Vitals / Vitals Measurements (GMRV*5.0*36)

Deployment, Installation, Back-Out, and Rollback Guide

February 2018

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
2/20/2018	1.0	Initial Release	C. Bell K. Meneguzzo

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Plan for new products going into the 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 or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Plan 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

List of Tables

List of Figures

1. Introduction

This document describes how to deploy and install Vitals v5.0.36.2 & Vitals Manager v5.0.36.1, 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. In cases where a non-developed COTS product is being installed, the vendor provided User and Installation Guide may be used, but the Back-Out Recovery strategy still needs to be included in this document.

1.1. Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 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. Specific instructions for installation, back-out, and rollback are included in this document.

1.2. Dependencies

The Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 projects are for installation on a fully patched VistA system. There are also two Graphical User Interface (GUI) components that should be running on a Windows system.

1.3. Constraints

Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 and the associated M patch are expected to be installed on existing VistA platforms. The hardware may reside at local or regional data centers. Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 utilize existing, nationally released security controls to control access.

2. Roles and Responsibilities

No one single entity is in charge of decision making for deployment, installation, back out and rollback of Vitals v5.0.36.2 & Vitals Manager v5.0.36.1. Rather, the Release Agent and Application Coordinators under the Veterans In Process will meet and approve deployment and install from an OI&T perspective. If an issue with the software arises, then the facility CIO and other site leadership will meet along with input from Patient Safety and Health Product Support to initiate a back out and rollback decision of the software along with Region and Site leadership. The following table provides Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 project information.

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

Team	Phase / Role	Tasks
Site personnel in conjunction with IT support – which may be local or regional.	Deployment	Plan and schedule deployment (including orchestration with vendors)
Site personnel in conjunction with IT support – which may be local or regional.	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.
Site personnel.	Deployment	Test for operational readiness
Site personnel in conjunction with IT support – which may be local or regional. The IT support will need to include person(s) to install the KIDS build as well as the personnel to deploy the GUI – which may be done on each machine, a shared network and/or the Citrix access gateway	Deployment	Execute deployment
Site personnel in conjunction with IT support – which may be local or regional. The IT support will need to include person(s) to install the KIDS build as well as the personnel to deploy the GUI – which may be done on each machine, a shared network and/or the Citrix access gateway	Installation	Plan and schedule installation
N/A – will work under the VistA ATO and security protocols.	Installation	Ensure authority to operate and that certificate authority security documentation is in place
N/A – no equipment is being added.	Installation	Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes
N/A – no new functionality is being introduced.	Installations	Coordinate training

Team	Phase / Role	Tasks
Facility CIO and IT 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)
Hardware and System support – no changes. Software support will be the HPS Clinical Sustainment team.	Post Deployment	Hardware, Software and System Support

Note: For Project Phase See Schedule

3. Deployment

The deployment is planned as a standard VistA National Patch Module patch rollout. Once approval has been given to nationally release, the patch GMRV*5.0*36 will be released from the National Patch Module. At this point, it will be available for installation and deployment at all sites.

Scheduling of test/mirror installs, testing and deployment to production will be at the site's discretion. It is anticipated there will be a 30-day compliance period.

3.1. Timeline

There is no timeline specifically for deployment. This is considered a maintenance release and installation will be at the site's discretion, within the constraints of the compliance period for the release.

3.2. Site Readiness Assessment

This section discusses the locations that will receive the Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 deployment.

3.2.1. Deployment Topology (Targeted Architecture)

Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 will be deployed to each VistA instance. That will include local sites as well as regional data processing centers. The executable will also be deployed to the Citrix Access Gateway.

3.2.2. Site Information (Locations, Deployment Recipients)

The initial deployment will be to IOC sites for verification of functionality. Once that testing is completed and approval is given for national release, Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 (GMRV*5.0*36) will be deployed to all VistA systems.

The Production (IOC) testing sites are:

- Salt Lake City VA Medical Center
- Tuscaloosa VA Medical Center

3.2.3. Site Preparation

There is no special preparation required for Vitals v5.0.36.2 & Vitals Manager v5.0.36.1. A fully patched VistA system is the only requirement.

3.3. Resources

N/A

3.3.1. Facility Specifics

N/A

3.3.2. Hardware

N/A

3.3.3. Software

N/A

3.3.4. Communications

Service Delivery and Engineering (SDE) Field Implementation Services will be sending out an Action item and National Change Order prior to the release of Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 advising them of the upcoming release.

Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 will be deployed using the standard method of patch release from the National Patch Module rather than a phased deployment. When patch GMRV*5.0*36 is released, the National Patch Module will send a notification to all the personnel who have subscribed to those notifications.

3.3.4.1. Deployment/Installation/Back-Out Checklist

The deployment and installation will be performed by site support personnel once it is nationally released.

4. Installation

Pre-installation and System Requirements

Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 assumes a fully-patched VistA system.

Platform Installation and Preparation

[VistA] This patch should be loaded during non-peak hours to minimize disruption to users. Installation will take less than 5 minutes. Users may remain on the system. [GUI] The time to deploy the GUI files will depend on which method the site utilizes for running the executable (network share, Citrix, individual workstation install, etc.) Download and Extract Files

Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 is being released as a PackMan Message distributed through Forum combined with a .ZIP file containing the GUI file(s).

The preferred method is to retrieve files from download.vista.med.va.gov.

This transmits the files from the first available server. Sites may also elect to retrieve files directly from a specific server.

Sites may retrieve the software and/or documentation directly using Secure File Transfer Protocol (SFTP) from the ANONYMOUS.SOFTWARE directory at the following

Table 2: OI Field Offices

Location	Site
Hines	fo-hines.med.va.gov
Salt Lake City	fo-slc.med.va.gov

Documentation can also be found on the VA Software Documentation Library at:

http://www.va.gov/vdl

Table 3: Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 Files to be Downloaded

File Name	File Contents	Download Format
GMRV_5_36.ZIP	Vitals and Vitals Manager executables	Binary

4.1. Database Creation

N/A

4.2. Installation Scripts

N/A

4.3. Cron Scripts

N/A

4.4. Access Requirements and Skills Needed for the Installation

Installation of Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 requires the following to install:

- Programmer access to VistA instance and ability to install KIDS build.
- Citrix Access Gateway (CAG) installs – access/ability to upload to the CAG.
- Network Share installs – access/ability to upload executable to the network share location.
- Individual work-station installs – access/ability to push executable to required work stations.

4.5. Installation Procedure

4.5.1. GMRV*5.0*36 VistA Installation

1. Choose the PackMan message containing this patch and invoke the INSTALL/CHECK MESSAGE PackMan option.

2. Select Kernel Installation & Distribution System Option: Installation

   1 Load a Distribution
   2 Verify Checksums in Transport Global
   3 Print Transport Global
   4 Compare Transport Global to Current System
   5 Backup a Transport Global
   6 Install Package(s)
   Restart Install of Package(s)
   Unload a Distribution

3. From this menu, must use the [Backup a Transport Global] option to create a back out Patch

4. Also from this menu, you may elect to use the following options:
   - Compare Transport Global to Current System
   - Verify Checksums in Transport Global
   - Use the Install Package(s) options and select the package GMRV*5.0*36

5. When prompted "Want KIDS to Rebuild Menu Trees Upon Completion of Install?" respond NO.

6. When prompted 'Want KIDS to INHIBIT LOGONs during the install? NO//' respond NO.

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

4.5.2. Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 GUI Installation

The ZIP file contains the Vitals and Vitals Manager GUI executables. Download the ZIP file and extract all the files.

4.5.2.1. Vitals and Vitals Manager GUI Methods of Installation

The following methods of installation for Vitals are available. Sites' choice of which method(s) to use will depend upon Regional/VISN policies, Local Area Network (LAN) performance or other local circumstances. User requirements, physical location and methods of connection to the VA network may warrant more than one of the options below to be used.

Note: Vitals Manager is not needed for every user. This is designed for users who are responsible for the Management of the Vitals package for this server.

- **Network (shared) installation:**

  This method is typically the simplest to maintain, providing the local network infrastructure is robust enough to handle the additional traffic caused by users running the GUI executables (Vitals.exe & VitalsManager.exe) across the LAN.

  The GUI executables (Vitals.exe & VitalsManager.exe), and help folder and files (VITALS.HLP & VITALSMANAGER.HLP), are copied to a network shared location. Users are provided with a desktop shortcut to run Vitals.exe and VitalsManager.exe directly from the network shared drive. The necessary command line parameters (VistA server address or name and RPC Broker Port number) are entered in the "Target" field of the shortcut properties

  At the time of a Vitals and/or Vitals Manager version update the copy of Vitals.exe and VitalsManager.exe and the help files are simply replaced, on the network share, with the new version.

  Any users requiring access to another site's Vitals.exe and/or VitalsManager.exe system can be given an alternate desktop shortcut with command line parameters appropriate to the intended target VistA system.

