Access and Identity Management (AIM) User Guide

Document Owner: Customer Readiness
## REVISION HISTORY

<table>
<thead>
<tr>
<th>VERSION NO. (Must match header)</th>
<th>DATE</th>
<th>REVISED BY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>7/16/13</td>
<td>RMadrigal</td>
<td>Initial document created</td>
</tr>
<tr>
<td>1.1</td>
<td>8/29/13</td>
<td>RMadrigal</td>
<td>Supplemental edits</td>
</tr>
<tr>
<td>1.2</td>
<td>9/9/13</td>
<td>RMadrigal</td>
<td>Supplemental edits</td>
</tr>
<tr>
<td>1.3</td>
<td>9/17/13</td>
<td>RMadrigal</td>
<td>Updated screenshots</td>
</tr>
<tr>
<td>1.4</td>
<td>10/9/13</td>
<td>RMadrigal</td>
<td>Final edits</td>
</tr>
<tr>
<td>2.0</td>
<td>12/23/13</td>
<td>RMadrigal</td>
<td>Added release 2 functionality</td>
</tr>
<tr>
<td>2.1</td>
<td>3/5/14</td>
<td>RMadrigal</td>
<td>Added list of auto-provisioned applications. Added notes regarding certificate creation and renewal. Added note regarding requests for endorsed users.</td>
</tr>
<tr>
<td>2.2</td>
<td>7/1/14</td>
<td>RMadrigal</td>
<td>Updated with ACL functionality, weekly expiry email.</td>
</tr>
<tr>
<td>2.3</td>
<td>7/25/14</td>
<td>RMadrigal</td>
<td>Updated with new Create ACL Group button</td>
</tr>
<tr>
<td>2.4</td>
<td>1/14/16</td>
<td>LStoloski</td>
<td>Updated with new endorsed user enhancements and email configuration</td>
</tr>
<tr>
<td>2.5</td>
<td>2/10/16</td>
<td>LStoloski</td>
<td>Updated with new auto provisioned applications</td>
</tr>
<tr>
<td>2.6</td>
<td>4/20/16</td>
<td>LStoloski</td>
<td>Revised endorsed user step by step instructions</td>
</tr>
<tr>
<td>2.7</td>
<td>02/16/17</td>
<td>Mahmadi</td>
<td>Revised ACL Group function and replaced all POC with UAA. Improve flow of information for users.</td>
</tr>
<tr>
<td>2.8</td>
<td>10/18/18</td>
<td>Monica M.</td>
<td>Updated with new AIM Enhancement Functionalities:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Ability to see the endorsement requestor(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Visibility to other UAA’s and their authorized “entities” and “contracts” within the same organization on the UAA Profile page</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Weekly Expiry Email option default to “Yes”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Email auto generation when the UAA provisioning request(s) are rejected by CAISO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auto generated email notification message to both organization UAA’s for each endorsement application request</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Author</td>
<td>Changes</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2.9</td>
<td>09/10/19</td>
<td>Monica M.</td>
<td>Added the Access Request Status section</td>
</tr>
<tr>
<td>2.10</td>
<td>04/08/20</td>
<td>Monica M.</td>
<td>Added clarification for OMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provided:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Modified Intro page</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Best Practices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Clarification for ACL group</td>
</tr>
<tr>
<td>3.0</td>
<td>06/04/20</td>
<td>SDainard</td>
<td>Added item # 11 under the 'Best Practices' section regarding the conflicting roles for RIMS users.</td>
</tr>
<tr>
<td>3.1</td>
<td>06/10/20</td>
<td>SDainard</td>
<td>Added section to 'Best Practices' and modified Create New User section regarding entering an individual's email address.</td>
</tr>
<tr>
<td>3.2</td>
<td>06/16/20</td>
<td>Monica M.</td>
<td>Adding clarification to the 'Best Practices' section regarding the between the 'ADJACENT RC WRITE EXTERNAL' role and 'RC MEMEBER READ ONLY EXTERNAL' role for webOMS.</td>
</tr>
<tr>
<td>3.3</td>
<td>01/20/2021</td>
<td>SDainard</td>
<td>Replaced screenshots to remove POC and add new tab for UAAs. Edited document.</td>
</tr>
<tr>
<td>3.4</td>
<td>09/18/2023</td>
<td>DVance</td>
<td>Updated screenshots for new tab called Manage Certificates. Added sections for Creating or Renewing a Certificate, Downloading Email Templates, Downloading Certificates Only, Resending Customer Passwords for Certificates, and Certificate Statues. Added #14 to Best Practice. Included additional verbiage to which environment users should be requesting. Instructions for how to End Date another UAA in an organization. Updated verbiage for How to Revoke a Certificate.</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Author</td>
