



Consolidated Technology Services • WA

Conceptual Design

Forefront Identity Manager

Karen McLaughlin

January 29, 2013



Overview

The purpose of this design is to provide information on the value – in addition to Global Address List Synchronization (GAL Sync) – that a full implementation of Forefront Identity Manager (FIM) could bring to the Enterprise Active Directory (EAD). A conceptual design for GAL Sync was presented at the CTS Advisory Council at the December 2012 meeting. A request for more information on the other services that FIM can provide was requested at that meeting.

FIM is the enabling technology for a more advanced identity management (IdM) strategy for the Enterprise Active Directory. The goal of an identity management system is to manage individual identifiers (accounts, attributes, groups, etc.), their authentication, authorization and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks. Much of the work that is necessary to successfully implement a larger IdM strategy for the Enterprise would be completed as part of a full FIM implementation. IdM for the Enterprise is being presented in a separate document.

A full implementation of FIM would bring the following business benefits to agencies that are members of the Enterprise Active Directory:

- Reduces administrative overhead for simple tasks such as password resets and group management
- Reduces costs and risk by automating identity management between identity sources.
- Enforces consistent use of attributes in the Active Directory by the use of policies, eliminating conflicts and functional issues when new applications are deployed (locally or in the cloud) that use EAD for identity management.
- Decreases administrator workload by automating:
 - provisioning and deprovisioning of user accounts.
 - authorization and authentication to resources in the Active Directory and other systems.
 - Many other administrative functions.



- Provides a method for synchronizing account information and passwords between different systems, extending the 'single signon' experience.

FIM Features and Services

FIM Synchronization Service

This design is based upon use of Microsoft technology known as Forefront Identity Manager (FIM). The 'heart' of any FIM implementation is the Synchronization Service. In its simplest implementation, the FIM Synchronization Service is implemented in the EAD root and used to synchronize object attributes from multiple identity stores and directories via LDAP.

In a full implementation of FIM, it is used as a single point for account management for all connected systems. FIM Management Agents are available for many directories and database systems to enable much of this synchronization 'right out of the box'. In addition, a Software Development Kit (SDK) is available to allow for programing of any needed custom management agents.

Once FIM is implemented fully, management of user accounts, groups and other identity information is accomplished within the FIM system and synchronized to all the connected systems by FIM. This aggregation of information forms what Microsoft refers to as the FIM 'Metaverse'. Once this is in place, agency administrators do not have to manage multiple identities across multiple systems for users, and users do not have to remember multiple accounts and passwords across these systems.

The synchronization service is also the key component for support of user self-service password reset, profile management, and group management.

User and Administrative Portal

The FIM portal is the interface for managing identities in the FIM Service. The FIM portal is based on SharePoint Web Services and allows end users and administrators to manage objects in the FIM Metaverse including:



- Self-Service Password Reset
- Distribution List and Group Management
- User and Profile Management

The FIM Portal is fully customizable and the user and/or administrator will only see the appropriate options based on permissions assigned them within the portal. This allows for a more granular control over who can modify identity information across systems and more complete auditing of changes made through FIM. After FIM is implemented in the enterprise, all account and password management should be done through the Portal so that identities are propagated correctly through all connected systems.

Self Service Password Reset (SSPR)

The FIM Self-Service password reset service allows users who have forgotten their password to pass certain “gates” in order to reset their password without administrator intervention. The password gates are established by Management Policy Rules (MPRs) and gating questions set by the administrator and other criteria and workflows. These can be customized for different agency requirements or even for different groups of users (i.e. contractors vs. State Employees).

Once an administrator grants permission, a user will be prompted to “register” for the self-service password reset functionality. After completing registration and supplying gating questions, they will be able to use the password reset functionality. They can do that from the Windows login screen, Outlook Web App or the FIM User Portal.

To further enhance SSPR, help desk staff can be delegated rights in the portal to reset ‘locked-out’ user accounts in order for the user to retry or change their passwords. If a user forgets their gating questions, administrators can be authorized to unlock their accounts and manually reset their password change ability through the portal.

FIM can further enhance password management by password synchronization across all systems with the Password Change Notification Service (PCNS) installed and running on their



domain controllers. Note that this synchronization only occurs as part of the password change event; FIM is not a password repository.

Group Management:

By default, FIM is designed to manage Active Directory groups but can be extended to manage group membership in other identity sources. FIM can manage Distribution Groups, Security Groups (Universal, Global and Domain Local) and mail-enabled groups with the same scope. There are three types of group management available in FIM:

- **Manual:** Many different scenarios exist for a manually managed group. A user can request to be added to, or removed from, a group through the user portal. The group owner must approve or disapprove the addition or removal.
- **Manager-based:** Membership is based on reporting relationships to a manager.
- **Criteria-Based:** Dynamic membership in a group, based on filters and policies.

All groups managed in FIM must have a group owner. This can be an individual or a service account. Workflows can be set up to automate these activities for a group. Groups can be managed by the owner through the FIM Portal or Outlook.

