Patient Centered Management Module (PCMM)

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



October 2026

WEBP*1.0*66

Department of Veterans Affairs

Office of Information and Technology

Revision History

Date	Version	Author	Description
10/06/2026	1.0	Booz Allen Hamilton/HDSO/PCMM Sys Admin	Baseline Version

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 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 the 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 as needed throughout the life cycle of the project for each build.

Table of Contents

1 Introduction 7
1.1 Purpose 7
1.2 Dependencies 7
1.3 Constraints 8
2 Roles and Responsibilities 9
3 Deployment 9
3.1 Site Readiness Assessment 9
3.2 Deployment Topology (Targeted Architecture) 9
3.3 Resources 9
3.3.1 Hardware 9
3.3.2 Software 10
3.3.3 Communications 10
3.4 Deployment/Installation/Back-Out Checklist 11
4 Installation 11
4.1 Pre-installation and System Requirements 11
4.1.1 Create Build Folder 2026.09.17-1.0-66-02 on App Server 11
4.1.2 Create Build Folder 2026.09.17-1.0-66-02 on Web Services Servers 11
4.2 Installation Procedure 11
4.2.1 Stop the Mirth Connect Service 11
4.2.2 Stop the SmartApp 11
4.2.3 Stop the Managed Servers, Delete the Old Builds 11
4.2.4 Add New Parameter to ciss.properties File 12
4.2.5 Delete Files from Managed Server Folders 12
4.2.6 Deploy the Latest Builds 12
4.2.7 Start the Mirth Connect Service 12
4.2.8 Start the SmartApp 12
4.3 Installation Verification Procedure 13
4.4 System Configuration 13
4.5 Database Tuning 13
5 Back-Out 13

5.1 Back-Out Procedures 13
5.2 Authority for Back-Out 13
6 Rollback Procedure 13
6.1 Rollback Considerations 14
6.2 Rollback Criteria 14
6.3 Rollback Risks 14
6.4 Authority for Rollback 14
6.5 Rollback Procedure 14
6.6 Rollback Verification Procedure 14
7 Risk and Mitigation Plan 14
8 Checksums 14
Appendix: Acronyms and Abbreviations 16

List of Tables

Table 1 – PCMM Application Dependencies 7
Table 4 – Hardware Specifications 9
Table 5 – Software Specifications 10
Table 7 – Acronyms and Abbreviations 16

List of Figures

No table of figures entries found.

1 Introduction

This document describes how to deploy and install the Patient Centered Management Module (PCMM) release WEBP*1*66 and how to back out and roll back to a previous version or dataset.

This document further details the criteria for determining if a back-out is necessary, the authority for making that decision, the order in which installed components will be backed out, the risks and criteria for a rollback, and the authority for acceptance or rejection of the risks.

1.1 Purpose

The purpose of this document is to provide a single, common plan that defines how the VA PCMM implementation will be deployed and installed, including how it is to be backed out and rolled back, if necessary.

The plan also identifies resources, a communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2 Dependencies

The PCMM application is dependent on the following systems, applications, and services:

Table 1 – PCMM Application Dependencies

Dependency	Type	Dependency Type	PCMM Use
Cerner Millennium	System	System	Cerner EHR solutions share a single design, which eases information sharing across care teams and venues. Care teams across the continuum use the system to document and access critical patient data, streamline workflows, and help with patient safety for active-duty service members, dependents, and Veterans.
Cerner OPENLink	Service	Data/Information	The Cerner interface engine provides extensive data transformation, message routing, and communications-protocol bridging.
VA SSH File Transfer Protocol (SFTP) Site	Service	Data/Information	The SFTP Site will be set up by the OEHRM group to allow for file transfers between VA and Cerner for various data-migration and syndication activities, including transfer of the patient, staff, and encounter files discussed in this document.

