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

Security Configuration Guide

February 2017

Department of Veterans Affairs (VA)

Office of Information and Technology (OI&T)

Enterprise Program Management Office (EPMO)

Revision History

Date	Version	Description	Author
02/15/2017	1.1	Corrected Figure 3 to reflect the SSLv3 check box is checked.	HealtheVet Web Services Client (HWSC) Project Team
10/20/2016	1.0	Initial document created for HealtheVet Web Services Client (HWSC) Patch XOBW*1.0*4.	HealtheVet Web Services Client (HWSC) Project Team

Table of Contents

List of Figures

Orientation

How to Use this Manual

The Security Configuration Guide defines the ordered, technical steps required to configure 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
ℹ	**NOTE / REF:** Used to inform the reader of general information including references to additional reading material.
⚠	**CAUTION / RECOMMENDATION / DISCLAIMER:** 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.

ℹ **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).

ℹ **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).

You can now use these **Back** and **Forward** command buttons in the Toolbar to navigate back and forth in the Word document when selecting hyperlinks within the document.

NOTE: This is a one-time setup and is automatically available in any other Word document once you install it on the Toolbar.

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*
- *HWSC 1.0 Patch XOBW*1.0 *4 Security Configuration Guide* (this manual)
- *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 Secure Socket Layer/Transport Layer Security (SSL/TLS) on OpenVMS systems.

1.1 Background

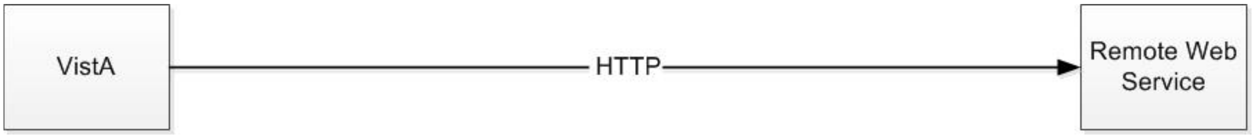
The HWSC software allows Veterans Health Information Systems and Technology Architecture (VistA) applications to make Hypertext Transfer Protocol (Secure) HTTP(S) connections from Veterans Health Information Systems and Technology Architecture (VistA) to remote HTTP(S) servers. HWSC uses a Caché library that makes HTTP or HTTPS requests.

On the initial deployment of HWSC (seven years ago), it was decided to disable the use of HTTPS secure connections from VistA due to a memory leak issue with VMS. The remote servers are capable of hosting their servers using HTTPS; however, due to this issue they are hosting them as HTTP.

1.1.1 Current Functionality

HWSC with SSL/TLS (HTTPS) works with other operating systems (i.e., Linux and Windows), but applications like Master Patient Index (MPI) have been forced to use HWSC *without* SSL/TLS (HTTPS). Figure 1 illustrates the current connection pathway using HTTP.

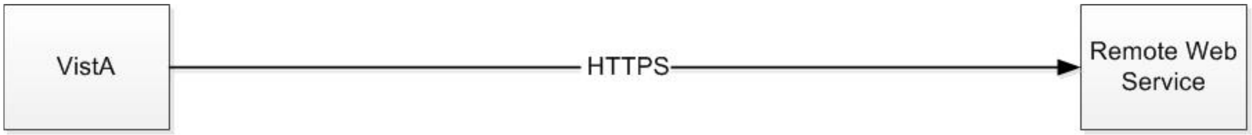
Figure 1: HWSC HTTP Connection—Current Functionality



1.1.2 Proposed Functionality

Enabling SSL/TLS on OpenVMS systems allows applications to use SSL/TLS consistently throughout the VA system. Figure 2 illustrates the proposed connection pathway using HTTPS.

Figure 2: HWSC and with HTTPS Connection—Proposed Functionality



1.2 Purpose

The purpose of this guide is to describe the configuration setup needed by VistA applications when using HWSC as a Web service client to secure its communication.

Since the proper configuration of a Web service client depends on the configuration of the corresponding remote Web service, minimal instructions are also provided for Web services hosted in a Java EE application server (WebLogic).

The configuration instructions are written for the following environments:

- Client-Side—Describes configuration instructions for HWSC-based VistA applications.
- Server-Side—Describes configuration instructions for typical systems currently in use at the VA (WebLogic Java EE application server).

