Kernel 8.0; Patch XU*8.0*702

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

August 2020

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

Enterprise Program Management Office (EPMO)

Revision History

Documentation Revisions

Date	Revision	Description	Authors
08/11/2020	1.3	Updates: Section 4.8.2.3: • Added explanatory note in Step 2, following Figure 9. • Added explanatory note in Step 4, following Figure 11. **Kernel 8.0; Patch XU*8.0*702**	VistA Infrastructure (VI) Development Team
07/22/2020	1.2	Updates: • Section 4.5, 4.8.2.1, and 7.2.2: Updated references to the DLL to reflect the latest version, which is Version **8.0.702.3**. • Section 4.8.2, 4.8.2.3, Figure 8, Figure 10, Figure 11, and Figure 15: Updated the **.rdox** file configuration steps that replace the old method. This resolves a latency issue found in the old setup where in some circumstances the Visual Basic (VB) script would not trigger. • Verified document is Section 508 conformant. **Kernel 8.0; Patch XU*8.0*702**	VistA Infrastructure (VI) Development Team
04/09/2020	1.1	Updates based on new DLL file for Patch XU*8.0*702 that is being pushed through SCCM: • Section 4.3.1; Table 10: Removed DLL reference within ZIP file. The DLL is pushed by SCCM nationally and will be available within Software Center. The DLL is *not* being released as part of the ZIP file. • Section 4.5: Changed DLL version reference to **8.0.702.2**. • Section 4.8.2.1: Changed DLL version reference to **8.0.702.2**. Section 7.2.2; Figure 15: New screenshot of DLL properties window	VistA Infrastructure (VI) Development Team

Date	Revision	Description	Authors
		for DLL Version **8.0.702.2**, which was created on **03/26/2020**. **Kernel 8.0; Patch XU*8.0*702**	
03/23/2020	1.0	Final Patch XU*8.0*702 Deployment, Installation, Back-Out, and Rollback Guide (DIBRG) for release: • Document baseline release revision number 1.0. • Deleted prior development document revision history. • Removed VA Intranet site links for upload to the VA Software Document Library (VDL) Internet site. **Kernel 8.0; Patch XU*8.0*702**	VistA Infrastructure (VI) Development Team

Patch Revisions

For the current patch history related to this software, see the Patch Module on FORUM.

Table of Contents

List of Figures

List of Tables

Orientation

How to Use this Manual

This manual provides advice and instructions for deploying and installing the Veterans Health Information Systems and Technology Architecture (VistA) Kernel Patch XU*8.0*702.

Intended Audience

The intended audience of this manual is the following stakeholders:

- Enterprise Program Management Office (EPMO)—VistA legacy and other development teams.
- System Administrators—Personnel responsible for regional and local computer management and system security on VistA M Servers and client workstations.
- Information Security Officers (ISOs)—Personnel at VA sites responsible for system security.
- Product Support (PS).
- Area Managers.
- Automated Data Processing Application Coordinator (ADPACS).
- Chief Health Informatics Officer (CHIO).

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.

CAUTION: To protect the security of VistA systems, distribution of this software for use on any other computer system by VistA sites is prohibited. All requests for copies of this software for *non*-VistA use should be referred to the VistA site's local Office of Information Field Office (OIFO).

Documentation Disclaimer

This manual provides an overall explanation and functionality of Kernel Patch XU*8.0*702; 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 websites for a general orientation to VistA. For example, visit the Office of Information and Technology (OIT) VistA Development 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 / DISCLAIMER /SKIP THIS STEP / RECOMMENDATION:** 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).
- Conventions for displaying TEST data in this document are as follows:
  - The first three digits (prefix) of any Social Security Numbers (SSN) begin with either “**000**” or “**666**.”
  - Patient and user names are formatted as follows:
    - [Application Name]PATIENT,[N]
    - [Application Name]USER,[N]

Where “*Application Name*” is defined in the Approved Application Abbreviations document and “*N*” represents the first name as a number spelled out and incremented with each new entry.

For example, in Kernel (XU) test patient names would be documented as follows:

XUPATIENT,ONE; XUPATIENT,TWO; XUPATIENT,14, etc.

For example, in Kernel (XU) test user names would be documented as follows:

XUUSER,ONE; XUUSER,TWO; XUUSER,14, etc.

- “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 in **boldface** and highlighted in yellow (e.g., **<Enter>**).
- Emphasis within a dialogue box is in **boldface** and highlighted in blue (e.g., STANDARD LISTENER: RUNNING).
- Some software code reserved/key words are in **boldface** 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.

  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).

  NOTE: Other software code (e.g., Delphi/Pascal and Java) variable names and file/folder names can be written in lower or mixed case.

Documentation Navigation

This document uses Microsoft® Word's built-in navigation for internal hyperlinks. To add **Back** and **Forward** navigation buttons to your toolbar, do the following:

1. Right-click anywhere on the customizable Toolbar in Word 2010 (*not* the Ribbon section).
2. Select **Customize Quick Access Toolbar** from the secondary menu.
3. Press the drop-down arrow in the "Choose commands from:" box.
4. Select **All Commands** from the displayed list.
5. Scroll through the command list in the left column until you see the **Back** command (circle with arrow pointing left).
6. Select/Highlight the **Back** command and press **Add** to add it to your customized toolbar.
7. Scroll through the command list in the left column until you see the **Forward** command (circle with arrow pointing right).
8. Select/Highlight the **Forward** command and press **Add** to add it to your customized toolbar.
9. Press **OK**.

You can now use these **Back** and **Forward** command buttons in your Toolbar to navigate back and forth in your Word document when clicking on 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.

REF: For more information, see the *Kernel 8.0 and Kernel Toolkit 7.3 Technical Manual*.

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). You can use the **List File Attributes** [DILIST] option on the **Data Dictionary Utilities** [DI DDU] 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" chapter in the "File Management" section of 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 8.0—VistA M Server software
  - Remote Procedure Call (RPC) Broker 1.1—VistA Client/Server software
  - VA FileMan 22.2 data structures and terminology—VistA M Server software

- M programming language
- Microsoft® Windows environment
- Terminal emulator software:

  Micro Focus® Reflection (v16)
- Microsoft® Visual Basic Editor:

  Ability to import macros as described in Section 4.8.2, "Client Workstation Instructions—Micro Focus® Reflection (v16)."

DISCLAIMER: The installation and configuration steps described in this manual should be performed by regional or local system administrators who maintain enterprise client workstations, as it requires Administrative privileges.

The instructions in this manual are written and can be used to set up on an individual client workstation (Dynamic Link Library [DLL] and Visual Basic [VB] script); however, they are intended more for national (mass) deployment. These instructions are intended for regional or local system administrators to set up a "push" version of the Micro Focus® Reflection (v16) terminal emulator software to invoke 2-Factor Authentication (2FA). The configured Reflection terminal emulator software would then be distributed (pushed) throughout the enterprise using a custom System Center Configuration Manager (SCCM) script to push the 2FA-enabled Reflection software settings files and the DLL to all required client workstations.

References

For additional information with regard to Patch XU*8.0*702 project team, 2FA, PIV, and IAM Link My Account, consult the following:

- Reflection PIV Project SharePoint (VA Intranet internal project team collaboration site)
- PIV Enabled Vista SharePoint (VA Intranet site)
- Link My Account Summary Sheet (VA Intranet site)
- PIV Help.docx(VA Intranet site)
- *Patch XU*8.0*702 Deployment, Installation, Back-Out, and Rollback Guide (DIBRG)* (this manual)
- *Patch XU*8.0*702 Quick Reference Guide*
- *Patch XU*8.0*702 VistA-Reflection PIV 2-Factor Authentication Test Plan* (VA Intranet site)

Readers who wish to learn more about Kernel should consult the following:

- *Kernel Release Notes*
- *Kernel Patch XU*8.0*702 Deployment, Installation, Back-Out, and Rollback Guide* (this manual)
- *Kernel 8.0 and Kernel Toolkit 7.3 Systems Management Guide*
- *Kernel 8.0 and Kernel Toolkit 7.3 Developer's Guide*
- *Kernel 8.0 and Kernel Toolkit 7.3 Technical Manual*
- Kernel VA Intranet website.

  This site provides additional information, documentation links, archives of older documentation and software downloads.

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) website: http://www.va.gov/vdl/

The Kernel documentation is located on the VDL at: https://www.va.gov/vdl/application.asp?appid=10

VistA documentation and software can also be downloaded from the Product Support (PS) Anonymous Directories.

1 Introduction

This document describes how to deploy and install the Veterans Health Information Systems and Technology Architecture (VistA) Kernel Patch XU*8.0*702, as well as how to back-out the product and rollback to a previous version or data set if required.

Kernel Patch XU*8.0*702 and associated components provides enhancements needed to implement Single Sign-On internal (SSOi) for identification and Personal Identification Verification (PIV) 2-Factor Authentication (2FA) of users into Veterans Health Information Systems and Technology Architecture (VistA) using the **Micro Focus® Reflection [v16]** terminal emulator software (see Figure 1).

Kernel Patch XU*8.0*702 adds code to VistA to accept an Identity and Access Management (IAM) Security Assertion Mark-up Language (SAML) token for PIV authentication using the **Micro Focus® Reflection [v16]** terminal emulator software.

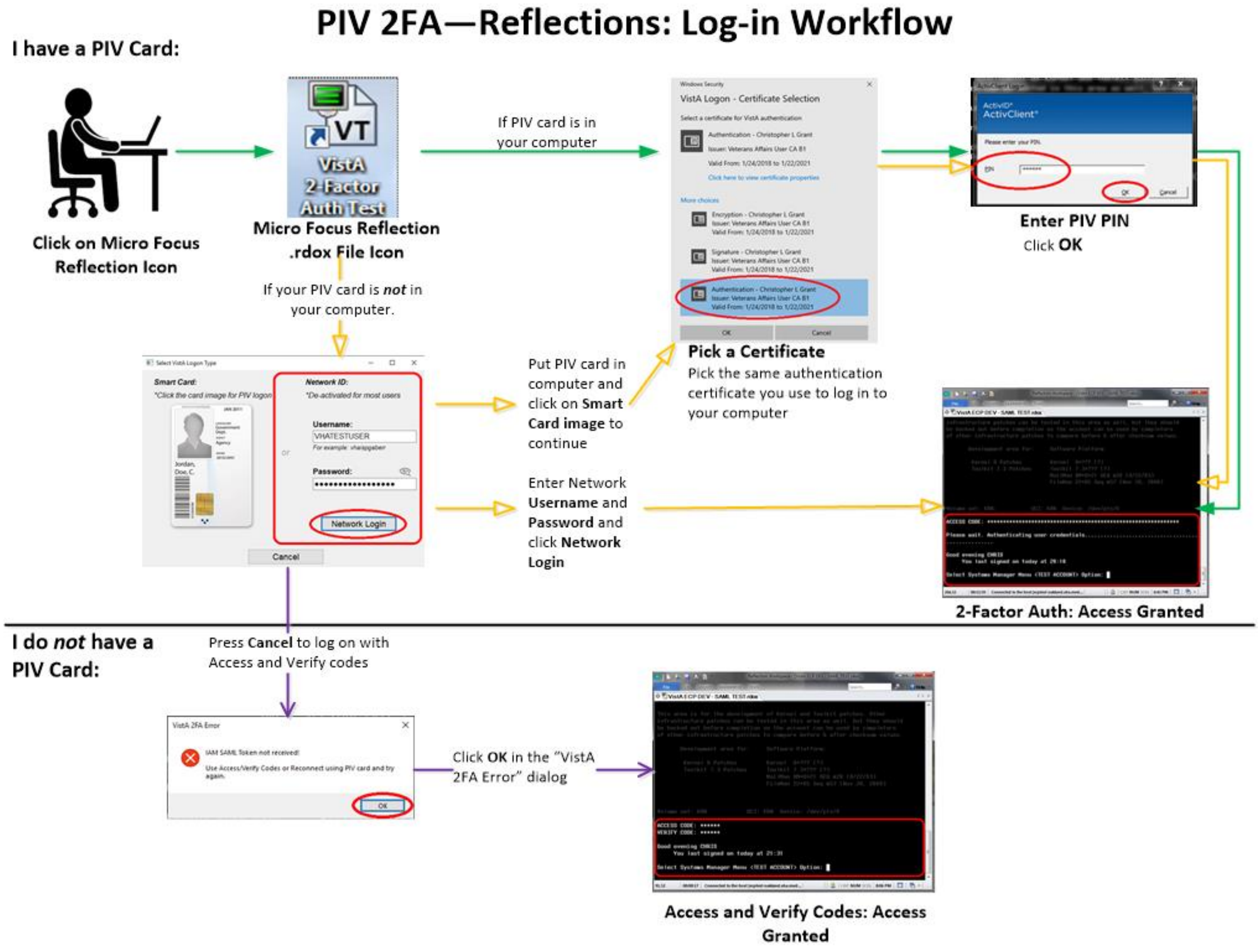
Kernel Patch XU*8.0*702 provides the VistA Kernel utilities needed to implement the following requirements:

> VAIQ #7613595 "Mandatory Use of PIV Multifactor Authentication to VA Information Systems" dated June 30, 2015, requires all VA Information Technology (IT) systems to be Personal Identification Verification (PIV)-enabled and requires the use of multifactor authentication when using a local, network, or remote account to log into a VA information system.
>
> The use of these utilities is expected to improve security and auditing capabilities in accordance with VA Handbook 6500, Appendix F and revision 4 of National Institute of Standards and Technology (NIST) SP 800-53. As required by Federal Information Processing Standards (FIPS) 199 and using guidance from NIST SP 800-60, the *recommended* security categorization for these applications is **HIGH**.
>
> Integration with Identity and Access Management (IAM) services are mandated by executive management via the following memorandums:
>
> - IAM Identity Services (IdS) mandate memorandum (VAIQ #7011145). All applications within VA *must* comply with IAM requirements to ensure that references to the identities of Veterans and their beneficiaries are accurate.
> - IAM Access Services (AcS) functionality within VA is mandated by VAIQ #7060071 REDACTED

The Visual Basic (VB) script and Dynamic Link Library (DLL) files that are distributed in association with this patch release are used to enable **Micro Focus® Reflection (v16)** 2-Factor Authentication (2FA) into IAM, and use the received IAM SAML token to authenticate into VistA:

- DLL performs the authentication with IAM and returns a SAML token.
- VB script calls the DLL and passes the SAML token to VistA.

Figure 1: PIV 2FA Reflection Login Workflow


PIV 2FA—Reflections: Log-in Workflow
I have a PIV Card:
Click on Micro Focus Reflection Icon
VT VistA 2-Factor Auth Test
Micro Focus Reflection .rdox File Icon
If PIV card is in your computer
If your PIV card is *not* in your computer.
VistA Logon - Certificate Selection
Pick a Certificate
Pick the same authentication certificate you use to log in to your computer
ActivClient
PIN
OK
Cancel
Enter PIV PIN
Click **OK**
Smart Card:
Network ID:
Username:
VHATESTUSER
Password:
Network Login
Cancel
Put PIV card in computer and click on **Smart Card image** to continue
Enter Network **Username** and **Password** and click **Network Login**
2-Factor Auth: Access Granted
I do *not* have a PIV Card:
Press **Cancel** to log on with Access and Verify codes
VistA 2FA Error
IAM SAML Token not received!
Use Access/Verify Codes or Reconnect using PIV card and try again.
OK
Click **OK** in the "VistA 2FA Error" dialog
Access and Verify Codes: Access Granted

1.1 Purpose

The purpose of this guide is to provide a single, common document that describes how, when, where, and to whom the VistA Kernel Patch XU*8.0*702 is deployed and installed, as well as how it is to be backed out and rolled back, if necessary. This guide also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, rollback, and troubleshooting are included in this document.

1.2 Dependencies

This section lists and describes all application, system, financial, and other dependencies for this deployment, including upstream processing.

1.2.1 Kernel Patch XU*8.0*702 Dependencies

- **VistA M Server**—Kernel Patch XU*8.0*702 is dependent on Kernel Patch XU*8.0*701 and Kernel Patch XU*8.0*659 being installed on the same VistA M Server.
- **Client Workstation**—The following terminal emulator software *must* be installed on the target client workstation in order to configure the software for 2-Factor Authentication (2FA):

  Micro Focus® Reflection (v16)

  ⚠ **DISCLAIMER: Department of Veterans Affairs (VA) does *not* own or maintain the Micro Focus® Reflection (v16) terminal emulator software. This document only describes how to configure that software to invoke 2-Factor Authentication (2FA). Ongoing maintenance of the Reflection software is outside the scope of this document.**

There are no other direct dependencies; other than the typical operating system and software dependencies described in Section 3.3.2, "Software."

