

IdSS/IdMI Overview for Mission Partners

OVERVIEW

The Identity Synchronization Service (IdSS) is a part of the DISA Enterprise Directory Services, a suite of products and services providing DoD Enterprise identity and contact attributes. Enterprise Directory Services is comprised of enterprise provisioning services, directory services, synchronization services, and DoD Enterprise White Pages in support of people discovery across the DoD community.

Identity Synchronization Service (IdSS)

IdSS connects to authoritative identity data sources including the Defense Manpower Data Center (DMDC) and the Global Directory Service (GDS) to collect and groom identity data, and to provision and maintain persona-based user objects in LDAP directories such as the Enterprise Applications Services Forest (EASF). IdSS controls all account creation, deletion, and updates into the EASF, and allows DISA mission partners to map DISA services, referred to as entitlements, to specific end-users.

IdSS Machine Interface (IdMI)

The IdSS Machine Interface (IdMI) provides a capability for machine to machine synchronization of DoD Persona data groomed by IdSS and populated in EASF. It is capable of providing a one-way data feed between EASF and DISA mission partners for populating and maintaining DOD Component level information technology (IT) directory systems such as Global Address Lists (GALs), Lightweight Directory Access Protocol (LDAP) directories and White Pages. The IdMI feeds include person and persona identity and contact data elements for personas that have a current DoD Common Access Card (CAC). It also includes the ability to provide synchronization for Non-Person Entity (NPE) objects in support of group management and distribution.

IdMI

IdMI Data

IdMI data feeds provide data elements identified in the data dictionary (See Appendix B). Note, while IdMI data provides data groomed by IdSS, ultimately DMDC is the accountable source for all data in the data dictionary, excluding email encryption certificates provided by DISA GDS, and DEE account data provided by DISA ESD for DEE migrated users. DISA will coordinate with DMDC to correct data discrepancies between DMDC provided source data and data transformed or augmented as part of the IdMI processing.

DISA ESD assumes that the DoD Component receiving the IdMI feed will use this data for populating their local Active Directory and White Pages system. Options to customize the feed include frequency of synchronization, push vs. pull, and other synchronization options.

Enterprise Service

DISA provides the IdMI feed as an Enterprise service. The architecture of the IdMI service was scaled to accommodate an IdMI connection per Combatant Command (COCOM), service, and agency (CC/S/A) *free of charge*. DISA provides synchronization services on both NIPRNet and SIPRNet feeds with the expectation that each CC/S/A will distribute the data to the CC/S/A managed Active Directory and White Pages system.

Technical Implications

IdMI provides synchronization from the IdMI Active Directory Lightweight Directory Service (AD LDS) to the CC/S/A synchronization service instance. To support IdMI, the CC/S/A enables a Lightweight Directory Access Protocol (LDAP) export from the ESD server infrastructure to their server, and must open one network port for the data feed.

DISA is currently considering an additional option that will expose the IdMI data via SQL Server views. There are some additional technical challenges related to implementing this solution that are internal to DISA, but the impact on customers would be that appropriate ports required to retrieve data from SQL Server views would need to be opened."

Network Implications

An unfiltered IdMI feed may require upwards of 25GB of storage, although, the amount of data pulled can be significantly reduced by limiting the data requested. An unfiltered initial sync with IdMI will require a full-sync using a sync engine, which will transfer approximately 20GB of data and take roughly 24hours to complete. The impact to the network will be based on available bandwidth.

After the initial full-sync into the CC/S/A instance, IdMI supports periodic incremental updates. Frequency of incremental updates can be specified during IdMI setup. After the full-sync, IdMI supports 100,000 incremental updates for roughly 200KB of data per week. Note that a full-sync may be needed approximately two to four times a year.

Synchronization Options

IdMI supports the following sync options:

- IdMI FIM Sync push to IdMI customer AD LDS
- Sync from IdMI AD LDS to component synchronization service instance (specify push or pull)
- AD LDS Replica partnership between IdMI AD LDS and component AD LDS Replica Partner. AD Replication is a dynamic network-sensitive latency-tolerant connection.

