Introduction to SACS

SACS Application Course

Introduction
Lesson 01 – Application Security
Lesson 02 – Data Import
Lesson 03 – Dashboard
Lesson 04 – Forms
Lesson 05 – Technical Review Checks (TRC)
Lesson 06 – Data Submissions
LESSON 01 – Application Security

SACS Application Security Performance Objective

a) User must be able to log into the SACS Application
b) User must be able to identify user roles and the permissions associated with that role
c) User must be able to create a user account
d) User must be able to perform User Management roles on user accounts.
The SACS application allows the user to manage permissions throughout the system to control user access per entity.

All users are required to have an account and log into the application with a username and password. An account not associated with an entity is considered a Public account. Each account which is associated with one or more entities will have one or more roles.

Each user is assigned specific levels of access (roles) by a user with the User Management role.
<table>
<thead>
<tr>
<th>USER ROLE</th>
<th>PERMISSIONS</th>
<th>How do I Get this Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Default account; ability to view budget and interim data for all entities and view published Unaudited Actuals. <em>No assigned roles or associated entities</em></td>
<td><strong>SELF REGISTER</strong> or User Management</td>
</tr>
<tr>
<td>Edit Draft Dataset</td>
<td>Basic data entry processes; abilities limited to draft datasets</td>
<td>User Management</td>
</tr>
<tr>
<td>Edit Dataset</td>
<td>Basic data entry processes across the submission</td>
<td>User Management</td>
</tr>
<tr>
<td>Dataset Approval</td>
<td>Ability to promote a draft dataset to the next state</td>
<td>User Management</td>
</tr>
<tr>
<td>Oversight</td>
<td>Review or edit a submission for which the entity has oversight responsibilities</td>
<td>User Management</td>
</tr>
<tr>
<td>Certify/Promote to CDE</td>
<td>Staff allowed to submit UA data and certify it; Formerly eTransfer access form users; <em>Can only be assigned by CDE</em></td>
<td><strong>CDE User Management</strong></td>
</tr>
<tr>
<td>User Management</td>
<td>Manages user accounts</td>
<td>Administration or User Management</td>
</tr>
<tr>
<td>Administration</td>
<td>Superuser; creates administration account</td>
<td><strong>CDE User Management</strong> or Administration</td>
</tr>
</tbody>
</table>
LESSON 01 – Application Security

Descriptions of District/COE SACS Security Roles

To begin, it is important to know where a user gets their role(s) and who grants the access to each user.

CDE USER MANAGEMENT Role

CDE User Management role
• Grants Administration and User Management roles to one COE user to ultimately delegate roles to related entities (upon initial setup)
LESSON 01 – Application Security

ADMINISTRATION Role

The highest level of user (role) at the COE/District is the COE Administrator role:
- Creates other Administration accounts and grants other Administration roles
- Considered a **SUPER USER** (ability to restore a prior version of a Submission via the Version History screen and unlock a locked submission)
- **This role is not in the normal workflow for data submissions**
The manager of user roles at the entity and/or related entities:
- Creates other *User Management* accounts and grants ALL other user roles.
  - For example, COE grants User Management role to one District user upon initial setup of the system
  - In another example, District user manager creates user accounts for district staff and assigns edit draft dataset, edit dataset, and/or dataset approval roles
- **This role is not in the normal workflow for data submissions**
OVERSIGHT Role

Oversight role
- 1st and 2nd Level Submission review for related entities
- Ability to reject and return submissions to the originating LEA
- Ability to edit datasets
- Ability to publish Budget and Interim submissions
- NOTE: Oversight role will also be used by districts who have authorized charter schools.
**LESSON 01 – Application Security**

**Certify/Promote to CDE**

**CDE USER ROLE**
- Analyst
- Consultant
- Publish
- Lead Workflow Consultant
- User Management
- Help Management
- Workflow Management
- Administration
- System Administration
- Validation Table
- Maintenance