1.2.2 2-Factor Authentication (2FA) Dependencies

Except for Kernel Patch XU*8.0*659 and XU*8.0*701, the following Kernel and RPC Broker patches are *not* direct dependencies of Kernel Patch XU*8.0*702; however, these patches are required for the overall implementation of 2FA:

- Kernel Patch XU*8.0*655 (released 09/15/2015)
- Kernel Patch XU*8.0*659 (released 08/30/2016)
- Kernel Patch XU*8.0*701 (released 02/11/2020)
- Kernel Patch XU*8.0*702 (this patch)
- RPC Broker Patch XWB*1.1*64 (released 11/18/2016)
- RPC Broker Patch XWB*1.1*65 (released 03/27/2017)
- RPC Broker Patch XWB*1.1*71 (release: TBD)

All of these patches adhere to the following policies:

- VAIQ #7613595 "Mandatory Use of PIV Multifactor Authentication to VA Information Systems" dated June 30, 2015, requires all VA IT systems to be PIV-enabled and requires the use of multifactor authentication when using a local, network, or remote account to log into a VA information system.
- The use of these utilities is expected to improve security and auditing capabilities in accordance with VA Handbook 6500 Appendix F and revision 4 of NIST SP 800-53. As required by FIPS 199 and using guidance from NIST SP 800-60, the recommended security categorization for these applications is HIGH.
- Integration with Identity and Access Management (IAM) services are mandated by executive management via the following memorandums:
    - IAM Identity Services (IdS) mandate memorandum (VAIQ #7011145). All applications within VA must comply with IAM requirements to ensure that references to the identities of Veterans and their beneficiaries are accurate.
    - IAM Access Services (AcS) functionality within VA is mandated by VAIQ #7060071 REDACTED

1.2.2.1 Kernel Patch XU*8.0*655

Kernel Patch XU*8.0*655 provided enhanced Single Sign-On (SSO) utilities to support advanced models for identification and authentication of users into VistA. Specifically, Identity and Access Management (IAM):

- Ensured enterprise mandate for Personal Identity Verification (PIV) compliance was met for VistA access.
- Ensured Continuous Readiness in Information Security Program (CRISP) on-boarding and off-boarding enterprise mandate was met for VistA access.
- Automated and improved accuracy in creation of VistA accounts as a path to moving Veterans Health Administration (VHA) and Veterans Business Administration (VBA) applications away from reliance on "anonymous" VistA accounts that represented systems rather than people.
- Integrated VistA user management within the IAM context and provided mapping from the VistA user identifier and enterprise user identifiers (Active Directory [AD], PIV).
- Integrated all forms of user access to VistA ("roll-and-scroll" terminal session, Computerized Patient Record System [CPRS], calls from remote systems, etc.) with the IAM SSO user session.
- Added the following to be used by the IAM Binding application and the IAM Provisioning application (both in development):
    - Five new remote procedures.
    - Two context options.
    - Two REMOTE APPLICATION (#8994.5) file entries.

NOTE: Kernel Patch XU*8.0*655 was released 09/15/2015.

1.2.2.2 Kernel Patch XU*8.0*659

Kernel Patch XU*8.0*659 provided enhancements needed to implement Single Sign-On Internal (SSOi) for identification and authentication of users into VistA. Specifically, Identity and Access Management (IAM):

- Added or updated remote procedures to provide Kernel support for the IAM Provisioning and IAM Binding applications.
- Added or updated remote procedures to fully implement Kernel processing of IAM Secure Token Service (STS) tokens for secure authentication and identification of users authenticated by IAM using Active Directory credentials (KERBEROS or PIV Card).
- Added the **XUS IAM BIND USER** and **XUS ESSO VALIDATE** remote procedures to the XUS SIGNON menu option to make them available to all users.

NOTE: Kernel Patch XU*8.0*659 was released 08/30/2016.

1.2.2.3 Kernel Patch XU*8.0*701

Kernel Patch XU*8.0*701 provided enhancements and security fixes for VistA user authorization via Single Sign-On Internal (SSOi). These enhancements and fixes include:

- Fixes serious SSOi (IAM STS SAML) token validation problems that were found in released Kernel Patch XU*8.0*659 in support of PIV 2FA. It introduces both "strict" and "*non*-strict" credential token validation to properly apply verifications.
- Fixes a problem affecting users with certain last names when using PIV 2FA.
- Completes the work that was started in Kernel Patch XU*8*630 in support of applications, such as Join Legacy Viewer (JLV).
- Allows the use of the SSOi token as a more secure alternative to the Broker Security Enhancement (BSE) token.
- Does *not* require users to change their Verify code when using PIV (SSOi).
- Fixes an existing improper lock synchronization on the FAILED ACCESS ATTEMPTS LOG (#3.05) file.

NOTE: Kernel Patch XU*8.0*701 was released 02/11/2020.

1.2.2.4 RPC Broker Patch XWB*1.1*64

RPC Broker Patch XWB*1.1*64 was the patch for the IAM "Link My Accounts" application. This patch made changes in the Remote Procedure Call (RPC) Broker listener processes to support emerging technologies and made bug fixes. As part of 2-Factor Authentication (2FA), this patch made the **XUS IAM BIND USER** RPC available to all users in any context to implement binding of the VistA user account to the user's Active Directory account using the Identity and Access Management (IAM) Binding application.

NOTE: RPC Broker Patch XWB*1.1*64 was released 11/18/2016.

1.2.2.5 RPC Broker Patch XWB*1.1*65

RPC Broker Patch XWB*1.1*65 was one in a series of patches to support the VA's transition to SSO with Identity and Access Management (IAM) Secure Token Service (STS). This patch provided the Delphi Broker Development Kit (BDK) utilities needed to implement this requirement. Delphi GUI client applications compiled with this BDK automatically made use of IAM STS tokens for user identification and authentication into VistA servers. Access codes/Verify codes are retained as an alternative method of authentication in case of an invalid STS token, STS server unreachable, or failure to install the required VistA-side patches.

NOTE: RPC Broker Patch XWB*1.1*65 was released 03/27/2017.

1.2.2.6 RPC Broker Patch XWB*1.1*71

RPC Broker Patch XWB*1.1*71 is another in a series of patches to support the VA's transition to SSO with Identity and Access Management (IAM) Secure Token Service (STS). This patch provides the Delphi Broker Development Kit (BDK) utilities needed to implement this requirement. Delphi GUI client applications compiled with this BDK will automatically make use of IAM STS tokens for user identification and authentication into VistA servers. Access codes/Verify codes are retained as an alternative method of authentication in case of an invalid STS token, STS server unreachable, or failure to install the required VistA-side patches.

This patch introduces a rewrite of the IAM/SAML token exchange without relying on Microsoft Internet Explorer as a COM layer and provides built-in SOAP/XML/SAML/Certificate Store communication and functionality. Additionally, this version of the BDK allows for Active Directory (AD) Username/Password authentication as a backup to PIV, in case of lost/forgotten PIV cards and the user requesting a temporary PIV card exemption to allow the use of AD authentication.

The DLL included with patch XU*8.0*702 was built with BDK components/code provided by this patch.

1.3 Constraints

This section describes the target physical environment for deployment. The Kernel security controls are operationally capable within full implementation of National Institute of Standards and Technology (NIST) controls. It is in compliance with Directive 6500, Section 508, and performance impacts of the deployment environment.

There are no constraints for Kernel Patch XU*8.0*702 release other than the operating system and software dependencies described in Section 3.3.2, "Software."

2 Roles and Responsibilities

This section lists the teams that will perform the steps described in this guide.

Table 2 identifies the technical and support personnel who are involved in the deployment, installation, back-out, and rollback of the Veterans Health Information Systems and Technology Architecture (VistA) Kernel Patch XU*8.0*702 release.

Table 2: Roles and Responsibilities

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	Enterprise Program Management Office (EPMO) Implementation Team	Deployment	Plan and schedule deployment (including orchestration with vendors).	Planning
2	EPMO Implementation Team	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Planning
3	Software Quality Assurance (SQA)	Deployment	Test for operational readiness.	Build
4	Product Support (PS)	Deployment	Execute deployment.	Release Prep Phase
5	EPMO Implementation Team	Installation	Plan and schedule installation.	Build Phase
6	EPMO Implementation Team	Installation	Ensure authority to operate and that certificate authority security documentation is in place.	Release Prep Phase
8	EPMO Implementation Team VistA Infrastructure (VI) Development Team	Installations	Coordinate training.	Release Prep Phase

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
9	EPMO Implementation Team VistA Infrastructure (VI) Development Team	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out).	Build Phase
10	SDE Field Operations (FO) Enterprise Operations (EO)	Post Deployment	Hardware, Software and System Support.	Post Release

3 Deployment

This section provides the schedule and milestones for the Kernel Patch XU*8.0*702 deployment.

Kernel Patch XU*8.0*702 deployment is planned as a simultaneous rollout. National release date is scheduled for 12/05/2019.

ℹ **NOTE:** This is just a *proposed* National release date. It is assumed that field testing would be done concurrent with software Quality assurance (SQA) review (starting 11/05/2019).

3.1 Timeline

Kernel Patch XU*8.0*702 deployment and installation is scheduled to run for **30** days from release, which is the typical Veterans Health Information Systems and Technology Architecture (VistA) national patch rollout schedule.

Table 3: Deployment Timeline

Deployment	Start	Finish
Patch Development and Release	08/27/2018	03/15/2020
Site Installation and Deployment	03/23/2020	04/23/2020
Sustainment	04/23/2020	Ongoing

3.2 Site Readiness Assessment

This section describes the Site Readiness Assessment for the locations that will receive Kernel Patch XU*8.0*702 deployment. This will be a national release of a VistA patch with an associated Visual Basic (VB) script and Dynamic Link Library (DLL) file to all VistA production sites.

Topology determinations are made by Enterprise Systems Engineering (ESE) and vetted by Enterprise Service Line (ESL), Field Office (FO), National Data Center Program (NDCP), and Austin Information Technology Center (AITC) during the design phase as appropriate. Field site coordination is done by ESL unless otherwise stipulated by ESL.

3.2.1 Deployment Topology (Targeted Architecture)

This section describes the deployment topology (local sites, etc.) for Kernel Patch XU*8.0*702.

Kernel Patch XU*8.0*702 will be distributed to local and regional system administrators and support personnel responsible for each of the **130** VistA parent systems. The VistA M Server code, VB script, and DLL will be available to developers from the Product Support (PS) Anonymous Directories.

NOTE: The code will be available to developers from secure file transfer [SFTP) sites listed in the patch description.

3.2.2 Site Information (Locations, Deployment Recipients)

Kernel Patch XU*8.0*702 VistA M Server code is directly deployed to all VA sites following the standard deployment procedure used for all VistA patches.

3.2.3 Site Preparation

This section describes the preparation required for the site at which the system will operate.

There are no special site preparations or changes that *must* occur to the operational site and no specific features or items that need to be modified to adapt to Kernel Patch XU*8.0*702.

As a precursor to Kernel Patch XU*8.0*702 deployment, the Kernel documentation set (including this Deployment, Installation, Back-Out, and Rollback Guide) will be added to the VA Software Document Library (VDL) at: https://www.va.gov/vdl/application.asp?appid=10

Table 4 describes preparation required by the site prior to deployment.

Table 4: Site Preparation

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
Not Applicable (N/A)	N/A	N/A	N/A	N/A

3.3 Resources

This section describes the hardware, software, facilities, documentation, and any other resources, other than personnel, required for the deployment and installation of Kernel Patch XU*8.0*702.

3.3.1 Hardware

There are no specific hardware requirements for installation of Kernel Patch XU*8.0*702 as it runs in a typical VistA M Server environment. There is also no need for specific hardware to assist in the deployment of Kernel Patch XU*8.0*702.

Table 5 describes hardware specifications required at each site prior to deployment of Kernel Patch XU*8.0*702.

Table 5: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
N/A	N/A	N/A	N/A	N/A	N/A

REF: For details about who is responsible for preparing the site to meet these hardware specifications, see Table 2.

3.3.2 Software

The installation of Kernel Patch XU*8.0*702 is a typical Kernel Installation & Distribution System (KIDS) install of a VistA patch in the following environments:

- VistA M Server Software Requirements
- Client Workstation Software Requirements

In addition to Kernel Patch XU*8.0*702 VistA M Server code, this software distribution includes a Visual Basic (VB) script and a Dynamic Link Library (DLL) file that are used to implement 2-Factor Authentication (2FA) with the Reflection terminal emulator software that is loaded on most client workstations.

3.3.2.1 VistA M Server Software Requirements

Table 6 lists the *minimum* software requirements for the VistA M Server in order to install and use Kernel Patch XU*8.0*702:

Table 6: VistA M Server—Minimum Software Requirements

Software	Version	Description
InterSystems Caché	2017.1.3 for Linux, Windows 7, and OpenVMS	Server Operating System Fully Patched.
Kernel	8.0	VistA Legacy Software Fully Patched M Accounts. Patches *must* be installed in published sequence.
Kernel Toolkit	7.3	VistA Legacy Software Fully Patched M Accounts. Patches *must* be installed in published sequence.
VA FileMan	22.2	VistA Legacy Software Fully Patched M Accounts. Patches *must* be installed in published sequence.
RPC Broker	1.1	VistA Legacy Software Fully Patched M Accounts. Patches *must* be installed in published sequence.
MailMan	8.0	VistA Legacy Software Fully Patched M Accounts. Patches *must* be installed in published sequence.

3.3.2.2 Client Workstation Software Requirements

Table 7 lists the *minimum* software requirements for the VistA M Server in order to install and use Kernel Patch XU*8.0*702:

NOTE: You only need to have the following terminal emulator software application installed on the client workstation.

Table 7: Client Workstation—Minimum Software Requirement

Software	Version	Description
Micro Focus® Reflection	16.x	Terminal Emulator Software.

NOTE: This section does *not* describe how to install the **Micro Focus® Reflection (v16)** terminal emulator software. Terminal emulator software is pushed to all client workstations and maintained by the Office of Information Field Office (OIFO) System Center Configuration Manager (SCCM) group.

In addition to Kernel Patch XU*8.0*702 VistA M Server code, this software distribution includes a Visual Basic (VB) script and a Dynamic Link Library (DLL) file that are used to implement 2-Factor Authentication (2FA) with the Reflection terminal emulator software that is loaded on most client workstations.

3.3.3 Communications

This section describes any notifications activities and how they will occur.

Prior to the deployment of Kernel Patch XU*8.0*702, a product announcement will be sent via email to current Points of Contact (POC) on record for each site describing the product and a brief description of the deployment and post-deployment support. Included will be links to the Kernel 8.0 VA Software Document Library (VDL) and Rational repositories, which contain further information about the release and the deployment, including the deployment schedule and required pre-installation activities.

Kernel Patch XU*8.0*702 Implementation Team will respond to email requests for assistance and further information and, where appropriate, re-direct these requests to specialist technical staff.

3.3.3.1 Deployment/Installation/Back-Out Checklist

Tracking of installation for VistA Kernel patches is monitored in FORUM.

Table 8 provides a checklist to be used to capture the coordination effort and document the day/time/individual when each activity (deploy, install, back-out) is completed for standard Kernel 8.0 patch releases and associated VB script and DLL to enable 2-Factor Authentication (2FA) with the Reflection terminal emulator software.

Table 8: Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual who completed task
Deploy			
Install Patch XU*8.0*702 on VistA M Server			
Install/Load VB Script and DLL			
Configure Reflection Software for 2-Factor Authentication (2FA)			
Back-Out			

4 Installation

Kernel Patch XU*8.0*702 provides enhancements needed to implement Single Sign-On internal (SSOi) for identification and authentication of users into Veterans Health Information Systems and Technology Architecture (VistA) for terminal emulator access (i.e., **Micro Focus® Reflection [v16]** terminal emulator software).

4.1 Pre-Installation and System Requirements

This section provides the minimum requirements for the product to be installed.

REF: For a list of the minimum hardware and software requirements, including platform, Operating System (OS), and storage requirements required for Kernel Patch XU*8.0*702, see the following:

- Section 3.3.1, "Hardware"
- Section 3.3.2, "Software"

Table 9 lists the items that installers should consider before installing Kernel Patch XU*8.0*702:

Table 9: Pre-Installation and System Requirement Considerations *before* Installing Kernel Patch XU*8.0*702

Item	Description
VistA M Servers	Kernel Patch XU*8.0*659 *must* be installed before installing Kernel Patch XU*8.0*702 in VistA.
Client Workstations Terminal Emulator Software	Verify the terminal emulator software that is in use on all client workstations. The current VA-approved terminal emulator software is: **Micro Focus® Reflection (v16)**

4.2 Platform Installation and Preparation

Kernel Patch XU*8.0*702 should be installed on VistA M Servers. Also, it requires additional system configuration for any installed terminal emulator software on client workstations (i.e., **Micro Focus® Reflection [v16]** terminal emulator software).

All VistA Infrastructure patches *must* be installed within **30** days of national release.

4.3 Download and Extract Files

The Kernel Patch XU*8.0*702 download files are listed in Table 10.

All Kernel software can be downloaded from the Product Support (PS) Anonymous Directories. Also, all Kernel documentation is available in Adobe® Acrobat PDF format and can be downloaded from the VA Software Document Library (VDL) website: https://www.va.gov/vdl/application.asp?appid=10

NOTE: For all patches, first read the patch installation instructions in the patch description located in National Patch Module (NPM) on FORUM.

