National Utilization Management Integration (NUMI)

Server Setup Guide

Release 1.1.14.2

April 2015

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

Date	Description	Author
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

Date	Description	Author
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.	D. Curl
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

Table of Contents

List of Tables

List of Figures

1. Introduction

This Server Setup Guide explains how to install National Utilization Management Integration (NUMI), Release 1.1.14.2.

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 Information Technology team and/or 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 request for a National Deployment is governed by the ProPath Release Management processes. Please 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 Medical Domain Web Services (MDWS), which runs on the web servers. 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 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, and make whatever data alterations are desired for the target environment (i.e., the removal of sensitive data in non-production environments). For an upgrade backup, work from the NUMI 13.2 or 14.0 databases. For a fresh install backup, work from the NUMI 1.1.14.2 database.

Database Platform installation, and Database Restoration Procedures

1. Install Windows Server 2008 on the database server platform

2. Download and install any critical patches for the Operating System
3. Install the 64 bit Microsoft SQL Server 2005 application according to local "best practices"

   3.1. Microsoft's Full Text Search is required for the NUMI installation

   3.2. Replication is necessary for the NUMI installation to use the alternate database reporting capability of NUMI

   3.3. Reporting Services is not necessary for installation on the NUMI database server

   3.4. NUMI's database will function properly in either and active/passive or active/active cluster, but clustering is not required for the NUMI application
4. Apply all appropriate patches (according to local best practices) to Microsoft SQL Server 2005
5. Install / restore the database components according to the instructions in section 5 Instructions for Installing Database Components.

2.2.2. Web Server

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

1. Install Windows Server 2008 on the web server platform
2. Download and install any critical patches for the Operating System on all web servers
3. Install Microsoft 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
7. Install MDWS 2.7.3.2 (pronounced "Meadows")
8. 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 2008 on the application server platform
2. Download and install any critical patches for the Operating System on all application servers
3. Install the CERME 2012.2 application
4. Install the NUMI application
5. Change the web.config file settings as needed

3. Pre-Installation Instructions and Preparation

This section explains the tasks that need to be performed before installing National Utilization Management Integration (NUMI) software. Before proceeding with the installation procedures, consult the list of requirements below.

3.1. Installation Process Requirements

It is assumed 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 2008

Database: SQL Server 2005

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 CPRS access in their VistA menu structure, such as in their secondary menu tree. The VistA menu name is CPRSChart (or CPRS GUI CHART). Table 1 and Table 2 identify the menus, options and settings these user accounts will need to have assigned.

Table 1: CPRS Rights

CPRS Rights
Primary Menu: XMUSER
Primary Menu: MailMan Menu
Secondary Menu: [OR CPRS GUI CHART]
Secondary Menu: CPRSChart Release 1.1.27.77
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 than 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

Please see the *NUMI Systems Management Guide* for information about the structure and components of the NUMI database.

5. 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, and make whatever data alterations are desired for the target environment (i.e., the removal of sensitive data in non-production environments). For an upgrade backup, work from the NUMI 13.2 or 14.0 databases. For a fresh install backup, work from the NUMI 1.1.14.2 database.

5.1. 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

    1.1. The application database (typically called NUMI) is necessary for proper function of the application

    1.2. The "auditing" database (typically called LogSyncDb) is necessary for proper functioning of the application and the synchronizer

    1.3. The CERMe database can be restored from an existing backup, or can be built from scratch from the CERMe installation media

        1.3.1. 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

        1.3.2. If the CERMe database is installed from media, follow the instructions provided by McKesson for installation

2. Restore the database backup to the existing server

    2.1. File paths will have to be altered according to local best practices

    2.2. User accounts may be, but are not required to be, restored with the database. NUMI requires the numi_user account to be setup.

    2.3. Database ownership may be altered so that the owning account for the NUMIdatabase complies with local best practices

    2.4. 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 6.18 Installing NUMI Synchronizer on the DB Server

6. Installation Procedure for Server 2008 R2

This section identifies the installation procedures that shall be followed.

6.1. Patch the OS

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 Microsoft's website. (Note: a restart of the servers may be necessary).

6.2. SQL Server Setup (Windows Server 2008 R2)

6.2.1. Role Setup

This applies to the SQL database server, with Windows Server 2008 R2 installed. Use Server Manager to install the File Services with the role services shown in Figure 1: SQL Server Role Services.

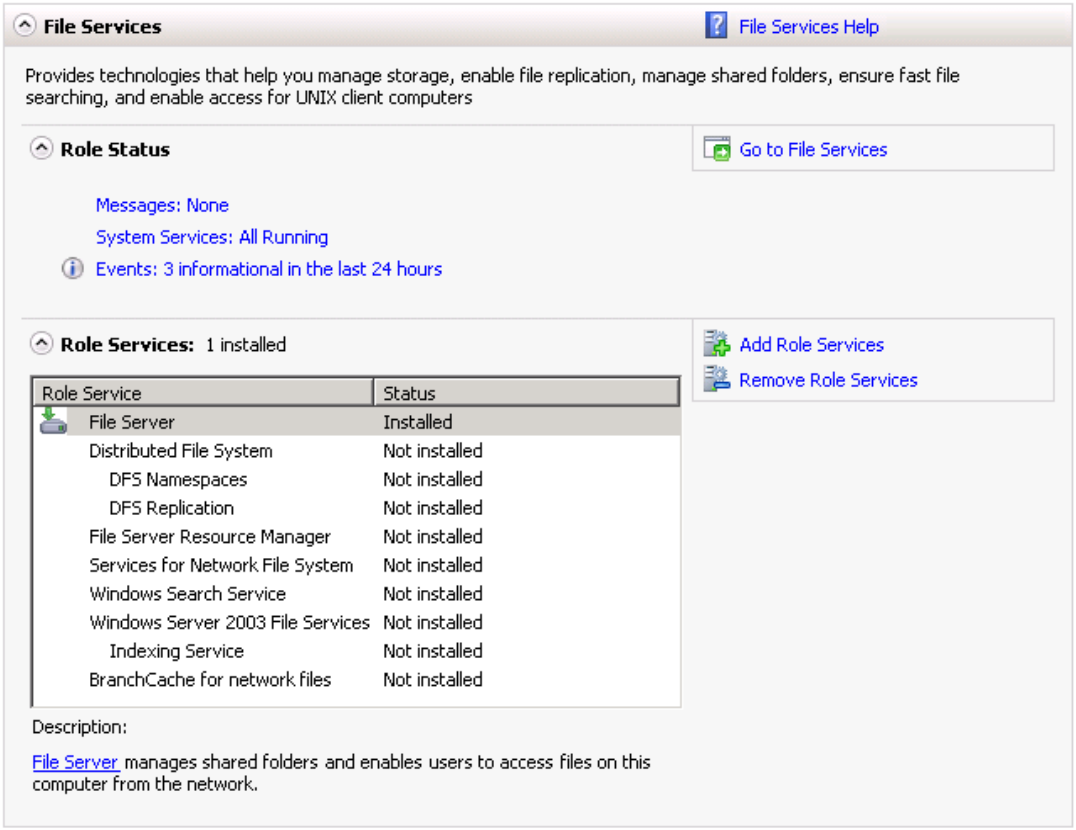

Figure 1: SQL Server Role Services

6.3. Web Server Setup (Windows Server 2008 R2)

6.3.1. Role Setup

This applies to the NUMI Exchange /MDWS web servers, with Windows Server 2008 R2 installed. Use Server Manager to install the File Services and Web Server (IIS) roles with the role services shown in Figure 2: NUMI Exchange / MDWS Role Services and Figure 3: NUMI Exchange / MDWS Web Services (IIS).

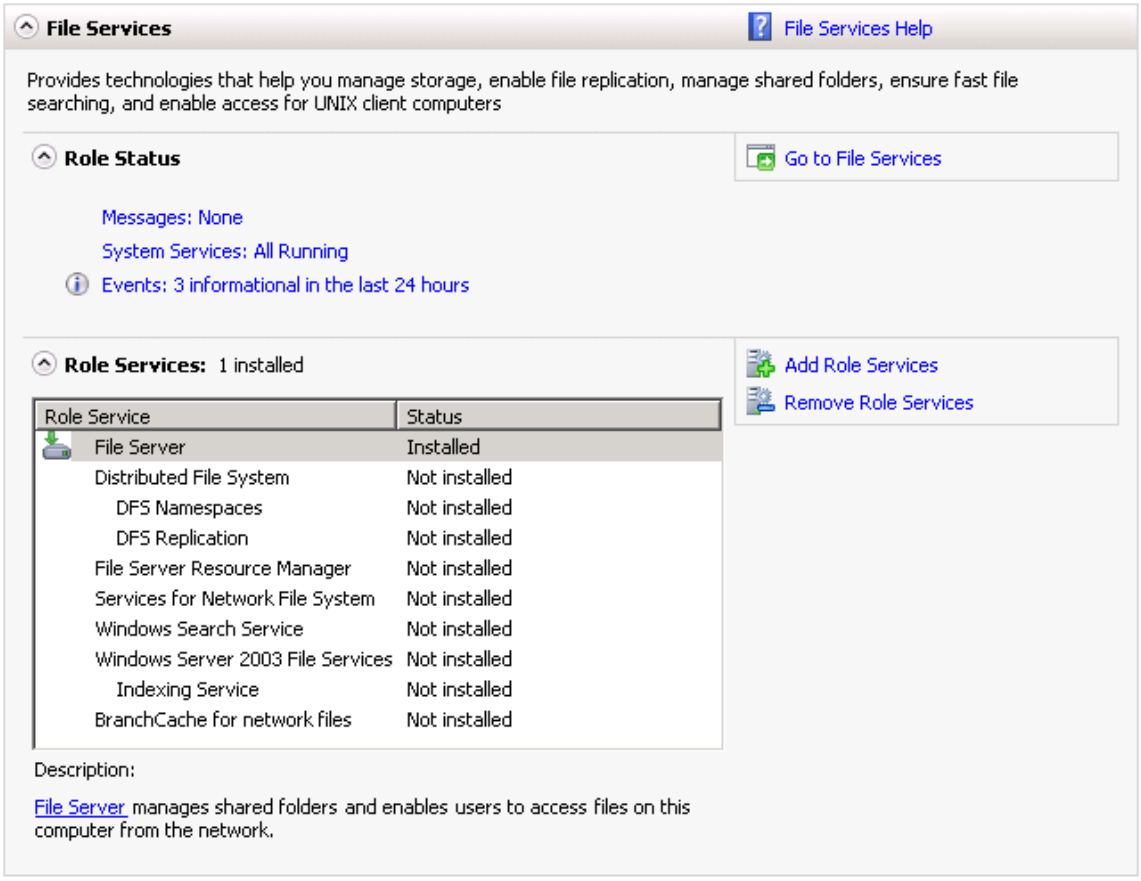

Figure 2: NUMI Exchange / MDWS Role Services

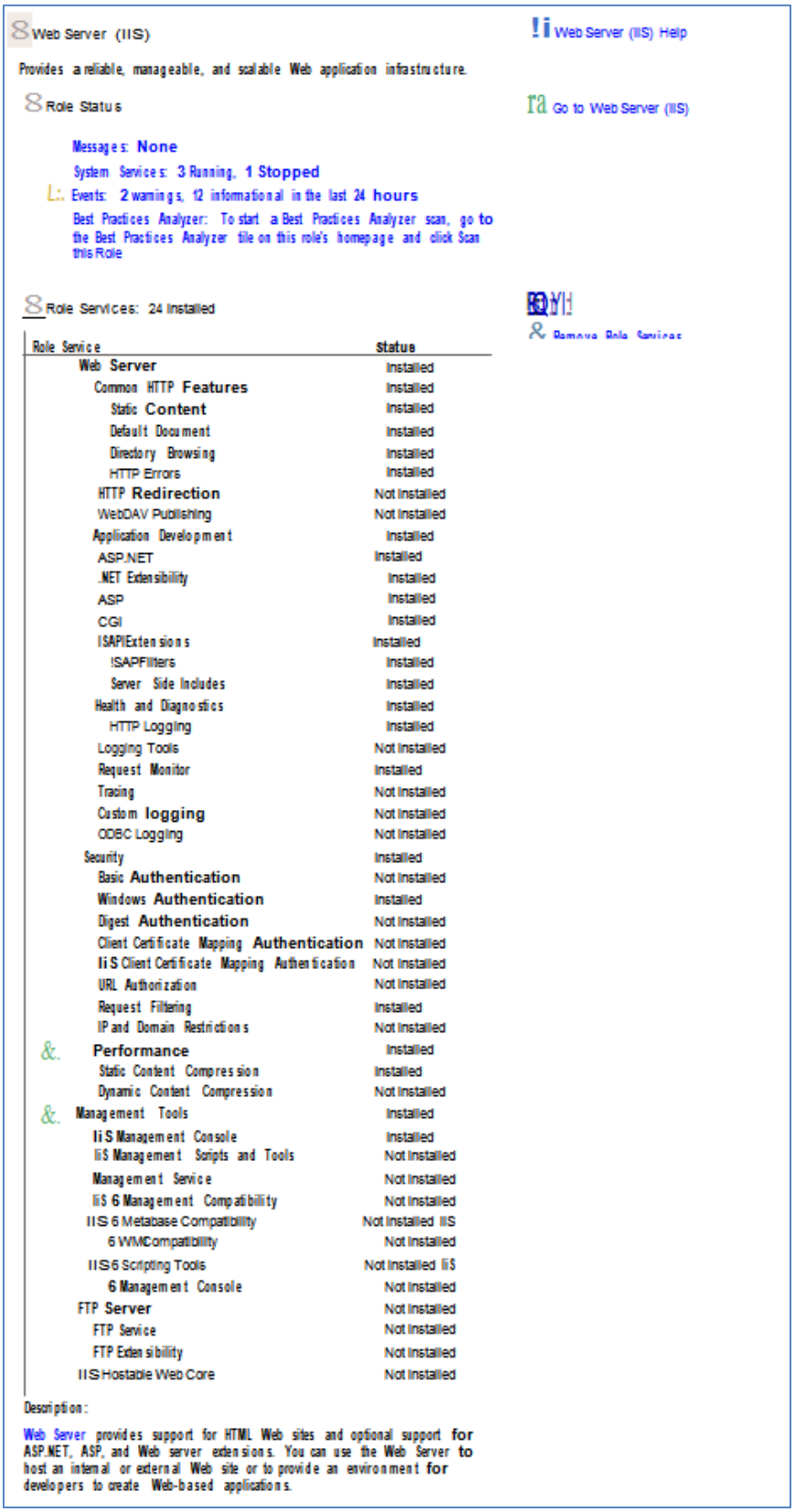

Figure 3: NUMI Exchange/MOWS Web Services (IIS)

6.3.2. ASP.NET 2.0 AJAX Extensions 1.0 Setup

Install the ASP.NET 2.0 AJAX Extensions 1.0 as detailed in section 6.5, Install Microsoft ASP.Net 2.0 AJAX Extensions 1.0.

6.3.3. Microsoft WSE 3.0 Setup

Install Microsoft WSE 3.0 as detailed in section 6.6 Install Microsoft Web Services Enhancements 3.0.

6.4. Application Server Setup (Windows Server 2008 R2)

6.4.1. Role Setup

This applies to the NUMI app servers, with Windows Server 2008 R2 installed. 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).

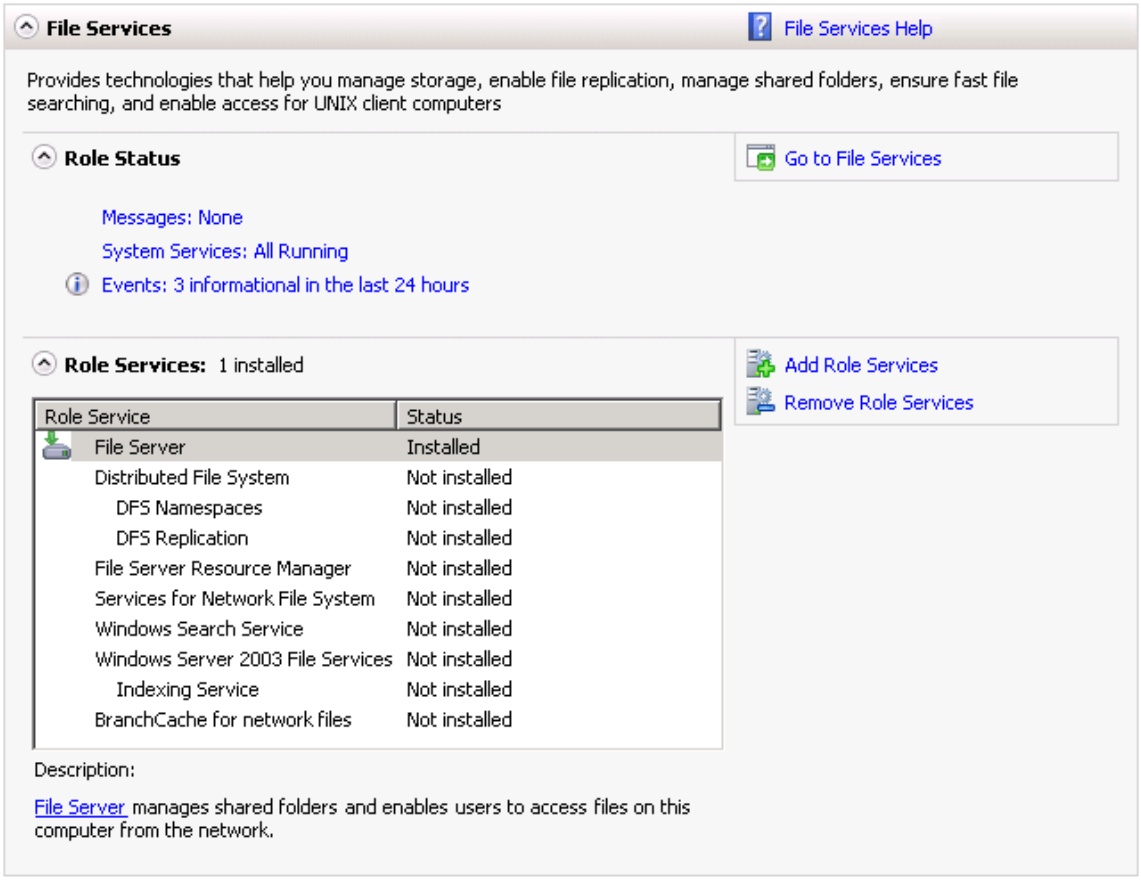

Figure 4: NUMI Role Services

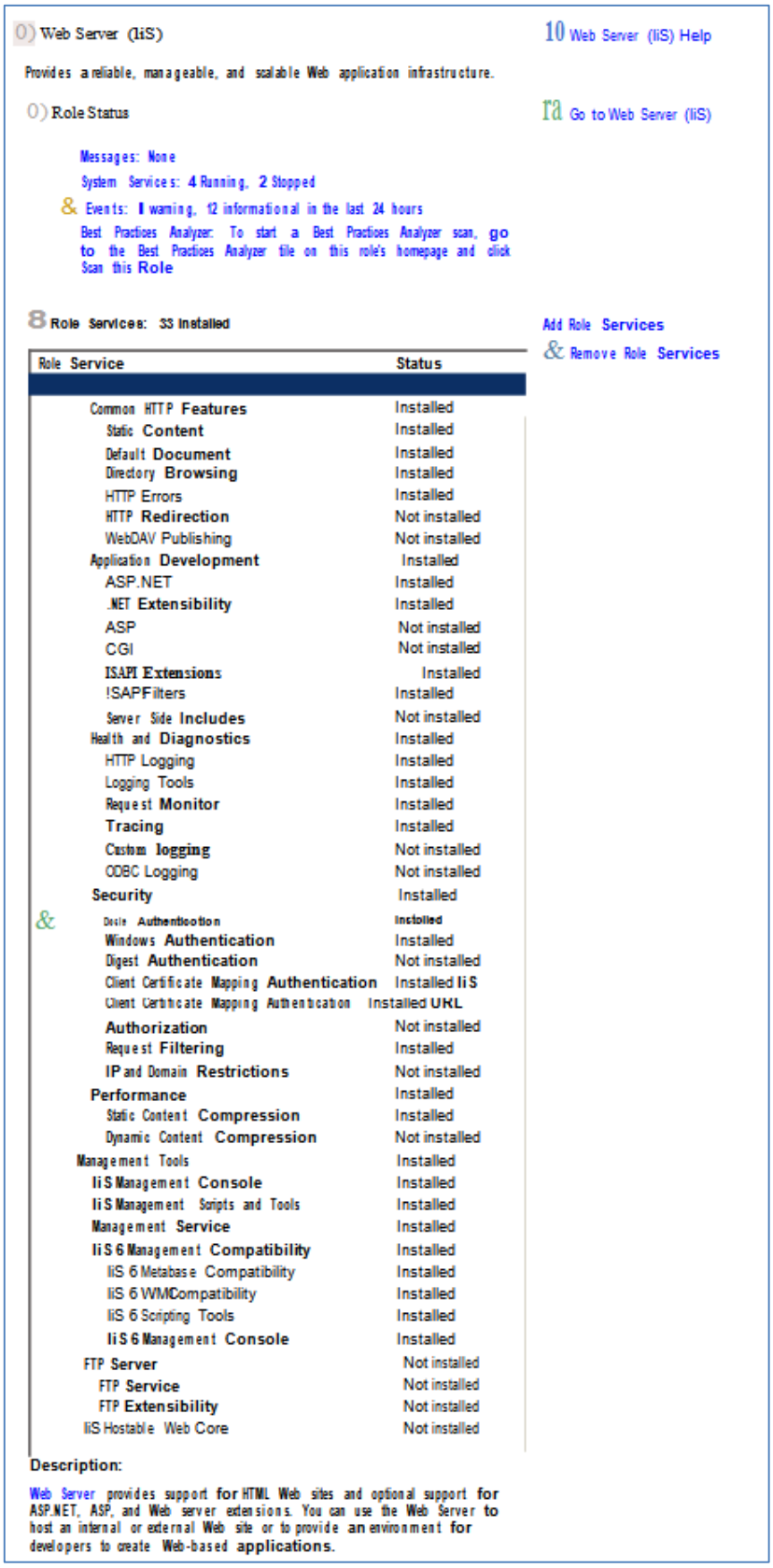

Figure 5: NUMI Web Services IIS

6.4.2. 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.