It is *recommended* that VistA system administrators focus on the “Client-Side” sections and system administrators who manage Java EE applications (e.g., Oracle® WebLogic) focus on the “Server-Side” sections.

1.3 Transport Layer Security Concepts

The Transport Layer Security (TLS) protocol allows applications to communicate across a network in a secure manner that prevents eavesdropping, tampering, and message forgery. It can be used for securing (by encryption) communication between network clients and network servers; and for authentication of the network client, network server, or both.

TLS authentication can use public key infrastructure (PKI) certificates to identify network clients and network servers.

This configuration guide provides instructions on setting up encrypted connections with or without certificates for authenticating network clients. The instructions can be extended if an application opts to also authenticate the network server (mutual authentication). A configuration that does *not* use certificates for authentication is called an encryption-only configuration.

1.4 HTTP Basic Authentication

Authentication of network clients can also be achieved at the Network Application Layer, as is done in the HTTP protocol with HTTP Basic Authentication. This requires the use of a username and password credentials to be set up by the network server and its network clients. The use of HTTP Basic Authentication *must* encrypt its communication to protect the credentials. It is *recommended* that applications using HTTP Basic Authentication also configure their applications with encryption-only configuration.

This configuration guide provides instructions on setting up HTTP Basic Authentication for authenticating network clients.

1.5 Web Service Security

Although there is a standard Web Service Security (WS-Security) for Simple Object Access Protocol (SOAP) Web services, at the time that the HWSC software was developed and released, the implementation of WS-Security in Caché was *not* fully implemented. Also, HWSC is used for implementing Representational State Transfer (REST)-based Web service clients for which WS-Security is *not* used.

REF: For alternatives to WS-Security, see the “Configuration Recommendations” section.

1.6 VistA Environment

VistA applications are hosted in a Caché environment that may 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 may serve as both. For larger sites, the number of Front-End and Back-End nodes can vary.

1.7 SSL/TLS Configuration in VistA

The main configuration artifact in a Caché system is an SSL/TLS configuration that VistA applications need to reference in their code.

1.8 Configuration Recommendations

It is *recommended* that the following configurations be chosen, in order of complexity:

1. Encryption-Only (see the "Encryption-Only Setup" section) with HTTP Basic Authentication (see the "HTTP Basic Authentication Configuration" section).

   Or:

2. Client Certificate Authentication (see the "HTTP Basic Authentication Configuration" section).

2 Encryption-Only Setup

2.1 Server-Side

These instructions are written for Oracle® WebLogic (WL) 8.1 to 10.3.6 Application Server.

NOTE: Other versions should have a similar path to the configuration.

Set up a WL server to use default settings for /Secure Socket Layer (SSL):

1. In the WebLogic Admin Console, navigate to:

   Servers → <*myserver*> → Configuration-General

   The <*myserver*> name depends on your installation.

2. Check the **SSL Listen Port Enabled** option.
3. In the same page, enter a port number in the **SSL Listen Port** text field (e.g., 7002).
4. Save the changes.
5. Restart the server.
6. Ensure that the SSL listen port is now active.

2.2 Client-Side

These instructions are written for Caché 2014.1.3 M Server.

NOTE: Patch XOBW*1.0*4 installs an SSL/TLS configuration named “encrypt_only” in all nodes of a Caché system. You can use the Caché System Management Portal to view the SSL/TLS configuration in the node where the Management Portal is hosted.

