Kernel 8.0; Patch XU*8.0*702
Quick Reference Guide

This document helps orient the end-user on how to work with the tools and components updated with Veterans Health Information Systems and Technology Architecture (VistA) Kernel Patch XU*8.0*702. It is a quick reference guide that includes links to additional resources.

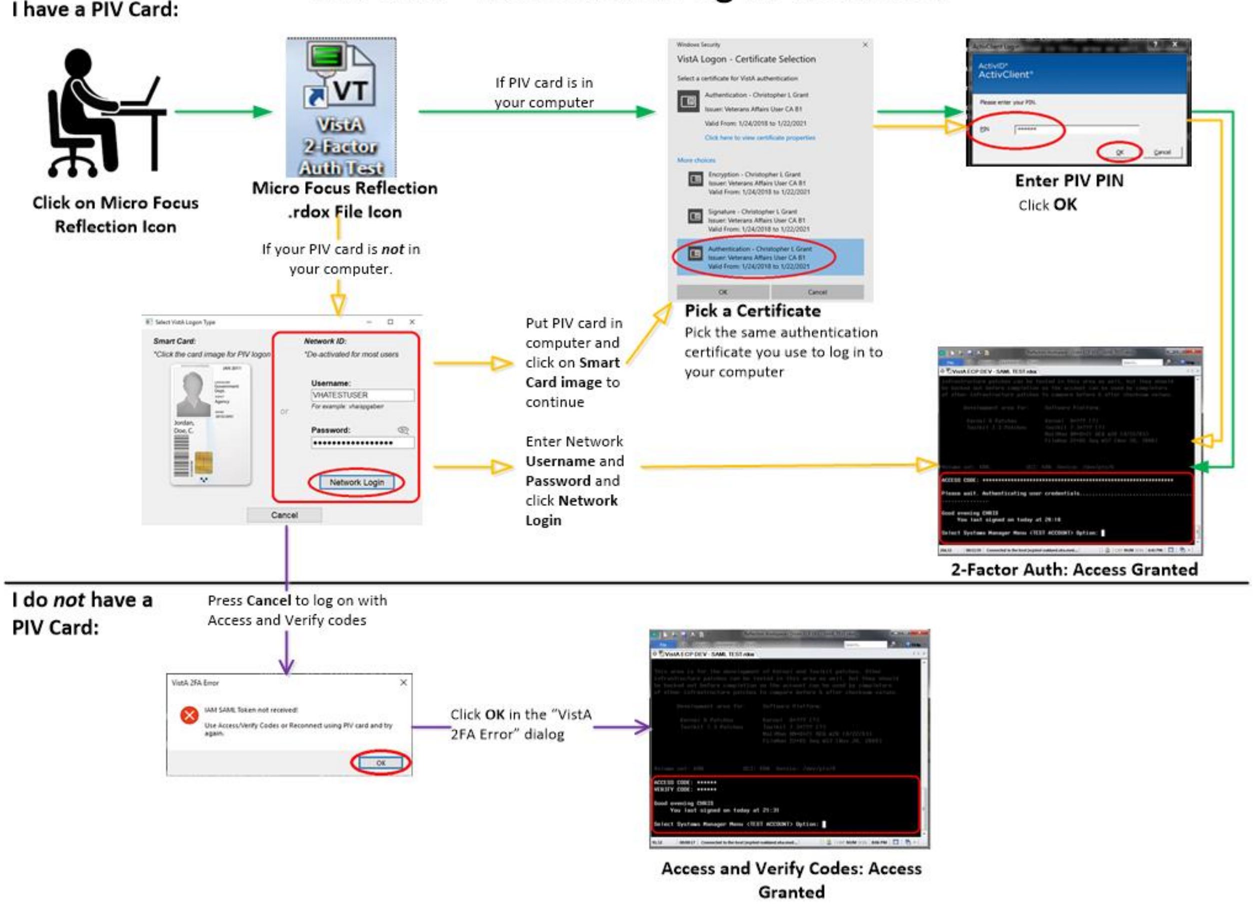
NOTE: Sites should update their "New Employee Orientation" materials to include an explanation about managing Access/Verify codes, Personal Identification Verification (PIV), 2-Factor Authentication (2FA), and Link-My-Account activities.

