

# **HealthVet Web Services Client (HWSC) 1.0 Patch XOBW\*1.0\*4**

## **Installation, Back-Out, and Rollback Guide**



**October 2016**

**Department of Veterans Affairs (VA)**

**Office of Information and Technology (OI&T)**

**Enterprise Program Management Office (EPMO)**

## Revision History

Date	Revision	Description	Author
10/20/2016	1.0	Initial document created for HWSC 1.0 Patch XOBW*1.0*4.	HealtheVet Web Services Client (HWSC) Project Team

# Table of Contents

Revision History .....	ii
List of Figures .....	iv
List of Tables .....	iv
Orientation .....	v
<b>1 Introduction .....</b>	<b>1</b>
1.1 Purpose .....	1
<b>2 Pre-installation and System Requirements.....</b>	<b>2</b>
2.1 Coordinate with System Administrator .....	2
2.2 VistA Environment, KIDS, and SSL/TLS Configurations .....	2
2.3 Skills Needed for the Installation.....	3
2.4 Access Requirements—Privileges and Permissions Needed for the Installation .....	3
2.4.1 VistA Programmer Access .....	4
2.4.2 Caché System Administration Account Access .....	4
2.4.3 cacheexport.xsd File Permissions (System Administrator) .....	4
2.5 Platform Installation and Preparation .....	5
2.6 Obtain and Extract Distribution Files .....	5
2.6.1 Software .....	5
2.6.2 Documentation.....	6
2.7 Installation Scripts.....	6
2.8 Cron Scripts .....	6
<b>3 Installation Procedure .....</b>	<b>6</b>
3.1 Patch Installation Instructions.....	6
3.2 Load and Install Distribution.....	7
3.3 Post-Installation Instructions (System Administrator).....	8
3.3.1 Create the “encrypt_only” SSL/TLS Configuration File .....	8
3.3.2 Verify the “encrypt_only” SSL Configuration File Exists.....	9
3.4 Sample KIDS Installation.....	11
3.5 Troubleshoot Installation Errors / Review Install File .....	12
3.5.1 Caché Error 6301 cacheexport.xsd Document Could Not Be Opened .....	12
3.5.2 Caché “<PROTECT>” Error .....	13
3.6 Database Creation .....	13
<b>4 Implementation Procedure .....</b>	<b>14</b>
4.1 Database Tuning.....	14
4.2 Verify Installation.....	14
<b>5 Back-Out Plan .....</b>	<b>15</b>
5.1 Back-Out Strategy .....	15
5.2 Back-Out Considerations .....	15
5.2.1 Load Testing .....	15
5.2.2 User Acceptance Testing .....	15

5.3	Back-Out Criteria .....	15
5.4	Back-Out Risks .....	15
5.5	Authority for Back-Out .....	15
5.6	Back-Out Procedure .....	15
<b>6</b>	<b>Rollback Plan .....</b>	<b>16</b>
6.1	Rollback Considerations.....	16
6.2	Rollback Criteria .....	16
6.3	Rollback Risks .....	16
6.4	Authority for Rollback .....	16
6.5	Rollback Procedure .....	16

## List of Figures

Figure 1: Post-Installation Instructions—Create the “encrypt_only” SSL/TLS Configuration File	8
Figure 2: Post-Installation Instructions—Confirmation of Successful Configuration File Creation	9
Figure 3: Post-Installation Instructions—Verifying the “encrypt_only” SSL Configuration File Exists: Successful.....	9
Figure 4: Post-Installation Instructions—Verifying the “encrypt_only” SSL Configuration File Exists: Unsuccessful .....	10
Figure 5: Sample HWSC Patch XOBW*1.0*4 Installation on a VMS System .....	11
Figure 6: Cache Error 6301 cacheexport.xsd: Primary Document Could Not Be Opened .....	12
Figure 7: Undeclared Attributes and Unknown Elements .....	13
Figure 8: Cache “<PROTECT>” Error (1 of 2) .....	13
Figure 9: Cache “<PROTECT>” Error (2 of 2) .....	13

## List of Tables

Table 1: Documentation symbol descriptions .....	vi
Table 2: HWSC Documentation .....	6

# Orientation

## How to Use this Manual

The Installation, Back-out, Rollback Guide defines the ordered, technical steps required to install the product, and if necessary, to back-out the installation, and to roll back to the previously installed version of the product.

Throughout this manual, advice and instructions are offered regarding the use of the HealtheVet Web Services Client (HWSC) Patch XOBW\*1.0\*4 software and the functionality it provides for Veterans Health Information Systems and Technology Architecture (VistA) software products.