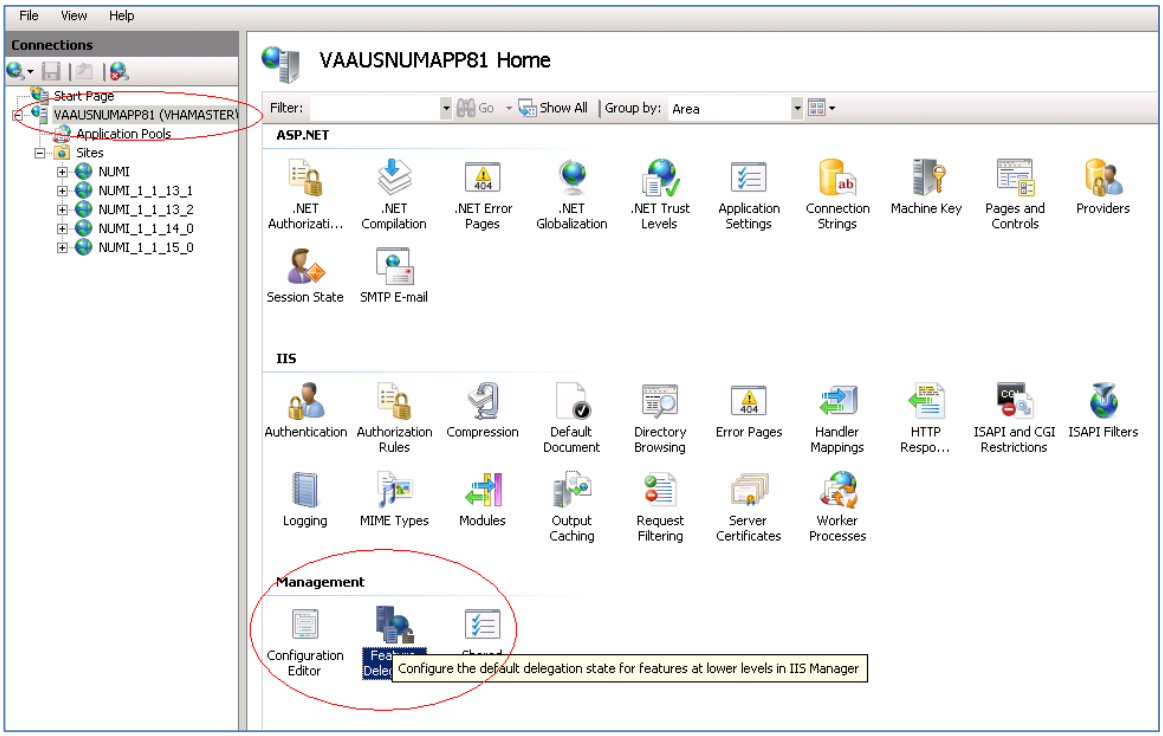

Figure 6: IIS Feature Delegation

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

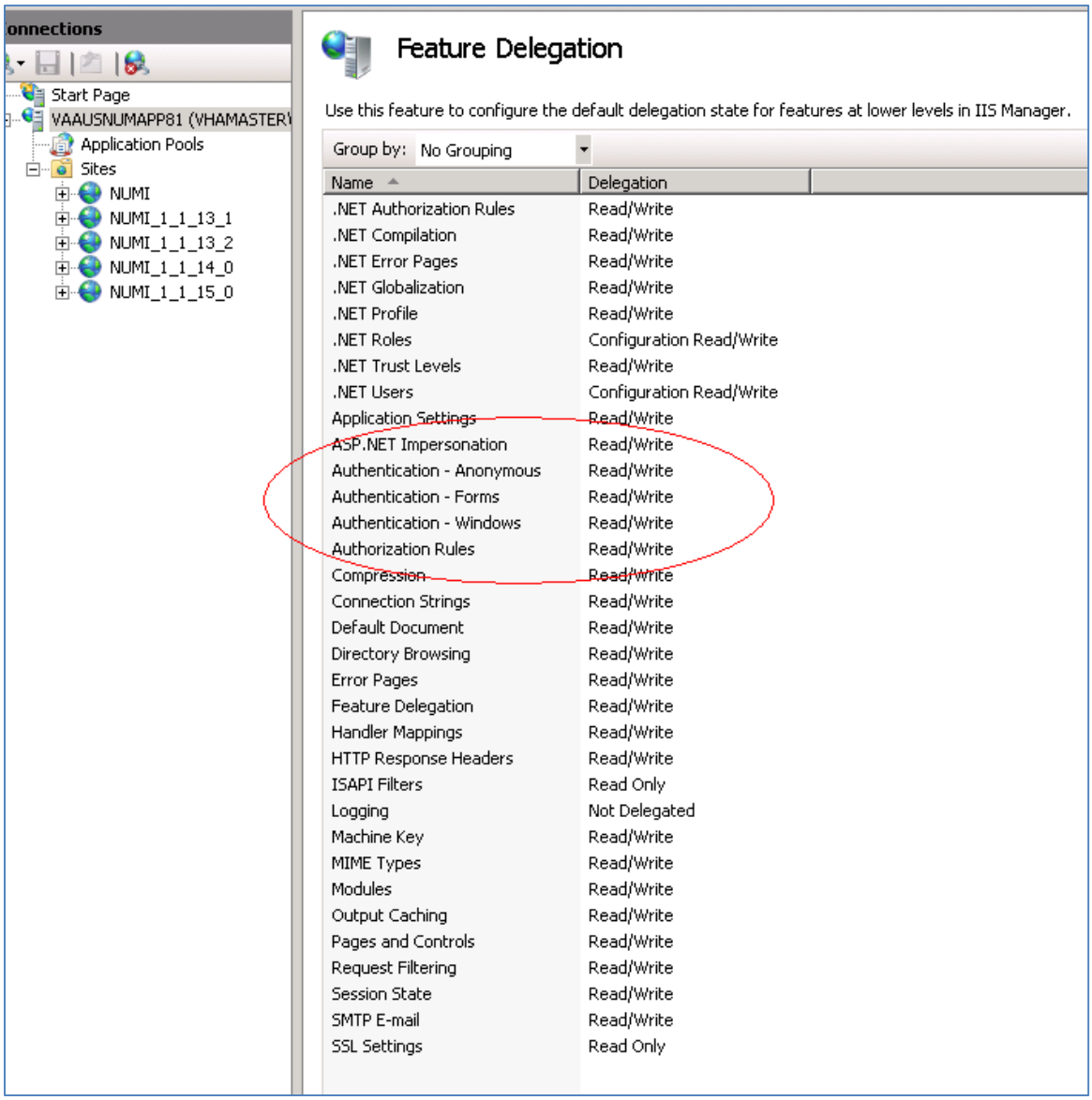

Figure 7: Feature Delegation Selection

6.5. Install Microsoft ASP.Net 2.0 AJAX Extensions 1.0

This applies to the **web** servers only.

1. Download the Microsoft ASP.Net 2.0 AJAX Extensions 1.0 from Microsoft'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: Microsoft ASP.Net 2.0 File Download-Security Warning window).

Figure 8: Microsoft 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: Microsoft ASP.Net 2.0 Internet Explorer-Security Warning window).

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

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

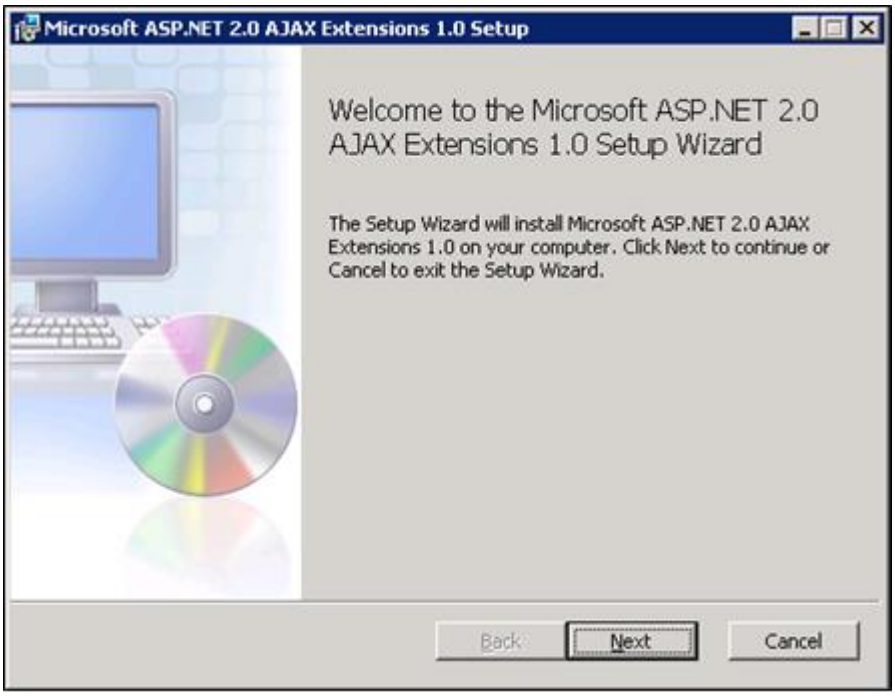

Figure 10: Microsoft ASP.NET 2.0 AJAX Extensions 1.0 Setup Wizard Window

6. *Click* the "**`I accept the terms in the License Agreement`**" checkbox, as illustrated in Figure 11: Microsoft ASP.NET 2.0 AJAX License Agreement window.

7. *Click* the <`Next`> button.

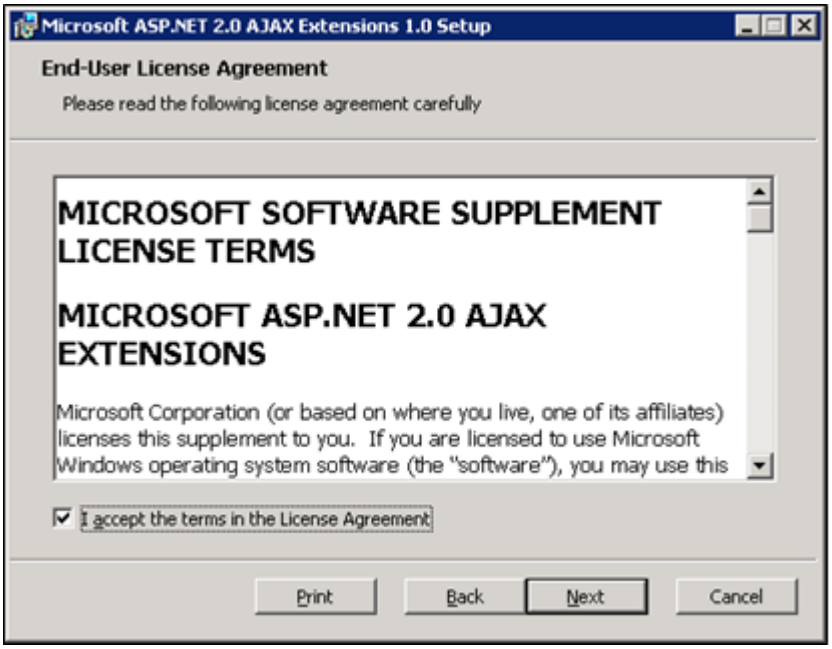

Figure 11: Microsoft ASP.NET 2.0 AJAX License Agreement Window

8. *Click* the <`Install`> button (shown in Figure 12: Microsoft ASP.NET 2.0 AJAX Installation window).

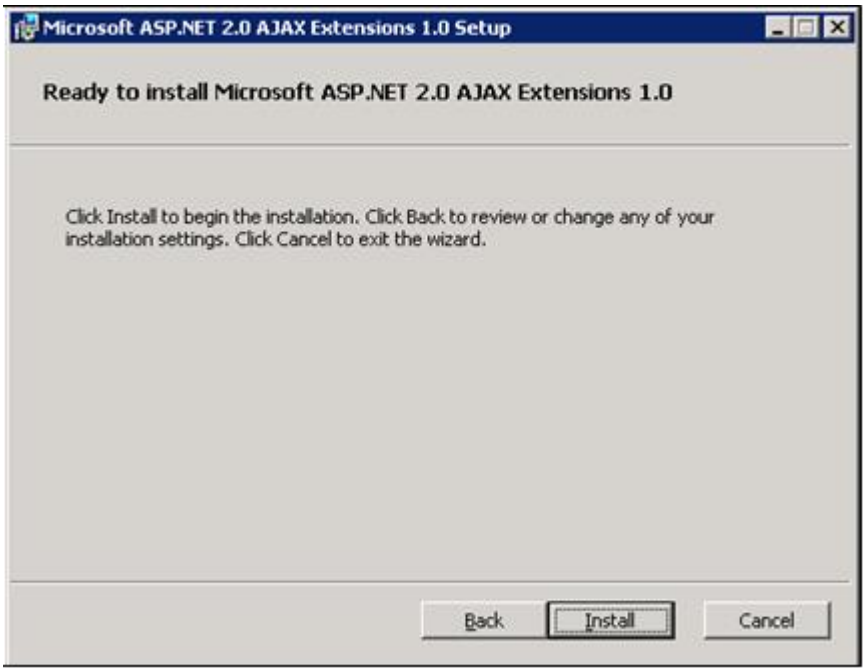

Figure 12: Microsoft ASP.NET 2.0 AJAX Installation Window

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

If you do not wish to view the release notes, *un-check* the "`Display Microsoft ASP.NET 2.0 AJAX Extensions 1.0 Release Notes`" checkbox.

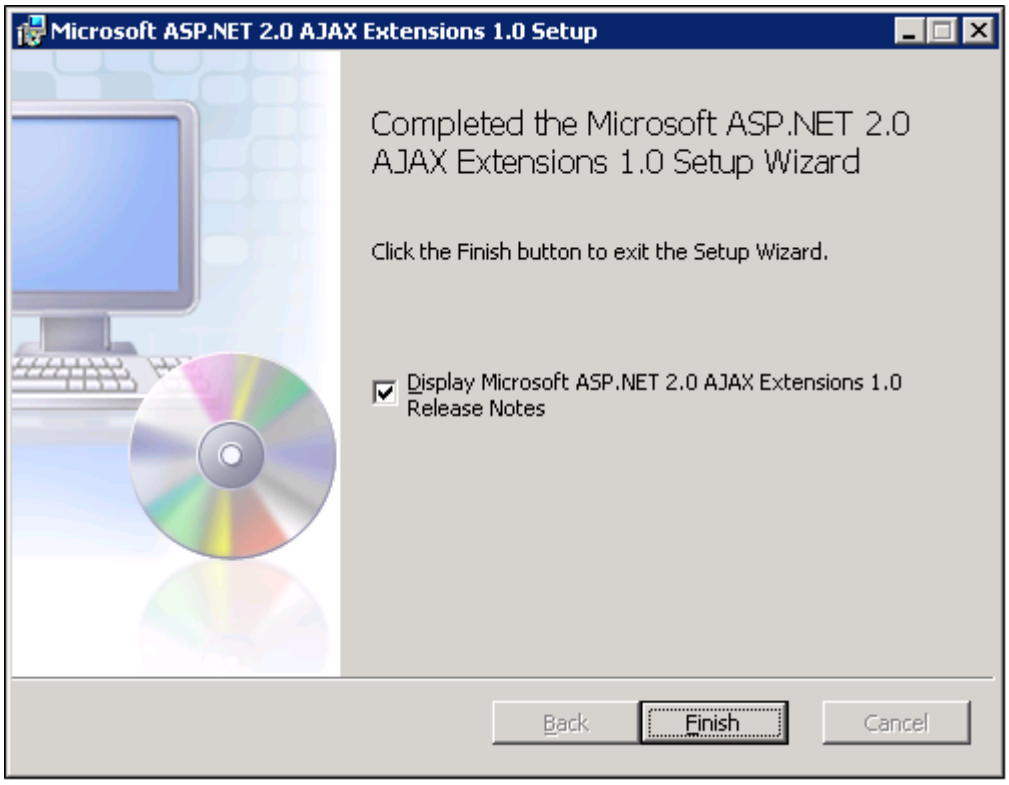

Figure 13: Microsoft ASP.NET 2.0 AJAX Completion window

6.6. Install Microsoft Web Services Enhancements 3.0

This applies to the **web** servers only.

1. Download the Microsoft Web Services Enhancements 3.0 from Microsoft's website.
2. Run the **Microsoft 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: Microsoft WSE 3.0 File Download-Security Warning window).

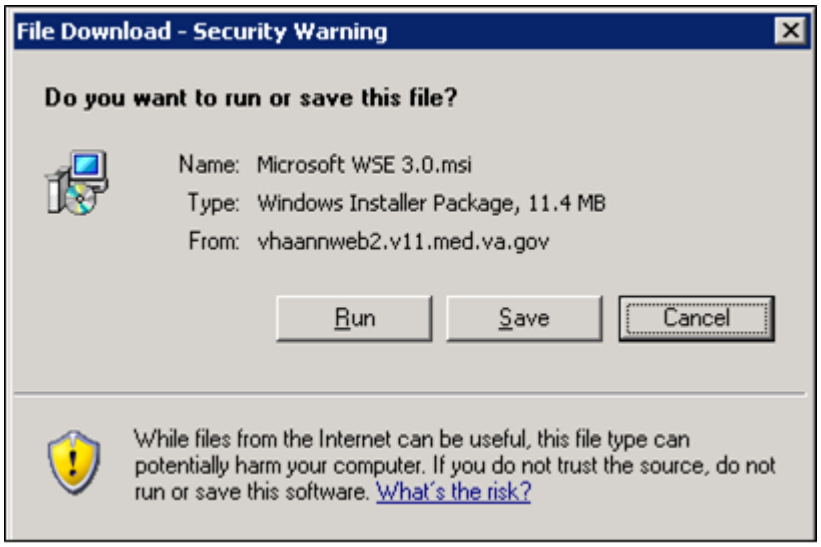

Figure 14: Microsoft WSE 3.0 File Download-Security Warning Window

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

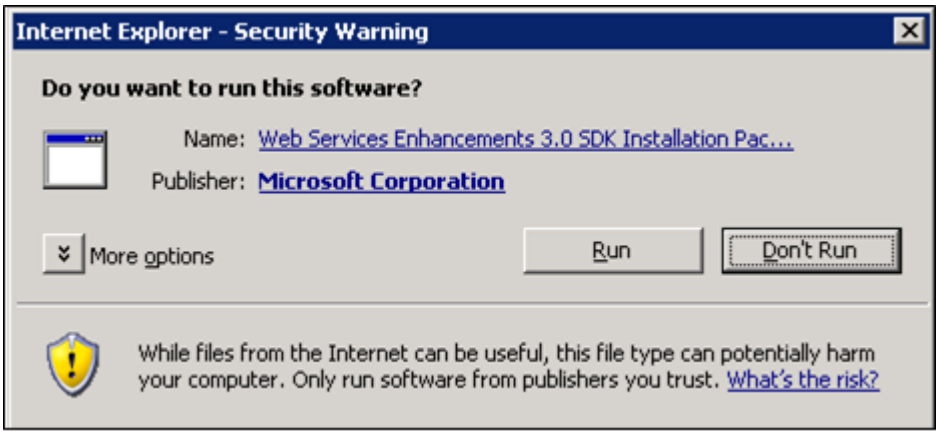

Figure 15: Microsoft WSE 3.0 Internet Explorer-Security Warning Window

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

Figure 16: Microsoft WSE 3.0 InstallShield Wizard Welcome Window

6. *Click* the "**I accept the terms in the license agreement**" checkbox, as illustrated in Figure 17: Microsoft WSE 3.0 License Agreement window.

