

National Utilization Management Integration (NUMI) Server Setup Guide



Version 1.1

March 2026

Department of Veteran Affairs

Office of Information and Technology (OIT)

Revision History

Date	Description	Author
03/12/2026	Updated SSOi SiteMinder to EntraId	REDACTED
08/06/2025	Updated Title Page and Footer to remove Minor versioning	REDACTED
07/01/2025	Updated release version number to 15.17	REDACTED
01/23/2025	Updated release version number to 15.16	REDACTED
05/16/2024	Updated release version number to 15.15	REDACTED
01/24/2024	Updated release version number to 15.14	REDACTED
11/1/2023	Updated release version number to 15.13	REDACTED
1/10/2023	Updated release version number to 15.11	REDACTED
7/7/2022	Updated CERMe RM 21.0.1 and InterQual View version 2022	REDACTED
11/15/2021	Updated release version number to 15.10	REDACTED
8/16/2021	Updated CERMe RM 20.0 and InterQual View version 2021	REDACTED
12/03/2020	Updated release version number (15.9.1) in footer and title. Month and year updated both in title and footer.	REDACTED
5/28/2020	Updated CERMe RM and InterQual View version (19.0/2020)	REDACTED
2/1/2020	Updated release version number (15.9)	REDACTED
08/28/2019	Updated release version number and added STS integration information (Section 13).	REDACTED
10/1/2018	Updated release version number (15.6)	REDACTED
04/23/2018	Update release version number (15.5)	REDACTED
02/19/2018	Updated release version number (15.7) and new Synchronizer installation instructions.	REDACTED
11/14/2017	Updated release version number (version 15.4) and CERME upgrade installation steps	REDACTED
5/25/2017	Reviewed document and revised	REDACTED, REDACTED
3/27/2017	Added CA WebAgent setup instructions	REDACTED
3/1/2017	Updates for IAM SSO integration changes	REDACTED
2/3/2017	Added steps to encrypt the configuration files	REDACTED
9/20/2016	Updated install instructions for 15.0 and updated CERME installation instructions and IIS and File service installation screenshots	REDACTED
09/12/2016	Updating document for NUMI 14.4 and .NET version. Made the Windows version generic	REDACTED
11/12/2015	Updated the version number from 14.2 to 14.3	REDACTED

Date	Description	Author
5/11/2015	Updated the version number from 14.1 to 14.2	REDACTED
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	REDACTED
8/2/2013	Removed references to CERMe 2012. Changed hard coded build name directory references to <install_dir>.	REDACTED
7/2/2013	Changed example directory references to remove 14.0	REDACTED
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.	REDACTED
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; 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.	REDACTED
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.	REDACTED
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.	REDACTED
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,	REDACTED

Date	Description	Author
	Installation During Off Peak Hours. Also reordered installation steps SQL and CERMe (now section 6.1 and 6.14) and added CERMe SSL	
03/25/2013	Modified section 6.15 for NUMI event folder, modified section 6.19	REDACTED
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	REDACTED
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	REDACTED
04/10/2012	Draft preliminary update for	REDACTED
10/13/2011	Updated CERME instructions in	REDACTED
08/24/2011	Refined MDWS instructions in section 6.12-6.15 per AITC	REDACTED
08/04/2011	Refined CERME instructions in section 6 per AITC Windows SA	REDACTED
08/02/2011	Updated section 9.9 per AITC	REDACTED
08/01/2011	Updated per issues found in AITC	REDACTED
08/28/2009	Updated document name to	REDACTED
07/14/2009	Updated to reflect "Release 1.1"	REDACTED
04/22/2009	Submitted to Medora Team for	REDACTED

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	3
3.1	Installation Process Requirements.....	3
3.1.1	Minimum Software Version.....	3
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	5
4.	Database Information	6
4.1.	Instructions for Installing Database Components.....	6
4.1.1	Database Installation / Restoration Procedures.....	6
5.	Installation Procedure for Server 2019	7
5.1.	Patch the Operating System	7
6.	SQL Server Setup (Windows Server 2019).....	7
6.1.	Role Setup	7
7.	Web Server Setup (Windows Server 2019)	8

7.1.	Role Setup	8
7.2.	ASP.NET 2.0 AJAX Extensions 1.0 Setup	11
7.3.	MS Web Services Enhancements (WSE) 3.0 Setup	11
8.	Application Server Setup (Windows Server 2019)	11
8.1.	Role Setup	11
8.2.	Feature Delegation.....	13
8.3.	Install MS ASP.Net 2.0 AJAX Extensions 1.0.....	14
8.4.	Install MS Web Services Enhancements 3.0	18
9.	Install SQL Server.....	22
9.1.	Download all SQL Server Patches.....	22
9.2.	Restore the Appropriate Databases for the NUMI Application.....	22
10.	Installing NUMI Exchange on Server 2019.....	23
10.1.	Unzip/Install NUMI Exchange Distribution.....	23
10.2.	NUMI Exchange Website Configuration	23
10.2.1	Application Pool Configuration	27
11.	Installing NUMI on Server 2019	30
11.1.	Software Copy Instructions.....	30
11.2.	NUMI Web Site Configuration.....	31
11.3.	Application Pool Configuration.....	36
12.	Microsoft Entrald Application Registration for the Web Server Configuration.....	40
12.1.	Microsoft Entrald Application Registration.....	40
13.	Secure Token Service Integration for SSOi	43
13.1.	Download Certificate Chain from appropriate endpoint	43
13.2.	Export server cert to .pfx.....	47
13.2.1	Load the Microsoft Management Console, Certificate Snap-in, for the local computer	47
13.3.	NumiWebApp.config keys	50
14.	Installing CERMe Software and Database from CERMe Installation CD.	50
14.1.	Install CERMe on the Application Server.....	50
14.2.	Install CERMe SSL Certificate	53
15.	Setting up NUMI Section in the Windows Event Log	58
15.1.	Validate XML Configuration File Settings	59

- 16. Perform Restart 61**
- 17. Test NUMI Web Site Functionality 61**
- 18. Installing NUMI Synchronizer on the Web Server..... 61**
 - 18.1. Installation Instructions..... 61**
 - 18.2. Uninstall: 63**
 - 18.3. Validate Installation: 63**
 - 18.4. Add Jobs to the SQL Server..... 63**
- 19. Post-Installation Considerations 64**
- 20. Acronyms and Descriptions 65**
- 21. NUMI Comparison Table 65**

List of Tables

Table 1: CPRS Rights.....	4
Table 2: CPRS Access Tabs	4

List of Figures

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

Figure 39: Application Pool Window.....	37
Figure 40: NUMI Application Pool Basic Settings.....	38
Figure 41: NUMI Application Pool Advanced Settings.....	39
Figure 42: Microsoft Entrald Application Registration	40
Figure 43: Application Registration Client Secret.....	41
Figure 44: Entrald Application Registration Redirect URIs.....	42
Figure 45: IIS Server Certificates.....	54
Figure 46: IIS Server Certificate Selection.....	55
Figure 47: IIS Certificate Details	56
Figure 48: keytool -keystore "C:\Certs\CERME.ks" -list.....	57
Figure 49: Creating a NUMI section in the Windows Event Log.....	59
Figure 50: Updating Settings in NUMI XML Configuration File	60

1. Introduction

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

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 2019 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 2019 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 2019
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 2019 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 2019 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) 22.0 InterQual View 2025 application
4. Install the NUMI application
5. Change the web.config file settings as needed

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 2019

Database: SQL Server 2019

3.1.2 Resources Required

Sys Admin, DBA

3.1.3 CPU Capacity

64GB RAM, Dual 2.20 GHz Intel Xeon® E5-2698 v4 – Database Server

12GB RAM, Dual 2.20 GHz Intel Xeon® E5-2698 v4 – Application Server

12GB RAM, Dual 2.20 GHz Intel Xeon® E5-2698 v4 – Web Server

3.1.4 Disk Space

Application server – 100 GB Web Services server – 100 GB

Database – E:900 GB, F:700 GB, L:200 GB, O:400 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 NUMI database 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 2019

This section identifies the installation procedures that shall be followed.

5.1. Patch the Operating System

This applies to all servers.

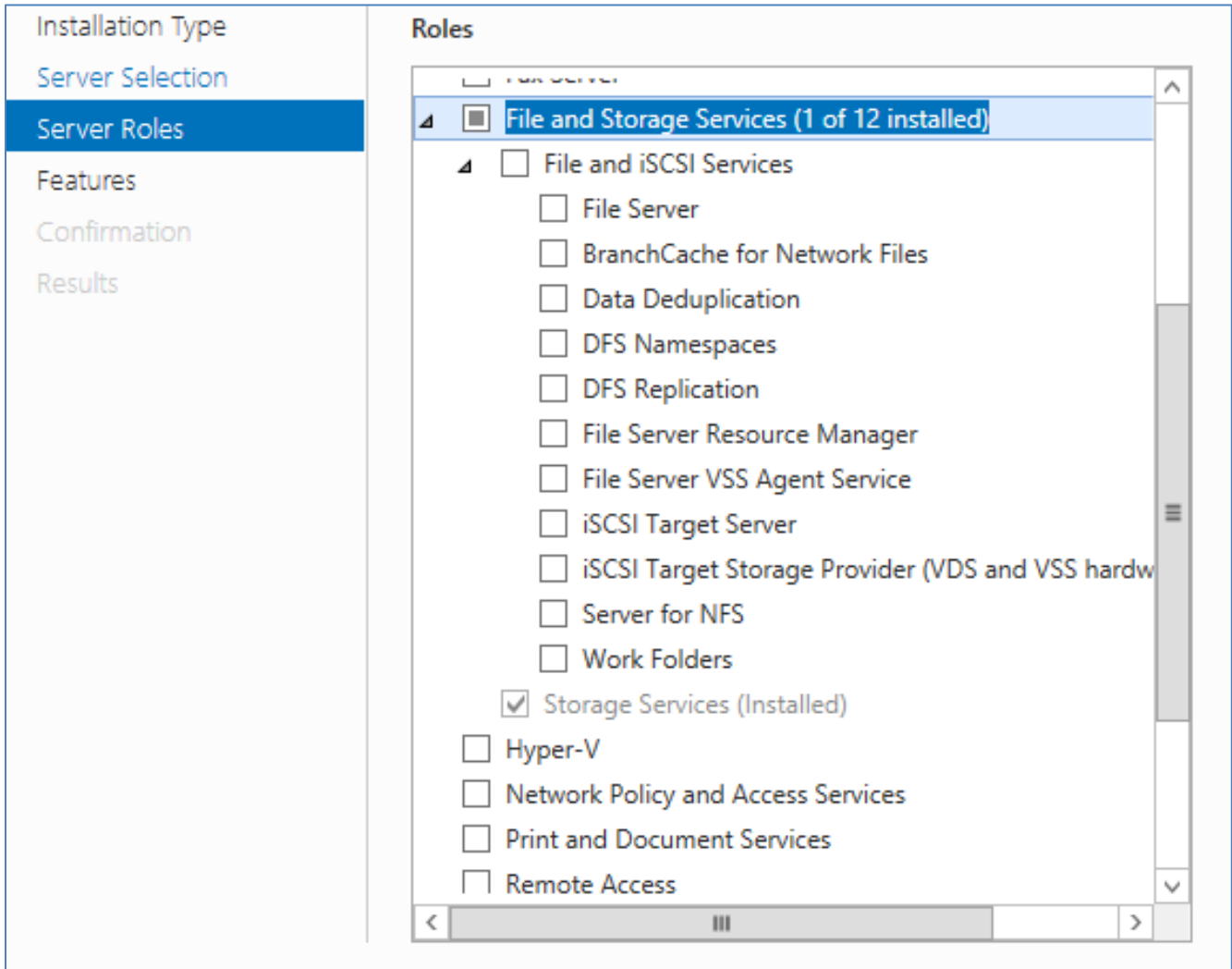
1. Open up an instance of Internet Explorer.
2. Select menu item <Tools/Windows Update>.
3. Follow the instructions on MS's website. (**NOTE:** A restart of the servers may be necessary).

6. SQL Server Setup (Windows Server 2019)

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 2019)

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

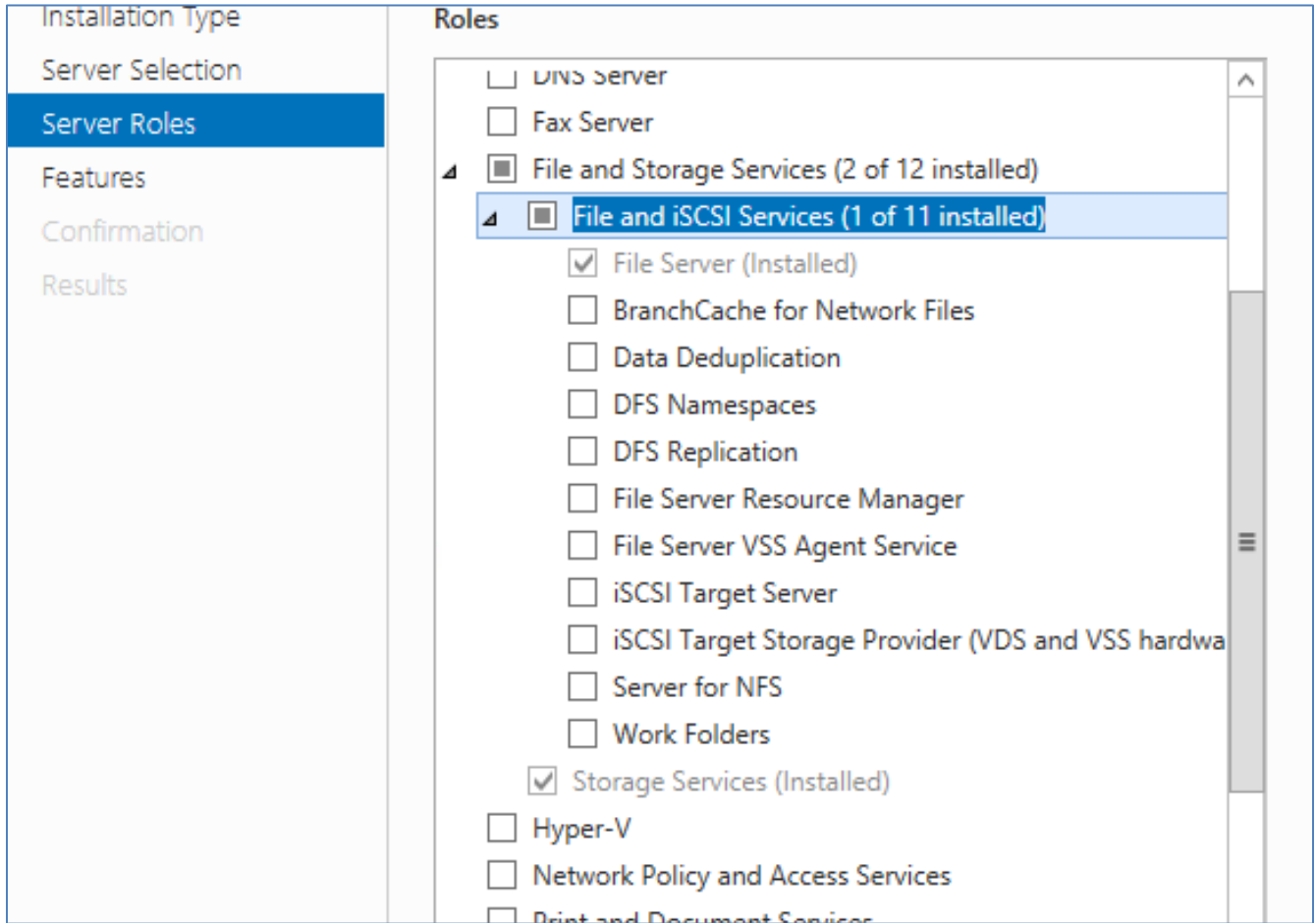
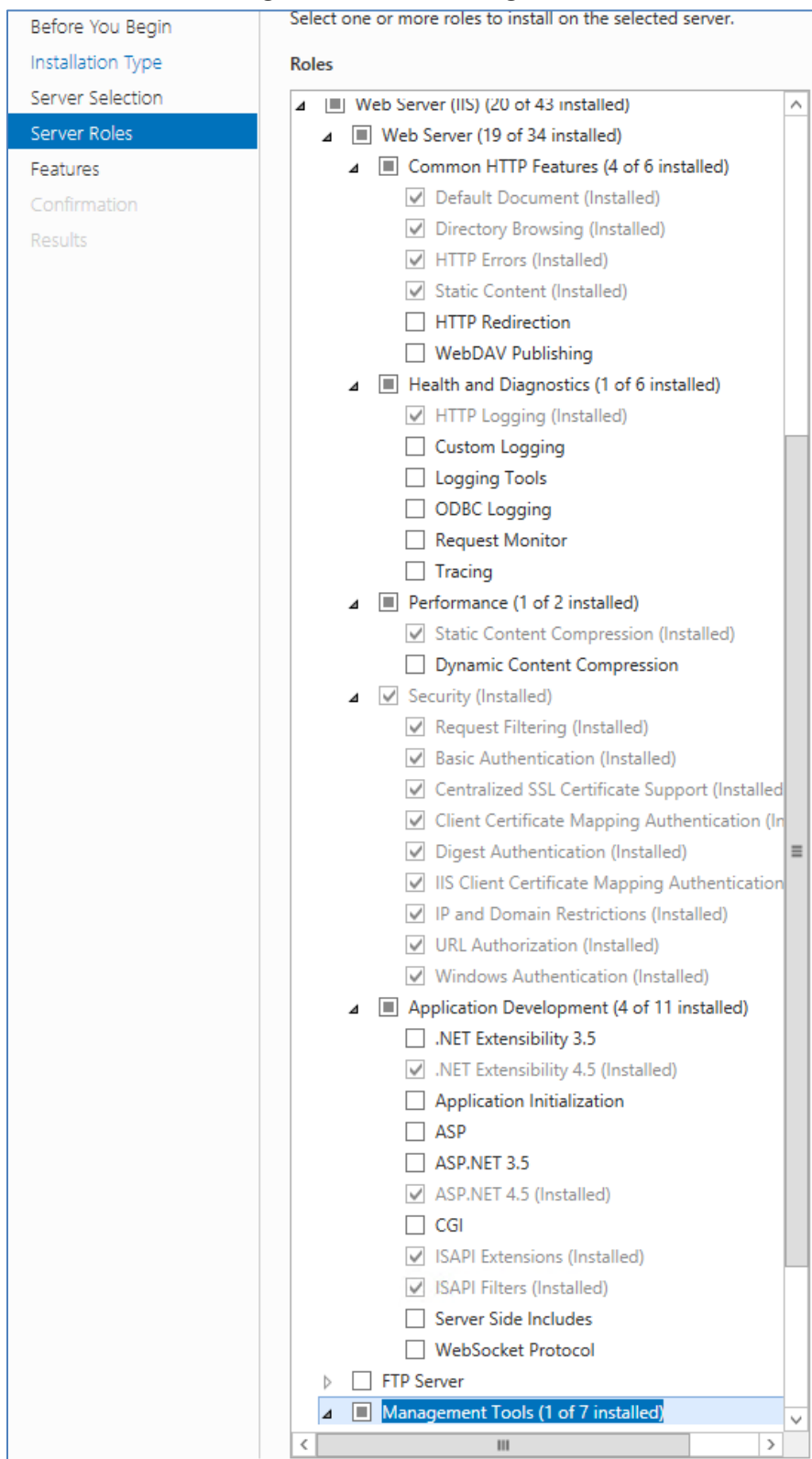


Figure 3: NUMI Exchange (IIS)



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 2019)

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 **Error! Not a valid bookmark self-reference.** and Figure 5: NUMI Web Services IIS.