Dependency	Type	Dependency Type	PCMM Use
Corporate Data Warehouse (CDW)	Service	Data/Information	CDW is an internal data service that interacts with and queries CDW-cached data. Data will be a scheduled task to load CDW into the PCMM environment. CDW data will reside within PCMM for lookup and reference within the PCMM decision logic. The data will have their own designated datastore due to being relational data.
Clinical Information Support System (CISS)	System	System	PCMM utilizes the Clinical Information Support System (CISS) framework as part of its implementation but does not share a CISS portal with any other application or partner systems outside of PCMM functionality
VistA	System	System	Synchronizes CPRS header information from VistA for PCP assignment status or Mental Health Treatment Coordinator (MHTC) assignment.
Master Patient Index (MPI)	System	System	Registers a patient from MPI broadcast messages and updates patient traits from MPI.

1.3 Constraints

The PCMM project team, software, and test servers will adhere to the following directives, policies, procedures, standards, and guidelines:

- Veteran-focused Integration Process (VIP)
- Section 508 Information Technology (IT) accessibility standards governed under 29 U.S.C 794d
- Health Insurance Portability and Accountability Act (HIPAA)
- VA DIRECTIVE 6508 – Privacy Impact Assessments
- VA Directive 6500 – Information Security Program
- One (1) VA Technical Reference Model (TRM)
- VA Standards & Conventions Committee (SACC) Codes Standards and Conventions
- PCMM will pass any Web Application Security Assessment (WASA) scans
- PCMM will not have any critical or high issues identified by a Fortify scan

2 Roles and Responsibilities

The following table identifies the interface's deployment, installation, back-out, and rollback roles and responsibilities.

3 Deployment

The deployment is planned as an iterative rollout.

3.1 Site Readiness Assessment

The PCMM application will exist within the VA Enterprise Cloud (VAEC) for SQA, ETS, INT, and production environments. The PCMM development team will maintain a local DEV environment to be used for sprint development and testing processes.

3.2 Deployment Topology (Targeted Architecture)

The figure below details the PCMM Deployment Topology (Targeted Architecture).

3.3 Resources

This section describes hardware, software, facilities, documentation, and any other resources, other than personnel, required for deployment and installation.

3.3.1 Hardware

PCMM is an enterprise application hosted at the VA Austin Information Technology Center (AITC).

The PCMM servers consist of eight virtual servers (VM), consisting of three application servers to accommodate end-user work, two application servers to support web service calls, and two database servers and one file share server to act as a quorum witness to the database cluster. Redundancies are achieved through replication of data at both the OS and application levels.

The architectural design of each group consists of different redundancies:

- The database servers are clustered at the Operating System (OS) level and database-application level. They are connected to a NetApp Data Storage to provide additional storage, redundancy, and availability.
- The application servers are not clustered at the OS level, but at the application level in two clusters: attended and unattended. Currently, the attended cluster contains one WL server, and the unattended cluster contains two WL servers. OS-level implemented synchronization and application clustering maintain the redundancies.

Table 2 – Hardware Specifications

Required Hardware	Quantity	Version	Configuration
Application Server	1	Linux-RHEL8.9	Attended Linux application server with WebLogic and Apache Web Server
Application Server	2	Linux-RHEL8.9	Unattended application servers with WebLogic
Application Server	2	Linux-RHEL8.9	Web services servers with WebLogic
Database Server	2	Windows 2019	Windows database server for PCMM-Web application
File Share Server	1	Windows 2019	Windows File Share Server

3.3.2 Software

The following table describes software specifications required prior to deployment. If there are site-dependent differences, those differences will need to be provided.

Table 3 – Software Specifications

Required Software	Manufacturer	Version	Configuration
Oracle WebLogic Server	Oracle	12.2.1.4.0	Standard
Java™ SE Development Kit 8	Oracle	1.8.0_501 (or higher)	Standard
Microsoft SQL Server	Microsoft	2019 (or higher)	Standard
Microsoft SQL Server Management Studio (SMS)	Microsoft	2019 (or higher)	Standard
Apache	Apache	2.4.6 (or higher)	Standard
jTDS driver	SourceForge	jtds-1.3.1.jar	Standard
VistALink	VistA	1.6	Standard
Mirth Connect	NextGen	4.7 (or higher)	Standard

3.3.3 Communications

- Notifications of scheduled maintenance periods that require the service to be offline or that may degrade system performance will be disseminated to the business-user community a minimum of 48 hours prior to scheduled events.
- Notifications to VA users for unscheduled system outages or other events that impact response times will be distributed within 30 minutes of an occurrence.
- Notifications to VA users for unexpected system outages or other events that impact the response time will be distributed to users as soon as possible.
- Notifications will be distributed to VA users regarding technical help-desk support for obtaining assistance with receiving and processing.

