National Utilization Management Integration (NUMI) Server Setup Guide

Release 1.1.15.16



Department of Veterans Affairs

January 2025

Revision History

Date	Description	Author
1/23/2025	Updated release version number to 15.16	Redacted
7/16/2024	Updated NUMI to use VDIF instead of VIA, 16.0 Release	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
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
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	Redacted

Date	Description	Author
	6.11, renamed MDWS 2.x to MDWS 2.7.3.2 in section 6.12, renamed section 6.12 to 6.11	
8/2/2013	Removed references to CERMe 2012. Changed hard coded build name directory references to <install_dir>.</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, Installation During Off Peak Hours. Also reordered installation steps SQL and CERMe (now section 6.1 and 6.14) and added CERMe SSL	Redacted
03/25/2013	Modified section 6.15 for NUMI event folder, modified	Redacted

Date	Description	Author
	section 6.19	
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. Intro	oduction	9
1.1.	Purpose	9
1.2.	Scope	9
1.3.	Target Audience	9
2. Dep	loyment Overview	9
2.1.	National Deployment Request	9
2.2.	Installing NUMI on the Servers	9
3. Pre-	Installation Instructions and Preparation1	1
3.1.	Installation Process Requirements 1	1
3.2.	Install Software in Test Environments 1	2
3.3.	Generate Pre-Installation Reports1	2
3.4.	Coordinate Installation with Other Teams 1	2
3.5.	Install Sequence Information for Multiple Patches1	2
3.6.	Logoff During Installation 1	2
3.7.	Average Amount of Time Required to Complete the Installation 1	3
4. Data	abase Information 1	4
4.1.	Instructions for Installing Database Components1	4
5. Inst	allation Procedure for Server 2019 1	5
5.1.	Patch the Operating System 1	5
6. SQL	Server Setup (Windows Server 2019) 1	5
6.1.	Role Setup 1	5
7. Web	b Server Setup (Windows Server 2019) 1	6
7.1.	Role Setup 1	6
7.2.	ASP.NET 2.0 AJAX Extensions 1.0 Setup 1	9
7.3.	MS Web Services Enhancements (WSE) 3.0 Setup 1	9
8. App	lication Server Setup (Windows Server 2019)1	9
8.1.	Role Setup 1	9
8.2.	Feature Delegation 2	21

8.3	8.	Install MS ASP.Net 2.0 AJAX Extensions 1.0	22
8.4	I.	Install MS Web Services Enhancements 3.0	26
9.	Insta	all SQL Server	30
9.1		Download all SQL Server Patches	30
9.2	2.	Restore the Appropriate Databases for the NUMI Application	30
10.	Insta	alling NUMI Exchange on Server 2019	31
10.	.1.	Unzip/Install NUMI Exchange Distribution	31
10.	.2.	NUMI Exchange Website Configuration	31
11.	Insta	alling NUMI on Server 2019	38
11.	.1.	Software Copy Instructions	38
11.	.2.	NUMI Web Site Configuration	39
11.	.3.	Application Pool Configuration	44
12.	Insta	all CA SiteMinder Web Agent for Single Sign On (SSO) on the Web server.	48
12.	.1.	Agent location	48
12.	.2.	Agent installation	48
12.	.3.	Agent configuration	52
13.	Secu	re Token Service Integration for SSOi	66
13.	.1.	Download Certificate Chain from appropriate endpoint	66
13.	.2.	Export server cert to .pfx	71
13.	.3.	NumiWebApp.config keys	73
14.	Insta	alling CERMe Software and Database from CERMe Installation CD	73
14.	.1.	Install CERMe on the Application Server	73
14.	.2.	Install CERMe SSL Certificate	76
15.	Sett	ing up NUMI Section in the Windows Event Log	81
15.	.1.	Validate XML Configuration File Settings	82
16.	Perf	orm Restart	84
17.	Test	NUMI Web Site Functionality	85
18.	Insta	alling NUMI Synchronizer on the Web Server	85
18.	.1.	Installation Instructions	85

18.2.	Uninstall:	86
18.3.	Validate Installation:	87
18.4.	Add Jobs to the SQL Server	87
19. Pos	t-Installation Considerations	87
20. Acr	onyms and Descriptions	88
21. NUI	VI Comparison Table	88

List of Tables

12
12
55
56
84
1 1 5 8

List of Figures

Figure 1: SQL Server Role Services	16
Figure 2: NUMI Exchange Role Services	17
Figure 3: NUMI Exchange (IIS)	18
Figure 4: NUMI Role Services	19
Figure 5: NUMI Web Services IIS	20
Figure 6: IIS Feature Delegation	21
Figure 7: Feature Delegation Selection	22
Figure 8: MS ASP.Net 2.0 File Download-Security Warning Window	23
Figure 9: MS ASP.Net 2.0 Internet Explorer-Security Warning Window	23
Figure 10: MS ASP.NET 2.0 AJAX Extensions 1.0 Setup Wizard Window	24
Figure 11: MS ASP.NET 2.0 AJAX License Agreement Window	24
Figure 12: MS ASP.NET 2.0 AJAX Installation Window	25
Figure 13: MS ASP.NET 2.0 AJAX Completion window	26
Figure 14: MS WSE 3.0 File Download-Security Warning Window	26
Figure 15: MS WSE 3.0 Internet Explorer-Security Warning Window	27
Figure 16: MS WSE 3.0 InstallShield Wizard Welcome Window	27
Figure 17: MS WSE 3.0 License Agreement Window	28
Figure 18: MS WSE 3.0 InstallShield Wizard Window	28
Figure 19: MS WSE 3.0 Installation Window	29
Figure 20: MS WSE 3.0 Completion Window	30
Figure 21: Add NUMI Exchange Website	31
Figure 22: NUMI Exchange Website	32
Figure 23: NUMI Exchange Basic Settings	33
Figure 24: NUMI Advanced Settings	33
Figure 25: NUMI Exchange Bindings	34
Figure 26: NUMI Exchange Authentication Settings	34
Figure 27: NUMI Exchange SSL Settings	35
Figure 28: Application Pool Window	36
Figure 29: NUMI Exchange Application Pool Basic Settings	36
Figure 30: NUMI Exchange Pool Advanced Settings	37
Figure 31: Unblocking Restricted Files in Installation ZIP File	38
Figure 32: Add NUMI Website	39
Figure 33: NUMI Basic Settings	40
Figure 34: NUMI Advanced Settings	41
Figure 35: NUMI Bindings	42

