Secondary eIDs Replaced with NetID Service Accounts

Greg Vogl, Identity and Access Management
Division of Information Technology
May 24, 2023
Agenda

1. Overview of Changes
   - From eID to CSU System NetID
   - From Secondary eIDs to Service Accounts
2. Instructions and Demos
   - How to Request, View and Manage Service Accounts
3. Questions and Answers
eID System End of Life – The Why

• eID is a custom developed set of software and integration processes

• In service since 2000 – technology is aging

• Tightly integrated with Banner’s Oracle database

• Dependent on Banner availability

• Identity onboarding is a full day behind HR system entry for new employees at best.
eID System End of Life – The Why (continued)

- CSU Fort Collins and CSU-Pueblo now share many systems to reduce duplication and costs.
- CSU is providing Identity & Access Management (IAM) for the CSU System.
- Provisioning technologies/systems have matured in 20 years.
- Modernize and improve IAM systems and processes.
Definitions

• **NetID** is the name for the **CSU System** Identity and Access Management (IAM) system
  – Maintained by CSU Division of IT

• The **CSU System NetID website** is a self-service web application
  – Currently serves CSU-Pueblo; CSU Fort Collins being added

• **midPoint** is the identity management software that is replacing eID processes
  – Credential store and provisioning engine

• Part of **InCommon Trusted Access Platform** IAM stack
  – Shibboleth for single sign-on
  – Grouper for access group management
From eID to NetID: What will change?

- **New** primary NetIDs will not look like eIDs.
  - The format of a new primary NetID is an uppercase C followed by a 9-digit CSU ID, for example: C812345678.

- CSU Fort Collins and CSU-Pueblo primary and secondary NetIDs will be stored in the same midPoint instance.

- Everyone will activate, view and update primary and secondary NetIDs on the [CSU System NetID website](#).
Secondary eID Changes

• Rebranded to **NetID Service Accounts**

• No longer owned by an individual
  – But previous secondary eID owner becomes initial admin

• Departments become account owners

• Requesters are limited
  – CSU Microsoft 365/Exchange **Resource Coordinators**

• Grouper-managed security groups

• Yearly audit process
Goals of NetID Service Accounts

- Controlled and audited access
  - Many secondary eIDs are used for shared access
  - Allows delegated administrators to manage access
  - 2FA for account management (not implemented yet)
- Allow access for processes where a personal NetID can't or shouldn't be used
- Limited use accounts
  - Provisioned for SSO on request – not by default
- Microsoft 365 account, including email (optional)
- Stored and managed in midPoint

CSU IT policies

- Acceptable Use for Computing and Networking Resources
- Information Technology Security
  - 4. Passwords
  
  The act of authentication is the assertion that a credential (a username or other identifier) is possessed and being used by the appropriate person.
Acceptable Uses of Service Accounts

**Group**

- **Email address** for shared contact and support
  - for a department, unit or website
- **Short** email address used as an alias
  - e.g. *depthelp@colostate.edu*
  - Automatically forward all mail to a shared mailbox
  - e.g. *dept_helpdesk@colostate.edu*
- Group access to CSU **lab or facility resources**
  - if regular NetID access is not practical
- **Short-term access for non-CSU partners**
  - e.g. training, conference or workshop attendees and guest speakers

**Individual or Machine**

- **Secondary inbox** for an individual
  - (e.g. for secondary job role or large student documents)
- A true **service account**
  - non-personal machine account, for batch jobs, scripts, automated services
- **Testing or logging**
  - IT, PC, software or web development
Alternatives: Email

Use Cases

- Only need a shared email account?
- Only need a mailing list?
- Need an email name over 8 characters?
- Need an email name with underscores?
- Prefer Gmail?

