DSS Order Tracking Manager Laboratory (DSS OTM-Laboratory) Web Application

Technical Manual and Security Guide

December 2020
Version 1.0

Department of Veterans Affairs
Document Storage Systems (DSS), Inc.

Revision History

Date	Version	Description
Dec 2020	1.0	Initial Version

Table of Contents

1. Product Description....1
   1.1. About this Guide....1
   1.2. Referenced Documents....1
   1.3. Section 508 Compliance....2
2. System Requirements....2
   2.1. Web Server Hardware....2
   2.2. Web Server/Application Software....2
   2.3. VistA and InterSystems Cache....4
3. VistA Routines....4
4. VistA Remote Procedure Calls....4
5. VistA Files....5
6. VistA Options....5
7. VistA Parameter Definitions....5
8. VistA Security Keys....5
9. VistA External Packages....5
10. Security....6
   10.1.VA Directive 6500....6
   10.2.VA Directive 6515....6
   10.3.Authentication and Authorization....6

1. Product Description

This is the first build of DSS Order Tracking Manager Laboratory GUI application. Order Tracking Manager (OTM) **Laboratory** is a web-based application pulling real-time information from VistA for the purpose of assisting staff who have a role with laboratory orders. Keeping your hand on where labs are for each patient is a huge task for providers. Knowing that labs have been ordered, if they have been collected and/or when they resulted then seeing those results in one nicely organized view is the goal of OTM Laboratory. Users can select which highly visible lab tests to monitor to create customized tracking filters. The application knows which labs you have ordered for each patient and will show you highly visible out of range (low or high) results.

The KIDS build DSSD 1.0 T2 supports the OTM Laboratory User Interface (UI) web-based application. The UI has a separate installation guide and release notes.

There are three components to the OTM application to comply with VA Enterprise Technical Architecture (ETA) three-tier, service-oriented architecture (SOA) design patterns.

1. **Web Application User Interfaces (UI):** Front end written in HTML5, CSS, and JavaScript.
2. **DSS VistA SOA Suite (VSOA): L**ightweight middle tier providing RESTful communication to VistA. VSOA is a separate DSS product used by other DSS web applications and is not discussed in detail in this manual.
3. **DSSD KIDS**: M application that resides within VistA to read/write data to/from the UIs. DSSD 1.0 supports OTM. The namespace for all components is DSSD*.

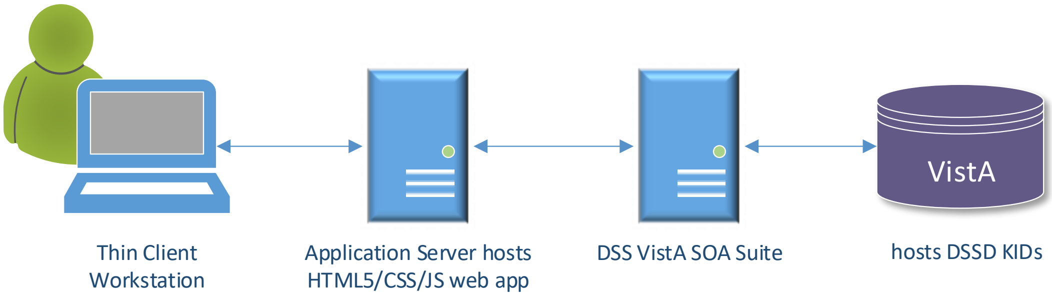

Figure 1: Architecture Overview Diagram

1.1. About this Guide

The *DSS Order Tracking Manager (OTM) Technical Manual* provides technical information about the application architecture and information for installing, configuring, managing, and troubleshooting local components of the OTM application.

1.2. Referenced Documents

The following documents and files are available via DSS Support Services or the OTM Product Line Manager:

- DSSD 1.0 Installation Guide
- DSSD 1.0 Release Notes

- OTM Install Guide (includes VSOA.js)
- DSS VistA SOA Suite Overview

1.3. Section 508 Compliance

OTM is Section 508 compliant. DSS tests and self-certifies all applications prior to installation within VA environments. We can provide test results upon request.