Figure 36: NUMI Authentication Settings	42
Figure 37: NUMI SSL Settings	43
Figure 38: NUMI Compression Settings	44
Figure 39: Applicatiaon Pool Window	45
Figure 40: NUMI Application Pool Basic Settings	46
Figure 41: NUMI Application Pool Advanced Settings	47
Figure 42: Security Warning	48
Figure 43: Preparing to install dialog	49
Figure 44: Web agent install wizard - Welcome screen	49
Figure 45: Web agent install wizard - License agreement screen	50
Figure 46: Web agent install wizard - Install location screen	50
Figure 47: Web agent install wizard - Review screen	51
Figure 48: Web agent install wizard - Agent configuration screen	51
Figure 49: Web agent install wizard - Install complete screen	52
Figure 50: Launch Web Agent Configuration Wizard	53
Figure 51: Web agent configuration wizard - Host registration	54
Figure 52: Web agent configuration wizard - Admin credentials	55
Figure 53: Web agent configuration wizard - Host name and configuration object	56
Figure 54: Web agent configuration wizard - Policy server IP Address	57
Figure 55: Web agent configuration wizard - FIPS mode setting	57
Figure 56: Web agent configuration wizard - Configuration file location	58
Figure 57: Web agent configuration wizard - Web server	58
Figure 58: Web agent configuration wizard - Agent configuration	59
Figure 59: Web agent configuration wizard - Sites selection	59
Figure 60: Web agent configuration wizard - Summary screen	60
Figure 61: Web agent configuration wizard - Completion screen	60
Figure 62: Web agent configuration wizard - Host registration	61
Figure 63: Web agent configuration wizard - Web server	62
Figure 64: Web agent configuration wizard - Agent configuration	62
Figure 65: Web agent configuration wizard - Sites selection	63
Figure 66: Web agent configuration wizard - Summary screen	64
Figure 67: Web agent configuration wizard - Previously configured sites	65
Figure 68: Web agent configuration wizard - Summary screen	65
Figure 69: Web agent configuration wizard - Completion screen	66
Figure 70: IIS Server Certificates	77
Figure 71: IIS Server Certificate Selection	78
Figure 72: IIS Certificate Details	79
Figure 73: keytool -keystore "C:\Certs\CERME.ks" –list	80
Figure 74: Creating a NUMI section in the Windows Event Log	82
Figure 75: Updating Settings in NUMI XML Configuration File	83

1. Introduction

This Server Setup Guide explains how to install National Utilization Management Integration (NUMI), Release 1.1.15.16.

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 Data Integration and Federation (VDIF), 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.

2.1.1 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.

2.2.1 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

2.3.1 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 2024 application
- 4. Install the NUMI application
- 5. Change the web.config file settings as needed
- 6. Install the SiteMinder Web Agent and configure it for the NUMI application Web site

3. Pre-Installation Instructions and Preparation

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

3.1. Installation Process Requirements

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

1.4.1 Minimum Software Version

Operating System: Windows Server 2019 Database: SQL Server 2019

1.5.1 Resources Required

Sys Admin, DBA

1.6.1 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

1.7.1 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.)

1.8.1 Devices (Servers, etc.)

- 1 Database Server
- 2 Application Servers
- 2 Web Servers
- 1 Data Warehouse Server 1 SQL Reporting Server

1.9.1 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.

5
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 1: CPRS Rights

Table 2: CPRS Access Tabs

	TUDIC E.		
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.

1.10.1 Database Installation / Restoration Procedures

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

5. Installation Procedure for Server 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.



Installation Type	Roles	
Server Selection		~
Server Roles	File and Storage Services (1 of 12 installed)	
Features	⊿ ☐ File and iSCSI Services	
Confirmation	File Server	
e a	BranchCache for Network Files	
Results	Data Deduplication	
	DFS Namespaces	
	DFS Replication	
	File Server Resource Manager	
	File Server VSS Agent Service	
	iSCSI Target Server	-
	iSCSI Target Storage Provider (VDS and VSS hardw	
	Server for NFS	
	Work Folders	
	Storage Services (Installed)	
	Hyper-V	
	Network Policy and Access Services	
	Print and Document Services	
	Remote Access	~
		1

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).



Installation Type	Roles
Server Selection	UND Server
Server Roles	Fax Server
Features	▲ ■ File and Storage Services (2 of 12 installed)
Confirmation	⊿ ■ File and iSCSI Services (1 of 11 installed)
Posults	✓ File Server (Installed)
Nesults	BranchCache for Network Files
	Data Deduplication
	DFS Namespaces
	DFS Replication
	File Server Resource Manager
	□ File Server VSS Agent Service ■
	iSCSI Target Server
	iSCSI Target Storage Provider (VDS and VSS hardwa
	Server for NFS
	Work Folders
	✓ Storage Services (Installed)
	Hyper-V
	Network Policy and Access Services
	Distand Desument 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.

Installation Type	Roles	
Server Selection	UNS Server	^
Server Roles	Fax Server	
Features	∡ ■ File and Storage Services (2 of 12 installed)	
Confirmation	File and iSCSI Services (1 of 11 installed)	
Reculte	✓ File Server (Installed)	
(Counto	BranchCache for Network Files	
	Data Deduplication	
	DFS Namespaces	
	DFS Replication	
	File Server Resource Manager	
	File Server VSS Agent Service	Ξ
	iSCSI Target Server	
	iSCSI Target Storage Provider (VDS and VSS hardwa	
	Server for NFS	
	Work Folders	
	Storage Services (Installed)	-
	Hyper-V	
	Network Policy and Access Services	
	Drint and Decument Conjugat	_

Figure 4: NUMI Role Services

Figure 5: NUMI Web Services IIS

Before You Begin	Select one or more roles to install on the selected server.
Installation Type	Roles
Server Selection	
Server Delec	■ Web Server (IIS) (20 of 43 installed)
Server Roles	■ Web Server (19 of 34 installed)
Features	∠ Common HTTP Features (4 of 6 installed)
Confirmation	Default Document (Installed)
Results	Urrectory Browsing (Installed)
	HIP Errors (Installed)
	Static Content (Installed)
	HITP Redirection
	WebDAV Publishing
	▲ Health and Diagnostics (1 of 6 installed)
	HTTP Logging (Installed)
	Custom Logging
	Logging Tools
	ODBC Logging
	Request Monitor
	Tracing
	⊿ Performance (1 of 2 installed)
	Static Content Compression (Installed)
	Dynamic Content Compression
	▲ ✓ Security (Installed)
	Request Filtering (Installed)
	Basic Authentication (Installed)
	Centralized SSL Certificate Support (Installed
	Client Certificate Mapping Authentication (In
	✓ Digest Authentication (Installed)
	IIS Client Certificate Mapping Authentication
	✓ IP and Domain Restrictions (Installed)
	✓ URL Authorization (Installed)
	✓ Windows Authentication (Installed)
	 Application Development (4 of 11 installed)
	.NET Extensibility 3.5
	✓ .NET Extensibility 4.5 (Installed)
	Application Initialization
	ASP ASP
	ASP.NET 3.5
	ASP.NET 4.5 (Installed)
	CGI
	✓ ISAPI Extensions (Installed)
	ISAPI Filters (Installed)
	Server Side Includes
	WebSocket Protocol
	FTP Server
	▲ Management Tools (1 of 7 installed)
	< III >

