**VA Medical Care Collections Fund (MCCF)**

**Electronic Data Interchange (EDI)**

**Transaction Applications Suite (TAS)**

Version 1.2

Deployment, Installation, Back-Out, and Rollback Guide



January 2019

Department of Veterans Affairs

Office of Information and Technology (OI&T)

**Revision History**

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| January 24, 2019 | 1.2 | Added Docker/API notes (reviewed LC 01292018) | David Betz |
| December 21, 2018 | 1.1 | Document Revision | Cheryl Lach |
| July 22, 2018 | 1.0 | Baseline version of document based on EPMO template v2.2 dated March 2016 | David Loban |

**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 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 (CD2), 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](#_Toc533672436)

[1.1 Purpose 1](#_Toc533672437)

[1.2 Dependencies 1](#_Toc533672438)

[1.3 Constraints 1](#_Toc533672439)

[2 Roles and Responsibilities 2](#_Toc533672440)

[3 Deployment 4](#_Toc533672441)

[3.1 Timeline 4](#_Toc533672442)

[3.2 Site Readiness Assessment 4](#_Toc533672443)

[3.2.1 Deployment Topology (Targeted Architecture) 5](#_Toc533672444)

[3.2.2 Site Information (Locations, Deployment Recipients) 5](#_Toc533672445)

[3.2.3 Site Preparation 5](#_Toc533672446)

[3.3 Resources 5](#_Toc533672447)

[3.3.1 Hardware 5](#_Toc533672448)

[3.3.2 Software 6](#_Toc533672449)

[3.3.3 Communications 7](#_Toc533672450)

[3.3.4 Deployment/Installation/Back-Out Checklist 7](#_Toc533672451)

[4 Installation 8](#_Toc533672452)

[4.1 Pre-installation and System Requirements 8](#_Toc533672453)

[4.2 Platform Installation and Preparation 8](#_Toc533672454)

[4.3 Download and Extract Files 8](#_Toc533672455)

[4.4 Database Creation 8](#_Toc533672456)

[4.5 Installation Scripts 8](#_Toc533672457)

[4.6 Cron Scripts 10](#_Toc533672458)

[4.7 Access Requirements and Skills Needed for Installation 10](#_Toc533672459)

[4.8 Installation Procedure 10](#_Toc533672460)

[4.9 Installation Verification Procedure 10](#_Toc533672461)

[4.10 System Configuration 10](#_Toc533672462)

[4.11 Database Tuning 11](#_Toc533672463)

[5 Back-Out Procedure 11](#_Toc533672464)

[5.1 Back-Out Strategy 11](#_Toc533672465)

[5.2 Back-Out Considerations 11](#_Toc533672466)

[5.2.1 Load Testing 11](#_Toc533672467)

[5.2.2 User Acceptance Testing 11](#_Toc533672468)

[5.3 Back-Out Criteria 11](#_Toc533672469)

[5.4 Back-Out Risks 11](#_Toc533672470)

[5.5 Authority for Back-Out 11](#_Toc533672471)

[5.6 Back-Out Procedure 12](#_Toc533672472)

[5.7 Back-out Verification Procedure 12](#_Toc533672473)

[6 Rollback Procedure 12](#_Toc533672474)

[6.1 Rollback Considerations 12](#_Toc533672475)

[6.2 Rollback Criteria 12](#_Toc533672476)

[6.3 Rollback Risks 12](#_Toc533672477)

[6.4 Authority for Rollback 12](#_Toc533672478)

[6.5 Rollback Procedure 12](#_Toc533672479)

[6.6 Rollback Verification Procedure 12](#_Toc533672480)

**Table of Tables**

[**Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities 2**](#_Toc534288645)

[**Table 2: eBusiness Master Deployment Schedule 4**](#_Toc534288646)

[**Table 3: Site Preparation 5**](#_Toc534288647)

[**Table 4: Hardware Specifications 5**](#_Toc534288648)

[**Table 5: Software Specifications 6**](#_Toc534288649)

[**Table 6: Deployment/Installation/Back-Out Checklist 7**](#_Toc534288650)

# Introduction

This document describes how to deploy and install MCCF EDI TAS version 1.1*,* as well as how to back-out the product and rollback to a previous version or data set.

## Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom MCCF EDI TAS 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.

## Dependencies

MCCF EDI TAS is fully dependent on the MAG cloud in addition to the VA Austin Information Technology Center (AITC) to provide connectivity into VA private resources (e.g., VistA).

Though MCCF EDI TAS is dependent on Cosmos DB for storage of copied or summarized data, VistA remains the permanent and authoritative data source. User identify and access control services are provided by VA Identity and Access Management (IAM) services.

In this release, there are no changes related to Cosmo DB. MCCF EDI TAS v1.1 changes are specific to IAM Single Sign-On Internal (SSOi), wherein MCCF EDI TAS end-users will be granted access by invoking IAM services to authenticate their VA Personal Identity Validation (PIV) cards. MCCF EDI TAS support within IAM was previously deployed to MAG cloud production by the IAM team.

## Constraints

Microsoft Azure Government cloud is the target production environment. This environment is connected to the VA via an ExpressRoute connection.

MCCF EDI TAS is a web based application and must be compliant with NIST 508 and all other VA requirements for similar applications.

# Roles and Responsibilities

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

| **ID** | **Team** | **Role** | **Task** | **Project Phase**  **(See Schedule)** |
| --- | --- | --- | --- | --- |
| 1 | PMO | PM | Determine and document roles and responsibilities of those involved in the deployment. | USD&P |
| 1 | PMO | PM | Plan and schedule deployment | USD&P |
| 2 | PMO | PM | Plan and schedule installation | USD&P |
| 3 | eBusiness | POR | Coordinate training | Pre-Prod |
| 4 | PMO | PM | Ensure authority to operate and certificate authority security documentation is in place | Pre-Prod |
| 5 | PMO &  eBusiness | Functional Analyst & Product Owner | Test for operational readiness | Pre-Prod |
| 6 | Development | PM | Confirm availability of back-out instructions and back-out strategy (identify criteria warranting back-out) | Pre-Prod |
| 7 | Development | Configuration Manager | Execute deployment | Warranty |
| 8 | PMO &  eBusiness | Functional Analyst & Product Owner | Test for operational readiness | Warranty |
| 9 | Development | System Administrator | Hardware, Software and System Support | Warranty |

# Deployment

The deployment is planned as a single event installation making MCCF EDI TAS v1.1 readily available to all authorized users.

This section provides the schedule and milestones for the deployment.

## Timeline

Incremental functionality will be deployed according to business owner acceptance and CD2 approval throughout the life of the contract. Deployment of Release 1.1 is planned for 2QFY19.

Table 2: eBusiness Master Deployment Schedule

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Bld** | **Delivery** | **FY18** | | | | **FY19** | | | |
| **1Q** | **2Q** | **3Q** | **4Q** | **1Q** | **2Q** | **3Q** | **4Q** |
| 1-3 | Architecture Design;  TAS User Interface Standards and Link to eBusiness Solutions SP;  Initial ATO | Dev - UAT |  | Pre-Prod | Warranty |  |  |  |  |
| 4-5 | Architecture Refinement;  IAM Interface (AITC first, then MAG migration);  ATO Renewal | Dev - UAT | Dev - UAT | Pre-Prod |  |  | Warranty |  |  |
| 6 | FHIR & VistALink  ATO Renewal | USD&P | Dev - UAT | Dev - UAT |  |  | Pre-Prod  Warranty |  |  |
| 7 | Field Connectivity 837 eBilling Support  ATO Renewal |  | USD&P | Dev - UAT | Dev - UAT |  | Pre-Prod | Warranty |  |
| 8 | Reporting ePharmacy Support  ATO Renewal |  |  |  | Dev - UAT | Dev - UAT |  | Pre-Prod | Warranty |
| 9 | TBD  ATO Renewal |  |  |  |  | Dev - UAT | Dev - UAT | Pre-Prod | Warranty |

## Site Readiness Assessment

MCCF EDI TAS is deployed into the MAG cloud and as such, all mechanical and physical connections are considered to be part of the service. See Section 1.2 for additional details.

This section discusses the locations that will receive the MCCF EDI TAS v1.1 deployment.

### Deployment Topology (Targeted Architecture)

MCCF EDI TAS v1.1 will be released to a single WEB VM in the MAG cloud environment. Specifically, application code will be deployed to VAC20WEBTAS210.va.gov.

