

SCDF User Account Plans

Presenter: Jason A. Smith

Co-Authors: Matt Cowan, John De Stefano, Ofer Rind

Thursday, August 13, 2026



@BrookhavenLab

History: How Did We Get Here?

Why SCDF Accounts Exist Separate From ITD AD Accounts?

- RCF created almost 30 years ago to manage RHIC Computing
- No centralized computing existed at BNL back then
- ITD's old user account system (before AD) was incompatible with RCF needs

Policy differences made merging difficult/impossible for many years

- We never delete accounts, never recycle/reuse uids/gids
- Password policies (length, complexity, expiration)
- Technical difficulties using AD on Linux

Multiple SCDF User Accounts

Was used to enforce resource separation between experiments

- Single primary group per user used to identify experiment
 - Was used by batch for resource scheduling long ago
 - Experiment data storage & file separation

Causes many problems for modern software and services

- Mattermost, Gitea, Drupal, etc. require single account per user
 - Conflicts with email address or other internal user data
- Extra burden on users & staff to manage multiple accounts
- Increased cyber security risk: more accounts to keep secure

Merging SCDF Accounts Into ITD AD

The policy & technical differences are no longer an issue

- AD accounts never expire (uids/gids never reused/recycled)
- Password policies modernized & roughly in sync
- Modern Linux works well with Microsoft AD

Advantages for users & SCDF admins

- Eliminate multiple accounts per user, single account to manage
 - Apply for one BNL account, then request access to SCDF resources
 - Conflicts with software and services are eliminated
 - Users no longer need to remember which account used for various services
 - Improves Cyber exposure, reduces attack surface (fewer total accounts)
- Improved password reset process & MFA (Duo replaces TOTP)
 - Basic account management administration offloaded to ITD
- Retire our aging AAI infrastructure instead of upgrading it

Still some technical challenges to test and overcome

- SCDF RH IdM server for local overrides (shell, ssh keys, groups, federated)
- Merging multiple accounts into one and resolving uid/gid conflicts

Proposed Account Plans & Changes

- Require BNL AD account before applying for SCDF account
 - Waiting for ITD to implement automatic uid/gid assignment for all new AD accounts (will eliminate all future conflicts during migration phase)
 - Will move SCDF new user form behind BNL login (more secure)
- Stop creating accounts for users who need to add/change experiment affiliation.
 - Assign secondary groups to primary account for users in multiple experiments
- Identify “Primary” SCDF account for users with multiple accounts
 - Matching BNL AD account where possible
 - Synchronize these Primary accounts with ITD AD
 - Resolve conflicts and edge cases where identified
- Deactivate all non-Primary SCDF accounts when ready (~300/2300)
 - Merge user’s data & files into primary account
- Setup testbed with SCDF Linux systems using ITD AD accounts & new RedHat IdM server for local overrides (shell, ssh-keys, group assignment, grid/federated/lightweight accounts, etc.)
- Federated account access through CManage will continue & expand