HealtheVet Web Services Client (HWSC) 1.0

Deployment, Installation, Back-Out, and Rollback Guide (DIBR)

August 2020

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

Enterprise Program Management Office (EPMO)

Revision History

Date	Revision	Description	Author
08/18/2020	1.0	XOBW*1.0*6: • Initial document created for HWSC 1.0 • Update Title page, Revision History, and Footers	HWSC Developers REDACTED

Table of Contents

1 Introduction

As the Department of Veterans Affairs (VA) and VistA applications employ further use of web services, there is a need to move towards more modern, secure communications protocols.

The current SSL/TLS configurations utilize older, insecure protocols. This patch will introduce a new SSL/TLS Configuration which utilizes TLSv1.2. This new configuration will be named ‘encrypt_only_tlsv12’.

Since there is no current software using this SSL/TLS ‘encrypt_only_tlsv12’ configuration, so there is no impact to current functionality. The new SSL/TLS configuration enables the VistA routines to make use of a newer security protocol.

1.1 Purpose

The purpose of this document is to provide instructions for setting up the TLSv1.2 configuration in the Cache Management Portal.

2 Pre-installation and System Requirements

2.1 Coordinate with System Administrator

Installers of the HWSC Patch XOBW*1.0*6 *must* coordinate with their respective system administration support group (e.g., HBMC Health Systems team) to receive assistance in performing the complete installation.

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.

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

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).
- Possess access to the Cache Management Portal with the **%All** or **%Manager** role.
- 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 create the HWSC Patch XOBW*1.0*6 Secure Socket Layer/Transport Layer Security (SSL/TLS) Configuration:

- Caché System Administration Account Access

2.4.1 Caché System Administration Account Access

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 **$ROLES**. For example:

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

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

2.5 Platform Installation and Preparation

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 2017.1.3** on **Linux**.
- 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 configuring the TLSv1.2 setup in the Cache Management Portal. 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.

2.6 Obtain and Extract Distribution Files

2.6.1 Software

The HWSC Patch XOBW*1.0*6 is an informational patch only.

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).

2.7 Installation Scripts

There are no installation scripts for HWSC Patch XOBW*1.0*6.

2.8 Cron Scripts

There are no cron scripts for the HWSC Patch XOBW*1.0*6.

3 Installation Procedure

3.1 Patch Installation Instructions

The following steps *must* be completed by a Cache Systems Manager with the %Manager role.

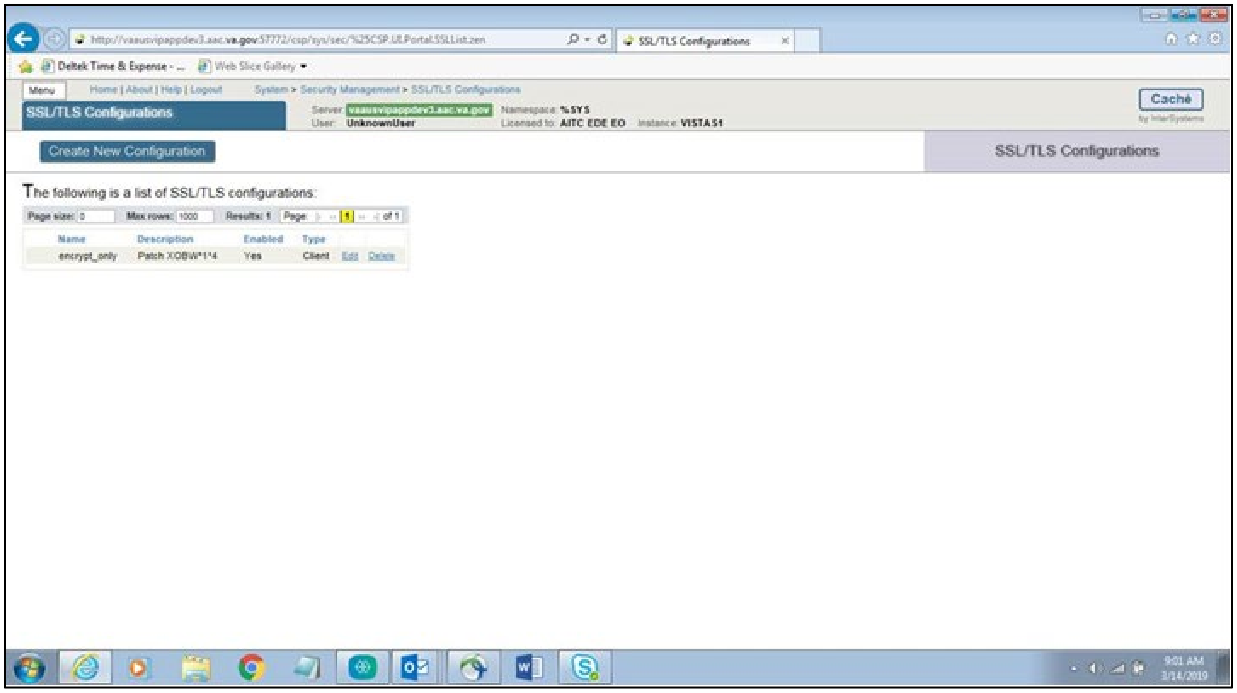
Patch XOBW*1.0*6 is an informational patch, and as such ***does not*** require a “true” installation of software. The System Administrator will set up the entire configuration via the Cache Management Portal.