<td>Changes</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3.5</td>
<td>10/06/2023</td>
<td>DVance</td>
<td>Added two notes for downloading certificates and whitelisting urls.</td>
</tr>
<tr>
<td>3.6</td>
<td>10/16/2023</td>
<td>DVance</td>
<td>Added section “Navigating to AIM”</td>
</tr>
<tr>
<td>3.7</td>
<td>11/16/2023</td>
<td>DVance</td>
<td>Added section “How to Reactivate Another UAA’s Expired Profile”. Also added a reminder that once a UAA profile has been end dated, authorized contracts and entities need to be wiped out.</td>
</tr>
<tr>
<td>3.8</td>
<td>12/28/2023</td>
<td>DVance</td>
<td>Updated verbiage to sections Create New User, Submit Access Request, and Access Request Status for certification download process.</td>
</tr>
<tr>
<td>3.9</td>
<td>02/15/2024</td>
<td>DVance</td>
<td>Updated the Renew a Certificate section to include updated screenshots with the “Provider” column.</td>
</tr>
<tr>
<td>4.0</td>
<td>03/05/2024</td>
<td>DVance</td>
<td>Added a clarifying Step 5 to “Create New User” section.</td>
</tr>
<tr>
<td>4.1</td>
<td>03/13/2024</td>
<td>DVance</td>
<td>Updated language to Step 5 to “Create a New User Section” and added clarifying language for how to End Date a UAA. Added verbiage for downloading a certificate on page 44.</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Navigating to AIM</td>
<td>8</td>
</tr>
<tr>
<td>Acknowledgement Message upon Login</td>
<td>8</td>
</tr>
<tr>
<td>Best Practices</td>
<td>10</td>
</tr>
<tr>
<td>UAA Profile – Landing Page</td>
<td>12</td>
</tr>
<tr>
<td>Create New UAA</td>
<td>13</td>
</tr>
<tr>
<td>How to Create New UAA</td>
<td>13</td>
</tr>
<tr>
<td>How to Add Contract and Authorized Entities to Selected UAA</td>
<td>14</td>
</tr>
<tr>
<td>How to Reactivate Another UAA’s Expired Profile</td>
<td>14</td>
</tr>
<tr>
<td>Create New Users</td>
<td>16</td>
</tr>
<tr>
<td>How to Create New User</td>
<td>16</td>
</tr>
<tr>
<td>How to End Date a User and a UAA</td>
<td>17</td>
</tr>
<tr>
<td>Submit Access Request</td>
<td>18</td>
</tr>
<tr>
<td>How to Submit an Access Request</td>
<td>18</td>
</tr>
<tr>
<td>Access Request Status</td>
<td>24</td>
</tr>
<tr>
<td>How to Submit Endorse User Access</td>
<td>25</td>
</tr>
<tr>
<td>UAA Submits Initial Endorse User Access Request to another UAA</td>
<td>25</td>
</tr>
<tr>
<td>Endorsed User Request Email Notification</td>
<td>28</td>
</tr>
<tr>
<td>UAA to Grant Endorse User Access Request</td>
<td>29</td>
</tr>
<tr>
<td>UnEndorse Users Endorsed to Me</td>
<td>32</td>
</tr>
<tr>
<td>View Endorsed Access Request History</td>
<td>33</td>
</tr>
<tr>
<td>View List of Endorsed Users</td>
<td>34</td>
</tr>
<tr>
<td>Create ACL Groups</td>
<td>36</td>
</tr>
<tr>
<td>How to Create a New ACL Group</td>
<td>36</td>
</tr>
<tr>
<td>How to Modify an ACL Group</td>
<td>39</td>
</tr>
<tr>
<td>How to Add Assets to an ACL Group</td>
<td>40</td>
</tr>
<tr>
<td>How to view an ACL Group</td>
<td>42</td>
</tr>
<tr>
<td>Certificate Process</td>
<td>43</td>
</tr>
<tr>
<td>How to Create or Renew a Certificate</td>
<td>43</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Downloading Email Templates with Attached Certificates</td>
<td>44</td>
</tr>
<tr>
<td>Downloading Only Certificates from AIM</td>
<td>46</td>
</tr>
<tr>
<td>Resending Customer Passwords for Certificates</td>
<td>48</td>
</tr>
<tr>
<td>Certification Status in AIM</td>
<td>49</td>
</tr>
<tr>
<td>How to Let a Certificate Expire</td>
<td>50</td>
</tr>
<tr>
<td>How to Revoke a Certificate</td>
<td>50</td>
</tr>
<tr>
<td>Request History</td>
<td>51</td>
</tr>
<tr>
<td>Check Status of an Access Request</td>
<td>51</td>
</tr>
<tr>
<td>Email Configuration</td>
<td>54</td>
</tr>
<tr>
<td>Features of User Interface</td>
<td>57</td>
</tr>
<tr>
<td>Application Toolbar</td>
<td>57</td>
</tr>
<tr>
<td>Filter Toolbar – User Access Tab</td>
<td>57</td>
</tr>
<tr>
<td>Results Window</td>
<td>58</td>
</tr>
<tr>
<td>Multiple Column Sorting</td>
<td>58</td>
</tr>
<tr>
<td>Export Menu</td>
<td>60</td>
</tr>
</tbody>
</table>
Introduction