Figure 4: NUMI Role Services

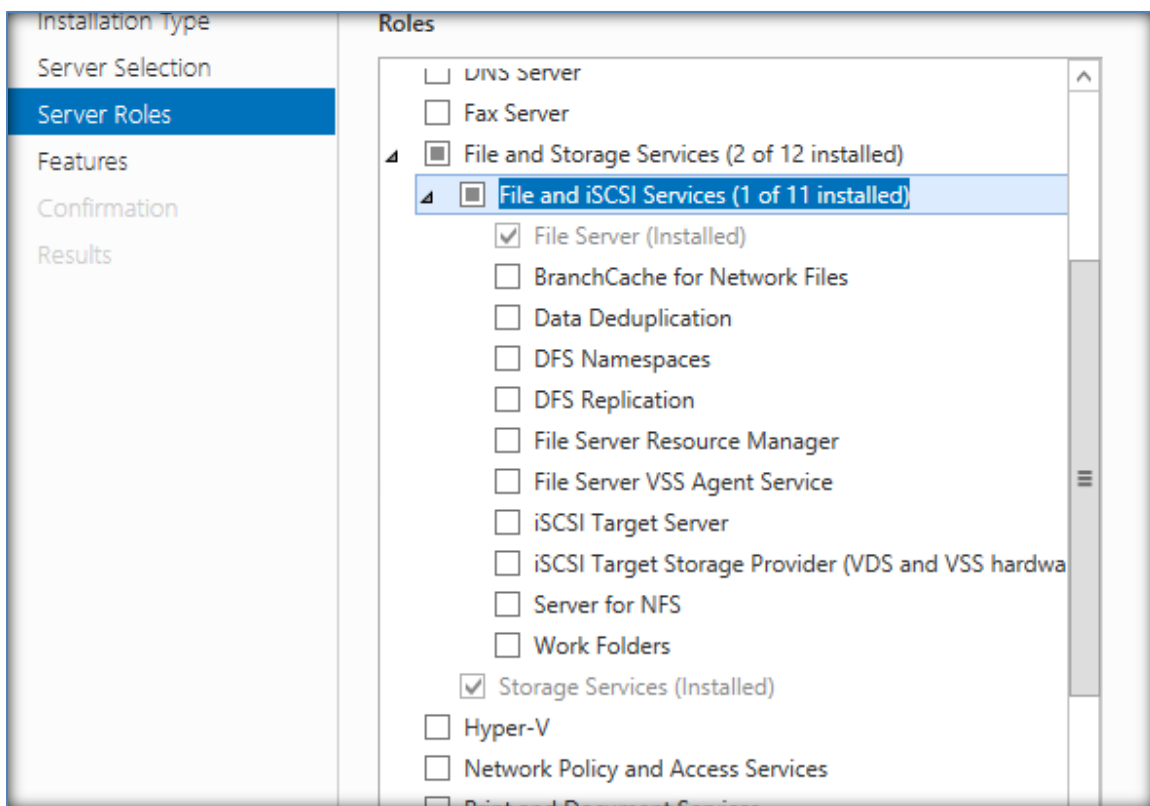
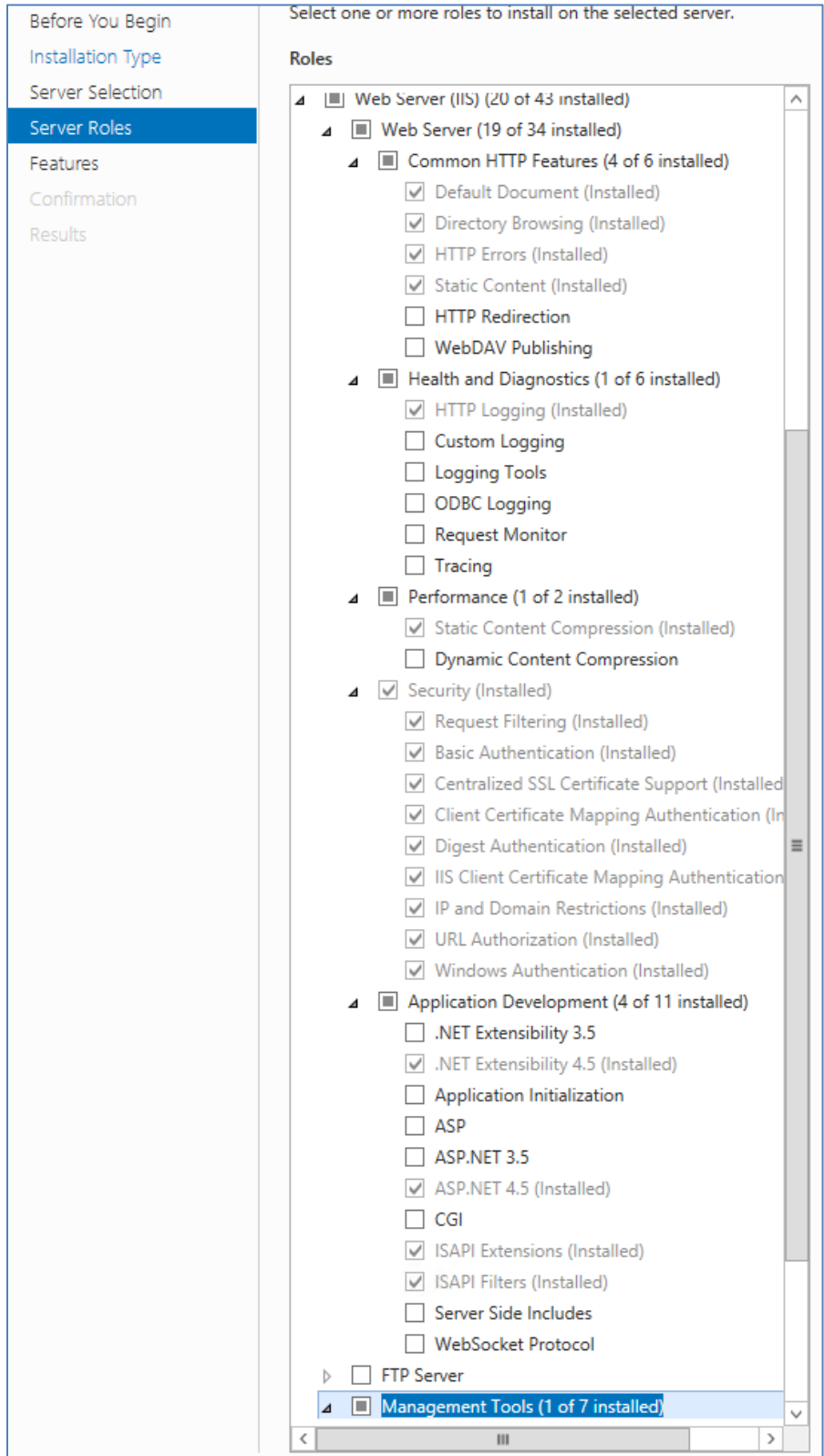


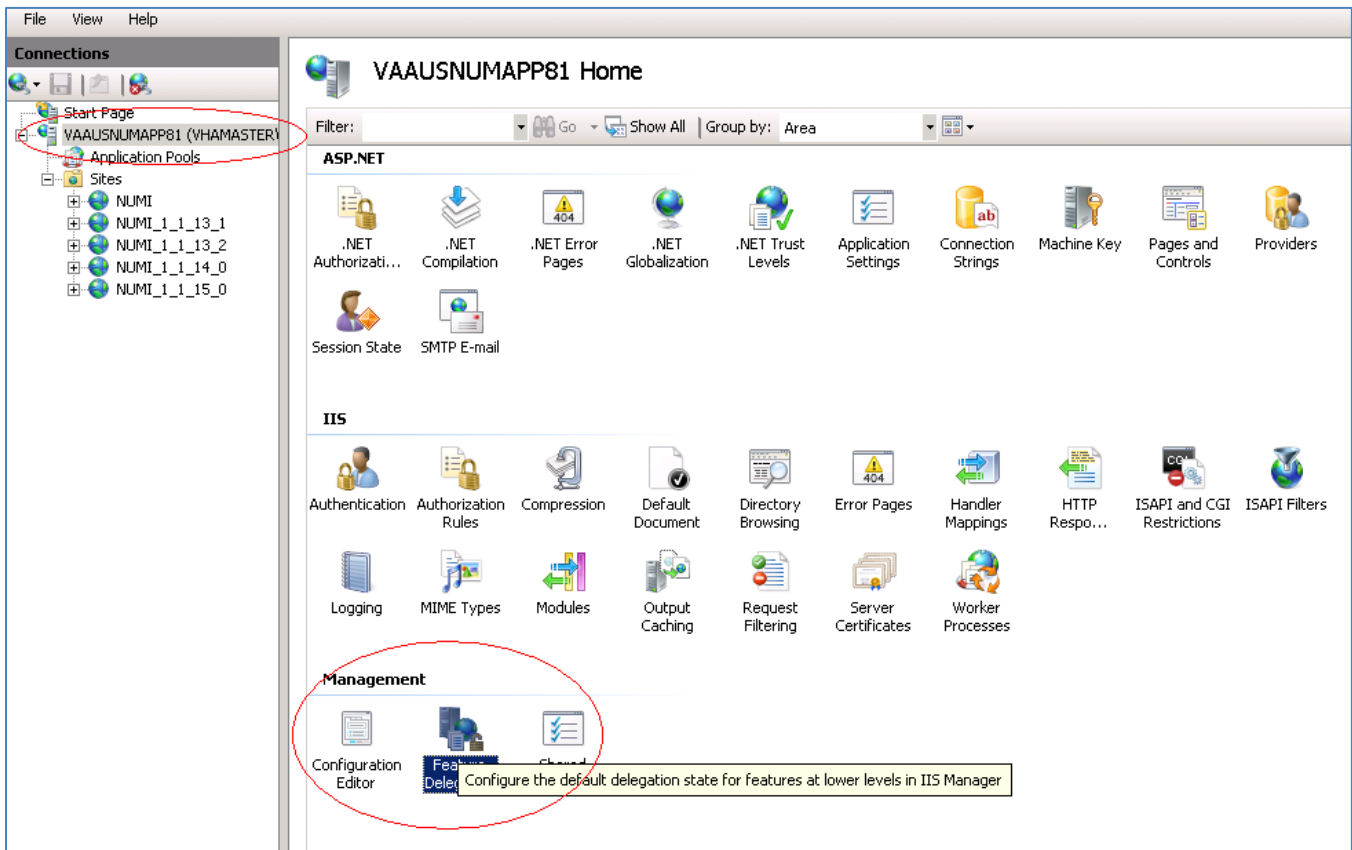
Figure 5: NUMI Web Services IIS



8.2. Feature Delegation

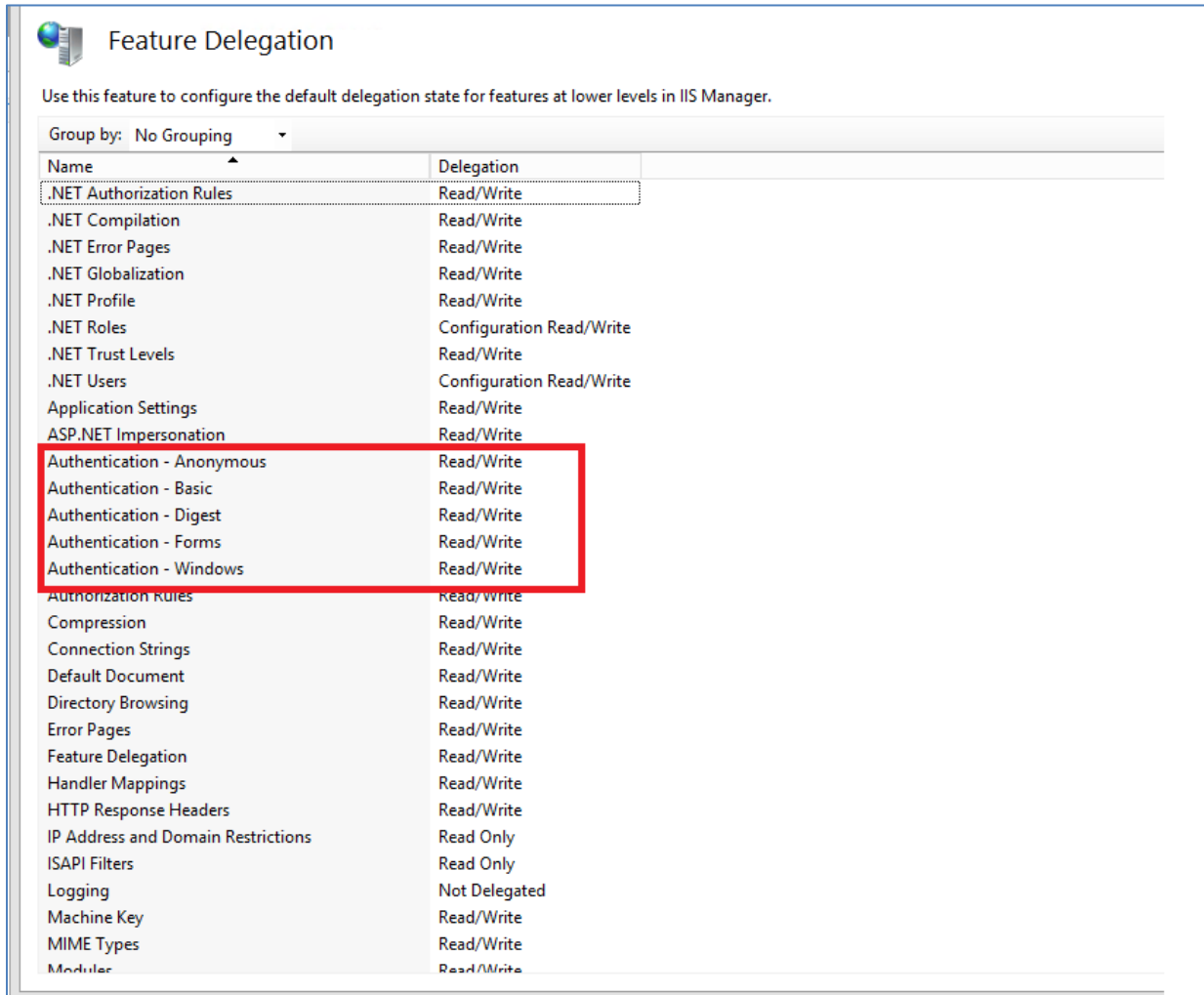
Select the main node in IIS, with the server name. Then double click on “Feature Delegation” item. Change the “Feature Delegation” settings for the server, as shown in Figure 6: IIS Feature Delegation.

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

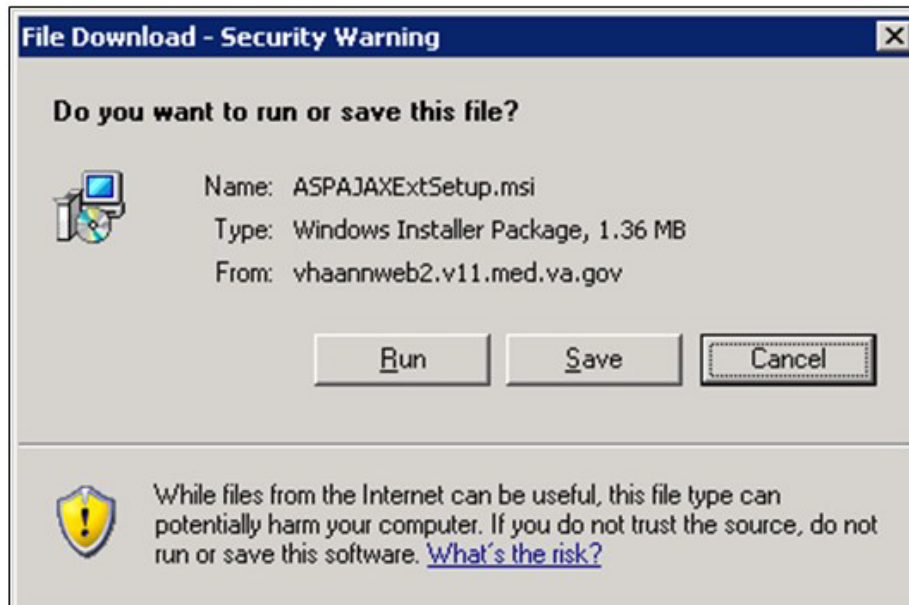


8.3. Install MS ASP.Net 2.0 AJAX Extensions 1.0

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



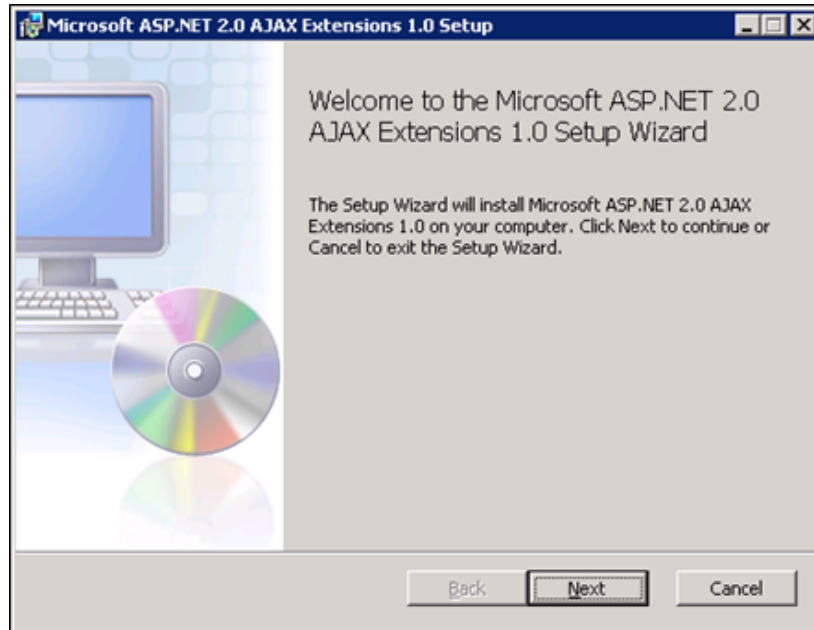
4. When the Internet Explorer – Security Warning window displays, click the <Run> button (shown in Figure 9: MS ASP.Net 2.0 Internet Explorer-Security Warning Window).

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).

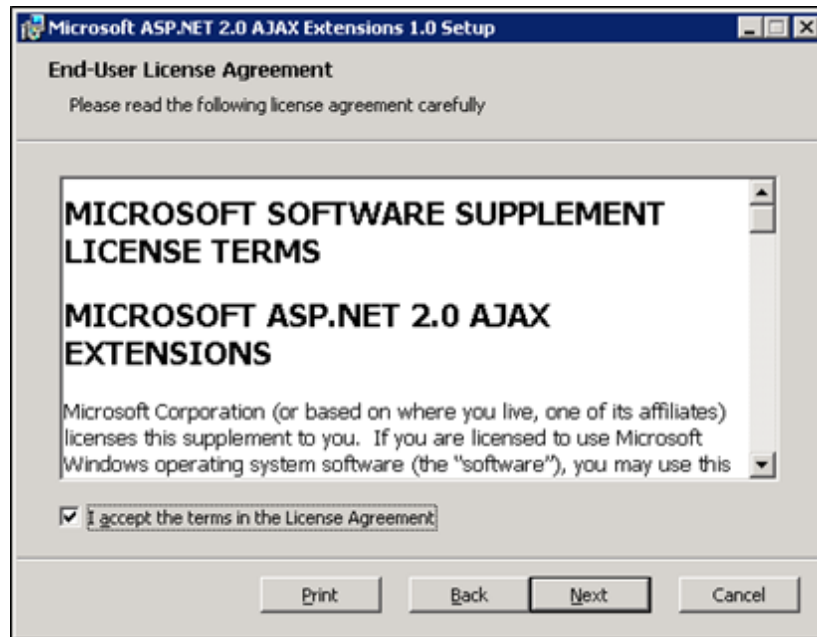
Figure 10: MS ASP.NET 2.0 AJAX Extensions 1.0 Setup Wizard Window



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.