  If a user requires access to an older or newer version of Vitals.exe or VitalsManager.exe (e.g. for testing purposes) a different version of Vitals.exe and/or VitalsManager.exe can be placed in a separate network location and the user be supplied with an appropriate alternate shortcut (different Target path and different VistA server command line parameters).

- **Citrix installation:**

  The GUI executables (Vitals.exe & VitalsManager.exe) and help folder and files (VITALS.HLP & VITALSMANAGER.HLP) are installed and run from a remote workstation, and the user views the remote workstation's screen on their local workstation.

  For the local site users, this method is on a similar level to the Network (shared) installation above. The users' workstations require only an appropriate shortcut (and the necessary Citrix Access Group (CAG) infrastructure).

  Note: For issues with CAG, please contact your local or national help desk.

For the Citrix Farm administrator, this method involves installations on the host in a similar manner to either the Gold Path or the Direct Access methods outlined below.

- **Local workstation installation:**

  Download the ZIP file and extract all the files.

  GMRV*5.0*36 - Vitals & Vitals Manager

  Vitals.exe, VitalsManager.exe and the associated help files will need to be installed in the same directory on workstations.

  Note: There is a national SCCM package to help sites or ITOPS distribute the Vitals and Vitals Manager GUIs.

- **Manual install:**

  This method is used primarily for advanced users and at testing locations.
  This method is somewhat changed from that used previously for Windows XP workstations.

  1. Locate the GMRV_5_36.ZIP and unzip the file.
  2. Copy the Vitals.exe and/or VitalsManager.exe to a test directory, for example, C:\VitalsTest. You may need to create this new directory.

  Note: You may need to have a user with Administrator rights complete this step.

  3. Create a Shortcut(s) and name it "Test Vitals36" and/or "Test VitalsManager36". This is to give the user another visual cue that this is not the normal Vitals icon.

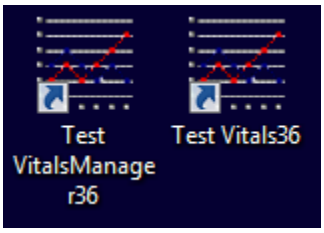

Figure 1: Vitals Icon

  4. Copy the Help folder and its contents (VITALS.HLP & VITALSMANAGER.HLP) into the same directory as CRHDShiftChgHandoff.exe (for example, c:\VitalsTest). This file should be in the same directory Vitals.exe and/or VitalsManager.exe.
  5. Determine the DNS server name or IP address for the appropriate VistA server.
  6. Determine the Broker RPC port for the VistA account.

7. Enter IP (or DNS name) and RPC port in the Target field of the Shortcut properties (or use ServerList.exe).

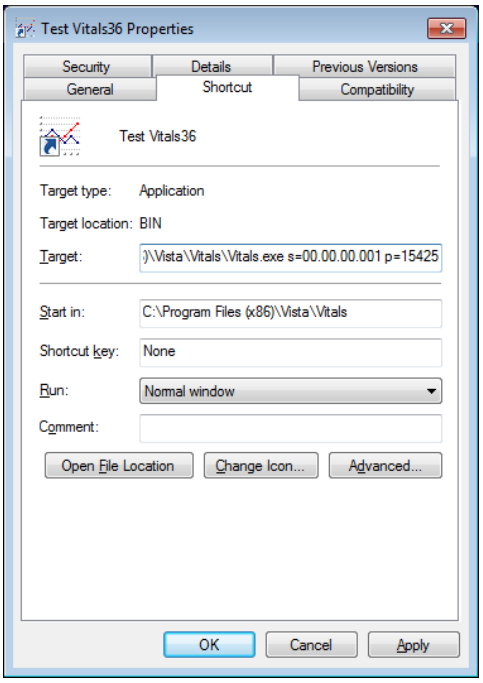

Figure 2: Test Vitals36 Properties Tab

Example of what the shortcut properties dialog might look like.

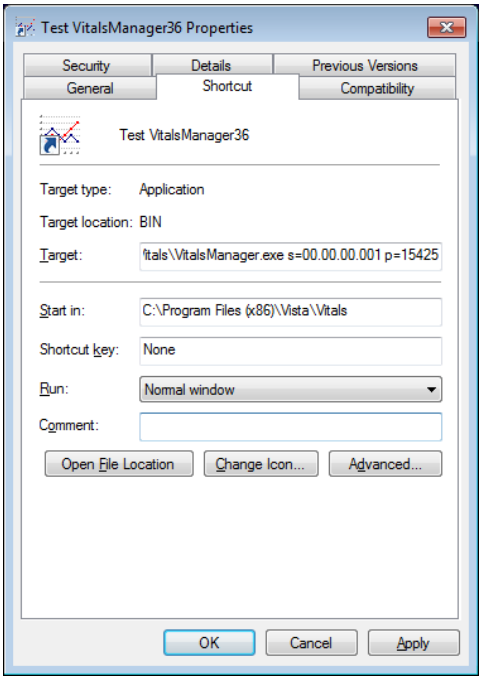

Figure 3: Test VitalsManager36 Properties Tab

The server and port number shown above are not real and are for example only.