The Access and Identity Management (AIM) application was developed to improve the process for requesting, obtaining, updating and maintaining user access to ISO applications.

The ISO maintains approximately 4,000 secured customer accounts granting access to roughly two dozen ISO applications. Each customer has designated one or more individuals within their organization to act as the User Access Administrator (UAA), authorized to initiate and maintain access to ISO applications.

The AIM application provides registered UAAs with the ability to view application-level access for all of their organization’s users as well as any users from other organizations who have access to their resources (endorsed users). Additionally, the AIM application will allow the established UAA to view the expiration date of their users’ certificates and automatically request a renewal from within the application.

If your organization has not established a set of designated UAAs, the following items are required:

1. Have an executed agreement with the ISO.
2. Review the [ISO User Access Administrator Establishment and Requirements](#).
3. Identify the designated UAA(s) and submit a [User Access Administrator Agreement](#) form.

UAA(s) can perform the following tasks in AIM:

- Create another UAA
- Create new users
- Update a user’s contact info (i.e. email address, etc.)
- Update the Weekly Expiry Email notifications of when users’ certificate are going to expire.
- Renew or revoke user’s certificate access
- Add/remove user’s application access
- Submit initial endorse user access
- Provision endorsed user access
- Review access request history
- View a list of Authorized Entities, Authorized Contracts, Associated Applications, Endorsed Users without Access
- Create/Modify/End Date ACL groups

Should you have any questions, please submit an inquiry through the CIDI application / [Contact Us](#) page, or contact your designated Client Representatives.
Navigating to AIM

There are several ways for a user to access the AIM application. Users can navigate to the links below and select AIM.

1. Through the main portal landing page here: https://portal.caiso.com
2. Through the Market Participant Portal here: https://mpp.caiso.com/
3. Through the WEIM portal (access for WEIM entities): https://weim.caiso.com/

Note: A certificate can be obtained by following the instructions for becoming a UAA for your company in the Introduction section of this document or by reaching out to an existing UAA of your organization to create one. Please keep in mind only UAAs will have access to AIM.

Acknowledgement Message upon Login

The acknowledgement MUST be accepted to use the AIM application. The following screen will appear the first time a UAA logs into AIM and again around the beginning of each calendar year:

Dear UAA,

In order to use the AIM application, the UAA must agree to the following terms and conditions:

- All application access requests will be submitted from established UAAs based on their area of responsibility.
- Users requesting access to ISO systems must be authorized by the UAA for the specific applications and permissions being requested based on the user’s role.
- All information submitted by your company in AIM, or on any ISO Application Access Request Form or Device Certificate Request form, will be current and accurate to the best of your company’s knowledge.
- UAAs will immediately revoke a user’s access to ISO applications when such access is no longer required due to the user’s termination or a change in their job responsibilities.
- All transactions occurring under a user’s certificate are the responsibility of that user.
- Sharing certificates among multiple users is not allowed.
- If a UAA or user believes a user’s certificate has been compromised, the UAA will contact the ISO immediately to revoke the certificate.
- UAAs will not provision any user or API access to an ISO production system for non-production purposes.
- All matters concerning the use of this application will be governed by the applicable terms set forth in the company’s existing agreements with the ISO.

☐ Check the box and submit to accept above UAA terms and conditions.

Please contact your client representative at 916-608-7320 with any questions.
After the box is checked and the **Submit** button clicked on, the follow screen will appear:

> Please close this window and reopen the AIM application in a new browser window.

Close the window and reopen the AIM application to begin using AIM.
Best Practices

1. Must review the ISO User Access Administrator Establishment and Requirements.

2. Organizations should establish a primary and secondary UAA for all ISO application access purposes.

3. For larger organizations, multiple UAAs may be required. It is the responsibility of the organization to determine if any of their designated UAAs should have a more limited capacity to provisioning access from other UAAs.

4. When one external entity requests user access to another entity’s data, the requesting entity endorses specified users to the other entity requesting the entity owning the data to provision the access to specified data.

5. It is the responsibility of each entity’s UAA to coordinate and validate the user’s identity and access requirements.

6. When creating a new user, use that new user’s individual email address in the dialogue box.

7. Sharing certificates is not allowable.

8. UAA(s) must validate:
   - User’s job role for requesting access to ISO systems and
   - User must be authorized for the specified applications and permissions being requested.

9. To ensure that user’s expiration certifications are not missed, select ‘YES’ for the Weekly Expiry Email option under the UAA page.

10. Creation of ACL groups can only be done for the following applications: CMRI, MRI-S meter data, webOMS, and ADS.

11. Endorsement of users across ISO applications using the Access Control List (ACL) process must have particular attention to not provision access to unauthorized or users not permitted to have access (i.e. merchant versus regulatory organization) in the AIM tool for the same company.
12. A RIMS application user can only have one role type per environment.

In the event that a user is provisioned dual roles (EXTERNAL IC FOR READ-ONLY and WRITE) within the same environment, an exception rule will be triggered. The error message can be seen at the bottom of the application screen.

Prior to implementing the exception rule flag, users who were provisioned both roles in RIMS were only able to see the projects that were listed under the read-only role when, in fact, they had other projects listed with read-write access.

13. For webOMS, the UAA for non-RC entities can only provision their users the ‘ADJACENT RC’ roles. The users can Read-Write or Read-only but not both as it would be considered conflicting roles. Non-RC entities should not have access to the RC MEMBER role.

14. It is important to note, webOMS must be provisioned separately from all other applications in a New Access Request.

15. For Access Request and Endorsed Access Requests, it is important that the Request ID has a blue background. If the background is white, the UAA needs to click on the Request ID number.
**UAA Profile – Landing Page**

The **UAA Profile** Tab displays contact information for an individual UAA.
Create New UAA

The **UAA**s Tab provides the ability to Create New UAA Profiles, Add Contracts to Selected UAA, and Add Entity to Selected UAA.

**How to Create New UAA**

1. To add a new UAA, navigate to the **UAA**s tab and click the **Create New UAA Profile** Button.

2. Select a **User**.
3. Select an **Environment**, **Start Date**, **End Date**, and then click **Submit**.

The new UAA will be able to access AIM as a UAA after about 30 minutes.
How to Add Contract and Authorized Entities to Selected UAA

1. To add a contract to a selected UAA, navigate to the **UAAs** tab and go to the **UAA Authorized Contracts** section.
2. Select the Provisionable Contract to be added.
3. Click the **Add Contracts to Selected UAA** button.
4. Select the Provisionable Entities to be added.
5. Click the **Add Entity to Selected UAA** button.