4.3.1 Distribution Files

Download the software and documentation distribution files in Table 10 that are needed to install Kernel Patch XU*8.0*702 on the VistA M Server and configure the terminal emulator software on the client workstation:

Table 10: Distribution Files

File Name	Type	Description
XU*8.0*702 Patch Description	ASCII	**Patch Description (PD)**. This provides any pre-installation instructions, instructions, and additional information to install the patch. Follow all patch installation instructions.
xu_8_0_p702_dibr.pdf	Binary	**Deployment, Installation, Back-Out, and Rollback Guide** (manual). Use this manual in conjunction with the patch description on FORUM.
XU_8_702.zip	Binary	**Visual Basic (VB) Script** (zip file). This zip file contains the following VB script file for the installation required for the **Micro Focus® Reflection (v16)** terminal emulator (roll-and-scroll) software on the client workstation: **XUSSOi-1.0p702_v16.bas (Micro Focus® Reflection [v16] VB script)**

4.3.2 Extract Zip Files

On the client workstation, extract all files from the **XU_8_702.zip** distribution file (Table 10):

1. Copy the **XU_8_702.zip** file to a temporary location. For example:

   C:\Temp\Patch-702

2. Use Microsoft® Windows Explorer to extract all of the files:

   a. Right-click on **XU_8_702.zip** file name.

   b. Select **Extract All**.

   c. In the “Extract Compressed (Zipped) Folders” dialogue, accept the default location displayed, or select a new destination folder.

   d. Select **Extract**.

4.3.3 File and Documentation Maintenance

Any required maintenance or changes to the DLL and VB Script (Table 10) will be deployed via a new patch with updated instructions included.

The included Kernel DLL is built using components/code from the RPC Broker Development Kit (BDK) released with RPC Broker Patch XWB*1.1*71. A new BDK would *not* require a change to the Kernel DLL, because none of the RPC Broker functions are being used, only the parts required for IAM 2FA authentication.

4.4 Database Creation

This section is not applicable. Kernel Patch XU*8.0*702 does *not* create any required databases. It uses the already installed VA FileMan database.

4.5 Installation DLL and VB Script

Kernel Patch XU*8.0*702 provides the following installation DLL and VB script via the XU_8_702.zip file (Table 10):

- **XUIAMSSOi.dll** (Version **8.0.702.3**)

  NOTE: The DLL file will be automatically placed on workstations with Micro Focus® Reflection installed by the Client Technologies team.

- **XUSSOi-1.0p702_v16.bas** (**Micro Focus® Reflection [v16]** Visual Basic script)

4.6 Cron Scripts

This section is not applicable. Kernel Patch XU*8.0*702 does *not* provide any cron scripts[1].

4.7 Access Requirements and Skills Needed for the Installation

General skills required to perform the Kernel Patch XU*8.0*702 installation are listed below:

- Back up the system

  [VistA M Server and Client Workstation]

- Copy files using commands

  [VistA M Server and Client Workstation]

- Run a Kernel Installation & Distribution System (KIDS) installation

  [VistA M Server]

[1] **Cron** is a time-based job scheduler in Unix-like computer operating systems. People who set up and maintain software environments use cron to schedule jobs (commands or shell scripts) to run periodically at fixed times, dates, or intervals. It typically automates system maintenance or administration. These scripts are suitable for scheduling repetitive tasks: Wikipedia; https://en.wikipedia.org/wiki/Cron

REF: Instructions for performing these functions are provided in vendor-supplied operating system manuals as well as other VA and VistA publications.

4.8 Installation Procedure

Separate installation procedures are provided in this guide for each of the following target environments:

- VistA M Server Instructions
- Client Workstation Instructions—Micro Focus® Reflection (v16)

4.8.1 VistA M Server Instructions

The instructions in this section are applicable for the Test and Production accounts in the Caché environment.

NOTE: Install the server software in a Test account *prior* to installing it in a Production account.

4.8.1.1 Confirm Distribution Files *(recommended)*

Verify that you have downloaded the files listed in Table 10.

4.8.1.2 Retrieve Released Kernel 8.0 Patches *(required)*

Prior to installation of the Kernel Development Kit, all current server-side patches should be installed.

Obtain all released Kernel 8.0 server-side patches from the Patch Module on FORUM or through normal procedures.

4.8.1.3 Install Kernel Patch XU*8.0*702

Install Kernel Patch XU*8.0*702 from the VistA MailMan message per directions in the patch description.

4.8.2 Client Workstation Instructions—Micro Focus® Reflection (v16)

This section describes how to configure the pre-installed **Micro Focus® Reflection (v16)** terminal emulator software (i.e., Reflection Workspace v16.0) as an interface to 2-Factor Authentication (2FA). The terminal emulator instructions are applicable to both modifying an existing session file (**.rdox**) individually on a workstation or a GOLD version of a **.rdox** session file that is setup to be distributed to many workstations.

NOTE: This section does *not* describe how to install the **Micro Focus® Reflection (v16)** terminal emulator software. Terminal emulator software is pushed to all client workstations and maintained by the Office of Information Field Office (OIFO) System Center Configuration Manager (SCCM) group.

The configuration of **Micro Focus® Reflection (v16)** for 2FA includes the following steps:

- Copy DLL to Reflection Program Files Folder—Copy the DLL to the location where **Micro Focus® Reflection (v16)** reads it on start up.

  NOTE: The DLL file will be automatically placed on workstations with Micro Focus® Reflection installed by the Client Technologies team.

- Import Visual Basic Script—Import VB Script to the “Project” environment within **Micro Focus® Reflection (v16)**, so the script is available to and contained within the configured **.rdox** file, allowing its portability for deployment to workstations.

- Set Connection Action—Set the Connection Action to:

  "**Run a macro or other action after the initial connection**” action (mapping that action to the “**XUSSOi.XUSSOProcess**” subroutine in the VB script).

4.8.2.1 Copy DLL to Reflection Program Files Folder

Copy the **XUIAMSSOi.dll** file to the location where **Micro Focus® Reflection (v16)** reads it on start up.

ATTENTION: This step requires Administrative privileges on the client workstation. Also, the DLL file will be automatically placed on workstations with Micro Focus® Reflection installed by the Client Technologies team.

On the client workstation, from the extracted files (see Section 4.3.2, “Extract Zip Files”), copy the **XUIAMSSOi.dll** file (Version **8.0.702.3**) into the following directory:

C:\Program Files (x86)\Micro Focus\Reflection

The DLL[2] file is copied to this location, so it is loaded when **Micro Focus® Reflection (v16)** is launched. This folder is also set in the PATH environment variable on all workstations that have the **Micro Focus® Reflection** software installed. This allows the DLL to be referenced without defined paths in the VB script, yet still load from a faster default path on the workstation.

4.8.2.2 Import Visual Basic Script

The step-by-step instructions in this section import the **XUSSOi-1.0p702_v16.bas** Visual Basic script to the "**Project**" environment within the **Micro Focus® Reflection (v16)** session file (**.rdox**), so the script is contained and available to the specific **.rdox** file and portable if it needs to be distributed to multiple workstations after setup.

For **Micro Focus® Reflection (v16)** terminal emulator software on the client workstation, do the following:

1. From the extracted files (see Section 4.3.2, "Extract Zip Files"), copy the **XUSSOi-1.0p702_v16.bas** Visual Basic script ("**v16**") into a temporary directory. For example:

   C:\Temp\Patch-702

   The **XUSSOi-1.0p702_v16.bas** file can be deleted after the installation is complete.

2. Open/launch an existing **Micro Focus® Reflection** session file (**.rdox**) that is configured to connect to a VistA system. At this point, a VistA connection is *not* needed, so the session can be allowed to timeout without entering ACCESS/VERIFY codes.

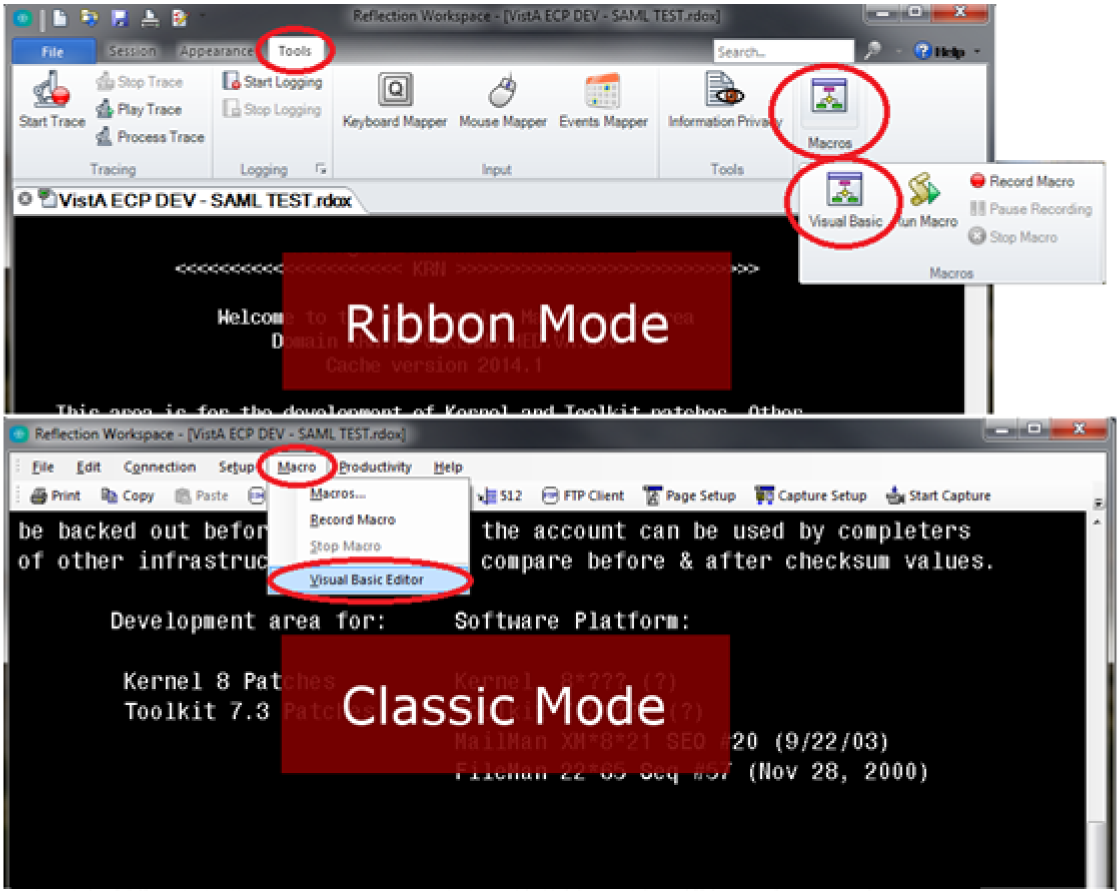
3. Depending on the **Micro Focus® Reflection (v16)** mode in use (see Figure 2), open the Microsoft® Visual Basic Editor by either of the following methods:

   - "Ribbon" Mode—On the **Tools** tab under **Macros**, select **Visual Basic**.
   - "Classic" Mode—From the **Macro** menu, select **Visual Basic Editor**.

[2] Dynamic Link Library (DLL) is a shared "library of executable functions or data that can be used by a Windows application. Typically, a DLL provides one or more particular functions and a program accesses the functions by creating either a static or dynamic link to the DLL. A static link remains constant during program execution while a dynamic link is created by the program as needed. DLLs can also contain just data. DLL files usually end with the extension .dll, .exe, .drv, or .fon.

A DLL can be used by several applications at the same time. Some DLLs are provided with the Windows operating system and available for any Windows application. Other DLLs are written for a particular application and are loaded with the application." Webopedia "Dynamic Link Library (DLL)" term definition; Author: Vangie Beal;Website: http://www.webopedia.com/TERM/D/DLL.html

Figure 2: Micro Focus® Reflection (v16)—Open "Visual Basic" Editor in "Ribbon" Mode or "Classic" Mode



```
<<<<<<<<<<<<<<<<<<<<<<< KRN >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Welcome to t
D main
     Cache version 2014.1
This area is for the development of Kernel and Toolkit patches. Other
```

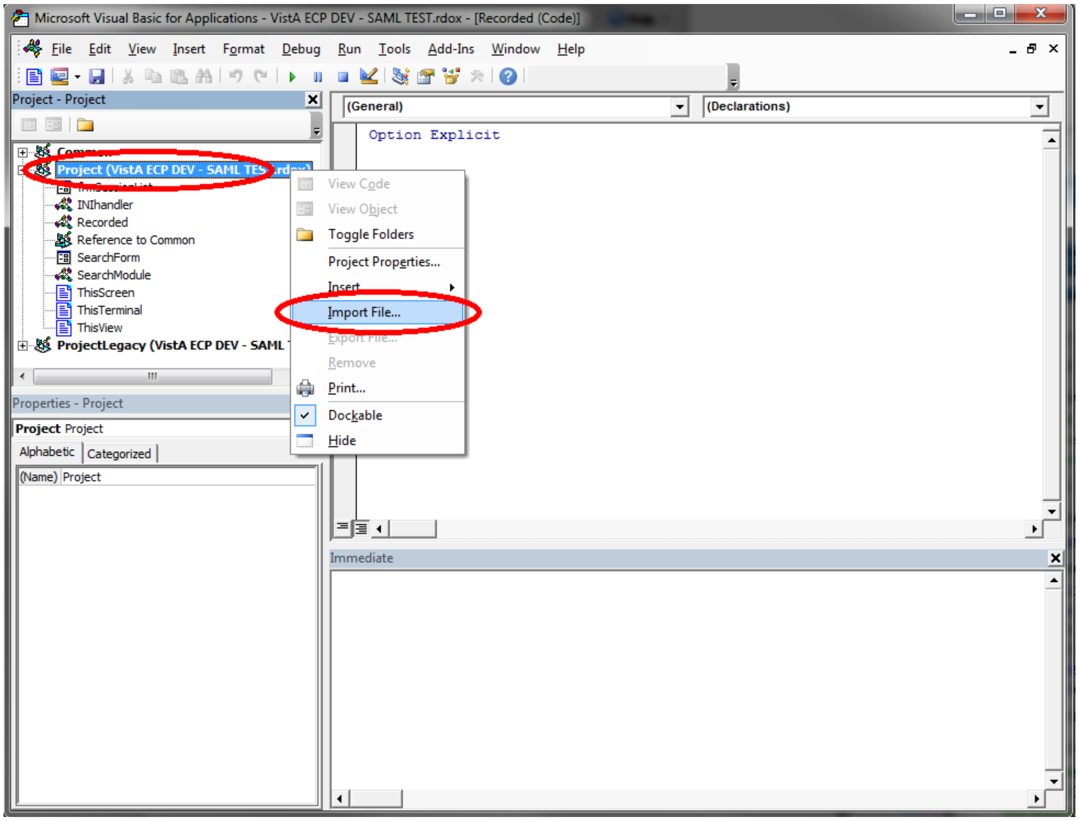
```
be backed out befor                the account can be used by completers
of other infrastruc                compare before & after checksum values.

     Development area for:      Software Platform:

      Kernel 8 Patches          Kernel 8*??? (?)
      Toolkit 7.3 Patches
                                MailMan XM*8*21 SEQ #20 (9/22/03)
                                FileMan 22*65 Seq #57 (Nov 28, 2000)
```

4. To import the VB script into the **.rdox** session file, using the Microsoft® Visual Basic Editor (Figure 3):

   a. Right-click on the **Project** group with the Project area.

   b. Select **Import File**.

Figure 3: Microsoft® Visual Basic Editor—Select File Menu Option



```
Option Explicit
```

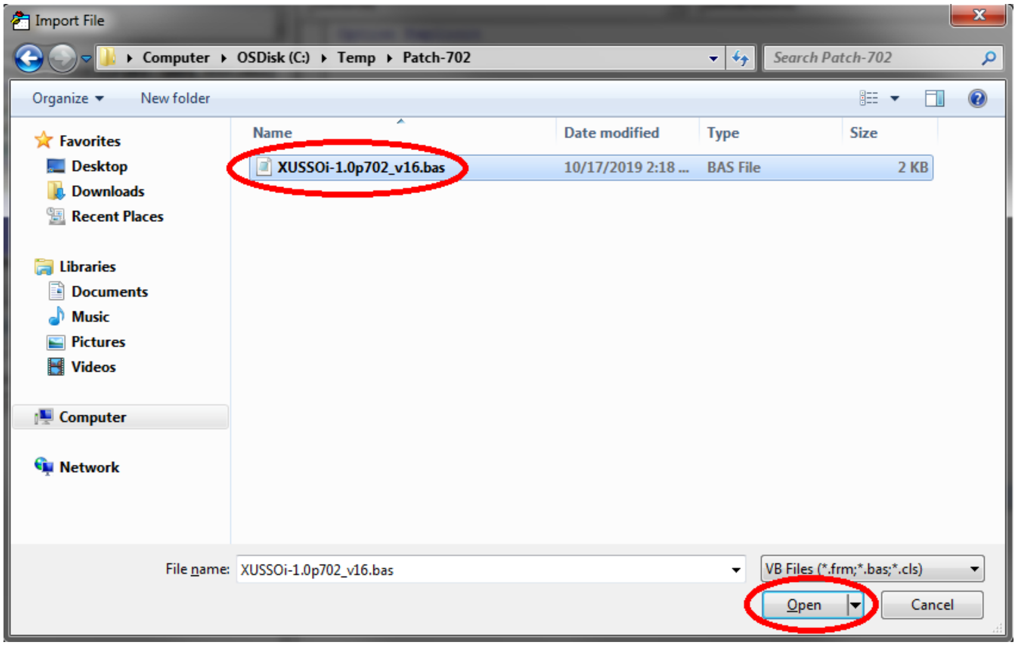
NOTE: The folder tree display in Figure 3 can vary depending on whether or not you have toggled the folder view on or off.