## Intended Audience

The intended audience of this manual is the following stakeholders:

- Information Resource Management (IRM)—System administrators and Capacity Management personnel at Department of Veterans Affairs (VA) sites who are responsible for computer management and system security on the VistA M Servers.
- Enterprise Program Management Office (EPMO)—VistA legacy development teams.
- Product Support (PS).

## Disclaimers

### Software Disclaimer

This software was developed at the Department of Veterans Affairs (VA) by employees of the Federal Government in the course of their official duties. Pursuant to title 17 Section 105 of the United States Code this software is *not* subject to copyright protection and is in the public domain. VA assumes no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic. We would appreciate acknowledgement if the software is used. This software can be redistributed and/or modified freely provided that any derivative works bear some notice that they are derived from it, and any modified versions bear some notice that they have been modified.

### Documentation Disclaimer

This manual provides an overall explanation of using the HealtheVet Web Services Client (HWSC) Patch XOBW\*1.0\*4 software; however, no attempt is made to explain how the overall VistA programming system is integrated and maintained. Such methods and procedures are documented elsewhere. We suggest you look at the various VA Internet and Intranet SharePoint sites and websites for a general orientation to VistA. For example, visit the Office of Information and Technology (OI&T) Enterprise Program Management Office (EPMO) Intranet website.





**DISCLAIMER: The appearance of any external hyperlink references in this manual does *not* constitute endorsement by the Department of Veterans Affairs (VA) of this Website or the information, products, or services contained therein. The VA does *not* exercise any editorial control over the information you find at these locations. Such links are provided and are consistent with the stated purpose of this VA Intranet Service.**

# Documentation Conventions

This manual uses several methods to highlight different aspects of the material:

- Various symbols are used throughout the documentation to alert the reader to special information. [Table 1](#) gives a description of each of these symbols:

**Table 1: Documentation symbol descriptions**

Symbol	Description
	<b>NOTE / REF:</b> Used to inform the reader of general information including references to additional reading material.
	<b>CAUTION / RECOMMENDATION / DISCLAIMER:</b> Used to caution the reader to take special notice of critical information.

- Descriptive text is presented in a proportional font (as represented by this font).
- “Snapshots” of computer online displays (i.e., screen captures/dialogues) and computer source code is shown in a *non*-proportional font and may be enclosed within a box.
  - User’s responses to online prompts are **bold** typeface and highlighted in yellow (e.g., **<Enter>**). The following example is a screen capture of computer dialogue, and indicates that the user should enter two question marks:

Select Primary Menu option: **??**

- Emphasis within a dialogue box is **bold** typeface and highlighted in blue (e.g., **STANDARD LISTENER: RUNNING**).
- Some software code reserved/key words are **bold** typeface with alternate color font.
- References to “**<Enter>**” within these snapshots indicate that the user should press the **Enter** key on the keyboard. Other special keys are represented within < > angle brackets. For example, pressing the **PF1** key can be represented as pressing **<PF1>**.
- Author’s comments are displayed in italics or as “callout” boxes.



**NOTE:** Callout boxes refer to labels or descriptions usually enclosed within a box, which point to specific areas of a displayed image.

- This manual refers to the M programming language. Under the 1995 American National Standards Institute (ANSI) standard, M is the primary name of the MUMPS programming language, and MUMPS is considered an alternate name. This manual uses the name M.
- All uppercase is reserved for the representation of M code, variable names, or the formal name of options, field/file names, and security keys (e.g., the XUPROGMODE security key).



**NOTE:** Other software code (e.g., Delphi/Pascal and Java) variable names and file/folder names can be written in lower or mixed case (e.g., CamelCase).

# How to Obtain Technical Information Online

Exported VistA M Server-based software file, routine, and global documentation can be generated using Kernel, MailMan, and VA FileMan utilities.



**NOTE:** Methods of obtaining specific technical information online is indicated where applicable under the appropriate section.

## Help at Prompts

VistA M Server-based software provides online help and commonly used system default prompts. Users are encouraged to enter question marks at any response prompt. At the end of the help display, you are immediately returned to the point from which you started. This is an easy way to learn about any aspect of VistA M Server-based software.

## Obtaining Data Dictionary Listings

Technical information about VistA M Server-based files and the fields in files is stored in data dictionaries (DD). Use the List File Attributes option on the Data Dictionary Utilities menu in VA FileMan to print formatted data dictionaries.



**REF:** For details about obtaining data dictionaries and about the formats available, see the “List File Attributes” section in the “File Management” section in the *VA FileMan Advanced User Manual*.

