



Consolidated Technology Services • WA

High Level Design

Forefront Identity Manager Global Address List Synchronization

Karen McLaughlin

November 30, 2012

Overview

The purpose of this design is to address a business need identified by agencies that are on the State Government Network (SGN) but are not using the Enterprise Active Directory Forest (EAD) and Shared State Email (SSE) services. These agencies have expressed a desire to have access to the EAD Exchange Global Address List (GAL) and combine its content with the address list in their own Exchange organizations.

This design is based upon use of Microsoft technology known as Forefront Identity Manager (FIM). FIM is able to synchronize object attributes from multiple identity stores and directories. For this specific business requirement, FIM allows the synchronization of mail-enabled user objects across non-joined Active Directory Forests without requiring a forest trust, and will keep this information updated automatically. This design will refer to this functionality as GAL Sync. Although GAL Sync is not the primary function of the FIM synchronization service, it is the only FIM function addressed by this design.

Per this design, the FIM synchronization service would be hosted in the EAD. Synchronization connectors would be put in place to Active Directory Forests that are not in EAD. Synchronization between these connected Forest would be managed by the EAD FIM Servers – other Forests would not need to install their own FIM Servers in order to participate.

Using FIM for GAL Sync neither requires, nor creates, a forest trust, and does not provide any cross-Forest authentication mechanism. In addition, FIM GAL Sync does not provide for any kind of Exchange calendar sharing or the sharing of Free/Busy information.

Opportunity

The OCIO Identity Management User Authentication Standard directs state agencies to use the EAD service. Some have not done so yet due to business and financial reasons. Others, such as

the Office of the Courts and Legislative Service Center are non-cabinet agencies, to which this standard does not apply.

These 'non-joined' agencies have to rely on manual methods to assemble and maintain State Employee contact information for other agencies. These agencies find it difficult to keep up with employee contact information that is changing on a regular basis as employees leave the state, change agencies or change positions. Agencies using EAD must also rely on manual methods to maintain contacts for employees in the non-EAD agencies. As a result, there is redundant but often conflicting contact information for a given employee in each of the forests, which can lead to misdirected or 'lost' emails.

This design replaces these manual methods with an automated synchronization of contact information between these separate Forests. This will improve accuracy and reduce effort, creating a 'unified GAL'.

Requirements

Business Requirements:

- A method for combining employee contact information across multiple Active Directory Forests without the use of forest trusts.
- Ability to exclude sensitive accounts from synchronization process, if desired.
- Require a minimum amount of human intervention to manage.

Functional Requirement:

- Synchronization must be current within any 48 hour window.
- Cost-effective and reliable.
- Able to synchronize with multiple agency forests simultaneously.
- Manage synchronization in a coordinated way from a central location.
- No negative impact on the day-to-day Active Directory operations for any of the participating agencies.
- Requires minimum administrative effort.

Non-Functional Requirements:



- Any participating agency must be on the SGN (no solution currently exists across discontinuous networks).
- Solution must be proven and vendor-supported for this purpose.
- Each forest will be responsible for configuring their Global Address List in order to display the synchronized contacts.
- Must not saturate network connections between participating forests.
- Domain Controllers in participating forests must be sized to handle the increased size of the Active Directory (.dit files).
- Implemented in a way to scale for other synchronization functionality, if available.

Recommended Solution:

Microsoft's Forefront Identity Manager Synchronization Service is the recommended solution. This is a proven technology with vendor support already available, and meets the stated requirements.

Challenges

Some of the challenges that were identified during research for this design were:

- The Legislative Service Center has the same Active Directory Forest Root name as the Enterprise Active Directory Forest (wa.lcl). This creates increased complexity in configuring FIM GAL sync for their use, especially in the area of Name resolution.
- The size of the GAL is significant. This can create an issue for agencies that want to connect Forests containing older domain controllers (DC) with insufficient disk space.
- Bandwidth issues between forests may elongate synchronization time.
- There may be training issues for agency employees who find the larger GAL difficult to navigate.
- Education may be required for agencies connecting to the GAL. They may not realize that each agency in EAD is responsible for keeping the contact information for their users updated, and thus the accuracy of the information in the GAL is variable.



