

Electronic Health Modernization
IFC Proxy Add/Order Resubmission 1.0
Deployment, Installation, Back-Out, and Rollback
Guide



November 2024

Department of Veterans Affairs

Office of Information and Technology

Revision History

Date	Version	Description	Author
11/2024	1.0	Initial draft	EHRM-IO

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback (DIBR) Guide for new products going into the Department of Veterans Affairs (VA) Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single location or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the DIBR Guide is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

1. Introduction	1
Purpose	1
Dependencies	1
Constraints	1
2. Roles and Responsibilities	1
3. Deployment	2
3.1 Timeline	2
3.2 Site Readiness Assessment	2
3.2.1 Deployment Topology (Targeted Architecture)	2
3.2.2 Site Information (Locations, Deployment Recipients)	2
3.2.3 Site Preparation	3
3.3. Resources	3
3.4. Hardware	3
3.5. Software	3
3.6 Communications	3
3.6.1 Deployment/Installation/Back-Out Checklist	3
4. Installation	3
4.1. Pre-installation and System Requirements	4
4.2. Platform Installation and Preparation	4
4.3. Download and Extract Files	4
4.4. Database Creation	4
4.5. Installation Scripts	4
4.6. Cron Scripts	4
4.7. Access Requirements and Skills Needed for the Installation	4
4.8. Installation Procedure	5
4.9. Installation Verification Procedure	6
4.10. Post-Installation Instructions	6
5. Back-Out Procedure	6
5.1. Back-Out Strategy	6
5.2. Back-Out Considerations	7
5.2.1 Load Testing	7
5.2.2 User Acceptance Testing	7
5.3. Back-Out Criteria	7
5.4. Back-Out Risks	7
5.5. Authority for Back-Out	7
5.6. Back-Out Procedure	7

5.7. Back-out Verification Procedure	8
6. Rollback Procedure	8
6.1. Rollback Considerations	8
6.2. Rollback Risks	8
6.3. Authority for Rollback	8
6.4. Rollback Procedure	8
6.5. Rollback Verification Procedure.....	8

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities.....	1
Table 2: Deployment/Installation/Back-Out Checklist.....	3

1. Introduction

This document is intended to guide the VA Medical Center (VAMC) Information Resources Management (IRM) Specialist or VA Testing Center engineer in the installation of the IFC Proxy Add/Order Resubmission multi-build. The build consists of four (4) patches: 1) DG*5.3*1096, 2) EHM*1*10, 3) GMRC*3*189 and 4) DG*5.3*1091. DG*5.3*1096 and DG*5.3*1091 are components of the Registration (DG) package. EHM*1*10 is a component of the Electronic Health Modernization (EHM) package. GMRC*3*189 is a component of the Consult/Request Tracking (GMRC) package.

Purpose

The purpose of this document is to describe how, when, where, and to whom the IFC Proxy Add/Order Resubmission multi-build is deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The document also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

Dependencies

The following patches must be installed before proceeding with installation of this multi-build:

- GMRC*3*169, GMRC*3*185, GMRC*3*202
- DG*5.3*1005, DG*5.3*1037

Constraints

There are no constraints for this patch.

2. Roles and Responsibilities

The deployment, installation, back-out, and rollback roles and responsibilities are shown in Table 1.

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

Team	Phase / Role	Tasks
EHRM-IO Deployment Team, VistA Team	Deployment	Plan and schedule deployment
EHRM-IO Deployment Team, VistA Team	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.

Team	Phase / Role	Tasks
EHRM-IO Deployment Team, VistA Team	Deployment	Test for operational readiness
EHRM-IO Deployment Team, VistA Team	Deployment	Execute deployment
Site-specific Regional IT Team	Installation	Plan and schedule installation
Site-specific Regional IT Team	Installation	Ensure authority to operate and that certificate authority security documentation is in place
Site-specific Regional IT Team	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)
EHRM-IO Deployment Team, VistA Team Product Development Team during warranty period, afterwards (software only) Tier 1, Tier 2, Tier 3 / VistA Maintenance	Post Deployment	Hardware, Software and System Support

3. Deployment

The patch will be released nationally subject to the standard patching procedures.

3.1 Timeline

TBD

3.2 Site Readiness Assessment

N/A

3.2.1 Deployment Topology (Targeted Architecture)

N/A

3.2.2 Site Information (Locations, Deployment Recipients)

The patch will be deployed to all Veterans Health Information Systems and Technology Architecture (VISTA) production instances. The IOC test sites are the Chalmers P. Wylie Ambulatory Care Center (Columbus, Ohio) and VA Portland Health Care System (Portland, Oregon and Vancouver, Washington).

3.2.3 Site Preparation

N/A

3.3. Resources

The IFC Proxy Add/Order Resubmission multi-build does not require any special or specific resources at a VistA system. The EHM*1*10 patch adds a new file – EHRM HL7 Message (#1609). This will have no measurable impact on database size, and older records will be regularly purged. The GMRC*3*189 patch expands the size of the REMOTE RESULT FILE ENTRY field (#.06) to the REQUEST/CONSULTATION file (#123) from 12 to 20 characters. This will have no measurable impact on database size.

3.4. Hardware

There is no specific hardware required other than that which already hosts the VistA system. This is a software enhancement that will not require additional hardware.

3.5. Software

There is no specific software required other than that which already hosts the VistA system.

3.6 Communications

The patch changes the content of selected HL7 messages but does not impact the manner that these messages are sent or received.

3.6.1 Deployment/Installation/Back-Out Checklist

The Release Management team will deploy the IFC Proxy Add/Order Resubmission multi-build.

Table 2: 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

The software for this build is being released in a host file named IFC_PROXY_ADD_ORDER_RESUBMISSION.KID. There are no pre-installation actions required of the installer. There is one post-installation action required of the installer. It is detailed below.