## Assumptions

This manual is written with the assumption that the reader is familiar with the following:

- VistA computing environment:
  - Kernel—VistA M Server software
  - VA FileMan data structures and terminology—VistA M Server software
- Microsoft® Windows environment
- M programming language

## Reference Materials

Readers who wish to learn more about HealtheVet Web Services Client (HWSC) should consult the following:

- *HWSC 1.0 Patch XOBW\*1.0\*4 Release Notes*
- *HWSC 1.0 Patch XOBW\*1.0\*4 Installation, Back-Out, and Rollback Guide* (this manual)
- *HWSC 1.0 Patch XOBW\*1.0\*4 Security Configuration Guide*
- *HWSC 1.0 Installation Guide*
- *HWSC 1.0 Systems Management Guide*
- *HWSC 1.0 Developer's Guide*

VistA documentation is made available online in Microsoft® Word format and in Adobe® Acrobat Portable Document Format (PDF). The PDF documents *must* be read using the Adobe® Acrobat Reader, which is freely distributed by Adobe® Systems Incorporated at: <http://www.adobe.com/>

VistA documentation can be downloaded from the VA Software Document Library (VDL):  
<http://www.va.gov/vdl/>



**REF:** See the [HealtheVet Web Services Client \(HWSC\) manuals on the VDL](#).

VistA documentation and software can also be downloaded from the Product Support (PS) Anonymous Directories.



# 1 Introduction

HealtheVet Web Services Client (HWSC) Patch XOBW\*1.0\*4 enables the use of Transport Layer Security/Secure Socket Layer (TLS/SSL) on OpenVMS systems.

## 1.1 Purpose

The purpose of this guide is to provide instructions for installing HealtheVet Web Services Client (HWSC) Patch XOBW\*1.0\*4.

## 2 Pre-installation and System Requirements

### 2.1 Coordinate with System Administrator

Installers of the HWSC Patch XOBW\*1.0\*44 *must* coordinate with their respective system administration support group (e.g., Region Operation Center) to receive assistance in performing the complete installation.

Depending on your level of access it is expected that the work can be split as follows:

- The patch installer concentrates on performing tasks in the “[Load and Install Distribution](#)” section.
- The system administrator performs tasks in the following sections:
  - [cacheexport.xsd File Permissions \(System Administrator\)](#)
  - [Post-Installation Instructions \(System Administrator\)](#)

The following sections explain the need to coordinate with your system administrator. The result of your coordination determines which steps you can perform and which steps *must* be performed by the system administrator.

### 2.2 VistA Environment, KIDS, and SSL/TLS Configurations

Installers *must* coordinate with their system administrator to understand the number of nodes where Veterans Health Information Systems and Technology Architecture (VistA) is running and understand which nodes to which the installer has access. This applies to both VistA Test and Production accounts. The result of this coordination determines which node to access to install the HWSC Patch XOBW\*1.0\*4 KIDS build.

VistA applications are hosted in a Caché environment that can contain a cluster of one or more computer nodes. The basic topology is split into a set of Front-End nodes and a set of Back-End nodes (database nodes). For a small site, a single computer node can serve as both. For larger sites, the number of Front-End and Back-End nodes can vary.

A traditional Kernel Installation and Distribution System (KIDS) installation is performed *ONCE and ONLY* on a Back-End database node. Changes to the Back-End node are visible to all other nodes, except for SSL/TLS Configurations.



**NOTE:** The HWSC Patch XOBW\*1.0\*4 KIDS build includes both traditional components and non-traditional components, like the SSL/TLS configuration that is visible only to the node where the KIDS build was installed.

The HWSC Patch XOBW\*1.0\*4 KIDS build installation in the Back-End node will install or update the following components:

- Routines (visible to all nodes)
- Class xobw.WebServiceProxyFactory (visible to all nodes)
- Class xobw.WebServer (visible to all nodes)
- The "encrypt\_only" Transport Layer Security (TLS/SSL) configuration (visible only to the node where the KIDS build is installed)



**NOTE:** The TLS/SSL configuration *must* be installed in all nodes, both front-end server nodes and database server nodes.

**REF:** For more information, see the “[Post-Installation Instructions \(System Administrator\)](#)” section.

## 2.3 Skills Needed for the Installation

The installer needs to be familiar with the VistA environment and coordinate with a system administrator to be able to do the following:

- Obtain VistA software from FORUM and Secure File Transfer Protocol (SFTP) download sites (i.e., Product Support Anonymous Directories).
- Run a Kernel Installation and Distribution System (KIDS) installation.
- Use the VistA **EVE** menu.
- Log in through your **Captive User** VistA logon account or through your **Programmer Support** logon account:
  - **Captive User**—Use this logon account when you log in directly to VistA using your Access and Verify code. It has a *non*-privileged **%Developer** role.
  - **Programmer Support**—Use this logon account when you log in first to the operating system (OS) and then to VistA. It can have higher privileged roles, such as **%All** or **%Manager**.
- Execute commands in Programmer mode when given [VistA Programmer Access](#).
- Execute commands in Programmer mode when given the **%All** or **%Manager** role ([Caché System Administration Account Access](#)).
- Understand VistA’s cluster of front-end and back-end (database) servers.