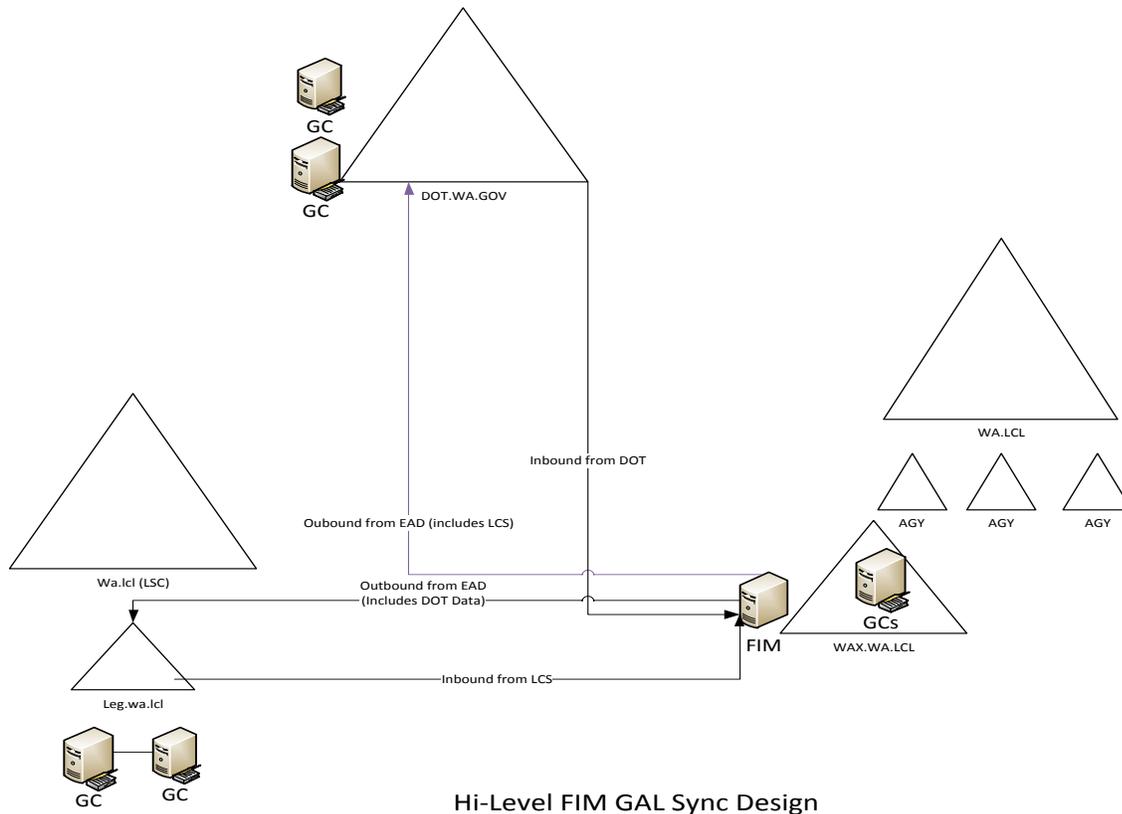
Consolidated Technology Services • WA

High-Level Design Forefront Identity Manager Global Address List Synchronization

- Initial design recommended an installation of Microsoft SQL Server on the same computer as the FIM Service due to potential latency. Installing SQL Server on the same computer with the FIM Server would incur additional cost and complexity.



Design



This design focuses on GAL Sync, a built-in function of FIM that creates mail-enabled objects for users that are then synced to other forests where user objects for them do not exist. It does this synchronization automatically on a scheduled basis without requiring manual creation of these mail-enabled objects by an AD administrator.