3.4 Deployment/Installation/Back-Out Checklist

The table below outlines the coordination effort and documents completed by individual and the day and time when each activity (deploy, install, and back-out) is completed for PCMM.

4 Installation

4.1 Pre-installation and System Requirements

4.1.1 Create Build Folder 2026.09.17-1.0-66-02 on App Server

On [REDACTED], create folder /u01/app/BUILDS/2026.09.17-1.0-66-02. Copy the following ear files into the folder: pcmmr_ear-1.0-66-02.ear, pcmmr_unattended_ear-1.0-66-02.ear, and cissUserManagement-1.0-66-01.ear.

4.1.2 Create Build Folder 2026.09.17-1.0-66-02 on Web Services Servers

On [REDACTED], create folder /u01/app/BUILDS/2026.09.17-1.0-66-02. Copy the following ear file into the folder: pcmmr_ear-1.0-66-02.ear.

4.2 Installation Procedure

4.2.1 Stop the Mirth Connect Service

On [REDACTED], stop the Mirth Connect service

```
dzdo service mcservice stop
```

4.2.2 Stop the SmartApp

On [REDACTED], stop the SmartApp process.

NOTE: Do these steps as the nodejs user

```
ps -ef | grep nodejs
```

Kill the process associated with `node ./smartApp.js`

4.2.3 Stop the Managed Servers, Delete the Old Builds

In the WebLogic console on [REDACTED], stop managed servers, Srv1, Srv2, and Srv4. Delete the previous pcmmr, pcmmr_unattended, and cissUserManagement deployments.

In the WebLogic console on [REDACTED], stop managed server, Srv1. Delete the previous pcmmr deployment.

4.2.4 Add New Parameter to ciss.properties File

On [REDACTED] make a backup of the current ciss.properties file in the PCMM_Domain/properties/pcmmProperties/SrvX folder.

Add this parameter to ciss.properties on each server:

```
hibernate.temp.use_jdbc_metadata_defaults=false
```

4.2.5 Delete Files from Managed Server Folders

On [REDACTED], delete cache, stage, and tmp folders below from the managed server folders.

```
cd /u01/app/oracle/user_projects/domains/PCMM_Domain/servers/Srv1
rm –rf ./cache/
rm –rf ./stage/
rm –rf ./tmp/
```

On [REDACTED], repeat the steps for Srv2 and Srv4 folders respectively.

4.2.6 Deploy the Latest Builds

In the WebLogic console on [REDACTED], deploy the pcmmr_ear-1.0-66-02.ear, pcmmr_unattended_ear-1.0-66-02.ear, and cissUserManagement-1.0-66-01.ear.

For pcmmr, target the Attended Cluster and set the deployment order to 95.

For pcmmr_unattended, target the Unattended Cluster and set the deployment order to 95.

In the WebLogic console on [REDACTED], deploy the pcmmr_ear-1.0-66-02.ear.

Target the Attended Cluster and set the deployment order to 95.

Start all the deployments and start all the managed servers.

4.2.7 Start the Mirth Connect Service

Once all deployments have started on [REDACTED], start the Mirth Connect service from [REDACTED].

```
dzdo service mcservice start
```

4.2.8 Start the SmartApp

Logon to [REDACTED]and switch to the nodejs user, then run the following commands:

```
cd /u01/app/SmartApp
startNodeJS
```

4.3 Installation Verification Procedure

The PCMM Sustainment Team will perform the standard smoke test for PCMM, plus UM smoke test.

4.4 System Configuration

System configuration changes are not applicable for this installation.

4.5 Database Tuning

Database adjustments are not applicable for this installation.

5 Back-Out

Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings.