4.1. Pre-installation and System Requirements

The patches listed below are required builds for the IFC Proxy Add/Order Resubmission multi-build. They are already installed at all production sites.

1. GMRC*3*169
2. GMRC*3*185
3. GMRC*3*202
4. DG*5.3*1005
5. DG*5.3*1037

4.2. Platform Installation and Preparation

This product is a set of VistA patches. Sites should install the build 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” to create a backup message of any routines exported with this patch.

4.3. Download and Extract Files

N/A.

4.4. Database Creation

N/A.

4.5. Installation Scripts

N/A.

4.6. Cron Scripts

N/A.

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

Pre-Installation instructions:

This build may be installed with users on the system although it is recommended that it be installed during non-peak hours to minimize potential disruption to users. This build should take less than 30 minutes to install. This patch should not be queued.

Installation Instructions:

1. Use the Load a Distribution option contained on the Kernel Installation and Distribution System Menu to load the Host file.

When prompted to "Enter a Host File:" enter
`/srv/vista/patches/SOFTWARE/IFC_PROXY_ADD_ORDER_RESUBMISSION.KID`

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 or build name IFC PROXY ADD/ORDER RESUBMISSION 1.0.
 - B. Select the Backup a Transport Global option to create a backup message. You must use this option for each patch contained in the Host File. For each patch you can specify what to backup, the entire Build or just Routines. The backup message can be used to restore just the routines or everything that will restore your system to pre-patch condition.
 - 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 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 the components of this patch, such as routines, 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.

4.9. Installation Verification Procedure

Verify completed installation by checking that the build components as listed in the patch description have been correctly installed onto the target VistA system.

4.10. Post-Installation Instructions

After patch installation has completed, restart the HL7 incoming filers.

First, use the Monitor, Start, Stop Filers [HL FILER MONITOR] option on the Filer and Link Management Options [HL MENU FILER LINK MGT] menu on the HL7 Main Menu [HL MAIN MENU] to stop the filers.

After the filers have stopped, use the Monitor, Start, Stop Filers [HL FILER MONITOR] option on the Filer and Link Management Options [HL MENU FILER LINK MGT] menu on the HL7 Main Menu [HL MAIN MENU] to start the filers.

In TaskMan, schedule the EHMHL7 PURGE option to run daily during off-peak hours. Retention periods are initially set during patch load to 30 days but can be customized at each VistA site by editing the RETENTION field (#1) for the EHRM HL7 Message file (#1609) using FileMan.

5. Back-Out Procedure

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

5.1. Back-Out Strategy

The Back-Out Strategy for VistA applications is complex and is not able to be a “one size fits all” strategy. The general strategy for VistA software back-out is to repair the code with a follow-up patch. The site should contact the Enterprise Program Management Office (EPMO) directly for specific solutions to their unique problems.

Although it is unlikely due to care in collecting approved requirements, software quality analyst (SQA) review and multiple testing stages (Primary Developer, Secondary Developer, and Component Integration Testing) a back-out decision due to major issues with this patch could occur during site Mirror Testing, Site Production Testing or after Release to the Field. The strategy would depend on during which of these stages the decision is made. If the decision is made during Site Production Testing, the normal VistA response would be for a new version of

the test patch to be produced to correct defects, unless the patch produces catastrophic problems. The test patch would be retested and upon successfully passing development team testing would be resubmitted to the site for testing. If the defects were not discovered until after release, OEHRM would produce the new patch, either to correct the defective components or to back-out.

5.2. Back-Out Considerations

It is necessary to determine if a wholesale back-out of the build is needed or if correcting through a new version of the build is a better course of action. A wholesale back-out of the patch will still require a new version.

5.2.1 Load Testing

N/A.

5.2.2 User Acceptance Testing

N/A.

5.3. Back-Out Criteria

The decision to back-out this VistA multi-build will be made by the Business Sponsor, EHRM-IO VA Leadership, VA OIT IT Program Manager, and the Development Team. Criteria will be determined based on separate and unique factors and will be evaluated upon post-patch installation use of the product.

5.4. Back-Out Risks

N/A.

5.5. Authority for Back-Out

Based on authority provided by the Business Sponsor, EHRM-IO VA Leadership and VA OIT IT Program Manager, the build can be backed out in accordance to their approval.

5.6. Back-Out Procedure

***WARNING: Use caution in performing these steps. Deletions cannot be undone!
There is no harm in leaving the build installed. As long as no other application calls the new API, then the routine will never be run.***

Removing the build from a site can be done by installing the backups of the four (4) patches created during patch installation.

5.7. Back-out Verification Procedure

The routines listed in the patch descriptions can be checked to see that the associated patch number is not present in line 2 of each routine. File #1609 can be checked to see that it is not present using FileMan to list the data dictionary.

6. Rollback Procedure

Rollback pertains to data associated with this patch.

6.1. Rollback Considerations

This patch does not supply or convert any data.

The decision to rollback this VistA patch will be made by the Business Sponsor, Electronic Health Record Modernization – Integration Office (EHRM-IO) VA Leadership, VA OIT IT Program Manager, and the Development Team. Criteria will be determined based on separate and unique factors and will be evaluated upon post-patch installation use of the product.

6.2. Rollback Risks

Rollback risks include being able to restore the database to how it looked before this patch was installed without introducing database corruption.

6.3. Authority for Rollback

Based on authority provided by the Business Sponsor, EHRM-IO VA Leadership and VA OIT IT Program Manager, the build can be rolled back in accordance to their approval.

6.4. Rollback Procedure

A new build to fix the problems should be developed.

6.5. Rollback Verification Procedure

Verify that all the above data components have been removed from the system as described in the previous section.