5. Navigate to the location where you saved the **XUSSOi-1.0p702_v16.bas** file in Step 1 (e.g., C:\Temp\Patch-702\v16):

   a. Select the **XUSSOi-1.0p702_v16.bas** file.

   b. Select **Open**, as shown in Figure 4.

Figure 4: Microsoft® Visual Basic Editor—Select XUSSOi-1.0p702_v16.bas File



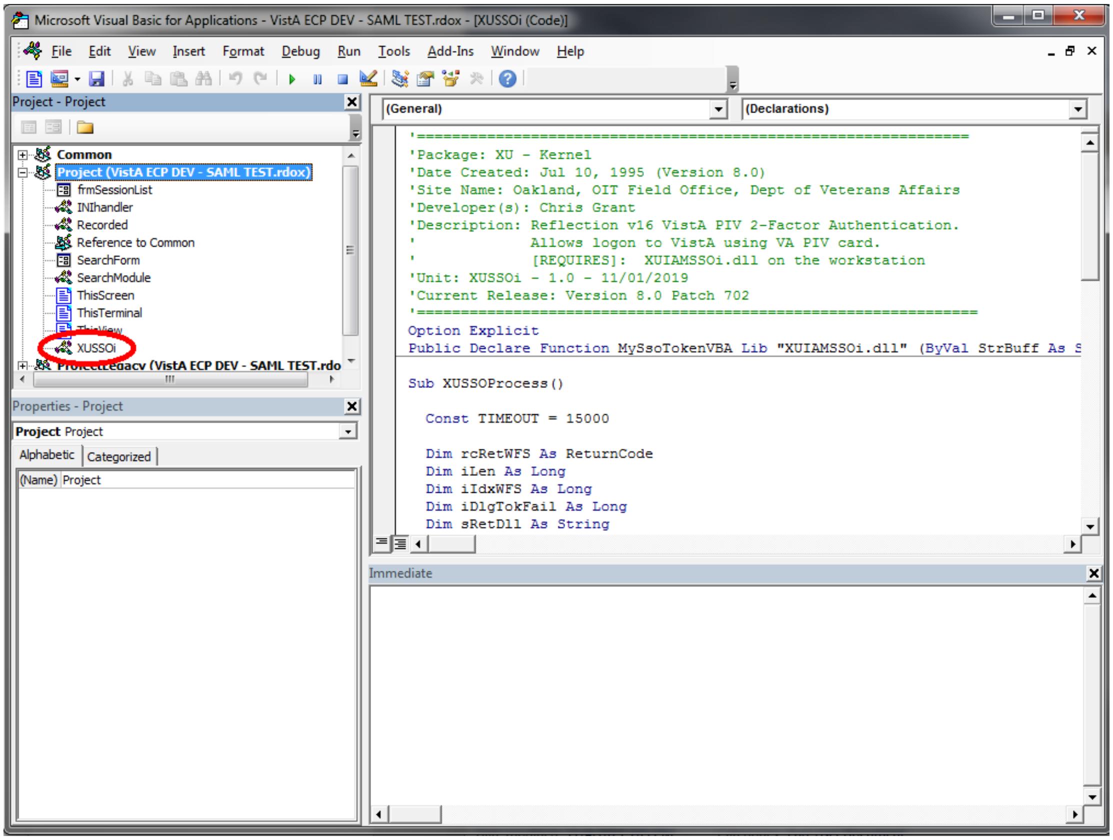
Name	Date modified	Type	Size
XUSSOi-1.0p702_v16.bas	10/17/2019 2:18 ...	BAS File	2 KB

File name: XUSSOi-1.0p702_v16.bas

VB Files (*.frm;*.bas;*.cls)

6. You should see the **XUSSOi** module listed under the “Project” project, as shown in Figure 5:

Figure 5: Microsoft® Visual Basic Editor—XUSSOi Module

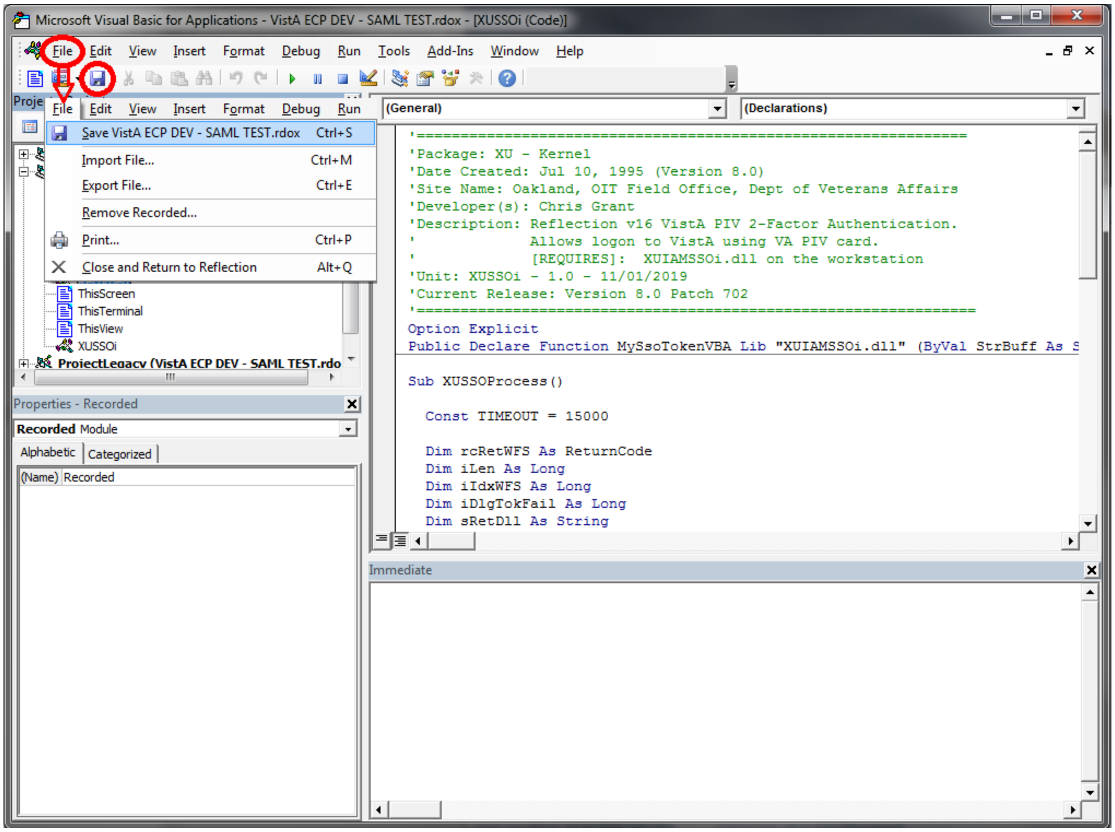

Microsoft Visual Basic for Applications - VistA ECP DEV - SAML TEST.rdox - [XUSSOi (Code)]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Project - Project
Common
Project (VistA ECP DEV - SAML TEST.rdox)
frmSessionList
INIhandler
Recorded
Reference to Common
SearchForm
SearchModule
ThisScreen
ThisTerminal
ThisView
XUSSOi
ProjectLegacy (VistA ECP DEV - SAML TEST.rdo
Properties - Project
Project Project
Alphabetic
Categorized
(Name) Project
(General)
(Declarations)
Immediate

```
'===============================================================
'Package: XU - Kernel
'Date Created: Jul 10, 1995 (Version 8.0)
'Site Name: Oakland, OIT Field Office, Dept of Veterans Affairs
'Developer(s): Chris Grant
'Description: Reflection v16 VistA PIV 2-Factor Authentication.
'             Allows logon to VistA using VA PIV card.
'             [REQUIRES]:  XUIAMSSOi.dll on the workstation
'Unit: XUSSOi - 1.0 - 11/01/2019
'Current Release: Version 8.0 Patch 702
'================================================================
Option Explicit
Public Declare Function MySsoTokenVBA Lib "XUIAMSSOi.dll" (ByVal StrBuff As S

Sub XUSSOProcess()

  Const TIMEOUT = 15000

  Dim rcRetWFS As ReturnCode
  Dim iLen As Long
  Dim iIdxWFS As Long
  Dim iDlgTokFail As Long
  Dim sRetDll As String
```

NOTE: The folder tree display in Figure 5 can vary depending on whether or not you have toggled the folder view on or off. Also, depending on the size of the project area of the editor window, scrolling may be required to see the newly imported module.

7. Select **Save** (blue disk icon) or select **File** and then **Save** from the menu, as shown in Figure 6:

Figure 6: Microsoft® Visual Basic Editor—Save Changes



```
'==============================================================
'Package: XU - Kernel
'Date Created: Jul 10, 1995 (Version 8.0)
'Site Name: Oakland, OIT Field Office, Dept of Veterans Affairs
'Developer(s): Chris Grant
'Description: Reflection v16 VistA PIV 2-Factor Authentication.
'             Allows logon to VistA using VA PIV card.
'             [REQUIRES]:  XUIAMSSOi.dll on the workstation
'Unit: XUSSOi - 1.0 - 11/01/2019
'Current Release: Version 8.0 Patch 702
'===============================================================
Option Explicit
Public Declare Function MySsoTokenVBA Lib "XUIAMSSOi.dll" (ByVal StrBuff As S

Sub XUSSOProcess()

  Const TIMEOUT = 15000

  Dim rcRetWFS As ReturnCode
  Dim iLen As Long
  Dim iIdxWFS As Long
  Dim iDlgTokFail As Long
  Dim sRetDll As String
```

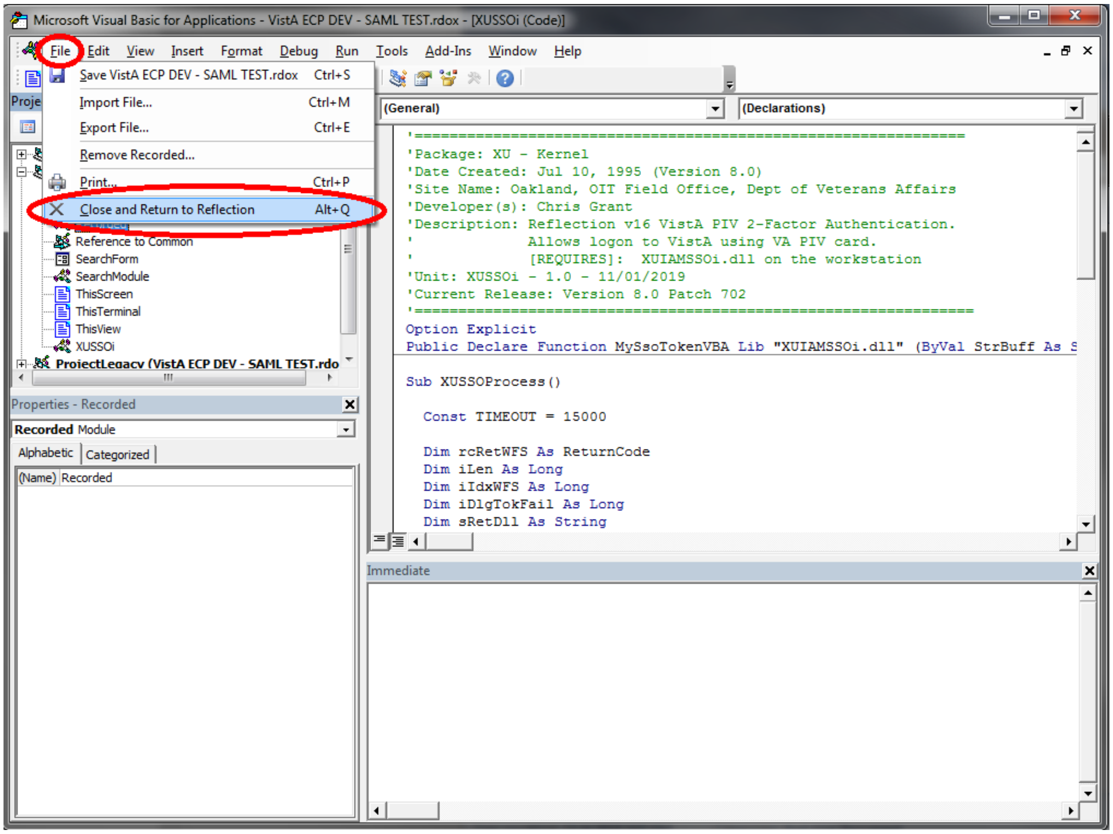
NOTE: The folder tree display in Figure 6 can vary depending on whether or not you have toggled the folder view on or off.

8. Close the Microsoft® Visual Basic Editor:

   a. Select **File**.

   b. Select **Close and Return to Reflection**.

Figure 7: Microsoft® Visual Basic Editor—Closing and Returning to Reflection



```
'===============================================================
'Package: XU - Kernel
'Date Created: Jul 10, 1995 (Version 8.0)
'Site Name: Oakland, OIT Field Office, Dept of Veterans Affairs
'Developer(s): Chris Grant
'Description: Reflection v16 VistA PIV 2-Factor Authentication.
'             Allows logon to VistA using VA PIV card.
'             [REQUIRES]:  XUIAMSSOi.dll on the workstation
'Unit: XUSSOi - 1.0 - 11/01/2019
'Current Release: Version 8.0 Patch 702
'================================================================
Option Explicit
Public Declare Function MySsoTokenVBA Lib "XUIAMSSOi.dll" (ByVal StrBuff As S

Sub XUSSOProcess()

  Const TIMEOUT = 15000

  Dim rcRetWFS As ReturnCode
  Dim iLen As Long
  Dim iIdxWFS As Long
  Dim iDlgTokFail As Long
  Dim sRetDll As String
```

4.8.2.3 Set Connection Action

This step sets the following Connection Action within the “Host Connections Settings” in **Micro Focus® Reflection (v16)**:

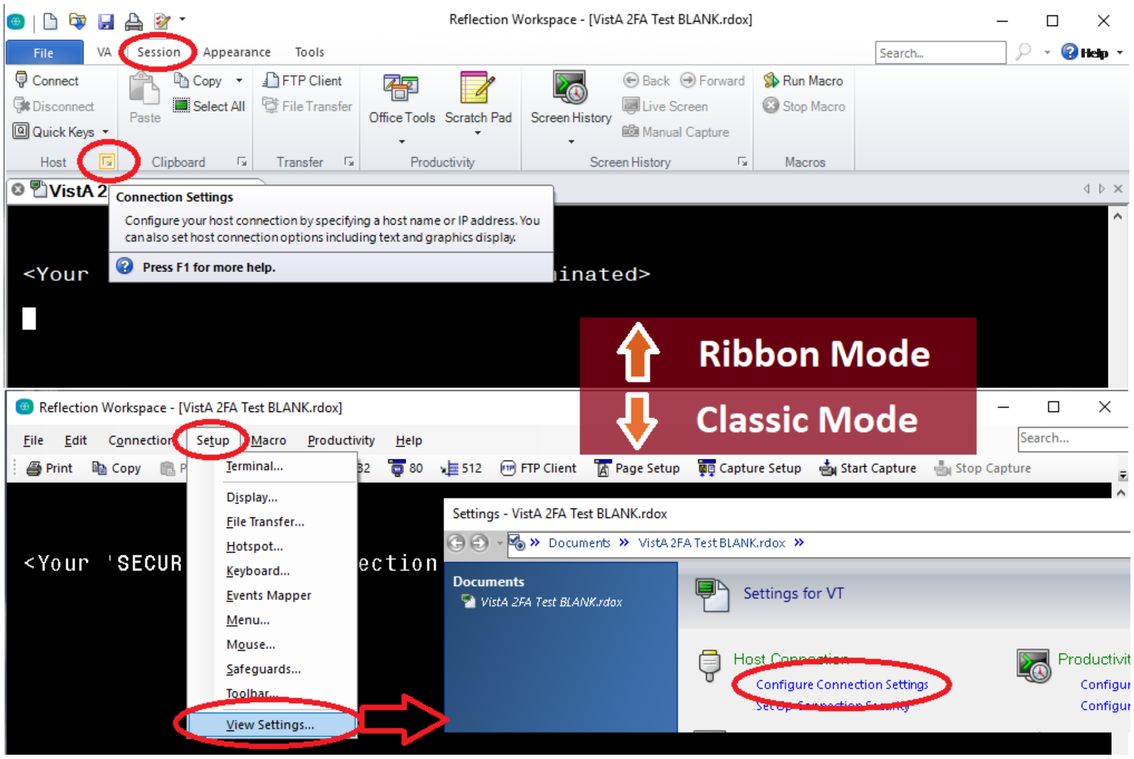
> **"Run a macro or other action after the initial connection**” action, which maps to the **XUSSOi.XUSSOProcess** VB subroutine.