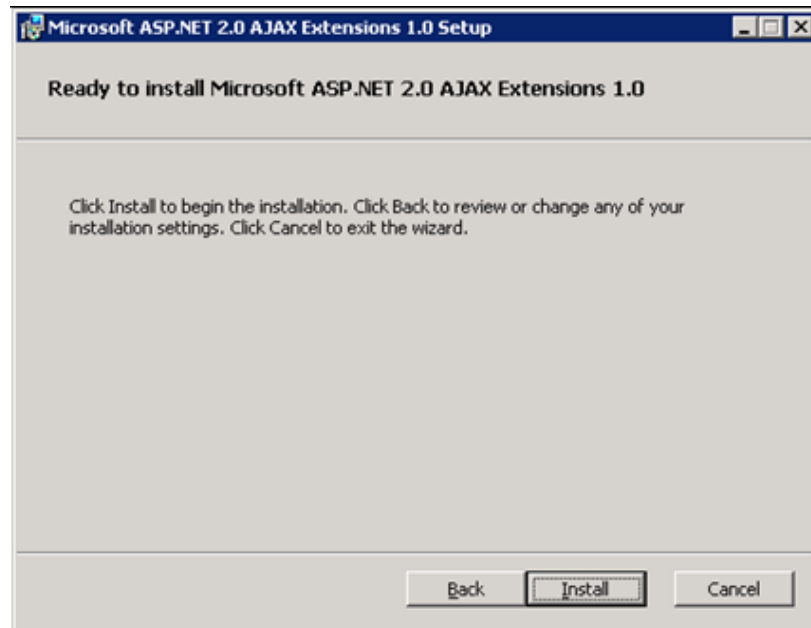
1. Click the <Next> button.

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

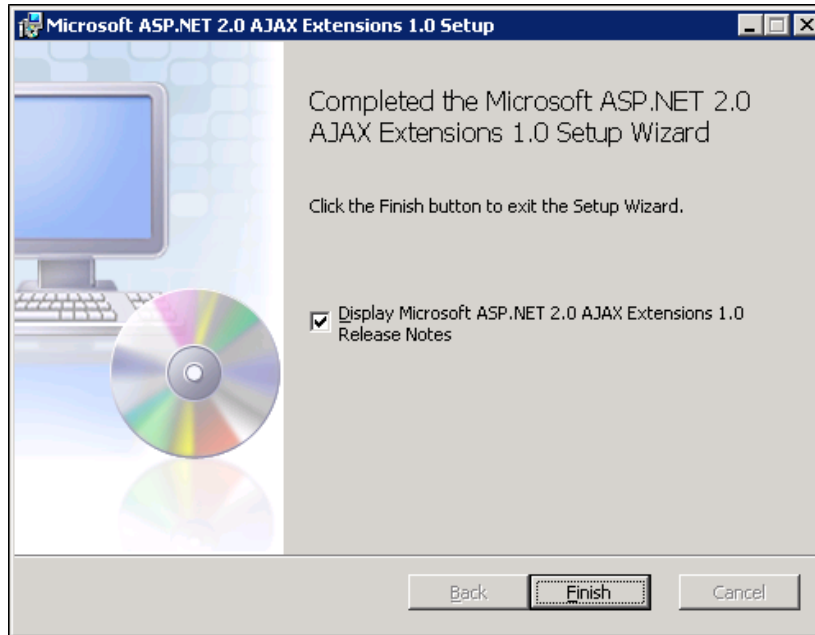


3. The installation is complete. Select the <Finish> button by clicking on it to exit the installation wizard, as depicted in Figure 13: MS ASP.NET 2.0 AJAX Completion window.



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

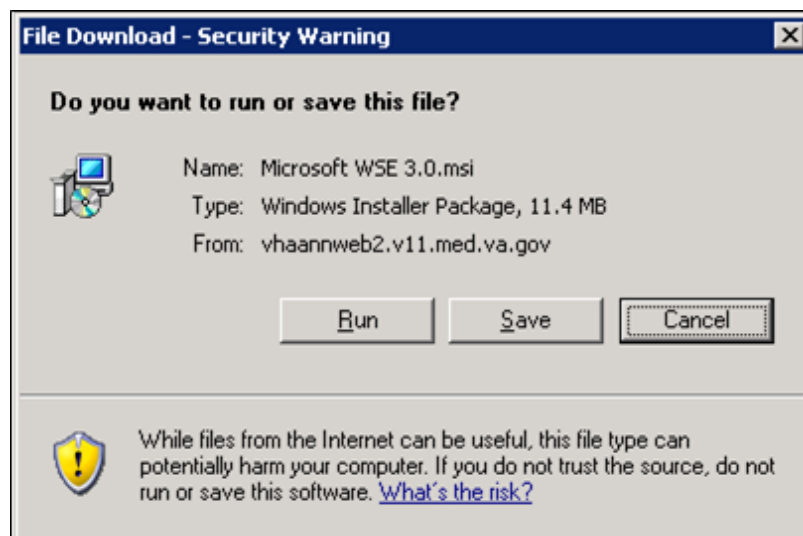


8.4. Install MS Web Services Enhancements 3.0

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



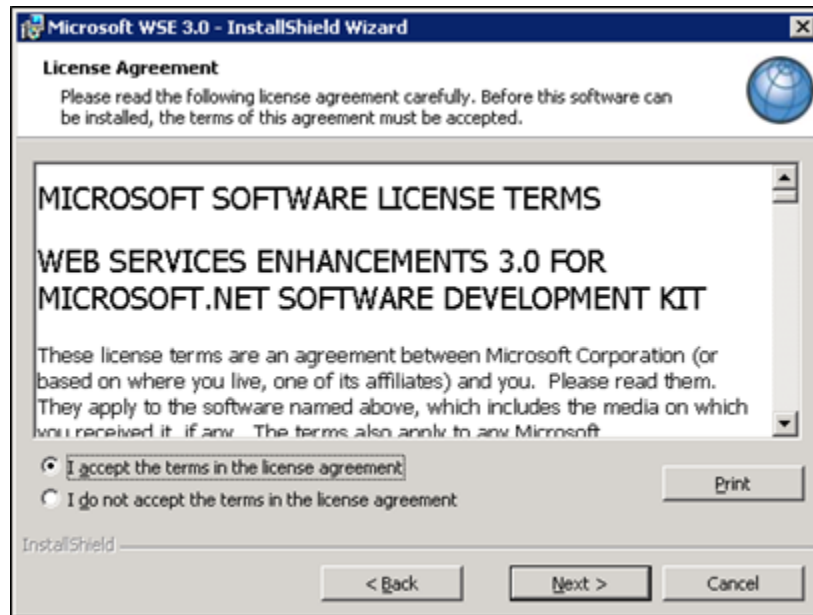
5. When the MS WSE 3.0 – InstallShield Wizard window displays, click the <Next> button (shown in Figure 16: MS WSE 3.0 InstallShield Wizard Welcome Window).

Figure 16: MS WSE 3.0 InstallShield Wizard Welcome Window



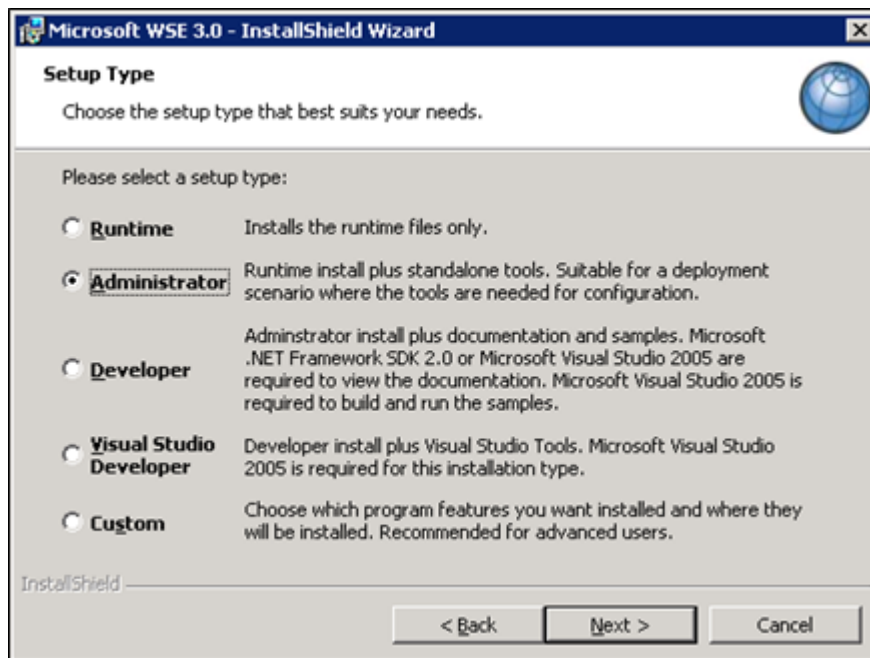
6. Click the "I accept the terms in the license agreement" checkbox, as illustrated in Figure 17: MS WSE 3.0 License Agreement Window.
7. Click the <Next> button.

Figure 17: MS WSE 3.0 License Agreement Window



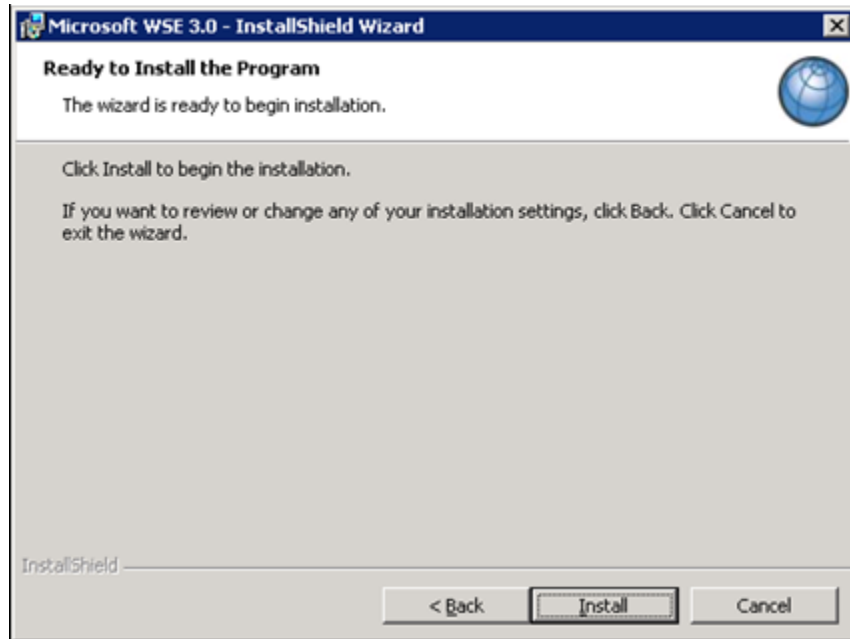
8. Click the <Administrator> radio button, as illustrated in Figure 18: MS WSE 3.0 InstallShield Wizard Window.
9. Click the <Next> button.

Figure 18: MS WSE 3.0 InstallShield Wizard Window



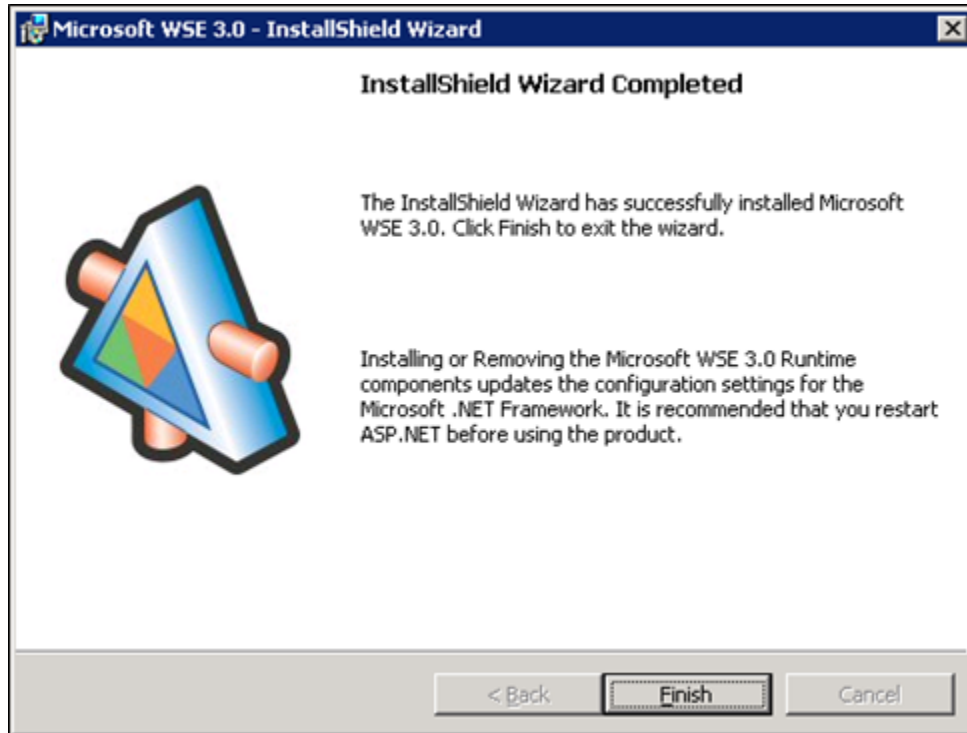
10. Click the <Install> button (shown in Figure 19: MS WSE 3.0 Installation Window).

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 2019 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 2019



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.

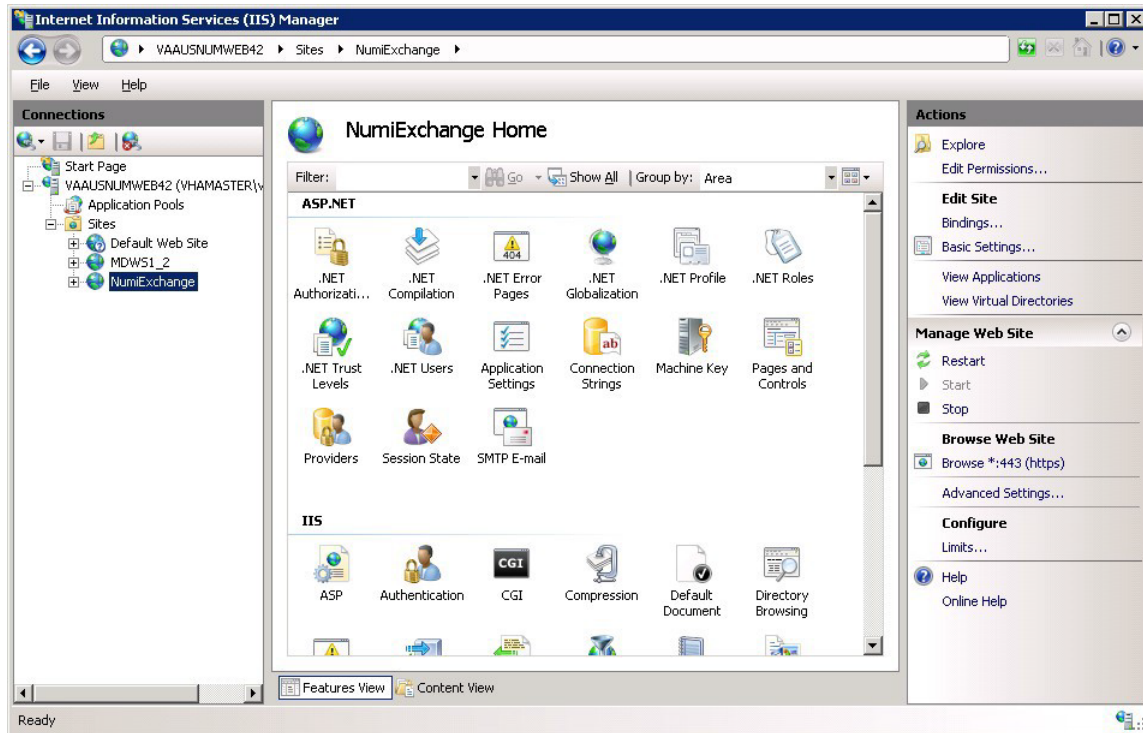
10.2. NUMI Exchange Website Configuration

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

The screenshot shows the 'Add Web Site' dialog box in IIS Manager. The 'Site name' field is set to 'NumiExchange' and the 'Application pool' is set to 'NumiExchange'. The 'Content Directory' section shows the 'Physical path' as 'D:\NumiExchange\NUMI_Increment6_Sprint2_Build_2'. The 'Binding' section is configured with 'Type' set to 'https', 'IP address' set to 'All Unassigned', and 'Port' set to '443'. The 'SSL certificate' is set to 'VAAUSNUMWEB81.aac.dva.va.gov'. The 'Start Web site immediately' checkbox is unchecked. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

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

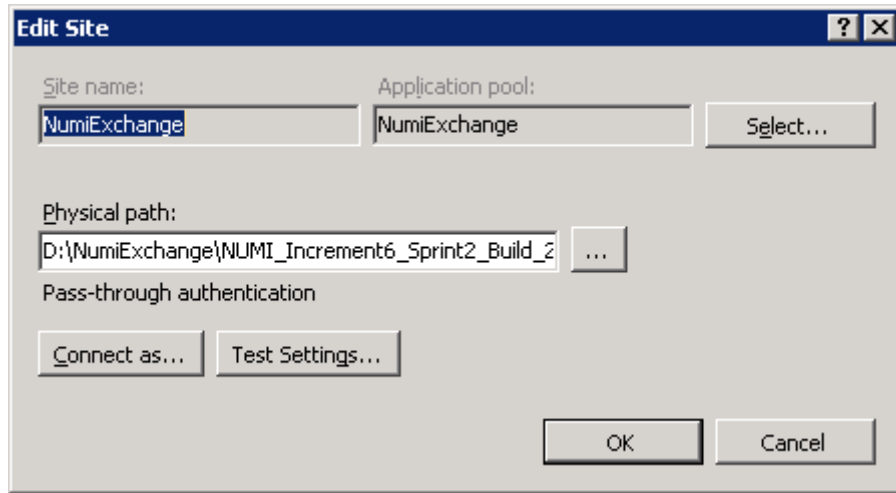
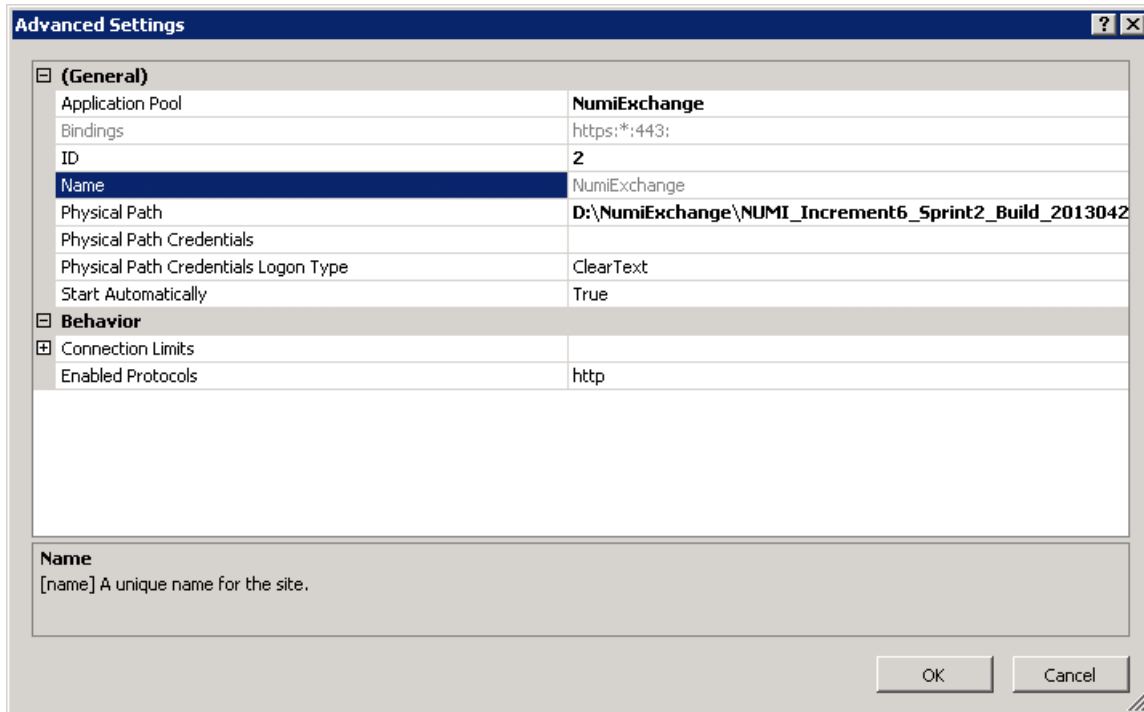
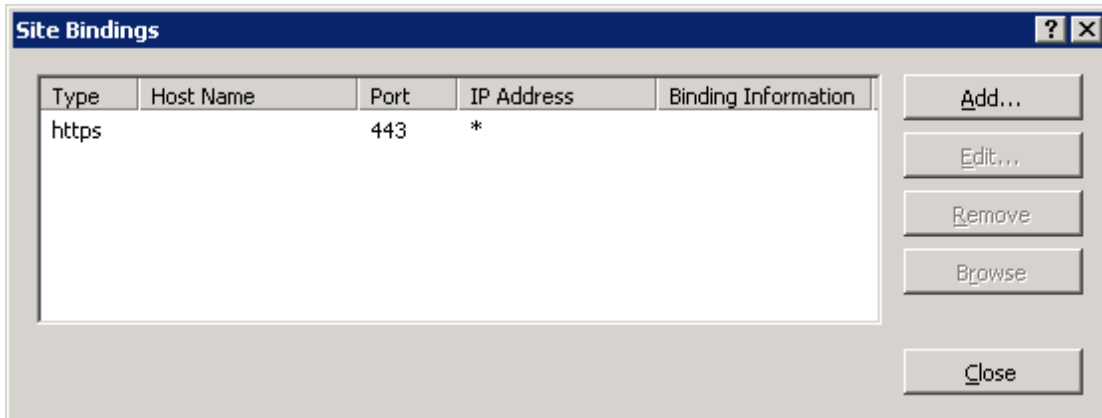