CSU Microsoft 365 resources

- **Shared Mailbox**
  - no shared password

- **Mailing List**
  - no separate mailbox
  - [New Mailing List form](#)

- **Email Alias**
  - flexible naming options

- **Gmail**
  - [Google Workspace for Education at CSU](#)
Alternatives: Document and File Sharing

Shared Drives

• **OneDrive for Business**
  – (5 TB, can be extended)
  – **Microsoft 365 at CSU**
  – **Share and Collaborate with OneDrive**

• **Google Drive**
  – (just 25 GB)
  – **Google Workspace for Education at CSU**
  – **Share files and other content with a group**

• Departmental network drives

Collaboration Tools and Websites

• **Microsoft Teams at CSU**
  – **File Sharing**

• **Microsoft SharePoint sites at CSU**

• **Google Sites**
  – **Google Workspace for Education at CSU**
Secondary eID to NetID Strategy

- Manage Service Account Credential
- Supply AuthN and Attributes
- Provision
- Supply Subjects
- Provision
- Provision
- Access
- Campus and SaaS Services

Diagram:
- midPoint Account Lifecycle Identifier Management
- CSU IdP
- SSO
- Group Owners
- IAM Admin
- Management of Reference Groups
- OpenLDAP/Active Directory
- Group PSPNG
- Grouper Access Governance, Policy, Audit, Compliance and Reference Groups
Project Timeline

Past

• June-July 2022
  – Existing secondary eIDs were selected for migration.

• July-Sept 2022
  – eIDs were rebranded to NetIDs.

Present

• May 24-30, 2023
  – No new secondary eIDs are requested or created.
  – No secondary password changes.

• May 31, 2023
  – NetID service accounts replace secondary eIDs.
  – NetIDs managed on CSU System NetID website.

Future (dates are tentative)

• July 21-23, 2023
  – Primary NetID account migration to MidPoint.
  – No primary or secondary account changes.

• July 24, 2023
  – CSU System NetID website fully replaces the CSU Fort Collins NetID (eID) website.

• October 2, 2023
  – Unmigrated Secondary eIDs are deactivated.
    • Microsoft account removed.
Requesting Migration of Secondary eIDs

1. Check your secondary eIDs in CSU Fort Collins NetID.

2. Check your secondary eIDs you requested for migration.
   - Do not need any migrated? No action needed.
   - Already requested? No action needed.
   - Need to migrate more NetIDs? Resubmit the form.
   - One of your secondary eIDs is missing but needs migration? Contact us.
   - Want an unused secondary eID deactivated immediately? Contact us.

3. Check your service account groups in Grouper.
   - A secondary eID you requested for migration is missing? Contact us.
Starting May 31, 2023, you can request new NetID service accounts.

1. Copy form from NetID FAQ: How do a request a service account?
2. Paste into an email to your Resource Coordinator.
3. They can review it and submit a Service Account Request.
CSU System NetID Temporary Login

- **May 31-July 20**
  - CSU System NetID header does not specify a campus
  - CSU Fort Collins Login goes to CSU Fort Collins NetID
  - Service Account Admins/Requesters and NetID admins have a separate login option for CSU System NetID

- **Starting July 24**
  - CSU Fort Collins Login goes to CSU System NetID
Viewing Your NetID Service Accounts

1. Log in to CSU System NetID.

2. Click View/Update > Service Accounts to display service accounts you administer.

3. Click a NetID to view or edit details of the service account.

Service Accounts

<table>
<thead>
<tr>
<th>Service Account</th>
<th>Dept</th>
<th>Initial Admin NetID</th>
<th>Initial Admin Name</th>
<th>Microsoft Account</th>
<th>Status</th>
<th>Created</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>gregvogl</td>
<td>1010</td>
<td>gregvogl</td>
<td>Greg Vogl</td>
<td>Yes</td>
<td>active</td>
<td>2013-09-06 15:25:17</td>
<td>2023-01-24 17:14:38</td>
</tr>
<tr>
<td>gtest</td>
<td>1010</td>
<td>gregvogl</td>
<td>Greg Vogl</td>
<td>Yes</td>
<td>inactive</td>
<td>2022-07-28 17:10:00</td>
<td>2022-07-28 17:10:00</td>
</tr>
<tr>
<td>gtest2</td>
<td>1010</td>
<td>gregvogl</td>
<td>Greg Vogl</td>
<td>No</td>
<td>active</td>
<td>2022-07-28 17:11:00</td>
<td>2022-07-28 17:11:00</td>
</tr>
<tr>
<td>iamhelp</td>
<td>1010</td>
<td>rmioke</td>
<td>Randy Mioke</td>
<td>Yes</td>
<td>active</td>
<td>2020-07-30 12:23:30</td>
<td>2020-08-07 23:16:45</td>
</tr>
</tbody>
</table>