## 2.4 Access Requirements—Privileges and Permissions Needed for the Installation

Installers *must* coordinate with their system administrator to determine which level of access they have.

The following privileges and permissions to resources are required in order to install the HWSC Patch XOBW\*1.0\*4 KIDS build and Secure Socket Layer/Transport Layer Security (SSL/TLS) Configuration:

- VistA Programmer Access
- Caché System Administration Account Access
- cacheexport.xsd File Permissions

An installer with a **Captive User** logon account has only the **Vista Programmer Access** and requires the assistance of a system administrator. An installer with a **Programmer Support** login account has **Caché System Administration Account Access**.

## 2.4.1 VistA Programmer Access

Installers *must* have **VistA Programmer Access** for installing Patch XOBW\*1\*4 KIDS build. DUZ(0) = “@” is required.



**NOTE:** Installers with a **Captive User** account see a warning that the SSL/TLS configuration could *not* be completed and need to coordinate with their system administrator to complete it as described in the “[Post-Installation Instructions \(System Administrator\)](#)” section.

## 2.4.2 Caché System Administration Account Access

Patch XOBW\*1\*4 KIDS also includes the Socket Layer/Transport Layer Security (SSL/TLS) Configuration installation step.



**NOTE:** Installers with a **Captive User** login account are *not* able to complete this step during the KIDS build installation and receive a warning, instructing them to obtain assistance from their system administrator to complete the last step of the KIDS build installation.

**REF:** For more information, see the “[Post-Installation Instructions \(System Administrator\)](#)” section.

Installers with a **Programmer Support** account should have the following roles (i.e., greater than the %Developer role):

- %All
- %Manager

To confirm you have the appropriate Caché privileges, look at \$USERNAME and \$ROLES. For example:

```
>W $USERNAME
vhaxxxxxxx
>W $ROLES
%All,%Developer
```

If you do *not* have one of the %All or %Manager roles, you *must* contact the system administrator for assistance.



**NOTE:** After successfully installing HWSC Patch XOBW\*1.0\*4, the elevated privileges are no longer necessary and should be removed.

## 2.4.3 cacheexport.xsd File Permissions (System Administrator)

Your site may already have the file permissions to an existing cacheexport.xsd file, which is used to parse XML files. To prevent file access errors (ERROR #6301) on the database server, the system administrator *must* open access to the file cacheexport.xsd, as well as the directory containing it. Do the following:

1. Navigate to the Caché install directory location for this Caché system.
2. Locate the file **cacheexport.xsd**, typically in the “bin” subdirectory.
3. Open up at least read access to everybody (world) to the directory containing **cacheexport.xsd**.
4. Open up at least read access to everybody (world) to the **cacheexport.xsd** file itself.

## 2.5 Platform Installation and Preparation

It is *recommended* that sites take the following approach to installing HealtheVet Web Services Client (HWSC) Patch XOBW\*1.0\*4:

1. Obtain the HWSC Patch XOBW\*1.0\*4 documentation.
2. Obtain the HWSC Patch XOBW\*1.0\*4 from the Patch module on FORUM or through normal procedures.
3. Install the software into a Test account.
4. Install the software into a Production system.

The following minimum software tools are required on your VistA Server in order to install and use the HWSC software:

- VistA account running on InterSystems' Caché for Linux, NT or OpenVMS.
- VistA accounts *must* contain the fully patched versions of the following packages:
  - HWSC 1.0
  - Kernel 8.0
  - Kernel Toolkit 7.3
  - MailMan 8.0
  - VA FileMan 22.0 (or higher)



**NOTE:** These software packages *must* be properly installed and fully patched prior to installing HWSC Patch XOBW\*1.0\*4. Patches *must* be installed in published sequence. You can obtain all released VistA patches (including patch description and installation instructions), from the Patch module on FORUM or through normal procedures.

The HWSC Patch XOBW\*1.0\*4 patch can be installed with users on the system, since the installation only affects the HWSC options; however, it is *recommended* that it be installed during *non-peak* hours to minimize potential disruption to users. Installation of the patch itself should take approximately 5 minutes; however, the configuration process will take longer.

