OneVA Drug Restrictions
PSS*1.0*239

Deployment, Installation, Back-Out, and Rollback Guide

July 2024

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
July 2024	1.0	Initial Version	Booz Allen Hamilton

Table of Contents

1. Introduction

This document describes how to deploy and install the OneVA Drug Restriction Enhancements patch PSS*1.0*239, as well as how to back-out the product and rollback to a previous version or data set. This document is a companion to the project charter and management plan for this effort.

1.1. Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the OneVA Drug Restriction Enhancements project will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule.

1.2. Dependencies

PSS*1*252 must be installed BEFORE PSS*1.0*239

1.3. Constraints

This patch is intended for a fully patched VistA system.

2. Roles and Responsibilities

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	Department of Veterans Affairs (VA) Office of Information and Technology (OIT), Health Services Portfolio (HSP) Patient Care Services (PCS), and Program Management Office (PMO)	Deployment	Plan and schedule deployment	Planning
2	Health Product Support and Field Operations (FO)	Deployment	Determine and document the roles and responsibilities of those involved in the deployment	Planning
3	Field Testing (Initial Operating Capability-IOC), Health Product Support Testing & Veteran-Focused Integration Process (VIP) Release Agent Approval	Deployment	Test for operational readiness	Testing
4	Application Coordinators	Release Deployment	Application Coordinators release patches	Deployment
5	HSP PCS and FO	Deployment	Execute deployment	Deployment

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
6	OIT, Development, Security, and Operations (DevSecOps) Infrastructure Operations (IO) and Individual Veterans Administration Medical Centers (VAMCs)	Installation	Plan and schedule installation	Deployment
7	Facility Area Manager and OIT support, which may be local or regional	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)	Deployment
8	VA OIT, HSP PCS, and the Development Team	Post Deployment	Hardware, Software and System Support	Warranty

3.   Deployment

The deployment is planned as a national general availability release. The scheduling of test/mirror installs, testing, and the deployment to production will be at the sites' discretion.

A national release is planned after testing has been successfully completed at initial operating capability (IOC) test sites.

Deployment will be performed by the local or regional OIT staff and supported by team members from these organizations: FO and Enterprise Operations. Other teams may provide additional support.

3.1.   Timeline

The deployment and installation is scheduled to run for 31 days, as depicted in the master deployment schedule for Pharmacy Operational Updates.

Table 2: Timeline

Task	Start	Finish
National Release	7/23/2024	7/23/2024
Compliance Period	7/24/2024	8/23/2024

3.2.   Site Readiness Assessment

This section discusses the locations that will receive the deployment of the OneVA Drug Restriction Enhancements patch PSS*1.0*239.

3.2.1.   Deployment Topology (Targeted Architecture)

This release will be deployed to all VistA instances.

3.2.2. Site Information (Locations, Deployment Recipients)

The IOC test sites are:

- Miami VA Healthcare System
- Minneapolis VA Healthcare System
- VA New Jersey Healthcare System

Upon national release all VAMCs are expected to install this patch prior to or on the compliance date. The software will be distributed through FORUM.

3.2.3. Site Preparation

The OneVA Drug Restriction Enhancements release does not require any special preparation by the site prior to deployment.

Table 3: Site Preparation

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
N/A	N/A	N/A	N/A	N/A

3.3. Resources

3.3.1. Facility Specifics

The OneVA Drug Restriction Enhancements release does not require any special or specific resources other than a functional VistA system.

Table 4: Facility-Specific Features

Site	Space/Room	Features Needed	Other
N/A	N/A	N/A	N/A

3.3.2. Hardware

The OneVA Drug Restriction Enhancements release does not require any special or specific resources other than a functional VistA system.

Table 5: Hardware Specifications

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

3.3.3. Software

The OneVA Drug Restriction Enhancements release does not require any special or specific resources other than a functional VistA system.

Table 6: Software Specifications

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

3.3.4. Communications

For national release, sites will receive communication that the release has occurred, which will normally be an Action Item or Bulletin.

Sites will use their internal communications to let their users know about upcoming installations and any associated downtime. This is critical as users can often slow the installation process if they are on the system while installers are trying to get the software installed.

Clinical Application Coordinators (CACs), installers, and other site personnel (as determined by the site) will need to coordinate installation dates and times. In addition, other support personnel may need to be consulted – such as the Citrix support, Client Technologies (if required).

3.3.4.1. Deployment/Installation/Back-Out Checklist

The Release Management team will deploy patch PSS*1.0*239, which is tracked in the National Patch Module (NPM) in FORUM, nationally to all VAMCs. FORUM automatically tracks the patches as they are installed in the different VAMC production systems as described in the previous section. One can run a report in FORUM to identify when the patch was installed in the VistA production at each site, and by whom. A report can also be run, to identify which sites have not installed the patch in their VistA production system as of that moment in time.

Therefore, this information does not need to be manually tracked. The table is included below if manual tracking is desired.