Service Accounts Help
Viewing and Editing a Service Account

- Admins can only edit Account Name and Description, Manage Admins, and Change Password.
- Need other changes? Contact us.
Changing Password of Service Account

- Passwords expiring May 1-Aug 1 extended 90 days
  - Expiration email notifications temporarily deactivated
  - Fort Collins primary and secondary NetIDs only
  - Intended to prevent lockout during NetID migration
- Many secondary eIDs have expired passwords
  - Check expiration dates of yours
  - IT security policy requires annual password changes
- Same password requirements as for primary NetIDs
  - Slight changes from Fort Collins NetIDs
- See FAQ for securely sharing password if necessary
Adding Service Account Administrators

• Recommendation
  – Add at least one person in addition to yourself.

• Reasons
  – They can be your backup in your temporary absence.
  – Transfer administration to someone else before you leave.

• People you might want to add
  – Your Resource Coordinator or RC group
  – Department IT staff member, admin assistant, or head

• People not to add
  – Students (who are not full-time faculty or staff)
  – Vendors (instead request an associate NetID from HR)
  – Anyone who should not have full control of the account
Viewing Service Account Grouper Groups

1. **Grouper** requires a campus IP address.
   - On Campus Ethernet or Wireless
   - CSU GlobalProtect VPN
2. **Log in to Grouper** with your NetID + Duo.
3. Click **My groups**.
4. Filter for **Service_Accounts** (if needed).
5. Click a **Folder** to view department groups.
6. Click a **Group name** to view members.
Adding Group Members

1. View existing members in Members tab under Entity name.
2. Click +Add members.
3. For Member name or ID, type the new admin’s name or NetID.
4. Click a member name to select it.
5. Click Add.
Adding an RC Group as a Member

• **Resource Coordinator groups** include primary and secondary (backup) coordinators.
  - Folder is `basis : sqlprod : exchange_resource`
  - Group name is a number (not department number)

1. Search Grouper for `exchange_resource` and the group name (or department name or number).
   - For multiple results, mouse over the name of each result to find the correct group and primary Resource Coordinator (RC).

2. **Add members** in your service account group
Revoking Group Memberships

1. Find the person under **Entity name**.

2. Under **Choose action**, select **Actions > Revoke membership**.
   - You can remove yourself to completely transfer service account administration to someone else.
   - You should not remove yourself until after you have added another member.
LDAP Entitlements

Creation, Release, Use

• Grouper groups can add entitlement attributes to user LDAP records.
• After single sign-on, Shibboleth releases LDAP attributes to apps.
• Apps like NetID use these attributes to assign roles and permissions.

Examples

• NetID admins can see entitlements at Person Admin > LDAP: https://eid.colostate.edu/csusystem/admin/ldap.aspx?netid=<netid>
• Service account requester entitlement: https://colostate.edu/netid/serviceaccount/requester
• Individual service account admin entitlement format: https://colostate.edu/netid/svc_acct/<netid>
NetID Admin Privileges

- **Service Account Admins** can view service account details, change the password, manage admins, and access the Microsoft 365 account including **Outlook email**.
  - They are members of Grouper groups for one or more service accounts.

- **Service Account Requesters**
  - Can view all service accounts
  - Can request new service accounts
  - Almost all requesters are **Resource Coordinators**

- All **NetID Admins** can view all service accounts.
Listing Service Accounts

- Restricted to Service Account Requesters and NetID Admins

1. Go to Admin > Service Account List
2. Search by NetID, initial admin, department
3. Defaults: MS account, your campus, active
4. Filter results – enter text in any field(s)
5. Click column header to sort by any field
6. Click a NetID to view service account details
Requesting Service Accounts

• Restricted to Service Account Requesters

1. Determine if a service account is appropriate.
   – If not, suggest alternatives to consider.

2. Assure the service account NetID has correct format.

3. Go to Admin > Service Account Request

4. Copy and paste details from the email.

5. Click Send Request.

• View the status of your past requests in the list.

• Click a NetID to view the request details.
   – Editable if status is still “requested”
More Information

- CSU Division of Information Technology: NetID
- CSU System NetID FAQ: Service Accounts
- CSU System NetID: Contacts