One method will be selected and agreement will only reflect the appropriate diagram:

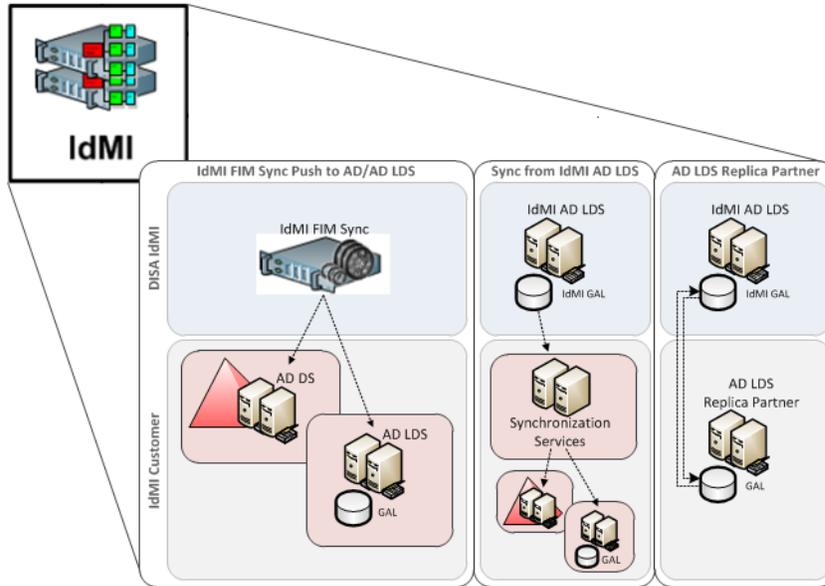


Figure 1 - IdMI Interfaces

How to get IdMI

The following requirements should be kept in mind for establishing an IdMI connection:

- **MOA Requirement:** DISA follows DoD instructions for interagency agreements. DoD instructions state an MOA is required for Reimbursable or Non-Reimbursable support agreements.

Note: DISA policy allows for a delegation of signature authority for specific types of agreement to the GS-15 level. DISA signature authority has been delegated by PEO-ES to Jason Martin for IdMI connections.

- **Protection of PII data:** The IdMI feed contains PII data. Either a Privacy Impact Assessment (PIA) or System of Record Notice (SORN) is required for the component level IT system the IdMI feed is connected to.

All systems receiving IdMI data must be accredited in accordance with DoD Instruction 8500.2.

To establish an IdMI connection, DISA ESD and the CC/S/A must work together to establish Memo of Agreement (MOA), obtain security accreditations, and coordinate technical resources to implement the connection. More details below:

- 1) CC/S/A and DISA ESD representatives meet to review requirements and understand what is involved for an IdMI
- 2) CC/S/A provides DISA with information needed to complete an MOA specifying points of contact and system information needed in the agreement.
- 3) CC/S/A works with DISA ESD to gather information to complete the IdMI Customer Interface Specification (CIS). This document formalizes the relationship and provides specific

authoritative detail to operate, maintain, and update the connection in support of the MOA. A CIS is required for every individual NIPRNet and SIPRNet connection established.

- a. The CIS must include the following information:
 - i. Synchronization Option (push or pull)
 - ii. External Interface Communication Requirements (IP addresses, Ports/Protocols)
 - iii. Frequency of synchronization (every 6 hours, daily)
 - iv. Component/Client requirements
 - v. Root Distinguished Name (DN) (not applicable for DISA push to Directory service)
- 4) DISA fills out the MOA and the IdMI CIS, and signs the MOA.
- 5) CC/S/A reviews the MOA and also signs.
- 6) CC/S/A provides a completed PIA for their directory system, needed to verify the directory system being populated has addressed privacy appropriately. PIA should comply with DoD Instruction 5400.16.
- 7) CC/S/A provides a copy of the Authority to Operation (ATO) for the directory system.

After the completed signed MOA is returned to DISA with all attachments, it takes a matter of days to establish the connection, depending upon how fast firewall rule changes are enacted at both DISA and the Component.