How to Reactivate Another UAA’s Expired Profile

When a UAA’s profile has expired, utilize the steps outlined below to reactivate and/or extend the date for another UAA’s profile.

1. After logging into AIM, navigate to the UAA’s tab.
2. After identifying the UAA with the inactive profile status, click the share icon under the Profile Column.

3. After clicking on the Profile Column, a pop-up window will open. Under the UAA Profile box, click on the pencil icon.

4. Extend the date as deemed appropriate and select update to save changes.
Create New Users

The **Users** tab provides the ability to view a list of users. The UAA will access this screen to create a new user.

The user list separates into three sections: **My Users** (users who belong to the UAA’s organization), **Users Endorsed to Us**, and **Users Endorsed by Us** (users from another organization granted/requested access to specific Entities, usually an SCID, or resources in specific applications).

**How to Create New User**

1. To add a new user, navigate to the **Users** tab and click the **Create New User** button.
2. Enter the user’s first name, last name, individual’s email address, and address information.
3. Select an account type of Externals for an individual person or Externals_System for system accounts.
4. Click **Submit**.
5. Newly Generated certificates will only be available to be downloaded by the UAA and emailed to the user for 5 days under the “Manager Certificates” tab. For instructions, please go to page 44 of the User Guide, “Downloading Email Templates with Attached Certificates.” This step is required before submitting an Access Request (instructions on page 18).

**Note:** Access Requests will be rejected for a new user certificate if a UAA has not downloaded and emailed the certificate to the user. For the status of a certificate, please see the “Cert Status” column on the “My Recently Renewed Certificates” section of the Manage Certificates Tab. For an explanation of a certificate status, see page 49 of the User Guide, “Certificate Status in AIM.”
How to End Date a User and a UAA

1. To end date a User, navigate to the User tab.
2. Under the My Users section, select the user that is being end dated.
3. Click the user’s profile button to initiate a new pop-out window.

4. To end date a UAA, navigate to the UAA tab and follow the same process below by clicking the UAA’s profile button to initiate a new pop-out window.

5. Navigate to the UAA Profile section and select the pencil icon.
6. From there, go to the End Date section and put the desired date – click Update when complete.
HINT: To quickly remove UAA privileges, change the End Date to yesterday’s date.

REMINDER: Once a UAA profile has been end dated, the authorized contracts and entities will need to be wiped out. To perform this task, highlight each contract and entity and click “X”.

Submit Access Request

The UAA will use the **Access Request** screen to submit new application Access Requests as well as view the status of submitted requests. Access requests will be rejected for new certificates if a UAA has not first downloaded and emailed the new certificate to the new user.

**How to Submit an Access Request**

1. Navigate to the **Access Request** tab.
2. Click the pencil icon to add a new request.
3. Click the **New Row** button.

![New Row button](image)

4. Type a description for the request and click the **Update** button.

![Update button](image)
5. From the **Select Users** tab, choose the names from the list of **Available Users**. (Note: Use “Ctrl + click” or “Shift + click” to select multiple names).

![Access and Identity Management User Guide](image)

**HINT**: If the middle buttons (Add All, Add, Remove, and Remove All) are not visible, please click on the UAA Profile tab, then the Access Request tab, and then the Request ID number. The buttons should reappear.

6. Click on the **Select Applications and Roles** tab.

7. Click on the desired application and role and click the Add button. (Note: Use “Ctrl + click” or “Shift + click” to select multiple applications).

8. (Optional) To remove access, click on the drop-down button in the **Action** column to change the selection from ADD to REMOVE.
9. (Optional – **Copy Current User Access** tab).
   a. To view the access of a specific user in order to grant the same access to
      a new user, click the **Copy Current User Access** tab.
   b. Click a name in the **Current Users** panel to view that user's access in the
      **Current User Access** panel.
   c. Click on the desired application/role/environment and click the **Add** button.
      (Note: Use “**Ctrl + click**” or “**Shift + click**” to select multiple
      application/role/environment options).

**HINT:** The normal provision for users is either PRODUCTION or MAP STAGE. The
STAGE environment is rarely used.
10. After all users, applications, roles, and environments are selected, click the **Update** button in the **Access Request** panel.
11. Review the request to ensure that it is accurate.

Click the **Submit** button in the **Access Request Preview** window to submit the request. (Note: If changes need to be made, close the preview window and edit the request as needed. Click the **Preview** button again and then click the **Submit** button.)
After reviewing the request, click the **Submit** button to complete the request.
Access Request Status

To check on the status of the application request, go to Access Request >> Request History

You can filter by the Request ID or any of the available options.

Provisioning access in AIM can take up to 24-48 hours to complete.
- If a certificate is new, and has not been downloaded by a UAA and emailed to the user, the Access Request will be rejected. Please follow up with the user to ensure they download and install their new certificate.

When requesting for MRI-S access, it may take a little longer as it requires additional validation.

- When provisioning access for MRI-S, you will noticed that under the Access Request History section, the Status will be shown as “PROCESSED”.

- Under the Access Request Details section, the Status will be updated to “ON_HOLD” and the Notes column will indicate that it is “On hold for CAISO approval”.

- Once the review process is complete, the Status will be updated to either “COMPLETED” or “REJECTED”. This additional validation is a prerequisite for the tariff compliance requirement when provisioning for meter data roles.
How to Submit Endorse User Access

UAA Submits Initial Endorse User Access Request to another UAA

Step 1: Click on Endorse/UnEndorse My Users sub tab under the Endorsed Access Request tab.