7. *Click* the <Next> button.

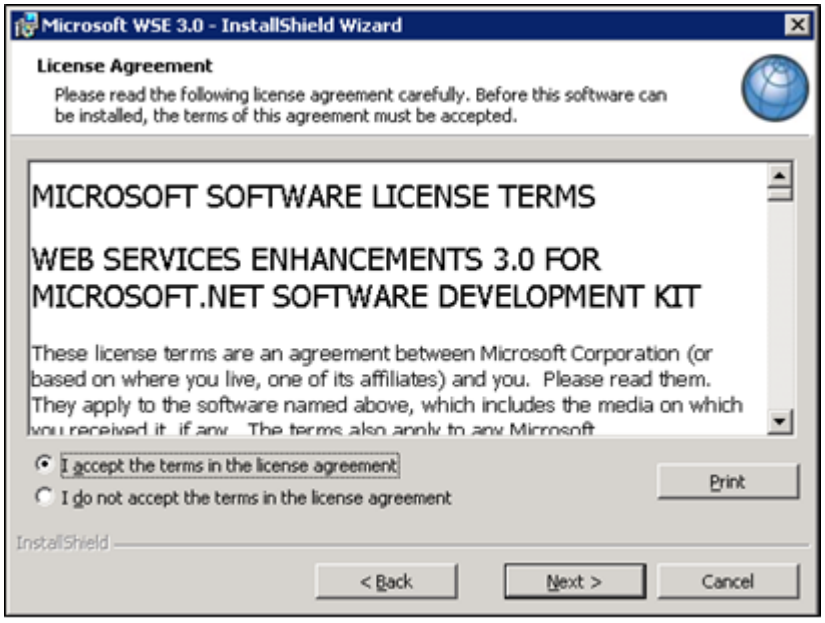

Figure 17: Microsoft WSE 3.0 License Agreement Window

8. *Click* the <Administrator> radio button, as illustrated in Figure 18: Microsoft WSE 3.0 InstallShield Wizard window.\

9. *Click* the <Next> button.

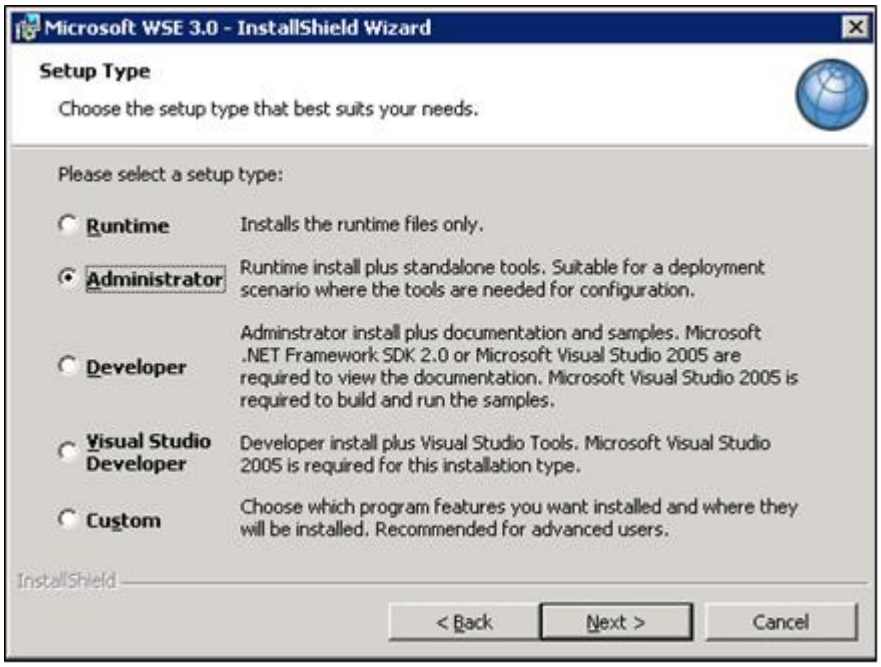

Figure 18: Microsoft WSE 3.0 InstallShield Wizard Window

10. *Click* the <`Install`> button (shown in Figure 19: Microsoft WSE 3.0 Installation window).

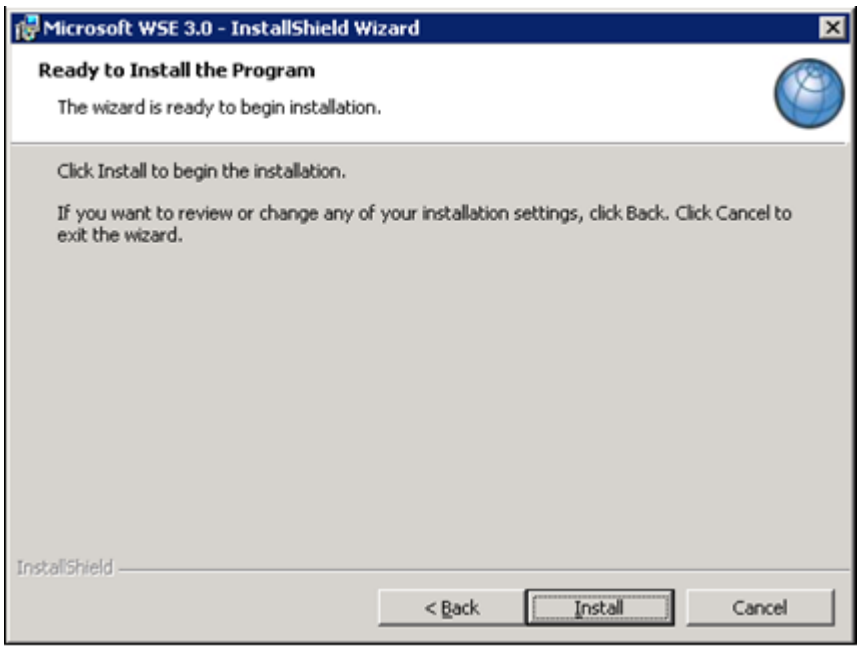

Figure 19: Microsoft WSE 3.0 Installation Window

11. *Click* the <`Finish`> button (shown in Figure 20: Microsoft WSE 3.0 Completion window).

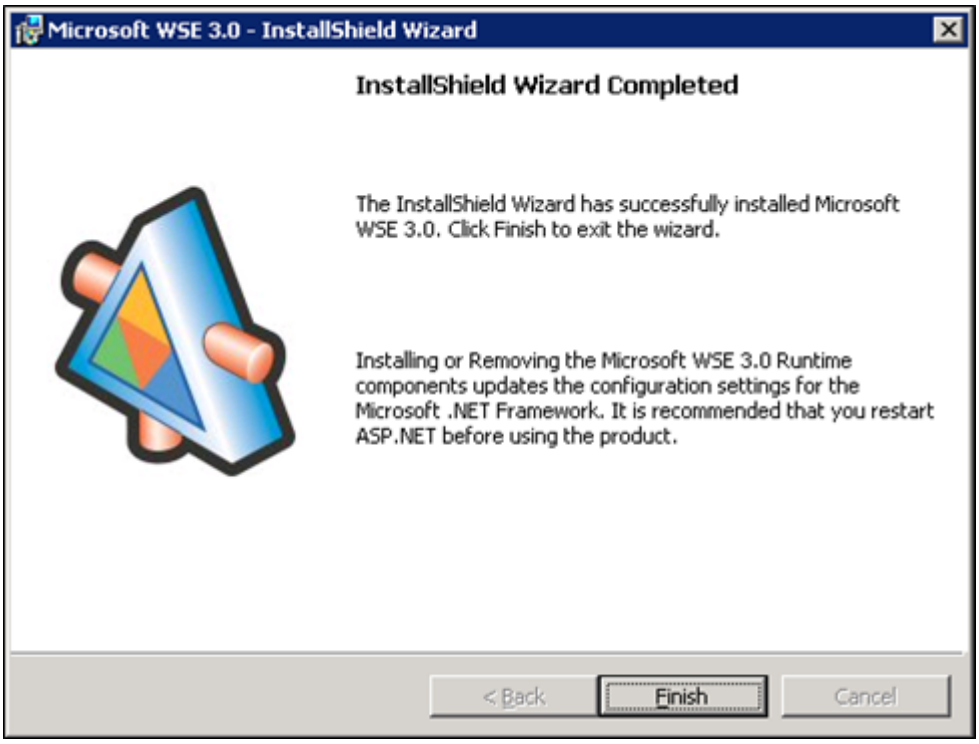

Figure 20: Microsoft WSE 3.0 Completion Window

6.7. Install SQL Server

Install the Microsoft SQL Server 2005 Database Server software only on the **database server**, applying both Microsoft installation instructions and local best practices.

All service packs through SP 3 are required; 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.

6.8. Download all SQL Server Patches

This applies to the **database server** only.

6.9. Restore the Appropriate Databases for the NUMI Application

This applies to the **database server** only.

Follow the instructions in section 5 Instructions for Installing Database Components.

6.10. Installing NUMI Exchange on Server 2008 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.

6.10.1. 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.

6.10.2. NUMI Exchange Web Site Configuration

Using IIS Manager, add a new web site and select the SSL certificate as shown in Figure 21: Add NUMI Exchange web site.