4.6. Installation Verification Procedure

Launch both the Vitals and Vitals Manager GUI and verify the splash screen now announces that you are running version 5.0.36.1. Log in to the desired server and verify that you do not receive a version mismatch.

4.7. System Configuration

N/A

4.8. Database Tuning

N/A

5. Back-Out Procedure

5.1. Back-Out Strategy

To revert to the Vitals and/or Vitals Manager GUI, the prior GUI would have to be redistributed. For Vitals this is version 5.0.27.5 and for Vitals Manager this is 5.0.27.3.

5.2. Back-Out Considerations

5.2.1. Load Testing

No load testing was performed on Vitals v5.0.36.2 & Vitals Manager v5.0.36.1. This was a maintenance release to correct defects discovered in Vitals v5.0.27.5 & Vitals Manager v5.0.27.3. There was no additional functionality included.

5.2.2. User Acceptance Testing

User acceptance testing was conducted by the three test sites listed in section 3.2.2.

The sites followed the provided test plan and executed the test cases according to the plan for the first build of GMRV*5.0*36. The sites either passed or failed any item based on testing. The tests were performed by Clinical Application Coordinators at each site who are familiar using the application. The test cases were then delivered with concurrence by the sites to the HPS Clinical Sustainment team. Any items that failed were re-developed and then sent back to the sites for the next build and further acceptance testing following the same process. Once in production, the same final test cases from the last build were tested in production. No subsequent builds were created as the test cases passed and sites signed off on concurrence for release of the product.

5.3. Back-Out Criteria

Back-out would only be considered if there was a catastrophic failure that causes loss of function for the application and a significant patient safety issue.

5.4. Back-Out Risks

Backing out Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 would result in the re-instatement of the issues addressed in Vitals v5.0.36.2 & Vitals Manager v5.0.36.1.

In addition, there is a risk that the process, which would be performed only in an emergent situation, would significantly impact patient care due to the interruption.

5.5. Authority for Back-Out

The Facility CIO has the final authority to require the rollback and accept the associated risks

5.6. Back-Out Procedure

These steps assume that the only reason to consider a back-out for Vitals v5.0.36.2 & Vitals Manager v5.0.36.1 is in the event of a catastrophic failure.

Note: the Vista Changes and GUI changes are independent of each other. In the case of a catastrophic failure of the GUI, the VistA Patch can remain in the system; consequently, if the catastrophic failure is in the VistA side, the site can back out the VistA patch and continue to use the updated GUI.

1. Contact the HPS Clinical Sustainment implementation team to notify them there has been a catastrophic failure with Vitals v5.0.36.2 & Vitals Manager v5.0.36.1. Use the following contacts :

Table 4: HPS CLIN Team Contact Information

Name & Title	Email	Telephone
James Hartin Project Manager	James.Hartin@va.gov	803-532-6699
Chris Bell Technical Leader	Christopher.Bell2@va.gov	941-592-5820

2. If the decision is made to proceed with back-out and rollback, the HPS Sustainment Clinical team be available to assist sites that have misplaced their backup PackMan message, as well as give you the instructions on downloading the executable.
3. [GUI] (if needed) Coordinate with the appropriate IT support, local and regional, to schedule the time to install GMRV*5.0*27 and to push out / install the previous GUI executable.
4. Once GMRV*5.0*27 and Vitals v5.0.27.5 & Vitals Manager v5.0.27.3 have been installed, verify operations before making available to all staff.

5.7. Back-out Verification Procedure

1. Ensure that both executables launches properly.
2. Perform site-specific testing appropriate to the areas where the catastrophic failure was identified.

6. Rollback Procedure

6.1. Rollback Considerations

N/A

6.2. Rollback Criteria

N/A

6.3. Rollback Risks

N/A

6.4. Authority for Rollback

The Facility CIO has the final authority to require the rollback and accept the associated risks

6.5. Rollback Procedure

Back-out will automatically rollback version.

6.6. Rollback Verification Procedure

N/A