Step 2: Select applicable user(s) from Available Users box. Then, click on the Add button to move applicable user(s) to the Selected Users box to the right. (Note: Use “Ctrl + click” or “Shift + click” to select multiple names).

Step 3: From the drop down box on the right side of Select an Organization, please select the organization that you would like the user to have access.

Step 4: Enter a brief description of your request. This description will be viewed by the granting UAA. Note: Please do not include any special characters in the description field. Otherwise, the Endorse Selected Users button will not work.

Step 5: Click the Endorse Selected Users button. See screen shot:
Endorsed/UnEndorse My Users – The top section of this display (Endorse My Users) shows a list of my users that are available to be Endorsed by other organizations. The bottom section of this display (UnEndorse My Users) shows a list of my users that are already Endorsed Users to other organizations and are ready to be UnEndorsed. Both of these sections are based on My Users. The top section is My Users to be Endorsed and the bottom section is My Users to be UnEndorsed.

- Remember that the act of endorsing is done at the certificate level – once a certificate is endorsed to another company, the Endorsed UAA and the Endorser UAA can manage the request to add additional access outside of AIM, although the access itself is provisioned via AIM by the Endorser UAA.
- If a certificate is already endorsed, the UAA will get an error in AIM.
- The Endorser UAA will see in the main UAA Profile tab that they have requests waiting.
**Note:** AIM will send out a generated email notification to both the organization’s UAA when endorsed user application request(s) are rejected by the ISO.

Example:

```
Dear User Access Administrator,

You have submitted the following access request on 09/12/2018:

<table>
<thead>
<tr>
<th>Name</th>
<th>User ID</th>
<th>Action</th>
<th>Environment</th>
<th>Application</th>
<th>Role</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMSTester05</td>
<td>OTESTER05x812</td>
<td>ADD</td>
<td>MAP-TEST</td>
<td>ADS</td>
<td>EXTERNAL READ-ONLY</td>
<td>PCG2</td>
</tr>
</tbody>
</table>

The request has been rejected by Caiso personel with reason: Tester05 can not have PCG2 access. Please call CAISO on 10/02/2018.

Please log into AIM via the ISO portal [https://portal.caiso.com/aim](https://portal.caiso.com/aim) to check the status of this request.

If you have any issues, please contact our support desk at HelpDesk@caiso.com or (888) 889-0450.

Regards,

CAISO Identity Management Operations
```
Endorsed User Request Email Notification

The UAA shall receive a generated email notification when users are endorsed to their organization for application access. The email will contain the name of the company that is submitting the endorsed user request.

Example:

Dear User Access Administrator,

Please note that the following users are being endorsed to your organization from ABC Energy, LLC.

ADS Tester 14 (xatester14122375)

Regards,
CAISO Identity Management Operations
UAA to Grant Endorse User Access Request

When a UAA logs into AIM, they will see the landing page. On this page, the UAA will see a list in the **Endorsed Users without Access** box. These are users from other organizations waiting for approval. This is the initial notice to the UAA to go to the **Endorsed Access Request** tab for approval/disapproval of their access request. The screenshot below captures the landing page with the **Endorsed Users without Access** notification box.
Step 1: The granting UAA will go to the Add/Remove Endorsed User Access sub-tab under the Endorsed Access Request tab. Please see previous screen shot.

Step 2: The granting UAA will click on the pencil icon to add a new request.
- Click on the New Row button.
- Type a description for the request and click the Update button.
- From the Select Endorsed Users tab, choose the names from the list of Available Users Endorsed to Me. (Note: User “Ctrl + click” or “Shift + click” to select multiple names).
- Click on the Select Applications and Roles tab.
- Click on the desired application and role and click the Add button. (Note: Use “Ctrl + click” or “Shift + click” to select multiple applications).
- (Optional) To remove access, click on the drop-down button in the Action column to change the selection from ADD to REMOVE.
- (Optional – Copy Current User Access tab).
  - To view the access of a specific user in order to grant the same access to a new user, click the Copy Current User Access tab.
  - Click a name in the Current Users panel to view that user’s access in the Current User Access panel.
  - Click on the desired application/role/environment and click the Add button. (Note: Use “Ctrl + click” or “Shift + click” to select multiple application/role/environment options).
- After all users, applications, roles, and environments are selected, click the Update button in the Access Request panel.
- Review the request to ensure that it is accurate.
- Click the Submit button in the Access Request Preview window to submit the request. (Note: If changes need to be made, close the preview window and edit the request as needed. Click the Preview button again and then click the Submit button.) Please see below screen shot:
Confirm Endorsement for Selected Users

Before the UAA(s) can complete the submission request for endorsing ISO application access to user(s) outside of their organization, the UAA must check the ‘The information contained herein is Confidential and subject to the FERC Standards of Conduct’ acknowledgement box in the AIM application.
UnEndorse Users Endorsed to Me

Step 1: Click on the Endorsed Access Request tab.

Step 2: Click on the UnEndorse Users Endorsed to Me sub-tab.

Step 3: From the list of users in the User Endorsed to Me box, select the applicable user.

Step 4: Click the Add button. This will move the selected user from left box to the right box Selected Users For UnEndorse.

Step 5: Click on the Un Endorse Selected Users button on the bottom of the left box. This will UnEndorse the selected user.

UnEndorse Users Endorsed to Me – This tab provide a list of Users Endorsed to Me (not my users) ready to be UnEndorsed. Unlike the previous screen, these users are not my users. These users are from other organizations, which have access to my data. The primary objective of this screen is to remove data access from Endorsed users to my organization.
View Endorsed Access Request History

Step 1: Click on the Endorsed Access Request tab.

