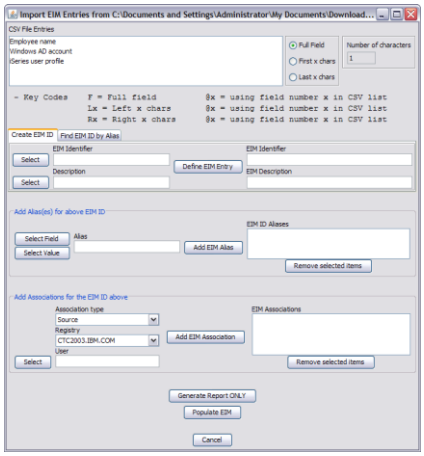
IBM Technology Expert Labs

Single Sign On Suite for IBM i

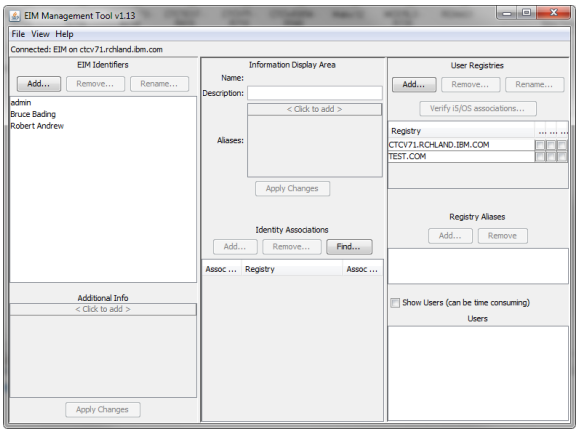
Simplify Single Sign On (SSO) implementation and reduce help desk costs

IBM Technology Expert Labs Power Delivery Practice is proud to provide a suite of tools uniquely designed to help your company get started with Single Sign On (SSO) with IBM i. SSO involves setting up Network Authentication Services (NAS) and then mapping Windows user profiles to IBM i user profiles using Enterprise Identity Mapping (EIM).



EIM Populator Tool

The EIM Populator Tool (EPT) is designed to help you load your existing user profiles into EIM at the start of your project. All current IBM i users that want to take advantage of SSO must be loaded into EIM, even if their Windows profile matches their IBM i profile. Normally, this is a manual process involving at least 20 clicks per user in IBM Navigator for i. With the EPT, a spreadsheet acts as the source and can load over 500 users into EIM per minute, all with a single mouse click! This tool is the perfect jump start to get all your users SSO enabled quickly and easily.



EIM Management Tool

The EIM Management Tool (EMT) is a Java based GUI that allows for ongoing maintenance of your EIM environment. This alternative to IBM Navigator for i brings all EIM items into a single management window allowing for easy access and configuration. Additional features include EIM export, EIM backup and restore, and the EIM Explorer tree-based visualizer.

EIM CL Commands

When users are created or deleted from IBM i, EIM mappings must also be created or deleted to allow the users SSO functionality. As mentioned above, the normal process involves manually creating an EIM Identifier and then adding at least two EIM Associations to the Identifier. However, you can use the power of the IBM i Create User Profile and Delete User Profile exit points to automatically

create and delete the EIM mappings. These exit points allow you to provide a simple program that automatically creates or deletes these items for you. The OS alone provides a series of complex and hard to use APIs. Delete user exit program included in package!

The SSO Suite includes a set of simple to use CL commands for creating and deleting EIM Identifiers and Associations. These commands are:

- ADDEIMID – Add EIM Identifier – call once per create user profile
- ADDEIMASSC – Add EIM Association – call once per source and target association
- ADDADDLINF – Add EIM Additional Info – add lookup info (for multiple target support)
- RMVEIMIDBN – Remove EIM Identifier – will remove associations as well
- RMVEIMID – Remove EIM by User Profile
- RMVEIMASSC – Remove EIM Association
- RMVADDLINF – Remove EIM Additional Info

Windows AD to IBM i Profile Synchronizer
This tool listens on changes of predefined Windows Active Directory groups and based on adding or removing memberships will create IBM i user profiles and the necessary EIM mappings for the given user. The configuration is performed via a XML configuration file. The program will register itself as an event listener to Windows AD and will perform actions for all groups that are configured in the XML configuration file.

Implementation Services
Need help securing your IBM i system? Our Expert Labs team is highly trained in the proper way to handle complex security configurations. We can guide you all the way from design to implementation. You don't have to undertake security yourself – allow IBM Expert Labs to be your trusted consultants to ensure a successful project!

Interested in a Quote or Learning More?
If you are interested in purchasing this asset or discussing it further with one of our consultants, please contact Ron Bibby at ronbibby@us.ibm.com! Or visit our website at https://ibm.biz/IBMiSecurity.

Statement of Good Security Practices
IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.