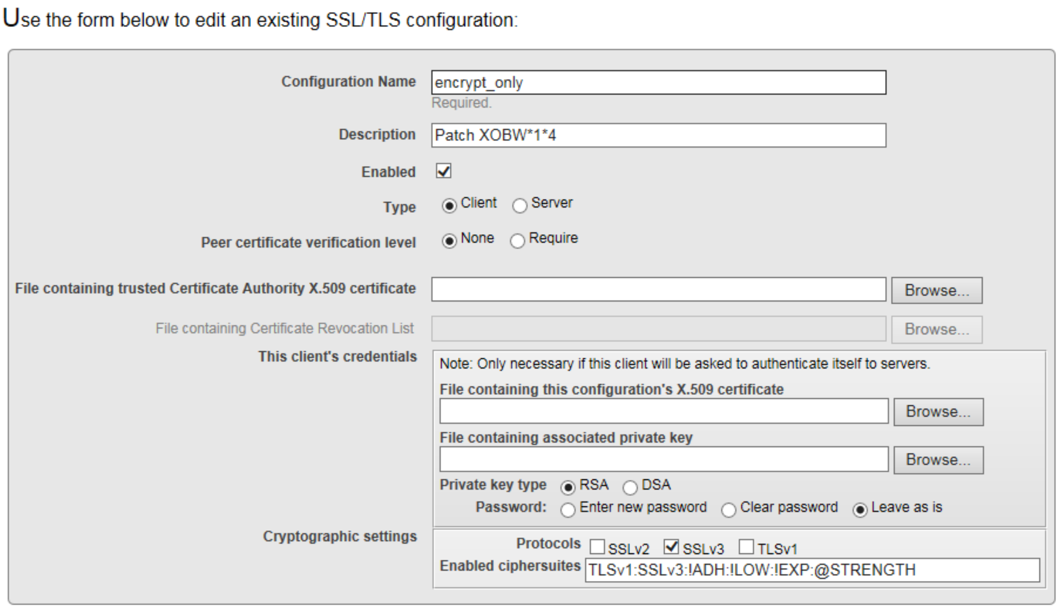
You can view and test the SSL/TLS configuration by using the Caché System Management Portal.

1. Locate the SSL/TLS configuration in the Caché System Management Portal.

   System Administration → Security → SSL/TLS Configuration

2. From the list of SSL/TLS configurations, select the “**encrypt_only**” choice by clicking the **edit** link.

Figure 3: Encryption-Only Setup—SSL/TLS configuration: Client-Side



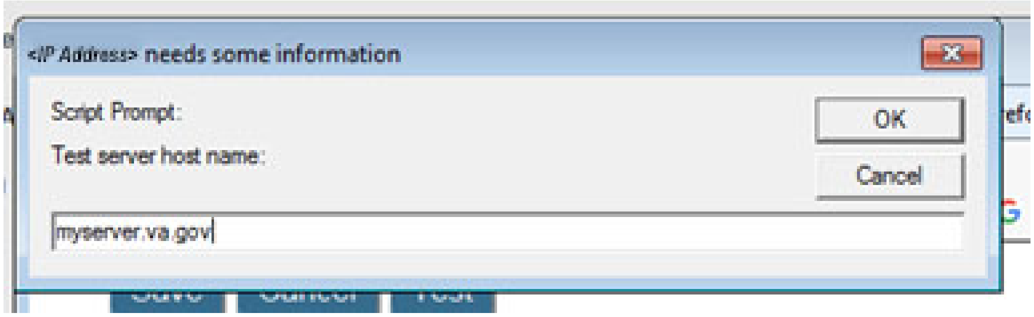
Use the form below to edit an existing SSL/TLS configuration:

Configuration Name	encrypt_only Required.
Description	Patch XOBW*1*4
Enabled	☑
Type	● Client ○ Server
Peer certificate verification level	● None ○ Require
File containing trusted Certificate Authority X.509 certificate	Browse...
File containing Certificate Revocation List	Browse...
This client's credentials	Note: Only necessary if this client will be asked to authenticate itself to servers. File containing this configuration's X.509 certificate Browse... File containing associated private key Browse... Private key type ● RSA ○ DSA Password: ○ Enter new password ○ Clear password ● Leave as is
Cryptographic settings	Protocols □ SSLv2 ☑ SSLv3 □ TLSv1 Enabled ciphersuites TLSv1:SSLv3:!ADH:!LOW:!EXP:@STRENGTH

3. Select the **Test** button to start testing the SSL/TLS configuration. You are prompted for the following information:

   - **Test server host name or IP address—**This is the server-side server configured in the "Server-Side" section. For example:

Figure 4: Encryption-Only Setup—SSL/TLS Configuration Test: Server Host Name or IP Address