Step 2: Click on the Endorsed Access Request History sub-tab.

Step 3: The Access Request History shows you a list of your recent access requests.

Step 4: When you select a record from Access Request History, all of the details of your request will be displayed on the Access Request Details panel.

Step 5: If you already know the request ID, you can simply place that ID in the Request ID field above Access Request History and then click the Apply button.

Endorsed Access Request History: This tab provides you with list of your recent Endorsed access requests. The top box shows you the history of your requests and the bottom box provides you with the details of the selected access request.
View List of Endorsed Users

There is a new sub tab under the Users tab called Users Endorsed to Us. This new tab provides a list of all Endorsed Users to your organization.

- **My Users** contains list of users belonging to my organization.
- **Users Endorsed to Us** contains a list of Endorsed Users to my organization (These users are not my employees, but they have access to my data).
Step 1: Click on the Users tab.

Step 2: Click on Users Endorsed to Us.

Step 3: Please allow time for users from other organizations to show up under Users Endorsed to Us. This is just a view display.

QUICK REFERENCE GUIDE TO ENDORSED ACCESS REQUEST SUB TABS

- **Endorse/UnEndorse My Users**: This sub tab is for REQUESTING UAA only. The users reflected under this sub tab belong to your organization.

- **UnEndorse Users Endorsed to Me**: This sub tab is for GRANTING UAA only. The users reflected under this sub tab do NOT belong to your organization.

- **Add/Remove Endorsed User Access**: This sub tab is for GRANTING UAA only. The users reflected under this sub tab do NOT belong to your organization.

- **Endorsed Access Request History**: This sub tab is for GRANTING UAA only. The users reflected under this sub tab do NOT belong to your organization.
Create ACL Groups

An Access Control List (ACL) defines the access rights each user has to particular assets. The ACL Groups screen provides the UAA with the ability to create new ACL groups to isolate and grant access to a single asset (or group of assets).

How to Create a New ACL Group

1. Click the ACL Groups tab
2. Click the Create ACL Group button to create an ACL group
3. Select the Environment and enter a Description for the ACL group.
4. Select a Start Date and an End Date for the ACL group and click the Submit button. Please note that the “Start Date” can be set to a past date.
Start Date may be set to a past date

Click Submit when finished
• Once an ACL Group is created, the effective date can be end-dated but **not** extended. The ACL users will still be able to view the data beginning from the 'Start Date' to the designated 'End Date'.

• ACL Group Start and End dates are unchangeable once created.

• The ACL Group cannot be deleted from AIM once created, but may be made non-provisionable by the UAA. This means that the UAA will not be able to provision new users to the non-provisionable ACL Group in AIM; however, the existing users will still have access to the data.

• The UAA can add new resources to the ACL Group, but cannot remove existing Resource IDs from the list.

• Once the ACL end date expires, the existing users can no longer see data for the trade dates after the end date, but those users will continue to have access to the data prior to the end date.

• The ISO **does not** send out a notification reminder to the UAA when the ACL Group end dates. It is the responsibility of the UAA to re-create a new ACL group and provision ACL users.

• The naming format for the ACL Groups will be 'EXC_[SCID]_[Autonum]'.
How to Modify an ACL Group

1. Select the ACL Group name then click on the pencil icon.

2. Now you can change Description and Status fields of the ACL Group. You can select “Provisionable” or “Non-Provisionable” from the drop down box in the Status Field. Provisionable means that you can provision this ACL Group to users. Non-Provisionable mean you cannot provision users to this ACL Group.
How to Add Assets to an ACL Group

1. Click the **Edit** button to add assets to the ACL group.

First select the ACL Group; then click on "Edit" to add resources.
2. Select an asset from the **Available Assets** list and click the **Add** button to add an asset to the ACL group.

3. Once you have selected applicable resources, click on the **Submit** button to **PERMANENTLY** add resources to the ACL Group or click the **Cancel** button to negate adding the selected resources to the ACL Group.

4. You cannot remove a resource from the ACL Group once assigned. The UAA will need to create a new ACL Group for the desired resource.
How to view an ACL Group

Click on an entry in the **ACL Groups** section to view the list of assets associated with that group.
Certificate Process

How to Create or Renew a Certificate

1. To create a new user, please follow directions for the section “How to Create New User” above.
2. To renew a certificate, navigate to the Manage Certificates tab. Click the box next to the user(s) and click the Generate Certificate button.

3. Once you have created the new user (or renewed the certificate of a current user) navigate to the Manage Certificates tab.
4. Click on the **Recently Renewed Certificates** link.

   ![Image of Recently Renewed Certificates](image1.png)

5. Navigate to the newly created (or renewed) user. The certificate download icons will now show next to the user’s name. **Certificate will only be available to download for 5 days.** If not downloaded within those 5 days, the UAA will need to generate a new certificate.

   ![Image of Certificate Download Icons](image2.png)

**Downloading Email Templates with Attached Certificates**

1. Click the icon on the **Download Email with Certificate Attached** column next to the selected user’s name.

   ![Image of Email Templates with Attached Certificates](image3.png)
2. An email will be created using the associated default email program with certificate attached.

3. Open the email template and verify that the user’s email address is correct and that the certificate bundle has been attached. Send the email and inform the user to download the certificate.