The design calls for organizational units (OUs) to be created in EAD for each of the external Forests to which it will sync. Inbound connectors synchronize their mail-enabled contacts to these OUs. Outbound connectors would then include these OUs in the synchronization sent to external Forests. Thus, only one FIM Synchronization Server is required, reducing complexity and costs.

Controlling Synchronization

The design calls for a global EAD policy that would examine an attribute on a mail-enabled object to determine whether that object should be synchronized. Either an existing attribute is used for this purpose, or a new attribute is created, could be determined by the Forest Resource and Application Developers Group. This approach is considered superior to the alternate 'static' approach of having each participating forest create a 'sync' OU, and reorganize their forest accordingly. This also reduces the FIM service support overhead for CTS, simplifies management of synchronization policies across the EAD forest, and gives control of which objects are synchronized to agency administrators.

Synchronizing with a WA.LCL Rooted Forest

This design calls for the installation of FIM in the EAD subdomain WAX.WA.LCL. In configuration of FIM connectors, the "root" would be specified as the sub-domain for each forest. For example, in connecting to LSC: WAX.WA.LCL would be the source/destination and LSC.WA.LCL would be the destination/source. This means that Host files will need to be maintained on the FIM server for domain controllers in the destination forest. This is not ideal, as these files will need to be manually maintained, but it solves the issue with identically-named Forest Roots.

Agency Planning and Mitigation of Impact on Active Directory

The design calls for firewall Port 389 or Port 636 to be opened between participating forests for either LDAP or Secure LDAP directory synchronization. Firewalls would also be opened inbound and outbound to domain controllers in the connected Forests.

FIM, and therefore this design, will only work for forests on the same network. For this reason, this design is based upon participating forests being on the SGN.

The time for synchronization to complete will be dependent on the network connection speed between the FIM Server and domain controllers on the Forest. In order to complete

synchronization within a reasonable time, this design specifies network connections between forests (and DCs) of at least 1 GB.

This design requires that DNS conditional forwarders be configured in both the destination and source forests that point to the FIM Servers and domain controllers. The LSC forest will be handled differently (see “Synchronizing with a WA.LCL Rooted Forest”).

Each participating forest will also need to provide a service account that has read/write access to the directory. In the EAD forest, this account will be limited to read/write access to the directory after installation is complete. The connected Forest administrators will control the password for this account and the account itself. This account will be used in both the inbound and outbound connector configuration.

Participating agencies will need to make sure that their Global Catalog (GC) servers have sufficient disk space to accommodate the increase in .dit file size reflected in a combined GAL. It is recommended that an agency have at least 10 GB of free disk space on each GC.

During implementation, CTS will request and compile statistical information from each external forest desiring to participate, including lists of employees and mail-enabled objects that they do not wish to synchronize. This will allow them to determine the impact to agency GC replication activities across the forests. CTS will communicate this information to all participating agencies as along with planned synchronization dates. This will allow agencies to delete any manually-maintained contacts from their forest in order to prevent confusion and collisions during synchronization. Agencies should also communicate with employees at that time about the changes a combined GAL will present.

Initial synchronization would be scheduled to occur over a weekend or some other time that will cause the least impact due to the large amount of replication traffic and activity that it will trigger.

Hardware and Software Requirements

The design calls for a base 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. The design does not specify a virtual server due to the I/O and processing requirements of this application. This server would have FIM installed with just the Synchronization Service running. The server would be installed in the WAX.WA.LCL domain due to the availability of agency GC servers, the Shared Exchange environment, and to enable communication with Forests that have the same root name as EAD.

At this time, FIM 2010 is not supported on Windows 2012, so the servers would use the Windows 2008 R2 Enterprise Edition.