Figure 24: NUMI Advanced Settings



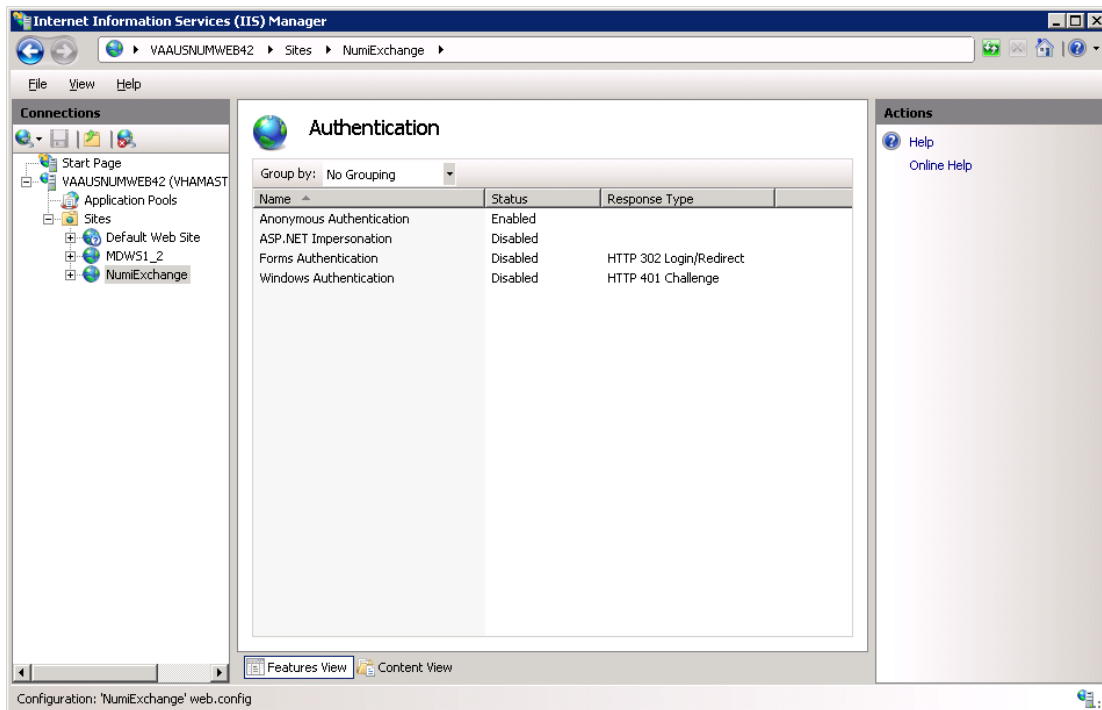
The NUMI Exchange web site bindings are shown in Figure 25: NUMI Exchange Bindings.

Figure 25: NUMI Exchange Bindings



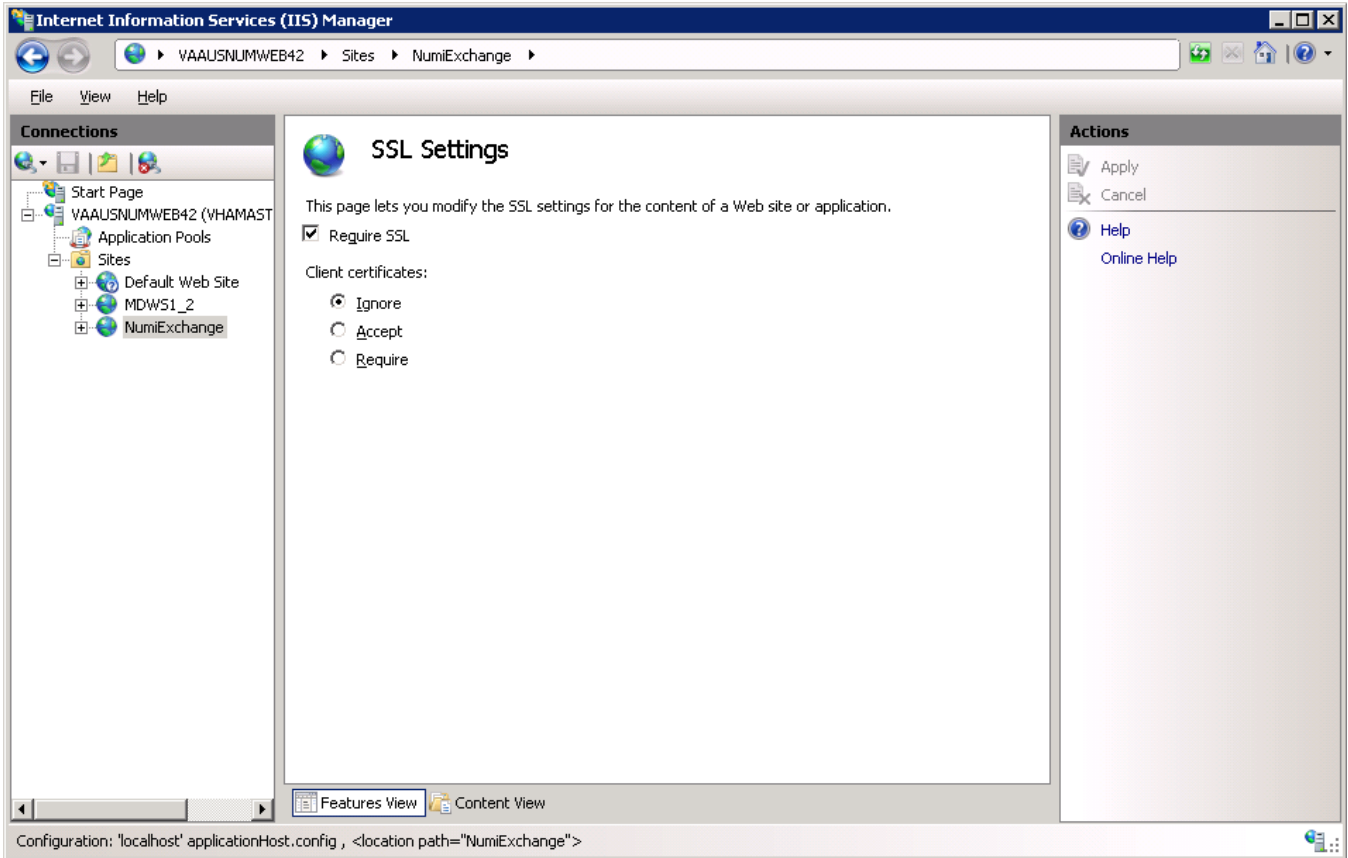
The NUMI Exchange web site authentication settings are shown in Figure 26: NUMI Exchange Authentication Settings.

Figure 26: NUMI Exchange Authentication Settings



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

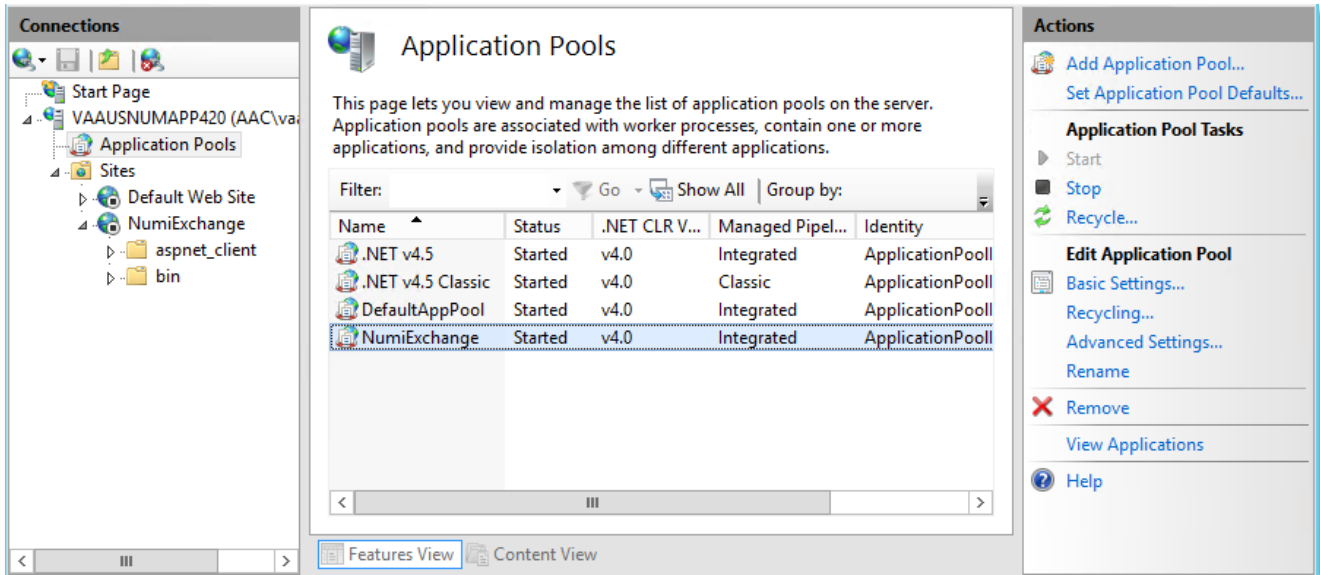
Figure 27: NUMI Exchange SSL Settings



10.2.1 Application Pool Configuration

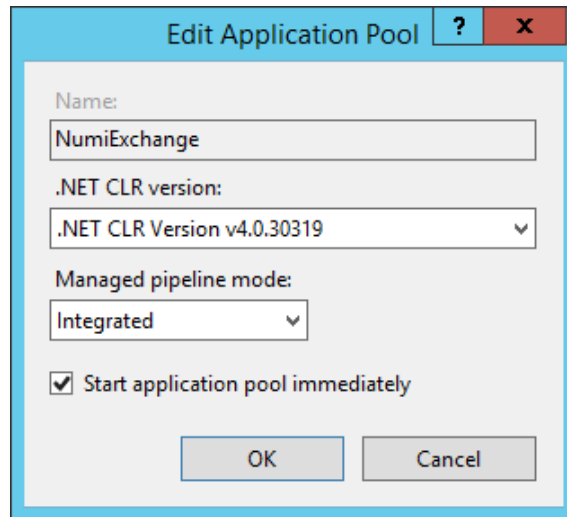
The NUMI Exchange application pool setup is shown in Figure 28: Application Pool Window.

Figure 28: Application Pool Window



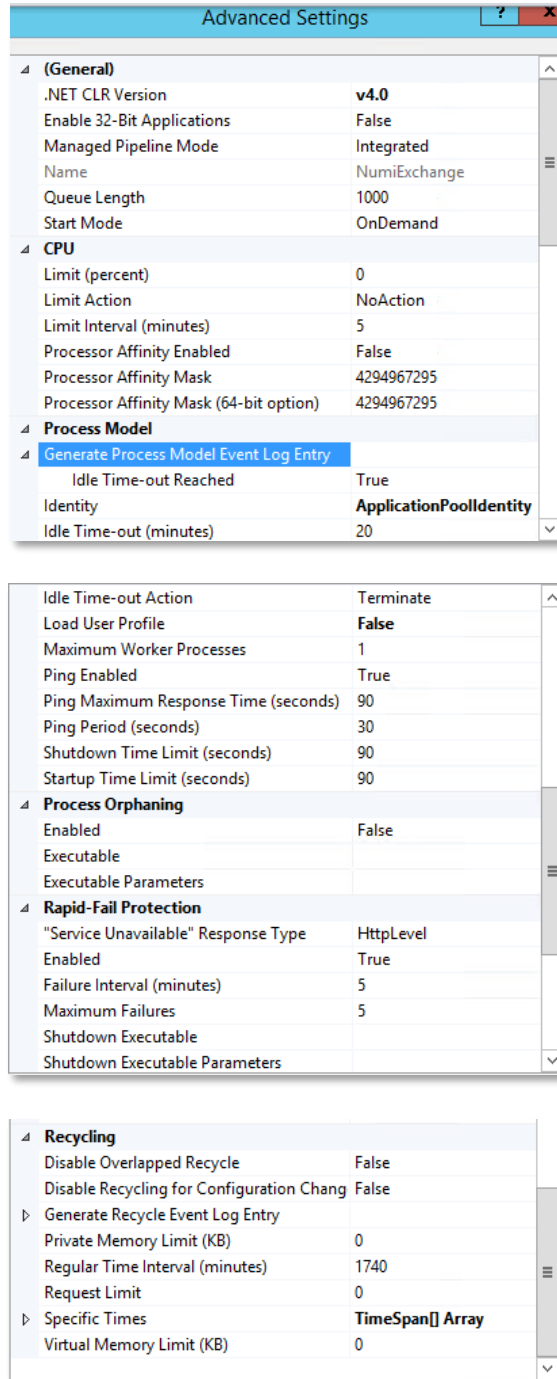
The NUMI Exchange application pool basic settings are shown in Figure 29: NUMI Exchange Application Pool Basic Settings.

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

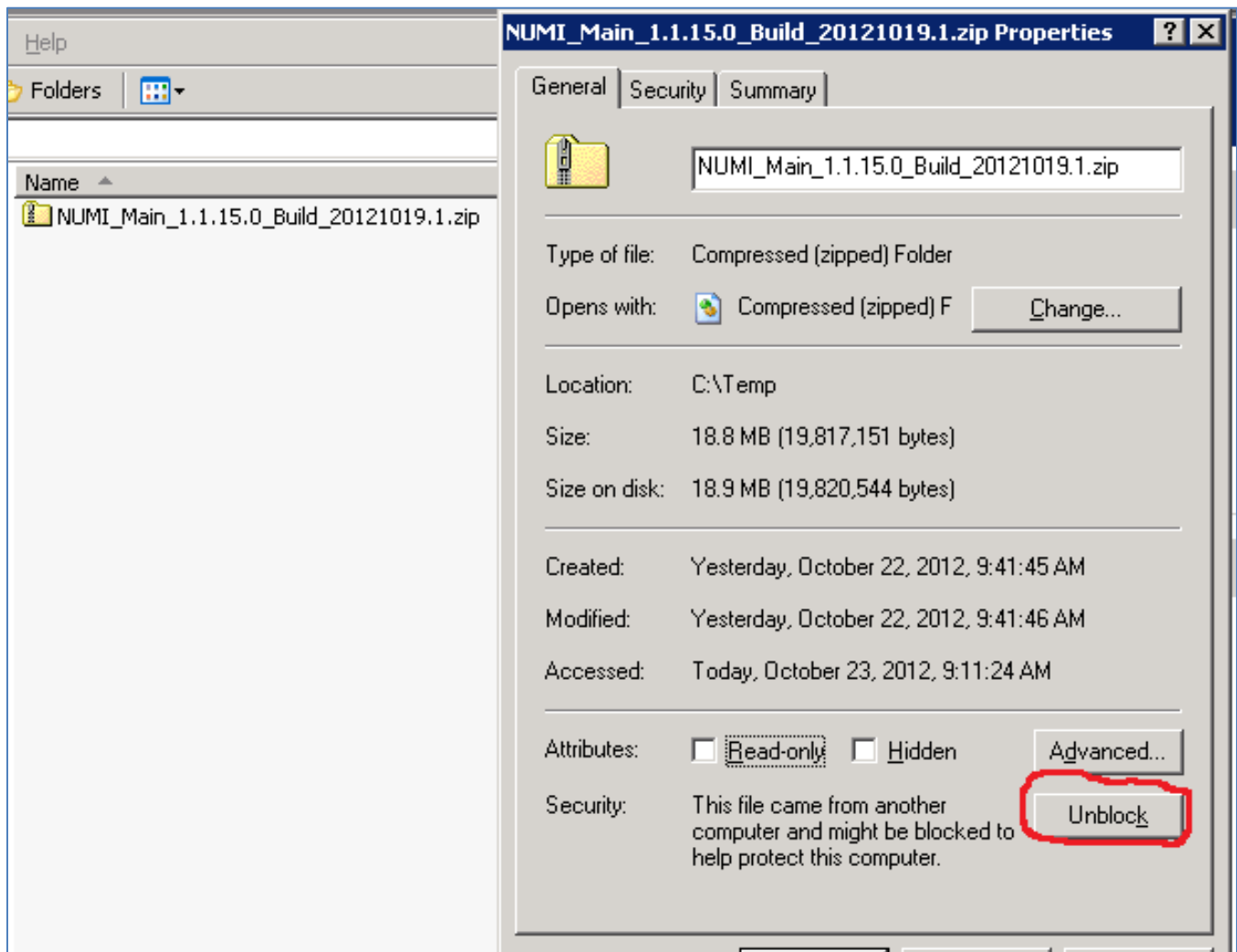


11. Installing NUMI on Server 2019

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: Unlocking 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

Add Web Site

Site name: NUMI Application pool: NUMI Select...

Content Directory

Physical path: D:\NUMI\<install_dir> ...

Pass-through authentication

Connect as... Test Settings...