## 2.6 Obtain and Extract Distribution Files

### 2.6.1 Software

The HWSC Patch XOBW\*1.0\*4 software distribution is contained in a KIDS PackMan message.

The KIDS PackMan message can be obtained from the Patch module on FORUM or through normal procedures.

Use the Kernel Installation & Distribution System (KIDS) to install the HWSC Patch XOBW\*1.0\*4 software.

## 2.6.2 Documentation

Documentation for HealtheVet Web Services Client is available on the VA Software Document Library (VDL) at: <http://www.va.gov/vdl/application.asp?appid=180>

VistA documentation and software can also be downloaded from the Product Support (PS) Anonymous Directories via Secure File Transfer Protocol (SFTP).

**Table 2: HWSC Documentation**

File Name	FTP Mode	Description
xobw_1_0_p4_ig.pdf	Binary	HWSC 1.0 Installation, Back-out, and Rollback Guide
xobw_1_0_p4_scg.pdf	Binary	HWSC 1.0 Security Configuration Guide
xobw_1_0_dg.pdf	Binary	HWSC 1.0 Developer's Guide
xobw_1_0_sg.pdf	Binary	HWSC 1.0 Systems Management Guide

## 2.7 Installation Scripts

There are no installation scripts for HWSC Patch XOBW\*1.0\*4.

## 2.8 Cron Scripts

There are no cron scripts for the HWSC Patch XOBW\*1.0\*4.

# 3 Installation Procedure

## 3.1 Patch Installation Instructions

This is a standard VistA patch installation. Use the Kernel Installation & Distribution System (KIDS) to install the HealtheVet Web Services Client (HWSC) Patch XOBW\*1.0\*4 software.



**REF:** Details regarding imported files, options, protocols, etc. can be found in the [HWSC 1.0 Systems Management Guide](#).

For VistA sites with a cluster of back-end database server nodes and front-end application server nodes, this patch should only be installed on the database server. The patch will do the following:

1. Update routines that will be available on all nodes.
2. Update the class xobw.WebServiceProxyFactory, which will be available on all nodes.
3. Update the class xobw.WebServer, which will be available on all nodes.
4. Create the Secure Socket Layer/Transport Layer Security (SSL/TLS) configuration “encrypt\_only”. Visible only on the installed node. You need to make it available on all nodes in your cluster, see the “[Post-Installation Instructions \(System Administrator\)](#)” section.

## 3.2 Load and Install Distribution

On configurations with a back-end database server and front-end application servers/commodity boxes, perform the following procedure:

1. Log onto the database server.
2. Choose the PackMan message containing this patch.
3. Choose the INSTALL/CHECK MESSAGE PackMan option.
4. From the Kernel Installation and Distribution System Menu, select the Installation Menu. From this menu, you may elect to use the following options. When prompted for the INSTALL NAME enter the patch name XOBW\*1.0\*4:
  - a. **Backup a Transport Global**—This option creates a backup message of any routines exported with this patch. It does not back up any other changes, such as DDs or templates.
  - b. **Compare Transport Global to Current System**—This option allows you to view all changes that will be made when this patch is installed. It compares all components of this patch (e.g., routines, DDs, templates, etc.).
  - c. **Verify Checksums in Transport Global**—This option allows you to ensure the integrity of the routines that are in the transport global.
5. From the Installation Menu, select the Install Package(s) option. When prompted for the INSTALL NAME, enter XOBW\*1.0\*4.
6. At the “Want KIDS to INHIBIT LOGONs during the install? NO//” prompt, enter **NO**.
7. At the “Want to DISABLE Scheduled Options, Menu Options, and Protocols? NO//” prompt, enter **NO**.
8. If prompted to “Want KIDS to Rebuild Menu Trees Upon Completion of Install? NO//”, enter **NO**.
9. Enter the Device you want to print the Install messages. For example:  

```
DEVICE: HOME// ;P-DEC NETWORK
```

Enter a “^” to abort the install.



**NOTE:** Do not queue the install, as the TaskMan process may not have the necessary privileges to perform the installation.



**NOTE:** Installers with a **Captive User** account will see a warning that the SSL/TLS configuration could *not* be completed and will need to coordinate with their system administrator to complete it as described in the “[Post-Installation Instructions \(System Administrator\)](#)” section.

## 3.3 Post-Installation Instructions (System Administrator)

The Transport Layer Security (SSL/TLS) configuration *must* be installed on each of the nodes in the cluster.

The installer should coordinate with their respective system administration support group (e.g., Region Operation Center) to receive assistance in performing the complete installation as described below.

The system administrator should check that the SSL/TLS configuration has been installed in the node where HWSC Patch XOBW\*1.0\*4 was installed, which is a Back-end database node.