Configure the terminal session **.rdox** file to trigger these events upon launching the session or when an open session is disconnected and reconnects, which forces the user to go through IAM and the RPC Broker’s 2-Factor Authentication.

To configure the **Micro Focus® Reflection (v16)** host settings connection action, do the following:

1. Depending on the Micro Focus® Reflection mode in use, open the **Connection Settings**, as shown in Figure 8:
    - “Ribbon” Mode—Under the **Sessions** tab, select the **Host Connection Settings** expansion button.
    - “Classic” Mode—Under the **Setup** menu, select the **View Settings** menu option, then select the **Configure Connection Settings** link in the “Settings for VT” page.

Figure 8: Micro Focus® Reflection (v16)—Select “Host Connection Settings” in “Ribbon” or “Classic” Mode



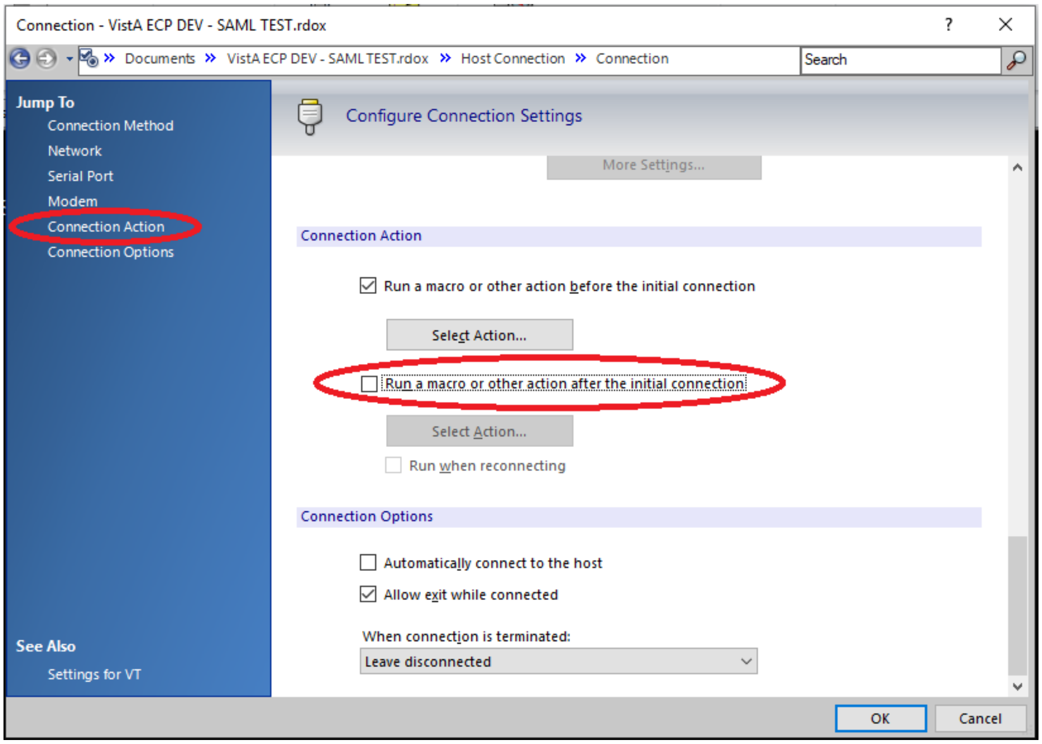
Connection Settings

Configure your host connection by specifying a host name or IP address. You can also set host connection options including text and graphics display.

Press F1 for more help.

2. In the “Configure Connection Settings” form:
   a. Select the **Connection Action** option on the left menu.
   b. Select the **Run a macro or other action after the initial connection** checkbox, as shown in Figure 9:

Figure 9: Micro Focus® Reflection (v16)—“Configure Connection Settings” Form: Select “Connection Action” Event



Connection - VistA ECP DEV - SAML TEST.rdox

Documents » VistA ECP DEV - SAML TEST.rdox » Host Connection » Connection

Configure Connection Settings

Connection Action

☑ Run a macro or other action before the initial connection

□ Run a macro or other action after the initial connection

□ Run when reconnecting

Connection Options

□ Automatically connect to the host

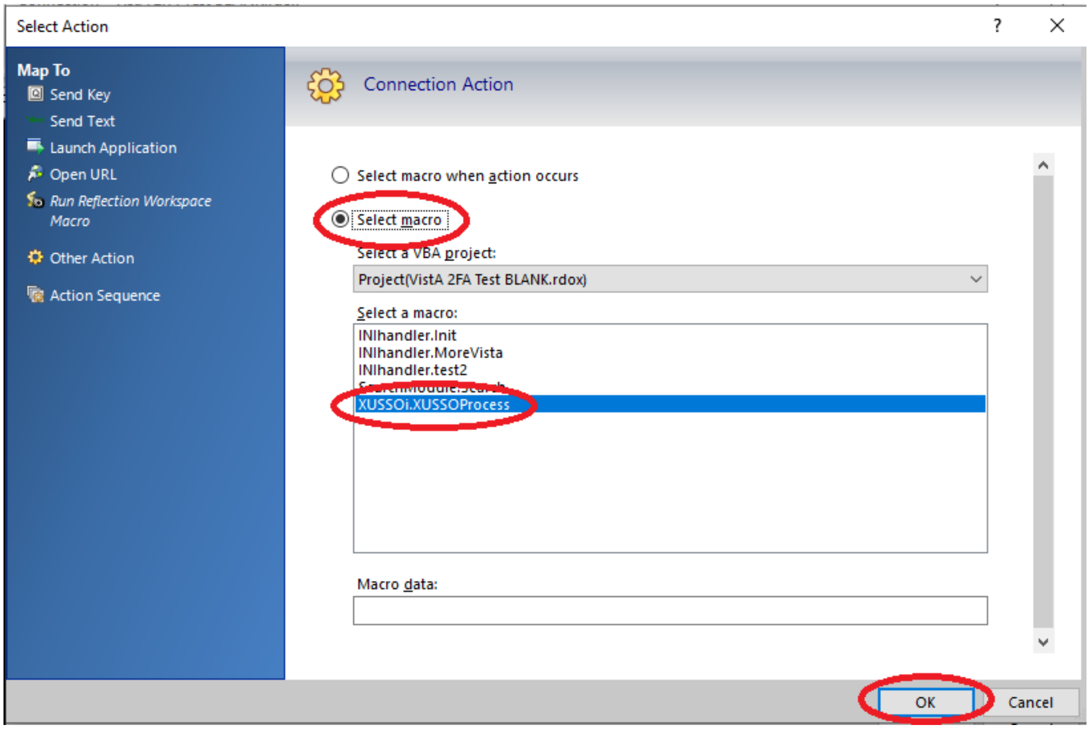
☑ Allow exit while connected

When connection is terminated: Leave disconnected

NOTE: The first Connection Action checkbox, **Run a macro or other action before the initial connection**, does ***not*** need to change. Some **.rdox** file configurations may have this box checked or unchecked, and that setting can be left as is. Only the second Connection Action checkbox, **Run a macro or other action after the initial connection**, which is circled in **RED** (Figure 9), needs to change as per these instructions.

3. In the “Connection Action” form (Figure 10):
    a. Select the **Select macro** option.
    b. Select **XUSSOi.XUSSOProcess** VB macro.
    c. Select **OK**, as shown in Figure 10.

Figure 10: Micro Focus® Reflection (v16)—“Connection Action” Form: “Select XUSSOi.XUSSOProcess” Macro



○ Select macro when action occurs

● Select macro

Select a VBA project:

Project(VistA 2FA Test BLANK.rdox)

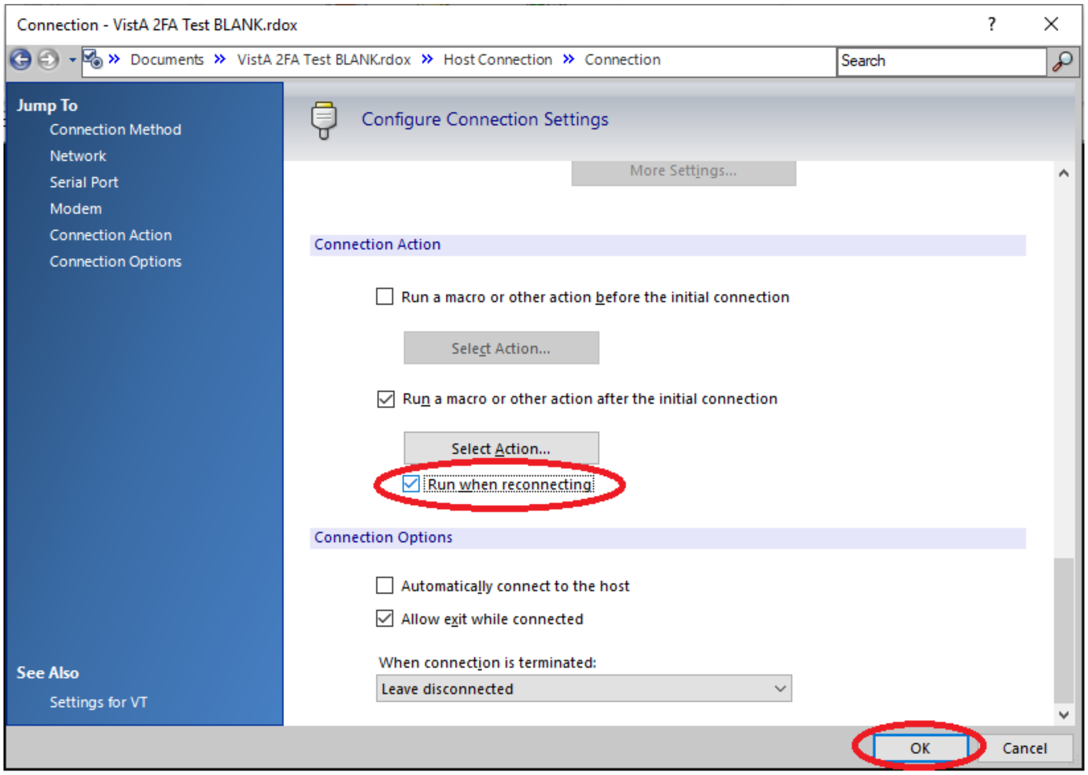
Select a macro:

INIhandler.Init
INIhandler.MoreVista
INIhandler.test2
SearchModule.search
XUSSOi.XUSSOProcess

Macro data:

4. When returned to the “Configure Connection Settings” form:
   a. Select the **Run when reconnecting** checkbox.
   b. Select **OK**, as shown in Figure 11.

Figure 11: Micro Focus® Reflection (v16)—Returned to the “Configure Connection Settings” Form: Select “Run when reconnecting”



Connection Action

☐ Run a macro or other action before the initial connection

☑ Run a macro or other action after the initial connection

☑ Run when reconnecting

Connection Options

☐ Automatically connect to the host

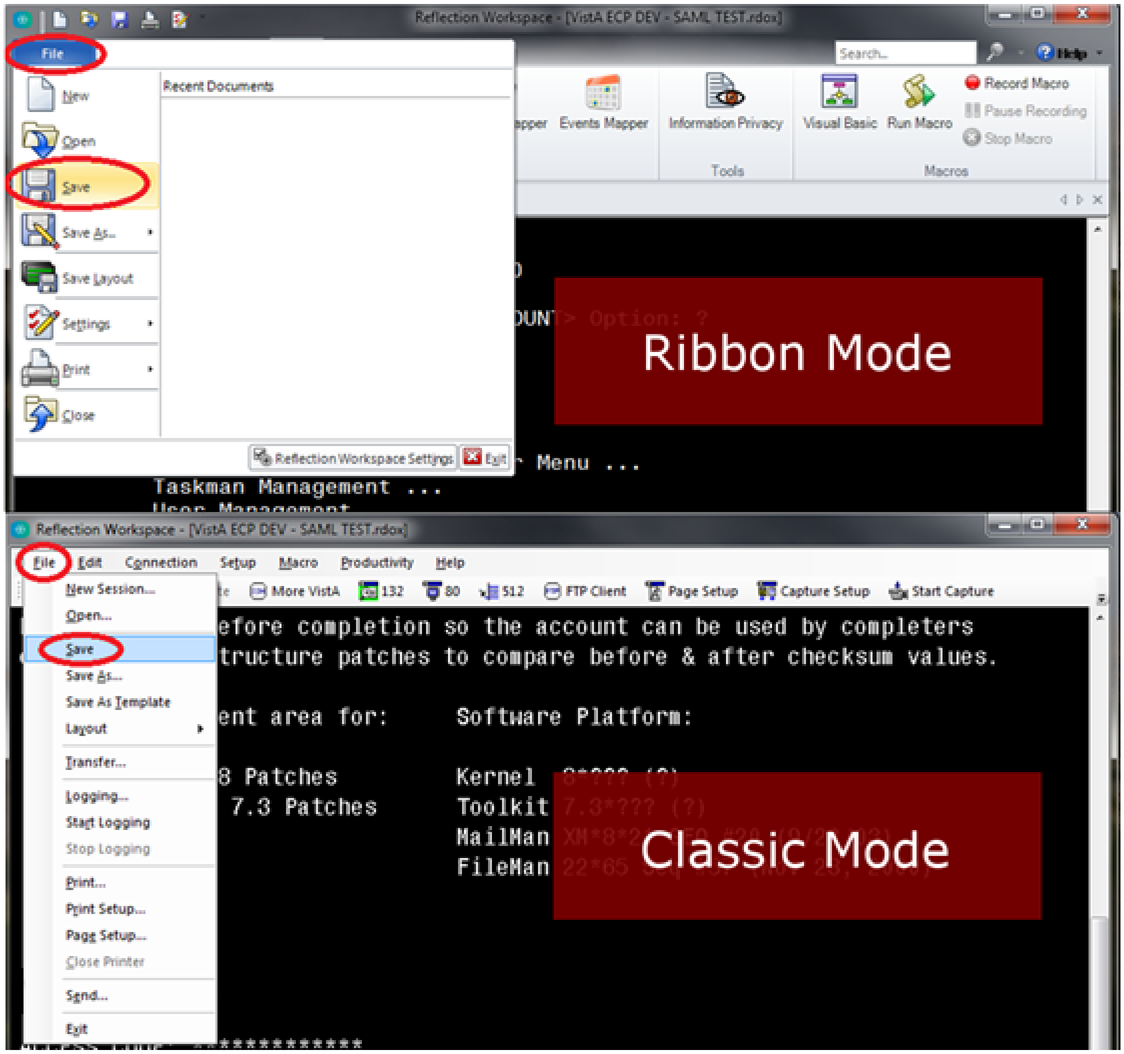
☑ Allow exit while connected

When connection is terminated: Leave disconnected

NOTE: The first Connection Action checkbox, **Run a macro or other action before the initial connection**, does ***not*** need to change. Some **.rdox** file configurations may have this box checked or unchecked, and that setting can be left as is. Only the third Connection Action checkbox, **Run when reconnecting**, which is circled in **RED** (Figure 11), needs to change as per these instructions.

5. Select the "**File**" menu and then "**Save**", as shown in Figure 12, to save the Micro Focus® Reflection terminal session.

Figure 12: Micro Focus® Reflection (v16)—Save Terminal Session File



```
OUNT> Option: ?
                                 Menu ...
 Taskman Management ...
 User Management
```

```
efore completion so the account can be used by completers
tructure patches to compare before & after checksum values.

ent area for:     Software Platform:

8 Patches         Kernel  8*??? (?)
 7.3 Patches      Toolkit 7.3*??? (?)
                  MailMan XM*8*2
                  FileMan 22*65
```

6. **Congratulations; you are done!** The **Micro focus® Reflection (v16)** terminal session is now enabled for 2-Factor Authentication (2FA).

   Repeat the configuration procedure for any remaining terminal sessions saved.