Binding

Type: http IP address: All Unassigned Port: 80

Host name:

Example: www.contoso.com or marketing.contoso.com

Start Web site immediately

OK Cancel

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

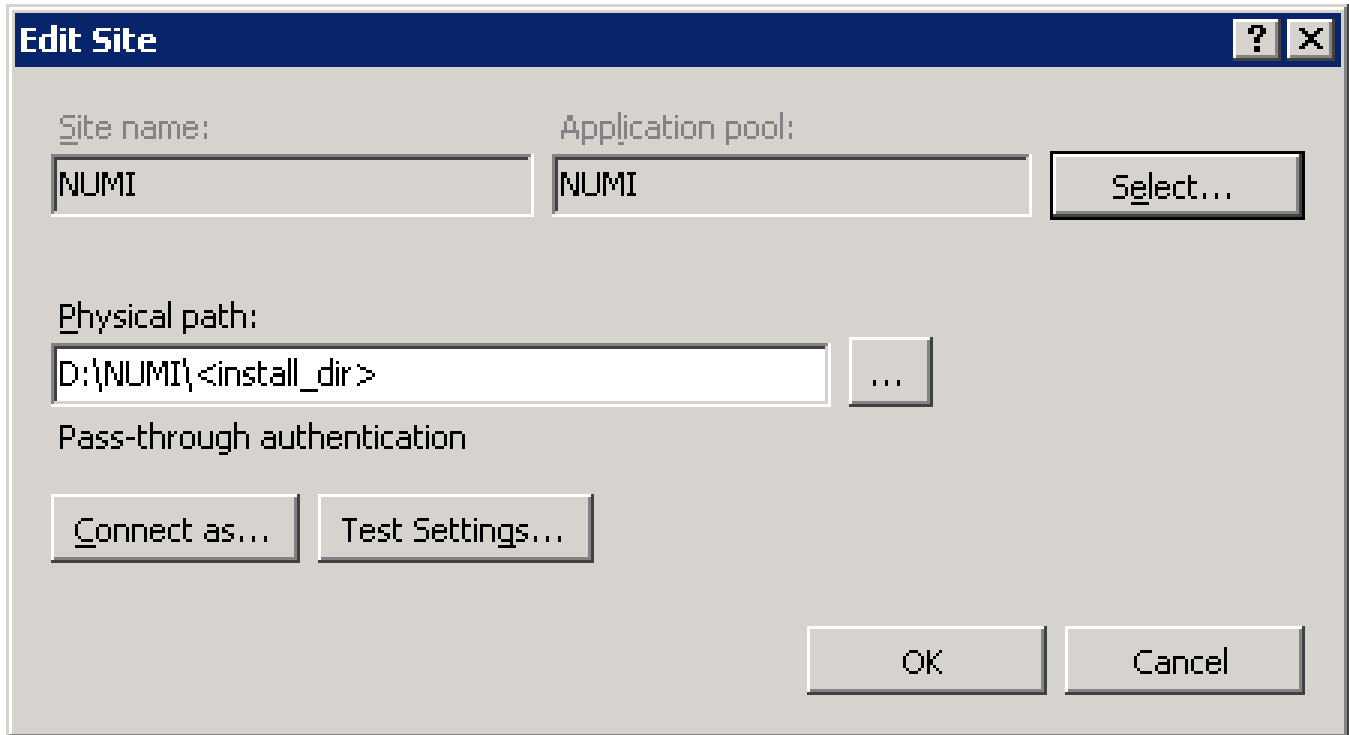
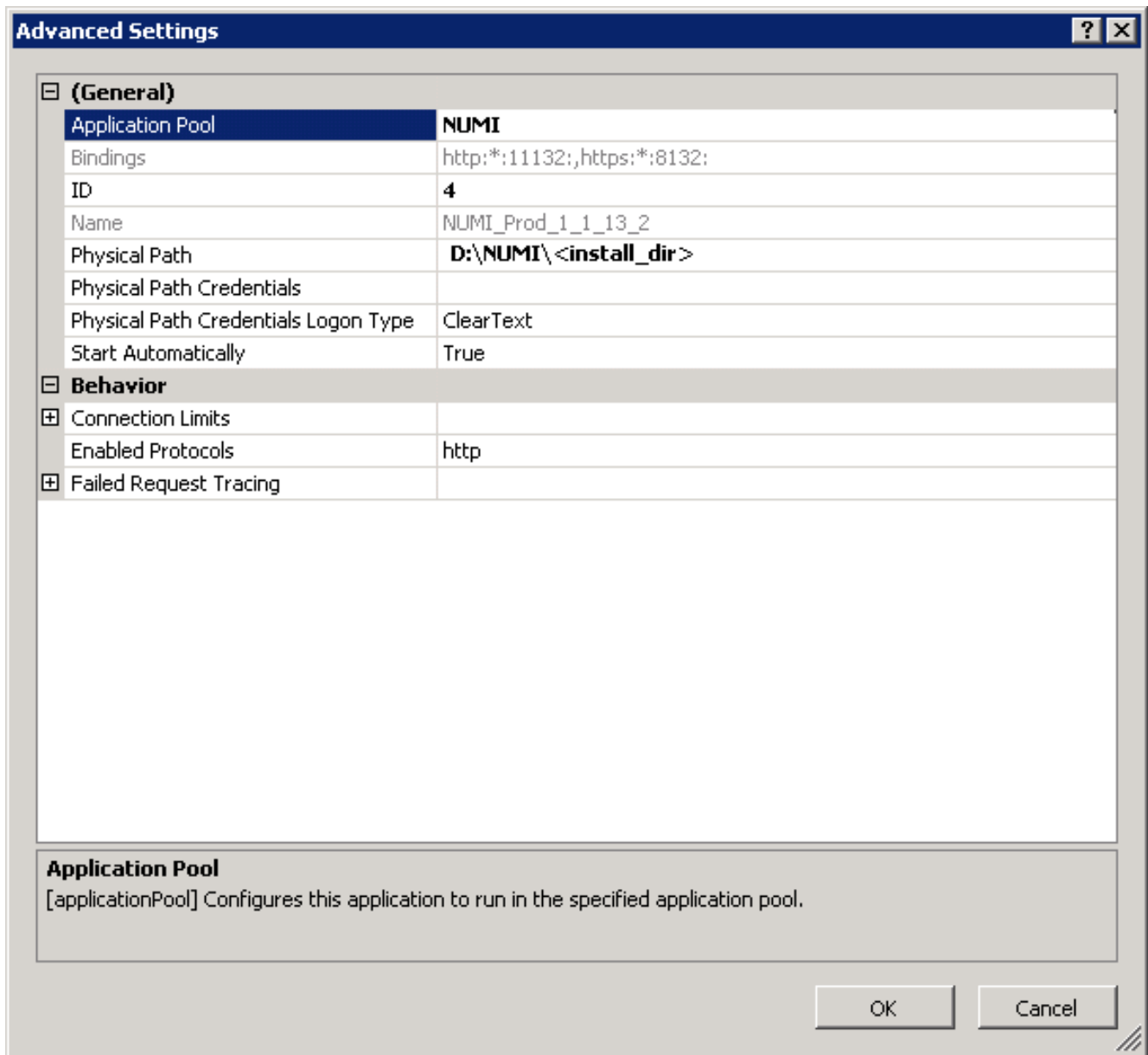
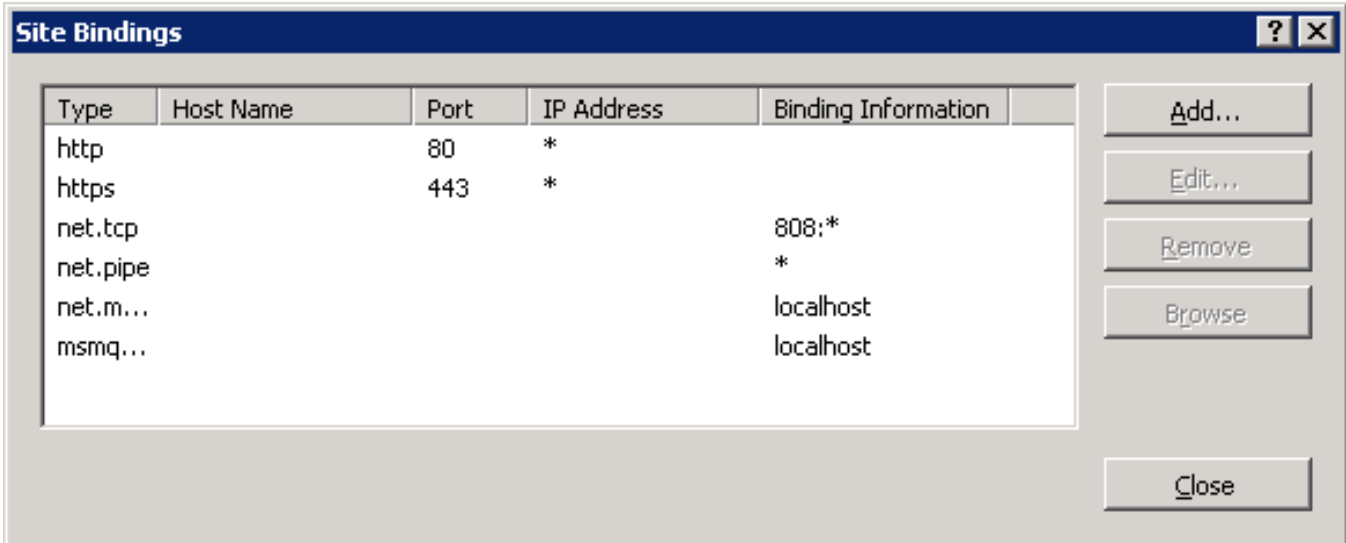


Figure 34: NUMI Advanced Settings



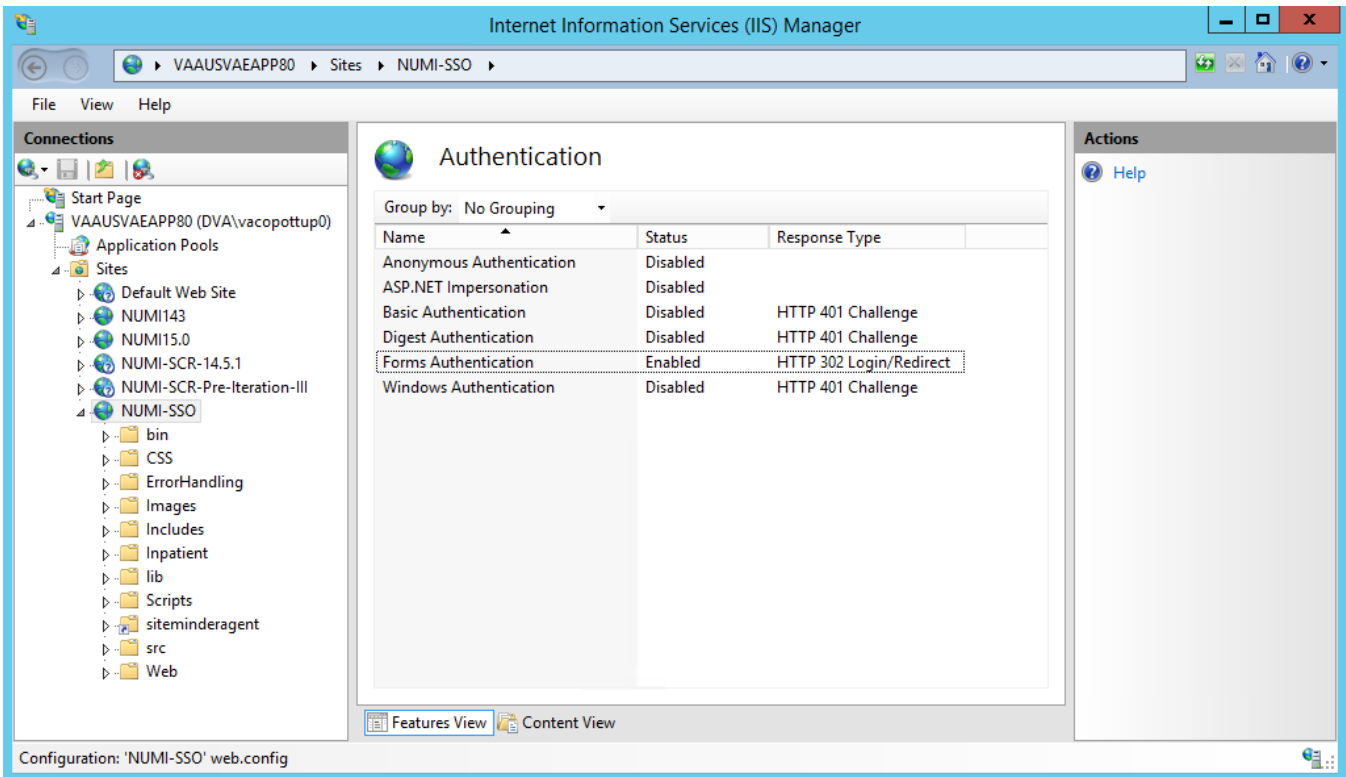
The NUMI web site bindings are shown in Figure 35: NUMI Bindings.

Figure 35: NUMI Bindings



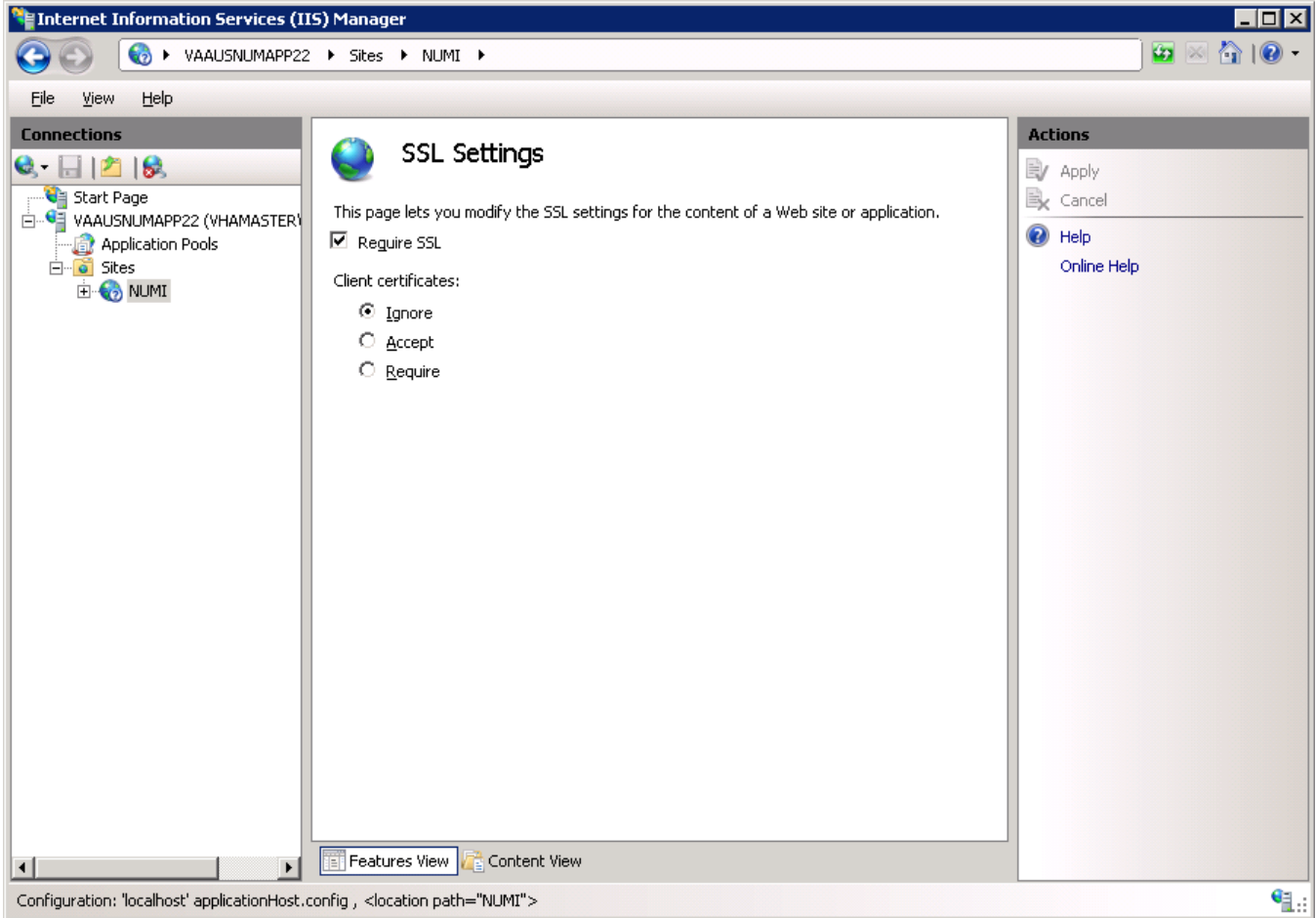
The NUMI web site authentication settings are shown in Figure 36: NUMI Authentication Setting. Make sure Forms Authentication is the only one enabled.

Figure 36: NUMI Authentication Settings



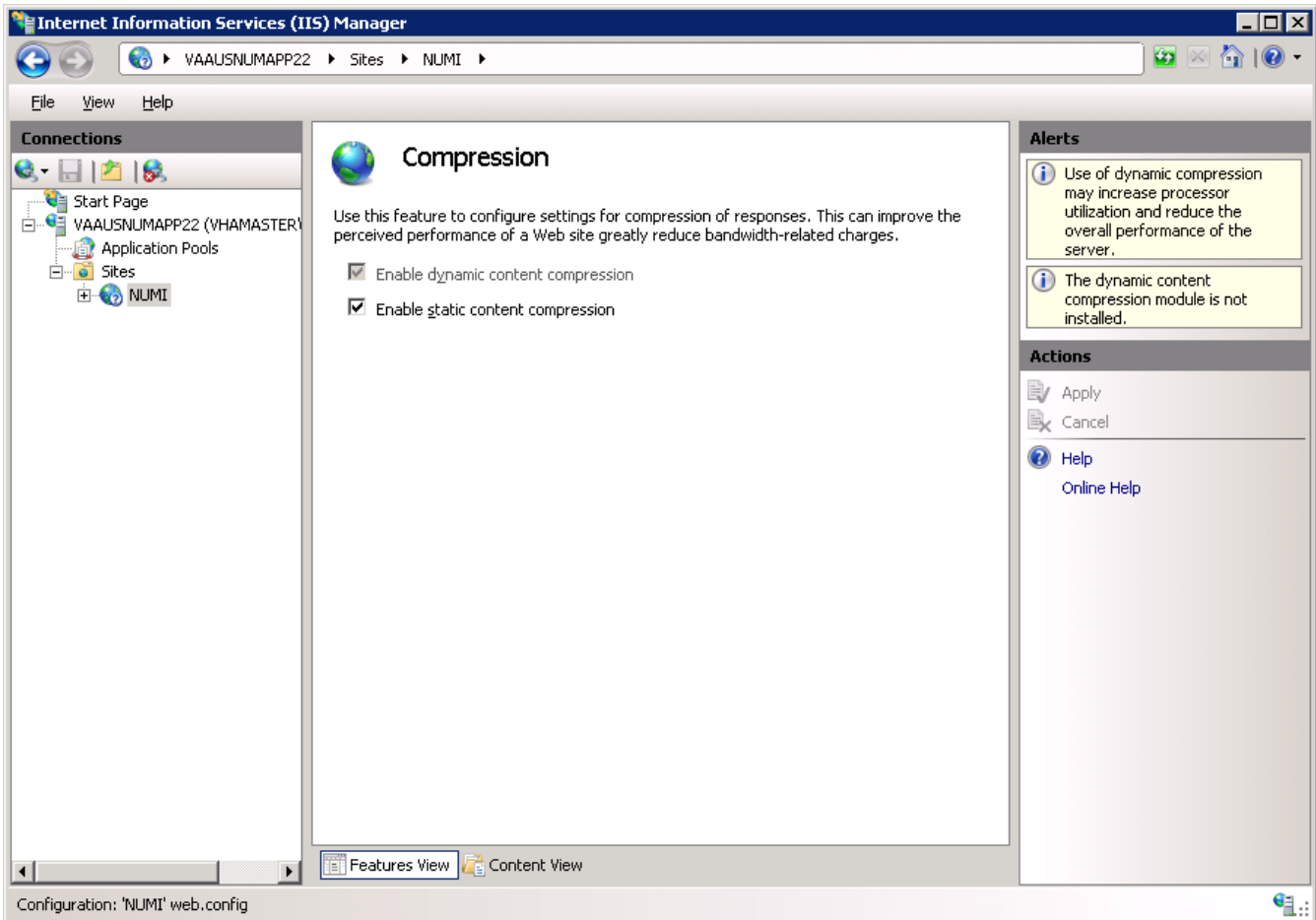
The NUMI website SSL settings are shown in Figure 37: NUMI SSL Settings.