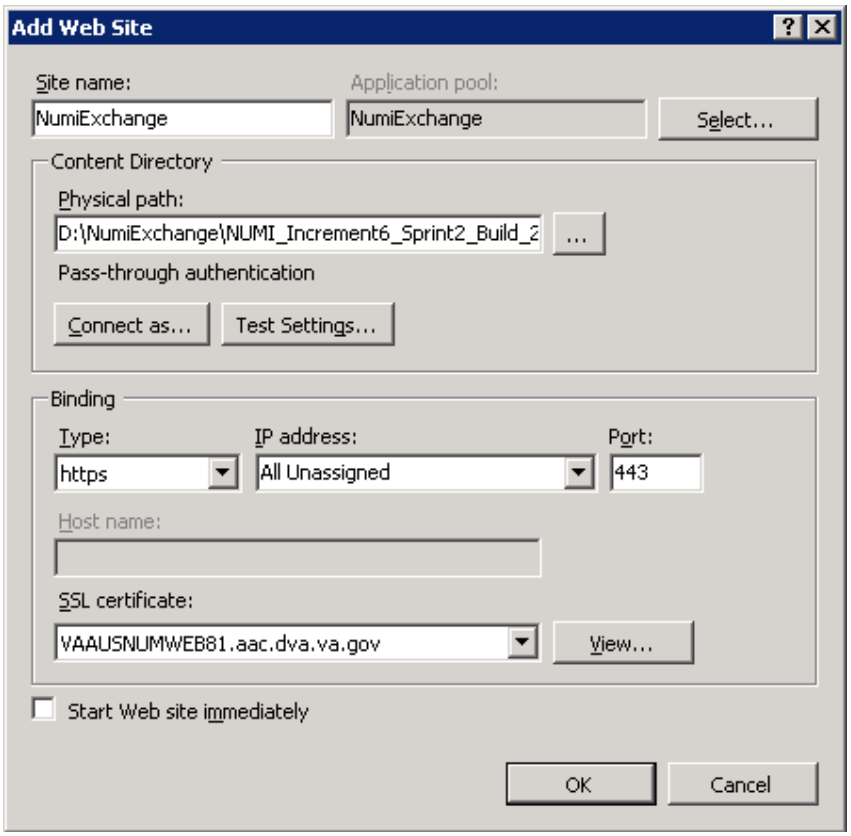

Figure 21: Add NUMI Exchange Website

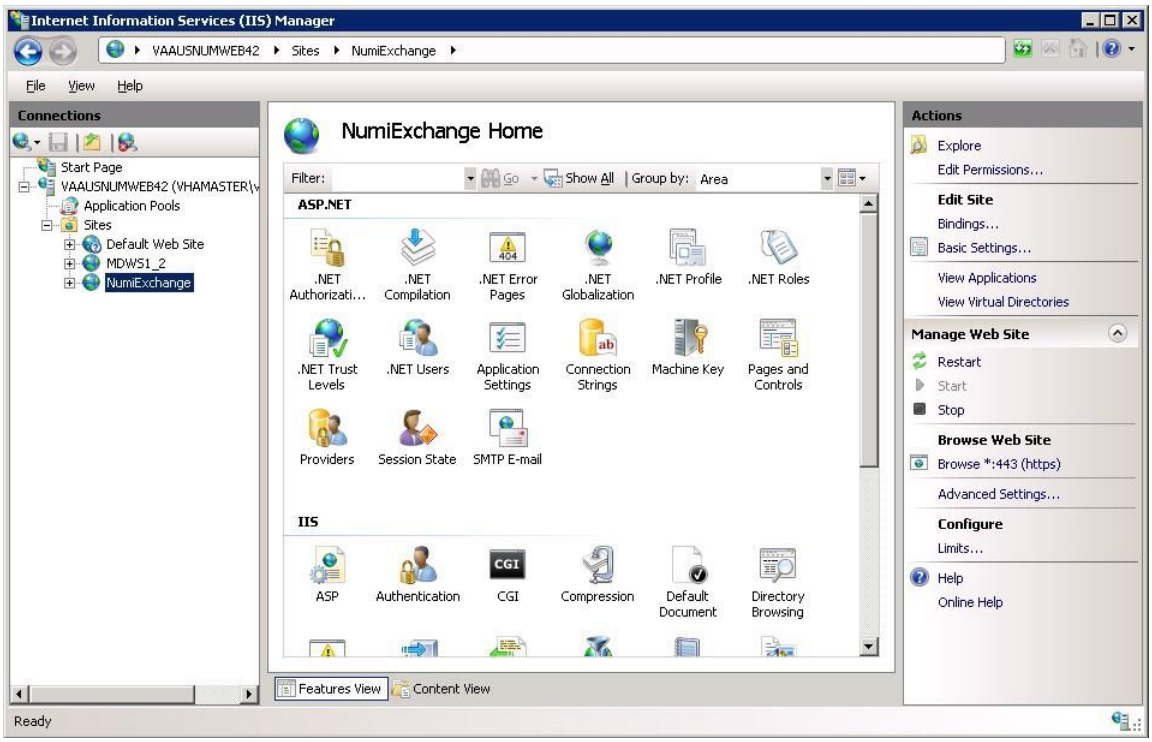

Figure 22: NUMI Exchange Website

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

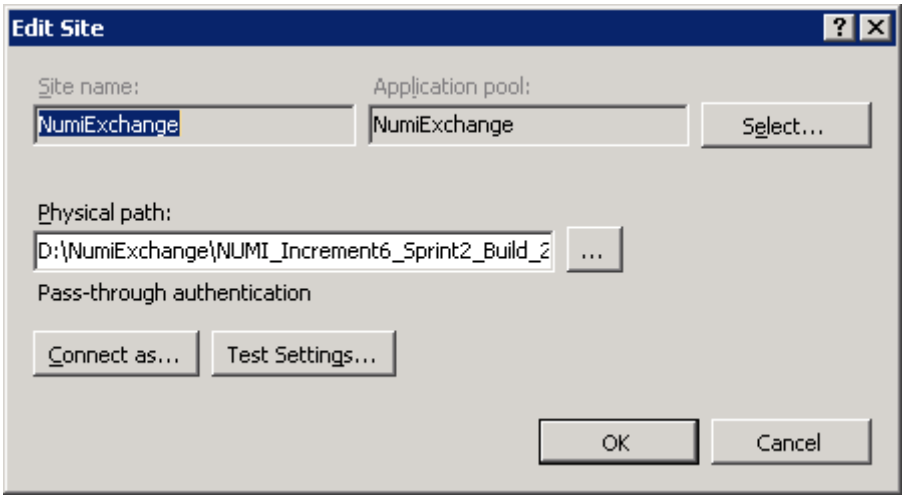

Figure 23: NUMI Exchange Basic Settings

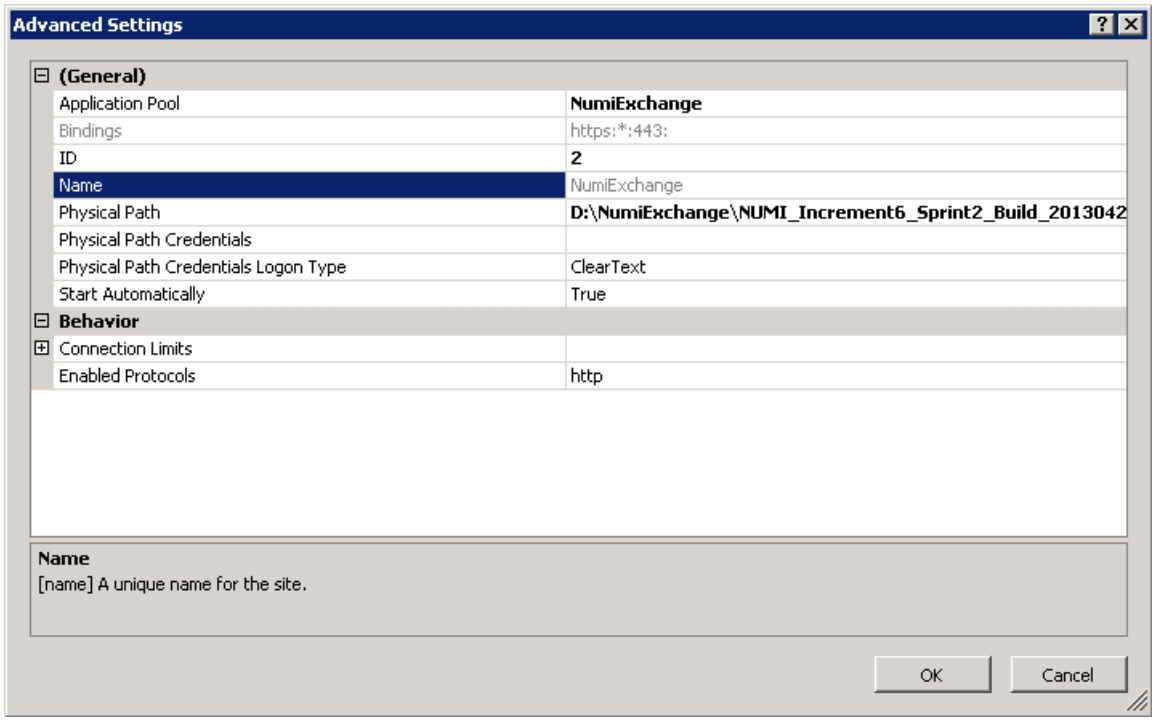

Figure 24: NUMI Advanced Settings

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

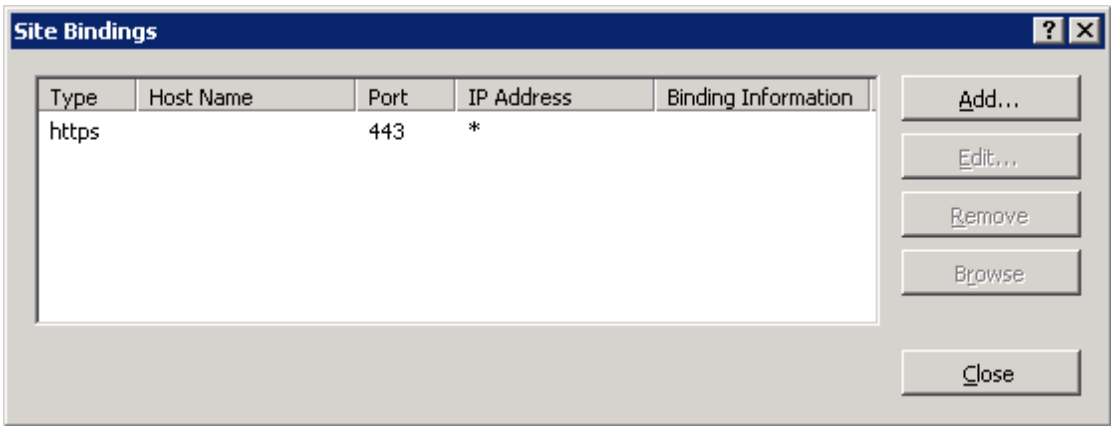

Figure 25: NUMI Exchange Bindings

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

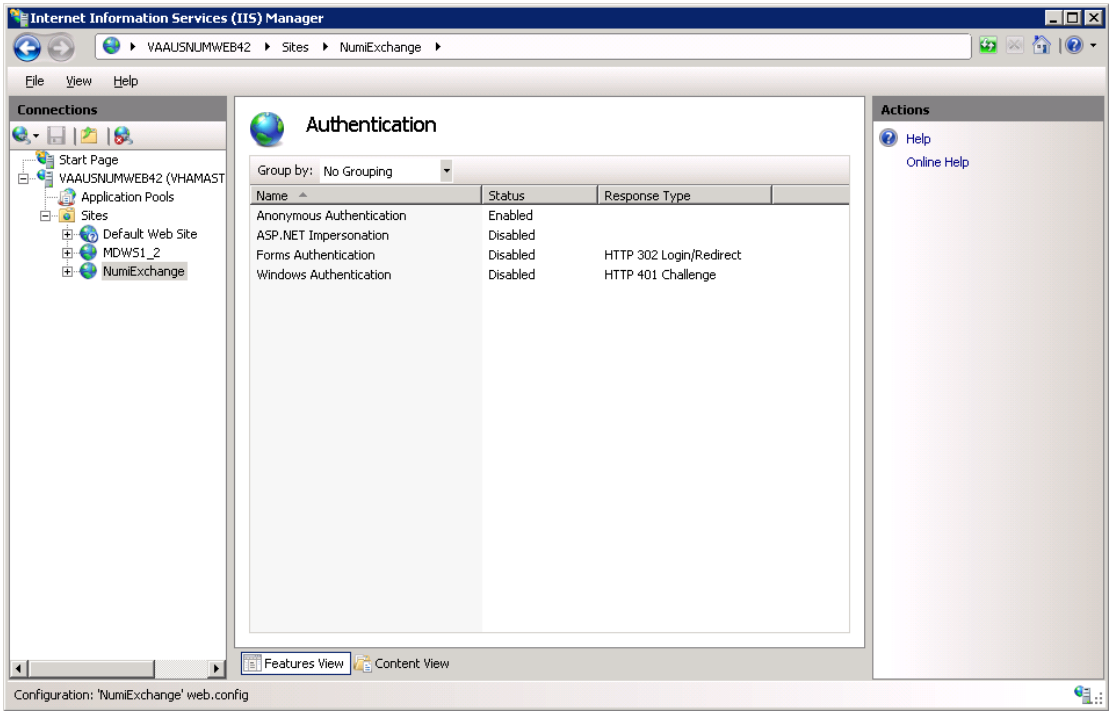

Figure 26: NUMI Exchange Authentication Settings

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

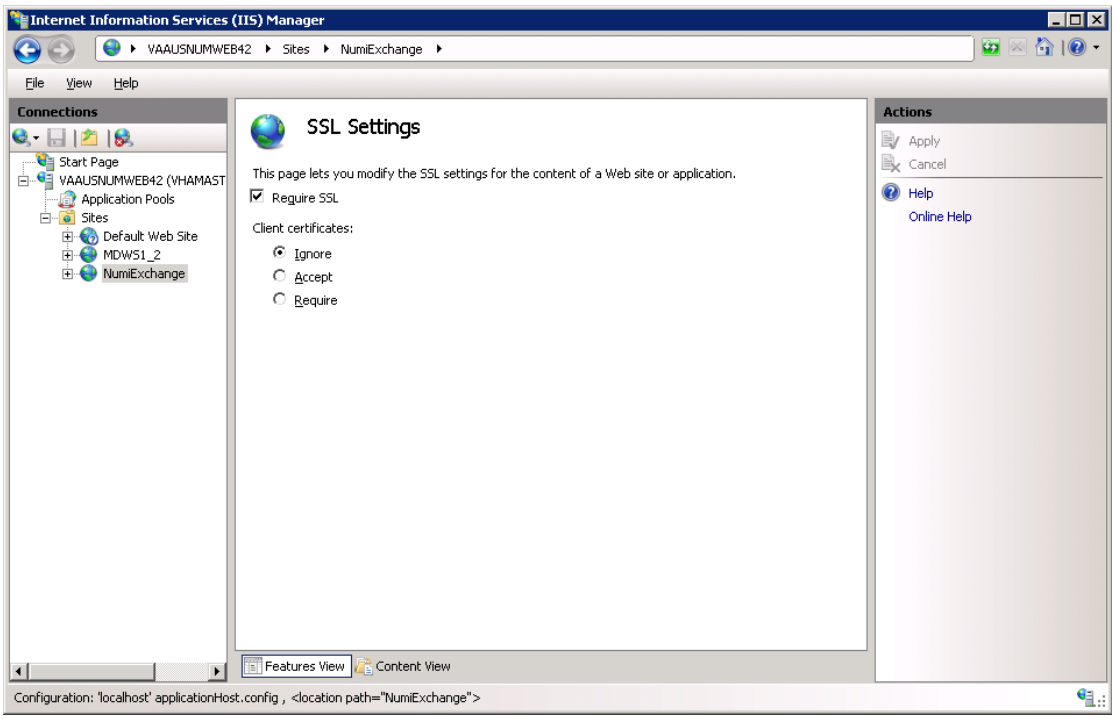

Figure 27: NUMI Exchange SSL Settings

6.10.3. Application Pool Configuration

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

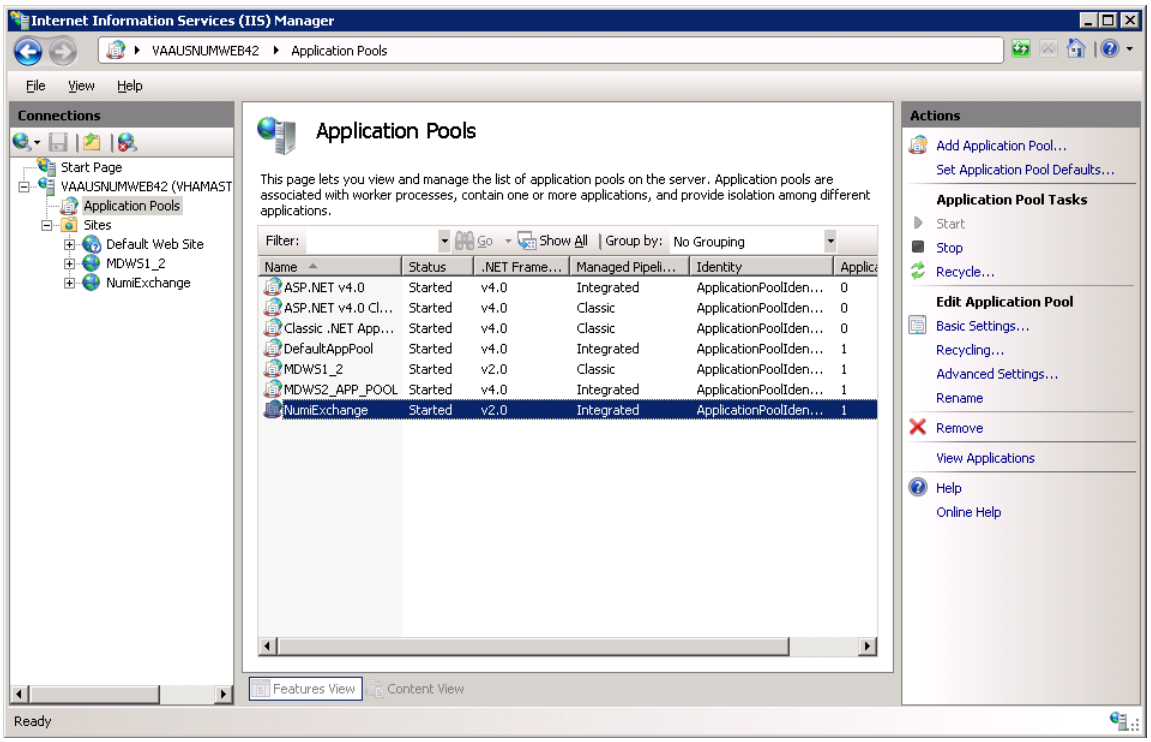

Figure 28: Application Pool Window

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

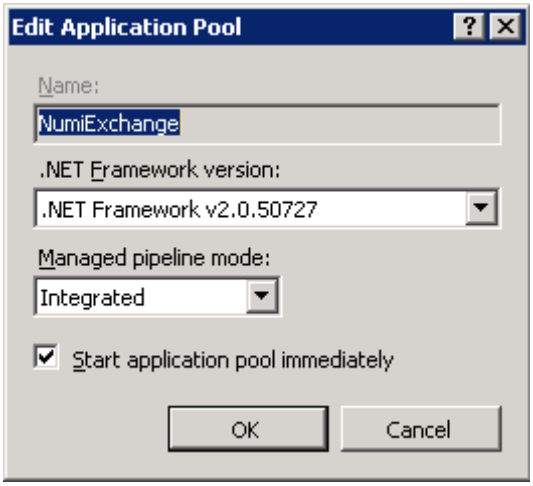

Figure 29: NUMI Exchange Application Pool Basic Settings

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

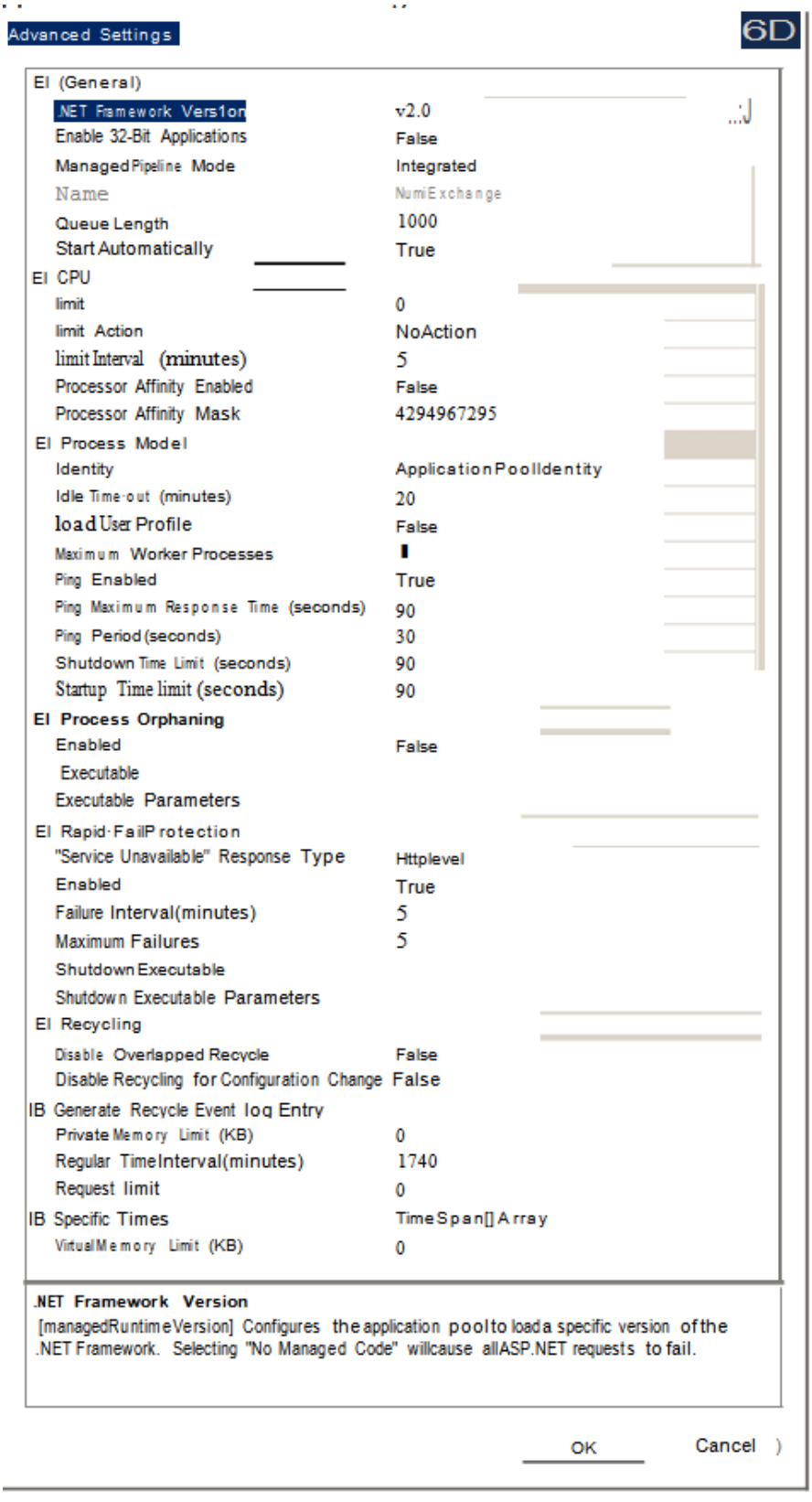

Figure 30: NUMI Exchange Pool Advanced Settings

6.11. Installing MDWS 2.7.3.2 on Server 2008 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.

6.11.1. Download MDWS

Download MDWS 2.7.3.2 from:

ftp://downloads.medora.va.gov/mdws

6.11.2. Install MDWS Distribution

Install MDWS following the MDWS Installation Instructions located at:

http://trac.medora.va.gov/web/wiki/Projects/MDWS/Installation

It is recommended that MDWS be installed in the D:\NUMI folder. e.g., D:\NUMI\NUMI2_7_3_2

The following steps from the MDWS Installation Instructions can be skipped:

- Step 4. SQL Server 2008 (optional for non-BSE installations).
- Step 6. Oracle ODAC Server Software.

web.config settings to update:

<system.webServer>

<defaultDocument >

<files>

<add value=”NumiService.asmx” />

</files>

</defaultDocument>

</system.webService>

6.11.3. MDWS Web Site Configuration

The MDWS web site configuration is shown in Figure 41: Configuring MDWS Website, Figure 42: MDWS Website Basic Settings and Figure 43: MDWS Website Advanced Settings.

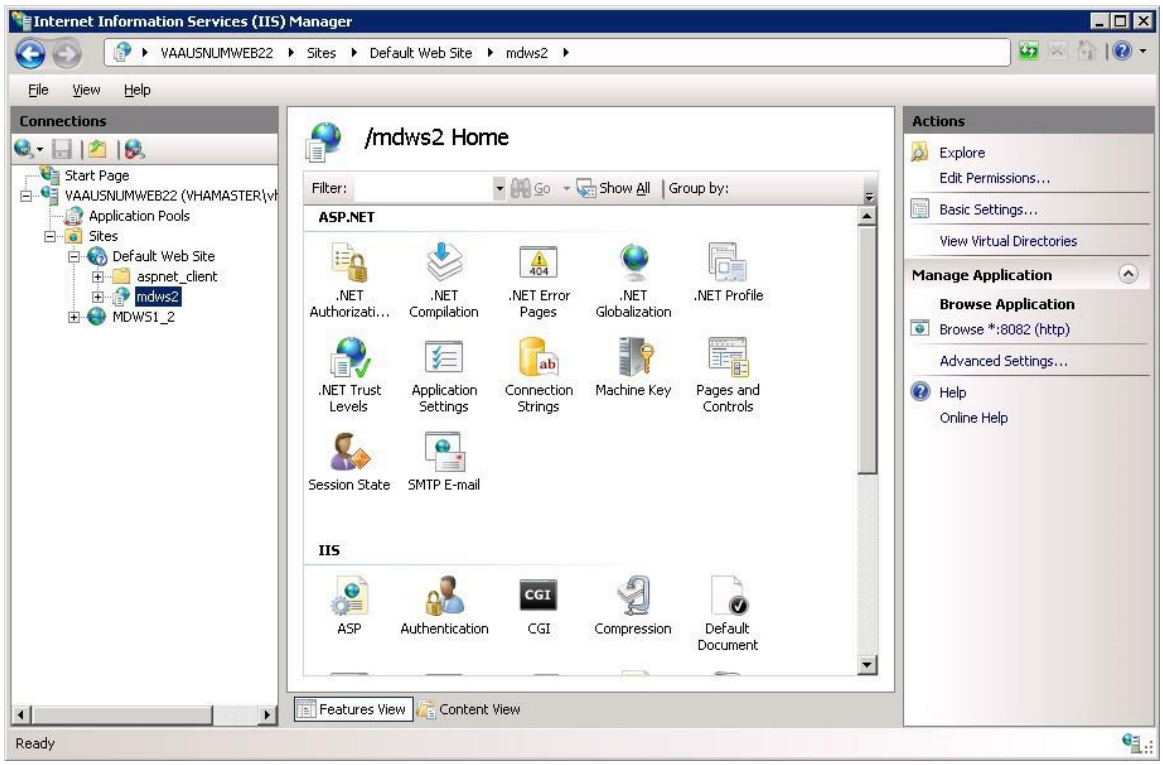

Figure 31: Configuring MDWS Website

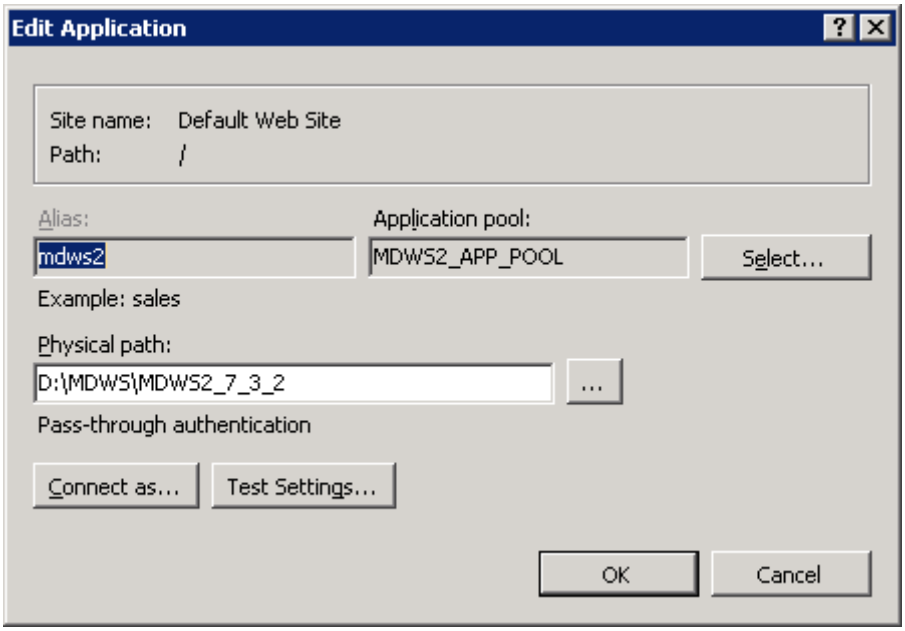

Figure 32: MDWS Website Basic Settings

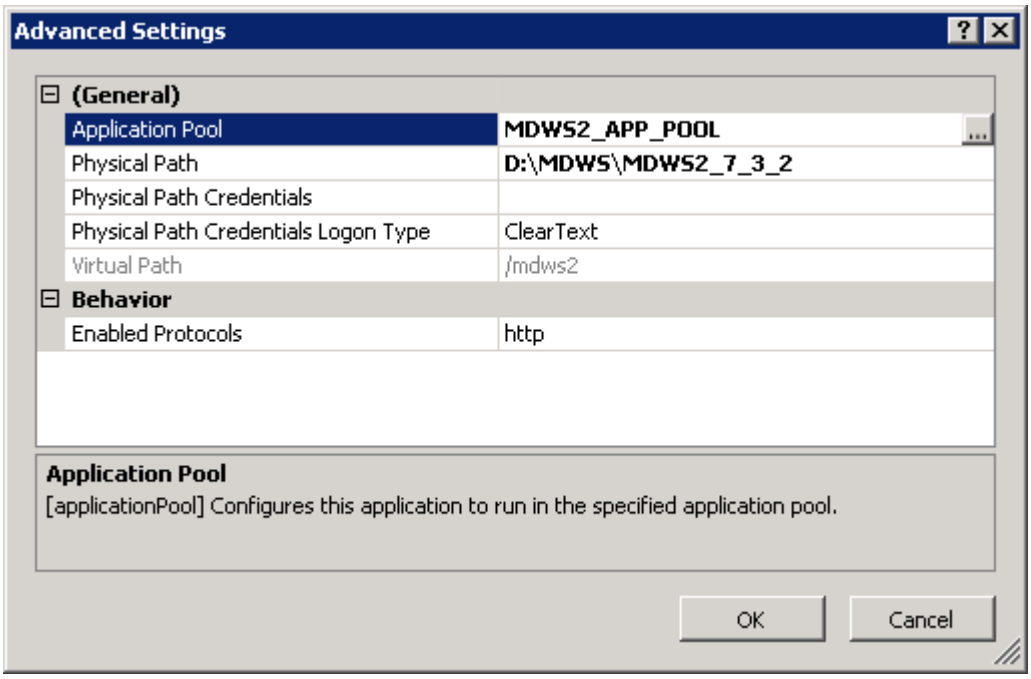

Figure 33: MDWS Website Advanced Settings

The MDWS bindings configuration is shown in Figure 44: MDWS Default Website and Figure 45: MDWS Bindings, If NUMI Exchange is installed on the server using port 80, then configure MDWS to use a different port, e.g., port 8082.

