Drug Accountability Upload 3.0

Deployment, Installation, Back-Out, and Rollback Guide (DIBR)



December 2021

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

Revision History

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 12/09/2021 | 1.0 | PSA\*3.0\*83:   * Addresses the defects pertaining to failed invoice uploads from McKesson * The unredacted version of this document is available in the SOFTWARE library for viewing REDACTED information | Liberty ITS |

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Guide 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 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](#_Toc88057250)

[1.1 Purpose 1](#_Toc88057251)

[1.2 Dependencies 1](#_Toc88057252)

[1.3 Constraints 1](#_Toc88057253)

[2 Roles and Responsibilities 2](#_Toc88057254)

[3 Deployment 3](#_Toc88057255)

[3.1 Timeline 3](#_Toc88057256)

[3.2 Site Readiness Assessment 3](#_Toc88057257)

[3.2.1 Deployment Topology (Targeted Architecture) 3](#_Toc88057258)

[3.2.2 Site Information (Locations, Deployment Recipients) 3](#_Toc88057259)

[3.2.3 Site Preparation 3](#_Toc88057260)

[3.3 Resources 4](#_Toc88057261)

[3.3.1 Facility Specifics 4](#_Toc88057262)

[3.3.2 Hardware 4](#_Toc88057263)

[3.3.3 Software 4](#_Toc88057264)

[3.3.4 Communications 4](#_Toc88057265)

[3.3.4.1 Deployment/Installation/Back-Out Checklist 5](#_Toc88057266)

[4 Installation 6](#_Toc88057267)

[4.1 Pre-installation and System Requirements 6](#_Toc88057268)

[4.2 Platform Installation and Preparation 6](#_Toc88057269)

[4.3 Download and Extract Files 6](#_Toc88057270)

[4.4 Database Creation 6](#_Toc88057271)

[4.5 Installation Scripts 7](#_Toc88057272)

[4.6 Cron Scripts 7](#_Toc88057273)

[4.7 Access Requirements and Skills Needed for the Installation 7](#_Toc88057274)

[4.8 Installation Procedure 7](#_Toc88057275)

[4.9 Installation Verification Procedure 7](#_Toc88057276)

[4.10 System Configuration 7](#_Toc88057277)

[4.11 Database Tuning 8](#_Toc88057278)

[5 Back-Out Procedure 8](#_Toc88057279)

[5.1 Back-Out Strategy 8](#_Toc88057280)

[5.2 Back-Out Considerations 8](#_Toc88057281)

[5.2.1 Load Testing 8](#_Toc88057282)

[5.2.2 User Acceptance Testing 8](#_Toc88057283)

[5.3 Back-Out Criteria 8](#_Toc88057284)

[5.4 Back-Out Risks 8](#_Toc88057285)

[5.5 Authority for Back-Out 9](#_Toc88057286)

[5.6 Back-Out Procedure 9](#_Toc88057287)

[5.7 Back-out Verification Procedure 9](#_Toc88057288)

[6 Rollback Procedure 9](#_Toc88057289)

[6.1 Rollback Considerations 9](#_Toc88057290)

[6.2 Rollback Criteria 9](#_Toc88057291)

[6.3 Rollback Risks 9](#_Toc88057292)

[6.4 Authority for Rollback 9](#_Toc88057293)

[6.5 Rollback Procedure 9](#_Toc88057294)

[6.6 Rollback Verification Procedure 9](#_Toc88057295)

List of Tables

[Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities 2](#_Toc88057296)

[Table 2: Site Preparation 3](#_Toc88057297)

[Table 3: Facility-Specific Features 4](#_Toc88057298)

[Table 4: Hardware Specifications 4](#_Toc88057299)

[Table 5: Software Specifications 4](#_Toc88057300)

[Table 6: Deployment/Installation/Back-Out Checklist 5](#_Toc88057301)

[Table 7: Associated Patch Files 6](#_Toc88057302)

# Introduction

This document describes how to deploy and install the Drug Accountability Upload (DAU) PSA\_MCKESSON\_UPLOAD.exe Version 3.0.83.1, Veterans Information Systems Technology and Architecture (VistA) informational patch PSA\*3.0\*83, as well as how to back-out the product and rollback to a previous state.

## Purpose

The purpose of this guide is to provide a single, common document that describes how, when, where, and to whom the DAU application will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The guide also identifies resources, and communication methods. Specific instructions for installation, back-out, and rollback are included in this document.

## Dependencies

Drug Accountability Upload (DAU) is dependent on a VistA instance to upload data to. PSA\*3.0\*26 and PSA\*3.0\*41 must be installed.