Figure 37: NUMI SSL Settings



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

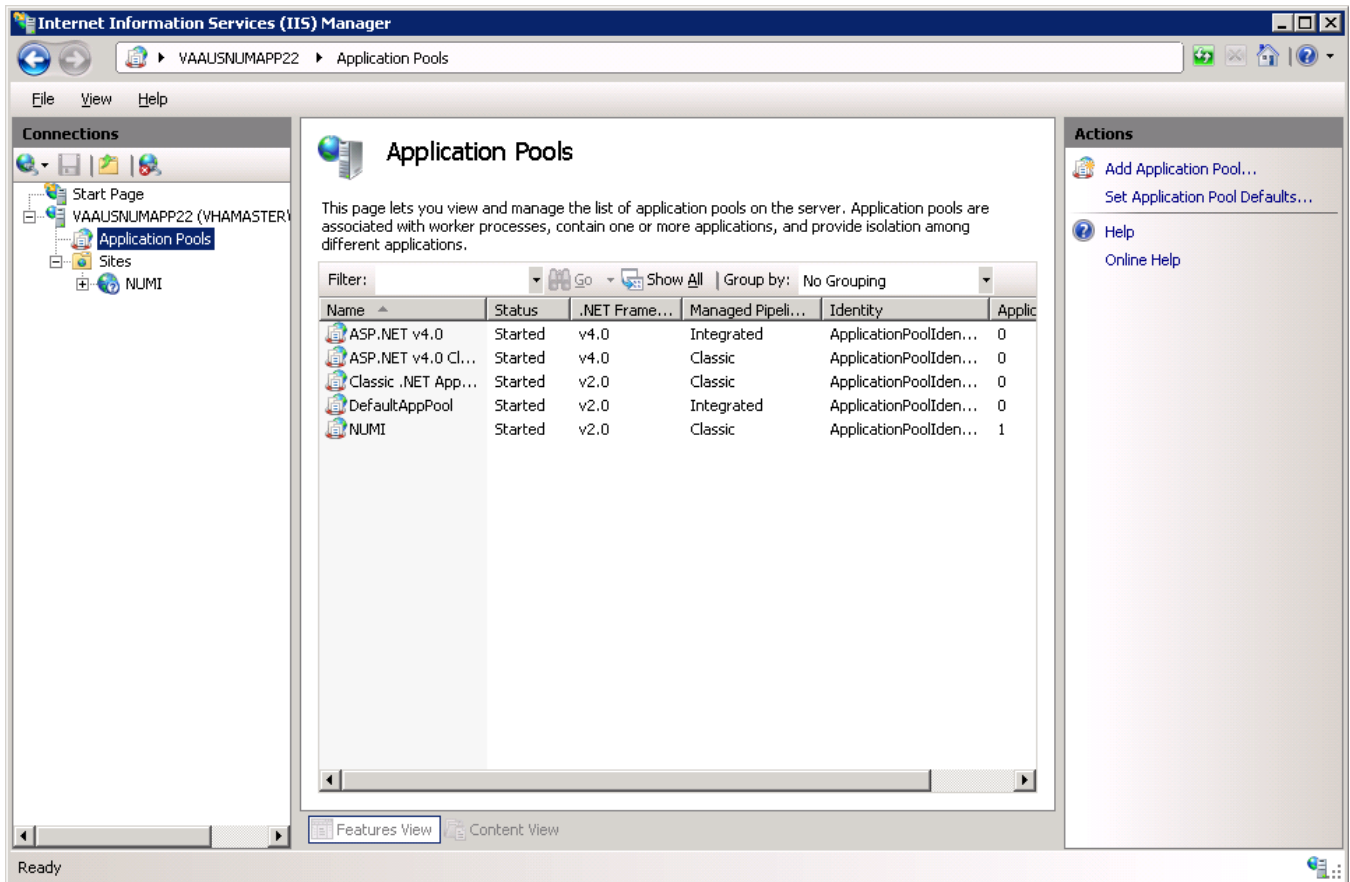
Figure 38: NUMI Compression Settings



11.3. Application Pool Configuration

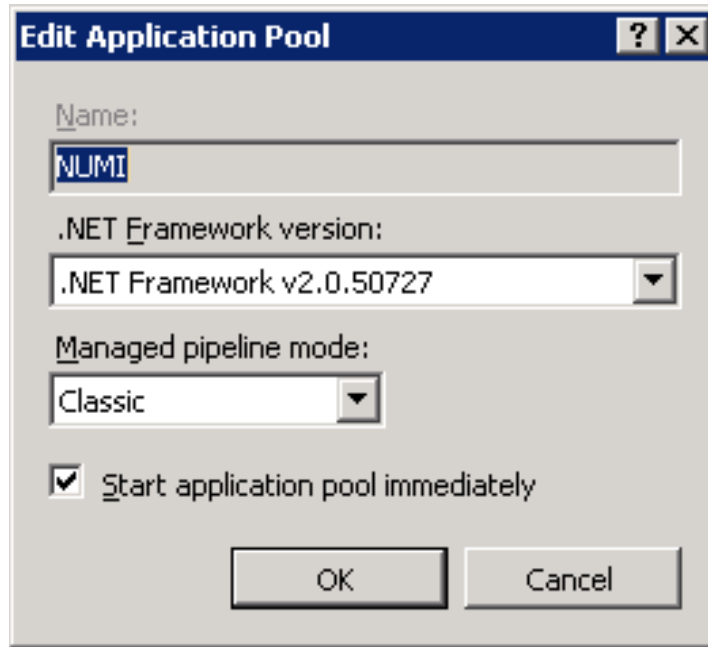
The NUMI application pool setup is shown in Figure 39: Application Pool Window.

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 **Error! Not a valid bookmark self-reference..**

Figure 41: NUMI Application Pool Advanced Settings

Advanced Settings 6D

EI (General)	
.NET Framework Version	v2.0
Enable 32-Bit Applications	False
Managed Pipeline Mode	Classic
Name	NUMI
Queue Length	1000
Start Automatically	True
EI CPU	
limit	0
limit Action	NoAction
limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
EI Process Model	
Identity	ApplicationPoolIdentity
Idle Time-out (minutes)	20
load User Profile	True
Maximum Worker Processes	
Ping Enabled	True
Ping Maximum Response Time (seconds)	90
Ping Period (seconds)	30
Shutdown Time limit (seconds)	90
Startup Time limit (seconds)	90
EI Process Orphaning	
Enabled	False
Executable	
Executable Parameters	
EI Rapid-Fail Protection	
"ServiceUnavailable" Response Type	Httplevel
Enabled	True
Failure Interval(minutes)	5
Maximum Failures	5
Shutdown Executable	
Shutdown Executable Parameters	
EI Recycling	
Disable Overlapped Recycle	False
Disable Recycling for Configuration Changes	False
IB Generate Recycle Event log Entry	
Private Memory Limit (KB)	0
Regular Time Interval(minutes)	120
Request limit	0
IB Specific Times	
Virtual Memory Limit (KB)	0

.NET Framework Version
 [managedRuntimeVersion] Configures the application pool to load a specific version of the .NET Framework. Selecting "No Managed Code" will cause all ASP.NET requests to fail.

OK Cancel

12. Microsoft Entra ID Application Registration for the Web Server Configuration

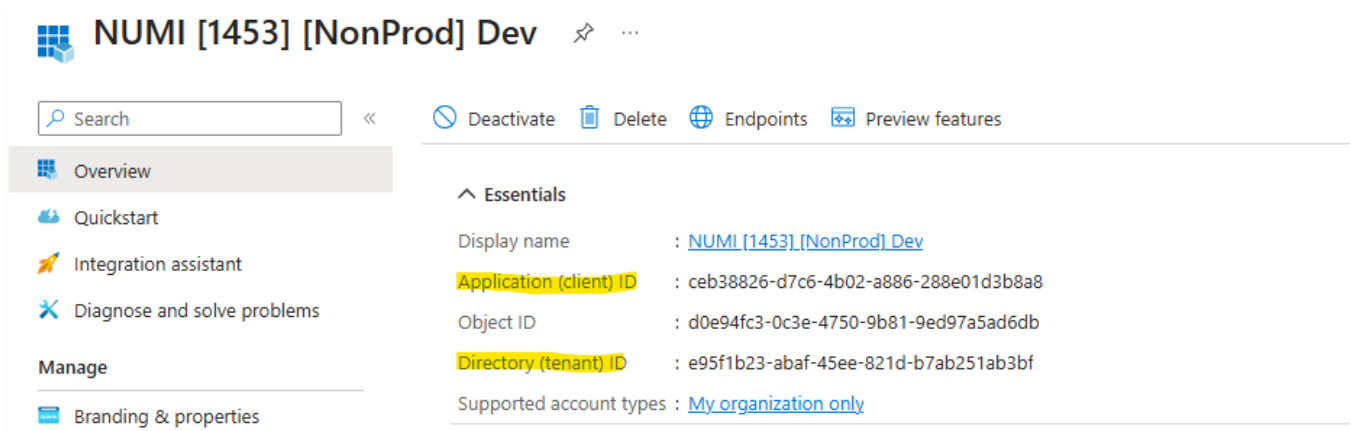
Microsoft Entra ID is the network based authentication method and pattern used by NUMI. Users must be authenticated with Microsoft Entra ID to use NUMI. There are several key configurations from the Entra ID Application Registration that need to be in the NUMI Web Server Configuration

12.1. Microsoft Entra ID Application Registration

Each NUMI environment has its own Application Registration. The key values needed are ClientId, TenantId, ClientSecret, and RedirectUri.

The values can be found on the Entra ID portal in these sections: REDACTED

Figure 42: Microsoft Entra ID Application Registration



The screenshot displays the Microsoft Entra ID portal interface for an application registration. The header shows the application name "NUMI [1453] [NonProd] Dev" with a search icon and a menu icon. Below the header is a search bar and a set of action buttons: Deactivate, Delete, Endpoints, and Preview features. The left sidebar contains navigation options: Overview (selected), Quickstart, Integration assistant, Diagnose and solve problems, Manage, and Branding & properties. The main content area is titled "Essentials" and lists the following details:

Display name	: NUMI [1453] [NonProd] Dev
Application (client) ID	: ceb38826-d7c6-4b02-a886-288e01d3b8a8
Object ID	: d0e94fc3-0c3e-4750-9b81-9ed97a5ad6db
Directory (tenant) ID	: e95f1b23-abaf-45ee-821d-b7ab251ab3bf
Supported account types	: My organization only

Figure 43: Application Registration Client Secret

NUMI [1453] [NonProd] Dev | Certificates & secrets

Search << Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems

Manage

Branding & properties
Authentication (Preview)
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

New support request

Some actions may be disabled due to your permissions. To request access, contact the application owner(s) or your administrators.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (4)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as applicati

+ New client secret

Description	Expires	Value ⓘ
test-pankaj	6/14/2026	NxN*****
NUMI Dev Secret	6/27/2026	mwI*****
WEB920	8/12/2026	55b*****
test1	8/16/2026	GTV*****

Figure 44: EntraID Application Registration Redirect URIs

The screenshot shows the EntraID application registration interface for NUMI [1453] [NonProd] Dev | Authentication (Preview). The left sidebar contains navigation options like Overview, Quickstart, Integration assistant, and Manage. The main content area is titled 'Redirect URI configuration' and includes a warning message: 'Some actions may be disabled due to your permissions. To request access, contact the application owner(s) or your administrator. View applic'. Below this, there's a search bar and a table of registered URIs.

Platform Type	Redirect URI
Web	https://vaausappnum920.aac.dva.va.gov/signin-oidc
Web	https://localhost:44300/signin-oidc
Web	https://localhost:44368/
Web	https://vaauswebnum920.aac.dva.va.gov/

The values are then added to the NUMI Web App Config.

```
<!-- Microsoft Entra ID (Azure AD) Configuration -->
<add key="owin:AutomaticAppStartup" value="true" />
<add key="ida:ClientId" value="ceb38826-d7c6-4b02-a886-288e01d3b8a8" />
<add key="ida:TenantId" value="e95f1b23-abaf-45ee-821d-b7ab251ab3bf" />
<!--Client expires August 12th 2026 must be changed on the entraid side -->
<add key="ida:ClientSecret" value="REDACTED" />
<add key="ida:RedirectUri" value=" REDACTED " />
<add key="ida:PostLogoutRedirectUri" value="REDACTED /" />
<add key="EntraIDSTSScope" value="api://idev.sts.va.gov/token"/>
```

Important note, the ClientSecret is only viewable in the portal in the session it was created, it must be copied and passed along. The secret also expires annually.

13. Secure Token Service Integration for SSOi

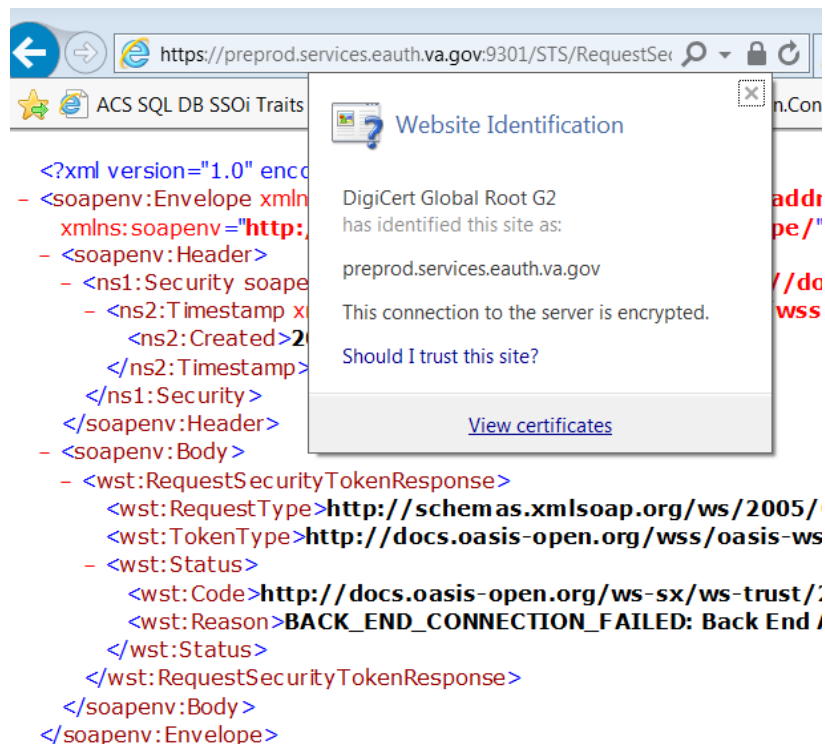
NUMI supports secure token service implementation through SSOi. Full details of the implementation can be found at REDACTED.

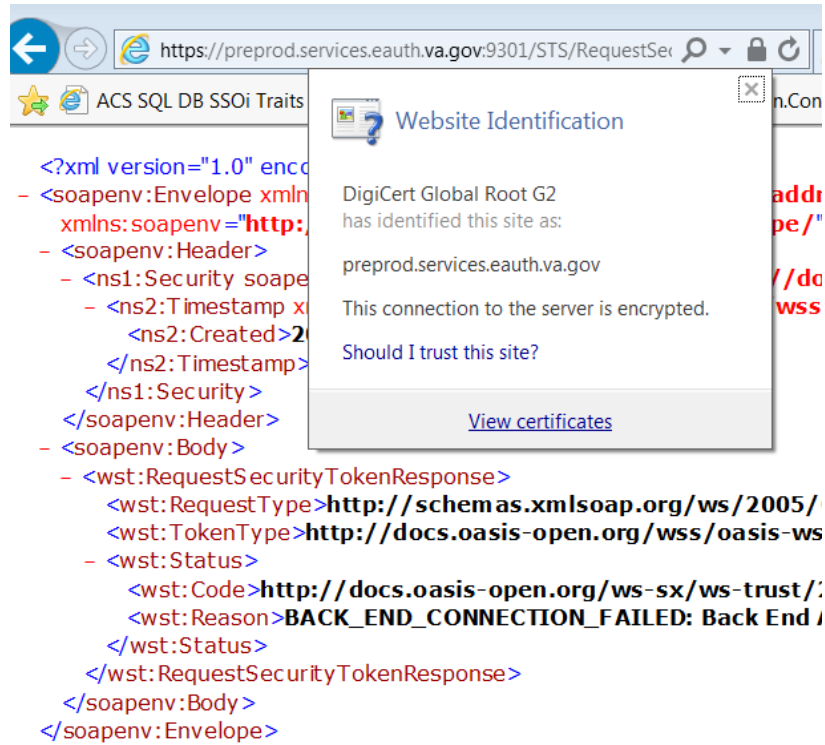
13.1. Download Certificate Chain from appropriate endpoint

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.

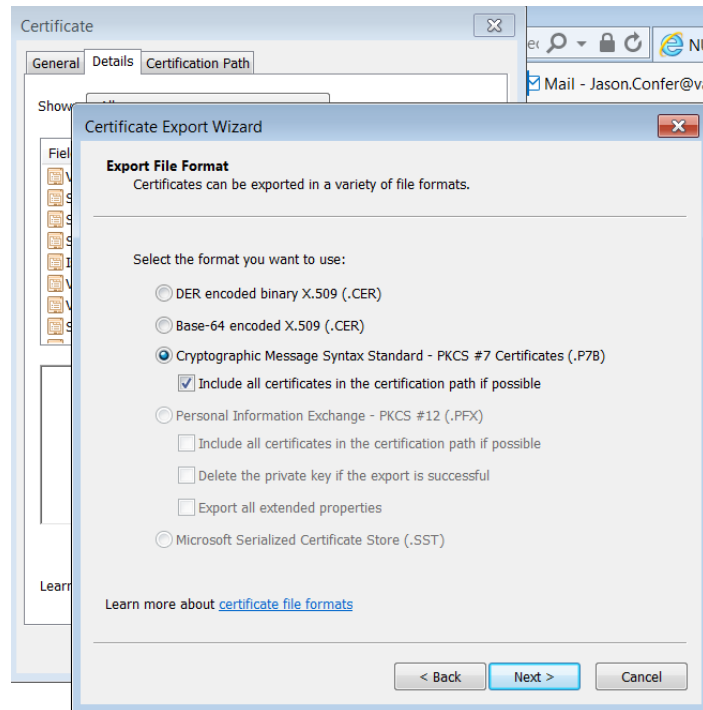
- iDEV: REDACTED
- SQA: REDACTED
- PREPROD: REDACTED
- PROD: REDACTED

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". REDACTED

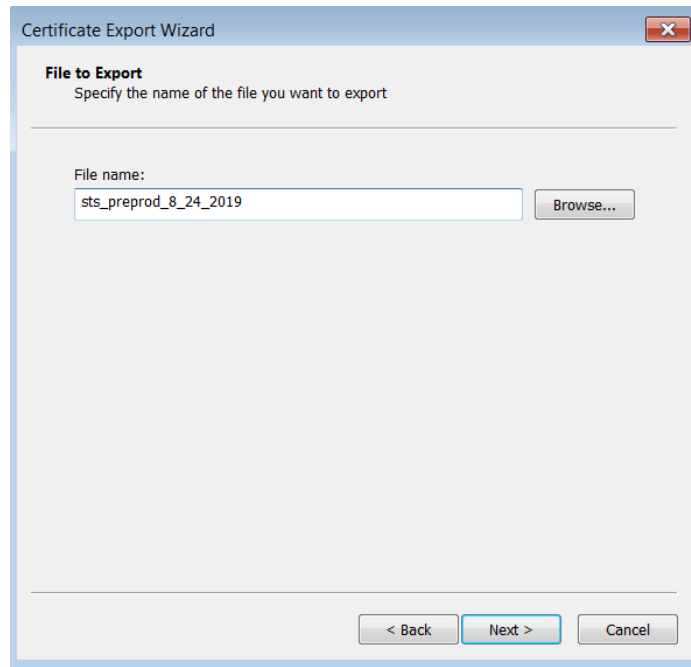




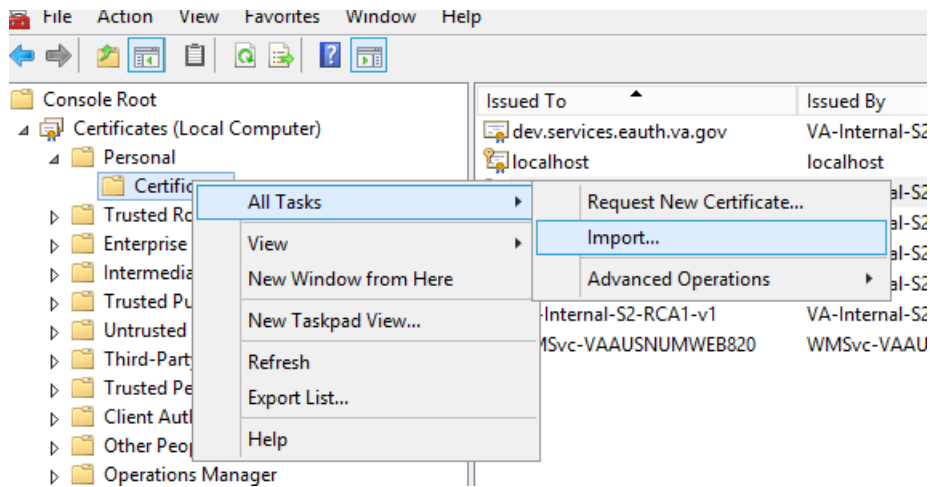
2. Click on the Details tab and select "Copy to file", choose PKCS and include all certificates in the path if possible



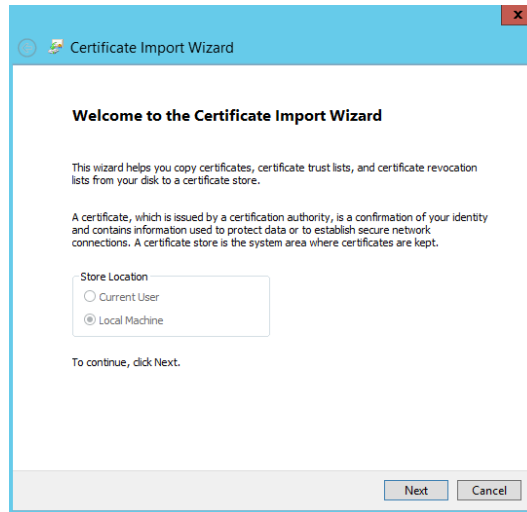
3. Save file as <endpointname_date>, click next then finish.