Table 7: Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual who completed task
Deploy	TBD	TBD	TBD
Install	TBD	TBD	TBD
Back-Out	TBD	TBD	TBD

4. Installation

4.1. Pre-installation and System Requirements

This release should not require any pre-installation changes to the current environment.

4.2. Platform Installation and Preparation

Below is a list of the applications involved in this project along with their patch numbers. The order of installation is not important.

APPLICATION/VERSION	PATCH
PHARMACY DATA MANAGEMENT v7.0	PSS*1.0*239

The VistA patches in this release should be installed into the test/mirror/pre-prod accounts before the production account as is the normal VistA patch installation standard convention. When installing any VistA patch, sites should utilize the option "Backup a Transport Global" in order to create a backup message of the "Build (including routines)" exported with this patch. Pre and Post-installation checksums are found in the Patch Description and in FORUM NPM.

4.3. Download and Extract Files

Download and extract files are not applicable for this VistA patch.

4.4. Database Creation

Database creation is not applicable for this VistA patch.

4.5. Installation Scripts

Installation scripts are not applicable for this VistA patch.

4.6. Cron Scripts

Cron scripts are not applicable for this VistA patch.

4.7. Access Requirements and Skills Needed for the Installation

To install this VistA patch, the patch installer must be an active user on the VistA system and have access to the VistA menu option "Kernel Installation & Distribution System" [XPD MAIN] and have VistA security keys XUPROG and XUPROGMODE. Knowledge on how to install VistA patches using the items on this menu option is also a required skill.

4.8. Installation Procedure

Installation Instructions:

1. Choose the PackMan message containing this build. Then select the INSTALL/CHECK MESSAGE PackMan option to load the build.

2. From the Kernel Installation and Distribution System Menu, select the Installation Menu. From this menu,

   a. Select the Verify Checksums in Transport Global option to confirm the integrity of the routines that are in the transport global. When prompted for the INSTALL NAME enter the patch name, PSS*1.0*239.

   b. Select the Backup a Transport Global option to create a backup message. You must use this option and specify what to backup: the entire Build or just Routines.

The backup message can be used to restore the routines and components of the build to the pre-patch condition.

    i.   At the Installation option menu, select Backup a Transport Global.

    ii.   At the Select INSTALL NAME prompt, enter your build PSS*1.0*239.

    iii.   When prompted for the following, enter "R" for Routines or "B" for Build.

Select one of the following:

        B   Build

        R   Routines

Enter response: Build

    iv.   When prompted "Do you wish to secure this message? NO//", press \<enter\> and take the default response of "NO".

    v.   When prompted with, "Send mail to: Last name, First Name", press \<enter\> to take default recipient. Add any additional recipients.

    vi.   When prompted with "Select basket to send to: IN//", press \<Enter\> and take the default IN mailbox or select a different mailbox.

c.   You may also elect to use the following options:

    i.   Print Transport Global - This option will allow you to view the components of the Kernel Installation and Distribution System (KIDS) build.

    ii.   Compare Transport Global to Current System - This option will allow you to view all changes that will be made when this patch is installed. It compares all of the components of this patch, such as routines, data dictionaries (DDs), templates, etc.

d.   Select the Install Package(s) option and choose the patch to install.

    i.   If prompted 'Want KIDS to Rebuild Menu Trees Upon Completion of Install? NO//', answer 'NO'.

    ii.   When prompted 'Want KIDS to INHIBIT LOGONs during the install? NO//', answer 'NO'

    iii.   When prompted 'Want to DISABLE Scheduled Options, Menu Options, and Protocols? NO//', answer 'NO'.

    iv.   When prompted 'DEVICE:' enter an output device for the installation.

    v.   If prompted 'Delay Install (Minutes): (0 - 60): 0//', answer 0.

4.9.   Installation Verification Procedure

Successful installation can be verified by reviewing the first two lines of the routines contained in the patch. The second line will contain the patch number in the [PATCH LIST] section.

The option Calculate and Show Checksum Values [XTSUMBLD-CHECK] can be run to compare the routine checksums to what is documented in the patch.

4.10. System Configuration

System configuration is not applicable for this VistA patch.

4.11. Database Tuning

Database tuning is not applicable for this VistA patch.

5. Back-Out Procedure

Back-Out pertains to a return to the last known good operational state of the software and appropriate platform settings. In the event of a catastrophic failure, the Area Manager may make the decision to backout the patch and rollback any necessary database changes. The Area Manager, working with site personnel, tier 2 product support, and the development team will be involved in the decision. However, the Area Manager will make the final decision.

5.1. Back-Out Strategy

Back-out Procedures are only needed if there are major problems (examples include the KIDS notice of incompletion or hard errors) resulting from the installation of this patch. You must have concurrence from HSP PCS support before a back-out can occur. Enter a ServiceNow ticket to obtain this concurrence.

