Dental Record Manager Plus (DRM Plus) Application

Installation Guide

DENT*1.2*72

Version 1.2

October 2018

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

Installation Guide

DENT*1.2*72 SEQ #70, dentalmrmtx V7.2.0.6 **October 2018**

Table of Contents

Pre-Installation Consideratons

The purpose of this patch is to ensure compatibility with the Windows 10 operating system update.

Installation Procedure

The DENT*1.2*72 patch is available on Forum. The DRM Plus EXEs and documentation are available on the ANONYMOUS SOFTWARE directory at one of the following Office of Information (OI) Field Offices. Sites may retrieve documentation in one of the following ways:

(1) The preferred method is to FTP the files from download.vista.med.va.gov, which will transmit the files from the first available server.

(2) Sites may also elect to retrieve the software and/or documentation directly using Secure File Transfer Protocol (SFTP) from the ANONYMOUS.SOFTWARE directory at the following OI Field Offices:

Hines	fo-hines.med.va.gov
Salt Lake	fo-slc.med.va.gov

The documentation will be in the form of Adobe Acrobat files. Documentation can also be found on the VA Software Documentation Library at:
https://www.va.gov/vdl/

The documentation includes:

File Description	File Name	FTP Mode
Dental ZIP file w/ exe	DENT_1_2_72.zip	BINARY

The DENT_1_2_72.zip file contains the following files:

File Name	Description
Dent_1_2p72_ig.pdf	DENT*1.2*72 installation guide
Dent_1_2p72_rn.pdf	DENT*1.2*72 release notes
Dent_1_2p72_tm.pdf	Technical Manual/Security Guide
dentalmrmtx.exe	DRM Plus v7.2.0.6
setupP72.exe	DRM Plus Component Installer v7.2.0.2

Users must exit the DRM Plus application in order to copy the executable to the appropriate production server. All open DRM Plus GUI applications should be closed (no users should be using the application).

Installation Instructions

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 v7.2.0.6

2. Run setupP72.EXE, on all Windows Workstations, Thin Client Servers, Windows Terminal Services Servers and Citrix Servers that need to launch the dentalmrmtx.exe that you moved to \DOCSTORE. These files are NOT run on the machine that hosts the \DOCSTORE folder. SetupP72.EXE is also required for new installs.

   Note: On some Windows Server machines the setupP72.EXE file will not update the CVision.ocx file in the \SysWOW64 directory. If the CVision.ocx version isn't 2.5.0.404 then Microsoft's Data Execution Prevention (DEP) may be the issue. Turn DEP off (call DSS tech support if you need help with this), reboot the machine and install the client side files by running setupP72.EXE. Additional information on DEP can be found at: http://support.microsoft.com/kb/875352

****

Please be careful to coordinate the server/client updates with each other so that the dental application works properly. You will know if the server/client files are NOT compatible because launching DRM Plus will cause approximately 30 client errors! This also means that you must carefully coordinate testing the new application in the TEST account since you must run setupP72.exe on a rarely used machine for the dental staff to test against, as they will not be able to run the production application after updating the client.

****

These are the NEW compatible DRM Plus files for patch 72:

dentalmrmtx.exe	v7.2.0.6	dated 10/22/2018 (server)
setupP72.EXE	v7.2.0.2	dated 04/18/2018 (client)

setupP72.EXE installs:

CVision.ocx	v2.5.0.404	dated 2/20/2018
cvlib2.dll	v2.5.0.12	dated 2/09/2018

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.

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 Backout 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. For existing DRM Plus sites, the DENT*1.2*72 release is backward compatible and should not require back out.

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*72, 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. Uninstall the setupP72.exe
4. Install the setupP66.exe – note this is the last version of the component install.
5. Install the previous version of DRM Plus executable (dentalmrmtx.exe v 6.9.0.116).
6. Enable access to users.
7. Test the software
8. Notify stakeholders of the outcome via Outlook.

MISCELLANEOUS INFORMATION
==========
DSS (Document Storage Systems):
Help Desk: 561-284-7200
Hours of Operation: 8:00 AM TO 7:00 PM (ET)
After-Hours Support: 561-284-7200, Option 1

VA Enterprise Service Desk: 855-673-4357