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

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

The configuration list with patch XOBW*1.0*4, prior to Patch XOBW*1.0*6, is shown in Figure 1.

Figure 1: Current Configuration List from Patch XOBW*1.0*4



http://vaausvipappdev3.aac.va.gov:57772/csp/sys/sec/%25CSP.UI.Portal.SSLList.zen
SSL/TLS Configurations
Deltek Time & Expense - ...
Web Slice Gallery
Menu
Home | About | Help | Logout
System > Security Management > SSL/TLS Configurations
Caché
by InterSystems
Create New Configuration
9:01 AM
3/14/2019

SSL/TLS Configurations

Server: vaausvipappdev3.aac.va.gov   Namespace: %SYS
User: UnknownUser   Licensed to: AITC EDE EO   Instance VISTAS1

The following is a list of SSL/TLS configurations:

Page size: 0   Max rows: 1000   Results: 1   Page: 1 of 1

Name	Description	Enabled	Type		
encrypt_only	Patch XOBW*1*4	Yes	Client	Edit	Delete

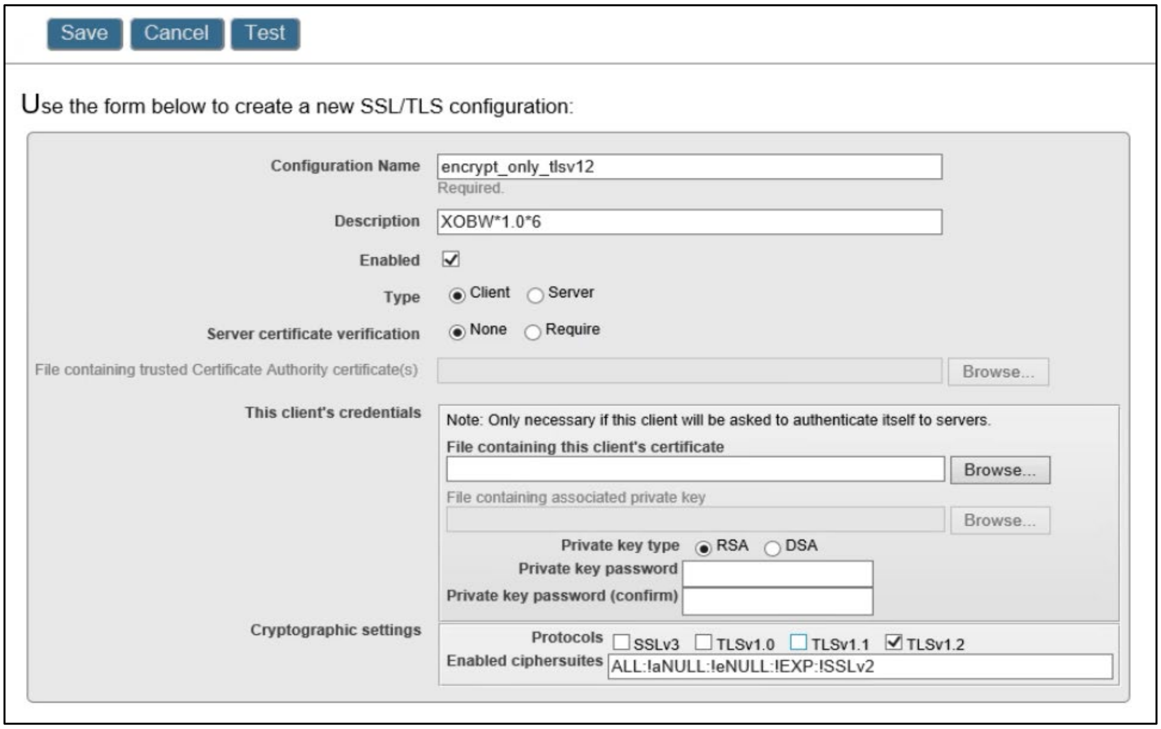
3.1.1 Cache System Management Portal

1. As a System Manager, open the Cache Management Portal.
2. Navigate to **System Administration**, **Security**, and then **SSL/TLS Configurations**.
3. Select **Create New Configuration** on the SSL/TLS Configurations web page.
4. Create the new configuration by setting the following information on the form.