5.1 Back-Out Procedures

1. On [REDACTED], stop the WebLogic managed servers, Srv1, Srv2, and Srv4.
2. Delete the new pcmmr_ear-1.0-66-02.ear, pcmmr_unattended_ear-1.0-66-02.ear, and cissUserManagement-1.0-66-01.ear deployments.
3. On [REDACTED], deploy and start the previous ear files:
   /u01/app/BUILDS/2026. 08. 20-1.0-65-03/pcmmr_ear-1.0-65-03.ear,
   /u01/app/BUILDS/2026.08.20-1.0-65-03/pcmmr_unattended_ear-1.0-65-03.ear,
   /u01/app/BUILDS/2026.08.20-1.0-65-03/cissUserManagement-1.0-65-03.ear

   On [REDACTED], deploy and start the previous ear file:
   /u01/app/BUILDS/2026.08.20-1.0-65-03/pcmmr_ear-1.0-65-03.ear
4. Copied the backed up ciss.properties file back into place on every server.
5. Start the WebLogic managed servers and proceed with testing.

5.2 Authority for Back-Out

Based on authority provided by the business sponsor and VA OIT IT program manager, PCMM can be backed out in accordance with their approval.

6 Rollback Procedure

Rollback pertains to data associated with this PCMM interface.

6.1 Rollback Considerations

It is necessary to determine if a wholesale rollback of the data associated with the PCMM interface is needed or if a better course of action would be correcting the data through a new version of the patch (if prior to a national release) or through a subsequent patch aimed at specific areas modified or affected by the original patch (after a national release).

6.2 Rollback Criteria

The decision to perform a wholesale rollback for this installation will be made by the business sponsor(s) and VA OIT IT program manager. Criteria will be determined based on separate and unique factors and evaluated upon post-installation use of the product.

6.3 Rollback Risks

There are no risks identified to perform a wholesale rollback of the database and deployment.

6.4 Authority for Rollback

Based on authority provided by the business sponsor and VA OIT IT program manager, PCMM can be rolled back in accordance with their approval.

6.5 Rollback Procedure

The rollback procedure steps are documented in Section 5.1 for the application and infrastructure. The back-out instructions are the same as those for the rollback of the application.

6.6 Rollback Verification Procedure

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

7 Risk and Mitigation Plan

The PCMM project team maintains a Program Risk Registry. Refer to this for all risks and mitigation plans for the PCMM project, including PCMM Web and VistA integration and the rest of the VA partner interfaces (Cerner Millennium, Cerner OpenLink, VA SFTP Site, and VA CDW).

8 Checksums

Below are the sha256 checksums for the PCMM 1.66 Release ear files. These checksums will be validated against the checksums on the Production PCMM servers before the ear files are deployed.

Patient Centered Management Module

[REDACTED]

Appendix: Acronyms and Abbreviations

Table 4 – Acronyms and Abbreviations

Acronym / Abbreviation	Definition
AITC	Austin Information Technology Center
AWS	Amazon Web Services
COTS	Commercial off-the-Shelf
CDW	Corporate Data Warehouse
CISS	Clinical Information Support System
CPU	Central Processing Unit
DAS	Data Access Service
DB	Database
DDL	Data Definition Language
ETL	Extract - Transform – Load
ETS	Enterprise Testing Service
EHR	Electronic Health Record
EHRM	Electronic Health Record Modernization
GovCloud	Government Cloud
HIE	Health Information Exchange
HL7	Health Level 7
HIPAA	Health Insurance Portability and Accountability Act
IAM	Identity and Access Management
IOC	Initial Operating Capability
IT	Information Technology
PCMM	Patient Centered Management Module
OIT	Office of Information and Technology
OEHRM	Office of Electronic Health Record Modernization
QA	Quality Assurance
SaaS	Software as a Service
SACC	Standards & Conventions Committee
SFTP	SSH File Transfer Protocol

Acronym / Abbreviation	Definition
TRM	Technical Reference Model
UAT	User Acceptance Testing
VA	U.S. Department of Veterans Affairs
VAMC	Veterans Affairs Medical Center
VIP	Veteran-focused Integration Process
VISN	Veterans Integrated Service Network
VistA	Veterans Information Systems and Technology Architecture
VM	Virtual Machine
WASA	Web Application Security Assessment