### Site Information (Locations, Deployment Recipients)

The MCCF EDI TAS project is deployed into the MAG cloud. The primary location is Microsoft’s facility in Virginia with a failover site planned for Austin, Texas. As web-based application and architecture, deployment to a single site makes processing available to end-users at all VA sites. Validation of deployment will be accomplished by the TAS functional analyst and the TAS business owner.

### Site Preparation

The MCCF EDI TAS ~~i~~s deployed into the MAG cloud and as such all site requirements are met and included in the subscription. Microsoft handles all physical resources, including power, racks, cooling, etc. MAG must be logically, not physical prepared. Preparation includes firewall configurations, as well as identity and access management configuration.

The following table describes preparation required by the site prior to deployment. **No site preparation is required for Release 1.1.**

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 |

## Resources

The MCCF EDI TAS project is deployed into the MAG cloud. Please refer to section 3.2.3 for additional details.

### Hardware

The following table identifies hardware specifications required in MAG prior to deployment.

Table 4: Hardware Specifications

| **Required Hardware** | **Server Function Type** | **Host Name** | **O/S** | **Model** | **RAM** |
| --- | --- | --- | --- | --- | --- |
| VM | FPC | vac20fpctas200 | Linux | A4m\_v2 4vCPUs | 32 GB |
| VM | WEB | vac20webtas210 | Linux | DS13-4\_v2 4vCPUs | 56 GB |
| *VM* | *WEB* | *vac20webtas211* | *Linux* | *TBD – Future Release* | *TBD* |
| *VM* | *APP* | *vac20apptas210* | *Linux* | *TBD – Future Release* | *TBD* |
| *VM* | *APP* | *vac20apptas211* | *Linux* | *TBD – Future Release* | *TBD* |
| *VM* | *DB* | *PAAS* | *Linux* | *TBD – Future Release* | *TBD* |
| *VM* | *APP* | *vac20apptas205* | *Windows* | *TBD – Future Release* | *TBD* |

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

### Software

The following table describes software specifications required in MAG prior to deployment.

Table 5: Software Specifications

| **Resource** | **Description** | **Version** |
| --- | --- | --- |
| RHEL | Red Hat Enterprise Linux | 7.3 |
| Encase | Provides the servlet needed for forensic examination of a Linux server by Encase | 1.0-2 |
| BESAgent | IBM BigFix Agent for Linux | 9.2.6.94-rhe5 |
| CentrifyDC | Centrify DirectControl Agent | 5.4.2-668 |
| ca-cs | CA McAfee Security Agent | N/A |
| Jenkins | Continuous Integration and Deployment Software to automate installation, build, and deployment of software | 2.73.3 |
| Ansible | Deployment and orchestration tool | 2.4.2.0 |
| SiteMinder | Provides policy-based authentication as well as single sign-on for Web-based applications | 12.51 cr08 |
| NPM | Package Manager for JavaScript | 5.x |
| Font Awesome | Enables customization of scalable vector icons used in CSS | 4.7.x |
| Apache HTTP Server | Provides a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards | 2.4.6-45 |
| Node.js | A JavaScript runtime built on Chrome’s VS Java Script engine | 8.x |
| PM2 | Advanced production process manager for Node.js | 2.4 |
| primeNG | A component library for Angular 2/4 that provides critical business UI functionality such as various data grids, pick lists, org charts, and autocomplete boxes. | 4.2 |
| AngularJS | Extends HTML vocabulary for an application so that the resulting environment is extraordinarily expressive, readable, and quick to develop. | 4.0 |
| U.S. Web Design System Framework | Open source UI components and visual style guide for U.S. government websites | 1.1.0 |

The software required to be deployed into the MAG cloud is a LINUX System image obtained from the VA Infrastructure Operations. All other required software is derived from either the VA Red Hat Satellite and/or the YUM Repositories, which includes the SiteMinder software added to this release, and/or the MCCF product specific repositories on the FPC servers. Cosmos DB is supplied as a PaaS (Platform as a Service).

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

### Communications

MAG provides monitoring and notification features which are used to alert technicians of errors.