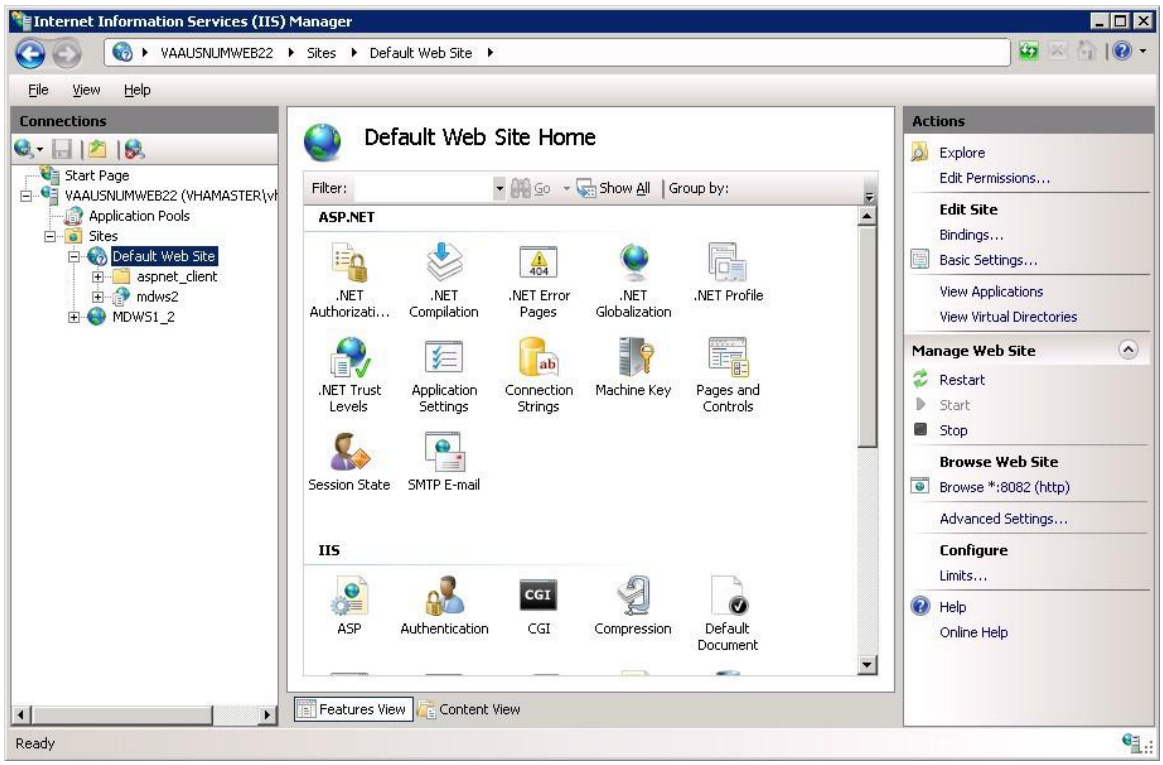

Figure 34: MDWS Default Website

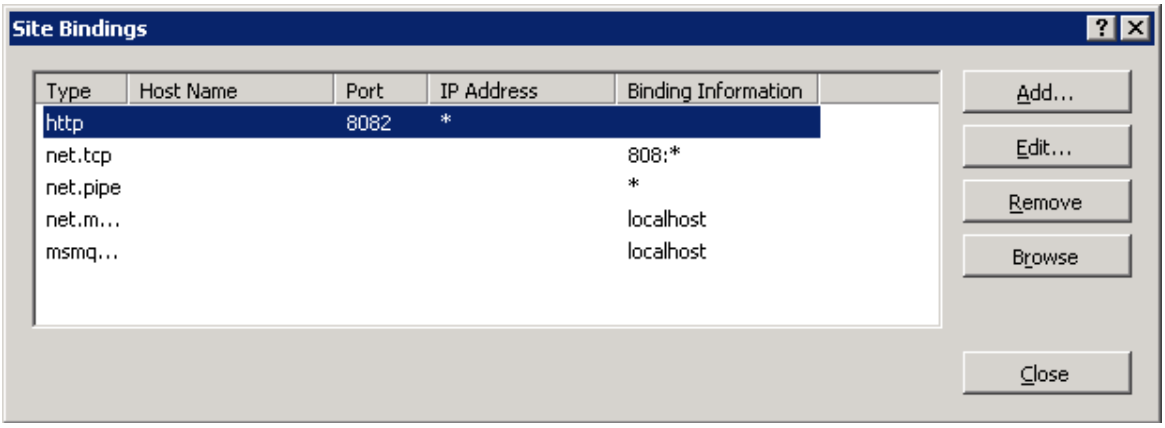

Figure 35: MDWS Bindings

The MDWS authentication setup is shown in Figure 46: MDWS Authentication.

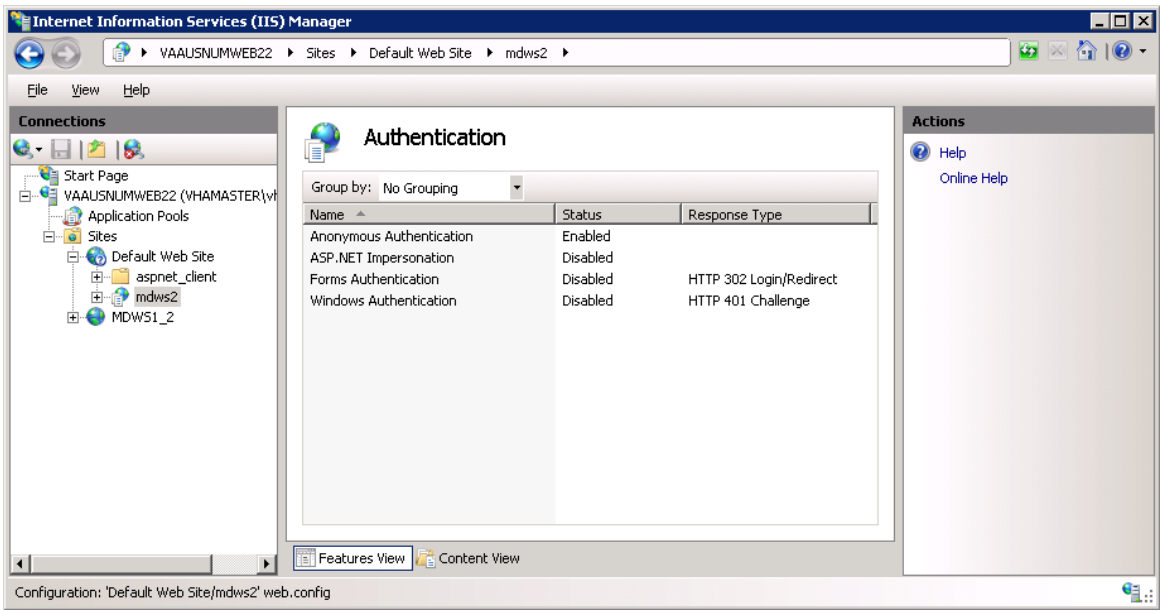

Figure 36: MDWS Authentication

6.11.4. Configuration File Setup

Web.Config

Verify the httpExecution timeout field in the MDWS web.config file:

<httpRuntime executionTimeout=”900” />

VhaSites.xml

If there are any new VistA sites to add to MDWS, add the site information in the MDWS VhaSites.xml file. Follow the same format used for existing sites already in the file. The file is located in the xml folder of the resources directory in the MDWS website directory. E.g., D:\MDWS\MDWS2_7_3_2\resources\xml\VhaSites.xml.

6.11.5. MDWS Application Pool Configuration

The application pool settings are shown in Figure 47: Configuring Application Pool Settings, Figure 48: MDWS Application Pool Basic Settings and Figure 49: MDWS Application Pool Advanced Settings.

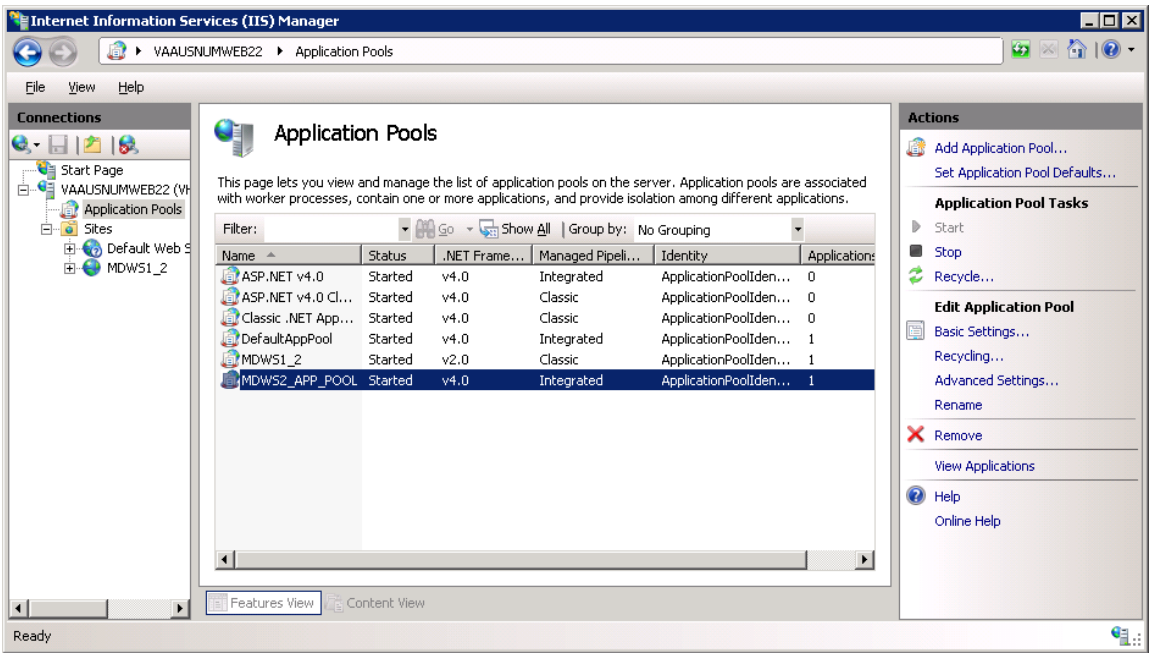

Figure 37: Configuring Application Pool Settings

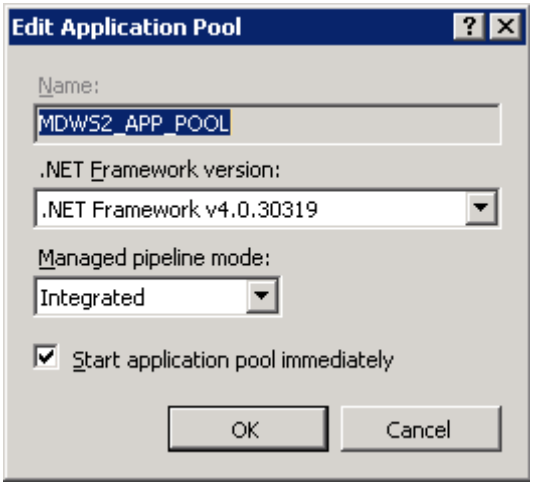

Figure 38: MDWS Application Pool Basic Settings

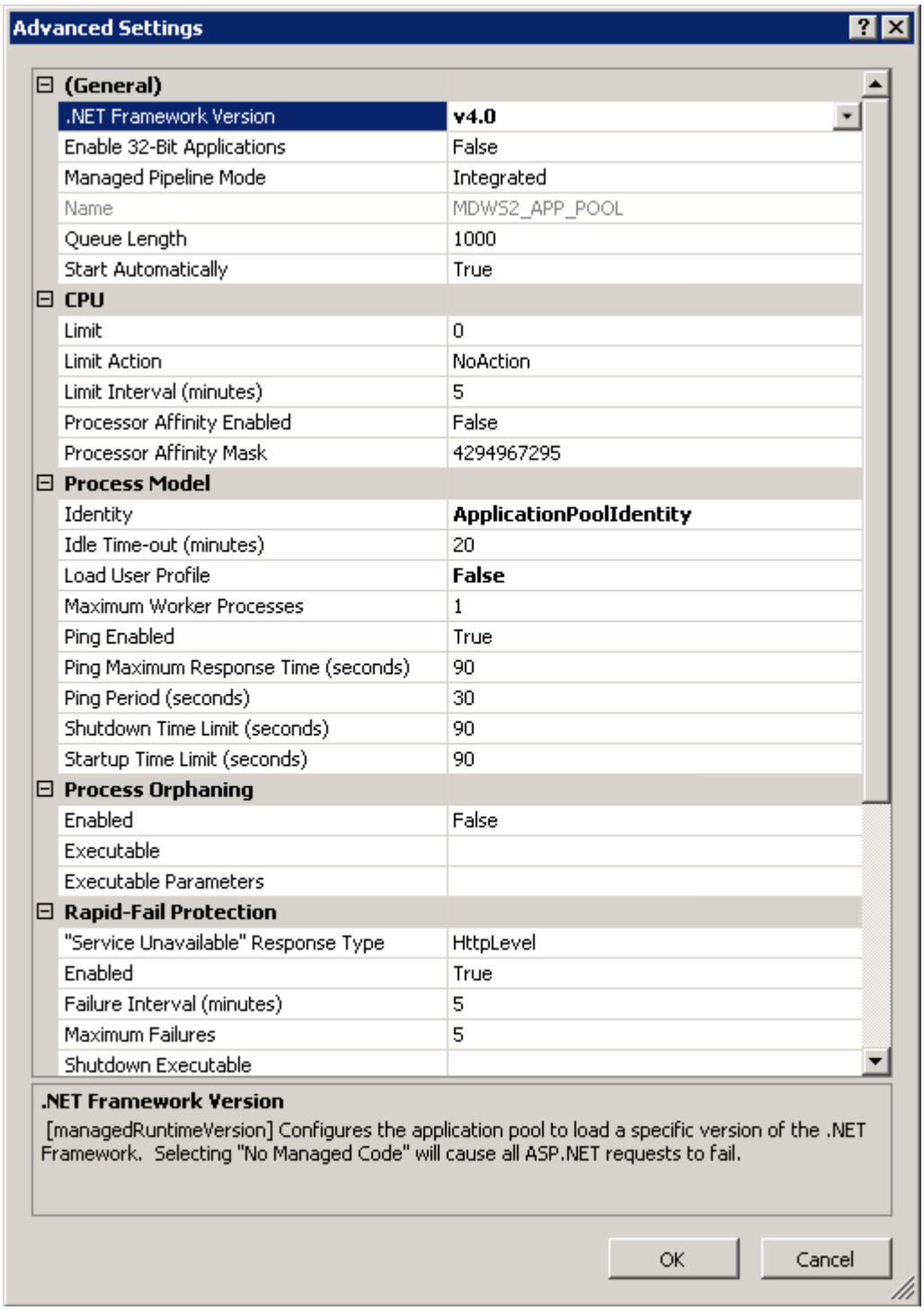

Figure 39: MDWS Application Pool Advanced Settings

6.11.6. To Restart IIS

1. *Click* <Start>.
2. *Click* the **Command Prompt** (or <Run>, depending on the Operating System).

3. Type: `IISReset.`
4. *Click* <`Enter`>.

 Watch the command lines to make sure IIS stops and then starts again.

6.11.7. To Test That MDWS Is Working

1. Open a browser on the **application** server and enter the following in the Address bar:

http://localhost/NumiService.asmx

2. You have the ability to enter either <`localhost`>, <`the actual IP address`> or <`the name of the server`>. Examples: http://localhost/NumiService.aspx and http://hostname.aac.va.gov/NumiService.aspx
3. *Click* the <`Go`> button on the browser to go to the address.
4. The ***NUMI SERVICE*** page will display.
5. Choose "ConnectAndLogin"
6. In the **Sitecode** field, enter the code for the VistA you are trying to access.
7. Put in your Access and Verify Codes for the username and password.
8. Leave the context field blank.
9. *Click* the <`Invoke`> button.
10. If the connection is successful, the VistA welcome message will display in the form of an xml file. Example:

```
<?xml version="1.0" encoding="utf-8" ?>
- <UserTO xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://mdws.med.va.gov/numi/NumiService">
  <name>Doe,John</name>
  <SSN>000000001</SSN>
  <DUZ>10000000000</DUZ>
  <siteId>506</siteId>
  <orderRole>0</orderRole>
  <greeting>Good evening DOE,JOHN</greeting>
  <siteMessage>.................. DEPARTMENT OF VETERANS AFFAIRS VVV
V*AAAA.............. ANN ARBOR VA HEALTH SYSTEM VVV V*A AAA.............
VVV V*A AAA.......... WARNING: UNAUTHORIZED ACCESS, INCLUDING VVV
V*AAAAAAAAAA........ USE OF ACCESS CODES OTHER THAN YOUR OWN, OR
VVVVV*A AAAAAAAA..... MISUSE OF THIS SYSTEM AND/OR ITS DATA IS A VVV*A
AAAAAAAA.... FEDERAL FELONY WARRANTING FBI INVESTIGATION. V*A
AAAAAAAA.. >>> Production Account <<< ---------------------------------
---------------------------------------------- USER HELP TO INCLUDE
VISTA ACCESS/VERIFY, TELEPHONE PINS, OR NETWORK ACCESS PROBLEMS:
Contact your service ADPAC or the Information Systems Help Desk
(x53500) Help Desk hours 7:00am - 4:30pm, Mon-Fri; for EMERGENCY
repairs after 4:30pm, please call the AOD at x55279. SYSTEM BACKUP
SCHEDULE: Monday - Friday 1:30 a.m. * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * VERIFY CODES must now be 8
characters long and contain at least one letter, one number, and one
symbol(!#$%&*.,><). Thank you. This is a PRODUCTION
account.</siteMessage>
  </UserTO>
```

Figure 40: Sample Welcome Message

If the Access and Verify codes are incorrect, this message will be imbedded in the xml:

```
<message>Not a valid ACCESS CODE/VERIFY CODE pair.</message>
```

If the Site code is incorrect, this message will be imbedded in the xml:

<message>No site for sitecode 50**</message>**

Other error messages my display due to connectivity issues.

11. After successfully testing the connection, *click* the <here> link in the following string:

'Click here for a complete list of operations'.

12. Select <Disconnect> from the list.

13. *Click* the <Invoke> button. This will prevent a connection from being left open.

6.12. Installing NUMI on Server 2008 R2

6.12.1. Software Copy Instructions

Right click on the zip file and 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.