In general, the system administrator should check on all the nodes, front-end servers, and database servers that the SSL/TLS Configuration has been installed, using the following sections (in any order):

- [Create the “encrypt\\_only” SSL/TLS Configuration File.](#)
- [Verify the “encrypt\\_only” SSL Configuration File Exists.](#)

### 3.3.1 Create the “encrypt\_only” SSL/TLS Configuration File

A new SSL/TLS Configuration file, “encrypt\_only”, is installed if there is *not* already an existing “encrypt\_only” configuration file.

To create the “encrypt\_only” SSL/TLS configuration file, do the following:

1. Log onto a node in the cluster.
2. At the VistA programmer prompt, enter the following code:

**Figure 1: Post-Installation Instructions—Create the “encrypt\_only” SSL/TLS Configuration File**

```
>D SSLCONF^XOBWP004

o 'encrypt_only' SSL Config successfully installed
  Configuration Values
CAFile      :
CAPath      :
CRLFile     :
CertificateFile :
CipherList  : TLSv1:SSLv3:!ADH:!LOW:!EXP:@STRENGTH
Description : Patch XOBW*1*4
Enabled     : 1
PrivateKeyFile :
PrivateKeyPassword :
PrivateKeyType : 2
Protocols   : 2
Type        : 0
VerifyDepth : 9
VerifyPeer  : 0
```



**CAUTION:** If you see a “<PROTECT>” error (see Section [3.5.2](#)), you do *not* have the appropriate access requirements; see the “[Access Requirements—Privileges and Permissions Needed for the Installation](#)” section.



3. When successful, you will see the following message:

**Figure 2: Post-Installation Instructions—Confirmation of Successful Configuration File Creation**

```
o 'encrypt_only' SSL Config successfully installed
```

4. Repeat Steps 1 - 3 for each node in the cluster.

### 3.3.2 Verify the “encrypt\_only” SSL Configuration File Exists

To verify the “encrypt\_only” SSL Config exists on a node, do the following:

1. At the Vista programmer prompt, enter the following code:  
`D CHCKEXST^XOBWP004("encrypt_only")`
2. If the “encrypt\_only” SSL Config was successfully created, the configuration values are displayed, as shown in [Figure 3](#):

**Figure 3: Post-Installation Instructions—Verifying the “encrypt\_only” SSL Configuration File Exists: Successful**

```
>D CHCKEXST^XOBWP004("encrypt_only")

Configuration Values
CAFile           :
CAPath           :
CRLFile          :
CertificateFile  :
CipherList       : TLSv1:SSLv3:!ADH:!LOW:!EXP:@STRENGTH
Description      : Patch XOBW*1*4
Enabled          : 1
PrivateKeyFile   :
PrivateKeyPassword :
PrivateKeyType   : 2
Protocols        : 2
Type             : 0
VerifyDepth      : 9
VerifyPeer       : 0
```



**CAUTION:** Make sure that you correctly spell the name of the configuration file, “encrypt\_only”. If the configuration does *not* exist, then repeat the “[Create the “encrypt\\_only” SSL/TLS Configuration File](#)” section; making sure to correctly spell the name of the configuration file.

If you see a “<PROTECT>” error (see Section [3.5.2](#)), you do *not* have the appropriate access requirements; see the “[Access Requirements—Privileges and Permissions Needed for the Installation](#)” section.

3. If the “encrypt\_only” SSL Config was *not* successfully created, an error message is displayed, as shown in [Figure 4](#):

**Figure 4: Post-Installation Instructions—Verifying the “encrypt\_only” SSL Configuration File Exists: Unsuccessful**

```
>D CHCKEXST^XOBWP004("encrypt_only1")  
  
>>>> 'encrypt_only' SSL Config doesn't exist.
```

## 3.4 Sample KIDS Installation

[Figure 5](#) is a sample HWSC Patch XOBW\*1.0\*4 install on a VMS system:

**Figure 5: Sample HWSC Patch XOBW\*1.0\*4 Installation on a VMS System**

```
1      Load a Distribution
2      Verify Checksums in Transport Global
3      Print Transport Global
4      Compare Transport Global to Current System
5      Backup a Transport Global
6      Install Package(s)
      Restart Install of Package(s)
      Unload a Distribution
Select Installation <TEST ACCOUNT> Option: 6 <Enter> Install Package(s)
Select INSTALL NAME: XOBW*1.0*4 <Enter> Loaded from Distribution 7/8/16@11:28:50
=> XOBW*1*4 TEST v7

This Distribution was loaded on Jul 08, 2016@11:28:50 with header of
XOBW*1*4 TEST v7
It consisted of the following Install(s):
XOBW*1.0*4
Checking Install for Package XOBW*1.0*4
Will first run the Environment Check Routine, XOBWP004

Install Questions for XOBW*1.0*4

Want KIDS to INHIBIT LOGONs during the install? NO// <Enter>
Want to DISABLE Scheduled Options, Menu Options, and Protocols? NO// <Enter>

Enter the Device you want to print the Install messages.
You can queue the install by enter a 'Q' at the device prompt.
Enter a '^' to abort the install.

DEVICE: HOME// ;P-DEC <Enter> NETWORK

Install Started for XOBW*1.0*4 :
Jun 14, 2016@09:51:06

Build Distribution Date: Jun 14, 2016

Installing Routines:...
Jun 14, 2016@09:51:06

Running Post-Install Routine: POST^XOBWP004.
Load started on 06/14/2016 09:51:06
Loading file /srv/vista/oak/user/hfs/xobw4.xml as xml
Imported class: xobw.WebServiceProxyFactory
Compiling class xobw.WebServiceProxyFactory
Compiling routine xobw.WebServiceProxyFactory.1
Load finished successfully.

o Support classes imported successfully.

Load started on 06/14/2016 09:51:06
Loading file /srv/vista/oak/user/hfs/xobw4b.xml as xml
Imported class: xobw.WebServer, compiling 2 classes, using 2 worker jobs
Compiling class xobw.WebServer
Compiling class xobw.WebServicesAuthorized
Compiling table xobw.WebServicesAuthorized
Compiling table xobw.WebServer
Compiling routine xobw.WebServer.1
```

```
Compiling routine xobw.WebServicesAuthorized.1
Load finished successfully.

o Support classes imported successfully.

o 'encrypt_only' SSL Config successfully installed.

Description: Patch XOBW*1*4

Updating Routine file.....

Updating KIDS files.....

XOBW*1.0*4 Installed.
Jun 14, 2016@09:51:06

Not a production UCI

NO Install Message sent
```

## 3.5 Troubleshoot Installation Errors / Review Install File

Review the contents of the install file and verify that no errors occurred. If an error did occur, check the following troubleshooting items to see if any match the error encountered.

If installation of HWSC PATCH XOBW\*1.0\*4 fails, the *recommended* action is to:

1. Review the install logs.
2. Determine and address the cause of install failure.
3. Re-run the HWSC PATCH XOBW\*1.0\*4 installation.

The HWSC PATCH XOBW\*1.0\*4 installation can be re-run as many times as necessary until a successful installation is achieved.

Some common installation errors are listed below.

### 3.5.1 Caché Error 6301 cacheexport.xsd Document Could Not Be Opened

You may encounter a Caché 6301 error as shown in [Figure 6](#), specifically referring to “cacheexport.xsd”:

**Figure 6: Cache Error 6301 cacheexport.xsd: Primary Document Could Not Be Opened**

```
Error: ERROR #6301: SAX XML Parser Error: Line: 2 Offset: 125 An exception
occurred! Type:RuntimeException, Message:Warning: The primary document entity
could not be opened. Id=_$1$DISK:[CACHESYS.ISC1.BIN]cacheexport.xsd at line 0
offset 0
```

And/Or, an error referring to undeclared attributes and unknown elements could be displayed following a Caché 6301error, as shown in [Figure 7](#):

**Figure 7: Undeclared Attributes and Unknown Elements**

```
Line: 2 Offset: 125 An exception occurred! Type:RuntimeException, Message:Warning:
The primary document entity could not be opened.
Id=$1$DISK:[CACHESYS.ISC1.BIN]cacheexport.xsd at line 0 offset 0Line: 2 Offset: 125
Unknown element 'Export' while processing
$1$DISK:[CACHESYS.ISC1.MGR.TEMP]568337052XWMf1.XML at line 2 offset 125
Line: 2 Offset: 125 Attribute 'generator' is not declared for element 'Export'
while processing $1$DISK:[CACHESYS.ISC1.MGR.TEMP]568337052XWMf1.XML at line 2
offset 125
Line: 2 Offset: 125 Attribute 'version' is not declared for element 'Export' while
processing $1$DISK:[CACHESYS.ISC1.MGR.TEMP]568337052XWMf1.XML at line 2 offset 125
Line: 2 Offset: 125 Attribute 'zv' is not declared for element 'Export' while
processing $1$DISK:[CACHESYS.ISC1.MGR.TEMP]568337052XWMf1.XML at line 2 offset 125
Line: 2 Offset: 125 Attribute 'ts' is not declared for element 'Export' while
processing $1$DISK:[CACHESYS.ISC1.MGR.TEMP]568337052XWMf1.XML at line 2 offset 125
Line: 3 Offset: 32 Unknown element 'Class' while processing
$1$DISK:[CACHESYS.ISC1.MGR.TEMP]568337052XWMf1.XML at line 3 offset 32
```

To fix this issue, follow the instruction in the “[cacheexport.xsd File Permissions](#)” section.