## Constraints

This patch is intended for a fully patched VistA system.

# Roles and Responsibilities

Table 1 identifies the technical and support personnel who are involved in the deployment of PSA\*3.0\*83. The VIP Triad (commonly referred to as the three in a box) will meet and approve deployment and installation.

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

| Team | Phase / Role | Tasks | Project Phase (See Schedule) |
| --- | --- | --- | --- |
| Veterans Affairs (VA) Office of Information and Technology (OIT), VA OIT Health Product Support, and developers | Deployment | Plan and schedule deployment | Planning |
| Site personnel in conjunction with local or regional Information Technology (IT) support | Deployment | Determine and document the roles and responsibilities of those involved in the deployment | Planning |
| Field Testing (Initial Operating Capability (IOC), Health Product Support Testing and VIP Triad | Deployment | Test for operational readiness | Testing |
| Health Product Support and Field Operations | Deployment | Execute deployment | Deployment |
| Site personnel in conjunction with local or regional OIT support | Installation | Plan and schedule installation | Deployment |
| Facility Chief Information Officer (CIO) 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 |
| VA OIT, VA OIT Product Support, and Governent Chief Information Office (GCIO) Development Team | Post Deployment | Hardware, Software and System Support | Warranty |

# Deployment

The deployment is planned as a standard national release in support of the Drug Accountability program.

## Timeline

This is considered a mandatory release and installation at the site will be required within the constraints of the compliance period for the release.

## Site Readiness Assessment

This section discusses the locations that will receive the deployment of the PSA\_MCKESSON\_UPLOAD.exe (which is included in VistA informational patch PSA\*3.0\*83).

### Deployment Topology (Targeted Architecture)

The PSA\_MCKESSON\_UPLOAD.exe graphic user interface (GUI) Version 3.0.83.1 included with PSA\*3.0\*83 is to be nationally released to all Veterans Affairs medical centers (VAMCs) and will be deployed to each requesting client as an executable.

### Site Information (Locations, Deployment Recipients)

The IOC sites are:

* Southern Arizona VA Health Care System (Tucson, AZ)
* St. Cloud VA Medical Center (St. Cloud, MN)

Upon national release all VAMCs will receive PSA\*3.0\*83 VistA Informational Patch, which will contain specific information for the location and retrieval of the executable.

### Site Preparation

There is no special preparation required for PSA\*3.0\*83. A fully patched VistA system is the only requirement.

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 |  |  |  |  |

## Resources

### 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 |  |  |  |

### 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 |
| --- | --- | --- | --- | --- | --- |
| Existing VistA systems |  |  |  |  |  |

Please see the Roles and Responsibilities table in [Section 2](#_Roles_and_Responsibilities) for details about who is responsible for preparing the site to meet these hardware specifications.

### 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 Drug Accountability Package within VistA |  | 3.0 |  |  |  |

Please see the Roles and Responsibilities table in [Section 2](#_Roles_and_Responsibilities) above for details about who is responsible for preparing the site to meet these software specifications.

### Communications

The sites that are participating in initial operating capability (IOC) testing will use the Patch Tracking message in Outlook to communicate with the developers and product support personnel.

#### Deployment/Installation/Back-Out Checklist

Table 6 provides a checklist to be used to capture the coordination effort and document the day/time/individual when each activity is completed. The deployment and installation will be performed by on-site support personnel once PSA\*3.0\*83 is nationally released.

Table 6: Deployment/Installation/Back-Out Checklist

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

# Installation

## Pre-installation and System Requirements

Download and extract the executable to an accessible folder. Create a shortcut of the executable, and place it on the user’s desktop.

A fully patched VistA Drug Accountability Package is required.

## Platform Installation and Preparation

Not applicable for PSA\*3.0\*83.

## Download and Extract Files

The PSA\*3.0\*83 patch description will be transmitted as a MailMan message from the National Patch Module (NPM) and this message can be pulled from there. The Zip file contains the executable and can be found, along with the end-user documentation, on the SOFTWARE directory.

https://REDACTED/SOFTWARE/

Redacted versions of the PSA\*3.0\*83 end-user documentation will be available on the VistA Document Library (VDL).

