HealtheVet Web Services Client (HWSC) 1.0
Patch XOBW*1.0*4

Release Notes

October 2016

Department of Veterans Affairs (VA)

Office of Information and Technology (OI&T)

Enterprise Program Management Office (EPMO)

Revision History

Date	Document Revision	Description	Author
10/20/2016	1.0	HealtheVet Web Services Client (HWSC), Patch XOBW*1.0*4 initial Release Notes document: • Installs a Caché SSL/TLS Configuration named “encrypt_only.” • Disables the flag that prevents the configuration and execution of TLS/SSL enabled HWSC web service clients, specifically for OpenVMS. • Disables verification of the remote server's host name. This is something that is enabled by default in Web browsers where a user is interacting with a browser; however, HWSC is a web service client with no user interaction. Also, RFC 2818 allows for disabling this verification when "the client has external information as to the expected identity of the server" to which HWSC applications can be configured to use.	HealtheVet Web Services Client (HWSC) Project Team

Table of Contents

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.

2 Purpose

These release notes cover the changes to the HealtheVet Web Services Client (HWSC) project with patch XOBW*1.0*4.

3 Audience

The audience for this document is Veterans Health Information Systems and Technology Architecture (VistA) application developers and Caché System Administrators.

4 HealtheVet Web Services Client Patch XOBW*1.0*4

Previous to this release, HWSC VistA applications were enabled to use Secure Socket Layer/Transport Layer Security (SSL/TLS) configurations to encrypt the connections; however, this worked on Linux systems, only. This feature was disabled in VistA applications on OpenVMS due to a problem with using SSL/TLS on OpenVMS systems. This is no longer the case. Thus, this feature has been enabled consistently on all VistA systems for both Linux and OpenVMS.

4.1 New Features and Functions

HWSC VistA applications can now enable SSL/TLS encryption to work in VistA applications on OpenVMS by referencing the “encrypt_only” SSL/TLS configuration or any new customized SSL/TLS configurations.

4.2 Enhancements and Modifications to Existing

Patch XOBW*1.0*4 makes the following enhancements to HWSC:

- Installs a Caché SSL/TLS Configuration named “encrypt_only” using SSL Version 3.
- Disables the flag that prevents the configuration and execution of TLS/SSL enabled HWSC Web service clients, specifically for OpenVMS.
- Disables verification of the remote server's host name. This is something that is enabled by default in Web browsers in which a user is interacting with a browser; however, HWSC is a Web service client with no user interaction. Also, RFC 2818 allows for disabling this verification when "the client has external information as to the expected identity of the server," which HWSC applications can be configured to use.

4.3 Known Issues

- The TLS/SSL configuration *must* be installed in all nodes of a VistA system, both front-end server nodes and database server nodes, as described in the *HealtheVet Web Services Client (HWSC) 1.0 Patch XOBW*1.0*4 Installation, Back-Out, and Rollback Guide*.
- The SSL/TLS configuration uses SSL version 3. The first application making use of SSL/TLS in HWSC is Master Patient Index (MPI), and the application needed to use SSL v 3 in order to connect to their PSIM remote server. In the future, all VA systems will be mandated to upgrade to higher versions of TLS and disable the use of older versions of SSL. When that happens, either a new XOBW patch will be issued to instruct system administrators to upgrade the SSL/TLS

configuration to a higher version of TLS, or control of these configurations will be given to the System Administrators' group, Health Systems Platform, so that they can do the SSL/TLS configuration upgrades directly.

We expect that any future changes to the SSL/TLS configuration will be coordinated with all the VistA application teams using SSL/TLS configurations, including HWSC-based applications and any other VistA applications that will have to use SSL/TLS encryption like HL7 applications. The coordination is important, so that the proper testing can be performed before the changes are made to the production systems.

- This is the first use of SSL/TLS security, and the first application that used it, MPI, used the SOAP messaging features of HWSC. The SSL/TLS security should work the same with applications using REST-based features as both styles use the same underlying security functionality of SSL/TLS. We expect that future applications using REST and SSL/TLS security will do the appropriate testing before they release their application.
- Also, another security feature that was not used in this release with MPI is the use of Certificate Authentication. We expect that future applications using Certificate Authentication will do the appropriate testing before they release their application.

4.4 Patch Numbering Scheme

There is an inconsistency in the numbering scheme used to describe this patch and should be noted. This patch contains changes to both M routines and Caché ObjectScript classes.

- The M routines correctly use the traditional patch numbering system on the second line as:

  ;;1.0;HwscWebServiceClient;**4**;September 13, 2010;Build 9

  Where the current version number is 1.0, the patch number is 4, and the build number is 9.

- The two Caché ObjectScript classes incorrectly use the following scheme in the class comment as:

  // HealtheVet Web Service Client v1 [**Build: 1.0.1.009**]

  Where "**Build: 1.0.1.009**" is interpreted as version 1.0, patch 1, and build 9. The number should correctly have been "**Build: 1.0.4.009**".

The most important number to consider is the current version, 1.0, which is correctly displayed in both the routines and the classes.

This patch numbering discrepancy will not break any functionality or affect any applications using this software.

5 Product Documentation

The following documents describe the new functionality introduced with this release:

- *HealtheVet Web Services Client (HWSC) 1.0 Patch XOBW*1.0*4 Installation, Back-Out, and Rollback Guide*
- *HealtheVet Web Services Client (HWSC): Patch XOBW*1.0*4 Security Configuration Guide*

HealtheVet Web Services Client (HWSC) user documentation can also be found on the VA Software Document Library (VDL) at: http://www.va.gov/vdl/application.asp?appid=180