**USER ROLE**
- Edit Draft Dataset
- Edit Dataset
- Dataset Approval
- Oversight
- Certify/Promote to CDE

**COE Certify/Promote to CDE role**
- Ability to submit Request for unaudited actuals Promoter access
- Ability to promote/demote a submission to the following states:
  - Promote to Pending CDE Authorization
  - Demote to Active Submission Returned
  - Demote to Resubmission Required (if rejected by CDE)
USER ROLE
- Edit Draft Dataset
- Edit Dataset
- Dataset Approval

DATASET APPROVAL
- Ability to see any draft dataset submissions within the assigned entity for review and promotion to the next level
  - Ability to promote a draft dataset to submission dataset
  - Ability to promote a submission dataset to reviewing agency
EDIT DRAFT/DATASET Role

EDIT DRAFT DATASET
- Basic data process abilities limited to Draft Datasets
- This role can only see datasets that are in the DRAFT state and owned by the current user.

EDIT DATASET
This role is assigned for data entry and to allow peers to collaborate and review datasets prior to promoting to reviewing entity.
- Basic submission process abilities
- This role can promote a dataset to Pending Internal Review state.
# LESSON 01 – Application Security

<table>
<thead>
<tr>
<th></th>
<th>Public</th>
<th>Edit Draft Dataset</th>
<th>Edit Dataset</th>
<th>Dataset Approval</th>
<th>Oversight</th>
<th>User Management</th>
<th>Administration</th>
<th>Certify/ Promote to CDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>District</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Charter School</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>COE</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>SELPA</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>*</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>CDE</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>SBE</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>JPA</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

* SELPA Oversight role is still under evaluation
LESSON 01 – Application Security

Adding a New User (Step 1 of 2)

1. Click New User Button

2. Enter User Information

3. Click Submit
LESSON 01 – Application Security

Adding a New User (Step 2 of 2)

Editing, adding, or deleting roles associated with an account

1. Click the **EDIT ENTITY ROLES** button to open the Entity Roles dialog box
2. Add or Delete roles for the account
3. Save Changes
To setup a password

- Password strength **must** meet the following criteria to be considered **STRONG**.
  - At least **8 characters** in length
  - Not be the same as email
  - At least one uppercase letter (**A-Z**)
  - At least one lowercase letter (**a-z**)
  - At least one number (**0-9**)
  - At least one special character ( ! @ # $ ^ & * - = _ + ? )
LESSON 01 – Application Security

Logging on to the SACS Application

- Access the **SACS Web Application** on the Internet
- Login using your **Entity specific Username** and **Password**
- Verify your **entity, account status and role**
- Updating your SACS user account **contact information**
Log in to the SACS Application

- Locate the **SACS Web Application** on the Internet
- Login using your Entity specific **Username** and **Password**
- Verify your entity, account status and role
- Updating your SACS user account **contact information**
LESSON 01 – Application Security

Logging to the SACS Application

- Locate the SACS Web Application on the Internet
- Login using your Entity specific Username and Password
- Verify your entity, account status and role
- Updating your SACS user account contact information
UNIT 01 – Application Security

### User Information

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Phone Number</th>
<th>Extension</th>
<th>Email / Username</th>
<th>Password Status</th>
<th>Account Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emanuel</td>
<td>Norman</td>
<td></td>
<td></td>
<td>enorman@fcmsure</td>
<td>Active</td>
<td>Active</td>
</tr>
</tbody>
</table>

### User Entity Roles

<table>
<thead>
<tr>
<th>Level</th>
<th>Entity Name</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>California Department of Education</td>
<td>99-00000-000000 California Department of Education</td>
<td>Analyst, Consultant</td>
</tr>
<tr>
<td>School District</td>
<td>01-81119-0000000 Alameda Unified</td>
<td>Administration</td>
</tr>
</tbody>
</table>

- Administration
- Dataset Approval
- Edit Dataset
- Edit Draft Dataset
- Oversight
- User Management
LESSON 01 – Application Security

