Master Patient Index (MPI)

Patch MPIF*1.0*63

Installation, Back-Out, and Rollback Guide

November 2016

Department of Veterans Affairs

Office of Information and Technology (OI&T)

Revision History

Date	Revision	Description	Author
Nov 2016	1.0	Initial document created for MPIF Patch MPIF*1.0*63.	Identity Services Project/Master Veteran Index Team

Table of Contents

1. Introduction

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. It provides installation instructions for Patch MPIF*1.0*63, as managed through the Master Patient Index Patch project.

1.1. Purpose

The purpose of this Installation Guide is to provide an explanation of how to install patch MPIF*1.0*63 software and set up the secure Web Server and Services necessary for the Veterans Health Information Systems and Technology Architecture (VistA) -to- Master Veteran Index (MVI) interface. The intended audience for this document is the Information Resources Management Service (IRMS) staff.

1.2. Scope

MPIF*1.0*63 addresses the Web Application Security Assessment (WASA) findings related to the passing of Personal Identifiable Information (PII) through Hypertext Transport Protocol (HTTP) communication by moving to support Hypertext Transport Protocol **Secure** (HTTPS) communications to the Person Service Identity Management (PSIM) system. The VistA system implements the VistA HealtheVet Web Services Client (HWSC) framework through Simple Object Access Protocol (SOAP) Web Services when communicating with the PSIM system.

2. Pre-installation and System Requirements

ALERT: MPIF* patches should NOT be installed on legacy systems to avoid issues with the legacy systems ending up as Treating Facilities.

2.1. Platform Installation and Preparation

2.1.1. Pre-Post Installation Overview

The installation steps are outlined below:

1. Retrieve the VISTAWEBSERVICE.WSDL file.
2. Place the VISTAWEBSERVICE.WSDL file in the Default Directory for Host File System (HFS), as stated in the PRIMARY HFS DIRECTORY field (#320) in the KERNEL SYSTEM PARAMETERS file (#8989.3), which is usually the USER$:[TEMP] folder on the VistA server. If using an SFTP utility to place the VISTAWEBSERVICE.WSDL file, please ensure that you have selected ASCII mode for the transfer.

   

   ALERT: VistA Linux system users must ensure that the Web Services Description Language (WSDL) file copied/stored in the Default HFS Directory is in **uppercase** (Name and Extension). The environment check process will not find the VISTAWEBSERVICE.WSDL file if it is in lower or mixed case as Linux is a case sensitive operating system, causing the installation process to abort.

3. Confirm that XOBW*1.0*4 was installed and all the instructions for setup have been completed, specifically Sections 3.3. and 3.3.3. *Verify the "encrypt_only" SSL Configuration File Exists.*

   To perform this check you'll need to:

   - Coordinate with your site's respective system administration group (e.g. Region Operation Center) to receive assistance in performing the SSL Configuration verification check described as follows:
     - Ask the system administrator to check that the SSL/TLS configuration has been installed in all nodes.
     - Ask the system administrator (with a **Programmer Support** account) to perform the verification check, assuming they have one of the following roles (e.g. greater than **%Developer** role):
       - %All
       - %Manager

Example of determining Roles currently held:

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

To check if the "encrypt_only" SSL Configuration exists on that node, enter the following code at the programmer prompt:

```
>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
```

If you get something similar to the above displayed where Protocols is equal to '2' then you are good to go and can proceed with installing patch MPIF*1.0*63.

If you get the following, then you'll need to go back to the XOBW*1.0*4 patch instructions and complete the setup before proceeding with the installation of patch MPIF*1.0*63.

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

        >>>>  'encrypt_only' SSL Config doesn't exist.
```

ALERT: However, if you get an error resembling the following, then you'll need to contact your Cache System Administrator to request %Manager or %All roles or you could request that the Cache System Manager install this patch.

