Access and Identity Management (AIM) Training

Radha Madrigal
Customer Service Department
December 1, 2015

The information contained in these materials is provided for general information only and does not constitute legal or regulatory advice. The ultimate responsibility for complying with the ISO FERC Tariff and other applicable laws, rules or regulations lies with you. In no event shall the ISO or its employees be liable to you or anyone else for any decision made or action taken in reliance on the information in these materials.
Agenda – Review AIM functionality

- View POC profile
- Create new user
- Add/remove user access
- View request history
- View users
- Endorsed user functionality
- Review applications tab
- Renew user certificate
- Manage access control list (ACL) groups
- Manage email notifications
Access and Identity Management (AIM) Application

• AIM provides registered application access Point Of Contacts (POCs) the ability to manage their user application access, including automated provisioning and removal as well as automated certificate renewals.

• Email POCrequests@caiso.com to obtain AIM access
Key Concepts

- A digital certificate is required to access ISO applications
- “Create new user” issues a new certificate for that user
- “Access request” grants access to specific applications
- “Endorsed user” has been given access to your organization’s assets, but is not directly employed by your organization
POCs for Multiple Organizations

- CAISO will distribute additional certificates for POCs representing multiple organizations

- Install all certificates in your Internet Explorer browser

- Upon login select applicable certificate for the organization you wish to provision access
POC Profile
• Information about the individual POC
Opt-out of Weekly Certificate Expiry Email

- POCs receive a weekly email notifying them of the user certificates that will be expiring in the near future

- A field on the **POC Profile** screen allows the POC to opt-out of these notices

- Change to “No” to opt-out of weekly emails
• List of ISO applications and SCIDs POC can grant access to
Create New User
Create New User

- Click **Create New User** button
- User must be created before access request can be submitted
Users – Create New User button

- System will validate new users based on last name and email match within the POC’s organization.

![Create New User Form](image-url)
Add/Remove User Access
Access Request – New Request

- Click pencil button to create new request
Access Request – New Request

- Click **New Row** button to add a new row
Access Request – New Request

- Enter a description for the new request
- Click **Update** button
• Select user(s) and click Add button
**Access Request – New Request**

![Access Request Interface](image)

- **User(s) move to Selected Users box**

<table>
<thead>
<tr>
<th>Available Users</th>
<th>Selected Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAM</td>
<td>Training User8</td>
</tr>
<tr>
<td>Training POC</td>
<td>AIM</td>
</tr>
<tr>
<td>Training User1</td>
<td>AIM</td>
</tr>
<tr>
<td>Training User10</td>
<td>AIM</td>
</tr>
<tr>
<td>Training User2</td>
<td>AIM</td>
</tr>
<tr>
<td>Training User3</td>
<td>AIM</td>
</tr>
<tr>
<td>Training User5</td>
<td>AIM</td>
</tr>
<tr>
<td>Training User6</td>
<td>AIM</td>
</tr>
<tr>
<td>Training User7</td>
<td>AIM</td>
</tr>
<tr>
<td>Training User9</td>
<td>AIM</td>
</tr>
</tbody>
</table>

- User ID: 152
- Request Description: Request for User8
- Updated By: XATRAININGPOC140071
- Updated Date: 11/30/2015 18:18

**New Access Request**

- **Request ID**: 152
- **Description**: Request for User8
- **Updated By**: XATRAININGPOC140071
- **Updated Date**: 11/30/2015 18:18

**Options**:
- Add All
- Add
- Remove
- Remove All

- **User(s) move to Selected Users box**
Move to Select Applications and Roles tab
Select Available Applications/Roles and click Add button
Add or remove access
• Choose Action, Application, Role, Environment and Entity (SCID) and click **Update** button
Access Request – New Request

- Click Preview button to review request.
Access Request – New Request

- Review access request for accuracy
- Click **Submit** button to complete request
View Request History
Access Request – Request History

- View requests for access
View Users

- My Users
- Endorsed Users
Users

- View “my users” and “users endorsed to me”

