Dental Record Manager Plus (DRM Plus) Application

Installation Guide

DENT*1.2*90

Version 1.2

April 1989 (VA Release)

(Revised June 2024)

Department of Veterans Affairs
Office of Information and Technology (OI&T)
Enterprise Program Management Office

Installation Guide

DENT*1.2*90 **June 2024**

Table of Contents

Pre-Installation Considerations

This release of DRM Plus consists of only an executable.

******NOTE******

DENT*1.2*90 is to be nationally released to all VAMCs using DRM Plus.

VAMCs using eDRM (Cerner) should **NOT** install the updated executable or KIDS build released with this patch.

****

Installation Procedure

The DENT*1.2*90 patch is available on Forum. The DRM Plus GUI and documentation are available at the following location:

The ZIP file may be obtained at:

/srv/vista/patches/SOFTWARE/DENT_1_2_90.ZIP

Documentation describing the details is included in this release. Documentation can be found on the VA Software Documentation Library (VDL) at: https//www.va.gov/vdl/

The documentation includes:

File Description	File Name	FTP Mode
Dental ZIP file	DENT_1_2_90.zip	BINARY

The DENT_1_2_90.zip file contains the following files:

Title	File Name	FTP Mode
DRM Plus Release Notes	DENT_1_2P90_RN.pdf	Binary
DRM Plus Installation Guide	DENT_1_2P90_IG.pdf	Binary
DRM Plus Technical Manual	DENT_1_2P90_TM.pdf	Binary
DRM Deployment, Installation, Backout & Rollback Guide(DIBORG)	DENT_1_2P90_DIBR.pdf	Binary
DRM Plus (9.0.0.4)	dentalmrmtx.exe	Binary

Patch Installation

==========

Pre/Post Installation Overview

THE FOLLOWING NEEDS TO BE COMPLETED FOR THIS PATCH TO WORK PROPERLY

There is no KID file with this patch. Site installation personnel need to place the DRM Plus executable (dentalmrmtx.exe) from the zip file in the appropriate directory.

Installation Instructions

Users must exit the DRM Plus application; the existing dentalmrmtx.exe

and users should not access DRM Plus until all post-installation steps are complete.

All open DRM Plus GUI applications should be closed (no users should be using the application).

It is not necessary to disable any DENTV* options.

Installation Instructions

GUI Installation:

1. Move dentalmrmtx.exe to the root of ...\DOCSTORE
   (replace existing file)
   '...\' indicates your path for where DRM Plus is located
   The version of the new exe is 9.0.0.4

Back-out Procedure

Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings. Successful back-out requires successful backup prior to installing software. Please read the Dental Record Manager Plus (DRM Plus) Application Deployment, Installation, Backout, and Rollback Guide for detailed instructions.

Back-out Strategy

The DRM Plus back-out strategy involves communication with stakeholders including site users, OI&T, help desk, developers, quality assurance, and any others such as VA business owners. This communication allows all parties to have an impact on the decision to back-out software, and to act on the plan to restore the environment(s) to a previous, working state. Step by step instructions are followed. Each installation will include specific back-out procedures relevant to the components and to the changes made to the system. Back-out may involve copying a previous version of an executable onto a production server or restoring VistA routines from a transport global.

Successful back-outs require conscientious following of installation steps, especially for any backup procedures. For example, the steps may state that installers copy the previous version of an executable to a safe storage area. If a previous version is not available at the site, DSS, Inc. will provide the necessary version of the software using SFTP or another approved transfer method. After the back-out, tests are performed to ensure the software is working, and then stakeholders are notified. A remediation plan is put into place to correct the issue(s) necessitating a back-out.

VistA KIDs builds cannot be backed out/restored in totality – only routines are part of a backup transport global. Special care is taken during development of VistA code (routines, files, remote procedures, etc.) to make them backward compatible with newer GUI versions to alleviate the issue and avoid typical critical scenario solutions such as emergency patches.

The decision to back-out a specific release needs to be made in a timely manner. Catastrophic failures are usually known early in the testing process – within the first two or three days. Sites are encouraged to perform all test scripts to ensure new code is functioning in their environment, with their data. A back-out should only be considered for critical issues or errors. The normal, or an expedited, issue-focused patch process can correct other bugs.

Back-out Considerations

Back-outs are not desirable, and the decision to back-out should involve stakeholders from various business units. A back-out should be performed as early after installation as possible to avoid issues with data (see roll-back section). If data corruption has occurred, or will occur, then sometimes it is safer to create an emergency fix to correct the problem, rather than return to a previous state.

Back-out Criteria

Stakeholders involved in the decision to back-out software should be prepared to answer the following questions:

- Was the installation performed correctly and completely? Installed component versions should be verified.
- What component(s) failed?
- Are failures specific to a user, or to all users? Failures for a specific user may be hardware or parameter setting-based issues (user profile, etc.).
- Is there a work-around for the failure?
- Is data involved in the failure?
- Who will make the decision to revert to a previous version?
- Who will perform the back-out?
- How soon can the back-out be performed?
- Does the staff responsible for the back-out understand the procedures?
- How soon after the decision has been made will the back-out be performed?
- What is the expected time required to perform a reversion?
- What are the communication procedures required in the event of a back-out?
- Has the Back-out Plan been successfully tested?
- What are the success criteria to be used to denote a successful back-out?

Back-out Risks

DSS, Inc. develops VistA KIDs builds to be backward compatible with previous versions to avoid back-out risks.

When a back-out is necessary, the instructions may include stopping to verify data and/or versions after certain steps. Following instructions carefully will mitigate back-out risks.

Authority for Back-out

For DENT*1.2*90, the VA Business owner has ultimate responsibility for the product. The business owner or their designee will make the decision to back-out an installation based on feedback from the stakeholders (users, DSS Development, DSS Installation, DSS Support, etc.)

Back-out Summary

For VA server components, the procedures can be performed in VA test account environments prior to performing them in the production account.

1. Notify stakeholders using MS Outlook.
2. Ensure users are not using DRM Plus.
3. If the development team has determined that the VistA routines should be restored, load the backup transport global (saved in Mailman during the installation process) and install the prior routines.
4. Enable access to users.
5. Test the software
6. Notify stakeholders of the outcome via Outlook.

MISCELLANEOUS INFORMATION
==========
DSS (Document Storage Systems): Help Desk: **REDACTED**
Hours of Operation: 8:00 AM TO 7:00 PM (ET) After-Hours Support: **REDACTED**

VA Enterprise Service Desk: **REDACTED**