```
.S $NAMESPACE="%SYS" ;Change namespace, revert back upon "Q"
  ^
<PROTECT>EXISTS+6^XOBWP004 */srv/vista/isa/cache/isar2tsvr/mgr/
```

4. Install the MPIF*1.0*63 patch. For additional information, please refer to Section 3.1 Installing the MPIF*1.0*63 patch.

During the patch installation the environment check routine MPIFWSC checks for the existence of the WSDL file in the Kernel Default Directory. If it doesn't exist, the install will NOT be permitted.

The POST-INIT routine POST^MPIFWSC imports the WSDL file into the WEB SERVICE file (#18.02) and programmatically creates the WEB SERVER file (#18.12) entry to support the transfer of PII information using HTTPS communications to PSIM. In addition, the "TWO" file entry will be automatically created in the MPI ICN BUILD MANAGEMENT file (#984.8), which will allow determination of the communication protocol (HTTP or HTTPS) to use when communicating with PSIM.

2.1.2. Minimum Required Packages

This MPIF patch can only be run with a standard Massachusetts General Hospital Utility Multi-Programming System (MUMPS) operating system and requires the following Department of Veterans Affairs (VA) software packages.

Package	Minimum Version Needed
Master Patient Index VistA (MPIF)	1.0
VA FileMan	22.0
Kernel	8.0
Web Service Client (XOBW)	1.0

The above software must be installed for this patch to be installed and fully patched.

2.2. Download and Extract Files

2.2.1. Required Patches

Patches MPIF*1.0*61 and XOBW*1.0*4 must be installed prior to installation of MPIF*1.0*63.

2.2.2. Software Retrieval

The files for this patch can be obtained from the ANONYMOUS.SOFTWARE directory at one of the OI Field Offices. The preferred method is to SFTP the file from DOWNLOAD.VISTA.MED.VA.GOV, which will transmit the file from the first available server. Alternatively, sites may elect to retrieve the file from a specific OI Field Office.

Oi Field Office	Address	Directory
Albany	FO-ALBANY.MED.VA.GOV	anonymous.software
Hines	FO-HINES.MED.VA.GOV	anonymous.software
Salt Lake City	FO-SLC.MED.VA.GOV	anonymous.software

The following is a list of the files related to this patch that will need to be downloaded.

File Name	Contents	Retrieval (Format)
VISTAWEBSERVICE.WSDL	WSDL	ASCII
MPIF_1_63.PDF	Install Guide	Binary

2.3. Database Creation

N/A.

2.4. Installation Scripts

N/A.

2.5. Cron Scripts

N/A.

2.6. Access Requirements and Skills Needed for the Installation

2.6.1. Access Requirements—Privileges and Permissions

Installers *must* have the following privilege and permission in order to install the MPI Patch MPIF*1.0*63:

Programmer Access: DUZ(0)="@" is required for installing the Patch MPIF*1.0*63.

Privileged Cache Account Role: %Manager or %All is required to perform the SSL/TLS check step.

File Access: Required to move/copy the VISTAWEBSERVICE.WSDL file into the Default Directory on the system.

2.6.2. Skills

The installer needs to know how to do the following:

- Obtain VistA software from FORUM and Secure File Transfer Protocol (SFTP) download sites.
- Run a Kernel Installation & Distribution System (KIDS) installation.
- Use the VistA EVE menu.
- Navigate VMS/UNIX directories.
- Transfer files using Secure File Transfer Protocol (SFTP).
- Use Web Services Options.
- Interpret information in the VistA KERNEL error trap.

3. Installation Procedure

WARNING – INSTALLATION RESTRICTIONS: Do NOT use the Production Web Server account settings when prompted during installation of the MPIF*1.0*63 patch in your Test Account, as this may send test patient information to the production MVI and PSIM systems. *Please use the Test Web Server* account settings when prompted, as responses are required to complete installation of the patch on the system. Installation should not be queued and it should take no longer than 2 minutes to complete.

3.1. Installing Patch MPIF*1.0*63

The following are the step-by-step instructions for installing all components of VistA Patch MPIF*1.0*63.

1. Choose the PackMan message containing this patch.
2. Choose the INSTALL/CHECK MESSAGE PackMan option.

   The Environment Check routine will automatically execute to verify the availability of the WSDL file.