<https://www.va.gov/vdl/application.asp?appid=87>

Table 7: Associated Patch Files

| File | Description |
| --- | --- |
| PSA\_MCKESSON\_UPLOAD\_P83.ZIP | Contains the executable |
| PSA\_MCKESSON\_UPLOAD.exe | PSA\*3.0\*83 GUI Version 3.0.83.1 |
| PSA\_3\_P83\_DIBR.DOCX | Microsoft Word version of the Deployment, installation, back-out, roll back guide |
| PSA\_3\_P83\_DIBR.PDF | Portable document format (PDF) version of the Deployment, installation, back-out, roll back guide |
| PSA\_3\_P83\_UM.DOCX | Microsoft Word version of the User Manual |
| PSA\_3\_P83\_UM.PDF | PDF version of the User Manual |

## Database Creation

Not applicable to DAU.

## Installation Scripts

Not applicable to DAU.

## Cron Scripts

Not applicable to DAU.

## Access Requirements and Skills Needed for the Installation

Staff will need access to FORUM’s NPM to view the patch description. Staff will also need access and the ability to download the zip file from the SOFTWARE directory. The executable is to be installed by each site’s or region’s designated VA OIT IT Operations Service, Enterprise Service Lines, or VistA Applications Division.

## Installation Procedure

DAU is a standalone application.

To install the application:

**Note:** For backup purposes, users can retrieve a backup copy of the previous PSA\_MCKESSON\_UPLOAD.exe Version 3.0.79.7 from the PSA\_MCKESSON\_UPLOAD\_P79.ZIP file located on the SOFTWARE directory.

1. Extract the PSA\_MCKESSON\_UPLOAD\_P83.ZIP file. Refer to [Section 4.3](#_Download_and_Extract) for the Zip file location.
2. Create a shortcut of the PSA\_MCKESSON\_UPLOAD.exe Version 3.0.83.1. Set specific server and port information to the target properties. For example:

C:\%folder location%\PSA\_MCKESSON\_UPLOAD.exe s=xxx-sup.vha.med.va.gov p=190xxx

1. Place a copy of the shortcut on the user’s desktop.

## Installation Verification Procedure

Execute the application. Users may be prompted to confirm their Personal Identification Verification (PIV) card by entering their Personal Identification Number (PIN). Upon successful login, the user should be presented with the application option for uploading an invoice. Select an invoice to begin the upload process. The application should return a successful upload message to the user. Login to VistA and verify the invoice has been uploaded.

## System Configuration

Not applicable to DAU.

## Database Tuning

Not applicable to DAU.

# Back-Out Procedure

Back-out pertains to returning to the last known good operational state of the software and appropriate settings. Retrieve the backup copy of the PSA\_MCKESSON\_UPLOAD.exe Version 3.0.79.7 from [Section 4.8](#_Installation_Procedure) and restore the version to the C:\ drive.

## Back-Out Strategy

A decision to back out could be made during Site Mirror Testing, during Site Production Testing, or after National Release to the field (VAMCs). The best strategy decision is dependent on the stage of testing during which the decision is made.

If a decision to back out is made after national release and within the designated support period a notification will be disseminated through the NPM in Forum and will list all the necessary steps.

## Back-Out Considerations

Changes implemented with PSA\_MCKESSON\_UPLOAD.exe Version 3.0.83.1 distributed in VistA Informational Patch PSA\*3.0\*83 will be reverted by restoring the executable to the previous version, 3.0.79.7.

### Load Testing

Not applicable to DAU.

### User Acceptance Testing

User Acceptance Testing for DAU is performed during the development of the DAU application. Testing will be conducted with a test user.

## Back-Out Criteria

Back-out will be considered if there is a catastrophic failure that causes loss of function for the DAU.

## Back-Out Risks

There are no back-out risks.

## Authority for Back-Out

The Facility CIO has the final authority to proceed with the back-out and accepts the associated risks.

## Back-Out Procedure

DAU is a standalone executable and does not require any special modification for removal. To remove DAU, delete the executable off of the user’s desktop and restore the PSA\_MCKESSON\_UPLOAD.exe Version 3.0.79.7 in the C:/. Create a new shortcut and copy to the user’s desktop, verify that the Version is 3.0.79.7.

## Back-out Verification Procedure

Ensure the executable or shortcut on the user’s desktop for Version 3.0.83.1 is removed and PSA\_MCKESSON\_UPLOAD.exe Version 3.0.79.7 has been restored.

# Rollback Procedure

Not applicable for PSA\*3.0\*83.

## Rollback Considerations

Not applicable for PSA\*3.0\*83.

## Rollback Criteria

Not applicable for PSA\*3.0\*83.

## Rollback Risks

Not applicable for PSA\*3.0\*83.

## Authority for Rollback

Not applicable for PSA\*3.0\*83.

## Rollback Procedure

Not applicable for PSA\*3.0\*83.

## Rollback Verification Procedure

Not applicable for PSA\*3.0\*83.