In addition, FIM synchronization requires a highly-connected Microsoft SQL Server. Microsoft recommends that SQL either be installed on the same server as the FIM Synchronization Service, or be attached via a 1 GB dedicated connection. This design is based upon using available capacity in our existing Exchange 2010 SQL environment, which has a 10 GB connection to the IBM Blade Chassis, and a unused node in the four node cluster. This configuration should be sufficient for the load anticipated for this service and is a more cost effective use of existing resources. To avoid impact to the Exchange 2010 service, synchronization would be scheduled for non-peak network hours.

High Availability and Disaster Recovery are accomplished in FIM by using a warm standby server. FIM is installed on the standby with the synchronization service 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.

Unless otherwise determined in the detailed design, synchronization of directory data is not a mission-critical need and should not require an alternate 'hot-site'. A 'warm standby' would be appropriate for this service. The ramifications of the service being unavailable would be that over time the data in the combined GAL would become stale, but it would still exist until the service could be restored.



Future Development of FIM

The GAL Sync function is only a small piece of the functionality available to EAD agencies from a FIM deployment. Future expansion of the service could add:

- Self-service password resets.
- Automated distribution list management.
- Workflows to manage directory information
- Synchronization with other identity stores to automate and standardize Active Directory information.

FIM is a scalable service offering and other features can be added in the future. This design was done in such a way as to not preclude the expansion of the FIM Service at a later date.

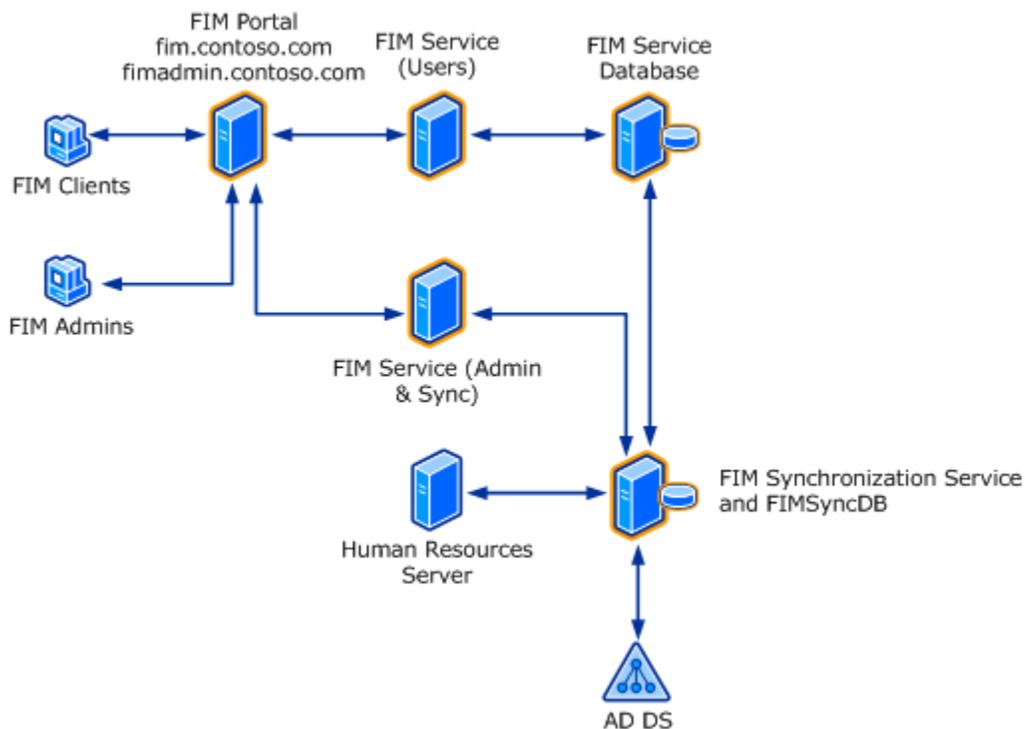


Diagram of Full FIM Deployment



CTS Effort to Deploy and Support:

Work to be Completed:

- Detailed Design work and a design review for the project
- Rates Development
- Configuring FIM in the EAD Pre-production environment and piloting with a customer agency
- Standing up the FIM Synchronization Service in the EAD Production environment, which includes:
 - installing and configuring hardware and FIM software
 - configuring the SQL instance on the existing Messaging Cluster
 - training staff on FIM support
 - Working with FRG/FAD to create/determine attribute and create filter list based on the attribute
 - Working with pilot production agencies to prepare for connections to their forests
 - working with the customer agencies to set up connectors
 - preparing the AD organization unit structure for synchronization
 - Creating 'recipient policies' in Exchange to add the new mail-enabled contacts to the GAL
 - Developing an OU structure to accommodate synchronizing for the EAD and all Forests as the central synchronization point for the organization.

Staffing resources necessary for the project would include Design, Project, Server Provisioning, Network, Security, AD and SQL subject matter experts.

Estimated Time to Implement: 6 - 10 months

Support and Maintenance: Support requirements for the FIM Synchronization Service are estimated at an average of 1 hour per day to maintain logs, create custom filter lists (if allowed); create new connectors as requested, resolve replication conflicts and failures and general maintenance and monitoring of the environment.

Agency Support Responsibilities:

EAD Agency tasks would include:

- removing any manually created contacts that will now be populated from other agency AD forests via FIM



- Determining and configuring objects that they do not wish to synchronize AND/OR work with CTS to create custom filter lists (may need to change their OU structure and move accounts in order to accomplish filtering rules)
- Evaluating their Global Catalog Servers and upgrading disk space as necessary to accommodate replication of additional object in the forest.
- Communicate with End Users about the addition of the mail-enabled contacts before initial synchronization.

Non-EAD Agency tasks would include:

- connect to the SGN (if they are not currently connected)
- create a service account with read/write access to their AD Forest Directory
- work with CTS to establish the synchronization connectors
- remove any manually created contacts that will now be populated from EAD via FIM
- Create DNS conditional forwarders to enable communication with the FIM Server or provide Host information for at least two global catalog servers in their Forest.
- Provide information to CTS to create DNS forwarders to their Forest in order to communicate with global catalogs and provide the names of at least two global catalog servers to specify in the connector.
- Work with CTS to verify that global catalog servers have enough disk space to accommodate the additional objects to be replicated into their forest.

User Training: End users need to be educated about the changes they can expect in the Exchange Global Address Lists as a result of synchronization with other agencies and the timing of when synchronizations can be expected to occur.

Estimated Project Effort and Costs:

The estimated project resource effort and cost is 1,194 hours and \$88,953.00.

Project Resource Costs:

Project Manager:	350 hours
Design:	200 hours (includes design, design review, cross agency team)
Network:	16 hours
Security:	48 hours
Storage:	16 hours
Server Provisioning:	24 hours



Operations

Active Directory: 450 hours (2 AD SMEs)

SQL Server: 90 hours

Consulting Costs:

Microsoft Active Directory DSE: 24 Premier Hours @ \$250 per hour = \$6,000

Total Cost Estimate for Hardware, Software and Support: \$5,207.39 per month for the first year and \$4,228.73 per month thereafter.

Production System:

Hardware Costs: \$2,142.03 per month

Percentage Cost for existing Messaging SQL Server Cluster: TBD

Software Costs: \$10,601.28 or \$978.66 per month for 12 months

Pre-Production Environment:

Hardware Costs: \$594.70 per month (2 Virtual Servers [2 Cores, 4 GB RAM])

Software Costs: \$1,142.68 (Included in monthly software costs above)

Support Costs: 1 hour per day (.125 of an FTE = \$1,492 per month)

SMEs for this High Level Design:

Karen McLaughlin, CTS, CSD Design and Planning

Jay Knowlton, CTS, Active Directory SME

Brian Casey, Microsoft, AD Dedicated Support Engineer