<IP Address> needs some information

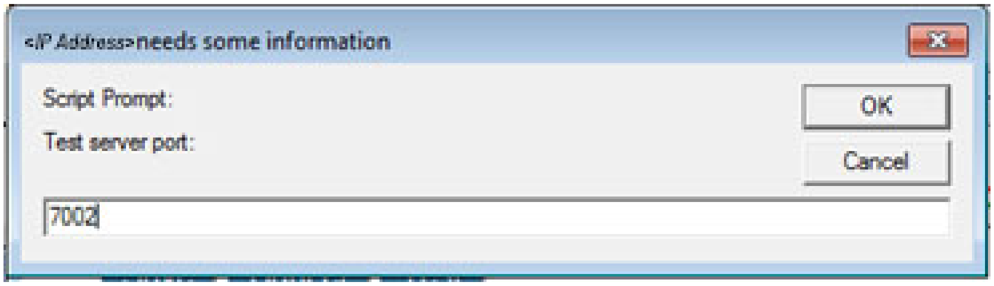
Script Prompt:

Test server host name:

myserver.va.gov

   - **Test server port—**This is the SSL port configured on the server-side server configured in the "Server-Side" section. For example:

Figure 5: Encryption-Only Setup—SSL/TLS Configuration Test: Server Port



<IP Address>needs some information

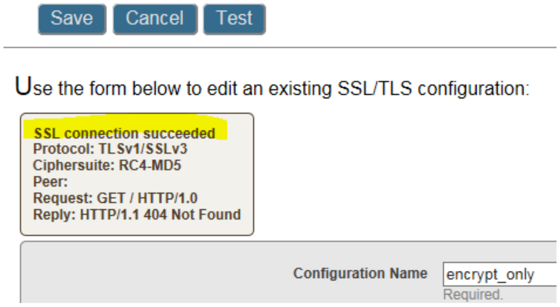
Script Prompt:

Test server port:

7002

4. You should see the following or similar information:

Figure 6: Encryption-Only Setup—SSL/TLS configuration Test: Sample Results



Use the form below to edit an existing SSL/TLS configuration:

SSL connection succeeded
Protocol: TLSv1/SSLv3
Ciphersuite: RC4-MD5
Peer:
Request: GET / HTTP/1.0
Reply: HTTP/1.1 404 Not Found

Configuration Name: encrypt_only
Required.

5. You are now ready, and can reference the “encrypt_only” SSL configuration in your WEB SERVER entry:

Figure 7: Encryption-Only Setup—SSL/TLS configuration Test: encrypt_only WEB SERVER Entry

```
SSL ENABLED: TRUE
SSL CONFIGURATION: encrypt_only
 SSL PORT: 7002
```

2.3 Potential Errors

You may encounter errors while testing the configuration. Some of the errors are listed below:

1. Ensure to enter the correct remote server host name or IP address.
2. Ensure to enter the correct remote server port number.
3. Ensure that your server and client systems are up to date with their use of SSL/TLS libraries.

ⓘ **NOTE:** In testing it was found that a Veterans Health Information Systems and Technology Architecture (VistA) system running on Linux could *not* establish an SSL session with an older WebLogic Application Server.

3 HTTP Basic Authentication Configuration

3.1 Server-Side

To enable the Web Services application to use Hypertext Transfer Protocol (HTTP) Basic Authentication you *must* have the following elements defined on the Java EE Application Server:

- A Security Realm User.
- A Security Realm Group.
- web.xml for the Web Services application.
- weblogic.xml for the Web Services application.

This allows a Veterans Health Information Systems and Technology Architecture (VistA) M Server Client to be registered in the JAVA EE Application Server hosting the Web Services application.

3.1.1 Security Realm Configuration

Create a user and group in the default security realm.

3.1.2 Create Security Realms Group

Create a security realms group that is given the role and privilege to invoke Web Services in the JAVA EE Application Server (e.g., **XOBW_Server_Proxies**).

3.1.2.1 Create Security Realms User

Create the user that is mapped to the username and password submitted by the client:

- USER**—**The name of the user to be mapped to the username in the security realm (e.g., **wsuser**)
- PASSWORD**—**The user's password to be mapped to the password in the security realm (e.g., **changeit**). The password *must* be kept secret and shared only to those clients allowed to invoke your Web Service.

NOTE: Coordinate with the person responsible for the VistA M Server Client—they need to know the values to be used as username and password in their implementation of HTTP Basic Authentication.

