VistA Audit Solutions (VAS) Switch Alert and No Pointer Reset

DG*5.3*1120

Deployment, Installation, Back-Out, and Rollback Guide

June 2024

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

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

Table of Contents

1. Introduction

This document describes how to deploy and install the Registration (PIMS/DG) VistA Audit Solutions (VAS) Switch Alert and No Pointer Reset patch DG*5.3*1120, 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 VAS Switch Alert and No Pointer Reset functionality 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

DG*5.3*1108 must be installed **BEFORE** DG*5.3*1120.

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 Information Governance (HIG) office.	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 Information Governance (HIG) Testing & VIP Release Agent Approval	Deployment	Test for operational readiness	Testing
4	Application Coordinators	Release Deployment	Application Coordinators release patches	Deployment
5	HIG and FO	Deployment	Execute deployment	Deployment

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
6	Office of Information and Technology (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, HIG, 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

After national release, the deployment and installation is scheduled to run for 31 days, as depicted in the master deployment schedule for VistA Audit Solution (VAS).

3.2. Site Readiness Assessment

This section discusses the locations that will receive the deployment of the VAS Switch Alert patch DG*5.3*1120.

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:

- Central Arkansas HCS, Little Rock, AR
- Tampa HCS, Tampa, FL
- Texas Valley Coastal Bend HCS, Harlingen, TX

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 following table describes preparation required by the site prior to deployment.

Table 2: 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 following table lists facility-specific features required for deployment.

Table 3: Facility-Specific Features

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

3.3.2. Hardware

The following table describes hardware specifications required at each site prior to deployment.

Table 4: 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 following table describes software specifications required at each site prior to deployment.

Table 5: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other
Fully patched Registration (PIMS), DG namespaced package within VistA	N/A	5.3	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 the patch DG*5.3*1120, 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 6: 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 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
REGISTRATION	DG*5.3*1120

The VistA patch 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 Installation. 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 DG*5.3*1120.
    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 DG*5.3*1120.
        iii. When prompted for the following, enter "B" for Build.

            Select one of the following:

                B Build (including Routines)

                R Routines Only

            Backup Type: 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, DG*5.3*1120.
        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 'Delay Install (Minutes): (0 - 60): 0//', answer 0.

4.9. Installation Verification Procedure

Successful installation can be verified by reviewing the first 2 lines of the routines contained in the patch. The second line will contain the patch number (1120) in the [PATCH LIST] section.

The option Calculate and Show Checksum Values [XTSUMBLD-CHECK] option 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 HIG 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 30 days 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. The only software component in the patch are routines, which may be backed out by installing the backup made prior to installation.

5.2.1. Load Testing

Load Testing is not applicable for this VistA patch.

5.2.2. User Acceptance Testing

User Acceptance is incorporated into the Initial Operating Capability (IOC) Pre-Prod testing.

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 HIG business team, or the patch produces catastrophic problems.

5.4. Back-Out Risks

Back-out risks consist of production software continuing to operate as it did prior to installing the patch, without the enhancements provided by the patch.

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 Health Information Governance (HIG) team) and the project development team.

5.6. Back-Out Procedure

The back-out plan for VistA applications is complex and not a "one size fits all" solution. The general strategy for a VistA back-out is to repair the code with a follow-up patch. The development team recommends that sites log a ticket if it is a nationally released patch.

5.7. Back-out Verification Procedure

Successful back-out is confirmed by verification that the back-out patch created prior to installation was successfully installed, including verification that new components were removed and modified components were returned to their pre-patch state. The first 2 lines of the routines in the patch will not contain the patch number (1120) in the [PATCH LIST] section. The Calculate and Show Checksum values [XTSUMBLD-CHECK] option may be run to compare the routines' checksums to the 'Before' checksums in the patch description.

6. Rollback Procedure

Not applicable.

6.1. Rollback Considerations

Not applicable.

6.2. Rollback Criteria

Not applicable.

6.3. Rollback Risks

Not applicable.

6.4. Authority for Rollback

Not applicable.

6.5. Rollback Procedure

Not applicable.

6.6. Rollback Verification Procedure

Not applicable.