```
      MPIF*1.0*63
    Will first run the Environment Check Routine, MPIFWSC
```

   Error message displayed if WSDL file is not available:

```
      MPIF*1.0*63
    Will first run the Environment Check Routine, MPIFWSC


    **** WSDL file VISTAWEBSERVICE.WSDL not found in USER$:[TEMP].
         You will need that prior to install.

    MPIF*1.0*63 Build will not be installed
              Jun 02, 2016@10:40:52
```

   NOTE: *VISTAWEBSERVICE.WSDL must be available in the Default Directory of the HFS before installation can be continued.*

3. Confirm that XOBW*1.0*4 was installed and all the instructions for setup have been completed, specifically Sections 3.3. and 3.3.3. *Verify the "encrypt_only" SSL Configuration File Exists.*

   To perform this check you'll need to:

   - Coordinate with your site's respective system administration group (e.g. Region Operation Center) to receive assistance in performing the SSL Configuration verification check described as follows:
     - Ask the system administrator to check that the SSL/TLS configuration has been installed in all nodes.

- Ask the system administrator (with a **Programmer Support** account) to perform the verification check, assuming they have one of the following roles (e.g. greater than **%Developer** role):
  - %All
  - %Manager

  Example of determining Roles currently held:

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

To check if the "encrypt_only" SSL Configuration exists on that node, enter the following code at the programmer prompt:

```
>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            : 4
       Type                 : 0
       VerifyDepth          : 9
       VerifyPeer           : 0
```

If you get the above displayed then you are good to go and can proceed with installing patch MPIF*1.0*63.

If you get the following, then you'll need to go back to the XOBW*1.0*4 patch instructions and complete the setup before proceeding with the installation of patch MPIF*1.0*63.

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

However, if you get an error resembling the following, then you'll need to contact your Cache System Administrator to request %Manager or %All roles or you could request that the Cache System Manager install this patch.

```
.S $NAMESPACE="%SYS" ;Change namespace, revert back upon "Q"
  ^
<PROTECT>EXISTS+6^XOBWP004 */srv/vista/isa/cache/isar2tsvr/mgr/
```

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 enter the patch number (i.e. MPIF*1.0*63):
   a. Backup a Transport Global – This option will create a backup message of any routines exported with this patch. It will not backup any other changes such as DDs or templates.
   b. Compare Transport Global to Current System – This option will allow you to view all changes that will be made when this patch is installed. It compares all components of this patch (routines, DDs, templates, etc.).
   c. Verify Checksums in Transport Global – This option will allow you to ensure the integrity of the routines that are in the transport global.
5. Startup KIDS. Select the Kernel Installation and Distribution System Menu [XPD MAIN] option.

```
          Edits and Distribution ...
          Utilities ...
          Installation ...
          Patch Monitor Main Menu ...
```

6. Select the Installation option.

```
Select Kernel Installation & Distribution System Option:
Installation

   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
```

7. Install the package.

```
   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 Option: Install Package(s)
```

8. Enter the package name.

```
Select INSTALL NAME:    MPIF*1.0*63 <Enter> Loaded from Distribution
6/24/16@15:04:39
     => MPIF*1*63 TEST v2
```

```
This Distribution was loaded on Jun 24, 2016@15:04:39 with header of
   MPIF*1*63 TEST v2
   It consisted of the following Install(s):
    MPIF*1.0*63
Checking Install for Package MPIF*1.0*63
Will first run the Environment Check Routine, MPIFWSC
```

9. Answer the Install Questions. (**Required to continue**)

```
Install Questions for MPIF*1.0*63


Enter the PORT Number for the MPINEWPSIMEXECUTE web service:  (1-99999):
Enter the name of the server for MPINEWPSIMEXECUTE:
```

Production Account Settings:

Port Number: **8957**

Server Name: **ps-prd.aac.va.gov**

Test Account Settings:

Port Number: **999**

Server Name: **TEST.NOT.APPLICABLE**

ALERT: Do NOT use the Production Account Settings in your test account as this may send test patient information to the MVI and PSIM production systems.

ALERT: Test Account Settings are only provided so that users can test the installation of the patch in their Test Account prior to installing into Production.

10. Answer NO to not inhibit logons.

