Financial Disclosure Management

LDAP Specification and Data Requirements

Last Revised: 5/20/2021

FDM Deployment LDAP Specification

ACTION ITEM

The Agency IT POC and any additional IT resources should review the attached LDAP Specification and determine if the Agency can meet the required pre-requisites to use FDM. The Agency IT POC and FDM IT POC will use this specification as a guide connect FDM to the Agency directory services

The FDM IT POC will work with the Agency IT POC to test all connections to ensure there is an exchange of Agency data for authentication and directory services. The Agency's IT POC will address all identified issues.

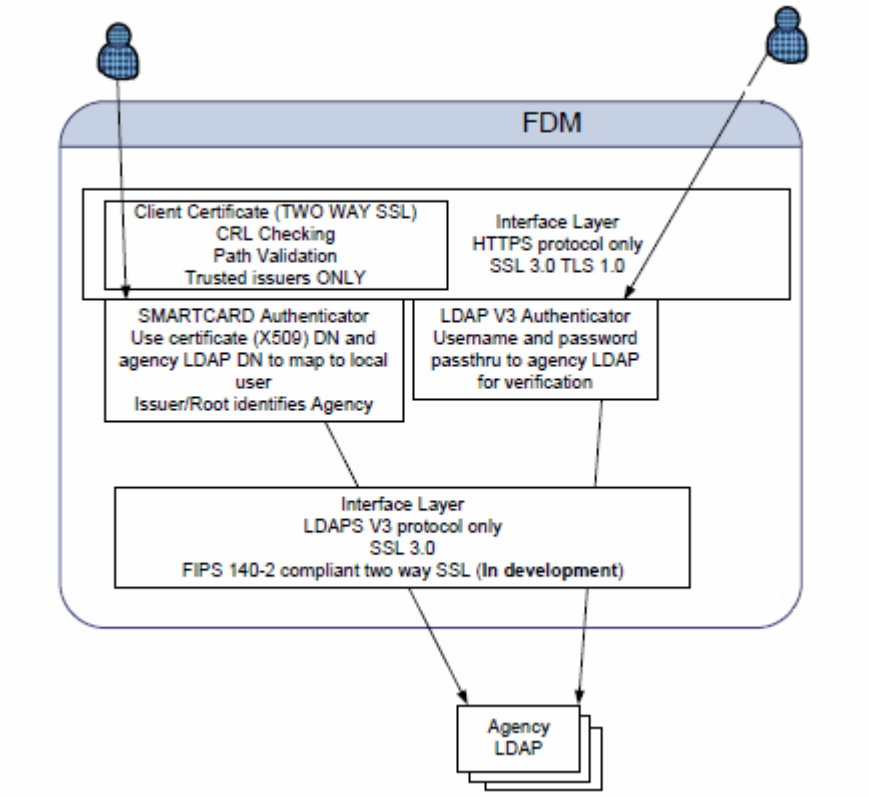
Introduction

This document is to be used by an Agency Technical POC who arranges access between FDM and the Agency's Directory and Authentication Services.

FDM requires access to two Agency supplied services: a NIST Level 2 authentication service and a user directory. The Agency's Interconnection Security Agreement (MOU/ISA) with FDM outlines the specific configuration required to establish a connection.

FDM Security Architecture Components

The follow depicts the logical architecture showing the core architectural components.



Current Identity Asserters

All identity asserters in FDM are managed by a J2EE 5 container thru a JAAS sub-system interface.

- Smartcard Authenticator - Currently only DOD CAC is supported. Non-DoD Agencies, wishing to use Smartcard Authentication can be dealt with on a case-by-case basis and may require additional funding outside of the current FSA (Functional Support Agreement) with FDM.
- LDAP Authenticator - Agency hosted LDAP is used to authenticate the agency users. LDAPS V3 protocol is used.