3.1.2.2 Assign User to the Security Realms Group

Assign the user created (e.g., **wsuser**) to the security realms group (e.g., **XOBW_Server_Proxies**).

3.1.3 web.xml File Configuration

Configure the Web Services application's web.xml file in order to use HTTP Basic Authentication.

3.1.3.1 Edit the Authentication Method

Edit the **<auth-method>** tag under the **<login-config>** tag in the web.xml file. For HTTP Basic Authentication, use **BASIC** as the authentication method, as shown in Figure 8:

Figure 8: Application Server—Edit the web.xml file to use BASIC authentication method

```
<login-config>
  <auth-method>BASIC</auth-method>
</login-config>
```

3.1.3.2 Define Web Services Security Roles and Constraints

Edit the following tags in the web.xml file:

- Edit the **<role-name>** tag under the **<auth-constraint>** tag under the <**security constraint>** tag to reference your Web Services security role.
- Edit the **<role-name>** tag under the **<security-role>** tag to reference your Web Services security role.

For example, use **XOBW_Server_Proxies** as the Web Services security role:

Figure 9: Application Server—Edit the web.xml file to define security roles and constraints

```
<security-constraint>
 . . .
  <web-resource-collection>
  . .
  </web-resource-collection>
  <auth-constraint>
    <description>These are the roles who have access</description>
    <role-name>XOBW_Server_Proxies</role-name>
  </auth-constraint>
 . . .
 </security-constraint
<security-role>
  <role-name>XOBW_Server_Proxies</role-name>
</security-role>
```

3.1.4 weblogic.xml File Configuration

Configure the application's weblogic.xml file in order to use HTTP Basic Authentication.

3.1.4.1 Define Web Services Security Roles to be Mapped to the Security Realm's Principal

Define any security roles that *must* be mapped to the Oracle WebLogic JAVA EE Application Server security realm's Principal. For example, use **XOBW_Server_Proxies** as the group (Principal):

Figure 10: Application Server—Defining security roles mapped to security realm's principal in the weblogic.xml file

```
<security-role-assignment>
  <role-name>XOBW_Server_Proxies</role-name>
  <principal-name>XOBW_Server_Proxies</principal-name>
</security-role-assignment>
```

3.2 Client-Side

To enable your VistA M Server Client to use HTTP Basic Authentication security, you *must* have an entry in the WEB SERVER file (#18.12)

3.2.1 Web Server File (#18.12) Configuration

Follow the instructions in Section 2 in the *HWSC Developer's Guide* when creating an entry in the WEB SERVER file (#18.12). The following fields *must* be defined to enable HTTP Basic Authentication security:

- STATUS: **ENABLED**
- LOGIN REQUIRED: **YES**
- USERNAME: <***wsuser***>
- PASSWORD: **<*Hidden*>**

NOTE: Username <*wsuser*> is just an example. You *must* obtain the values for the USERNAME and PASSWORD from the person responsible for the J2EE Application Server hosting the corresponding Web Service.

4 Client Certificate Authentication Configuration

4.1 Server-Side

To enable the Web Services application to use Client Certificate Authentication you *must* have the following elements defined on the remote Web server. For example a Java EE Application Server (JEE):

A user that corresponds to the CN of the Caché system.

In a JEE server this corresponds to:

- Security Realm User for the Caché system
- Security Realm Group
- Security Realm DefaultIdentityAsserter
- SSL Configuration to require client certificates
- web.xml file for the Web Services application
- weblogic.xml file for the Web Services application

This allows a Veterans Health Information Systems and Technology Architecture (VistA) M Server Client to be registered in the remote server hosting the Web Services application.

Additional details for setting up the server-side are described in the sections that follow.

4.1.1 Security Realm Configuration

Create a user and group in the default security realm.

4.1.1.1 Create Security Realms Group

Create a security realms group that is given the role and privilege to invoke Web Services in the JAVA EE Application Server (e.g., **XOBW_Server_Proxies**).

4.1.1.2 Create Security Realms User

Create the user that is mapped to the CN of the client certificate (e.g., **a1.fo-oakland.med.va.gov**)

- USER—The Domain Name Service (DNS) name of the host server (e.g., **a1.fo-oakland.med.va.gov)**
- PASSWORD—The password can be anything the user chooses, since it is never shared with anyone, not even the client user.