4.9 Installation Verification Procedure

To verify the installation of Kernel Patch XU*8.0*702 on the VistA M Server and within the Micro Focus® Reflection client software, do the following:

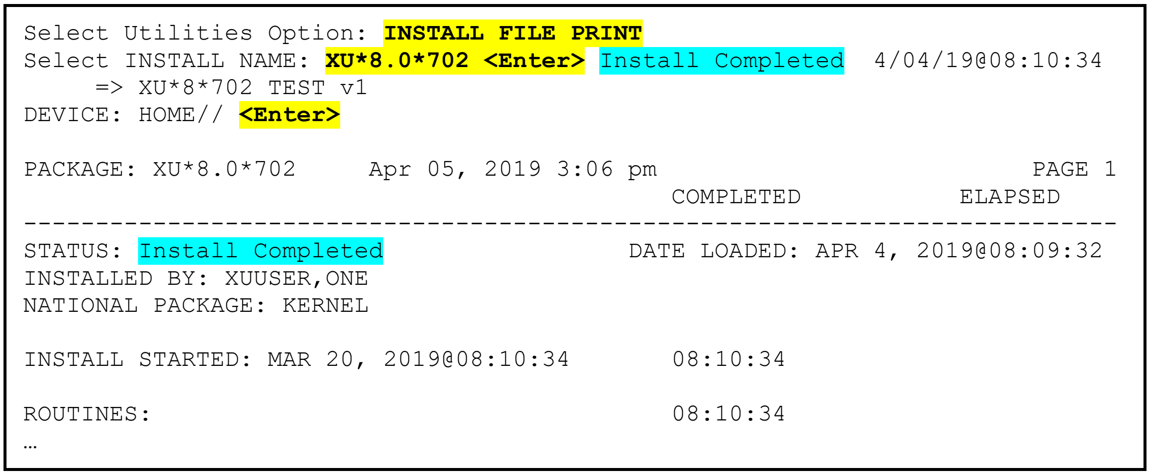
1. VistA M Server:

   Verify the installation using the KIDS **Install File Print** [XPD PRINT INSTALL FILE] option, located under the **Utilities** [XPD UTILITY] menu.

   a. At the "Select INSTALL NAME:" prompt, enter **XU*8.0*702**.

   b. Confirm that the STATUS field is "**Install Completed**", as shown in Figure 13:

Figure 13: Verify the Kernel Patch XU*8.0*702 Installation was Completed on the VistA M Server (Excerpt)



```
Select Utilities Option: INSTALL FILE PRINT
Select INSTALL NAME: XU*8.0*702 <Enter> Install Completed  4/04/19@08:10:34
     => XU*8*702 TEST v1
DEVICE: HOME// <Enter>

PACKAGE: XU*8.0*702     Apr 05, 2019 3:06 pm                         PAGE 1
                                             COMPLETED             ELAPSED
----------------------------------------------------------------------------
STATUS: Install Completed                 DATE LOADED: APR 4, 2019@08:09:32
INSTALLED BY: XUUSER,ONE
NATIONAL PACKAGE: KERNEL

INSTALL STARTED: MAR 20, 2019@08:10:34       08:10:34

ROUTINES:                                    08:10:34
…
```

2. Terminal Emulator Software on the Client Workstation:

   Micro Focus® Reflection (v16):

   Verify the configuration information matches what is shown in the "Set Connection Action" section.

CONGRATULATIONS: The installation of Kernel Patch XU*8.0*702 on the VistA M Server and client workstation is complete!

4.10 System Configuration

Kernel Patch XU*8.0*702 does *not* require any VistA M Server system configuration.

For client workstations, follow the configuration procedures listed in the "Set Connection Action" section.

4.11 Database Tuning

This section is not applicable. Kernel Patch XU*8.0*702 does *not* require any database tuning.

5 Back-Out Procedure

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

5.1 Back-Out Strategy

This section describes the back-out strategy for Kernel Patch XU*8.0*702, including the established time limits or other parameters that comprise the rationale for the 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 removal of data, files, and routines. In the case of future patches and releases, the back-out strategy would be dependent on the contents of the released functionality and could include restoration of file definitions, routines or data.

5.2 Back-Out Considerations

Back-out considerations would include impact on production Veterans Health Information Systems and Technology Architecture (VistA) end-user client workstations and impact on Wide Area Network (WAN).

Kernel Patch XU*8.0*702 is server software that involves installation in the following environment:

> Veterans Health Information Systems and Technology Architecture (VistA) M Servers

5.2.1 Load Testing

Not applicable for Kernel Patch XU*8.0*702. There are no resources or standards set for Kernel load testing, and a load testing environment is *not* available.

5.2.2 User Acceptance Testing

User Acceptance Testing (UAT) for the Kernel Patch XU*8.0*702 was performed by test sites and Software Quality Assurance (SQA) during the development and testing phase.

5.3 Back-Out Criteria

Kernel Patch XU*8.0*702 VistA M Server back-out criteria follow existing VistA back-out procedures. There are additional back-out criteria for configuration updates made to the existing **Micro Focus® Reflection (v16)** terminal emulator software.

5.4 Back-Out Risks

Kernel Patch XU*8.0*702 VistA M Server back-out risks are the same risks established with existing VistA back-out procedures. There are additional back-out risks for configuration updates made to the existing **Micro Focus® Reflection (v16)** terminal emulator software.

5.5 Authority for Back-Out

The authority for the need of back-out would reside with Veterans Health Administration (VHA), Office of Information and Technology (OIT), and Enterprise Program Management Office (EPMO) representatives.

5.6 Back-Out Procedure

Kernel Patch XU*8.0*702 installation updates the following routine on the VistA M Servers:

^XUS

There are no other VistA M Server software updates.

To back-out Kernel Patch XU*8.0*702 in VistA, and back-out configuration updates to the **Micro Focus® Reflection (v16)** terminal emulator software, do the following (in any order):

1. VistA M Server:
    a. Open the VistA MailMan message created during the "Backup a Transport Global" step of the patch installation process (i.e., *Kernel 8.0 and Kernel Toolkit 7.3 Systems Management Guide*, Section 23.7.8, "Backing Up Transport Globals").
    b. Follow the installation sequence (i.e., *Kernel 8.0 and Kernel Toolkit 7.3 Systems Management Guide*, Section 23.7.1, "Installation Sequence") to load and install a patch from a PackMan message. This installation restores the original (pre-patch) VistA routine.

2. Terminal Emulator Software on the Client Workstation: **Micro Focus® Reflection (v16)**
    a. Remove/Delete the event from the Event Mapper and the XUSSOi macro that were enabled during the configuration process performed in the "Set Connection Action" section.
    b. Use a backup copy of the modified terminal session (**.rdox**) file to copy over the updated one to remove the changes done in the configuration process.

5.7 Back-Out Verification Procedure

To verify the back-out of Kernel Patch XU*8.0*702, do the following:

1. VistA M Server:

   Verify that the last patch listed in line **2** of routine ^XUS is patch **659**, and *not* **702**.

   Select the First Line Routine Print option [XU FIRST LINE PRINT] to display the following:

   Figure 14: Verifying Back-Out of Kernel Patch XU*8.0*702 on the VistA M Server

```
Select Routine Tools Option: FIRST <Enter> Line Routine Print

PRINTS FIRST LINES

All Routines? No => NO

Routine: XUS
Routine: <Enter>
1 routine

(A)lpha, (D)ate ,(P)atched, OR (S)ize ORDER: A// <Enter>
Include line (2), Include lines 2&(3), (N)one: None//2
DEVICE: HOME// <Enter> TELNET PORT  Right Margin: 80// <Enter>

             FIRST LINE LIST   UCI: VISTA,ROU   04/05/2019
XUS       ;SFISC/STAFF - SIGNON ;09/22/15  09:25
          ;;8.0;KERNEL;**16,26,49,59,149,180,265,337,419,434,584,659**;Jul
           10, 1995

              1 ROUTINES
```

2. Terminal Emulator Software on the Client Workstation: **Micro Focus® Reflection (v16)**

   Attempt to make a client connection to VistA. If *not* prompted for 2-factor authentication (PIV and PIN), then you have successfully disabled/removed the macro.

6 Rollback Procedure

Rollback pertains to data. This section includes the specific steps to roll back to the previous state of the data and platform settings, if required. It includes the order of restoration for multiple interdependent systems.

Kernel Patch XU*8.0*702 does *not* export any data, so no database rollback is required.

6.1 Rollback Considerations

This section is not applicable. Kernel Patch XU*8.0*702 does *not* export any data, so there are no rollback considerations required.

6.2 Rollback Criteria

This section is not applicable. Kernel Patch XU*8.0*702 does *not* export any data, so there are no rollback criteria required.

6.3 Rollback Risks

This section is not applicable. Kernel Patch XU*8.0*702 does *not* export any data, so there are no rollback risks.

6.4 Authority for Rollback

Rollback *can* be authorized by system administrators once a problem has been identified. Office of Information and Technology (OIT) and Enterprise Program Management Office (EPMO) VistA Infrastructure (VI) Development Team should be informed immediately via a MailMan message sent to:

VA OIT PD Infrastructure Dev. & Doc. ***InfrastructureDevDoc@va.gov***

6.5 Rollback Procedure

This section is not applicable. Kernel Patch XU*8.0*702 release does *not* export any data, so no rollback procedure is required.

6.6 Rollback Verification Procedure

This section is not applicable. Kernel Patch XU*8.0*702 release does *not* export any data, so no rollback verification procedure is required.

7 Troubleshooting

7.1 Installation Notes

The installation is a two-part process that includes component installation in the following environments:

- VistA M Server
- Client Workstation

REF: For detailed installation instructions, see the Patch XU*8.0*702 Patch Description (PD) on FORUM and the Patch XU*8.0*702 Deployment, Installation, Back-Out, and Rollback Guide (DIBRG).

7.1.1 VistA M Server

Install Kernel Patch XU*8.0*702 KIDS Build on the VistA M Server. Patch XU*8.0*702 adds code to the signon routine **^XUS** to accept IAM SAML token for authentication using terminal emulator (roll-and-scroll) interface.

REF: For patch install instructions, see the XU*8.0*702 Patch Description (PD) on FORUM.

7.1.2 Client Workstation

Install the following components on all workstations:

- **Micro Focus® Reflection (v16)**—Terminal Emulator Software.
- **.rdox** File—Micro Focus® Reflection session file.
- **Visual Basic (VB) Script**—Used within Reflection, it calls the DLL and passes the SAML token to VistA.
- **DLL**—Performs the authentication with IAM and returns a SAML token.

The Visual Basic (VB) script and DLL enable Micro Focus Reflection 2-factor authentication into IAM, and using the received IAM SAML token to authenticate into VistA.

7.2 DLL and .rdox Session Files

Kernel Patch XU*8.0*702 project team created the **XUIAMSSOi.dll** file. This DLL performs the authentication with Identity and Access Management (IAM) and returns a Security Assertion Mark-up Language (SAML) token. Associated with the DLL file is the Micro Focus® Reflection session file known as a **.rdox** file, which is configured to connect to VistA using IAM PIV 2FA.

7.2.1 Phased Rollout of DLL and .rdox Files

The **XUIAMSSOi.dll** file *must* be pushed to all workstations; the Micro Focus Reflection **.rdox** file can be located on a centralized server.

7.2.1.1 DLL File

Client Tech will push out the **XUIAMSSOi.dll** file to all workstations. During the testing phase, Client Tech will push the **XUIAMSSOi.dll** file out to those workstations specified by test sites (e.g., ADPAC workstations). Upon national release, Client Tech will push the **XUIAMSSOi.dll** file out to *all* client workstations.

7.2.1.2 .RDOX File

The **.rdox** file is a configuration file with no set standard and can vary from region, VISN, facility, user group, and users. In addition, the **.rdox** file is hosted on a variety of platforms. Each functional group is responsible for updating the **.rdox** file baselines and redistributing them accordingly. Users will still be accessing Micro Focus® Reflection as they have prior to 2FA update. Information Technology Operations and Services (ITOPS) is responsible for communicating the upgrade as they implement the **.rdox** changes across the enterprise. The following is a list of ITOPS functional groups responsible for these changes:

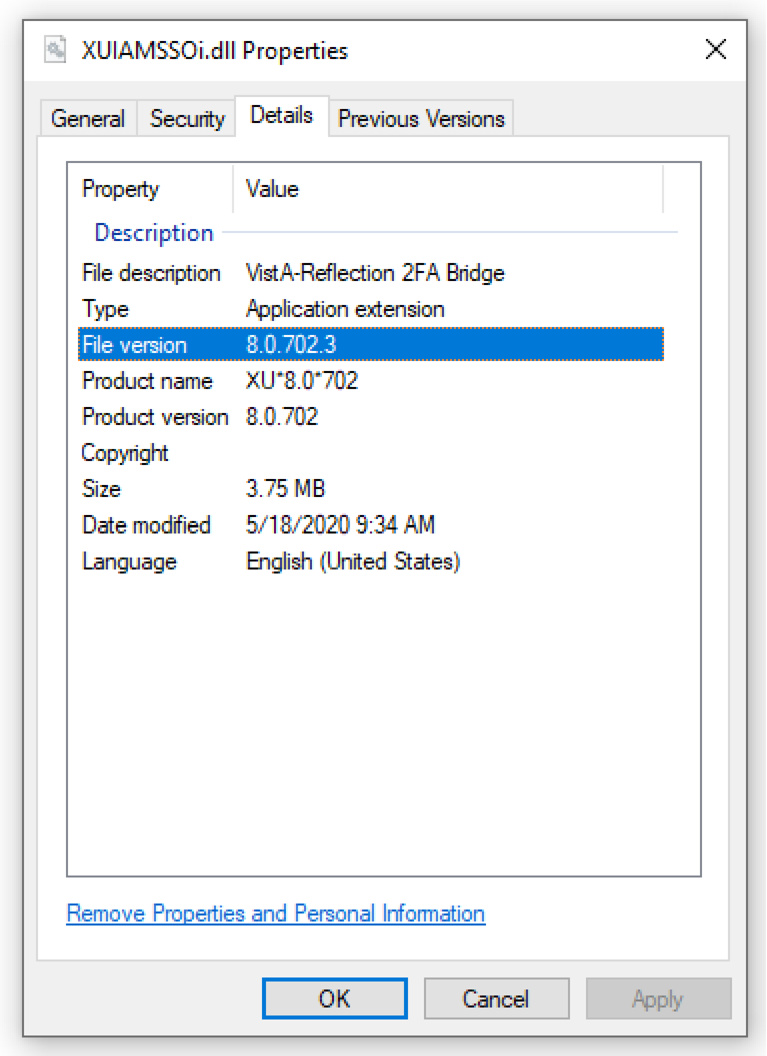
- **Client Desktop Work Station Support**—SO IO PS ESL Client Technologies Division
- **Citrix Virtual Desktop Support**—SO IO PS ESL Back Office Citrix Division
- **VistA Application Consolidated Server (VACS) support**—SO IO HBMC FO Applications Division

7.2.2 Verify Correct DLL File

Users should first verify their workstation has the correct and latest **XUIAMSSOi.dll** file installed on their workstation, since an old DLL file (i.e., 2017 beta version from cancelled patch XU*8.0*681) may be lurking on some workstations.

Figure 15 shows a screenshot of the metadata for the current and correct DLL. The current file was modified/built on **05/18/2020** and has an actual file version number of **8.0.702.3**.

Figure 15: XUIAMSSOi.dll File Properties Dialogue—Details Tab



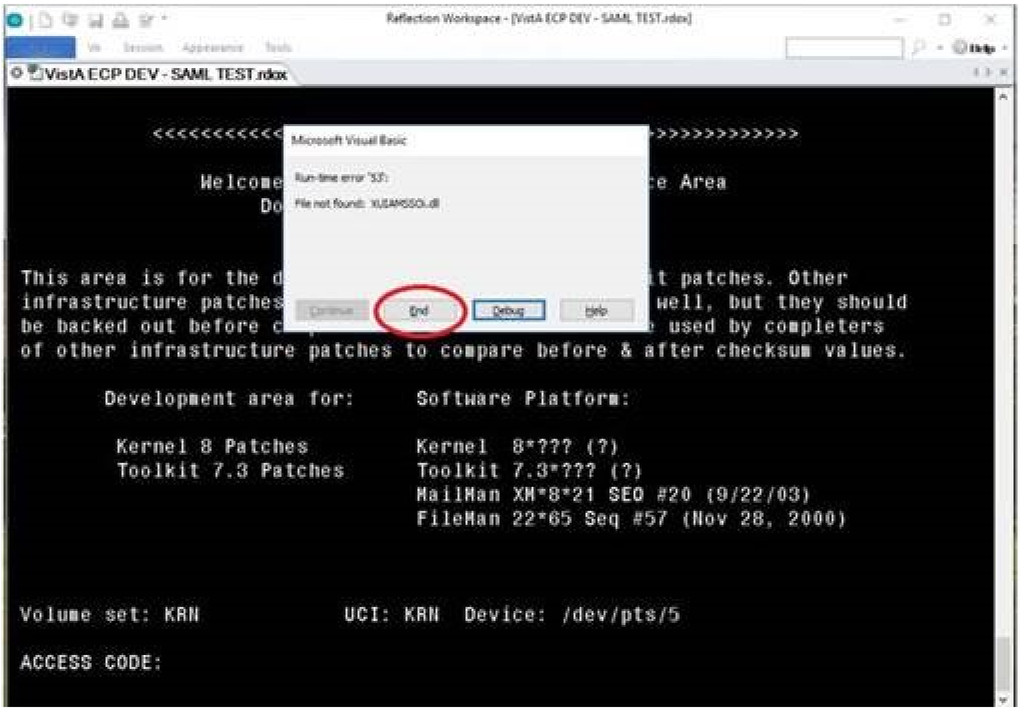
Property	Value
Description	
File description	VistA-Reflection 2FA Bridge
Type	Application extension
File version	8.0.702.3
Product name	XU*8.0*702
Product version	8.0.702
Copyright	
Size	3.75 MB
Date modified	5/18/2020 9:34 AM
Language	English (United States)

7.2.3 Missing DLL

Client Tech pushes the **XUIAMSSOi.dll** file to *all* machines. If a machine is *not* turned on at the time of the push, the **XUIAMSSOi.dll** file will *not* be installed on the user's machine.