```
Want KIDS to INHIBIT LOGONs during the install? NO// NO
```

11. Answer NO to not disable scheduled, menu options and protocols.

```
Want to DISABLE Scheduled Options, Menu Options, and Protocols?
NO//NO
```

12. Enter the device name you want to print the install messages.

```
Enter the Device you want to print the Install messages.
You SHOULD NOT queue the installation.
Enter a '^' to abort the install.

DEVICE: HOME//

Install Started for MPIF*1.0*63 :
```

```
              Jun 24, 2016@15:09:43

Build Distribution Date: Jun 24, 2016

 Installing Routines:...
              Jun 24, 2016@15:09:43

 Installing PACKAGE COMPONENTS:

 Installing REMOTE PROCEDURE..
              Jun 24, 2016@15:09:43

 Running Post-Install Routine: POSTINIT^MPIFWSC.
Compilation started on 06/24/2016 15:09:44 with qualifiers 'dk'
Compiling class MPIPSIM.VistAWebServicePort
Compiling routine MPIPSIM.VistAWebServicePort.1
Compiling class MPIPSIM.VistAWebServicePort.execute
Compiling routine MPIPSIM.VistAWebServicePort.execute.1
Compilation finished successfully in 4.156s.

 o  WEB SERVICE 'MPI_PSIM_NEW EXECUTE' addition/update succeeded.

>>> MPI_PSIM_NEW EXECUTE entry added to WEB SERVICE file #18.02

>>> Adding TWO entry to the MPI ICN BUILD MANAGEMENT (#984.8) file
    <<<

 Updating Routine file......

 Updating KIDS files.......

 MPIF*1.0*63 Installed.
              Jun 24, 2016@15:09:47

Install Complete
```

Receiving the above message during install indicates the installation of MPIF*1.0*63 is complete.

13. Using FileMan (FM), confirm that the Web Service and Web Server entries were setup correctly.

```
>D P^DI

VA FileMan 22.0

Select OPTION: INQUIRE TO FILE ENTRIES

OUTPUT FROM WHAT FILE: WEB SERVER// <Enter> WEB SERVER
Select WEB SERVER NAME: MPI_PSIM_NEW EXECUTE
ANOTHER ONE: <Enter>
STANDARD CAPTIONED OUTPUT? Yes// <Enter> (Yes)
Include COMPUTED fields:  (N/Y/R/B): NO// <Enter> - No record
number (IEN), no Computes
```

```
NAME: MPI_PSIM_NEW EXECUTE
SERVER: ps-prd.aac.va.gov
  STATUS: ENABLED                       DEFAULT HTTP TIMEOUT: 30
LOGIN REQUIRED: YES
SSL ENABLED: TRUE
  SSL CONFIGURATION: encrypt_only       SSL PORT: 8957
WEB SERVICE: MPI_PSIM_NEW EXECUTE       STATUS: ENABLED
```

```
Select WEB SERVER NAME: <Enter>
Select OPTION: INQUIRE TO FILE ENTRIES
OUTPUT FROM WHAT FILE: WEB SERVER// <Enter> WEB SERVICE (3
entries)
Select WEB SERVICE NAME: MPI_PSIM_NEW EXECUTE
ANOTHER ONE: <Enter>
STANDARD CAPTIONED OUTPUT? Yes// <Enter> (Yes)
Include COMPUTED fields:  (N/Y/R/B): NO// <Enter> - No record
number (IEN), no Computed Fields
```

NOTE: *Check the WEB SERVICE listing to confirm that there is information for the WSDL. If there is no WSDL information for the entry then the patch did not install correctly and will need to be re-installed.*