Requirements for Authentication

FDM utilizes an Agency LDAP for authentication and search. The LDAP authentication allows a bind, using LDAP v.3 or latest version protocol, to verify that the presented username and password are correct. The LDAP used for authentication and directory service can be the same. If the authentication service and directory are different, then the user-id for both must be unique and the same on both LDAP servers.

FDM does not maintain authentication information and employs the user's logon credentials, user-id and password, to log in to the Agency's directory over a secured connection.

The username and password must exist in the LDAP server.

Note: The Agency authentication services administrators will need to let their users know exactly what format is required for username and password.

Search

FDM uses the Agency's LDAP directory to search for individuals and assign roles. In addition, FDM draws user data to populate new user's contact information one time, during initial registration only.

> **Note:** Updating Agency LDAP information does not automatically update a user's FDM contact information.

The following attributes must be populated in the Agency's LDAP directory:

- User id
- Last Name
- First name
- E-mail

The LDAP must also support the following search attributes within FDM:

- Is equal to
- Starts with

Query Constraints

FDM expects a maximum of 200 records returned for any search.

Agency PIV/CAC/SMARTCARD LDAP Connection Requirements

- The Agency must provide all Root CAs for any certificate that will be used by the Agency's Users.
- The subject of the certificate must contain a unique identifier for an individual user.
- The Unique identifier in the subject of the certificate must be attribute located and accessible by FDM in the Agency's LDAP.
- The certificates that are presented by the Agency's Users must follow and abide by x509 standards.
- The Agency should provide a representative certificate to the FDM technical team via signed email or attachment.
- The Agency's LDAP should meet all of the above requirements.

LDAP to PIV/CAC/SMARTCARD transition

- The Agency must meet the above requirements.
- The Agency must make a formal request to the FDM technical team to initiate the process.

Userid Setup Information

It is recommended that the userid not change throughout the Agency's use of FDM. Changing, a unique id is not recommended because FDM does not audit the Agency's LDAP to authenticate the duplicate user account with the first. Once the user is established in FDM, they will use this ID forever.

- Duplicate Account Side Effects
  - Additional Agency costs may be assessed
  - User Login problems that result in a flood of calls to the FDM Help Desk.
  - Modification of FDM User Accounts by FDM DBA
  - Lost access to previously entered data in FDM.
- User ID character specifications
  - Valid characters include a-z, A-Z, 0-9, '-' (dash), '_' (underscore), and space.
  - Maximum character length is 64 characters

Note: Please inform the FDM project team prior to agency setup if your agency requires special characters (!@#$%^&*_-+=') for your user ids.

Accessibility Requirements

- The Agency's LDAP directory must be accessible to all instances of FDM including:
  - FDM Production
  - FDM Training
  - FDM QA
  - FDM Dev

Availability Requirements

- The Agency LDAP directory must be available 24/7.
- The Agency must notify the FDM Help Desk **(732) 720-6454** if the LDAP will not be available during normal business operating hours.

Data Requirements

Required Fields (Persisted in FDM from LDAP)

Last Name - 44 Alphanumeric

First Name - 34 Alphanumeric

E-mail - 60 alphanumeric

Non-Required Fields (Persisted in FDM from LDAP)

Middle Name - 1 character

Telephone Number - 40 alphanumeric

Non-Required Fields not persisted in FDM*

(*Displayed during Search and Select in the Directory lookup details. These fields provide additional information that helps uniquely identify users during registration.)

Suffix

Nick Name

Forwarding e-mail

Organization Address

State/Province

Postal Code

Street

Country

City of Current Station

Continental Location

State of Current Station

Zip Code

Other Phone Number

Organization*

MACOM Code

Basic Branch

CINC

UIC

HQDA Description

Title

AKO Account Type

Primary Military Occupational Specialty

Current Military Occupational Specialty

Rank

Rank/Grade*Agency*

FDM Best Practices Guidelines

ACTION ITEM

The Agency IT POC and any additional IT resources should review the attached technology "Best Practices" for using FDM and determine if the Agency can meet the required pre-requisites. The Agency IT POC and FDM IT POC will use this specification as a guide to ensure end user access to FDM is seamless.