NOTE: Coordinate with the person responsible for the VistA Caché Server Client, they can give you their signed public key digital certificate for you to look at it, or you can ask them for the contents of the Common Name (CN) field.

4.1.1.3 Assign User to the Security Realms Group

Assign the user created (e.g., **a1.fo-oakland.med.va.gov**) to the security realms group (e.g., **XOBW_Server_Proxies**).

4.1.1.4 Edit Security Realm DefaultIdentityAsserter

Add and edit the security realm's DefaultIdentityAsserter properties with the following values:

- Types: **X.509**
- Default User Name Mapper: **Enable**
- Default User Name Mapper Attribute Type: **CN**
- Default User Name Mapper Attribute Delimiter: **(Leave Blank)**

4.1.2 SSL Client Behavior Configuration

Make sure that your JEE Application Server is already enabled for SSL connectivity. For Client Certificate Authentication to work, the **Two Way Client Cert Behavior** property *must* be set to "**Client Certs Requested And Enforced**," which is the most restrictive.

4.1.3 web.xml File Configuration

Configure the Web Services application's web.xml file in order to use Client Certificate Authentication.

4.1.4 Edit the Authentication Method

Edit the **<auth-method>** tag under the **<login-config>** tag in the web.xml file. For Client Certificate Authentication, use **BASIC** as the authentication method, as shown in Figure 11:

Figure 11: Application Server—Edit the web.xml file to use CLIENT-CERT authentication method

```
<login-config>
  <auth-method>CLIENT-CERT</auth-method>
</login-config>
```

4.1.4.1 Define Web Services Security Roles and Constraints

Edit the following tags in the web.xml file:

- Edit the **<role-name>** tag under the **<auth-constraint>** tag under the <**security constraint>** tag to reference your Web Services security role.
- Edit the **<role-name>** tag under the **<security-role>** tag to reference your Web Services security role.

For example, use **XOBW_Server_Proxies** as the Web Services security role:

Figure 12: Application Server—Edit the web.xml file to define security roles and constraints

```
<security-constraint>
  . . .
  <web-resource-collection>
  . .
  </web-resource-collection>
  <auth-constraint>
    <description>These are the roles who have access</description>
    <role-name>XOBW_Server_Proxies</role-name>
  </auth-constraint>
  . . .
 </security-constraint
<security-role>
  <role-name>XOBW_Server_Proxies</role-name>
</security-role>
```

4.1.5 weblogic.xml File Configuration

Configure the application's weblogic.xml file in order to use Client Certificate Authentication.

4.1.5.1 Define Web Services Security Roles to be Mapped to the Security Realm's Principal

Define any security roles that *must* be mapped to the Oracle WebLogic JAVA EE Application Server security realm's Principal. For example, use **XOBW_Server_Proxies** as the group (Principal):

Figure 13: Application Server—Defining security roles mapped to security realm's principal in the weblogic.xml file

```
<security-role-assignment>
  <role-name>XOBW_Server_Proxies</role-name>
  <principal-name>XOBW_Server_Proxies</principal-name>
</security-role-assignment>
```