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

Group by: No Grouping -	
Name	Delegation
NFT Authorization Rules	Read/Write
NET Compilation	Read/Write
NET Error Pages	Read/Write
NET Globalization	Read/Write
NET Profile	Read/Write
NET Roles	Configuration Read/Write
NET Truct Levels	Read (Mrite
NET licer	Configuration Read/Write
Application Settings	Read Ovrite
ASD NET Improvemention	Read/Write
Astheretiseties Assessments	Read/write
Authentication - Anonymous	Read/write
Authentication - Basic	Read/ Write
Authentication - Digest	Read/write
Authentication - Forms	Read/Write
Authentication - Windows	Read/Write
Authorization Rules	Read/ Write
Compression	Read/Write
Connection Strings	Read/Write
Default Document	Read/Write
Directory Browsing	Read/Write
Error Pages	Read/Write
Feature Delegation	Read/Write
Handler Mappings	Read/Write
HTTP Response Headers	Read/Write
IP Address and Domain Restrictions	Read Only
ISAPI Filters	Read Only
Logging	Not Delegated
Machine Key	Read/Write
MIME Types	Read/Write

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).

Do you y	want to run or save this file?
1	Name: ASPAJAXExtSetup.msi Type: Windows Installer Package, 1.36 MB From: vhaannweb2.v11.med.va.gov <u>R</u> un <u>S</u> ave <u>Cancel</u>
U F	While files from the Internet can be useful, this file type can botentially harm your computer. If you do not trust the source, do no un or save this software. <u>What's the risk?</u>

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



 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

Microsoft ASP.NET 2.	AJAX Extensions 1.0 Setup	_ 🗆 🗙
End-User License A	greement	
Please read the follow	ing license agreement carefully	
MICROSOF	T SOFTWARE SUPPLE RMS	MENT
MICROSOF	T ASP.NET 2.0 AJAX IS	
Microsoft Corporat licenses this supple Windows operating	on (or based on where you live, on ment to you. If you are licensed to system software (the "software"),	e of its affiliates) use Microsoft you may use this 💌
☑ I accept the terms	n the License Agreement	
	Print Back	Next Cancel

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

File Down	load - Security Warning	×
Do you	want to run or save this file?	
18	Name: Microsoft WSE 3.0.msi Type: Windows Installer Package, 11.4 MB From: vhaannweb2.v11.med.va.gov	
	<u>R</u> un <u>S</u> ave Cancel	
1	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. <u>What's the risk?</u>	

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

Internet	Explorer - Security Warning 🛛 🛛 🔀
Do you	want to run this software?
	Name: <u>Web Services Enhancements 3.0 SDK Installation Pac</u> Publisher: <u>Microsoft Corporation</u>
× Mo	re options
٩	While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. <u>What's the risk?</u>

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: N	MS WSE 3.0	InstallShield	Wizard	Window
--------------	-------------------	---------------	--------	--------



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

🖓 Microsoft W5E 3.0 - InstallShield Wizard 🛛 🗙
Ready to Install the Program The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstaliShield
< <u>B</u> ack <u>Instal</u> Cancel

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.

ld Web Site				?
<u>S</u> ite name:		Application po	ol:	
NumiExchange		NumiExchange	•	S <u>e</u> lect
-Content Directo	ory			
D:\NumiExchai	nge\NUMI_In(rement6_Sprint2_I	Build_2	
Pass-through	authentication	1		
Connect as	. Test Set	tings		
Binding				
Type:	IP add	tress:	Port	
https	✓ All Un	assigned	▼ 443	
Host name:				
<u>S</u> SL certificate	¢.			
VAAUSNUMW	EB81.aac.dva	.va.gov	▼ <u>V</u> iew	
🗌 Start Web sit	e i <u>m</u> mediately			
			1	1
			OK	Cancel

Figure 21: Add NUMI Exchange Website



Figure 22: NUMI Exchange Website

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

Figure 23: NUMI Exchange Basic Settings

5ite name:	Application pool:	
JumiExchange	NumiExchange	Select
hysical path: :\NumiExchange\NUMI	Tocrement6 Sprint2 Build 2	
A fradmicken drige fradmic		
ass-through authentica		
Pass-through authentica	Settings	



Applio Bindin	ation Pool	NumiExchange		
Bindin				
	iys	https:*:443:		
ID		2		
Name		NumiExchange D:\NumiExchange\NUMI_Increment6_Sprint2_Build_2013042		
Physic	cal Path			
Physic	cal Path Credentials			
Physic	cal Path Credentials Logon Type	ClearText		
Start	Automatically	True		
3 Beha	vior			
E Conne	ection Limits			
Enabl	ed Protocols	http		
Name	Δ unique name for the site			

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

Site Bindings ? X Type Host Name Port IP Address Binding Information Add... https 443 * Edit... Edit... Remove Browse Browse Edit...

Figure 25: NUMI Exchange Bindings

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

🕒 🕑 🛛 🌒 🕨 VAAUSNUMWEB	🔄 🗠 🖄 I 🖉				
<u>F</u> ile ⊻iew <u>H</u> elp					
Connections	Actions				
۶- 🗟 🖄 😣					
Start Page	Group by: No Grouping			Online Help	
Application Pools	Name 🔺	Status	Response Type		
C G OFault Web Site G G Default Web Site G MDWS1_2 C G G NumExchange	ASP.NET Impersonation Forms Authentication Windows Authentication	Disabled Disabled Disabled	HTTP 302 Login/Redirect HTTP 401 Challenge		
Einen hinn 'htenit uch sond' uch sond	E reatures View				

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

2.11.1 Application Pool Configuration

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

Connections						Ac	tions
	This page lets you vier Application pools are applications, and prov	w and man associated vide isolatio	OIS age the list of a with worker pro on among differ	oplication pools on cesses, contain one ent applications.	the server. e or more		Add Application Pool Set Application Pool Defaults Application Pool Tasks Start
Þ 🔞 Default Web Site	Filter:	• 1	🖉 Go 🛛 🕁 Sho	w All Group by:	Ŧ		Stop
a 🔞 NumiExchange	Name 📩	Status	.NET CLR V	Managed Pipel	Identity	*	Recycle
⊳ ، 🚰 aspnet_client ⊳ ، 🚰 bin	.NET v4.5 .NET v4.5 Classic DefaultAppPool	Started Started	v4.0 v4.0 v4.0	Integrated Classic Integrated	ApplicationPool ApplicationPool		Edit Application Pool Basic Settings
	NumiExchange	Started	v4.0	Integrated	ApplicationPool		Advanced Settings Rename
						×	Remove
							View Applications
	٢		ш		>	0	Help
< III >	Features View	Content Vie	w				