If the system is down, or the application isn’t responding correctly due to other extenuating circumstances, the following actions should be taken:

* Determine if the system (servers) or if the software is not responding.

1. Is the server up and available?
2. Is the application responding?

* Notify the appropriate support personnel of the incident and document the incident following processes regarding system outage notification.
* Notify the user community that the system and/or software is unavailable.

### Deployment/Installation/Back-Out Checklist

MCCF EDI TAS and its components are provided as Software as a Service (SaaS). Software deployment makes new/revised functionality instantly available to end-users. If application operability is unacceptable for any reason, a back-out plan is not executed. Instead, a prior version is quickly redeployed from Rational Team Concert (RTC) using TAS automated deployments.

Table 6: Deployment/Installation/Back-Out Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| Activity | Day | Time | Individual to Complete Task |
| Deploy | 02-15-2019 | 3:00 PM ET | Configuration Manager |
| Install | Included above | Included above | Configuration Manager |
| Back-Out | N/A | N/A | N/A |

# Installation

## Pre-installation and System Requirements

The VA must provide a MAG cloud subscription with sufficient capacity for the listed hardware (Virtual Machines) and software. The VA must provide connectivity from the VA network to MAG, and the MAG environment must be set up for deployment to occur. A valid and usable RHEL 7.3 VM image must be available to deploy VMs. DNS must be accessible to validate domain registry. Centrify must be available to enable authentication.

## Platform Installation and Preparation

Ansible will handle automated installation and deployment of components applicable to Release 1.1.

**Builds/rebuilds are not a planned part of Release 1.1**, but instructions are provided for reference in the event of unplanned consequences. Instructions related to standing up MAG for the MCCF EDI TAS are contained in this document:



## Download and Extract Files

All MCCF EDI TAS software is pulled from the private VA satellite and MCCF repositories. All software deployment is managed by the Jenkins Continuous Integration automation tool which meets existing VA requirements.

## Database Creation

The MCCF EDI TAS utilizes the Cosmos DB which is Platform as a Service (PaaS). **Cosmos DB is not included in Release 1.1.**

## Installation Scripts

The installation of MCCF EDI TAS is managed by the Jenkins Continuous Integration automation tool. **No changes are planned in Release 1.1 to currently installed Jenkins**, but the installation process is provided in the event of unplanned problems. Jenkins installation process follows:

|  |  |  |
| --- | --- | --- |
| **Jenkins Continuous Integration Server Installation** | | |
| Order | Name | Location |
| 1 | installRTCToolsPipeline | Jenkins/INSTALL\_TASKS |
| 2 | InstallCITools | Jenkins/INSTALL\_TASKS |
| 3 | installFortifyPipeline | Jenkins/INSTALL\_TASKS |
| 4 | installGlobalNPM\_Packages | Jenkins/INSTALL\_TASKS |
| 5 | installSinopiaPipeline | Jenkins/INSTALL\_TASKS |
| 6 | installTomcatPipeline | Jenkins/INSTALL\_TASKS |

1. From the Jump Server (VAC20VHACRCB.VHA.MED.VA.GOV) login to the Jenkins Continuous Integration Server.
2. The Configuration Manager will login using their username and password
3. Select INSTALL\_TASKS
4. Select installRTCToolsPipeline->Build with Parameters
   1. Enter MAG\_PROD
   2. Click “Build” button
   3. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 3)
5. Select installCITools->Build with Parameters
   1. Enter MAG\_PROD
   2. Click “Build” button
   3. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 4)
6. Select installFortifyPipeline->Build with Parameters
   1. Enter MAG\_PROD
   2. Click “Build” button
   3. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 5)
7. Select installGlobalNPM\_Packages
   1. Enter MAG\_PROD
   2. Click “Build” button
   3. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 6)
8. Select installSinopiaPipeline->Build with Parameters
   1. Enter MAG\_PROD
   2. Click “Build” button
   3. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 7)
9. Select installTomcatPipeline->Build with Parameters
   1. Enter MAG\_PROD
   2. Click “Build” button
   3. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 8)

The Jenkins Continuous Integration automation outlined above is executed as outlined below to install Release 1.1 in MAG. Web installation process follows:

|  |  |  |
| --- | --- | --- |
| **Web and Application Server Installation** | | |
| Order | Name | Location |
| 1 | installWebserver | Jenkins/INSTALL\_TASKS |
| 2 | installNPM | Jenkins/INSTALL\_TASKS |
| 3 | installSiteminder | Jenkins/INSTALL\_TASKS |

Required software packages for the Web Servers are also installed from the Jenkins Continuous Integration Server.