### 3.5.2 Caché “<PROTECT>” Error

You may encounter a protection error during the HWSC PATCH XOBW\*1.0\*4 KIDS installation or during the creation and verification of the SSL/TLS Configuration as shown in [Figure 8](#) and [Figure 9](#):

**Figure 8: Cache “<PROTECT>” Error (1 of 2)**

```
>D SSLCONF^XOBWP004
. . .
<PROTECT>EXISTS+6^XOBWP004 */srv/vista/oak/cache/oakr0ta01/mgr/
```

Or:

**Figure 9: Cache “<PROTECT>” Error (2 of 2)**

```
>D CHCKEXST^XOBWP004("encrypt_only")
. . .
<PROTECT>EXISTS+6^XOBWP004 */srv/vista/oak/cache/oakr0ta01/mgr/
```

These errors indicate that you do not have the appropriate access requirements. For more information, see the “[Access Requirements—Privileges and Permissions Needed for the Installation](#)” section.

## 3.6 Database Creation

The HWSC Patch XOBW\*1.0\*4 installation does *not* create any databases. HWSC uses the existing VA FileMan database.

## **4 Implementation Procedure**

### **4.1 Database Tuning**

There are no special database tuning requirements for HWSC Patch XOBW\*1.0\*4.

### **4.2 Verify Installation**

To verify the installation, follow the procedures in the “[Verify the “encrypt\\_only” SSL Configuration File Exists](#)” section.

## **5 Back-Out Plan**

Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings.

In the case that a back-out of this release is required a patch needs to be created and deployed to all sites that have installed the original patch. In the case of an initial release this new patch would need to remove any existing data, remove Veterans Health Information Systems and Technology Architecture (VistA) files associated with the package and remove routines associated with this package. Contents of a back-out patch for future releases would be dependent on the functionality released at that time.

### **5.1 Back-Out Strategy**

The need for a back-out would be determined by all affected organizations. This would primarily include representatives from Veterans Health Administration (VHA) and Enterprise Program Management (EPMO). In the case of the initial release a back-out would include removal of data, files and routines. In the case of future patches and releases the back-out strategy would be dependent on the contents of the released functionality and could include restoration of file definitions, routines or data.

### **5.2 Back-Out Considerations**

Back-out considerations would include impact on production VistA end-users and impact on Wide Area Network.

#### **5.2.1 Load Testing**

Not applicable for HWSC.

#### **5.2.2 User Acceptance Testing**

HWSC User Acceptance Testing (UAT) is performed during VistA patch testing at test sites.

### **5.3 Back-Out Criteria**

The HWSC back-out criteria follow existing VistA back-out procedures.

### **5.4 Back-Out Risks**

The HWSC back-out risks are the same risks established with existing VistA back-out procedures.

### **5.5 Authority for Back-Out**

The authority for the need of back-out would reside with VHA and EPMO representatives.

### **5.6 Back-Out Procedure**

The HWSC Patch XOBW\*1.0\*4 installation does not affect any existing VistA applications. If there is a need to back out to the previous state, you can back up the one routine being modified using the KIDS Backup a Transport Global option [XPD BACKUP]. The ObjectScript classes and SSL/TLS Configuration would be returned to their previous state by the creation of a patch to replace the ObjectScript classes and remove the SSL/TLS Configuration.

## **6 Rollback Plan**

Rollback pertains to data.

HealtheVet Web Services Client (HWSC) Patch XOBW\*1.0\*4 does not export any data.

### **6.1 Rollback Considerations**

N/A. HWSC Patch XOBW\*1.0\*4 does not export any data.

### **6.2 Rollback Criteria**

N/A. HWSC Patch XOBW\*1.0\*4 does not export any data.

### **6.3 Rollback Risks**

N/A. HWSC Patch XOBW\*1.0\*4 does not export any data.

### **6.4 Authority for Rollback**

Rollback *can* be authorized by system administrators once a problem has been identified. Enterprise Program Management Office (EPMO) should be informed immediately via a MailMan message sent to:

VA OIT PD Infrastructure Dev. & Doc. <InfrastructureDevDoc@va.gov>

### **6.5 Rollback Procedure**

N/A. HWSC Patch XOBW\*1.0\*4 does not export any data.