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

NumiExchang	e	
NET CLR vers	ion:	
.NET CLR Ver	ion v4.0.30319	
Managed pip	eline mode:	
Integrated	~	
🖌 Start appli	ation nool imm	nediately

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

	Advanced Setti	ngs 🥂	
4	(General)		^
	.NET CLR Version	v4.0	
	Enable 32-Bit Applications	False	
	Managed Pipeline Mode	Integrated	
	Name	NumiExchange	-
	Queue Length	1000	
	Start Mode	OnDemand	
4	CPU		F
	Limit (percent)	0	
	Limit Action	NoAction	
	Limit Interval (minutes)	5	
	Processor Affinity Enabled	False	
	Processor Affinity Mask	4294967295	
	Processor Affinity Mask (64-bit option)	4294967295	1
⊿	Process Model		
4	Generate Process Model Event Log Entry		
	Idle Time-out Reached	True	
	Identity	ApplicationPoolIdentity	
	Idle Time-out (minutes)	20	V

Figure 30: NUMI Exchange Pool Advanced Settings

	Idle Time-out Action	Terminate	^
	Load User Profile	False	
	Maximum Worker Processes	1	
	Ping Enabled	True	
	Ping Maximum Response Time (seconds)	90	
	Ping Period (seconds)	30	
	Shutdown Time Limit (seconds)	90	
	Startup Time Limit (seconds)	90	
⊿	Process Orphaning		
	Enabled	False	
	Executable		_
	Executable Parameters		=
⊿	Rapid-Fail Protection		
	"Service Unavailable" Response Type	HttpLevel	
	Enabled	True	
	Failure Interval (minutes)	5	
	Maximum Failures	5	
	Shutdown Executable		
	Shutdown Executable Parameters		~

4	Recycling		
	Disable Overlapped Recycle	False	
	Disable Recycling for Configuration Chang	False	10
Þ	Generate Recycle Event Log Entry		
	Private Memory Limit (KB)	0	
	Regular Time Interval (minutes)	1740	=
	Request Limit	0	
Þ	Specific Times	TimeSpan[] Array	
	Virtual Memory Limit (KB)	0	
			Y

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.

Help	NUMI_Main_1.1	1.15.0_Build_20121019.1.zip Properties 💦 🔀
> Folders	General Secu	urity Summary
		NUMI_Main_1.1.15.0_Build_20121019.1.zip
NOMI_Main_1,1,15.0_Build_20121019,1.2ip	Type of file:	Compressed (zipped) Folder
	Opens with:	S Compressed (zipped) F Change
	Location:	C:\Temp
	Size:	18.8 MB (19,817,151 bytes)
	Size on disk:	18.9 MB (19,820,544 bytes)
	Created:	Yesterday, October 22, 2012, 9:41:45 AM
	Modified:	Yesterday, October 22, 2012, 9:41:46 AM
	Accessed:	Today, October 23, 2012, 9:11:24 AM
	Attributes:	Egead-only Hidden Advanced
	Security:	This file came from another computer and might be blocked to help protect this computer.

Figure 31: Unblocking Restricted Files in Installation ZIP File

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

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

11.2. NUMI Web Site Configuration

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

<u>5</u> ite name:	Application pool:	
NUMI	NUMI	Select
-Content Directory Physical path:		
D:\NUMI\ <install_dir< td=""><td>×</td><td>m</td></install_dir<>	×	m
Pass-through auther	tication	
<u>C</u> onnect as	est Settings	
Binding		
	IP address:	Port:
Host name:		
197 1989 - 199 - 199		
Example: www.conto	oso.com or marketing.contoso.co	m
- 	2003/2002	
Start Web site imme	diately	

Figure 32: Add NUMI Website

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

Figure 33: NUMI Basic Settings

Edit Site			? ×
Site name:	Application pool:		S <u>e</u> lect
Physical path: D:\NUMI\ <install_dir></install_dir>		j	
Pass-through authentication	<u>1</u> s		
		ок	Cancel

Figure 34: NUMI Advanced Settings

∃ (General)		
Application Pool	NUMI	
Bindings	http:*:11132:,https:*:8132;	
ID	4	
Name	NUMI_Prod_1_1_13_2	
Physical Path	D:\NUMI\ <install_dir></install_dir>	
Physical Path Credentials	2	
Physical Path Credentials Logon Type	ClearText	
Start Automatically	True	
Behavior		
Connection Limits		
Enabled Protocols	http	
Failed Request Tracing		
Application Pool		
Application Pool [applicationPool] Configures this applicati	ion to run in the specified application pool.	

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

Figure 35: NUMI Bindings

Гуре	Host Name	Port	IP Address	Binding Information	<u>A</u> dd
nttp		80	*		
https		443	*		Edit.,,
net.tcp				808:*	Demous
net.pipe				*	Remove
net.m				localhost	Browse
msmq				localhost	

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

8	Internet Inform	nation Services	(IIS) Manager		- 🗆 🗙
€ VAAUSVAEAPP80 → Site	s ► NUMI-SSO ►			69	× 🙆 🔞 •
File View Help					
File View Help Connections Con	Authentication Group by: No Grouping • Name • Anonymous Authentication ASP.NET Impersonation Basic Authentication Digest Authentication Forms Authentication Windows Authentication	Status Disabled Disabled Disabled Enabled Disabled	Response Type HTTP 401 Challenge HTTP 401 Challenge HTTP 302 Login/Redirect HTTP 401 Challenge	Actions	
 → - ib → - Scripts → - isiteminderagent 	Features View Content View				
Configuration: 'NUMI-SSO' web.config					G:

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.

- 🗆 × Nanager Information Services (IIS) Manager 😡 🖂 🏠 I 🔞 🗸 \bigcirc 🔞 ► VAAUSNUMAPP22 ► Sites ► NUMI ► File View Help Connections Alerts Compression 🔍 - 🔚 🖄 🕵 Use of dynamic compression may increase processor 📬 Start Page utilization and reduce the Use this feature to configure settings for compression of responses. This can improve the E 🥞 VAAUSNUMAPP22 (VHAMASTER) perceived performance of a Web site greatly reduce bandwidth-related charges. overall performance of the Application Pools server. M Enable dynamic content compression (i) The dynamic content 🗄 🏀 NUMI compression module is not installed. $\mathbf{\overline{M}}$ Enable static content compression Actions EV Apply Cancel Help Online Help 🛐 Features View 🛛 🚰 Content View 4 Configuration: 'NUMI' web.config • ...