```
NAME: MPI_PSIM_NEW EXECUTE              TYPE: SOAP
DATE REGISTERED: JUN 22, 2016@08:48:15
  PROXY CLASS NAME: MPIPSIM.VistAWebServicePort
CONTEXT ROOT: psim_webservice/VistAWebService
  AVAILABILITY RESOURCE: ?wsdl
 WSDL:   <?xml version="1.0" encoding="UTF-8"?> <definitions xmlns:tns="VISTA"
 xmlns:wsr="http://www.openuri.org/2002/10/soap/reliability/" xmlns:mime="http:/
/schemas.xmlsoap.org/wsdl/mime/"
 xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:http="http://schem
as.xmlsoap.org/wsdl/http/"
 xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:soap12enc="http
://www.w3.org/2003/05/soap-encoding"
 xmlns:conv="http://www.openuri.org/2002/04/wsdl/conversation/" xmlns:soap="http
://schemas.xmlsoap.org/wsdl/soap/"
 xmlns:s="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas.xmlsoap.org/ws
```

```
dl/" targetNamespace="VISTA">
     <message name="execute">
         <part xmlns:partns="http://www.w3.org/2001/XMLSchema" name="requestXML"
 type="partns:string">
         </part>
     </message>
     <message name="executeResponse">
         <part xmlns:partns="http://www.w3.org/2001/XMLSchema" name="responseXML
" type="partns:string">
         </part>
     </message>
     <portType name="VistAWebServicePort">
         <operation name="execute">
             <input message="tns:execute">
             </input>
             <output message="tns:executeResponse">
             </output>
         </operation>
     </portType>
     <binding type="tns:VistAWebServicePort" name="VistAWebServicePort">
         <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/ht
tp" />
         <operation name="execute">
             <soap:operation style="rpc" soapAction="" />
             <input>
                 <soap:body use="encoded" namespace="VISTA" encodingStyle="http:
//schemas.xmlsoap.org/soap/encoding/" />
             </input>
             <output>
                 <soap:body use="encoded" namespace="VISTA" encodingStyle="http:
//schemas.xmlsoap.org/soap/encoding/" />
             </output>
         </operation>
     </binding>
     <service name="VistAWebService">
         <port name="VistAWebServicePort" binding="tns:VistAWebServicePort">
             <soap:address location="http://ps-dev.commserv.healthevet.va.gov:81
10/psim_webservice/VistAWebService" />
         </port>
     </service> </definitions>
```

4. Post-Installation/Implementation Procedure

4.1. Web Server and Web Services Post-Installation Check

After successfully installing patch MPIF*1.0*63 in Production, which will setup the Web Server and Web Service entries, the user can test the communication by selecting the CK--Check Web Service Availability option as shown in the next two screens, as follows.

NOTE: *This is accomplished through the XOBW WEB SERVER MANAGER (Web Server Manager) menu option. Production accounts will most likely have significantly more Web Server entries than shown below.*

```
Web Server Manager            Jun 24, 2016@09:37:36          Page:    1 of    1
                        HWSC Web Server Manager
                       Version: 1.0     Build: 31

 ID    Web Server Name           IP Address or Domain Name:Port
 1    *MPI_PSIM_EXECUTE          address:port
 2    *MPI_PSIM_NEW EXECUTE      ps-prd.aac.va.gov:8957 (SSL)









          Legend:  *Enabled
AS  Add Server                          TS  (Test Server)
ES  Edit Server                         WS  Web Service Manager
DS  Delete Server                       CK  Check Web Service Availability
EP  Expand Entry                        LK  Lookup Key Manager
Select Action:Quit// CK <Enter> Check Web Service Availability
Select Web Server:  (1-4): 2...
```

```
Web Service Availability                                  Jun 24, 2016@09:37:37
Web Server:
 2    *MPI_PSIM_NEW EXECUTE          ps-prd.aac.va.gov:8957

  1 Unable to retrieve '?wsdl' for MPI_PSIM_NEW EXECUTE
   o HTTP Response Status Code: 401









          Enter ?? for more actions

    Actions
Select Action:Quit//
```

Figure 1. Production Account Display (Service Availability Check failed)

NOTE: *If you see the "HTTP Response Status Code: 401" that will indicate that the username and password have not been configured yet. MPI staff will update the username and password remotely once we have confirmed that the patch was successfully installed. Then Information Resource Management (IRM) will be asked to check the web service again and they should now see that the service is available.*

If IRM executes the ***Check Web Service Availability*** option above in their TEST account, they will see the following error as the TCP/IP address/Port account settings entered for the TEST account during patch installation do NOT actually point (nor should they) to a valid system to connect to.