If the **XUIAMSSOi.dll** file is *not* available when a user launches the (new) **.rdox** file, they will be alerted that the software *cannot* find the DLL file and then prompted for their Access/Verify codes. If the **XUIAMSSOi.dll** file is missing, the user receives an error message and should select **End**, then the ACCESS CODE prompt will be presented to login, as shown in Figure 16.

Figure 16: Microsoft Visual Basic Error—Missing XUIAMSSOi.dll File



Reflection Workspace - [VistA ECP DEV - SAML TEST.rdox]
VistA ECP DEV - SAML TEST.rdox
Microsoft Visual Basic
Continue
End
Debug
Help

Run-time error '53':

File not found: XUIAMSSOi.dll

```
             <<<<<<<<<<<                              >>>>>>>>>>>>>

                 Welcome                              e Area
                      Do

 This area is for the d                               t patches. Other
 infrastructure patches                               well, but they should
 be backed out before c                               used by completers
 of other infrastructure patches to compare before & after checksum values.

        Development area for:     Software Platform:

         Kernel 8 Patches         Kernel  8*??? (?)
         Toolkit 7.3 Patches      Toolkit 7.3*??? (?)
                                  MailMan XM*8*21 SEQ #20 (9/22/03)
                                  FileMan 22*65 Seq #57 (Nov 28, 2000)


 Volume set: KRN           UCI: KRN  Device: /dev/pts/5

 ACCESS CODE:
```

7.3 Micro Focus Connection Setting/Configuration

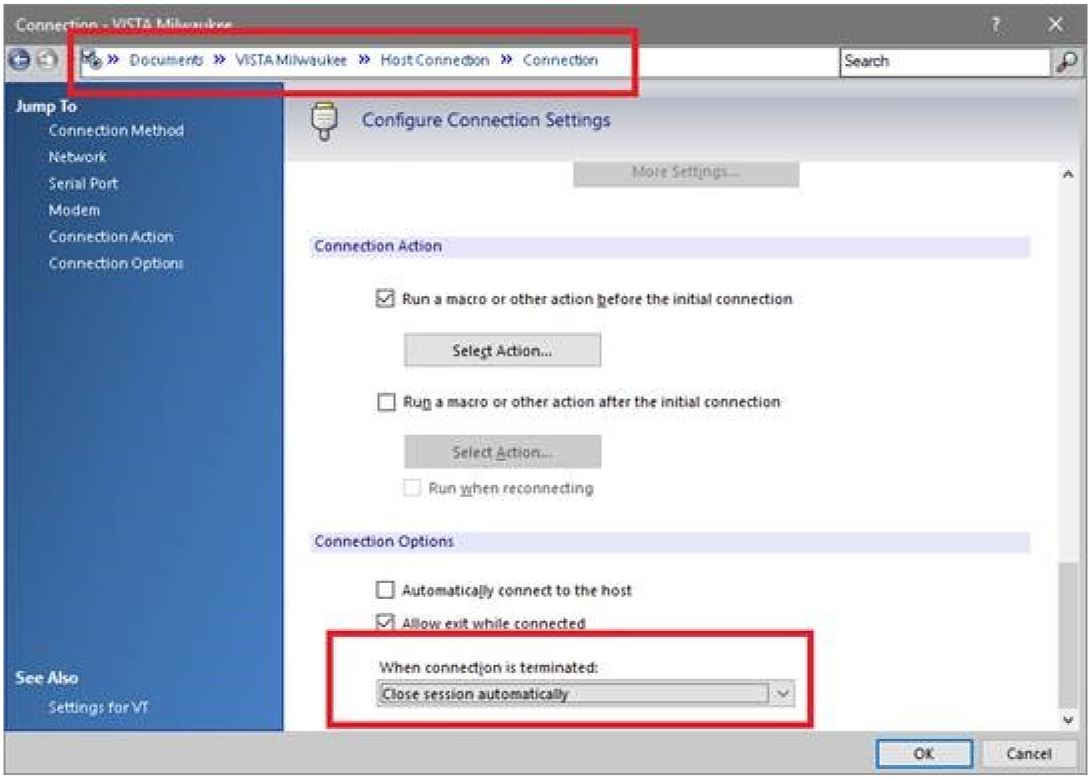
This section addresses the scenario when your Micro Focus® Reflection session window keeps closing on time out. The "**Leave disconnected**" connection setting keeps the Micro Focus® Reflection session window open if you time out; you would just need to press **Enter** to get prompted to reconnect.

To prevent your Micro Focus® Reflection session window from closing on time-out, do the following:

1. In **Micro Focus® Reflection (v16)**, do the following:
    a. Select **File**.
    b. Select **Settings**.
    c. Select **Host Connection**.
    d. Select **Configure Connection Settings**.

2. Scroll down to the “**Connection Options**” section at the bottom of the screen.
3. Locate the “**When Connection is Terminated:**” box.
4. Change the setting to “**Leave disconnected**.”

Figure 17: Micro Focus Reflection—Connections Page (Sample)



Connection - VISTA Milwaukee

Documents » VISTA Milwaukee » Host Connection » Connection

Configure Connection Settings

Connection Action

☑ Run a macro or other action before the initial connection

□ Run a macro or other action after the initial connection

□ Run when reconnecting

Connection Options

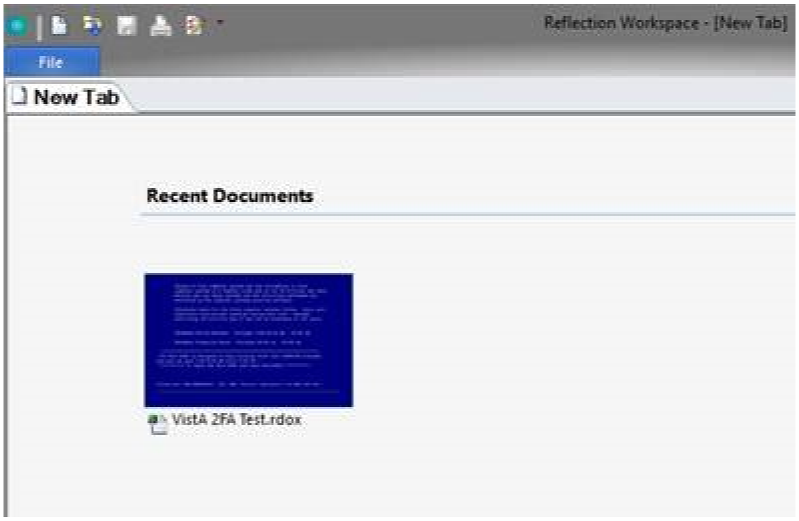
□ Automatically connect to the host

☑ Allow exit while connected

When connection is terminated: Close session automatically

If you fail to change this setting, when your session disconnects, the session window does *not* stay open and you do not have the option to press **Enter** to reconnect.. It automatically closes and goes straight to the Reflection **New Tab/Recent Documents**, as shown in Figure 18:

Figure 18: Micro Focus Reflection—New Tab Page



7.4 New User Signon Processes

This section describes the scenario when a new user (brand new Access/Verify codes) attempts to use the IAM **Link My Account** webpage to provision their PIV card with a VistA system. The results are that you *cannot* link your PIV to a VistA account if the Verify code is **NEW** or **EXPIRED**. Technically, a new or expired Verify code is the same thing, since assigning a new Verify code to a user just presets the code's expiration date back by several years; thus, forcing an entry of a new Verify code during the user's first login.

To provision new users and link their PIV to VistA, do the following:

1. Log onto VistA for the first time using assigned Access/Verify code pair:
    a. Use a PIV-enabled **.rdox** session file for Micro Focus® Reflection.
    b. Press **CANCEL** at the PIV card prompt.
    c. Press **OK** in the dialog that no SAML Token was received.
    d. Enter your initial Access/Verify codes provided and change your Verify code.

2. Use the IAM **Link My Account** website to provision your PIV card to the VistA system using your Access and Verify codes the user created in Step 1.

    REF: Follow the sample steps to provision your account in the "Link My Account" section.

3. Complete. Subsequent PIV logons to that VistA system would be functional and future Verify code expirations will be ignored when logging in using their PIV card.

7.4.1 Verify Code Expiration Bypass

VistA Kernel Patch XU*8.0*701 (released on 2/11/2020 and a compliance date of 2/18/2020) includes a logic fix to bypass the Verify code expiration check when successfully logged into VistA using PIV/SAML credentials. This allows Patch XU*8.0*702 and Micro Focus® Reflection to mimic the behavior of applications that use the Remote Procedure Call (RPC) Broker to connect to VistA (e.g., CPRS). The difference is that the RPC Broker applications do their connections through the Broker Transmission Control Protocol (TCP) port for communication, and with the Reflection method it is doing the communication through Secure Shell (SSH) and passing information to the VistA logon (**XUS**).

This Verify code expiration bypass also maintains the bypass if Active Directory (Username/Password) is used for SAML authentication by eliminating the check for Level of Assurance (LOA), since both Active Directory and PIV/PIN use STS SAML exchange for authentication and are both identified as SSO in the SAML certificate. The logic checks if the authentication contains "**SSO**," which allows the logic to work for both authentication methods and the ability to bypass the Verify code expiration check.

NOTE: Using the Active Directory credentials gives a credential Level of Assurance (LOA) a "**2**" rating, which is using typed codes for authentication as opposed to full 2-Factor Authentication (PIV Card and PIN), which would be a "**3**" rating for the LOA.

7.5 Link My Account

All Micro Focus® Reflection users need to use **Link My Account** (LMA) for associating your Personal Identification Verification (PIV) credentials to your VistA credentials.

NOTE: Users who do *not* have a PIV card or know their Personal Identification Number (PIN) number can cancel out of the PIV/PIN authentication process and choose to use either of the following authentication processes:

- Active Directory (AD) Username and Password—Possible if the user is logged into the workstation with AD Credentials and launching a 2FA configured **.rdox** session file.
- VistA Access/Verify code

From the **Link My Account Summary Sheet** site (VA Intranet site), follow the step-by-step instructions (see ServiceNow **KB0013359** [VA Intranet site]) to link your Provisioning Account and VistA Account. For example, to link/bind your PIV credentials to your VistA account(s) using the Computerized Patient Record System (CPRS) application, do the following:

1. Close all open applications and browser windows.
2. Open an Internet browser (e.g., Microsoft Internet Explorer) and navigate to the **IAM Provisioning Service Link VistA to User** task (VA Intranet site).

3. If you are *not* already logged into a Single Sign-On (SSO) application, the site prompts you to log in:

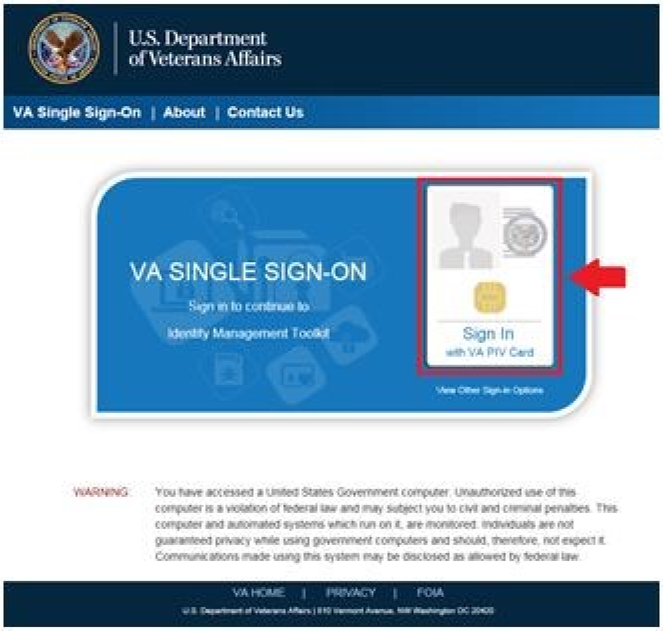
    a. Select the **PIV** card.

    b. Browse and select your authentication certificate from the displayed list. The certificate should read:

        Issuer: Veterans Affairs User CA B1

    c. Enter your **PIN**.

Figure 19: PIV VA Single Signon Page



U.S. Department of Veterans Affairs
VA Single Sign-On | About | Contact Us
VA SINGLE SIGN-ON
Sign in to continue to
Identity Management Toolkit
Sign In
with VA PIV Card
View Other Sign-in Options

WARNING: You have accessed a United States Government computer. Unauthorized use of this computer is a violation of federal law and may subject you to civil and criminal penalties. This computer and automated systems which run on it, are monitored. Individuals are not guaranteed privacy while using government computers and should, therefore, not expect it. Communications made using this system may be disclosed as allowed by federal law.

VA HOME | PRIVACY | FOIA
U.S. Department of Veterans Affairs | 810 Vermont Avenue, NW Washington DC 20420

If you receive the following errors after logging in, see the indicated knowledge article for resolution, and then continue to Step 4:

- Page Cannot Be Displayed: Verify the correct Internet Explorer settings, required by the VA for PIV use (see ServiceNow: **KB0013570** [VA Intranet site]).
- You are in compatibility mode and certain features in the TK will not work as expected: Turn off compatibility view (see ServiceNow: **KB0013476** [VA Intranet site]).

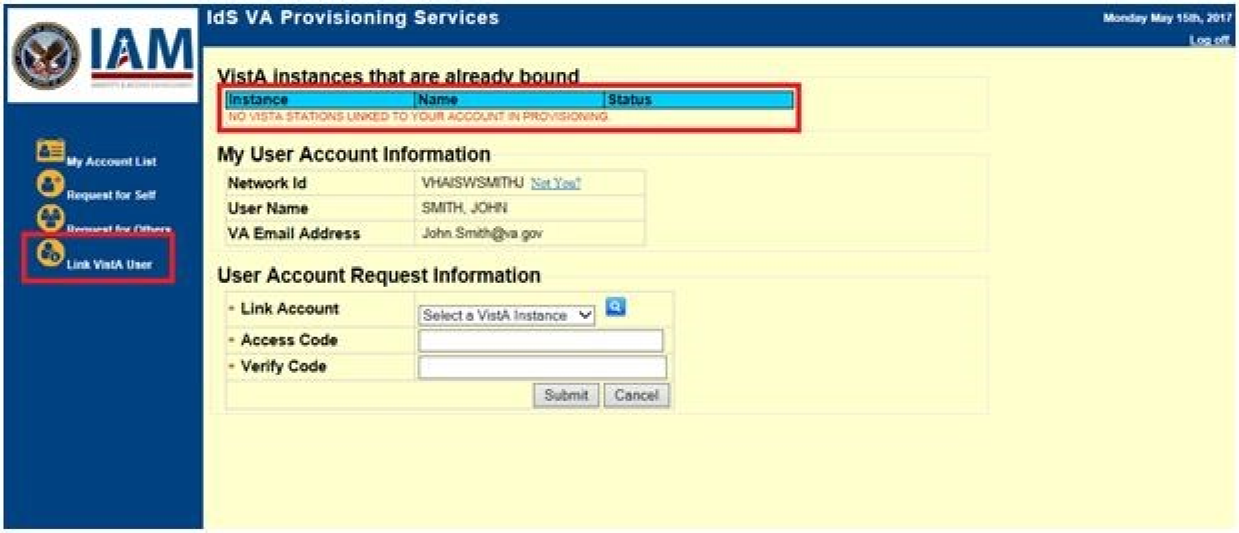
4. The "**Link VistA User**" page opens. If it does *not* open, select the **Link VistA User** menu option from the navigation links on the left of the page.

    After selecting **Link VistA User**, the following message is displayed:

    No VistA Stations Linked to your account in Provisioning

Users can ignore this message.