Figure 38: NUMI Compression Settings

11.3. Application Pool Configuration

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

Harmet Information Services (IIS	i) Manager						
	Application Pools						🖸 🖂 🙆 I 🔞 🕶
<u>Eile View H</u> elp							
Connections	Application This page lets you view associated with worker y different applications.	on Pool and manage processes, c	S • the list of applica contain one or mo	ation pools on the re applications, ar	server. Application pools an d provide isolation among	e	Actions Add Application Pool Set Application Pool Defaults Help Oplication
E Sites	Filter:	- 6	🛛 🔄 👻 😽 Show	v <u>A</u> ll Group by:	No Grouping	•	
2	Name 🔺	Status	.NET Frame	Managed Pipeli.	Identity	Applic	
	ASP.NET v4.0 ASP.NET v4.0 Cl Classic .NET App DefaultAppPool NUMI	Started Started Started Started Started	v4.0 v4.0 v2.0 v2.0 v2.0	Integrated Classic Classic Integrated Classic	ApplicationPoolIden ApplicationPoolIden ApplicationPoolIden ApplicationPoolIden	0 0 0 1	
Ready							G.

Figure 39: Applicatiaon 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

Edit Application Pool	? ×
Name:	
NUMI	
.NET Framework version:	
.NET Framework v2.0.50727	-
Managed pipeline mode:	
Classic	
Start application pool immediately	ncel

The NUMI application pool advanced settings are shown in **Error! Not a valid bookmark self**reference.

EI (General)	
INET Framework Version	v2.0
Linetice 32-Bit Applications	Faise Charain
Managed Pipeline Mode	CI2SSIC
Name	
Start Automatically	1000
	The
limit	0
limit Action	NoAction
limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
El Process Model	Sector database and sector secto
Identity	ApplicationPooldentity
Idle Time-out (minutes)	20
load User Profile	True
Maximum Worker Processes	111 11
Ping Enabled	True
Ping Maximum Response Time (seconds)	90
Ping Period (seconds)	30
Shutdown Timelimit (seconds)	90
Startup Time limit (seconds)	90
El Process Orphaning	
Enabled	False
Executable	
Executable Parameters	
Rapid-FailProtection	
"ServiceUnavailable" Response Type	Httplevel
Enabled	True
Failure Interval(minutes)	5
Maximum Failures	5
Shutdown Executable	
Shutdown Executable Parameters	
El Recycling	-
Disable Overlapped Recycle	False
Disable Recycling for Configuration Changes	False
B Generate Recycle Event log Entry	
Private Memory Limit (KB)	0
Request limit	120
Request mint	U Time S a coll A recu
Dispectific Times	Ime spant Array
virtual Memory Limit (KB)	U

Figure 41: NUMI Application Pool Advanced Settings

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

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

12.1. Agent location

The current version of software can be found below:

\\<mark>Redacted</mark> \Partners_Share\CA_SiteMinder_WebAgents\Windows\Current

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

12.2. Agent installation

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

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



Figure 42: Security Warning

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

Figure 43: Preparing to install dialog



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





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



Figure 45: Web agent install wizard - License agreement screen

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

Figure 46: Web agent install wizard - Install location screen

2	CA SiteMinder Web Agent	_ 🗆 X	
	Choo	se Install Location	
technologies	Specify a location for the Web Agent. If the path the word "webagent," the installation program v called "webagent" and appends it to the end of	does not contains will create a folder your path.	
	Where would you like to install?		
	C:\Program Files\CA\webagent		
	Restore Default Fol	der Choose	
InstallAnywhere			
Cancel	Pre	vious	

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



Figure 47: Web agent install wizard - Review screen

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

Figure 48: Web agent install wizard - Agent configuration screen



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

the server is restarted to continue with next steps.



Figure 49: Web agent install wizard - Install complete screen

12.3. Agent configuration

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



Figure 50: Launch Web Agent Configuration Wizard

If you were configuring the agent for the first time on this specific server, you would need to register the host with the IAM server. In that case, follow the instructions in Section 3.12.1.

Otherwise, skip to Section 3.13.1. Launch the Web Agent Configuration Wizard as described in Figure 50 and continue with the steps in that section.

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

iisreset

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

3.12.1 Configuring for the first time

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

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



Figure 51: Web agent configuration wizard - Host registration

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

Admin Password: <will be provided>

	Admin Registratio
Enter the name and pass register trusted hosts with This entry must match the Server.	word of an administrator who has the right to n the Policy Server. e name of an administrator defined in the Policy
Admin User Name Admin Password Confirm Admin Password Enable Shared Secret	threg threg Rollover
	Enter the name and pass register trusted hosts with This entry must match the Server. Admin User Name Admin Password Confirm Admin Password Enable Shared Secret

Figure 52: Web agent configuration wizard - Admin credentials

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

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

Table 3: IAM Host Configuration Object

3	CA SiteMinder Web A	gent	x
	Trusted Hos	t Name and Config	guration Object
technologies	Specify the name of the host y Enter the name of the host cor a host configuration object name	ou want to register with th nfiguration object. The na me already defined on the	ne Policy Server. ame must match e Policy Server.
	Trusted Host Name vaa Host Configuration Object SQA	usvaeweb80.aac.dva.va.go	v
InstallAnywhere		Previous	s Next

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

4. Add the three IP Address of Policy Server one at a time in the 'IP Address' box from Table 4 based on the IAM environment you are trying to connect to and click 'Next' in the dialog as shown in the **Error! Not a valid bookmark self-reference.**.