```
Web Service Availability                                  Jun 24, 2016@09:37:37
Web Server:
 2    *MPI_PSIM_NEW EXECUTE          TEST.NOT.APPLICABLE:999

  1 Unable to retrieve '?wsdl' for MPI_PSIM_NEW EXECUTE
   o ERROR #6059: Unable to open TCP/IP socket to server TEST.NOT.APPLICABLE:999









          Enter ?? for more actions

    Actions
Select Action:Quit//
```

Figure 2. Test Account Display (Service Availability Check failed)

```
Web Service Availability      Jun 24, 2016@12:03:21          Page:    1 of    1
Web Server:
 2    *MPI_PSIM_EXECUTE          ps-prd.aac.va.gov:8957

  1  MPI_PSIM_NEW EXECUTE is available









          Enter ?? for more actions

    Actions
Select Action:Quit//
```

Figure 3. Service Availability Check Success

4.2. Monitoring Error Trap for Errors

After MPI has remotely configured and switched your site over to using the secure (SSL/TLS) connection, sites may see the following similar error in their error trap if the XOBW*1.0*4 patch was not completely installed on all nodes.

```
<ZSOAP>zInvokeClient+203^%SOAP.WebClient.###:##:##  ROU:NODEXXX    ####
```

Specific details of the error can be found in the XOBEOARR variable when researching the specifics of the error as shown below:

```
XOBEOARR("text",1)=ERROR #6085: Unable to write to socket with
SSL/TLS configuration 'enc
XOBEOARR("text",2)=rypt_only', error reported 'SSL/TLS configuration
'encrypt_only' is no
XOBEOARR("text",3)=t activated.'
```

If you are seeing errors similar to this, then SSL/TLS configuration that was supposed to occur during installation of patch XOBW*1.0*4 may not have been configured on one or more front-end or back-end nodes. The initial error above will indicate the current node the error occurred on (i.e., **NODEXXX**), but there could be other nodes where installation also did not occur.

From the XOBW*1.0*4 installation guide, the following command (assuming the user has the appropriate privileges) can be run on a specific node to see if SSL/TLS has been installed.

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

 >>>>  'encrypt_only' SSL Config doesn't exist.
```

Once confirmed that SSL/TLS has NOT been configured on the front-end and/or back-end node, the user can (again assuming they have the appropriate privileges) execute the following command to install SSL/TLS on that node:

```
>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
```

Additional information if needed on XOBW*1.0*4 can be found in the installation guide XOBW_1_0_P4_IG.(pdf/doc).

4.3. System Configuration

N/A.

4.4. Database Tuning

N/A.

5. Back-Out Procedure

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

The back-out procedure for Patch MPIF*1.0*63 is to restore the routines back to the previous state, using the back-up message created during installation. Communications will automatically revert to the existing HTTP communication link as before once the routine is restored.

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 the restoration of a routine. In the case of future patches and releases the back-out strategy would be dependent on the contents of the released.

5.2. Back-out Considerations

None. The system changes were minimal and the routine changes are used based upon a parameter that allows either the HTTP or HTTPS communication to be utilized. The parameter can easily be returned to allow HTTP communication.

5.2.1. Load Testing

N/A.

5.2.2. User Acceptance Testing

MPIF User Acceptance Testing (UAT) is performed in a near-production environment and verified by the Healthcare Identity Management team (HC IdM).

5.3. Back-out Criteria

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

5.4. Back-out Risks

The MPIF back-out risks are the same risks established with existing VistA back-out procedures. However, they are considered minimal as the software will continue to use the existing/original HTTP communication link.

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 MPIF back-out procedure would consist of restoring the original routine using the back-up message created during the patch installation.

6. Rollback Procedure

The MPIF*1.0*63 patch does not export any data so there is no rollback procedure required.

6.1. Rollback Considerations

N/A.

6.2. Rollback Criteria

N/A.

6.3. Rollback Risks

N/A.

6.4. Authority for Rollback

N/A.