2. System Requirements

This section covers hardware and software requirements for successful installation of OTM. For details about the SOA middle tier, VSOA.js, the DSS VistA SOA Suite Overview document can be provided by DSS.

2.1. Web Server Hardware

OTM is a browser-based software application. The UI component runs on a client's web browser using HTML5, CSS, and JavaScript (JS) and requires application servers to support bi-directional messaging with the database. OTM use VistA as the database of record for all transactions. As server-based software, the server hardware sizing requirements for CPU, memory, disk, network bandwidth are driven by the size of the audience. The software can run on minimal server hardware for light use but will require additional horsepower to provide services to larger groups of users (specifically when multiple OTM modules are used at a site).

A typical thin client application will involve the following server components:

Component	Description	Server
Thin Client Application	Thin Client supporting HTML, CSS, and JS files located on a web server.	HTTP / Web Server
Application Server	Custom Application Specific Business Logic Layer, possibly including an application specific database.	RESTful Application Server
VSOA.js Server	VistA Web Service Provider. Composed of web services that are specific VistA RPC web service methods	VSOA Server

The server components are to be deployed on two or more physical (or virtual) servers, but are capable of running on a single server with multiple network interfaces. Implementation decisions can be made by sites with assistance from DSS technical resources.

For the physical or virtual server, Windows 2019 are recommended in standard VA Office of Information & Technology, Continuous Readiness in Information Security Program (CRISP) compliant configuration.

2.2. Web Server/Application Software

Client workstation web browsers are responsible for viewing and interacting with the delivered HTML web application. The browser application is a combination of HTML5, JavaScript and CSS. A modern HTML5-compliant browser is required for use. OTM performs best using Chrome.

There are four primary components required for OTM:

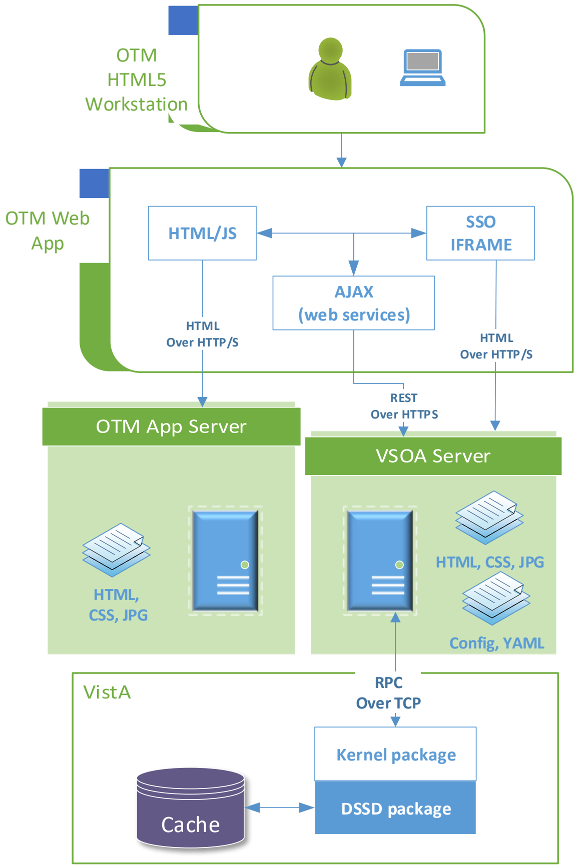

Figure 2: Architecture Diagram

1. Thin Client Web App – a responsive user interface (UI) composed of presentation-only component that interfaces with web services hosted by an Internet application server. We construct our thin client applications with standards compliant HTML5, CSS, and JavaScript software. Our UI adapts to the varying display sizes of end-user computing devices ranging from mobile devices to laptops and desktop/workstation with modern web browsers.
2. App Server – hosts application-specific business logic and communicates downstream to VA services such as IAM and ultimately VSOA and VistA. Application Services are provided exclusively for use by the Web App and are made available in the form of RESTful Web Services that transport data as JSON data structures.
3. VSOA.js Server – contains a node.js based web service platform customized to provide rapid development of services in an SOA environment. VSOA's purpose is exclusively to host RESTful web services for VistA-based processes. VSOA can support multiple VistA instances and can be installed at local or regional data centers.
4. The DSSD VistA Kernel and Distribution System (KIDS) file provides database APIs for the web UI.