Logging to the SACS Application

- Locate the SACS Web Application on the Internet
- Login using your Entity specific Username and Password
- Verify your entity, permissions and role
- Updating your SACS user account contact information

User Information

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Phone Number</th>
<th>Extension</th>
<th>Email / Username</th>
<th>Password Status</th>
<th>Account Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emanuel</td>
<td>Norman</td>
<td></td>
<td></td>
<td>enorman@fcm...</td>
<td>Active</td>
<td>Active</td>
</tr>
</tbody>
</table>
Managing your SACS User Account

- Change your SACS password
- Change your email address/username
- Change your entity (if you are associated with more than one)
- **Reset** your password
- Notes about the status of your account
  - You will be logged out of system with 30 minutes of inactivity. **Save your work often.**
  - You will be notified by email that your account is **locked** **after 5 failed** attempts to login
  - You will be notified by email that your password will expire **in 12 days**
  - You will be notified by email that your password has expired **after 90 days**
  - You will be notified by email that your password has expired **for 1 year** and will be **inactive**
- Indicate whether you would like to **OPT-IN** to the **Beta Testing** email distribution list
LESSON 01 – Application Security

Managing SACS User Accounts

- Viewing specific SACS users
  - View all **PUBLIC** user accounts on the User List
  - View all **LOCKED** and **INACTIVE** user accounts on the User List
  - View all **ACTIVE** accounts for your specific entity on the User List
  - Use the **filter/sort feature** to view specific accounts on the User List

- Modifying specific information on existing accounts
Viewing specific SACS user accounts:
- View all PUBLIC user accounts on the User List
- View all LOCKED and INACTIVE user accounts on the User List
- View all ACTIVE accounts for your specific entity on the User List
- Use the filter/sort feature to view specific accounts on the User List

Modifying specific information on existing accounts:
- Manage SACS user accounts
  - Issue a Password Reset to an existing SACS user account
  - DELETE a SACS user account

Select the View User List on the Top Ribbon under the Users menu to view the User List.
LESSON 01 – Application Security

Managing SACS User Accounts

View all PUBLIC user accounts on the User List

View all LOCKED, ACTIVE and/or INACTIVE user accounts on the User List

View all PUBLIC user accounts on the User List

View all LOCKED, ACTIVE and/or INACTIVE user accounts on the User List

Modify specific information on existing accounts

Manage SACS user accounts

Issue a Password Reset to an existing SACS user account

DELETE a SACS user account
LESSON 01 – Application Security

Managing SACS User Accounts

Use the **filter/sort feature** to view specific accounts on the User List.
Managing SACS User Accounts

- **Viewing specific SACS users**
  - View all **PUBLIC** user accounts on the User List
  - View all **LOCKED** and **INACTIVE** user accounts on the User List
  - View all **ACTIVE** accounts for your specific entity on the User List
  - Use the **filter/sort feature** to view specific accounts on the User List

- **Modifying specific information on existing accounts**
LESSON 01 – Application Security

Managing SACS User Accounts

Entering user information
1. Click the **EDIT USER** button to open the EDIT PROFILE dialog box
2. Enter user information for the account.
3. Click the **SAVE ALL CHANGES** button.

Edit Profile

- **User Information**
  - **First Name**: EmanuelLEA
  - **Last Name**: LEAUser
  - **Phone Number**: 123-456-7890
  - **Email / Username**: emanuelnorman@outl...
  - **Password Status**: Active
  - **Account Status**: Active
  - **Action**: Edit
  - **Password**
LESSON 01 – Application Security

Editing, adding, or deleting roles associated with an account

1. Click the **EDIT ENTITY ROLES** button to open the Entity Roles dialog box
2. Add or Delete roles for the account
3. Save Changes
LESSON 01 – Application Security

SACS Application Security Quiz

Quiz is located at: SACS Application Security Quiz