Since each site may have their own protocol for communicating to end-users, this document helps provide guidance that could be used in a variety of ways.

The intended audience for this document includes the following site personnel:

- Area Managers
- Automated Data Processing Application Coordinator (ADPACS)
- Chief Health Informatics Officer (CHIO)

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.
Windows Security
Click here to view certificate properties
More choices
OK
Cancel
ActivID ActivClient
PIN
OK
Cancel
Enter PIV PIN
Click **OK**
Pick a Certificate
Pick the same authentication certificate you use to log in to your computer
Select VistA Logon Type
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
OK
Click **OK** in the "VistA 2FA Error" dialog
Access and Verify Codes: Access Granted

VistA Logon - Certificate Selection

Select a certificate for VistA authentication

Authentication - Christopher L Grant
Issuer: Veterans Affairs User CA B1
Valid From: 1/24/2018 to 1/22/2021

Encryption - Christopher L Grant
Issuer: Veterans Affairs User CA B1
Valid From: 1/24/2018 to 1/22/2021

Signature - Christopher L Grant
Issuer: Veterans Affairs User CA B1
Valid From: 1/24/2018 to 1/22/2021

Authentication - Christopher L Grant
Issuer: Veterans Affairs User CA B1
Valid From: 1/24/2018 to 1/22/2021

Please enter your PIN.

PIN: ******

Smart Card:
*Click the card image for PIV logon

Network ID:
*De-activated for most users

Username: VHATESTUSER
For example: vhaispgaber

Password: ****************

IAM SAML Token not received!

Use Access/Verify Codes or Reconnect using PIV card and try again.

```
ACCESS CODE: ******
VERIFY CODE: ******

Good evening CHRIS
     You last signed on today at 21:31

Select Systems Manager Menu <TEST ACCOUNT> Option:
```

Prerequisites

Make sure you have the following tools and access available:

- **PIV Card Reader—**Confirm that you have a working Smart Card reader (which may be on the keyboard, on the side of a laptop, or separate).
- **PIV Card—**Make sure your PIV card is active and up-to-date.
- **Personal Identification Number (PIN)—**Know your PIV card PIN.
- **Link My Account—**For first time user, make sure you link your VistA credentials to your PIV credentials using the Identity and Access Management (IAM) **Link My Account** application.
- **DLL File—**Performs the authentication with IAM and returns a Security Assertion Mark-up Language (SAML) token. You do *not* need to download this file; Client Tech pushes this file to all workstations.

  REF: If you get a DLL error, see the "Missing DLL" section in the *Patch XU*8.0*702 Deployment, Installation, Back-Out, and Rollback (DIBR) Guide*.
- **.rdox File—**Micro Focus® Reflection [v16] terminal emulator software session file. Information Technology Operations and Services (ITOPS) configures this file for you and makes it available via the Region 2 Gold Star Test folder.

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.
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.

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.

Users that do *not* have a PIV card or know their Personal Identification Number (PIN) number may cancel out of the PIV/PIN authentication process and continue to use your 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.

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 **IO.PS.FO.CLIENTTECH.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: **IO.PS.FO.ClientTech.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 **IO.PS.FO.BackOffice.Citrix**
        - **Operational Questions**: Can be emailed to OIT ITOPS IO PS ESL Back Office Citrix Leadership OITITOPSSOIOPSESLBackOfficeCitrixLeadership@va.gov

- **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**

References

Please refer to the following internal VA links and documents for additional information with regard to Patch XU*8.0*702 project team, 2FA, PIV, and IAM Link My Account:

- Reflections PIV Project SharePoint (VA Intranet site 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 (DIBR) Guide*
- *Patch XU*8.0*702 Quick Reference Guide* (this manual)
- *Patch XU*8.0*702 VistA-Reflection PIV 2-Factor Authentication Test Plan* (VA Intranet site)