Although it is unlikely due to care in collecting approved requirements, Software Quality Assurance (SQA) review and multiple testing stages (Unit testing, Component Integration Testing, User Acceptance Testing) a back-out decision due to major issues with this patch could occur during site Mirror Testing, Site Production Testing or after National Release to the Field. The strategy would depend upon the stage of testing when the decision is made. If during Site Production Testing, unless the patch produces catastrophic problems, the normal VistA response would be for a new version of the test patch correcting defects to be produced, retested and upon successfully passing development team testing would be resubmitted to the site for testing. If the defects were not discovered until after national release but during the warranty support period, the patch may be backed out by restoring the backup created prior to install. If the defects were discovered after the end of the warranty support period, a new patch will be entered into the National Patch Module on FORUM and go through all the necessary milestone reviews etc. as an emergency patch.

5.2. Back-Out Considerations

Changes implemented with the patch should be backed-out in their entirety.

5.2.1. Load Testing

Load Testing is not applicable for this VistA patch.

5.2.2. User Acceptance Testing

User Acceptance is detailed in the Pharmacy Operational Updates Jira project site.

5.3. Back-Out Criteria

It may be decided to back-out this patch if the project is canceled, the requested changes implemented by the patch are no longer desired by VA OIT and the Pharmacy Business team, or the patch produces catastrophic problems.

5.4. Back-Out Risks

Back-out risks consist primarily of allowing existing deficient software to continue operating as it did prior to the OneVA Drug Restrictions patch PSS*1.0*239.

5.5. Authority for Back-Out

Any back-out decision should be a joint decision of the Area Manager, the Business Owner (or their representative) and the Program Manager with input from the HSP PCS Application Coordinator, HPS Support, the project development team.

5.6. Back-Out Procedure

The back-out plan for VistA applications consists of installing the patch backup created prior to installation. The PSS*1.0*239 build contains a restore routine that is executed when a backup of the patch is installed. The restore routine returns non-routine components that are not restored by the standard backup installation to their pre-patch state. Data associated with the new data dictionary field is also removed from the database prior to the removal of the field.

The components restored by the restore routine are listed below.

Component Type	Component Name	Action Performed
Input Template	PSSCOMMON	Restored
Data Dictionary	RESTRICT FOR ONEVA PHARMACY (#907) field in the DRUG (#50) file	Deleted

5.7. Back-Out Verification Procedure

Successful back-out is confirmed by verification that the back-out patch was successfully implemented, including verification that new components were removed and modified components were returned to their pre-patch state.

The back-out verification details are listed below.

Component Type	Component Name	Back-Out Result
Routine	PSSLOOK	Restored
Input Template	PSSCOMMON	Restored
Data Dictionary	RESTRICT FOR ONEVA PHARMACY (#907) field in the DRUG (#50) file	Deleted

6.   Rollback Procedure

6.1.   Rollback Considerations

Data records introduced by this patch are automatically removed when the patch is backed-out by installing the patch backup created prior to installation.

6.2.   Rollback Criteria

The only criteria for rollback is the back-out of the patch.

6.3.   Rollback Risks

No rollback risks have been identified.

6.4.   Authority for Rollback

Since rollback occurs automatically when the patch is backed-out, authority for rollback is dependent on the back-out decision and authority.

6.5.   Rollback Procedure

The rollback plan for VistA applications consists of installing the patch backup created prior to installation. The PSS*1.0*239 build contains a restore routine that is executed when a backup of the patch is installed. The restore routine returns non-routine components that are not restored by the standard backup installation to their pre-patch state. Data associated with the new data dictionary field is also removed from the database prior to the removal of the field.

6.6.   Rollback Verification Procedure

There is no user option to verify rollback. Rollback verification may only be performed by manually searching the global file storage location of the data dictionary field, since the data dictionary is removed during the back-out/rollback process. The ^%GCHANGE utility is one method that may be used to verify that neither of the two values (zero or one) are stored in the field's global file storage location. This method works at the time this was written because the global node associated with the rolled-back data (^PSDRUG(,6)) contained data for only two data dictionary fields, and the rolled-back data would have been stored in the second caret ("^") delimited piece. A search for the strings "^0" and "^1" in the ^PSDRUG(,6) global node using the Find feature of ^%GCHANGE should produce no results. This verifies successful rollback as the data would always be preceded by a caret ("^"), it would always be equal to a one or a zero, and the only other data stored at that node is the first caret delimited piece, which cannot be preceded by a caret.

Example, using the ^%GCHANGE utility to search for data in the second caret delimited piece of the ^PSDRUG(,6) global node and verifying no results are displayed:

```
VISTA>D ^%GCHANGE

Output on
Device:
Right margin: 80 =>

Global ^PSDRUG(,6)
(F) Find, (C) Change every, or (X) Execute code: F=>
Find every: ^0

Global ^PSDRUG(,6)
(F) Find, (C) Change every, or (X) Execute code: F=>
Find every: ^1

Global ^
VISTA>
```