**VistA Patch Display Page: 1**

**=============================================================================**

**Run Date: MAR 13, 2019 Designation: XOBW\*1\*5 TEST v**

**Package : WEB SERVICES CLIENT Priority : MANDATORY**

**Version : 1 Status : UNDER DEVELOPMENT**

**=============================================================================**

**Associated patches: (v)XOBW\*1\*0 <<= must be installed BEFORE `XOBW\*1\*5'**

**Subject: TLS v1 CONFIGURATION**

**Category: INFORMATIONAL**

**Description:**

**===========**

**XOBW\*1\*5**

**As the VA and VistA applications makes additional usage of web services**

**there is a need to move towards more modern secure communications**

**protocols.**

**There currently exists a SSL/TLS configuration by the name of**

**'encrypt\_only', that is defined for the SSLv3 Protocol only.**

**This patch is designed to introduce the addition of a new TLS v1**

**CONFIGURATION by the name of 'encrypt\_only\_tlsv1'. This new configuration**

**will be defined for TLSv1 (Cache 2014) / TLSv1.2 (Cache 2017).**

**Instructions:**

**============**

**The following tasks must be completed by a Cache Systems Manager with the**

**%Manager ROLE.**

**Cache 2014:**

**1. As a System Manager open the Cache Management Portal**

**2. Navigate to System Administration -> Security -> SSL/TLS**

**Configurations**

**3. Select the "Create New Configuration" button on the SSL/TLS**

**Configurations web page.**

**4. Create the new configuration; setting the following information into**

**the form.**

**a. Configuration Name: encrypt\_only\_tlsv1**

**b. Description: encrypt\_only\_tlsv1**

**c. Enabled: Checked**

**d. Type: Client**

**e. Peer certificate verification level: None**

**f. Private key type: RSA**

**g. Password: Leave as is**

**h. Protocols:**

**A. SSLv2: Un-Checked**

**B. SSLv3: Un-Checked**

**C. TLSv1: Checked**

**i. Enabled ciphersuites: TLSv1:SSLv3:!ADH:!LOW:!EXP:@STRENGTH**

**Cache 2017:**

**1. As a System Manager open the Cache Management Portal**

**2. Navigate to System Administration -> Security -> SSL/TLS**

**Configurations**

**3. Select the "Create New Configuration" button on in the SSL/TLS**

**Configurations web page.**

**4. Create the new configuration; setting the following information into**

**the form.**

**a. Configuration Name: encrypt\_only\_tlsv1**

**b. Description: encrypt\_only\_tlsv1**

**c. Enabled: Checked**

**d. Type: Client**

**e. Peer certificate verification level: None**

**f. Private key type: RSA**

**g. Password: Leave as is**

**h. Protocols:**

**A. SSLv3: Un-Checked**

**B. TLSv1.0: Un-Checked**

**B. TLSv1.1: Un-Checked**

**C. TLSv1.2: Checked**

**i. Enabled ciphersuites: ALL:!aNULL:!eNULL:!EXP:!SSLv2**

**Note: The TLS/SSL configuration must be installed in all nodes, both**

**front-end server nodes and database server nodes. See Post-Installation**

**section.**

**Patch Components:**

**-----------------**

**Files & Fields Associated:**

**File Name (Number) Field Name (Number) New/Modified/Deleted**

**------------------ ------------------- --------------------**

**N/A**

**Forms Associated:**

**Form Name File # New/Modified/Deleted**

**--------- ------ --------------------**

**N/A**

**Mail Groups Associated:**

**Mail Group Name New/Modified/Deleted**

**--------------- --------------------**

**N/A**

**Options Associated:**

**Option Name Type New/Modified/Deleted**

**----------- ---- --------------------**

**N/A**

**Protocols Associated:**

**Protocol Name New/Modified/Deleted**

**------------- --------------------**

**N/A**

**Security Keys Associated:**

**Security Key Name**

**-----------------**

**N/A**

**Templates Associated:**

**Template Name Type File Name (Number) New/Modified/Deleted**

**------------- ---- ------------------ --------------------**

**N/A**

**Additional Information:**

**TLS/SSL Configurations:**

**-----------------------**

**Configuration name: encrypt\_only\_tlsv1**

**New Service Requests (NSRs):**

**----------------------------**

**N/A**

**Patient Safety Issues (PSIs):**

**-----------------------------**

**N/A**

**Test Sites:**

**----------**

**TENNESSEE VALLEY HCS**

**VA HEARTLAND - WEST**

**Documentation Retrieval Instructions:**

**------------------------------------**

**Software and Documentation Retrieval Instructions:**

**----------------------------------------------------**

**Documentation describing the new functionality introduced by this patch**

**is available.**

**The preferred method is to retrieve files from download.vista.med.va.gov.**

**This transmits the files from the first available server. Sites may**

**also elect to retrieve files directly from a specific server.**

**Sites may retrieve the software and/or documentation directly using**

**Secure File Transfer Protocol (SFTP) from the ANONYMOUS.SOFTWARE directory**

**at the following OI Field Offices:**

**Albany: fo-albany.med.va.gov**

**Hines: fo-hines.med.va.gov**

**Salt Lake City: fo-slc.med.va.gov**

**Host File:**

**----------**

**There is no host file in this release.**

**Documentation:**

**--------------**

**Title File Name FTP Mode**

**----------------------------------------------------------------------**

**Patch XOBW\*1.0\*5 Installation Guide xobw\_1\_0\_p5\_ig.pdf Binary**

**Blood Bank Team Coordination**

**============================**

**Blood Bank Clearance:**

**EFFECT ON BLOOD BANK FUNCTIONAL REQUIREMENTS: Patch XOBW\*1\*5 contains**

**changes to a package referenced in ProPath standard titled: BBM Team**

**Review of VistA Patches. This patch does not alter or modify any VistA**

**Blood Bank software design safeguards or safety critical elements**

**functions.**

**RISK ANALYSIS: Changes made by patch XOBW\*1\*5 have no effect on Blood**

**Bank software functionality, therefore RISK is none.**

**Installation Instructions:**

**--------------------------**

**See The HealtheVet Web Services Client (HWSC): Patch XOBW\*1.0\*5**

**Installation Guide, xobw\_1\_0\_p5\_ig.pdf.**

**Routine Information:**

**====================**

**No routines included.**

**=============================================================================**

**User Information:**

**Entered By : ANWER,MOHAMED Date Entered : FEB 21,2019**

**Completed By: Date Completed:**

**Released By : Date Released :**

**=============================================================================**