From experience, we have found the following to be best practices when adopting FDM within your Agency. Investing in these best practices minimizes risk and increases long-term success with FDM. We recommend coordinating with your IT POC and Security personnel to discuss these best practices and the impacts they may have on your FDM users.

Guest Accounts

One very important early activity to consider is whether some of your Filer's use assistants to help them complete their reports. FDM does allow Filers to appoint one or more Filer Assistants to help enter report information. If a Filer wishes to appoint an assistant that is a "non-employee" such as a financial advisor or spouse, this person must be defined as a guest user in your Agency directory and provided with a separate username and password for logging in to FDM.

It is recommended that these "guest accounts" be sponsored and approved by an individual who is an active and full account user of the Agency Directory. Approval and sponsorship of Agency guest accounts must be completed outside of FDM. Once a "guest" is added to the Agency directory, the Filer can add them as their assistant in FDM.

> **Note:** Assistants may not submit a report nor make any changes after a Filer has submitted (eSigned) a report. Only Filers may amend reports (those a Filer first eSigned, then amended).

Terminating Employees

Terminating/terminated employees will no longer be able to access FDM once their account/User ID privileges are removed from the Agency directory. Creating a "guest account" in your Agency Directory may be a work around for allowing these Filers to submit their Termination reports in FDM.

Accessing FDM from Home

Once a user is registered in FDM, they can access FDM from any computer using either your Common Access Card (CAC) or your Agency User Name and Password.

FDM Minimum System requirements

To ensure Agency end user access to FDM is seamless, please inform the FDM IT POC and Local IT support to make sure your FDM users have the following setup on their computers.

FDM is fully compliant with the Army Gold Master desktop configuration. Components of the desktop not regulated by AGM may require updating.

1. Browser: Internet Explorer (IE) 7.0

2. Adobe Acrobat Reader 10.1 or greater

3. JRE: Sun JRE 1.5 or greater

4. CAC reader & any of this middleware:

- ❖ Activcard 6.2
- ❖ PKI Certificates - Download and Install (on the desktop) PKI Root Certificates from http://dodpki.c3pki.chamb.disa.mil
  - Registered User's CAC/PKI Certificates
  - Identity
  - Encryption
  - Digital Signature

Note: The user's computer will automatically register the user's PKI Certificates following the initial insertion of the CAC if the requirements above are the met.

5. Internet Options

- ❖ Be sure Popup Blockers are off
- ❖ Cookies are enabled
- ❖ Javascript enabled

Security Settings

FDM uses a secure Internet connection to guarantee that the transmission of data from the server to you is secure. Agency IT POCs and local IT support should ensure to configure FDM user's browser security, content, and advanced settings to trust the FDM website or add FDM to Agency's trusted sites list.

Check that your IE is properly set up to use SSL 2.0 and SSL 3.0.

Website Security Certificate

Some users may receive the message, "There is a problem with this website's security certificate." This is a Web Browser message to indicate to users that they are on a secure site, and (just as importantly) that the secure site is the one that they were expecting to visit.

If you do not wish for your users to receive the warning that the site is untrusted/insecure continually, the proper PKI certificates for FDM should be installed on their computers by local PC Support help desk.

- See https://www.fdm.army.mil/helpSupport/knowledgeCenter.htm for a listing of the required certificates necessary for using FDM.

  Note: The PKI Certificate is not a CAC certificate.

Notifications (Plan for Spam)

A key activity when using FDM is sending notifications to Filers and Reviewers. Agencies should anticipate that mail server filters might intercept legitimate FDM messages as spam. Unfortunately, this means FDM users may not receive FDM notifications that a report is ready for review or should be completed.

We recommend your FDM IT POC contact your e-mail administrators to determine the best method for preventing legitimate FDM message from being caught in Agency spam filters. Possibly, by adding FDM to an approved send list.