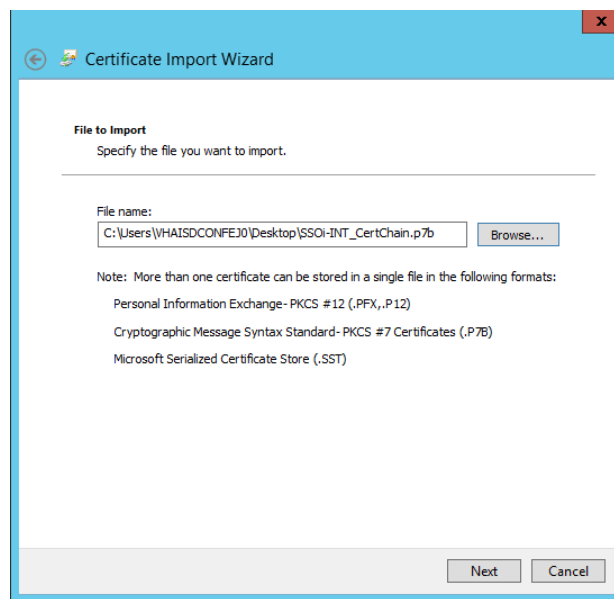
4. Optional – Reuse this file if another web server requires this STS endpoint's certificate.
5. In MMC, right click Computer-Personal store and import the certificate created in Step 9.



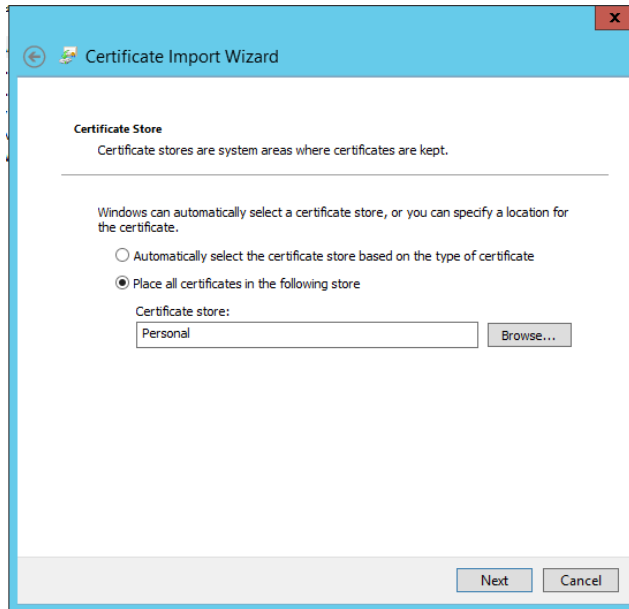
6. Import for local machine



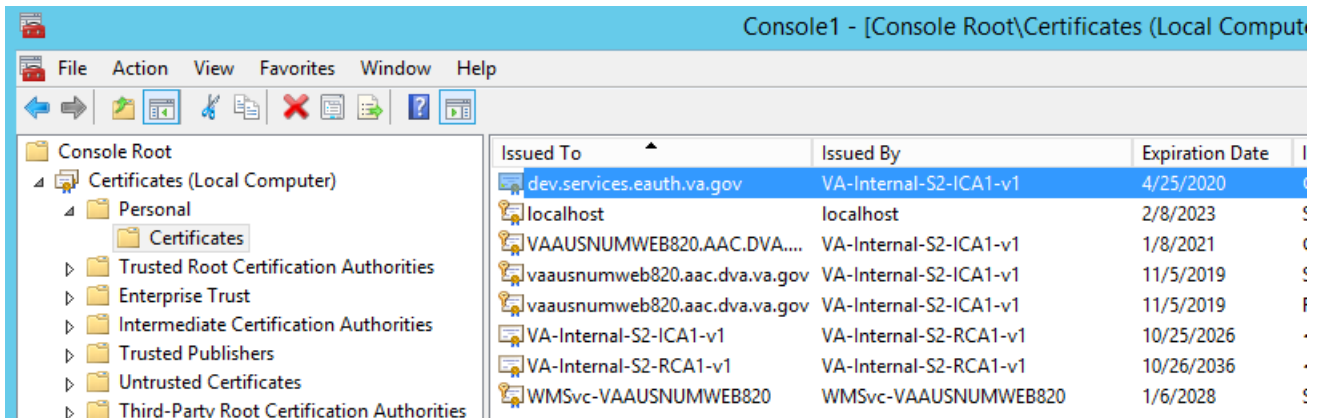
7. Browse to file created in step 10 and click Next



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

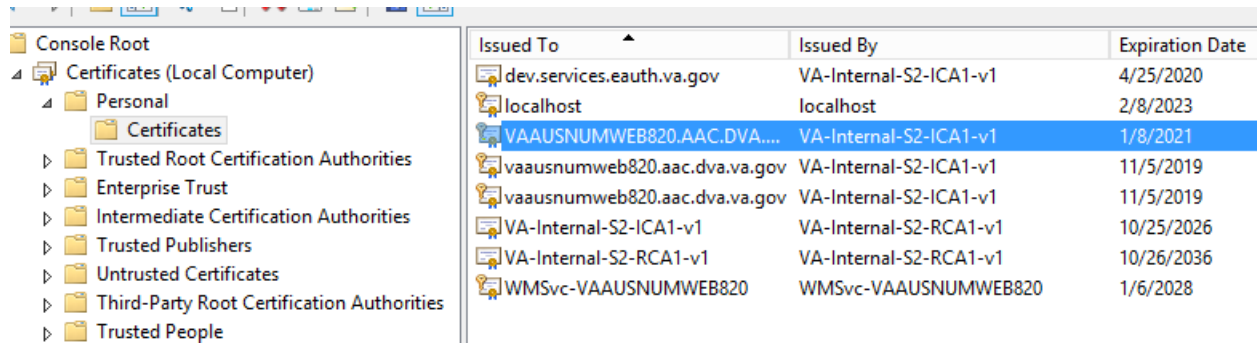


13.2. Export server cert to .pfx

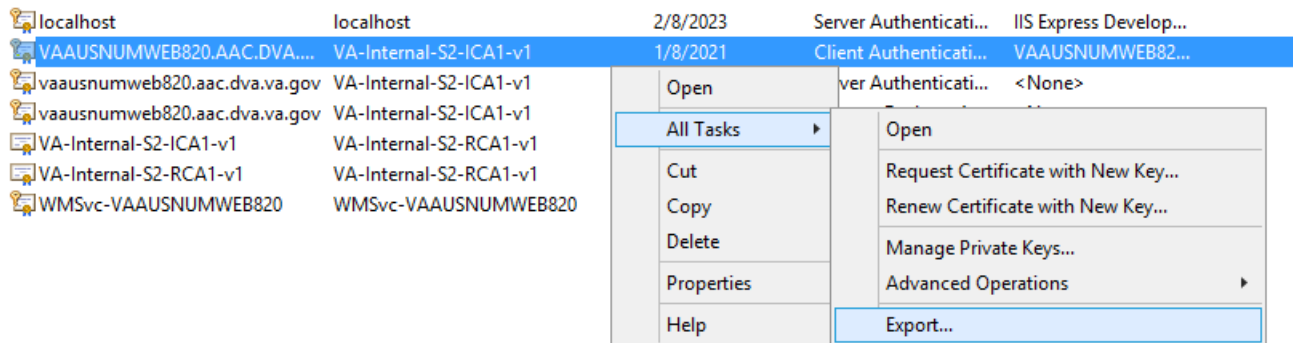
This is a copy of the .cer installed locally to the computer/personal account. It should be the one served by IIS when you navigate to the website.

13.2.1 Load the Microsoft Management Console, Certificate Snap-in, for the local computer

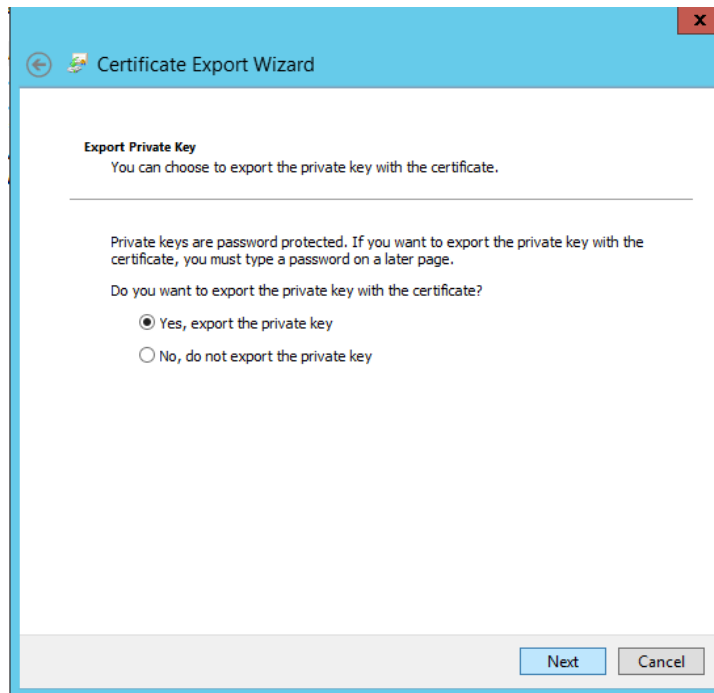
1. Find the server cert in the personal folder



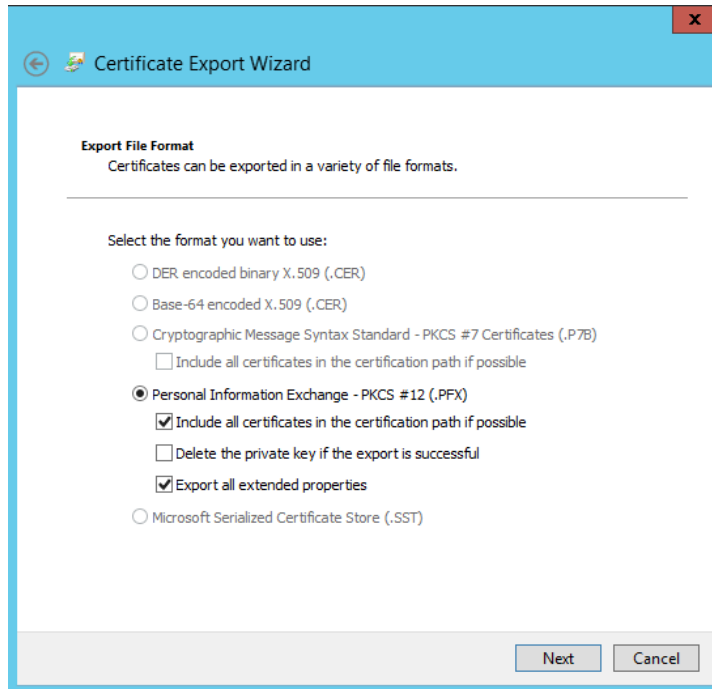
2. Right click and export the certificate



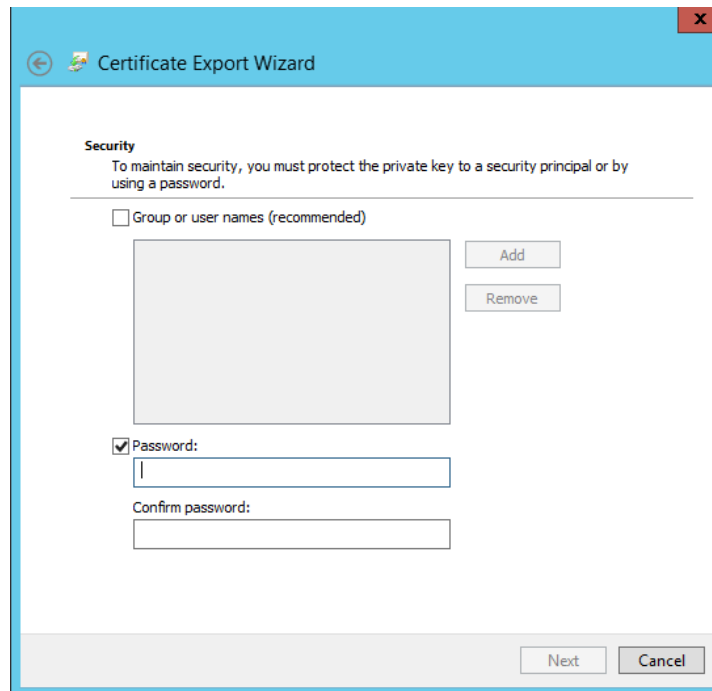
3. Select "Yes, export private key" and choose next



4. Select "Export all extended properties" and choose next



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



6. 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="REDACTED" />  
<ADD KEY="STSEENABLED" 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) 21.0.1 InterQual 2022 for NUMI 15.10 will be installed based on an existing installation of CERMe 20.1. The CERMe installation would be performed using a dump of the existing CERMe 20.1 database. Listed below are the steps to restore the database and install CERMe:

1. Restore CERMe 20.1 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 EDGE Browser.
3. Click on the Install Review Manager 21.0.1 / InterQual View 2022 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 should open the CERMe login page.
17. Now follow the steps below to update CERMe to CERMe 21.0.1.
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>
```

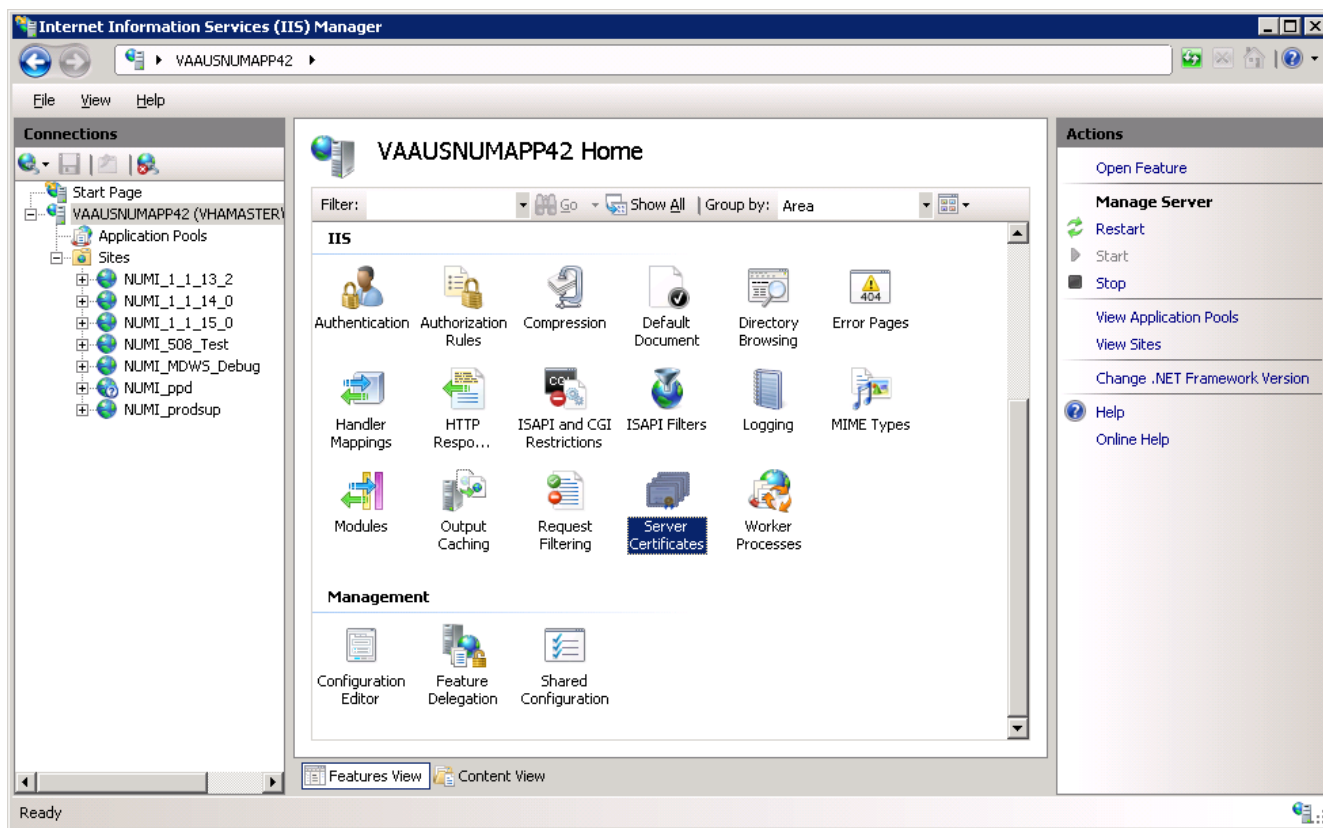
21. Start CERMe Service from the Windows Services.
22. Go to CERMe URL: `http://<server>:8357/rm/login` Login with the credential provided, and go to the menu Help > About. It should show Version InterQual Review Manager™ 21.0.1 (Build 4).
23. This completes the installation of the CERMe RM 21.0.1 InterQual View 2022.

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.

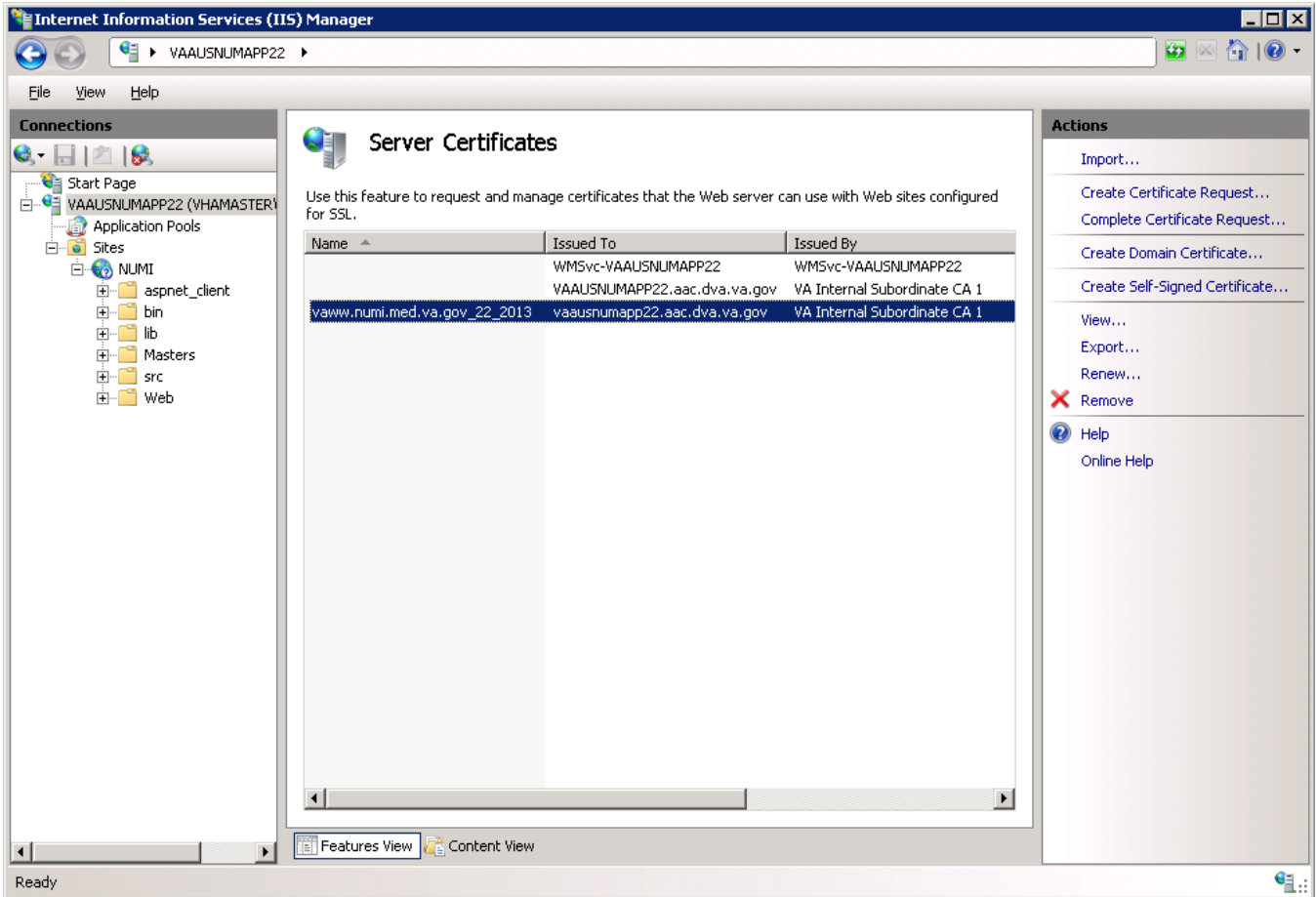
1. Use IIS Manager to export the current certificate to a .pfx file. Select the server name in the Connections pane and double click on the Server Certificates in the IIS pane as shown in Figure 45.

Figure 45: IIS Server Certificates



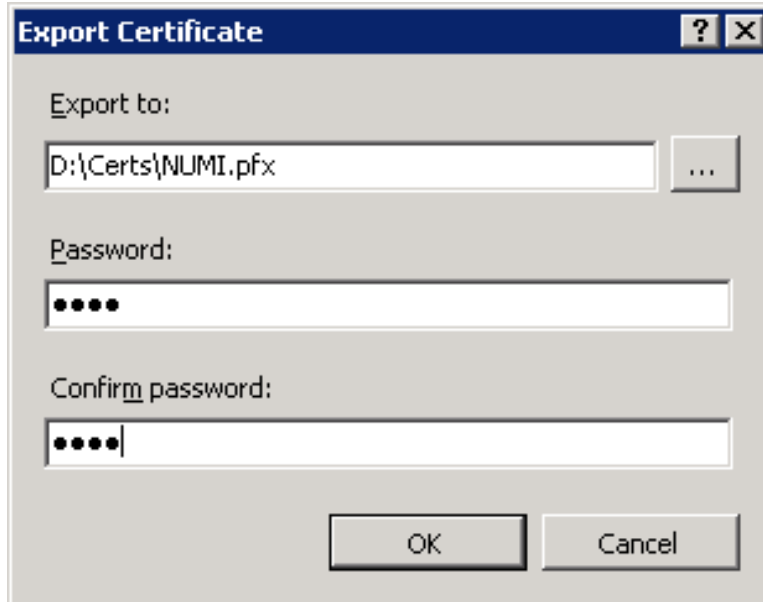
2. Select the certificate to export and click on the "Export..." link in the Actions pane, as shown in Figure 46.

Figure 46: 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 47. This password will be used in subsequent steps.

Figure 47: 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 48: keytool -keystore "C:\Certs\CERME.ks" -list