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
<th>Email</th>
<th>Status</th>
<th>Cert Expiration Date</th>
<th>PROFILE ACCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training POC</td>
<td>AIM</td>
<td><a href="mailto:NRITest@caiso.com">NRITest@caiso.com</a></td>
<td>Active</td>
<td>10/31/2014</td>
<td></td>
</tr>
<tr>
<td>Training User1</td>
<td>AIM</td>
<td><a href="mailto:traininguser1@caiso.com">traininguser1@caiso.com</a></td>
<td>Active</td>
<td>10/31/2014</td>
<td></td>
</tr>
<tr>
<td>Training User2</td>
<td>AIM</td>
<td><a href="mailto:TNgo@caiso.com">TNgo@caiso.com</a></td>
<td>Active</td>
<td>10/31/2014</td>
<td></td>
</tr>
<tr>
<td>Training User3</td>
<td>AIM</td>
<td><a href="mailto:TNgo@caiso.com">TNgo@caiso.com</a></td>
<td>Active</td>
<td>10/31/2014</td>
<td></td>
</tr>
<tr>
<td>Training User7</td>
<td>AIM</td>
<td><a href="mailto:rkmadrigel@caiso.com">rkmadrigel@caiso.com</a></td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training User10</td>
<td>AIM</td>
<td><a href="mailto:rkmadrigel@caiso.com">rkmadrigel@caiso.com</a></td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training User9</td>
<td>AIM</td>
<td><a href="mailto:rkmadrigel@caiso.com">rkmadrigel@caiso.com</a></td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training User6</td>
<td>AIM</td>
<td><a href="mailto:rkmadrigel@caiso.com">rkmadrigel@caiso.com</a></td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training User5</td>
<td>AIM</td>
<td><a href="mailto:rkmadrigel@caiso.com">rkmadrigel@caiso.com</a></td>
<td>Active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Users – My Users

- Contains All users within the POC’s organization
- Columns in ALL CAPS contain clickable fields that will display a pop up window containing additional information
User Profile (PROFILE button)

- Personal contact and certificate information for selected user
- POC will access this screen to revoke all access from a specific user
Current User Access (ACCESS button)

- Lists all applications and entities the selected user has access to
- If the user has been endorsed by another organization, the entity for that organization will be included on this list
Users – Users Endorsed to Me

- Displays all endorsed users
Current Endorsed User Access (ENDORSED ACCESS button)

- Displays a list of all applications the endorsed user has access to
Endorsed User Functionality

- Endorsed Users Without Access (in POC Profile)
- Endorse/UnEndorse My Users
- UnEndorse Users Endorsed to Me
- Add/Remove Endorsed User Access
- Endorsed Access Request History
Users endorsed to your organization who have no access to your data are shown here.
Endorsed Access Request – Endorse/UnEndorse My Users

- Endorse your user to another organization
- Request can contain multiple users
- One organization at a time
Endorsed Access Request – Endorse/UnEndorse My Users

- Use this screen to “UnEndorse” or remove your user’s access to another organization’s assets
• Use this screen to “UnEndorse” or remove ALL access from another organization’s user
Endorsed Access Request – Add/Remove Endorsed User Access

Use this screen to add/remove access for an endorsed user
(Note: These steps are the same as those on slides 14-22)
Endorsed Access Request – Endorsed Access Request History

- View requests for access for endorsed users
Applications
### Applications

**Applications**

- **View list of users sorted by application**
- **My users**
- **Endorsed users**
- **Use filters to sort this list**
- **Click Apply to view all users for all applications**

<table>
<thead>
<tr>
<th>Application</th>
<th>First Name</th>
<th>Last Name</th>
<th>Certificate Expiration Date</th>
<th>Role</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>STAGE</td>
</tr>
<tr>
<td>ADS</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>MAP-STAGE</td>
</tr>
<tr>
<td>AIM</td>
<td>AIM</td>
<td>Training POC</td>
<td>10/31/2014</td>
<td>POC</td>
<td>STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>MAP-STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User3</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User3</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>MAP-STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User2</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User2</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>MAP-STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>MAP-STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>MAP-STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>MAP-STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>MAP-STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>STAGE</td>
</tr>
<tr>
<td>CMRI</td>
<td>AIM</td>
<td>Training User1</td>
<td>10/31/2014</td>
<td>EXTERNAL READ-ONLY</td>
<td>MAP-STAGE</td>
</tr>
</tbody>
</table>

**Note:**

- **POC Profile**
- **Users**
- **Applications**
- **Certificate Renewal**
- **ACL Groups**
- **Access Request**
- **Endorsed Access Request**
- **Email Configuration**

---

ISO PUBLIC – © 2015 CAISO
Certificate Renewal
Certificate Renewal

- Use filters to display certificates in date increments
- Cannot be renewed more than 90 days in advance
- Click the **Renew** or **Let Expire** button to manage user’s certificate
Access Control List (ACL) Groups
Access Control List (ACL) Functionality

• An Access Control List (ACL) defines the access rights each user has to particular assets (resources)

• ACL functionality added for Outage Management System (OMS) application at the asset level

• POCs will create a new ACL group to isolate and grant access to a single asset (or group of assets)
Access Control List (ACL) Functionality

1. Create ACL group
2. Add assets to group
Email Configuration

- Allows POC to provide additional email addresses to receive email notification of system activity

Note: This screen contains draft text that will be updated when AIM enhancements are activated.
Conclusion

- View POC profile
- Create new user
- Add/remove user access
- View request history
- View users
- Endorsed user functionality
- Review applications tab
- Renew user certificate
- Manage access control list (ACL) groups
- Manage email notifications
Questions?
Questions?

- **POCrequests@caiso.com**
- Massih Ahmadi
  - mahmadi@caiso.com
  - 916-608-5861