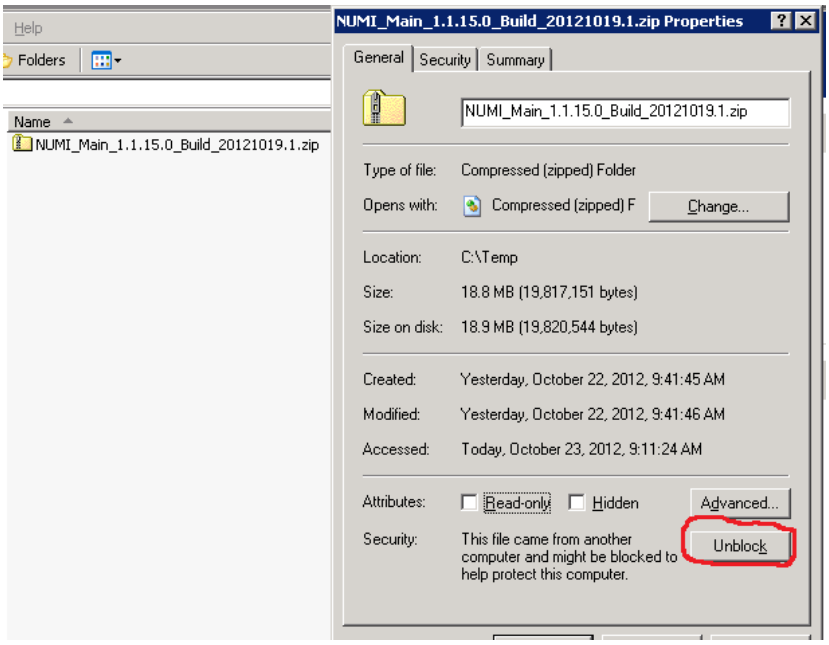

Figure 41: Unblocking Restricted Files in Installation ZIP File

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.

6.12.2. NUMI Web Site Configuration

Using IIS Manager, add a new web site as shown in Figure 52: Add NUMI web site.

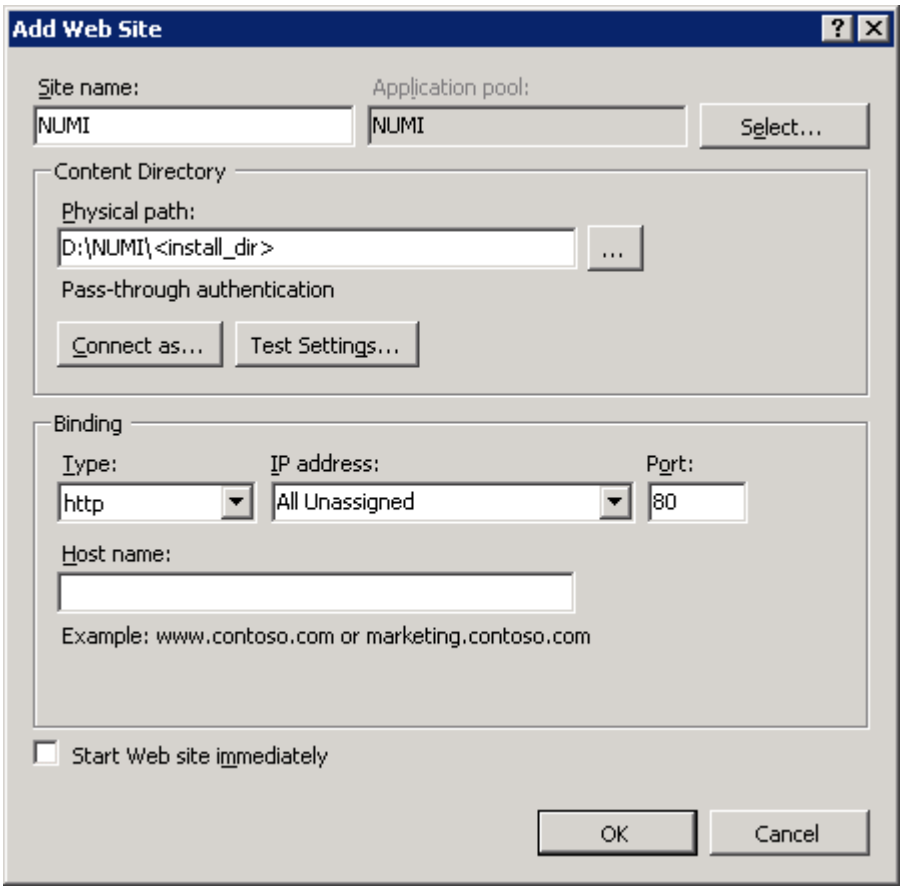

Figure 42: Add NUMI Website

The NUMI web site basic and advanced settings are shown in Figure 53: NUMI Basic Settings and Figure 54: NUMI Advanced Settings.

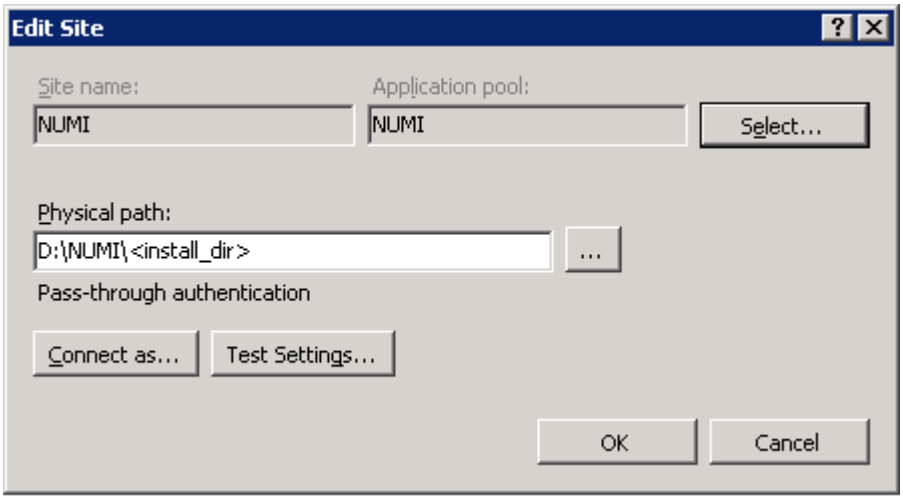

Figure 43: NUMI Basic Settings

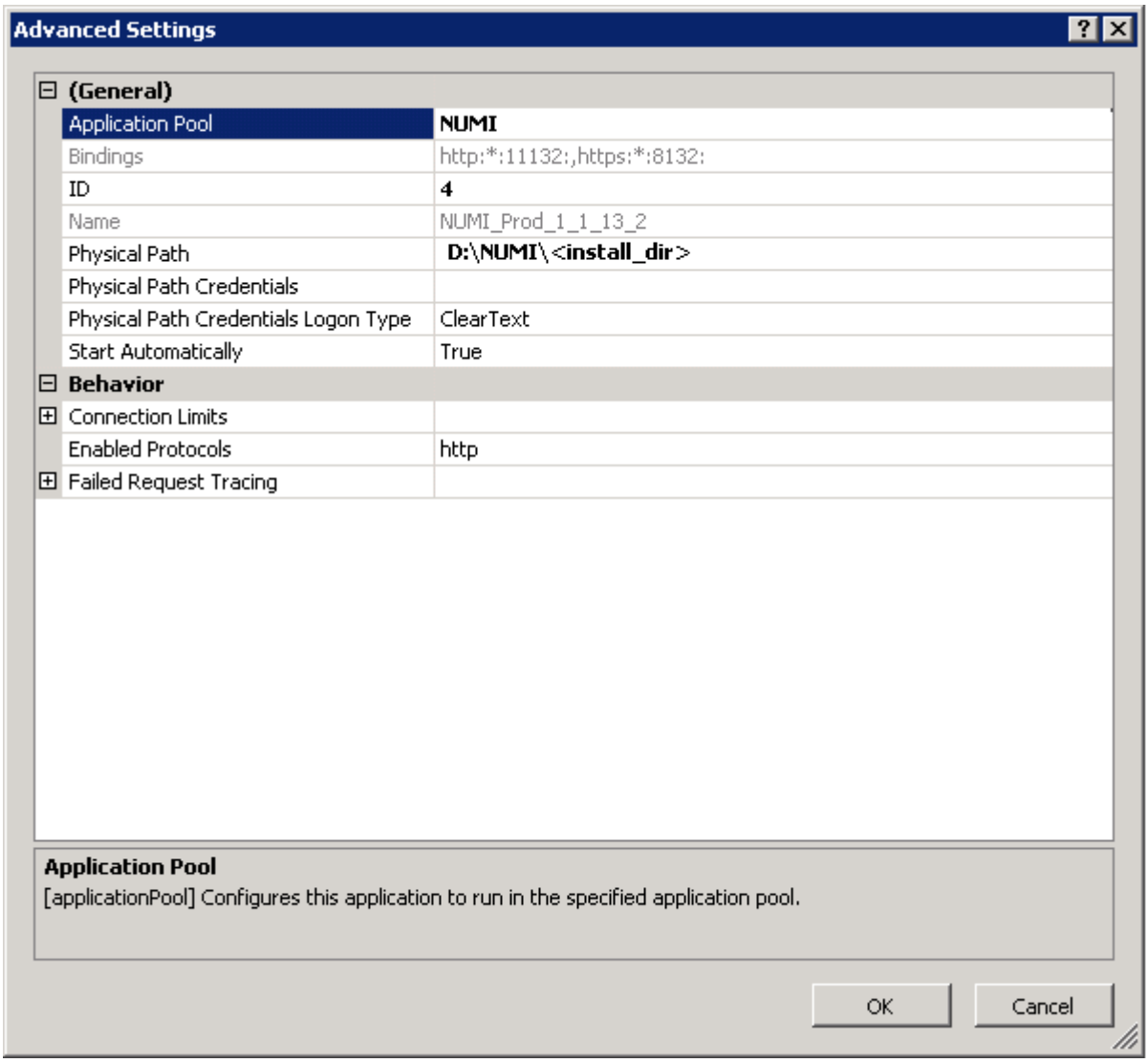

Figure 44: NUMI Advanced Settings

The NUMI web site bindings are shown in Figure 55: NUMI Bindings.

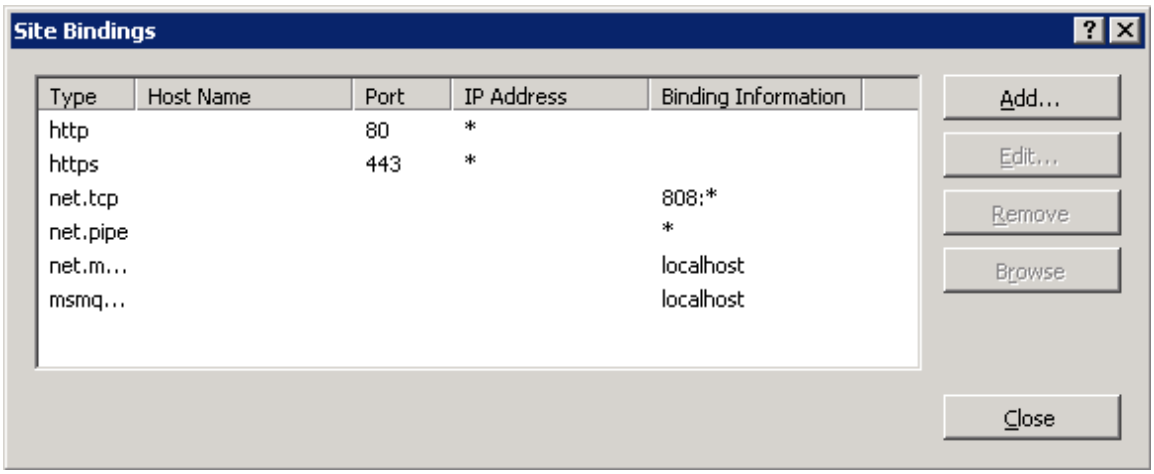

Figure 45: NUMI Bindings

The NUMI web site authentication settings are shown in Figure 56: NUMI Authentication Settings and Figure 57: NUMI Provider Settings. Make sure NTLM is before Negotiate in the Providers dialog.

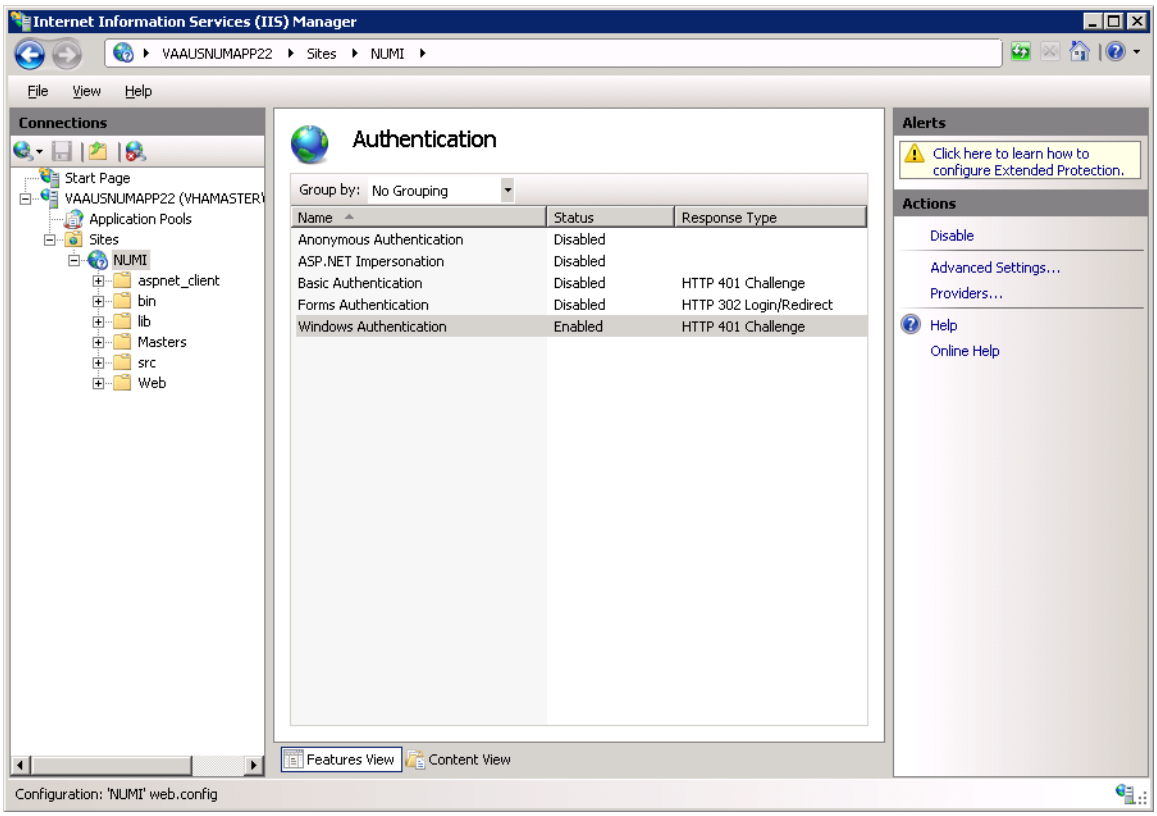

Figure 46: NUMI Authentication Settings

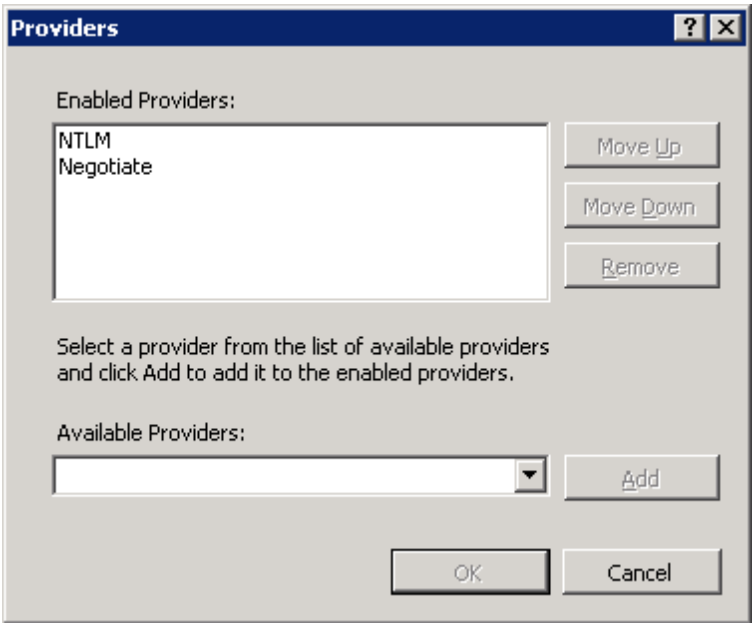

Figure 47: NUMI Provider Settings

The NUMI website SSL settings are shown in Figure 58: NUMI SSL Settings.

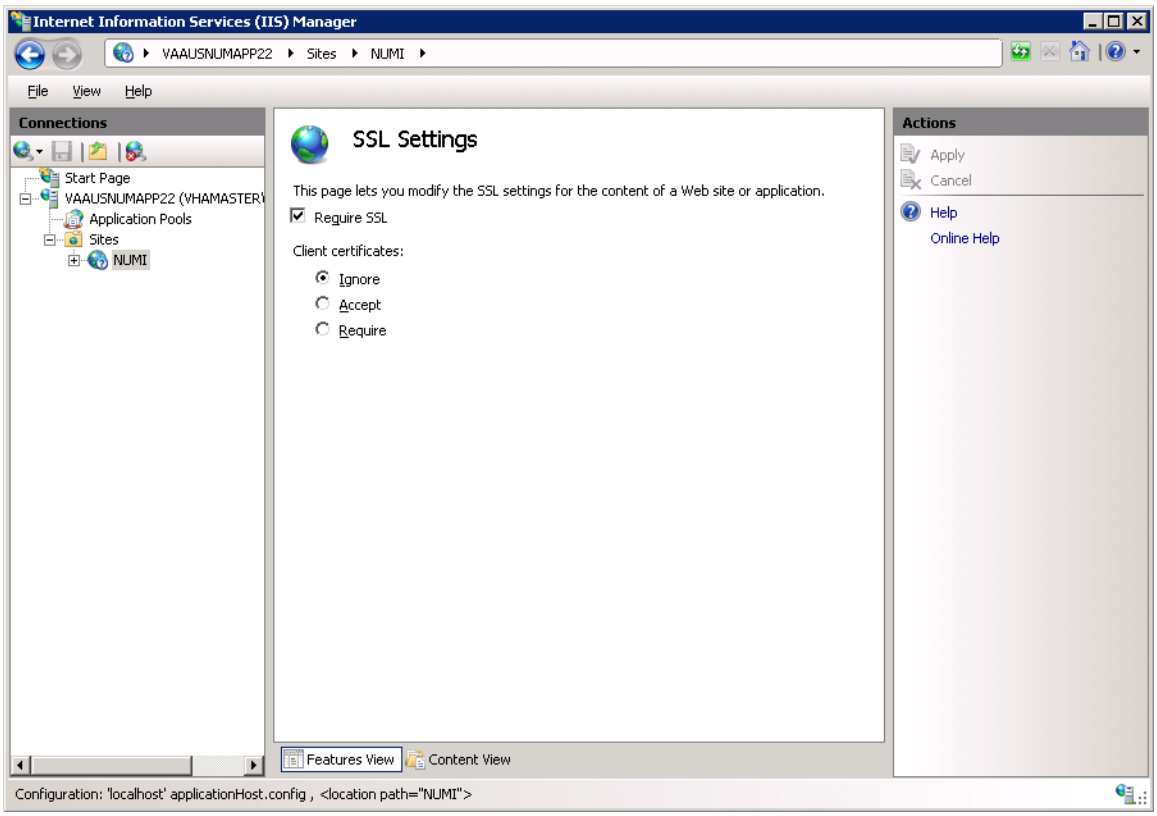

Figure 48: NUMI SSL Settings

The NUMI web site compression settings are shown in Figure 59: NUMI Compression Settings.