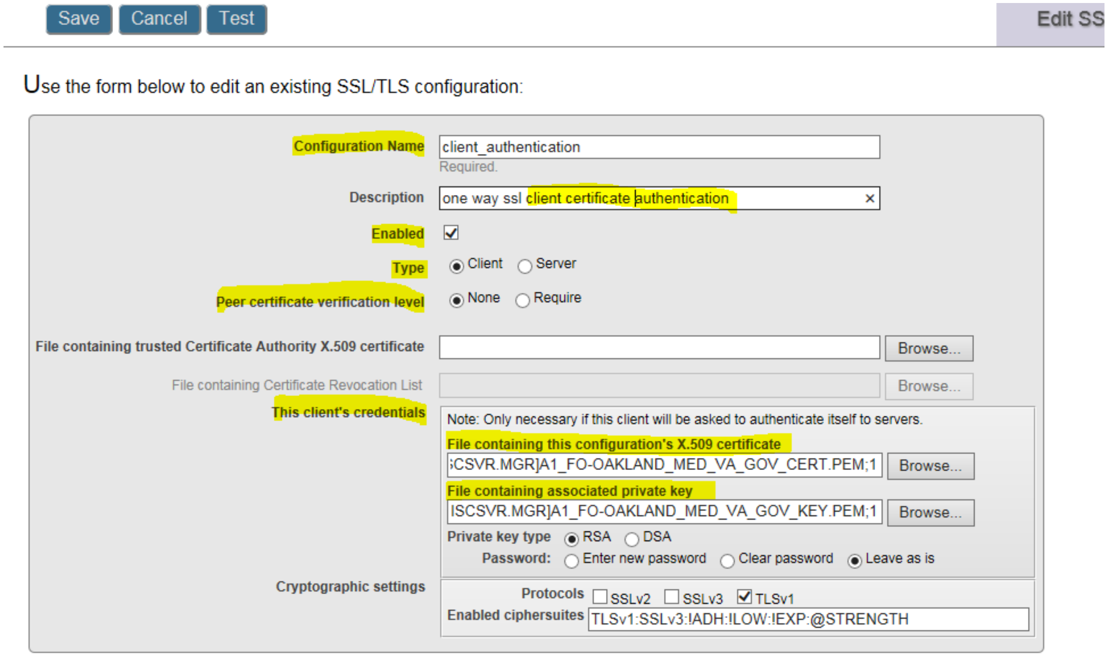
4.2 Client-Side

These instructions are written for Caché version 2014.1.3 or later.

4.2.1 SSL/TLS Configuration

Your VistA system administrator needs to create an SSL/TLS configuration in the Caché System Management Portal similar to the example in Figure 14. Also, in systems that have more than one node, the configuration needs to be created in all nodes.

Figure 14: Client Certificate Authentication Configuration—SSL/TLS Configuration



Use the form below to edit an existing SSL/TLS configuration:

Configuration Name: client_authentication
Required.

Description: one way ssl client certificate authentication

Enabled: ☑

Type: ● Client ○ Server

Peer certificate verification level: ● None ○ Require

File containing trusted Certificate Authority X.509 certificate:

File containing Certificate Revocation List:

This client's credentials:
Note: Only necessary if this client will be asked to authenticate itself to servers.
File containing this configuration's X.509 certificate: ;CSVR.MGR]A1_FO-OAKLAND_MED_VA_GOV_CERT.PEM;1
File containing associated private key: ISCSVR.MGR]A1_FO-OAKLAND_MED_VA_GOV_KEY.PEM;1
Private key type: ● RSA ○ DSA
Password: ○ Enter new password ○ Clear password ● Leave as is

Cryptographic settings:
Protocols: □ SSLv2 □ SSLv3 ☑ TLSv1
Enabled ciphersuites: TLSv1:SSLv3:!ADH:!LOW:!EXP:@STRENGTH

The SSL/TLS Configuration requires two files: The Caché system's identity certificate; and the corresponding Caché system's private key. Your Caché system is identified by its CN value in the certificate. Make note of it.

NOTE: Typical system certificates are issued for the purpose of identifying a server, your Caché system is used as the client; therefore, make sure that you request your certificate for the purpose of client as well.

4.2.2 VistA Client Private Key and Certificate

Create the necessary private key file and corresponding digital certificate from the VA's site:

1. To start the VA PKI SSL request process, browse to the following location:

   http://vaww.pki.va.gov/ssltls/

   REF: Be sure to read the "Request Process" section on that Web page.

2. Obtain a digital certificate for your VistA server and the corresponding private key; these files are used as the client certificate and the client private key respectively.
3. Make a note of the **CN** field value in the certificate. In this example, the CN is defined for a VistA server identified as follows:

   CN=**a1.fo-oakland.med.va.gov**

   NOTE: This name is used by the remote Web service server to identify a trusted system (user).

4. Place the two files in the Caché system.
5. Edit the SSL/TLS configuration file and browse to their location and select them.
6. Save your SSL/TLS configuration.