All OTM processes use JavaScript. That includes JavaScript running on the browser and JavaScript running on the server. The OTM servers *serve* JavaScript (and CSS and HTML) to browser-based clients. The JavaScript delivered to browsers run on the browsers. But in addition, OTM servers also *service* web requests (SOA Services). Like all development languages and technologies, both the JavaScript development for the browsers and the JavaScript development running on the servers is complemented by very large development communities and their open-source software libraries.

2.3. VistA and InterSystems Cache

The DSSD 1.0 KIDS build is required, along with existing legacy applications, to support all OTM functions. DSSD 1.0 will run on multiple InterSystems Cache releases including 2011, 2014, 2017, etc. with no special modifications. See the DSSD 1.0 Installation Guide for details and example installation of the KIDS build.

DSS OTM-Laboratory requires the Patient Flow Suite, DSSW 1.0, build. Without DSSW 1.0, DSSD 1.0 cannot be installed.

Once the DSSD 1.0 KIDS build is installed, VA Information Technology (IT) personnel must assign secondary menu options to appropriate users.

3. VistA Routines

The DSSD KIDS build contains a number of routines which encapsulate the business rules for the database interaction.

```
             FIRST LINE LIST   UCI: VAH,ROU   12/09/2020
DSSDPAT   ;DSS/KC - Patient Header ; Dec 09, 2020@13:49
          ;;1.0;DSS OTM LABORATORY;;Dec 9, 2020;Build 2
          ;Copyright 1995-2020, Document Storage Systems, Inc., All Rights Reserved
DSSDPOB   ;DSS/KC - Pending Obsolete Orders ; Dec 09, 2020@13:49
          ;;1.0;DSS OTM LABORATORY;;Dec 09, 2020;Build 2
          ;Copyright 1995-2020, Document Storage Systems, Inc., All Rights Reserved
DSSDUTL   ;DSS/KC - Utility RPCs ; Dec 09, 2020@13:49
          ;;1.0;DSS OTM LABORATORY;;Dec 09, 2020;Build 2
          ;Copyright 1995-2020, Document Storage Systems, Inc., All Rights Reserved
DSSDVW    ;DSS/KC - Lab Worklist View ; Dec 09, 2020@13:49
          ;;1.0;DSS OTM LABORATORY;;Dec 09, 2020;Build 2
          ;Copyright 1995-2020, Document Storage Systems, Inc., All Rights Reserved
```

4. VistA Remote Procedure Calls

Remote Procedures (RPCs) describe the input parameters, tag, routine and output for APIs used by the web application. RPCs are converted to web services using VSOA.js, where YAML files contain the OpenAPI documentation accessible to web developers. VSOA.js allows the data returned by an RPC to be formatted in JavaScript Notation (JSON).

```
REMOTE PROCEDURE List                                NOV 05, 2020@15:14   PAGE 1
NAME
    DESCRIPTION
--------------------------------------------------------------------------------


DSSD PATIENT FLAGS
       Returns JSON array containing the patient flags
DSSD PENDING OBSOLETE
       Returns a list of lab orders soon to be "obsoleted" (cancelled by the lab)
       based on LRJPON
DSSD PENDING OBSOLETE PARAMS
       Returns the system settings controlling the auto-cancel/obsolete of pending lab
       orders.
DSSD VIEW ORDERS BY PROVIDER
       Returns a list of lab orders by provider for a date range.
```

5. VistA Files

During analysis of the business requirements for OTM, the DSS team determined that no additional data files were needed to streamline the radiology workflow and track administrative tasks.