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

Table 4: SiteMinder Policy Server IP Address

3	CA SiteMinder Web Agent	x
	Policy Server IP Ac	Idress
technologies	For example: 111.12.12.2:1234 or myserver:1234 (IPv4) [2001:db8::1428:57ab]:1234 (IPv6) or [2001:db8::1428:57ab] or 2001:db8::1428:57ab NOTE: Include the port number in the IP address only if your Policy Server is behind a firewall.	*
	IP Address v Remove Add	
	10.227.238.46 10.227.238.47 10.227.238.48	
InstallAnywhere		
Cancel	Previous	lext

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

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

Figure 55: Web agent configuration wizard - FIPS mode setting



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



Figure 56: Web agent configuration wizard - Configuration file location

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

Figure 57: Web agent configuration wizard - Web server

3	CA SiteMinder Web Agent	_ 🗆 🗙
	Se	lect Web Server(s)
technologies	Select which web server(s) you wish to configur Unselect a web server to unconfigure that web preserve a web server, do not unselect that web	re as Web Agent(s). server. To o server.
	Microsoft IIS 8.0	
InstallAnywhere	Pre	vious Next

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



Figure 58: Web agent configuration wizard - Agent configuration

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

Fiaure	59: Web	agent	configuratio	on wizard	- Sites	selection

2	CA SiteMinder Web Agent	- • ×
	Select	Virtual Site(s)
technologies	Select virtual sites(s) to be configured. Already config can be unconfigured, reconfigured and preserved in t	ured sites he next step.
	☐ <u>Select All</u> ☐ Default Web Site ✔ Numi	
InstallAnywhere	Previous	Next

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



Figure 60: Web agent configuration wizard - Summary screen

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

Figure 61: Web agent configuration wizard - Completion screen



3.13.1 Reconfiguration configuration

NOTE: The steps below are if you want to reconfigure one or more websites in IIS due to say

re-deployment. The server should have already been registered with IAM using the steps in Section 3.12.1.

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

2	CA SiteMinder Web Agent	_ 🗆 🗙
	н	lost Registration
technologies	Select 'Yes' to register this Agent with the Policy Server Select 'No' to register later.	er.
	 Yes, I would like to do Host Registration now. <u>No, I would like to do Host Registration later</u> Warning: You have already registered this Agent with 	n a Policy Server.
InstallAnywhere Cancel	Previo	us Next

Figure 62: Web agent configuration wizard - Host registration

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

3	CA SiteMinder Web Agent	×
	S	elect Web Server(s)
technologies	Select which web server(s) you wish to config Unselect a web server to unconfigure that we preserve a web server, do not unselect that we	jure as Web Agent(s). b server. To leb server.
	Microsoft IIS 8.0	
InstallAnywhere	P	revious Next

Figure 63: Web agent configuration wizard - Web server

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

Figure 64: Web agent configuration wizard - Agent configuration

2	CA SiteMinder Web Agent	<u>– – ×</u>
	Default Agent C	onfiguration Object
technologies	Enter the name of the ACO that defines the defau Web Agent in Policy Server for Microsoft IIS Serve independent agent configurations for application Application Pools.	It configuration of the r. To support pools, select Manage
	Default Agent Configuration Object	fig
	Enable Agent Manage Application Pools	
InstallAnywhere Cancel	Pr	evious Next

4. Select the NUMI website and any other sites where you want to enable SSO on and

click 'Next'. The sites that were previously configured will remain selected and cannot be changed (unconfigured) as shown in Figure 65.

3	CA SiteMinder Web Agent
	Select Virtual Site(s)
technologies	Select virtual sites(s) to be configured. Already configured sites can be unconfigured, reconfigured and preserved in the next step.
	☐ Select All ☐ Default Web Site ✓ NUMI15.0 ✓ NUMI-SSO
InstallAnywhere	Previous Next

Figure 65: Web agent configuration wizard - Sites selection

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



Figure 66: Web agent configuration wizard - Summary screen

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

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



Figure 67: Web agent configuration wizard - Previously configured sites

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





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



Figure 69: Web agent configuration wizard - Completion screen

13. Secure Token Service Integration for SSOi

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

13.1. Download Certificate Chain from appropriate endpoint

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

- iDEV: https://<mark>Redacted</mark>9301/STS/RequestSecurityToken
- SQA: https://Redacted:9301/STS/RequestSecurityToken
- PREPROD: https:// Redacted:9301/STS/RequestSecurityToken
- PROD: https://Redacted 9301/STS/RequestSecurityToken
- 1. Install the full certification chain from the matching IAM environment(s). This can be obtained by visiting the link and clicking the lock icon and choosing "View Certificates". https://services.eauth.va.gov:9301/



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.

ertificate Export Wizard	×
File to Export Specify the name of the file you w	vant to export
File name:	
sts_preprod_8_24_2019	Browse
	< Back Next > Cancel

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

	Issue	d To) ^	Issued By
l Computer)	Galde Callo	ev.se calh	ervices.eauth.va.gov ost	VA-Internal- localhost
All Tasks	,		Request New Certificat	e al-
View	•		Import	al-
New Window from Here		20	Advanced Operations	* al-
New Taskpad View		Int	ternal-S2-RCA1-v1	VA-Internal-
Refresh		15/	C-VAAUSNUMWEB820	WIVISVC-VAA
Help		-		
	All Tasks All Tasks View New Window from Here New Taskpad View Refresh Export List Help	I Computer) Issue I Computer Issue I Computer) Issue I Computer Issue I Computer Issue Iss	I Computer) Issued To adev.se All Tasks Issued To adev.se View Issued To adev.se New Window from Here Issued To adev.se New Window from Here Integration New Taskpad View Integration Refresh Issued To adev.se Export List Help	Issued To Geomputer) All Tasks All Tasks View New Window from Here New Taskpad View Refresh Export List Help

6. Import for local machine

Welcome to the	Certificate Im	port Wizard	
This wizard helps you cop lists from your disk to a co	y certificates, certifica rtificate store.	te trust lists, and c	ertificate revocation
A certificate, which is issu and contains information connections. A certificate	ed by a certification a used to protect data o store is the system ar	uthority, is a confirr r to establish secur ea where certificat	nation of your identity e network es are kept.
Store Location			
 Current User Local Machine 			
To continue, <mark>dick</mark> Next.			

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

File to Import			
Specify the file y	ou want to import.		
File name:			
C:\Users\VHAI	DCONFEJ0\Desktop\SSOi-IN	T_CertChain.p7b	Browse
Personal Info Cryptographi Microsoft Ser	rmation Exchange- PKCS #12 : Message Syntax Standard- alized Certificate Store (.SST)	(.PFX,.P12) PKCS #7 Certificates ()	(.P7B)

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

Certificat	e Store	
Certi	ficate stores are system areas where certificate	s are kept.
Wind the c	ows can automatically select a certificate store, ertificate.) Automatically select the certificate store based) Place all certificates in the following store	or you can specify a location for d on the type of certificate
	Certificate store:	
	Personal	Browse
	H1 7/2	

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

	Consol	le1 - [Console Root\Certific	ates (Local Comp	ut
File Action View Favorites Window Hel	p			
🛅 Console Root	Issued To	Issued By	Expiration Date	1
⊿ Grtificates (Local Computer)	dev.services.eauth.va.gov	VA-Internal-S2-ICA1-v1	4/25/2020	- 1
🔺 🚞 Personal	🕼 localhost	localhost	2/8/2023	3
Certificates	VAAUSNUMWEB820.AAC.DVA	VA-Internal-S2-ICA1-v1	1/8/2021	(
Trusted Root Certification Authorities	🛱 vaausnumweb820.aac.dva.va.gov	VA-Internal-S2-ICA1-v1	11/5/2019	5
Enterprise Trust	vaausnumweb820.aac.dva.va.gov	VA-Internal-S2-ICA1-v1	11/5/2019	F
Intermediate Certification Authorities	VA-Internal-S2-ICA1-v1	VA-Internal-S2-RCA1-v1	10/25/2026	3
Trusted Publishers	VA-Internal-S2-RCA1-v1	VA-Internal-S2-RCA1-v1	10/26/2036	
 Intrusted Certificates Intrusted Certification Authorities 	WMSvc-VAAUSNUMWEB820	WMSvc-VAAUSNUMWEB820	1/6/2028	

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.