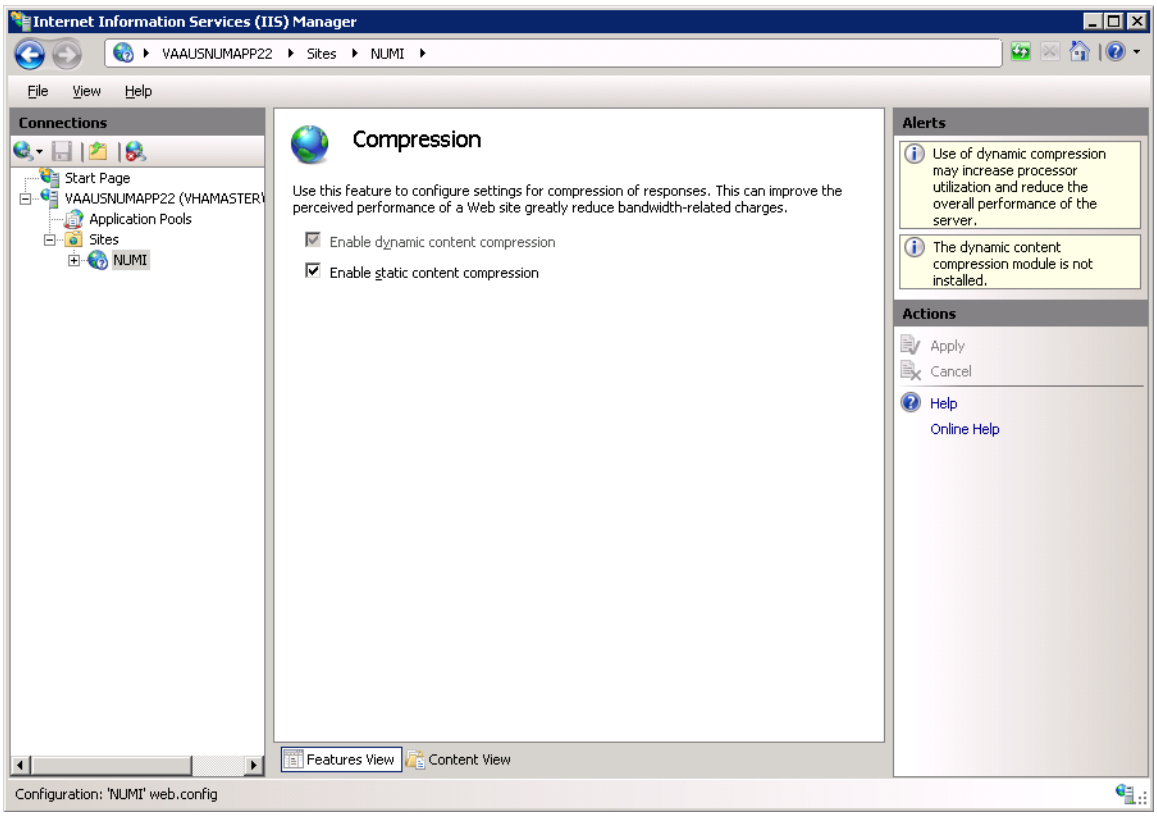

Figure 49: NUMI Compression Settings

6.12.3. Configuration File Setup

Verify the httpExectuion timeout field in the NUMI web.config file:

<httpRuntime executionTimeout=”300” />

6.12.4. Application Pool Configuration

The NUMI application pool setup is shown in Figure 60: Application Pool window.

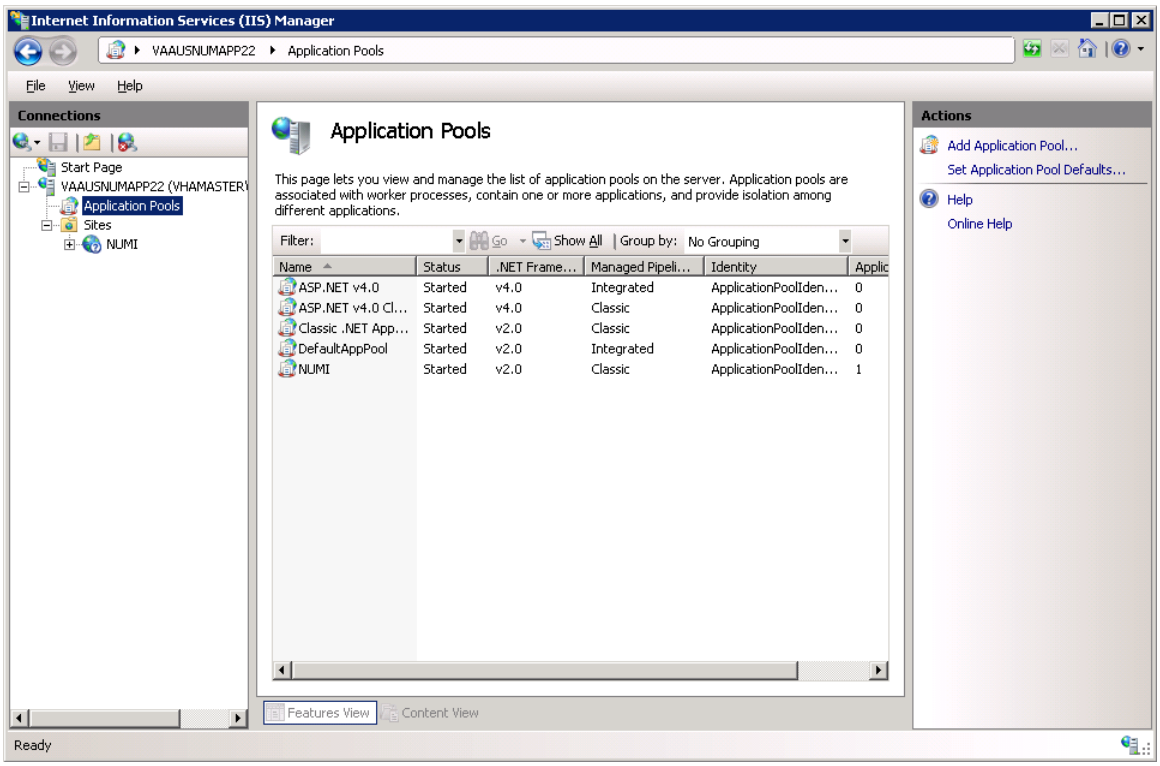

Figure 50: Application Pool Window

The NUMI application pool basic settings are shown in Figure 61: NUMI Application Pool Basic Settings.

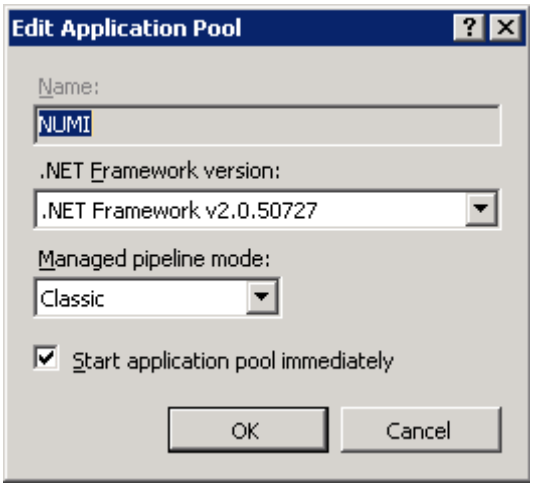

Figure 51: NUMI Application Pool Basic Settings

The NUMI application pool advanced settings are shown in Figure 62: NUMI Application Pool Advanced Settings.

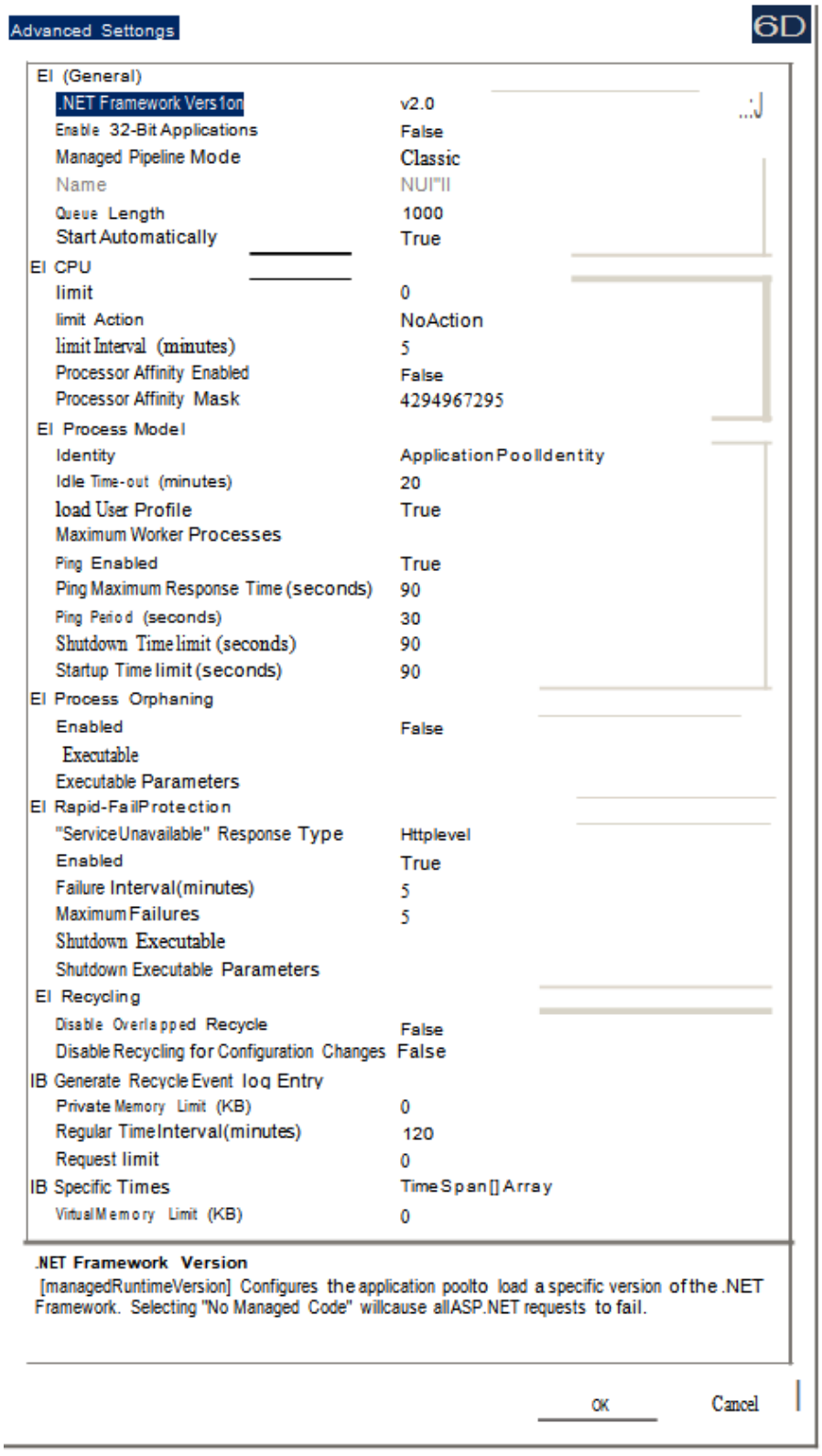

Figure 52: NUMI Application Pool Advanced Settings

6.13. Installing CERME (COTS Product) Software and Database from CERMe Install CD

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

6.13.1. Install CERME on the Application Server

CERMe install helpful hints: VERSION 12.0 (2013) CUSTOMER ID: **1102**

PRODUCT KEY: 755638-507216-296082-523246-21

ORGANIZATION: Department of Veterans Affairs

1. Verify that CERME database is already set up before proceeding with the software installation.

2. If the installation does not start automatically, double click the install.htm file (using Internet Explorer) in the root directory to open the setup welcome page.

3. On license information page, enter the CERME license information provided above and then click "Next".

4. Select Review Manager Enterprise and then click "Next". Select New Installation and then click "Next".

5. When the 'Choose Components" install window is reached select all of the checkboxes and then click "Next".

6. Choose a directory based on local policy (example D:\ Program Files), "Next".

7. On the database page, select "SQL Server" from the dropdown and then click "Next".

8. Enter the **CERME** database connection information, including the database server name, database name (**CERME**), port **1433**, instance (**leave blank**), and the database user credential (user ID **CERME**, DBA assistance required for the password).

9. Choose default settings on the rest of the steps.

10. Use a separate database to store report data and then click **No.**

11. On the "**Install Jetty**" window, select **Yes** to install Jetty.

Installation of the software should start after going through all the setup steps.

After the CERMe application version n.n.n.n and database is installed the following configuration needs to be done.

1. Add the below element in **ReviewManager.xml** file which is located <home directory> \ McKesson\CERME\Jetty\

e.g., D:\Program Files (x86)\McKesson\CERME\Jetty\ReviewManager_xml

Add this element in Config group bottom.

<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"/>

2. NOTE- If after successfully setting up the server, it is possible that NUMI will run, but not show any CERMe information. If the user right-clicks on the blank information and views source, they may see a warning about invalid log-in. This is usually because the Integrated Login information entered in the xml file did not get propagated to the CERMe service. Usually, restarting the CERMe service will fix the problem. Before performing a Service Restart, verify ReviewManager.xml contains the correct server name for the desired database access as configured below:

3. Open **jetty.xml** file from <home directory> \ McKesson\CERME\Jetty\etc folder.

<ConParams name="McKCERME" DBtype="MSS" DBCID=""
Driver="net.sourceforge.jtds.jdbc.Driver"
URL="jdbc:jtds:sqlserver://<database_server>:1433/cerme;sendStringParam etersAsUn

icode=false" ABAutoSumConnectionName="" ABIQCConnectionName="" RMDB="Y"

/>

<PoolParams dbname="McKCERME" Size="25" PoolMax="35" UseCount="200"

Timeout="600"

4. Change the default port to **"8357"** from "80".

e.g., <Set name="Port"><SystemProperty name="jetty.port" default="8357"/></Set>

6.13.2. 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 63: IIS Server Certificates.

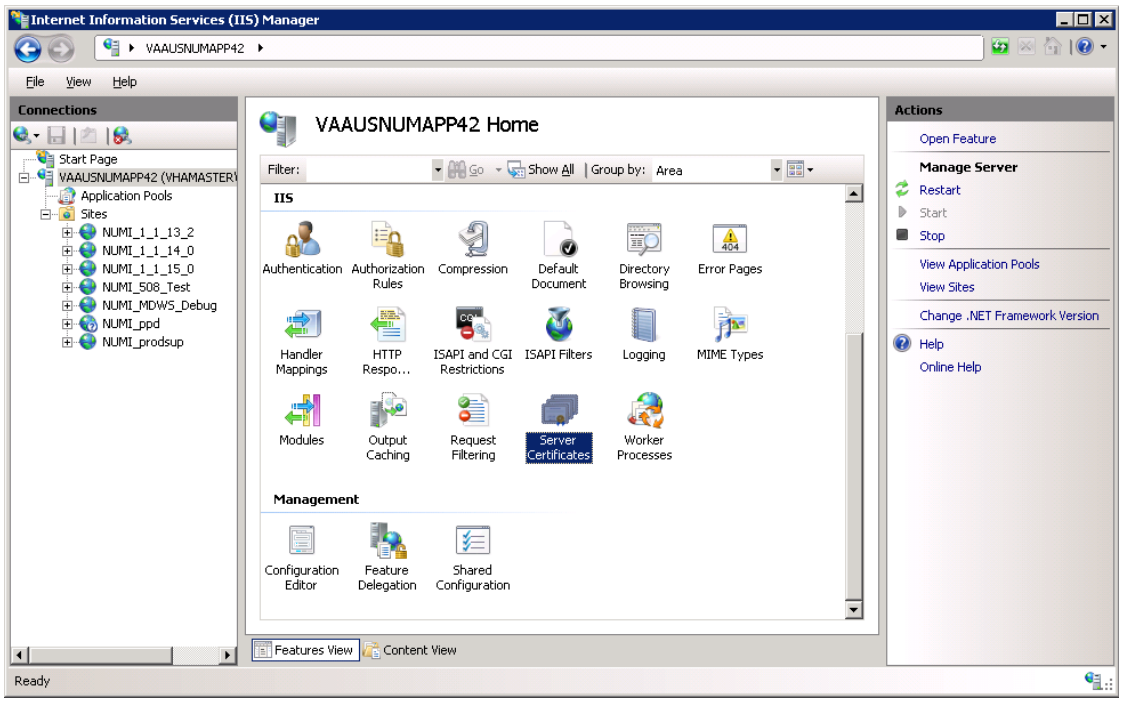

Figure 53: IIS Server Certificates

2. Select the certificate to export and click on the "Export…" link in the Actions pane, as shown in Figure 64: IIS Server Certificate Selection.

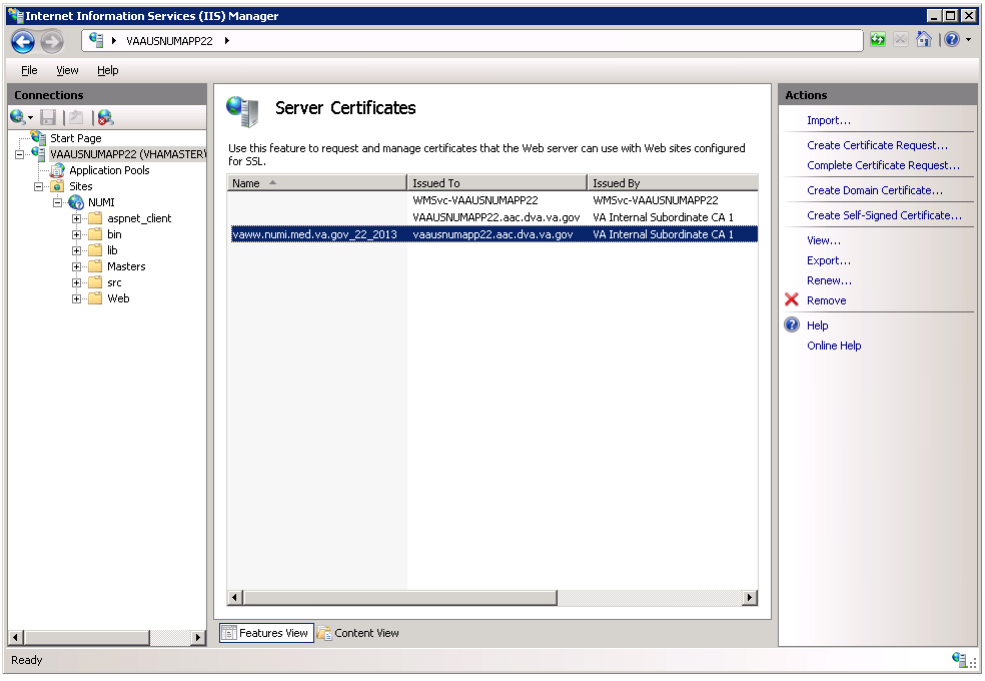

Figure 54: IIS Server Certificate Selection

3. Set the name of the .pfx file. Set the password, e.g., use numi (all lowercase) for the password, as shown in Figure 65: IIS Certificate Details. This password will be used in subsequent steps.