**Note:** Ensure that your organization whitelists are able to download from the website “aim.caiso.com”. Additionally, whitelist emails from the domain “caiso.com”, so users can receive their password emails. Notify users that the emails will be coming from “caiso.com” (If they typically do not receive emails from CAISO, it may have gone into their spam folder).”
Downloading Only Certificates from AIM

1. Click the icon on the Download Certificate Only column next to the selected user’s name.

2. The certificate “bundle” (zip file) will be downloaded to your computer and can be found in your browser’s **Recent Downloads** folder.
3. On the **Managing Certificates** tab, click on the **UAA Click Here** link at the top of the screen. This will provide you with scripting to add to the email you will send the user.

4. Copy the wording from the popup.

5. Paste the wording from the pop-up into an email (using your default email application) and attach the certificate bundle.

**Note:** When a certificate downloads, it is in a .p12 extension. Your organization will need to allow email attachments with .p12 extensions. If this is not possible, a new
method will be needed to share the certificates with the users. Some email systems may have issues sending these types of attachments (ex. Mozilla Thunderbird).

**Resending Customer Passwords for Certificates**

1. Navigate to the **Managing Certificates** tab and ensure that the customer’s email address is correct.

2. Ensure that you have downloaded the certificate and send it to the user.

3. Click on the icon in the **Resend Password** column.
4. By design, password emails will not be sent until approximately 5 minutes after certificates have been downloaded. If the user still has not received the email, please call the Service Desk for assistance.

Dear User “SALLY SMITHx30215”,

The password below is required to install your California ISO CMA Certificate. The certificate will be provided to you by a User Access Administrator from within your organization.

Password: 7d6MDtTnPV

* If you cut and paste this password it will likely insert a space at the end and show as invalid when trying to submit, please check and remove the space if it is present.

For instructions on how to install your certificate, visit: [https://www.caiso.com/informed/Pages/Notifications/Default.aspx](https://www.caiso.com/informed/Pages/Notifications/Default.aspx).

If you have any further questions, contact our support desk at ServiceDesk@caiso.com or (888) 889-0450.

For more information related to the Applications Access Request process, visit the ISO System Access and California ISO Applications documentation posted on our California ISO website at: [http://www.caiso.com/participate/Pages/ApplicationAccess/Default.aspx](http://www.caiso.com/participate/Pages/ApplicationAccess/Default.aspx)

By requesting access to ISO applications or tools, you may occasionally receive emails specific to that tool, such as notifications, outages or reminders.

Regards,

CAISO Identity Management Operations

CertificateRequests@caiso.com

---

**Certification Status in AIM**

<table>
<thead>
<tr>
<th>Cert Status</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>AIM has just started processing the certificate.</td>
</tr>
<tr>
<td>Getting Ready To Email Password</td>
<td>The certificate has been downloaded and AIM is about to send the password to the user.</td>
</tr>
<tr>
<td>Certificate Available for Download</td>
<td>The certificate has been created and is ready to be downloaded by the UAA.</td>
</tr>
<tr>
<td>UAA Did Not Collect Certificate</td>
<td>After the certificate was ready to be downloaded, the UAA did not download it. <strong>Note: CAISO only keeps the certificate for 5 days. After 5 days we remove the certificate information and you will have to create a new certificate request.</strong></td>
</tr>
<tr>
<td>Completed</td>
<td>The certificate process has completed.</td>
</tr>
</tbody>
</table>
How to Let a Certificate Expire

1. To let a certificate expire, navigate to the Manage Certificates tab.
2. The Manage Certificates tab will display the My Users With Expiring Certificates list. This list will show all users whose certificates are expiring within 90 days or less. (Note: If the certificate expiration date is further into the future, the user will not appear on this list.)
3. Click the Let Expire button on an individual line item. Another option is to use the “Shift + click” or “Ctrl + click” functionality to select multiple users simultaneously. After selecting multiple users, click the Let Selections Expire button to apply it to all items selected.

How to Revoke a Certificate

1. To revoke a user’s certificate, navigate to the User tab.
2. Find the correct user and click on the button in the Profile column.
3. From the User Profile screen, click the Revoke User button.
4. A confirmation message will appear that states: “Are you sure you want to revoke the user certificate and remove all application access for this user? This action cannot be undone.”
5. Click OK to revoke the user’s certificate.
6. Once the OK button is clicked, the certificate will be revoked and all application access will be removed. This change will be reflected in AIM after the next data sync period (usually within 12 – 24 hours). Note: If a user’s certificate is revoked by mistake, the UAA should contact the Service Desk and ask them to re-activate the certificate by being sent a new certificate registration email that will then allow the UAA to add access back.
Request History

Check Status of an Access Request

1. To check the status of an access request, navigate to the Access Request tab and click on the Request History link.
2. Click on an individual line item in the Access Request panel.
3. The list of items requested will display in the Access Request Details panel.
4. Review the Status column for each line item to verify that the requested access was granted.
   a. Submitted: The access request has been submitted and is waiting for the approval process to run.
   b. Approved: The access request has been approved and is waiting to be processed.
   c. Processing: The access request is being processed.
   d. Completed: The access request has been completed and the user can now access the application.
   e. Rejected: The access request has been rejected and will not be processed. See the notes column for the reason it was rejected.
Click on an individual access request in the Access Request panel to show the Access Request Details at the bottom of the screen.
**Note:** An Access Request will begin with a status of “Submitted”. It will then move to “Processing”. Finally, it will have a status of “Processed”. This does not mean that all access was granted. The UAA must review each of the line items in the Access Request Details to verify that access was granted to a specific user.