Figure 20: Ids VA Provisioning Services Page—Link VistA User



VistA instances that are already bound

Instance	Name	Status
NO VISTA STATIONS LINKED TO YOUR ACCOUNT IN PROVISIONING		

My User Account Information

Network Id	VHAISWSMITHJ Not You?
User Name	SMITH, JOHN
VA Email Address	John.Smith@va.gov

User Account Request Information

• Link Account	Select a VistA Instance
• Access Code	
• Verify Code	

5. Select a VistA instance:

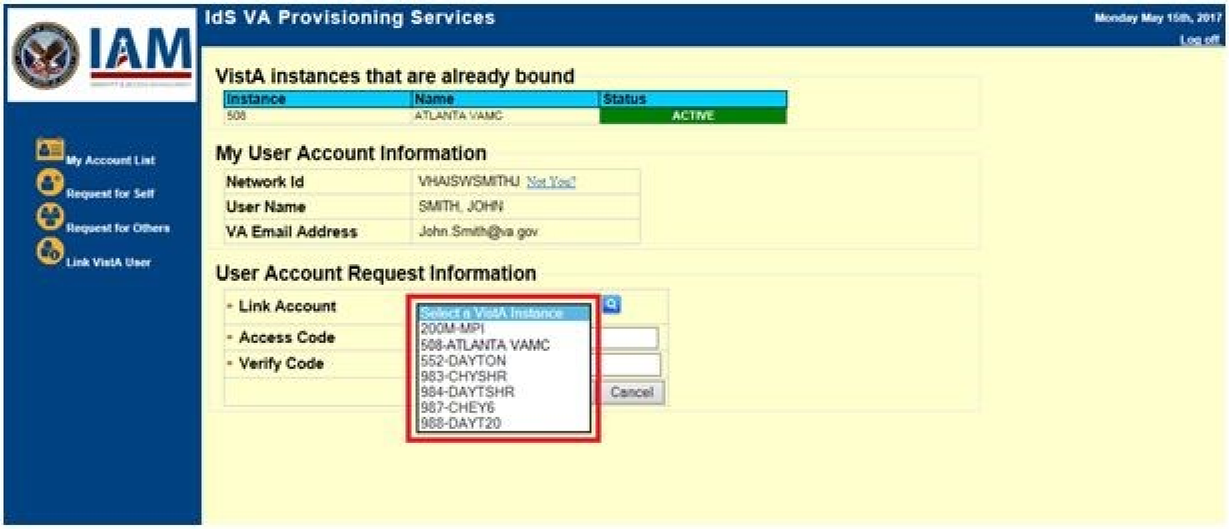
   a. Move to the “User Account Request Information” section.

   b. From the **Link Account** drop-down menu, select a VistA Instance.

NOTE: The VistA Instance list is sorted by station number. If station ends in a letter or contains a letter, select the parent station for your division. For example, if your station is **576A** or **576A5**, select **576** station number.

TIP: To jump to a station on the list, type the station number. The selection jumps to that spot in the drop-down menu.

Figure 21: Ids VA Provisioning Services Page—Selecting VistA Instance



VistA instances that are already bound

Instance	Name	Status
508	ATLANTA VAMC	ACTIVE

My User Account Information

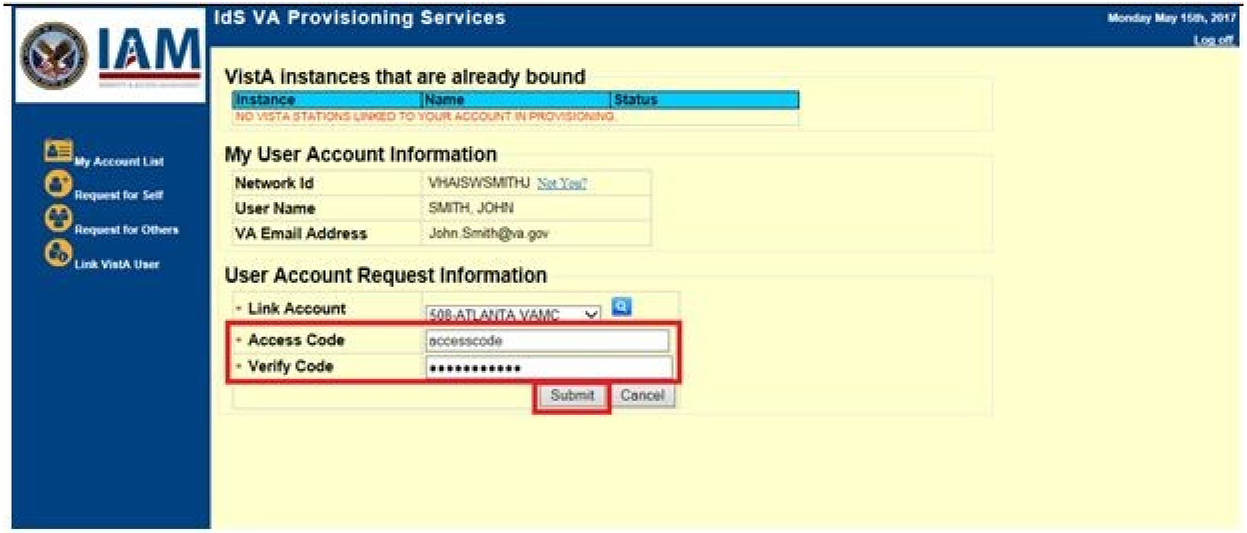
Network Id	VHAISWSMITHJ Not You?
User Name	SMITH, JOHN
VA Email Address	John.Smith@va.gov

User Account Request Information

- Link Account: Select a VistA Instance
  - 200M-MPI
  - 508-ATLANTA VAMC
  - 552-DAYTON
  - 983-CHYSHR
  - 984-DAYTSHR
  - 987-CHEY6
  - 988-DAYT20
- Access Code
- Verify Code

6. Enter your VistA/CPRS Access code and Verify code for that VistA instance, and then select **Submit**.

Figure 22: Ids VA Provisioning Services Page—Entering VistA Access and Verify Code



VistA instances that are already bound

Instance	Name	Status
NO VISTA STATIONS LINKED TO YOUR ACCOUNT IN PROVISIONING.		

My User Account Information

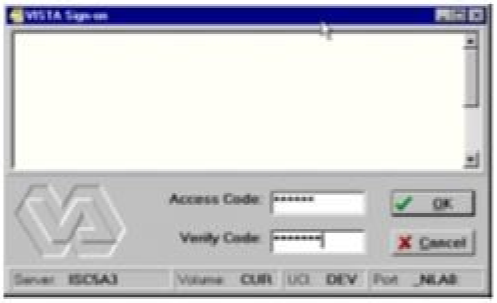
Network Id	VHAISWSMITHJ Not You?
User Name	SMITH, JOHN
VA Email Address	John.Smith@va.gov

User Account Request Information

Link Account	508-ATLANTA VAMC
Access Code	accesscode
Verify Code	••••••••••••

NOTE: Access code may also be known as VistA or CPRS code, and Verify code may also be knowns as VistA or CPRS password. It is the same information entered to log into VistA and CPRS.

Figure 23: VistA Sign-On Dialogue



Access Code: *******

Verify Code: ********

Server ISC6A3 Volume CUR UCI DEV Port _NLA8

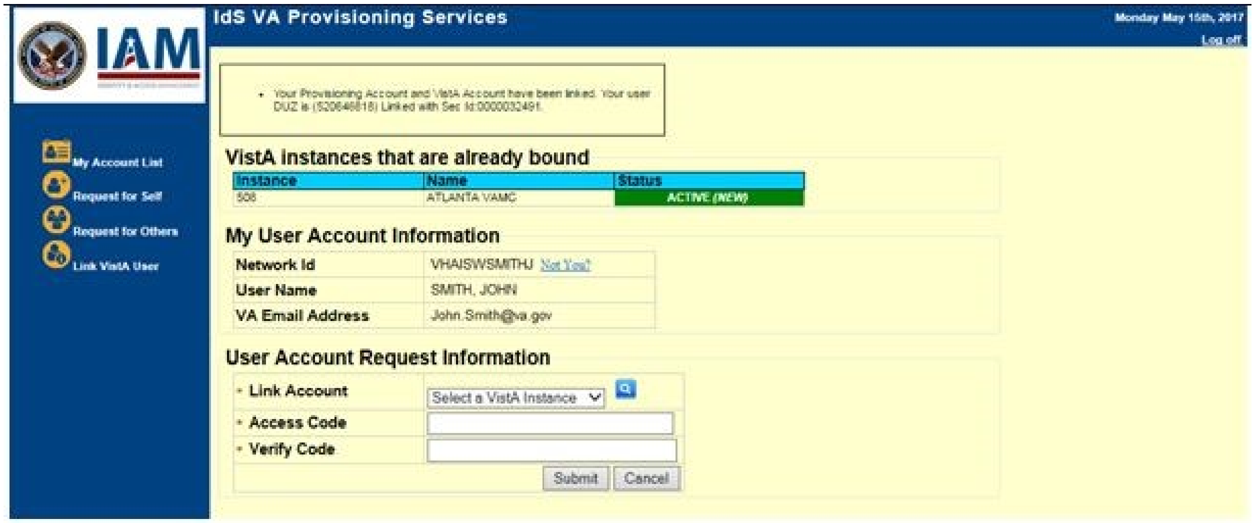
7. Once you select **Submit**, if the Access/Verify code was accepted and successful, the application returns the following message:

   > Your Provisioning Account and VistA Account have been linked. Your user DUZ is (*XXXXX*) Linked with Sec ID: *XXXXXXXX*.

   There may be a delay before the link is successful. If this happens, the application returns the message: Your request has been staged. You will receive an email once the linkage is complete. You can check back to see if the link is complete. Once the link is complete, you will see the connected instance as shown in Figure 24.

8. Verify the newly linked VistA account in the list of Instance Names.

Figure 24: Ids VA Provisioning Services Page—Verifying VistA Instance Selection



- Your Provisioning Account and VistA Account have been linked. Your user DUZ is (520646818) Linked with Sec Id:0000032491.

VistA instances that are already bound

Instance	Name	Status
508	ATLANTA VAMC	ACTIVE (NEW)

My User Account Information

Network Id	VHAISWSMITHJ Not You?
User Name	SMITH, JOHN
VA Email Address	John.Smith@va.gov

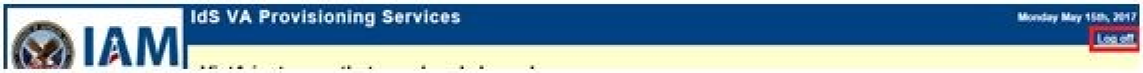
User Account Request Information

Link Account	Select a VistA Instance
Access Code	
Verify Code	

9. If you have access to more than one VistA account, repeat Steps 5-7 until all VistA accounts have been linked.

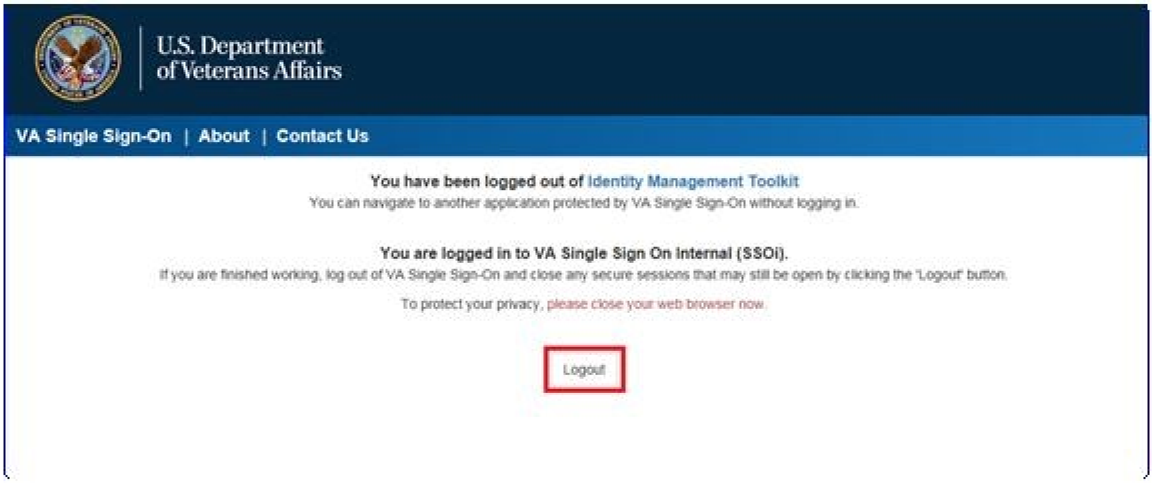
10. Click **Log off** at the top right of the page to go to the IAM SSOi session page.

Figure 25: Ids VA Provisioning Services Page—Logout



11. Click **LOGOUT** at the bottom of the page to close IAM SSOi session.

Figure 26: IAM SSOi Session Page—Logout



You have been logged out of Identity Management Toolkit
You can navigate to another application protected by VA Single Sign-On without logging in.

You are logged in to VA Single Sign On Internal (SSOi).
If you are finished working, log out of VA Single Sign-On and close any secure sessions that may still be open by clicking the 'Logout' button.

To protect your privacy, please close your web browser now.

12. You have successfully linked your PIV credentials to your VistA account(s)! After linking your PIV to VistA credentials, you will select your certificate and enter your PIN to access Micro Focus Reflection.

7.6 Technical Support

For help in troubleshooting PIV IAM 2FA signon issues, please consult the following:

- **PIV Issues**—Contact your local PIV Office PIV Badge Office, Enterprise Service Desk (ESD) Support: **1-855-673-4357** (TTY **844-224-6186**), or email **PIVHelpRequests@va.gov**.
- **VistA account or Access/Verify Issues**—Contact your local Information Technology (IT) support or Enterprise Service Desk (ESD) Support: **1-855-673-4357** (TTY **844-224-6186**).
- **Link my Account Issues**—Contact the IAM Help Desk via Enterprise Service Desk (ESD):
  - Phone: **1-855-673-4357**.
  - TTY (Hearing Impaired Only): **1-844-224-6186**.

These lines are available **24** hours a day, **7** days a week.

- **DLL Issues—**If missing the **XUIAMSSOi.dll** file, send a ServiceNow (SNOW) ticket to the Client Tech **REDACTEDCLIENTTECH.TRIAGE** group.
- **.rdox File Issues—**Support entity depends on where the file is hosted:
  - **Client Desktop Work Stations Support**—SO IO PS ESL Client Technologies Division**:**
    - **Technical Issues:** Please submit ticket into Service Now (SNOW) and assign to your Client Tech SNOW support team or: **REDACTEDClientTech.Triage**
    - **Operational Questions:** Can be emailed to **OIT ITOPS IO PS Client Tech Division Chiefs**
  - **Citrix Application Host Support**—SO IO PS ESL Back Office Citrix Division:
    - **Technical Issues:** Please submit ticket into Service Now (SNOW) and assign to **REDACTEDBackOffice.Citrix**
    - **Operational Questions**: Can be emailed to OIT ITOPS IO PS ESL Back Office Citrix Leadership **REDACTED**
  - **VistA Application Consolidated Server (VACS; Gold Star)** and/or **Network Application Share Server Support**—SO IO HBMC FO Applications Division:
    - **Technical issues Support:** Please submit a Service Now (SNOW) ticket to the VAD Clinical SNOW support group (**1**, **2**, **3**, or **4**) that coincides with your former region:
      - **IO.HBMC.FO.APP.VADKERNELassign1**
      - **IO.HBMC.FO.APP.VADKERNELassign2**
      - **IO.HBMC.FO.APP.VADKERNELassign3**
      - **IO.HBMC.FO.APP.VADKERNELassign4**
    - Operational Questions: Can be emailed to: **OIT ITOPS SO IO HBMC APP Vista Apps Supervisors**; **REDACTED**

7.7 Issues and Concerns

Table 11 lists any known Micro Focus® Reflection software limitations or issues with regard to PIV IAM 2FA:

Table 11: Known Issues

Issue	Resolution	Comments
Restart Session [XURELOG] Routine: In VistA roll-and-scroll, after signing in with 2FA, if you run the Restart Session [**XURELOG**] routine, it does *not* trigger you to sign in using 2FA. The only option is to re-sign in using Access/Verify (A/V) codes.	User *must* log out and log back in; restart your session.	Unfortunately, there is no automatic workaround for this issue. Once the user is logged into VistA, the Reflection macro is stopped and no longer listening to any triggers. It is only when the user is disconnected and reconnects, the macro starts up again. So, with something like **XURELOG** that logs off and on (but does *not* disconnect), only the A/V codes are available.
Mismatched .rdox and .ini Files (used with the INIHandler macro already in the field): Modifying and renaming a **.rdox** file without properly renaming the associated **.ini** file to match.	User *must* make sure the renamed **.rdox** file has a an associated **.ini** file with the same name.	If a standard **.rdox** file is being modified with the script and given a different name, then the associated **.ini** file that goes along with it needs to be copied and given the same name. This should *not* be an issue if the modified **.rdox** file has the same name as the original **.rdox** file. For example: If you were to modify the existing file **FILE1.rdox** and named the modified file **FILE2.rdox**; you would then need to copy the **FILE1.ini** and name the copy **FILE2.ini**, so both file names would still match and stay in synch. Alternatively, if you first renamed the existing **FILE1.rdox** file to **FILE1_old.rdox** and named the modified file to **FILE1.rdox**, then you would *not* need to copy and rename the existing **FILE1.ini** file, since both names would still match and be in synch.