

IdF Management Agent for Microsoft FIM

Bridging the Identity Divide



Features

- Native Authentication
- Bi-Directional User Profile Synchronization
- State-based Delta Import Support
- State-based Full Import Support
- Password Management
- Alias Management
- Catalog Management
- Resource Management (Data Sets & General Resources)
- System Management
- Enhanced Role Management
- Enhanced Performance
- Extend custom / legacy applications

IdF Advanced Adapter Suite

- CA-ACF2
- CA-Top Secret
- IBM-RACF
- IBM-i (OS400)

IdF Adapter Editions

- Enterprise Edition
- Standard Edition
- Express Edition

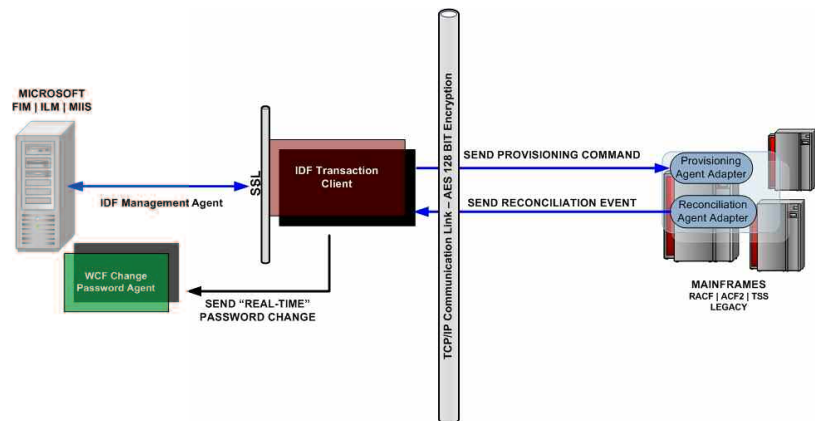
IdF Management Agent provides Microsoft enterprise class support for mainframe and midrange systems. The technology built on .NET working in concert with IdF's Advanced Adapter series presents the enterprise with a harmonious interaction between the two environments.

IdF Management Agent securely provides native support for the bi-directional administration of user profiles, administration of fine grain authorization of data sets, resource profiles and batch jobs. The relationship also provides reconciliation services, synchronizes services and password management between IdF Advanced Adapters and Microsoft Forefront Identity Manager, ILM and MIIS.

The IdF Advance Adapters are tightly integrated with the IdF Management Agent allowing Forefront Identity Manager, ILM, or MIIS to reconcile state-based full and delta imports along with real-time password synchronization for ease of population of mainframe / host based system id's and profiles.

The IdF Advanced Adapter is comprised of two components, the Pioneer and Voyager Agents. Both agents work together with the IdF transaction client allowing the mainframe to communicate natively with the IdF management agent. This elegant

Figure 1. IdF Microsoft FIM | ILM | MIIS Architecture



IdF Pioneer Agent

The Pioneer (provisioning) agent receives Identity and Authorization change events, effectuating requested changes upon the target system. The Pioneer agent is a mainframe-installed component that executes native requests that are sent from Microsoft FIM | ILM | MIIS.

IdF Voyager Agent

The Voyager (reconciliation) agent sends real-time notification events of user profile changes to FIM | ILM | MIIS from the target hostsystem. The agent detects events such as user addition and deletion and changes in status, attribute, group membership and/or password.

User Management

- Create, modify, or delete mainframe user
- Set one-time-use password (Administration Reset)
- Change password (Self service change) **ADVANCED**
- Revoke, resume, or disable user
- List user information
- Add or remove user from group / profile
- Add or remove user to General Resource Profile **ADVANCED**
- Build groups, associate users to groups
- Authorize or Un-Authorize use of resources, facilities and data sets **ADVANCED**
- Detect and report native delete user **ADVANCED**
- Detect and report native revoke user status **ADVANCED**
- Detect and report native resume status **ADVANCED**
- Detect and report native changes to user attributes **ADVANCED**

Group / Profile Management

- Add Group / Profile
- Remove Group / Profile
- List Profile (Including User Membership)
- Assign or Un-Assign User Membership (Multiple Users)
- Detect and report native group membership changes **ADVANCED**

Password Management

- Change password (Self service change) **ADVANCED**
- Resume (reset) password
- Replace password
- Detect native password change **ADVANCED**
- Synchronize native password in real-time **ADVANCED**

Role Management

- Search all group / roles (including membership) **ADVANCED**
- Query all user memberships **ADVANCED**
- Detect native role changes **ADVANCED**

System Management

- Alias management **ADVANCED**
- Provision of resource profiles (datasets, DASD volumes, tape volumes, load modules) **ADVANCED**
- Assign or Un-Assign user membership or ownership to resource profiles **ADVANCED**
- Retrieve resource profile information **ADVANCED**

Connection & Security

- Authentication or authorization
- Message to / from Transaction Client from Idf MA use SSL
- Passing messages to / from mainframe from Transaction Client are AES Encrypted
- Detect and report native user logon or authentication (by user logon, TSO command line or batch jobs) **ADVANCED**

Transaction Management & Scalability

- Use of memory sub-pools for event processing
- Processing in native commands **ADVANCED**
- Ability to store transactions for communication or system failure recovery **ADVANCED**
- Capture of mainframe initiated change events to meet compliance requirements **ADVANCED**

Extensibility

- Ability to integrate with Security Manager custom attributes **ADVANCED**
- Ability to provision to custom applications **ADVANCED**

System Requirements

Microsoft FIM | ILM | MIIS Requirements:

- .Net Framework 3.0 or above
- MIIS SP2 or above
- FIM RC0 or above

IBM Mainframe OS Requirements:

- OS/390
- z/OS 1.6 – 1.9

Security Managers:

- RACF on z/OS
- CA-ACF2 on z/OS 6.2 – 12.x
- CA-Top Secret on z/OS 5.2 – 12.x

IBM i5 OS Requirements:

- IBM i5/OS R5V2 or greater

For More Information

To learn more about Identity Management solutions for mainframe and legacy systems please visit us at www.identityforge.com.