FIM-managed groups do not equate to existing Active Directory groups by default. An initial way to bridge this gap is to create a new group in FIM and add the corresponding Active Directory group as a member. Full definition of membership can be completed later.

Management Policies and Workflows

If the synchronization Service is the 'heart' of FIM, the Management Policy Rules (MPRs) and workflows are the 'muscles'. Every action that happens in FIM is enabled by a MPR and/or workflows. Policies work with the FIM synchronization service to define

- how account information is managed
- who is authorized to access resources
- how attributes are populated



- which system is authoritative for individual attribute information
- what information can be input into attributes
- and many other tasks.

For example, a simple workflow tied to a self-service password reset could be:

- John Smith uses the self-service portal to request that his password be reset.
- An automated email is sent to him with a Personal Identification Number (PIN) to be used to reset his password.
- John is then able to submit the PIN along with answers to gating questions to reset his password.
- An automated email is sent to John's manager and the agency security department as an FYI in case John Smith's account might be compromised.

Another workflow for deprovisioning a user could look something like this:

- When the employee status attribute in the HRMS system becomes "inactive" the user account is automatically disabled in Active Directory
- The agency keycard database system, which has used the SDK to interface with FIM, automatically revokes the employee's card access to the office building.
- An automated email is sent to their manager, the agency HR department, Information Technology System Administrator and Building Security Administrator as an FYI of the actions taken...
- Additional actions can then be taken by the various departments as outlined in either a manual or further automated workflow steps.

FIM comes with hundreds of standard MPRs that can be used or customized and chained into workflows. Custom MPRs can also be created.



Design

This design covers a full implementation of FIM. It is inclusive of the implementation effort and costs found in the previously created High Level Design for GAL Sync .

Beyond the infrastructure required for the Synchronization Service, a full implementation of FIM will also require:

- a FIM Service Server
- an additional SQL FIM Service database instance
- a FIM Portal Server.

Both server functions can be implemented on virtual machines. The database instance can be housed on the same SQL Server that hosts the synchronization database.

Provisioning just the Synchronization feature of FIM (as proposed for GAL Sync) does not require the purchase of client access licenses (CALs) from Microsoft to use. However, the additional features required for a full FIM implementation *will* require the purchase of CALs for all users that use the more advanced features of FIM. These CALs are not currently included in the State's Enterprise Agreement and would need to be purchased by agencies or added to the Enterprise Agreement.

Hardware and Software Requirements

The FIM GAL Sync High Level Design (Synchronization Service only) specified the installation of one physical IBM H23 Blade with Dual 8-Core Processors, 64 GB of RAM, (2) 300 GB hard drives and 300 GB of Raid 1 SAN Storage. This configuration would also be sufficient to run the FIM Synchronization Service load under a full FIM implementation.

The FIM Portal Server and FIM Service Servers do not have the processing requirements of the synchronization service and can be deployed on virtual machines.

In addition, a full FIM implementation will require an additional separate SQL instance. The FIM GAL Sync design was based upon using available capacity in our existing Exchange 2010 SQL environment, which has a 10 GB connection to the IBM Blade Chassis, and an unused node in



the four node cluster. This configuration should be also sufficient for the additional instance and load anticipated for this service.

High Availability and Disaster Recovery are accomplished in FIM by using a warm standby server for the FIM Synchronization and Service roles. FIM is installed on the standby with the services turned off. The Messaging SQL Cluster is already in a high-availability configuration, so no further work needs to be done for SQL. The Standby Server would be provisioned as a virtual machine. If failover is necessary, a slight degradation in service would mean that synchronization times would increase until service could be restored to the physical environment.

A full test and pre-production environment needs to be created for the testing and verifying of new workflows and policies before they are implemented in the Production FIM System. A process for approval and implementation of custom management agents, MPRs and workflows will also need to be developed.

Estimated Costs:

Hardware and Software:

Total Cost Estimate for Hardware, Software: \$7,100 per month for the first year and \$3,400 per month thereafter.

Production System:

Hardware Costs: \$2,800 per month

(One Physical Server and 2 VMs)

Percentage Cost for existing Messaging SQL Server Cluster: TBD

Software Costs: \$30,000 or \$2,500.00 per month for 12 months

Pre-Production Environment:

Hardware Costs: \$600 per month (2 Virtual Servers [2 Cores, 4 GB RAM])

Software Costs: \$1,200

Licenses:

As discussed in the GAL Sync implementation, CALs are not required for the FIM synchronization service. However, any of the additional features of FIM require a client access



license. The FIM client access license is currently listed as **\$11.37 per user** on the select agreement.

FTEs:

It is estimated that between 2.5 to 3.5 FTEs at the ITS5 and ITS6 level will be required for administrative maintenance and workflow programming (see 'CTS Support Responsibility' below for more detail).

Vendor Costs:

The implementation of GAL Sync, synchronization between Active Directory and FIM, and SSPR could be implemented without consulting support.