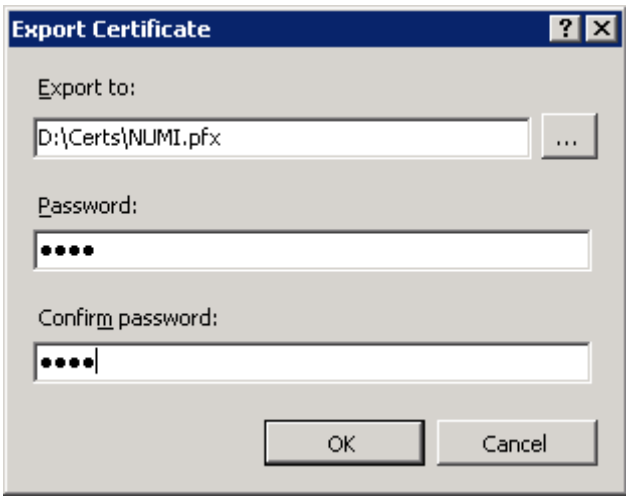

Figure 55: IIS Certificate Details

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)\McKesson\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 -keystore "D:\Certs\CERME.ks" –list

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

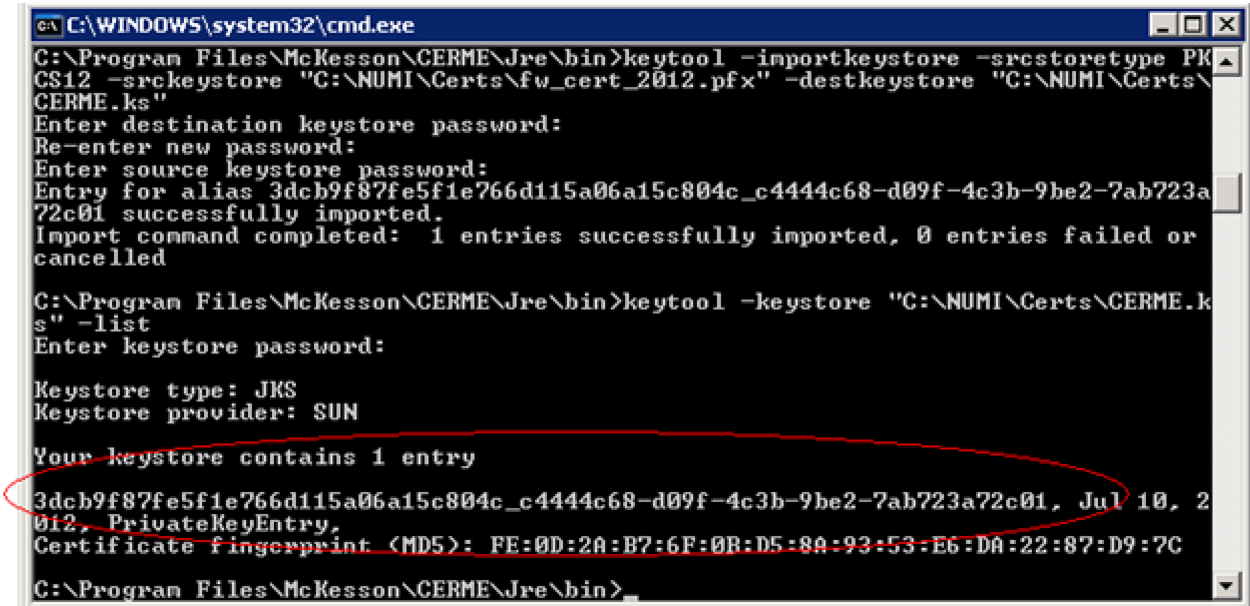

Figure 56: keytool -keystore "C:\Certs\CERME.ks" –list

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)\McKesson\CERME\Jetty\etc

Open the jetty.xml file in the same directory and scroll down to the “add a HTTPS SSL listener” section, (pictured below). If the items highlighted in red exist in your file, delete them. They are xml comments and will cause the section to be ignored. Items highlighted in yellow may need to be updated.

<!-- -->

<!-- To add a HTTPS SSL listener -->

<!-- -->

<!-- if NIO is not available, use org.eclipse.jetty.server.ssl.SslSocketConnector -->

<!--

```
<Call name="addConnector">
  <Arg>
    <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
          <Set name="Port">8443</Set>
          <Set name="maxIdleTime">30000</Set>
    <Set name="Acceptors">2</Set>
    <Set name="AcceptQueueSize">100</Set>
          <Set name="Keystore"><Property name="jetty.home" default="."
/>/etc/CERME.ks</Set>
          <Set name="Password">secret</Set>
          <Set name="KeyPassword">reallysecret</Set>
    <Set name="truststore"><Property name="jetty.home" default="."
/>/etc/CERME.ks</Set>
          <Set name="trustPassword">secret</Set>
    </New>
   </Arg>
  </Call>
-->
```

10. 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 completely restart, 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

11. 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.

6.14. 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\Microsoft.NET\Framework\v2.0.50727

2. Install Command - Type InstallUtil.exe /I < source folder full path >**\bin\NumiWebApp.dll** under Framework v2.0 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.

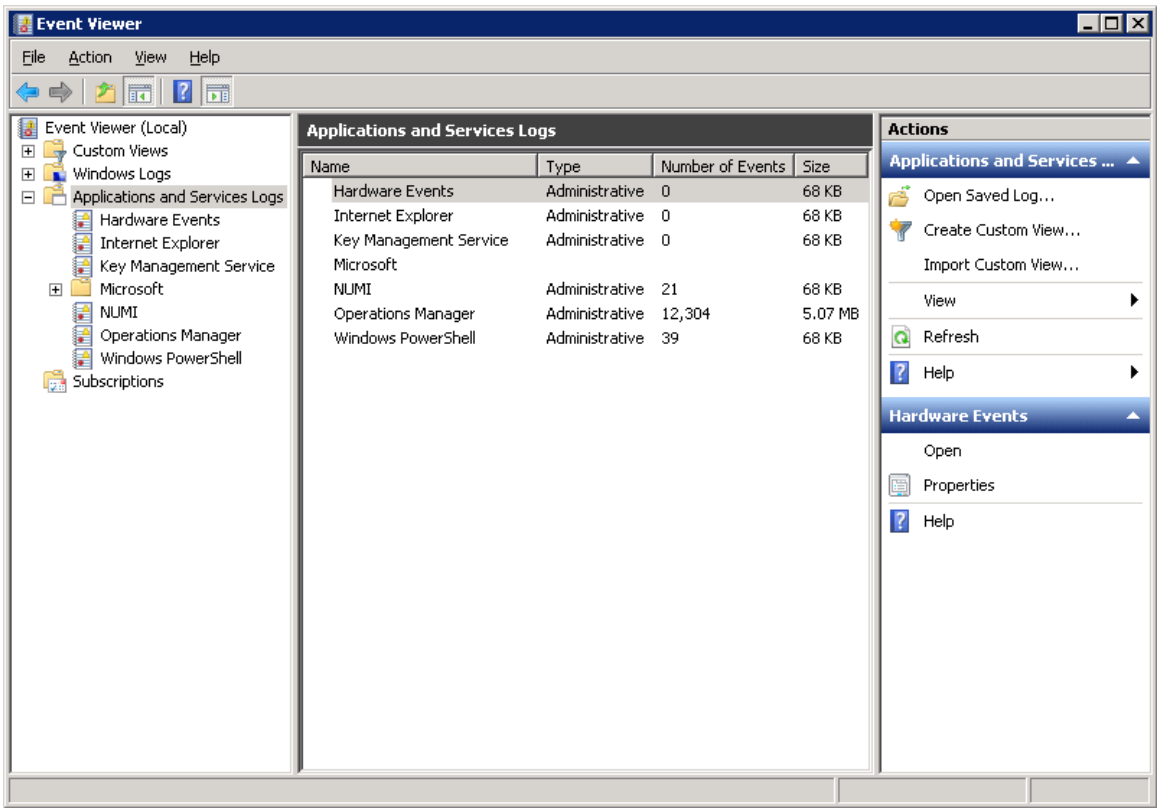

Figure 57: Creating a NUMI section in the Windows Event Log

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.

6.15. 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:

2. <!-- change this setting to point to the appropriate config file for the deployment. -->

<appSettings configSource="src\\main\\resources\\xml\\deployment\\numiwebapp.config"/>

<connectionStrings/>

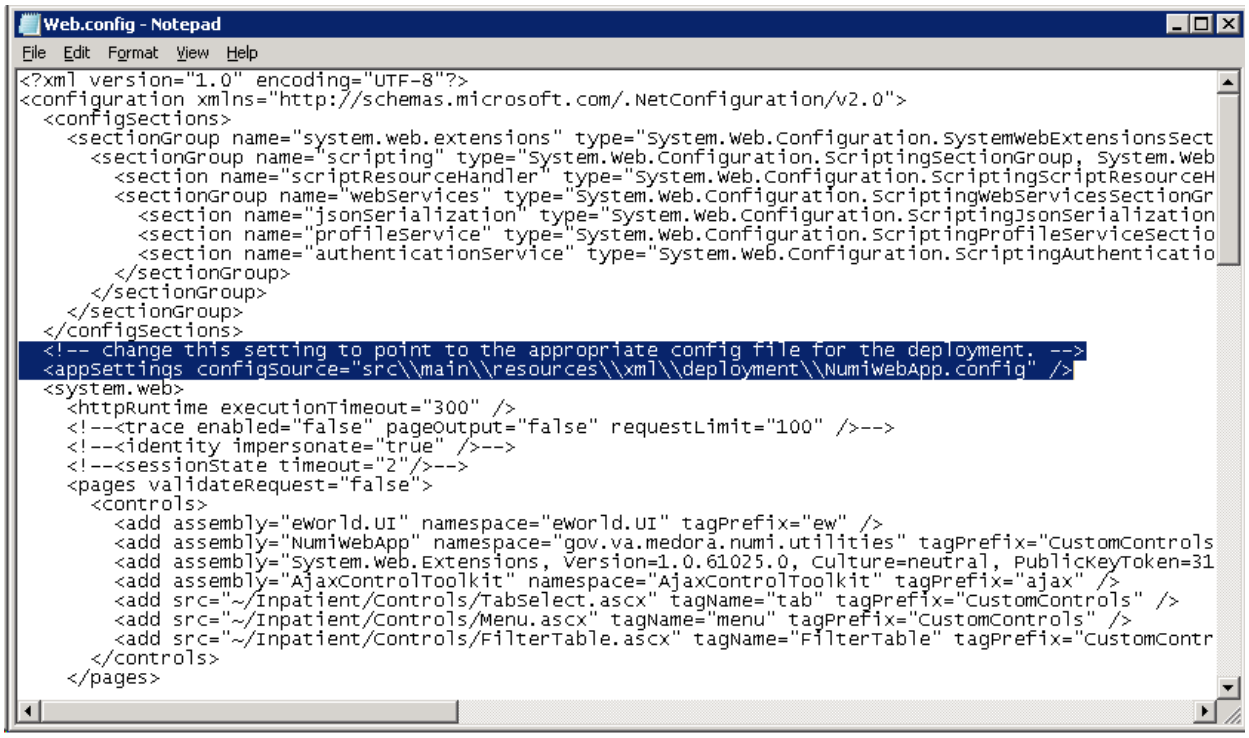

Figure 58: Updating Settings in NUMI XML Configuration File

3. Edit the application settings in the **config** file indicated in the previous entry. Make sure to enter the MDWS server 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:

<add key="serviceUrl" value="http://<enter_mdws_server>/NumiService.asmx" />

<add key="numiDbConnectionString" value="Data Source=<enter_database_server>;Database=NUMI;User ID=numi_user;Password=xxxxxxxx;Trusted_Connection=False" />

<add key="reportDbConnectionString" value="Data Source=<enter_database_server>;Database=NUMI;User ID=numi_user;Password=xxxxxxxx;Trusted_Connection=False" />

6.16. 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>.

6.16.1. Test NUMI Web Site Functionality

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

6.17. Installing NUMI Synchronizer on the DB Server

6.17.1. Software Copy Instructions

1. Right click on the zip file, select "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.

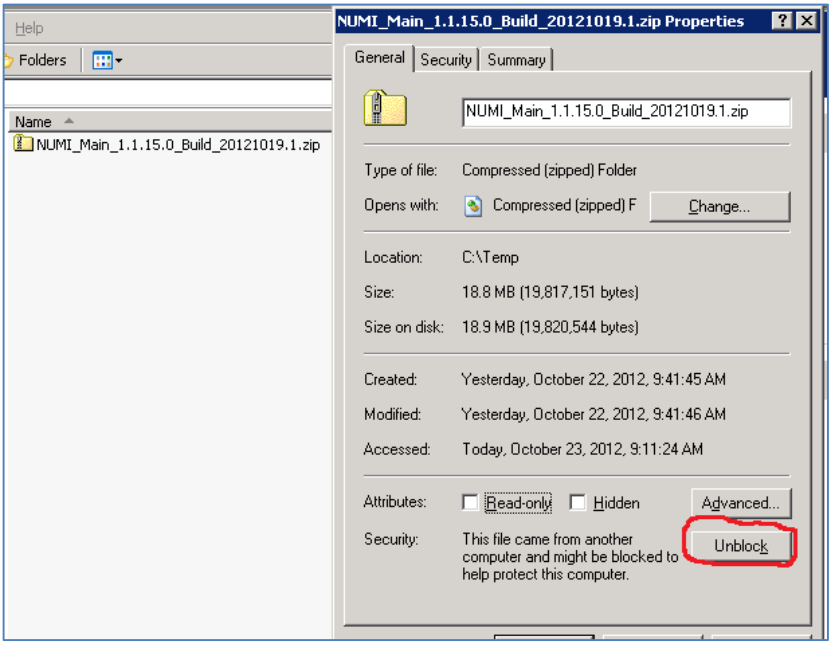

Figure 59: Unblocking Restricted Files in Installation ZIP file

It is recommended that Synchronizer 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

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

3. Open Config File - Open **synchronizer.exe.config** file in notepad under D:\NUMI\ <install_dir> folder.

4. Make sure the configSource points to the Synchronizer.config file path location, e.g., <appSettings configSource="src\\main\\resources\\xml\\deployment\\Synchronizer.config" />

Verify the httpExecution timeout field:

<httpRuntime executionTimeout="900" />

Note: All server configuration targeted files are located at

<destination>:\synchronizer\src\main\resources\xml\deployment

5. Edit the Synchronizer.config file to point to the MDWS server that the synchronizer will be using, e.g.,

<app key=”serviceUrl” value=”http://vaausnumweb42:8081/NumiService.asmx” />

6. Edit the Synchronizer.config file to point to the Database server that the synchronizer will be using, e.g.,

<app key=”numiDbConnectionString” value=”Data Source=vaausnumsql83;Database=NUMI;User ID=numi_user;Password=xxx;Trusted_Connection=False” />

7. NOTE: If you are going to specify a different visitor account than the standard DOD visitor, then enter the appropriate visitor information in the Sunchronizer.config file. If you do create a new visitor for your environment, you will need to add the new visitor record to the NumiUser table in the NUMI database, similar to the standard DOD visitor that is already in the table.

8. Change Directory - Go to command prompt (run as Administrator) and change current directory to Framework v2.0 bit folder e.g.,

C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727

9. Install Command - Type installutil.exe –I < source folder full path > **\synchronizer.exe** (Figure 70: Synchronizer.exe window) under Framework v2.0 folder and press enter. E.g., installutil.exe -I D:\NUMI\<install_dir>\synchronizer.exe

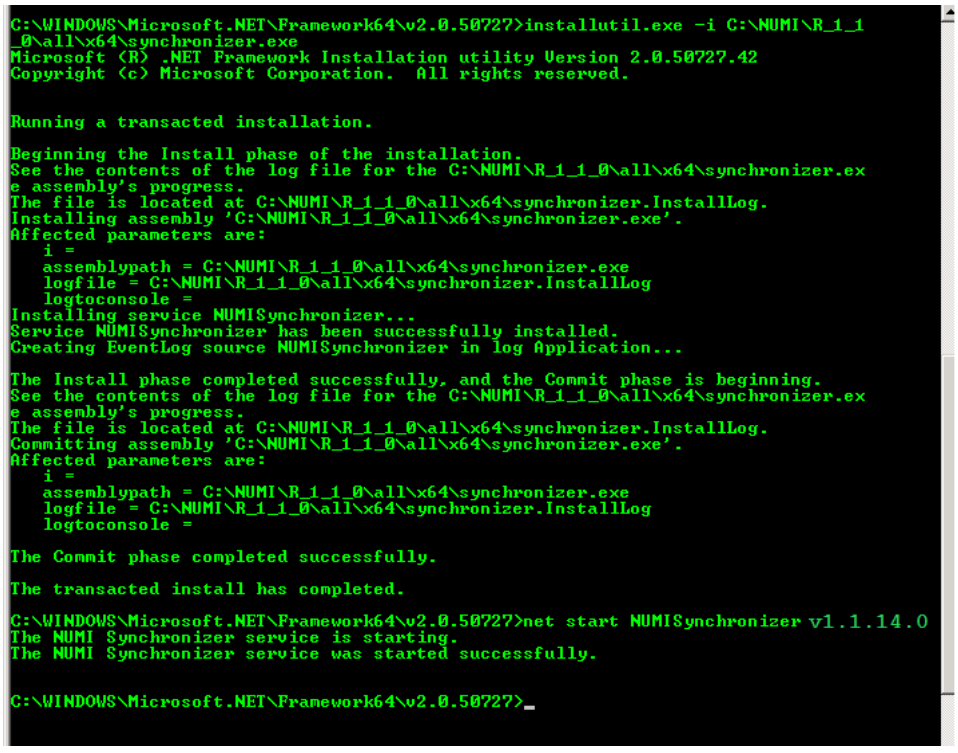

Figure 60: Synchronizer.exe Window

Start Synchronizer –

Note: The Synchronizer name is hard coded. The synchronizer name can be found during synchronizer setup (See Figure 70: Synchronizer.exe window). The status lines

“Installing Service: xxx” and “Service xxx has been successfully installed” show the synchronizer name.

10. Go to “Services” via “Administration Tools”, right click on the service, and select Start (See Figure 71: Starting the Service). Alternately, you could enter “services.msc” in the run box to bring up the Services Explorer window. Verify

‘Started’ is displayed in the Status column in the row for the Synchronizer Service.

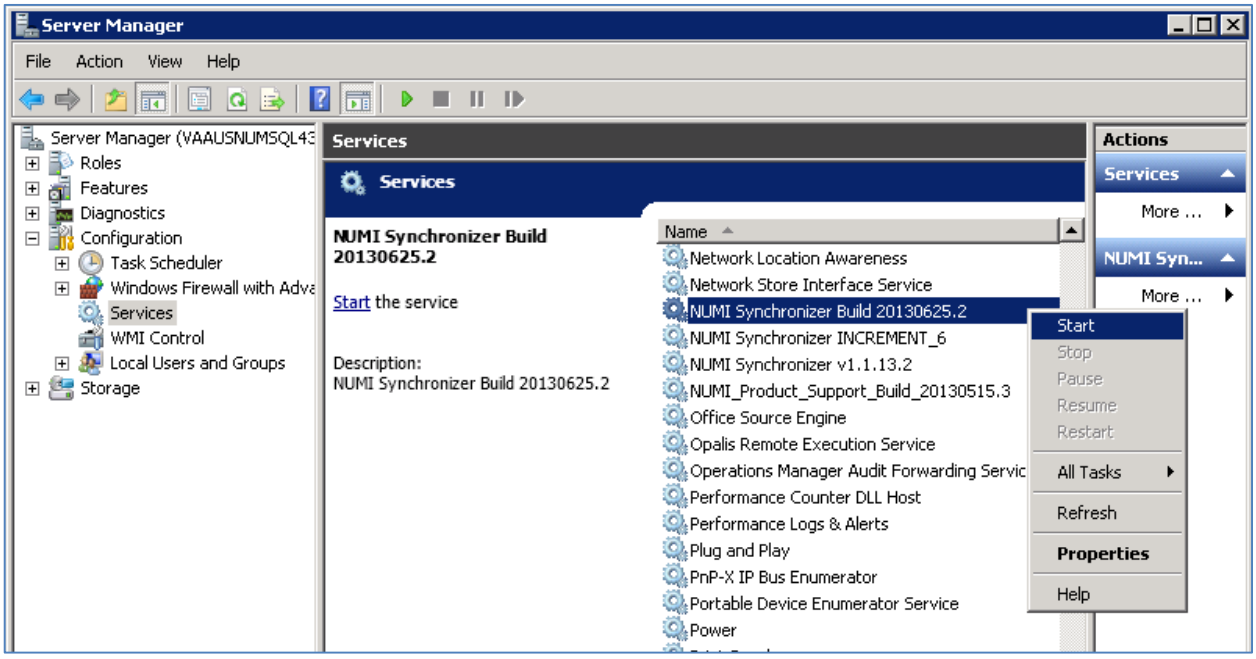

Figure 61: Starting the Service

Uninstall:

If you need to uninstall the NUMI Synchronizer services use: installutil.exe -u

C:\NUMI\ synchronizer\synchronizer.exe

Please see the event logs if you have any issues.

Validate Installation:

To confirm the synchronizer installation

Open Microsoft 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.

6.18. Add Jobs to the SQL Server

There are three jobs that must be added to the SQL Server, specifically,

NUMI_PhysicianAdvisorPatientReview_AutoExpire LogSynchDB_ValidateSynchronizer 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 checks that stays have been imported within the last 3 hours and reports the problem to a pre-defined e-mail distribution list, as decided by the needs of the particular 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.

7. Post-Installation Considerations

If this is applicable to NUMI, this information will be provided by the appropriate project teams.

Acronyms and Descriptions

Acronym	Description
CERMe	CareEnhance Review Management Enterprise
CPU	Central Processing Unit
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
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
UM	Utilization Management
URL	Uniform Resource Locator