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

1. Find the server cert in the personal folder

Console Root	Issued To	Issued By	Expiration Date
 Gertificates (Local Computer) Personal 	🔄 dev.services.eauth.va.gov 🛱 localhost	VA-Internal-S2-ICA1-v1 localhost	4/25/2020 2/8/2023
 Certificates Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Third-Party Root Certification Authorities 	VAAUSNUMWEB820.AAC.DVA vaausnumweb820.aac.dva.va.gov vaausnumweb820.aac.dva.va.gov vaausnumweb820.aac.dva.va.gov VA-Internal-S2-ICA1-v1 VA-Internal-S2-RCA1-v1 WMSvc-VAAUSNUMWEB820	VA-Internal-S2-ICA1-v1 VA-Internal-S2-ICA1-v1 VA-Internal-S2-ICA1-v1 VA-Internal-S2-RCA1-v1 VA-Internal-S2-RCA1-v1 WMSvc-VAAUSNUMWEB820	1/8/2021 11/5/2019 11/5/2019 10/25/2026 10/26/2036 1/6/2028

Trusted People

2. Right click and export the certificate

🛱 localhost	localhost	2/8/2023 S	erver Authenticati	IIS Express Develop
🙀 VAAUSNUMWEB820.AAC.DVA	VA-Internal-S2-ICA1-v1	1/8/2021 C	lient Authenticati	VAAUSNUMWEB82
vaausnumweb820.aac.dva.va.gov	VA-Internal-S2-ICA1-v1 VA-Internal-S2-ICA1-v1 VA-Internal-S2-RCA1-v1 VA-Internal-S2-RCA1-v1 WMSvc-VAAUSNUMWEB820	Open	ver Authenticati	<none></none>
なる なる いた なる いた いた にた にた いる にた いる にた いる した い した した した した した した した した した した		All Tasks 🔸	Open	
		Cut Copy Delete	Request Certif Renew Certific Manage Privat	icate with New Key cate with New Key te Keys
		Properties	Advanced Op	erations 🔸
		Help	Export	

3. Select "Yes, export private key" and choose next
| Free to be to be | |
|-------------------------------------|---|
| You can choose | e to export the private key with the certificate. |
| | et et strittens anns anns et al et autout |
| Private keys ar
certificate, you | e password protected. If you want to export the private key with the
u must type a password on a later page. |
| Do you want to | export the private key with the certificate? |
| • Yes, ex | port the private key |
| 🔿 No, do | not export the private key |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

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

Export File Format Certificates can be exported	n a variety of file formats.
Select the format you want to) use:
O DER encoded binary X	.509 (.CER)
O Base-64 encoded X.50	9 (.CER)
O Cryptographic Messag	e Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certifica	tes in the certification path if possible
Personal Information E	xchange - PKCS #12 (.PFX)
✓ Include all certifica	tes in the certification path if possible
Delete the private	key if the export is successful
Export all extende	d properties
O Microsoft Serialized Ce	rtificate Store (.SST)
 Microsoft Serialized Ce 	rtificate Store (.SST)

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

To maintain security, you must prote using a password.	ect the private key to a security principal or by
Group or user names (recommen	ded)
	Add
	Remove
Password:	
Carfur analysis	
Commin password;	

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="https:// Redacted:9301/STS/RequestSecurityToken"/>
<add key="STSEnabled" value="true"/> <!-- Set "true" to enable STS service integration -->
<add key="STSCertificatePath" value="D:\\numi_web820.pfx"/>
<add key="STSCertificatePassword" value="numi123"/>
```

STSEnabled - anything but "true" will disable STS and revert to access/verify

14. Installing CERMe Software and Database from CERMe Installation CD

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

14.1. Install CERMe on the Application Server

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

CERMe Review Manager (RM) 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 is 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"><Property
name="rewrite.originalPathAttribute"><Property
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:

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 70.



Figure 70: IIS Server Certificates

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

View Help hections Start Page VALUSNUMAPP22 (VHAMASTER) Contraine Deals	Server Certifi	cates		
ections	Server Certifi	cates		
Start Page VAAUSNUMAPP22 (VHAMASTER)				Actions Import
Application Pools	Start Page Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.			
🗄 🧕 Sites	Name *	Issued To	Issued By	Create Domain Certificate
⊡		WMSvc-VAAUSNUMAPP22 VAAUSNUMAPP22.aac.dva.va.gov	WMSvc-VAAUSNUMAPP22 VA Internal Subordinate CA 1	Create Self-Signed Certificate.
B B B B B B B B B B B B B B B B B B B				View Export Renew Remove Help Online Help

Figure 71: IIS Server Certificate Selection

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

Figure 72: IIS Certificate Details

xport Certificate					? ×
Export to:					
D:\Certs\NUMI.pfx					
Password:					
••••					
Confir <u>m</u> password:					
••••					
	-	01/	-	<i>c</i>	. 1
		OK		Cance	el

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

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

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

5. Execute the following command:

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

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

6. Execute the following command:

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

Make a note of the long, auto-generated alphanumeric value circled in red below. Recommended actions are to copy, paste the entire command prompt output to notepad to copy, and paste this value. Figure 73: keytool -keystore "C:\Certs\CERME.ks" -list

C:\WINDOWS\system32\cmd.exe	_ 🗆 ×
C:\Program Files\McKesson\CERME\Jre\bin>keytool -importkeystore -srcstorety; CS12 -srckeystore "C:\NUMI\Certs\fw_cert_2012.pfx" -destkeystore "C:\NUMI\C CERME ke"	pe PK
Enter destination keystore password: Re-enter new password:	
Enter source keystore password: Entry for alias 3dcb9f87fe5f1e766d115a06a15c804c_c4444c68-d09f-4c3b-9be2-7a 72c01 successfully imported. Import command completed: 1 entries successfully imported, 0 entries faile cancelled	b723a d or
C:\Program Files\McKesson\CERME\Jre\bin>keytool -keystore "C:\NUMI\Certs\CE s" -list Enter keystore password:	RME.k
Keystore type: JKS Keystore provider: SUN	
Your keystore contains 1 entry	
3dcb9f87fe5f1e766d115a06a15c804c_c4444c68-d09f-4c3b-9be2-7ab723a72c01, JuV 012, PrivateKeyEntry, Certificate fingerprint_(MD5):_FE:0D:2A:B7:6F:0B:D5:8A:93:53:E6:DA:22:87:D9	10, 2 :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.

- 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).

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

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

15. Setting up NUMI Section in the Windows Event Log

- 1. Change Directory Go to command prompt (run as Administrator) and change current directory to Framework v2.0 bit folder e.g., C:\WINDOWS\MS.NET\Framework\v4.5.x
- 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.

Event Viewer File Action View Help					
Event Viewer (Local)	Applications and Services L	ogs			Actions
 Windows Logs Applications and Services Logs Hardware Events Internet Explorer Key Management Service Microsoft NUMI Operations Manager Windows PowerShell Subscriptions 	Name Hardware Events Internet Explorer Key Management Service Microsoft NUMI Operations Manager Windows PowerShell	Administrative Administrative Administrative Administrative Administrative Administrative	Number of Events 0 0 21 12,304 39	5128 68 KB 68 KB 68 KB 5.07 MB 68 KB	Open Saved Log Open Saved Log Create Custom View Import Custom View View Refresh Help Hardware Events Open Properties
					Relp

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

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

15.1. Validate XML Configuration File Settings

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

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

Settings to update:

```
<appSettings
configSource="src\\main\\resources\\xml\\deployment\\numiwebapp.conf
ig"/>
<connectionStrings/>
```



📕 Web.config - Notepad
Eile Edit Format View Help
<pre> Lime Luk Tightak Jew Lup </pre>
<pre><!-- change this setting to point to the appropriate config file for the deployment--> <appsettings configsource="src\main\\resources\\xml\\deployment\\NumiwebApp.config"></appsettings> <system.web></system.web></pre>
<pre><add assembly="eworld.UI" namespace="eworld.UI" tagprefix="ew"></add></pre>

2. Edit the application settings in the config file indicated in the previous entry. Make sure to enter the VDIF 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="<VDIF Service URL>" />
<add key="RequestingApp" value="<Requesting App ID to be identified
in VDIF>"/>
<add key="IsSynchronizer" value="true"/>
<add key="WSDLusername" value="<VDIF WSDL username>"/>
<add key="WSDLpassword" value="<VDIF WSDL password>"/>
<add key="numiDbConnectionString" value="Data
Source=<enter_database_server>;Database=NUMI;User
ID=numi_user;Password=xxxxxxx;Trusted_Connection=False" />
<add key="SSOLogoutUri" value="..." /></a>
```

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

Table 5: SSOLogoutUri v	/alues
-------------------------	--------

Environment	Value		
DEV	https:// Red	ted /centrallogin/lc	oggedout.aspx
SQA	https:// Red	ted /centrallogin/lc	oggedout.aspx
Preprod	https:// Red	ted /centrallogin/lc	oggedout.aspx
PROD	https:// Red	ted /centrallogin/lc	oggedout.aspx

- 3. Follow the steps below to encrypt the updated NumiWebApp.config
 - a. Open a command prompt and change to .Net Framework 4.x directory (e.g. C:\Windows\MS.NET\Framework64\v4.x.x)
 - b. Run command :

.\aspnet_regiis.exe -pef "appSettings"
D:\NUMI\<install dir>

- c. The command should execute successfully and give the following message: Encrypting configuration section... Succeeded!
- d. Verify that the
 src\\main\\resources\\xml\\deployment\\NumiWebApp.config
 file does not contain any plain text passwords any more.

NOTE:

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

To make any future changes to the

src\\main\\resources\\xml\\deployment\\NumiWebApp.config first decrypt the file by
running command:

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

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

16. Perform Restart

Restart IIS

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

17. Test NUMI Web Site Functionality

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

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="http://</pre>
Redacted:57700/csp/healthshare/hsaccvdappl/HS.Local.VA.HS.Access.VWS
L.Service.NUMIService.cls" />
<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="https://</pre>
Redacted:9301/STS/RequestSecurityToken"/>
<add key="STSEnabled" value="true"/>
<add key="STSCertificatePath"
value="D:\\NUMI\Synchronizer\numisyncsga.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

NUMI Synchronizer		NUM Synchronizer - Regularly pol	s conf Automatic	Local System
Offline Files	Start	iles service performs n	nainte Disabled	Local System
🖏 OpenSSH Authe	Stop	d private keys used for	publi Disabled	Local System

For an upgrade in place:

1. Stop the existing service from services.msc

NUMI Synchronizer	MUMI Supe	bronizer - Regularly polls conf	Automatic	Local System
Offline Files	Start	iles service performs mainte	Disabled	Local System
🖏 OpenSSH Authe	Stop	d private keys used for publi	Disabled	Local System

2. Copy the Sychronizer 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

🔄 > This PC > APPS (D:) > NUMI > Synchronizer - Copy							
-			Name ^	Date modified	Туре	Size	
-			🔄 Common.dll	9/14/2022 7:54 AM	Application extens	351 KB	
5	1		📓 Common.Logging.dll	8/25/2022 11:36 AM	Application extens	28 KB	
s	*		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	
			lnpatient.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	

3. Start the service from services.msc

NUMI Synchronizer		NUMI Synchronizer - Regularly polls conf	Automatic	Local System
Offline Files	Start	iles service performs mainte	Disabled	Local System
OpenSSH Authe	Stop	d 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
НТТР	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
VDIF	Veterans Data Integration and Federation
VistA	Veterans Information Systems Technology Architecture

21. NUMI Comparison Table

NUMI Version	CERMe RM	InterQual View	CA SiteMinder	Windows Server	MS SQL Server
15.4	16.1	2017.2	12.51	2012 R2	2012
15.5	17	2018.1	12.51	2012 R2	2012
15.6	17	2018.1	12.51	2012 R2	2012

15.8	18.1	2019.1	12.51	2012 R2	2012
15.9	19.0	2020	12.51	2012 R2	2012
15.9.1	20.0	2021	12.52	2019	2019
15.10	21.0.1	2022	12.52	2019	2019
15.11	21.0.1	2022	12.52	2019	2019
15.14	21.0.1	2022	12.52	2019	2019
15.15	22.0	2024	12.52	2019	2019
15.16	22.0	2024	12.52	2019	2019
16.0	22.0	2024	12.52	2019	2019