Points of Contact

Questions may be directed to:

DISA Product Management Team:
disa.meade.esd.list.idss-product-management@mail.mil

Appendix A: Acronyms

AD	Active Directory
ATO	Approval to Operate
CAC	Common Access Card
CC/S/A	Combatant Command (COCOM), service, and agency
CIS	Customer Interface Specification
COCOM	Combatant Command
DECC	Defense Enterprise Computing Center
DEE	DoD Enterprise Email
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DN	Domain Name
DOD	Department of Defense
EASF	Enterprise Application Services Forest
ESD	Enterprise Services Directorate
GAL	Global Address List
GDS	Global Directory Service
IdAM	Identity Access Management
IdMI	IdSS Machine Interface
IdSS	Identity Synchronization Service
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement
NIPRNET	Non-Secure Internet Protocol Routing Network
NPE	Non-Person Entity
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
PMO	Project Management Office
SIPRNET	Secret Internet Protocol Routing Network
SORN	System of Record Notice

Appendix B: IdSS Architecture and Data Flow

The following diagram illustrates the flow of identity and contact data through the IdSS and EASF architecture. IdSS connects to authoritative identity sources to collect and groom identity information. The Defense Manpower Data Center (DMDC) is the authoritative source for identity data and Global Directory Service (GDS) is the source for encryption certificates. IdSS controls all account creation, deletion, and updates into the EASF. EASF data is made available to DISA mission partners through IdMI.

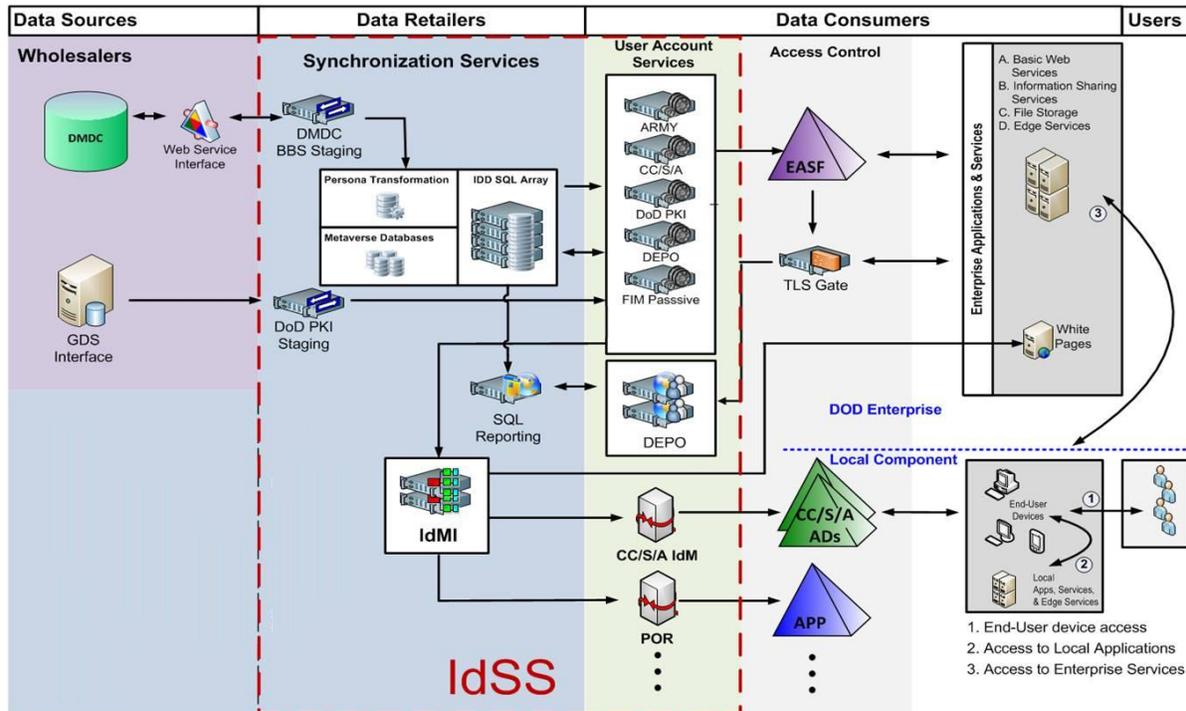


Figure 2 - Data flow through the IdSS and EASF Architecture