The implementation of synchronization between systems, workflow and MPR automation, and provisioning and deprovisioning of users would require a consulting engagement, (such as with MCS) and would require resources to be committed from both CTS and EAD member agencies for the duration of the implementation.

Total Costs:

Here are the total **ESTIMATED** costs for CTS to deploy and support the infrastructure for FIM:

Item	Monthly Cost
Hardware and Software (Avg. over first 5 years)	\$ 4,140.00
3 FTEs (1 ITS6, 1 ITS5, ITS4)	\$42,395.00
Total Monthly Cost*	\$46,535.00

***Does not include the cost of client access licenses, which would be purchased by the agency (11.37 per FTE) or Project/Consulting Costs.**

If the decision is to recover these costs via an increase in the EAD rate, that would amount to \$1.01 per user per month.

Not estimated in this document are the FTE costs required for governance, standardization effort, and EAD join costs (for non-EAD members). These would be quantified and addressed in each phase of the FIM roll-out (see Agency Implementation Responsibility).



Implementation approach and level of effort:

The full implementation of FIM would be a multi-phased project with escalating effort to implement. Implementation by agencies could also be “staged” with agencies adopting different features as they are ready. Deployment of the infrastructure necessary to support FIM will be a comparatively small effort – the main effort will come out of the larger IdM project to develop, standardize, and implement processes and business practices into the FIM System.

If GAL Sync is implemented first (as requested by the Legislative Service Center) the synchronization service would be deployed as part of that effort. A project for full implementation of FIM could then proceed at its own pace with the addition of virtual web servers for the User and Management portal and the staged implementation of additional FIM Services.

The following is a quick overview of the approach to a full implementation of FIM in the EAD by order of effort and complexity:

- Implementation of the synchronization engine and connection to EAD.
- Implementation of GAL Sync for Legislative Service Center and other non-EAD customers.
- Implementation of the User Portal for Self-Service Password Reset
- Implementation of Group Self-management for new groups
- Transition of existing groups to the user portal for self-management.
- Implementation of synchronization of attributes between EAD and an external authoritative identity store such as Washington State’s Human Resources Management System (HRMS). This will require determination of the values and uses of attributes in the EAD and mapping these attributes between identity stores, creation of workflows, and determination of key attributes used for synchronization.
- Automation of provisioning and deprovisioning of users, creating workflows, policies and auditing.

CTS Support Responsibility:

CTS responsibilities would include support for the FIM Service, managing and monitoring synchronization between systems, created management agents and implementing connectors



between FIM and other data stores, creating, implementing and managing all management policy rules and workflows. Also required would be collaboration with the IdM Governance Groups and Agency Administrators on the creation of MPRs, Workflows, and Management Agents. This would be an ongoing requirement as EAD member agency business processes change.

Support costs cannot be broken out at this time by each individual FIM module, but would be determined through a more detailed design. However, for a full FIM implementation, it is estimated basic support would require:

- 2- 3 Full-time FIM administrators to monitor and manage FIM Services and Synchronization;
- A part-time Programming Resource for custom Management Agents, Filters, Management Policy Requests, Workflows, etc.

Support levels will be determined, in part, on how much standardization can be agreed upon by the governing groups. Support costs will increase based on the amount of requested customization and the resulting complexity caused by customization of the FIM Service

Agency Implementation Responsibility (reference the separate Identity Management – IdM document):

- Participate with other EAD agencies in an Identity Management Strategy for the EAD.
- Working with CTS, EAD Governance and internal business partners, determine business processes that pertain to groups, password reset and other tasks
- Determine agency systems that hold identity information that should be included in the agency IdM strategy.
- Work with CTS to determine authoritative sources for identity information.
- Make changes to their Active Directory structure, firewalls and attribute usage as required to implement FIM Services.
- Install software on desktops and servers as needed to enable FIM Services for users and administrators.
- Train agency administrators on FIM Services so they are knowledgeable on the features and options that FIM can provide for Identity Management.
- Train users on different FIM Services as they are implemented and the use of the FIM Portal.



Agency Support Responsibilities:

As each of the modules of FIM is implemented, agency identity administration will gradually move from existing management tools (ADUC, SQL, etc.) to the FIM administrative portal. As much as possible, functionality in FIM will be delegated to agency administrators, as allowed by each module of FIM.

Agency administrators will be responsible for working with business partners within their agency to identify processes that should be implemented into MPRs and workflows in FIM and determining which identity stores need to be connected to the FIM Synchronization Service. For MPRs and workflows that are not under their control, they will need to work with CTS FIM administrative staff to develop and edit workflows based on new or evolving business practices of the agency.

SMEs for this Conceptual Design:

Karen McLaughlin, CTS, CSD Design and Planning

Brian Casey, Microsoft, AD Dedicated Support Engineer

Resources:

Implementing Forefront Identity Manger 2010

<http://technet.microsoft.com/en-us/forefront/ff793470>