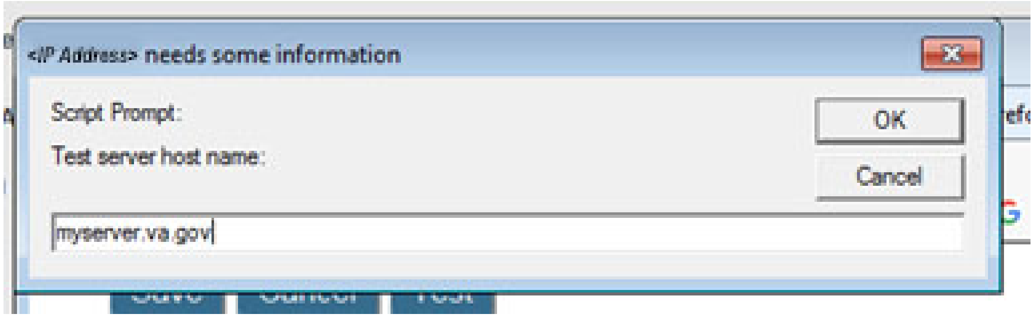
4.2.3 Testing the SSL/TLS Configuration

NOTE: To perform this test, you need to know the server-side's host name or IP address and the port listening for SSL/TLS connections.

1. Select the **Test** button to start testing the SSL/TLS configuration. You are prompted for the following information:

   - **Test server host name or IP address—**This is the server-side server configured in the "Server-Side" section. For example:

Figure 15: Client Certificate Authentication Configuration—Testing the SSL/TLS Configuration server host name or IP address



<IP Address> needs some information

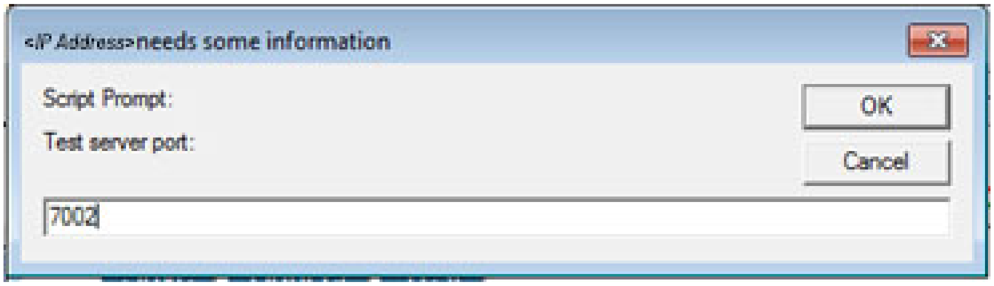
Script Prompt:

Test server host name:

myserver.va.gov

- **Test server port—**This is the SSL port configured on the server-side server configured in the "Server-Side" section. For example:

Figure 16: Client Certificate Authentication Configuration—Testing the SSL/TLS Configuration server port



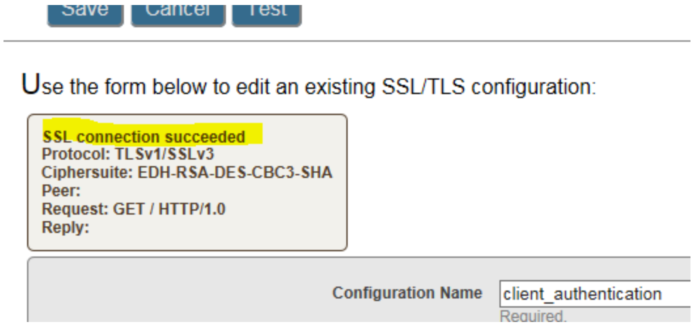
Script Prompt:

Test server port:

7002

2. You should see the following similar information:

Figure 17: Client Certificate Authentication Configuration—Sample Results



Use the form below to edit an existing SSL/TLS configuration:

```
SSL connection succeeded
Protocol: TLSv1/SSLv3
Ciphersuite: EDH-RSA-DES-CBC3-SHA
Peer:
Request: GET / HTTP/1.0
Reply:
```

Configuration Name: client_authentication

Required.

3. You are now ready, and can reference the "client_authentication" SSL/TLS configuration in your WEB SERVER entry.

To enable your VistA M Server Client to use Client Certificate Authentication security, you *must* follow the instructions in Section 3 in the *HWSC System Management Guide*. Also, define the configuration elements via an entry in the WEB SERVER file (#18.12) with values for the following fields:

- SSL ENABLED: **TRUE**
- SSL CONFIGURATION: SSL/TLS configuration (e.g., **client_authentication**).
- SSL PORT: Server's SSL/TLS port number (e.g., **7002**).