In the Access Request Details section, the status options are Submitted, Approved, Processing, Completed, and Rejected.
Email Configuration

Email Configuration tab is a new enhancement, which provides a UAA the ability to add additional email recipients on 7 different AIM automated notifications. Below is a list of these automated notifications:

- Application Access Request
- Certificate Renewal from UI
- Renew User Certificate from UI
- Revoke User Certificate from UI
- Submit a New User from UI
- Notification for certificates expiring within 30 days, 60 days, 90 days and new users
- User Revocation Email

Steps to add additional emails:

1. Please click on the Email Configuration tab per screen shot below

![Email Configuration tab](image)

1. Select applicable Certificate Events. Example in screen shot below is “Application Access Request”
2. Click on the pencil icon under the **Email List semicolon separated** panel in the screen shot below:

![Email Notification Events](image)

3. Click the **New Row** button under the **Email List semicolon separated** box in the screen shot below:

![Email Notification Events](image)

4. A free text field will be activated. Please list applicable email recipients separated by semicolon in this field.

5. When your list is finalized, please click on the **Update** button under the **Email List semicolon separated** panel.
6. If you need to delete an email address, select that email address and click on the **Update** button. Select the entire email address and click the Delete button **on your keyboard**. It will look like the screen shot below. Then, simply click on the **Update** button. This will remove that email address.
Features of User Interface

Application Toolbar

The application toolbar contains the application or browser-based functions.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>←</td>
<td>Goes to the previous display in browsing history</td>
</tr>
<tr>
<td>→</td>
<td>Goes to the next display in browsing history</td>
</tr>
<tr>
<td>⏹️</td>
<td>Stops loading the current display</td>
</tr>
<tr>
<td>⚪</td>
<td>Refreshes the display in the current window</td>
</tr>
<tr>
<td>📐</td>
<td>Zoom out</td>
</tr>
<tr>
<td>🕵️</td>
<td>Zoom in</td>
</tr>
<tr>
<td>🛡️</td>
<td>Log out</td>
</tr>
</tbody>
</table>

Filter Toolbar – User Access Tab

The filter toolbar contains the account filtering options.

<table>
<thead>
<tr>
<th>User ID</th>
<th>First Name</th>
<th>Email</th>
<th>Certificate Expiration</th>
<th>Status</th>
<th>Account Type</th>
<th>Apply</th>
<th>Reset</th>
</tr>
</thead>
</table>

- Apply: Refreshes user data with the filters
- Reset: Restores filters to default settings
- * wildcard search: Use the asterisk (*) wildcard symbol to search for user information. (e.g. Enter Chris* in the First Name field and click the Apply button to display a list of users whose first names begin with “Chris”. The search results will display users who are named Chris, Christopher, Christine, etc.) To ensure that you see all records meeting your search criteria, add the “*” at the end to display multiple records.
Results Window

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restore sort to default setting (removes user-created multiple column sorting, which is described in detail on the following page)</td>
</tr>
<tr>
<td></td>
<td>The Inline Filter works as a toggle. Click the icon to filter data based on the content of a particular column. Press Enter after entering the filter criteria. (Note: Wildcard symbols can be used in this column, but they are not necessary. For example, searching for <em>UAA</em> or UAA will provide the same results.)</td>
</tr>
<tr>
<td></td>
<td>Exporting (to Excel, Word, CSV)</td>
</tr>
</tbody>
</table>

Results Window – Multiple Pages

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Navigate to the first page of data</td>
</tr>
<tr>
<td></td>
<td>Navigate to the previous page of data</td>
</tr>
<tr>
<td></td>
<td>Navigate to the next page of data</td>
</tr>
<tr>
<td></td>
<td>Navigate to the last page of data</td>
</tr>
<tr>
<td></td>
<td>Go to specific line item entered in search box</td>
</tr>
</tbody>
</table>

Multiple Column Sorting

Clicking on a column in the results window enables the user to sort the data in ascending or descending order.

Here is an example of how to use multiple sorting:

- Click a column header. The data is sorted in ascending order and the following icon appears in the column header: . This indicates the first level sorting.

- Click another column. The data is sorted in ascending order. The icon in the first column changes to: . The following icon appears in the second column: . This indicates the second level sorting.

- Click another column. The data is sorted in ascending order and the following icon appears in the column header: .
- Click the same column again. The data is sorted in descending order. The icon in the column header is changed to:

- Continue to click column headers to deselect and then reprioritize the sorting order.

The following image shows the example explained above:
Export Menu

<table>
<thead>
<tr>
<th>Export Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export All</td>
<td>All data points will be exported to Excel</td>
</tr>
<tr>
<td>Export Page</td>
<td>The current page will be exported to Excel</td>
</tr>
<tr>
<td>Export Wizard</td>
<td>The user can customize the data export</td>
</tr>
</tbody>
</table>

Export Wizard

The Export Wizard enables the user to export data in the following three file types:
- Export Excel
- Export CSV
- Export Word

The Export Wizard can be customized using the following options:
- Enable Grid Export: If a display contains multiple grids, the user can select specific grids to export. (Note that the CSV format can only export one grid).
- Display Name: The user can modify the name of a column that will appear in the data export.
- Enable/Disable Column Visibility: The user can select which columns to include in the exported file.
- Custom Column Width: The user can choose to modify the width of a specific column.
- Rows to Export: All Rows, or the Original Page.
Once the user has selected the export parameters, click the **Export** button to generate a file.

**Note:** The maximum number of rows that can be exported is 10,000. If the number of rows available exceeds 10,000, only the first 10,000 rows will be exported. It is recommended to use filters to limit the number of results that are displayed in order to export all rows.