<VIA Service URL>" />
<add key="VIARequestingApp" value="<Requesting App ID assigned by VIA>"/>
<add key="VIAConsumingAppToken" value="<Consuming App token assigned by VIA>"/>
<add key="VIAConsumingAppPassword" value="<Consuming app password assigned by
VIA>"/>
<add key="numiDbConnectionString" value="Data
Source=<enter_database_server>;Database=NUMI;User
ID=numi_user;Password=xxxxxxxx;Trusted_Connection=False" />
<add key="SSOLogoutUri" value="…" />
```

Modify the value of '`SSOLogoutUri`'setting to one of the URLs from the table below which is based on the installed environment.

Table 5: SSOLogoutUri values

Environment	Value
DEV	https://logon.dev2.iam.va.gov/centrallogin/loggedout.aspx
SQA	https://ssologon.sqa.iam.va.gov/centrallogin/loggedout.aspx
Preprod	https://ssologon.preprod.iam.va.gov/centrallogin/loggedout.aspx
PROD	https://ssologon.iam.va.gov/centrallogin/loggedout.aspx

3. Follow the steps below to encrypt the updated NumiWebApp.config
   a. Open a command prompt and change to .Net Framework 4.x directory (e.g.

```
C:\Windows\MS.NET\Framework64\v4.x.x)
```

b. Run command :

```
.\aspnet_regiis.exe -pef "appSettings"
D:\NUMI\<install_dir>
```

c. The command should execute successfully and give the following message:

```
Encrypting configuration section...
Succeeded!
```

d. Verify that the `src\\main\\resources\\xml\\deployment\\NumiWebApp.config` file does not contain any plain text passwords any more.

NOTE:

Important: Make sure there is no unencrypted copy of the NumiWebApp config file in the server

To make any future changes to the src\\main\\resources\\xml\\deployment\\NumiWebApp.config first decrypt the file by running command:

```
.\aspnet_regiis.exe -pdf "appSettings" D:\NUMI\<install_dir>
```

Make changes to the configuration as needed and follow the above steps to encrypt it again.

16. Perform Restart

Restart IIS

1. Click <Start>.
   2. Click the Command Prompt (or <Run>, depending on the Operating System)
   3. Type: IISReset
   4. Click <Enter>.

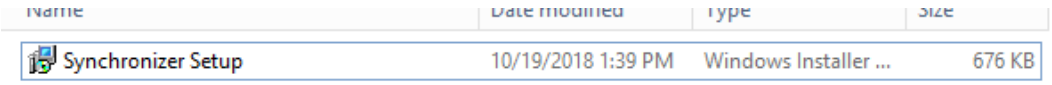
17. Test NUMI Web Site Functionality

Open Internet Explorer and type: http://servername/Web/Home.aspx e.g., https://vaausnumapp40/Web/Home.aspx

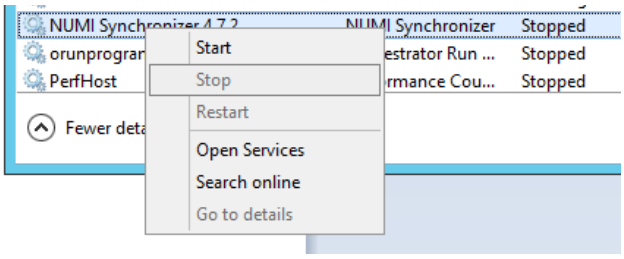
18. Installing NUMI Synchronizer on the DB Server

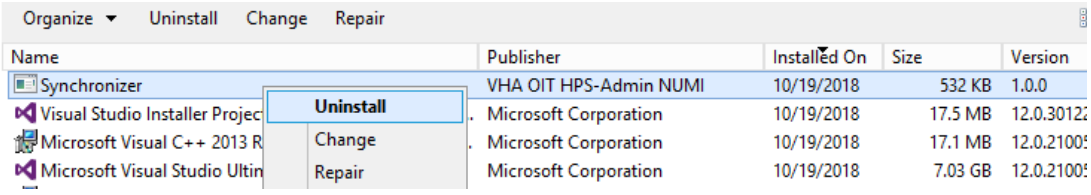
18.1. Installation Instructions

1. Copy the Sychronizer_Setup.msi file to the intended environment. This file will be provided by Tier 3 maintenance and should be stored on each environment



- If an upgrade in place, stop the existing service in task manager and uninstall from program files

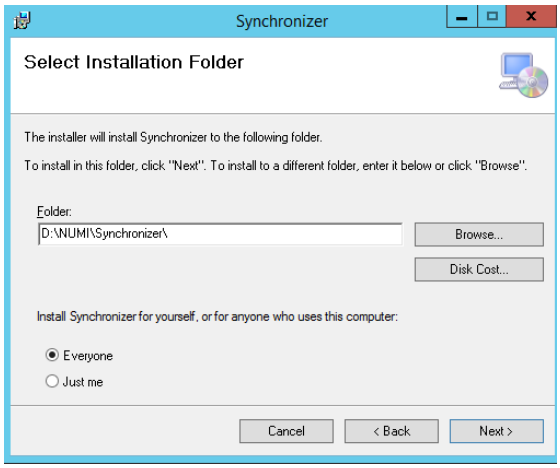




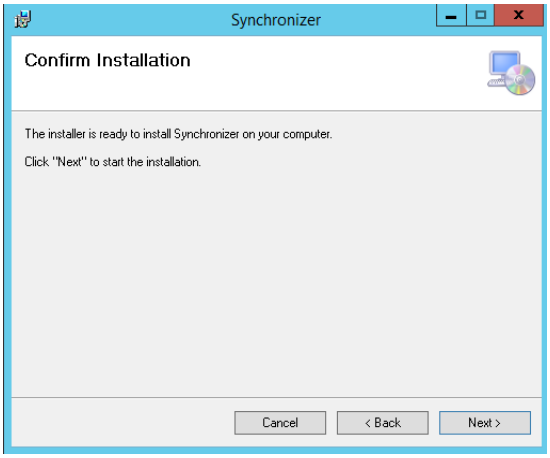
2. Launch the Synchronizer Setup file

3. Click Next

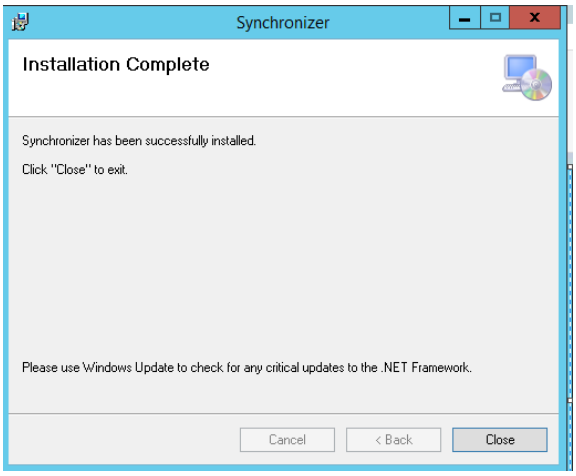
4. Choose the everyone option and browse to the desired directory



5. Click next



6. Click Close



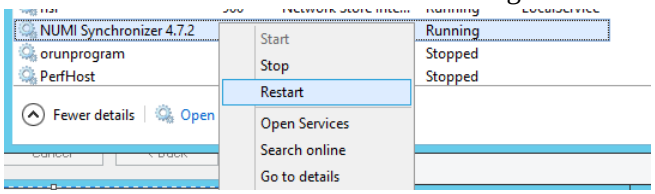
7. Enter the connection information for VIA & NUMI DB into the Synchronizer.config and Sychronizer.exe.config. Use the database server full name in source, e.g. VAAUSNUMSQLXX.aac.dva.va.gov where XX is the number of the database.

<!-- VIA Service configuration -->

<add key="VIAServiceURL" value=" **https://vaww.via.va.gov/via-webservices/services/NumiService**" />

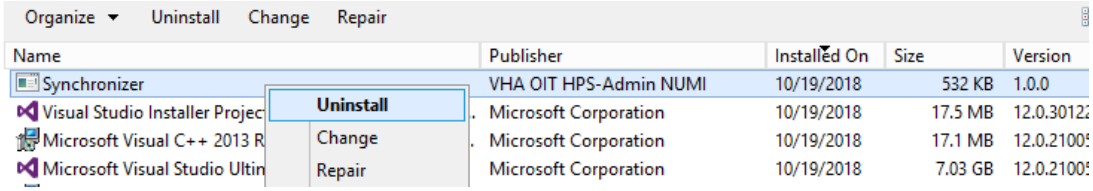
<add key="VIARequestingApp" value="**NumiBatch**"/>
<add key="VIAConsumingAppToken" value="***(SEE PW VAULT)"/> PW Vault under "NUMI Synchronizer PWs (VIARequestingApp)***" **Under NOTES section**
<add key="VIAConsumingAppPassword" value="***(See PW VAULT)"/> PW Vault under "NUMI Synchronizer PWs (VIARequestingApp)***" **Under NOTES section**
<add key="numiDbConnectionString" value="Data Source=***VAAUSNUMSQLXX.aac.dva.va.gov***;Database=***NUMI***;User ID=***numi_user***;Password= ***PW Vault under "NUMI Synchronizer PWs (VIARequestingApp)"NOTES section*** ;Trusted_Connection=False" />
<add key="reportDbConnectionString" value="Data Source=***VAAUSNUMSQLXX.aac.dva.va.gov***;Database=***NUMI***;User ID=**numi_user**;Password=***PW Vault under "NUMI Synchronizer PWs (VIARequestingApp)"*** NOTES section;Trusted_Connection=False" />

8. Restart the service from task manager or the services mmc.



18.2. Uninstall:

If you need to uninstall the NUMI Synchronizer services use add/remove programs and right click on the synchronizer.



18.3. Validate Installation:

To confirm the synchronizer installation

Open MS SQL Server Management Studio after 2 hours. Open a new query and type:

```
Use numi go.
Select TOP 1000 * from patientstay.
```

Click the <Execute> button to run the query. New records shall display.

18.4. Add Jobs to the SQL Server

There are 3 jobs that must be added to the SQL Server:

1. NUMI_PhysicianAdvisorPatientReview_AutoExpire
2. LogSynchDB_ValidateSynchronizer
3. NUMI_AlterIndex_Rebuild

These jobs can be installed from scripts (included in the build) or, if you are transferring from another server, you can right click on each job and script as DROP and CREATE.

Backup the jobs before you run the scripts. Modify the scripts to replace the @owner_login_name with the owner login name appropriate for your installation, if necessary.

NUMI_PhysicianAdvisorPatientReview_AutoExpire is a job that executes the Stored Procedure usp_PhysicianAdvisorPatientReview_AutoExpire every day at midnight. The Stored Procedure looks for Physician UM Advisor (PUMA) Reviews that have not been completed within 14 days and marks them as Completed with a reason description of Expired.

LogSynchDB_ValidateSynchronizer is job that executed the stored procedure LogSyncDB.dbo.usp_LogSync_ValidateSynchronizer every hour. This stored procedure confirms imported stays within the last 3 hours and reports the problem to a pre-defined e- mail distribution list determined by the needs of the installation.

NUMI_AlterIndex_Rebuild is a job that executes the stored procedure NUMI.dbo.usp_AlterIndex_Rebuild. This stored procedure rebuilds the indexes for the tables in the NUMI database.

19. Post-Installation Considerations

If there are post-installation considerations for NUMI, this information will be provided by the appropriate project teams.

20. Acronyms and Descriptions

Acronym	Description
CERMe	Care Enhance Review Management Enterprise
CPRS	Computerized Patient Record System
CPU	Central Processing Unit
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IAM	Identity and Access Management
IIS	Internet Information Services
MDWS	Medical Domain Web Services
NUMI	National Utilization Management Integration
PM	Project Manager
PUMA	Physician UM Advisor
QA	Quality Assurance
SQL	Standard Query Language
SSL	Secure Socket Layer
SSO	Single Sign On
UM	Utilization Management
URL	Uniform Resource Locator
VIA	VistA Integration Adaptor
VistA	Veterans Information Systems Technology Architecture

21. Numi Comparison Table

NUMI Version	CERMe RM	InterQual View	CA SiteMinder	Windows Server	MS SQL Server
15.4	16.1	2017.2	12.51	2012 R2	2012
15.5	17	2018.1	12.51	2012 R2	2012
15.6	17	2018.1	12.51	2012 R2	2012
15.8	18.1	2019.1	12.51	2012 R2	2012
15.9	19.0	2020	12.51	2012 R2	2012