6. VistA Options

There is one broker type option for the user interface:

```
DSSD MAIN MENU                    MENU TEXT: DSS OTM Laboratory Broker Menu
  TYPE: Broker (Client/Server)
 DESCRIPTION:   This option contains the remote procedures needed by the DSS
 OTM Laboratory application.
```

7. VistA Parameter Definitions

VistA parameters allow the applications to store system and user settings that drive functionality. Each application has its own word processing parameter to store settings as they see fit. Application parameters should not be set using VistA XPAR options, but only though the OTM web UI.

```
NAME: DSSD PARAMETERS
  DISPLAY TEXT: DSS OTM Laboratory Parameters
  MULTIPLE VALUED: Yes                  VALUE DATA TYPE: word processing
  INSTANCE DATA TYPE: free text
 DESCRIPTION:
 Contains various parameters for the DSS OTM Laboratory application.
PRECEDENCE: 1                           ENTITY FILE: SYSTEM
PRECEDENCE: 5                           ENTITY FILE: USER
```

8. VistA Security Keys

The following security keys need to be assigned to administrative users within OTM. Users require these keys to access configuration and user settings within the web UI.

```
NAME: DSSD ADMIN
  DESCRIPTIVE NAME: DSS OTM Laboratory Admin
  KEEP AT TERMINATE: NO
 DESCRIPTION:   Users with this key have administrative privileges in the DSS
 OTM Laboratory application.
```

9. VistA External Packages

OTM reads and writes data to legacy VistA packages. As a Class I and National Package application vendor, DSS understands the need for Integration Control Registrations (ICRs) to avoid issues when custodial applications make changes to VistA components (routines, files, etc.) As a company, we are a subscriber to hundreds of ICRs for our many applications, and many of these are common APIs used by OTM. We have never been required to formally request an ICR for a non-national application, but we do actively monitor ICRs and VistA releases to catch issues before they are felt at a site.

OTM relies on the following legacy packages:

- Adverse Reaction Tracking (GMRA)
- Consult/Request Tracking (GMRC)

- FileMan (DI)
- Kernel (XU, XLF, XPAR)
- Lab Service (LR)
- Order Entry/Results Reporting (OR)
- Patient Care Encounter (PX)
- Patient Flow Suite (DSSW)
- Registration (DG)
- Scheduling (SD)
- VA Certified Components (DSIC)

10. Security

10.1. VA Directive 6500

VA Directive 6500 contains policies designed to protect data created, stored and transmitted by VA systems and business processes. The OTM application is installed within the VA network and accessed by VA internal users only.

10.2. VA Directive 6515

VA Directive 6515 contains policies concerning the use of web-based resources to facilitate collaboration and improve employee effectiveness through seamless access to information.

10.3. Authentication and Authorization

Per the Memorandum dated Jun 27, 2016, all new and existing systems must be developed and/or upgraded to use Personal Identity Verification (PIV). PIV enforces 2-factor authentication by requiring a physical card and PIN#.

OTM is VistA-integrated and require VistA access/verify codes to allow access to the Cache database and associated routines and other components. The VistA portion of the PIV mandate is being tested and implemented within a patch to the Kernel package. Along with PIV, Identity Access Management (IAM) provides single sign-on capabilities through a web agent deployed to the OTM application server.

When interfacing with a PIV-enabled system, an SSOi integrated web application such as OTM will participate in a somewhat complex exchange of tokens passed between SiteMinder, the Application Server, VA Secure Token Service (STS) and VistA through VSOA.js as follows:

1. A thin client/browser user accesses a web site configured with an X509 certificate authentication scheme. This authentication scheme works along with the client browser. The user enters their PIV PIN Code, which allows the browser to forward the users PIV certificate to the web server. The PIN code does not travel over the network.

2. The CA SiteMinder web agent installed within the web server receives the certificate and "converses" with VA IAM services to validate the certificate. Once verified, Siteminder will embed an encrypted hash user identifier within an http header (named ea_auth_hash) and forward the request to the DSS Web Application Server.

3. OTM will therefore receive only authenticated requests. However, in order to interface with VistA, it must pass through a SAML token it receives when the ea_auth_hash identifier is provided to the VA STS system. Once received, the SAML token is forwarded through VSOA.js into a new XUS login RPC within VistA named XUS ESSO VALIDATE.

4. A PIV-enabled VistA system maintains connection information and related information within the REMOTE APPLICATION (#8994.5) file. With this information, VistA is able to verify the SAML token. VistA then matches the verified token with a stored token within VistA to match the user and authorize use of VistA as configured for that user.

PIV and single sign-on integration with VistA requires VistA Kernel patch (XU*8*659, Single Sign-on Provisioning and Implementation). VSOA.js must be being modified to enable SSOi.