```

C:\WINDOWS\system32\cmd.exe
C:\Program Files\McKesson\CERME\Jre\bin>keytool -importkeystore -srcstoretype PK
CS12 -srckeystore "C:\NUMI\Certs\Fw_cert_2012.pfx" -destkeystore "C:\NUMI\Certs\
CERME.ks"
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias 3dcb9f87fe5f1e766d115a06a15c804c_c4444c68-d09f-4c3b-9be2-7ab723a
72c01 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or
cancelled

C:\Program Files\McKesson\CERME\Jre\bin>keytool -keystore "C:\NUMI\Certs\CERME.k
s" -list
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

3dcb9f87fe5f1e766d115a06a15c804c_c4444c68-d09f-4c3b-9be2-7ab723a72c01, Jul 10, 2
012, PrivateKeyEntry,
Certificate fingerprint (MD5): FE:0D:2A:B7:6F:0B:D5:8A:93:53:E6:DA:22:87:D9:7C

C:\Program Files\McKesson\CERME\Jre\bin>

```

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., REDACTED
12. Replace the "/web/home.aspx" portion with CERMe' s secure port, (8443 by default), e.g REDACTED

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

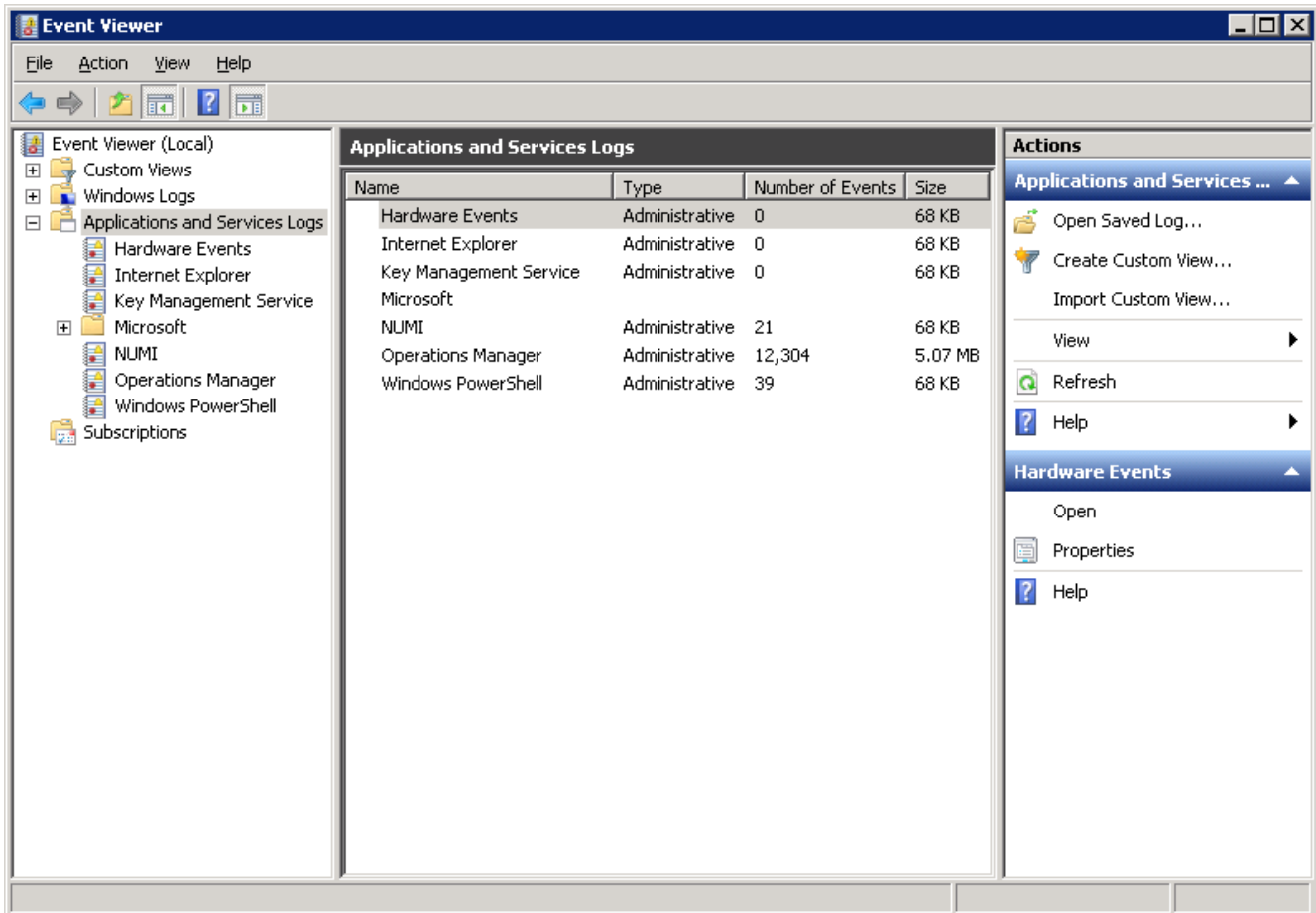
15. Setting up NUMI Section in the Windows Event Log

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 49: 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\\web.config

Settings to update:

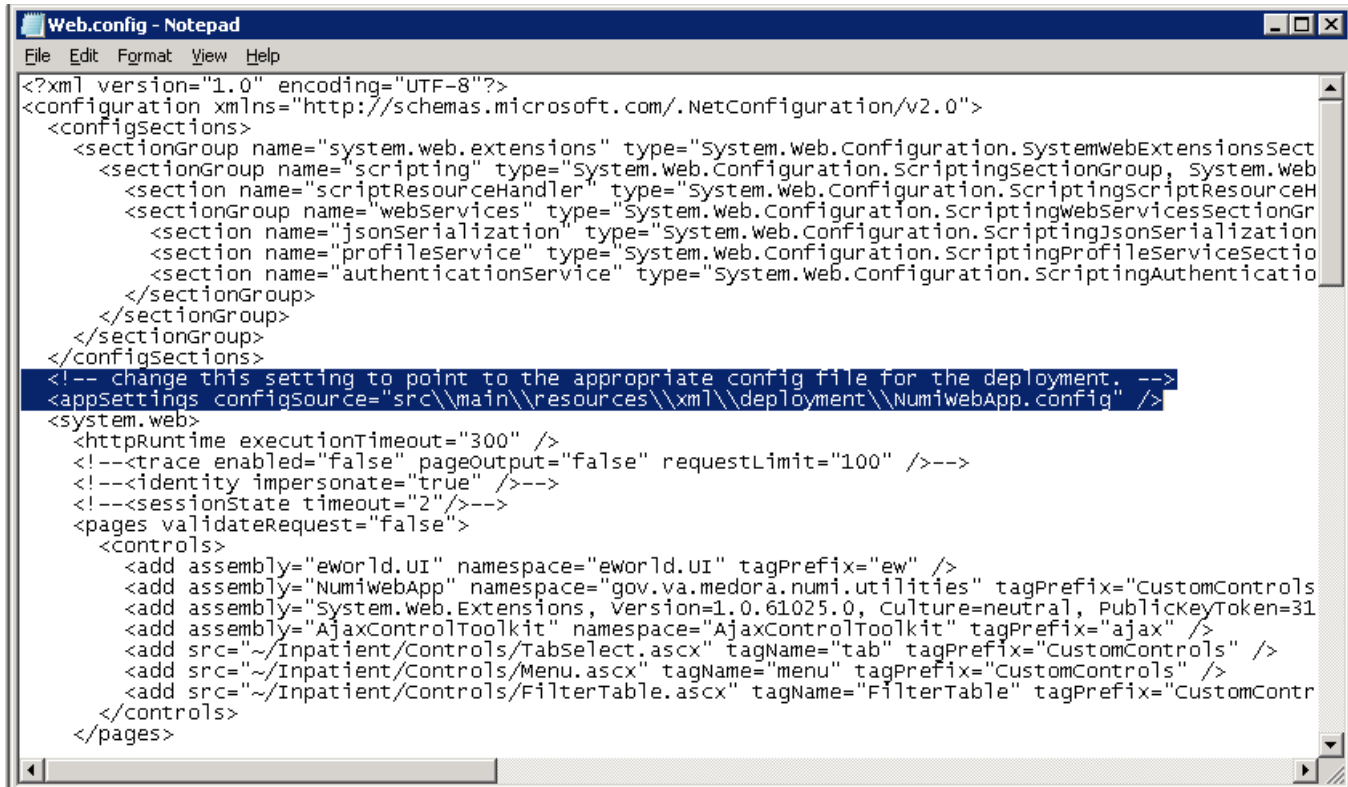
```
<!-- CHANGE THIS SETTING TO POINT TO THE APPROPRIATE CONFIG FILE FOR THE DEPLOYMENT. -->
```

```

<APPSETTINGS
CONFIGSOURCE=" SRC \ \MAIN \ \RESOURCES \ \XML \ \DEPLOYMENT \ \NUMIWEBAPP .CONF
IG" />
<CONNECTIONSTRINGS />

```

Figure 50: 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:

```

<!-- SERVICE CONFIGURATION -->
<ADD KEY="SERVICEURL" VALUE="<VIA SERVICE URL>" />
<ADD KEY="REQUESTINGAPP" VALUE="<REQUESTING APP ID TO BE IDENTIFIED
IN VIA>" />
<ADD KEY="ISSYNCHRONIZER" VALUE="TRUE" />
<ADD KEY="WSDLUSERNAME" VALUE="<VIA WSDL USERNAME>" />
<ADD KEY="WSDLPASSWORD" VALUE="<VIA WSDL PASSWORD>" />
<ADD KEY="NUMIDBCONNECTIONSTRING" VALUE="DATA
SOURCE=<ENTER DATABASE SERVER>;DATABASE=NUMI;USER
ID=NUMI_USER;PASSWORD=XXXXXXXX;TRUSTED_CONNECTION=FALSE" />

```

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...
SUCCEDED!
```
 - 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 REDACTED e.g., REDACTED

18. Installing NUMI Synchronizer on the Web Server

18.1. Installation Instructions

For a new installation:

1. Open CMD in Administrator mode

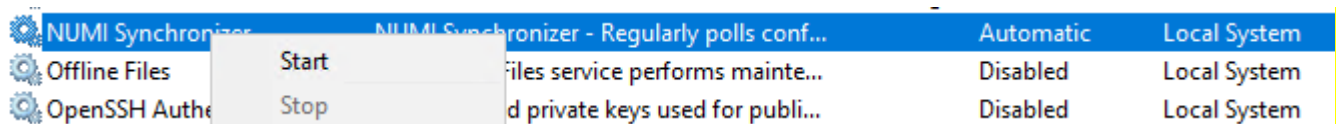
2. Enter 'cd C:\Windows\Microsoft.NET\Framework\v4.0.30319'
3. Enter 'InstallUtil.exe D:\NUMI\Synchronizer\Synchronizer2.exe'
4. View the NUMI Synchronizer service on services.msc
5. Close the CMD prompt
6. Verify/Update the Synchronizer2.exe.config data

```
<!-- SERVICE CONFIGURATION -->
<!-- VISTA SERVICE CONFIGURATION -->
<ADD KEY="SERVICEURL" VALUE=" REDACTED
<ADD KEY="REQUESTINGAPP" VALUE="NUMI_SYNC" />
<ADD KEY="ISSYNCHRONIZER" VALUE="TRUE" />
<ADD KEY="WSDLUSERNAME" VALUE="VWSL_NUMI" />
<ADD KEY="WSDLPASSWORD" VALUE="<PW>" />

<!-- STS CONFIGURATION -->
<ADD KEY="STSENDPOINT" VALUE=" REDACTED
<ADD KEY="STSEENABLED" VALUE="TRUE" />
<ADD KEY="STSCERTIFICATEPATH"
VALUE="D:\ \NUMI\SYNCHRONIZER\NUMISYNCSQA.PFX" />
<ADD KEY="STSCERTIFICATEPASSWORD" VALUE="<PW>" />

<!-- DATABASE CONNECTIONS -->
<ADD KEY="NUMIDBCONNECTIONSTRING" VALUE="DATA
SOURCE=VAAUSSQLNUM###.AAC.DVA.VA.GOV;DATABASE=NUMI;USER
ID=NUMI_USER;PASSWORD=<PW>;TRUSTED_CONNECTION=FALSE" />
<ADD KEY="REPORTDBCONNECTIONSTRING" VALUE="DATA
SOURCE=VAAUSSQLNUM###.AAC.DVA.VA.GOV;DATABASE=NUMI;USER
ID=NUMI_USER;PASSWORD=<PW>;TRUSTED_CONNECTION=FALSE" />
```

7. Start the service from services.msc



Service Name	Description	Startup Type	Log On As
NUMI Synchronizer	NUMI Synchronizer - Regularly polls conf...	Automatic	Local System
Offline Files	Files service performs mainte...	Disabled	Local System
OpenSSH Authen...	d private keys used for publi...	Disabled	Local System

For an upgrade in place:

1. Stop the existing service from services.msc

NUMI Synchronizer	NUMI Synchronizer - Regularly polls conf...	Automatic	Local System
Offline Files	Files service performs mainte...	Disabled	Local System
OpenSSH Auth	OpenSSH private keys used for publi...	Disabled	Local System

- Copy the Synchronizer distribution folder/files to the intended environment in the NUMI directory. This folder will be provided by Tier 3 maintenance and should be stored on each environment

Name	Date modified	Type	Size
Common.dll	9/14/2022 7:54 AM	Application extens...	351 KB
Common.Logging.dll	8/25/2022 11:36 AM	Application extens...	28 KB
Common.pdb	9/14/2022 7:54 AM	Program Debug D...	1,304 KB
Inpatient.dll	9/14/2022 7:54 AM	Application extens...	158 KB
Inpatient.pdb	9/14/2022 7:54 AM	Program Debug D...	576 KB
Microsoft.Web.Services2.dll	3/21/2012 5:46 AM	Application extens...	692 KB
Synchronizer2.exe	9/14/2022 7:54 AM	Application	22 KB
Synchronizer2.exe.config	9/14/2022 7:35 AM	XML Configuratio...	3 KB
Synchronizer2.pdb	9/14/2022 7:54 AM	Program Debug D...	70 KB
TOReflection.dll	8/25/2022 11:36 AM	Application extens...	24 KB

- Start the service from services.msc

NUMI Synchronizer	NUMI Synchronizer - Regularly polls conf...	Automatic	Local System
Offline Files	Files service performs mainte...	Disabled	Local System
OpenSSH Auth	OpenSSH private keys used for publi...	Disabled	Local System

18.2. Uninstall:

If you need to uninstall the NUMI Synchronizer services use services.msc and right click on the synchronizer to stop it. Then right click the Synchronizer and go to properties and disable it. Then open CMD in Admin mode and enter 'sc delete "NUMI 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	Windows Server	MS SQL Server
15.4	16.1	2017.2	2012 R2	2012
15.5	17	2018.1	2012 R2	2012
15.6	17	2018.1	2012 R2	2012

15.8	18.1	2019.1	2012 R2	2012
15.9	19.0	2020	2012 R2	2012
15.9.1	20.0	2021	2019	2019
15.10	21.0.1	2022	2019	2019
15.11	21.0.1	2022	2019	2019
15.14	21.0.1	2022	2019	2019
15.15	22.0	2024	2019	2019
15.16	22.0	2024	2019	2019
15.17	22.0	2025	2019	2019