Configuration Name:	encrypt_only_tlsv12
Description:	XOBW*1.0*6
Enabled:	Checked
Type:	Client
Peer certificate verification level:	None
Private key type:	RSA
Password:	Leave as is
Protocols:	
SSLv3:	Un-Checked
TLSv1.0:	Un-Checked
TLSv1.1:	Un-Checked
TLSv1.2:	Checked
Enabled ciphersuites:	ALL:!aNULL:!eNULL:!EXP:!SSLv2

The new configuration setup for Cache 2017 is shown in Figure 2.

Figure 2: Cache 2017 Configuration Setup



Use the form below to create a new SSL/TLS configuration:

Configuration Name: encrypt_only_tlsv12
Required.

Description: XOBW*1.0*6

Enabled: ☑

Type: ● Client ○ Server

Server certificate verification: ● None ○ Require

File containing trusted Certificate Authority certificate(s): Browse...

This client's credentials:
Note: Only necessary if this client will be asked to authenticate itself to servers.
File containing this client's certificate: Browse...
File containing associated private key: Browse...
Private key type: ● RSA ○ DSA
Private key password:
Private key password (confirm):

Cryptographic settings:
Protocols: □ SSLv3 □ TLSv1.0 □ TLSv1.1 ☑ TLSv1.2
Enabled ciphersuites: ALL:!aNULL:!eNULL:!EXP:!SSLv2

3.2 Post Installation Procedure

A post-installation procedure is not applicable for Patch XOBW*1.0*6, as this patch does not involve the installation of any software. The System Administrator is advised to use the Cache Management Portal to set up all the nodes. Patch XOBW*1.0*6 is an informational patch only, and as such does not require a "true" installation of software. The System Administrator will set up the entire configuration via the Cache Management Portal.

4 Implementation Procedure

4.1 Verify Installation

The installer should coordinate with their respective system administration support group (e.g., HBMC Health Systems team) to receive assistance in performing and verifying the complete installation via the Cache Management Portal.

5 Back-Out Plan

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

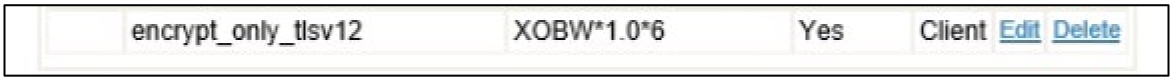
Since this is an informational patch only, please follow the instructions in the Back-Out Procedure to remove the new SSL/TLS Configuration using the Cache Management Portal.

5.1 Back-Out Procedure

The HWSC Patch XOBW*1.0*6 installation does not affect any existing VistA applications. If there is a need to back out to the previous state, please perform the steps below.

Prior to back-out, the configuration setup of Patch XOBW*1.0*6 appears as shown in Figure 3.

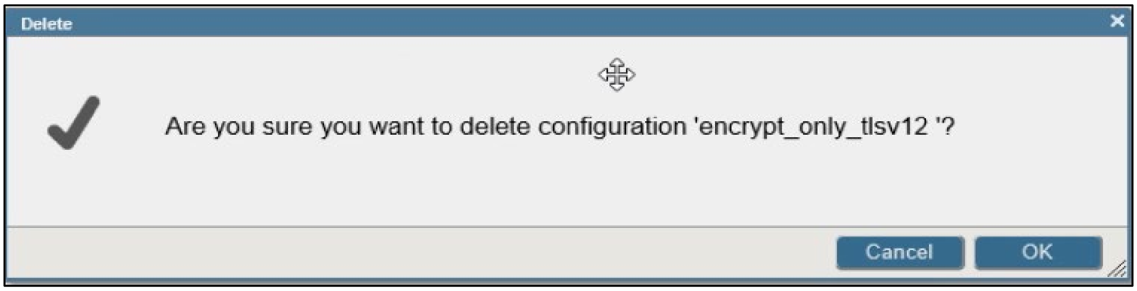
Figure 3: Cache TLS/SSL Configuration List



encrypt_only_tlsv12	XOBW*1.0*6	Yes	Client	Edit Delete

1. Select the "Delete" link for the 'ecrypt_only_tlsv12' configuration. A pop-up window appears as shown in Figure 4.

   Figure 4: Confirm Deletion of the Configuration

   Delete

   Are you sure you want to delete configuration 'encrypt_only_tlsv12 '?

2. Select Yes to confirm deletion of the configuration. The back-out procedure is now complete and the 'encrypt_only_tlsv12' configuration will no longer be visible in the SSL/TLS Configuration list.