1. From the Jump Server (VAC20VHACRCB.VHA.MED.VA.GOV) login into the Jenkins Continuous Integration Server.
2. The Configuration Manager will login using their username and password.
3. Select INSTALL\_TASKS
4. Select installWebserver->Build with Parameters
   1. Enter MAG\_PROD
   2. Click “Build” button
   3. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 3)
5. Select installNPM->Build with Parameters
   1. Enter MAG\_PROD
   2. Click “Build” button
   3. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 3)
6. Select installSiteminderWebAgent->Build with Parameters
   1. Enter MAG\_PROD
   2. Click “Build” button
   3. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 3)

## Cron Scripts

Cron scripts run nightly to extract VistA data for web-based reporting. **Cron scripts are not applicable to Release 1.1.**

## Access Requirements and Skills Needed for Installation

VA Information Security Management requires individuals to have permissions specific to one’s role and the resource being accessed. To create a VM, a user must have Virtual Machine Contributor role. **No new VMs will be created in Release 1.1.**

End user access to MCCF EDI TAS is managed through the VA IAM services, and is not applicable to the installation of Release 1.1.

## Installation Procedure

The installation of MCCF EDI TAS is managed by the Jenkins Continuous Integration automation tool. Refer to WEB installation in section 4.5 for installation scripts.

## Installation Verification Procedure

Each layer of the application has a set of tests which validate the performance of that layer’s functionality. This occurs prior to deployment. A health monitoring service endpoint exists to check system status. MAG uses the health monitoring service endpoint to monitor status and provide notifications of system issues.

Installation of Release 1.1 will be validated by a successful login by the TAS functional analyst and the TAS product owner.

## System Configuration

Configuration of Release 1.1 is specific to the SiteMinder Agent necessary to employ IAM SSOi. Configuration is accomplished automatically via TAS deployment automation.

## Database Tuning

**Database deployment processing is a future release and not applicable to Release 1.1.**

# Back-Out Procedure

Software deployment makes new/revised functionality instantly available to end-users. If application operability is unacceptable for any reason, a back-out plan is not executed. Instead, a prior version is quickly deployed from Rational Team Concert (RTC) using TAS automated deployments.

## Back-Out Strategy

Redeployment of software components for a prior version is performed as follows:

1. From the Jump Server (VAC20VHACRCB.BHA.MED.VA.GOV) login the Jenkins Continuous Integration Server.
2. The Configuration Manager will login using their username and password
3. Select MCCF\_TAS
4. Select the filename of the release to be deployed from this location: <https://vac20fpctas800.va.gov/rtc/tas>.
5. Select deploy\_RTC\_MCCF\_TAS\_Core->Build with Parameters
   1. Enter deployment\_filename obtained in step 4
   2. Enter MAG\_PROD
   3. Click “Build” button
   4. Ensure build completed successfully
      1. If build failed, research error and restart build (go back to Step 3)

## Back-Out Considerations

Successful deployment of Release 1.1 will be determined by the successful authentication of the TAS functional analyst and/or the TAS product owner.

### Load Testing

Usage volume will not change with the deployment of Release 1.1.

### User Acceptance Testing

Successful authentication of the TAS functional analyst and/or the TAS product owner. No other user acceptance testing is required.

## Back-Out Criteria

Unsuccessful authentication or non-responsive IAM processing.

## Back-Out Risks

None.

## Authority for Back-Out

TAS Functional Analyst or TAS Product Owner will determine if Release 1.1 is preserved or backed out.

## Back-Out Procedure

Refer to section 5.

## Back-out Verification Procedure

Refer to section 5.

# Rollback Procedure

**Database and/or data changes are not applicable in Release 1.1.**

## Rollback Considerations

N/A

## Rollback Criteria

N/A

## Rollback Risks

N/A

## Authority for Rollback

N/A

## Rollback Procedure

N/A

## Rollback Verification Procedure

N/A