AIM New Certificate Process for UAAs

Rashele Wiltzius
October 3, 2023

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.
Make sure to keep yourself muted unless you have a question

If you have a question, you may either ask over the phone or in the chat

If you want to ask a question, you can virtually “raise your hand” in WebEx
Agenda

_In this training, we will:_

- Learn the differences between the old/current certificate creation and renewal process and the new certificate creation and renewal process
- Look at and discuss an overview of the changes in AIM
- Walk through the new certificate creation and renewal process (demo)
- Discuss next steps
Current Certificate Process

**UAA**
- Add User

**CAISO**
- Send certificate request to user

**End User**
- Key in information and passcode

**CAISO**
- Verify data and approve (3-10 days)

**End User**
- Retrieve cert with passcode and install root + cert (in correct order)
New Certificate Process

UAA downloads certificate from AIM and emails to end user.

End User

UAA

Add User

Download cert “bundle”

Email Cert passcode

Store cert public key

**Note:** Cert “bundle” includes both root and certificate
Reminder

- Remember to “de-duplicate” your user email addresses for best performance!
- Instructions on this process can be found [here](#).

Note: For certificates for access to confidential data covered by NDAs, it is important that end users use the email address they provided in their Exhibit A to the NDA their company submitted.
Note: if in incognito or private modes are used when downloading certificate as an attachment, it will force you to “Save As”. Otherwise, this behavior does not happen in Chrome or Edge.
NEW AIM Certificate Tab

The image shows a screen from the California ISO Access and Identity Management (AIM) system. The screen is titled "My Users Expiring Certificates" and includes a table listing users with expiring certificates. The table columns include Last Name, First Name, Emp No, Email, Cert Expiration Date, Cert Expiry Status, Cert Status, PROFILE, and ACCESS.

Some rows from the table are highlighted to indicate the options available for managing certificates. The options include selecting all users, generating certificates, and setting certificates to expire.
Creating a New User

To start the certificate creation process for a new user, create a new user in AIM on the Users tab (no changes).
New Process to Renew or Expire Certificates

To renew a user’s certificate, click the box next to the name(s) and click the **Generate Certificate** button.
New Screen to Create and Renew Certs

To create a new certificate, click on the Recently Renewed Certificates link.
Questions
## Cert Statuses 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. <em>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.</em></td>
</tr>
<tr>
<td>Completed</td>
<td>The certificate process has completed.</td>
</tr>
<tr>
<td>Something Went Wrong – Certificate</td>
<td>There was failure while trying to process the certificate. If this status has not change after approximately 2 hours, contact customer support.</td>
</tr>
<tr>
<td>Invalid Cert Request</td>
<td>The certificate request was deemed to be invalid. This is a very rare occurrence. Please contact customer support to determine why this occurred.</td>
</tr>
<tr>
<td>Password Emailed to User</td>
<td>The password has been emailed to the user.</td>
</tr>
<tr>
<td>Processing Before Provider</td>
<td>CAISO is processing the certificate request.</td>
</tr>
<tr>
<td>Processing At Provider</td>
<td>The certificate is being processed by the certificate provider.</td>
</tr>
</tbody>
</table>
Certificate Instructions

Certificate instructions on email have been updated to reflect the new process.

Dear User “S2 2x30026”,

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 : S$3kw@EHT


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

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

Regards,
CAISO Identity Management Operations
CertificateRequests@caiso.com
Certificate Error

If:

• Your user has never had a previous CAISO certificate

• You are still using the old AIM URL (pre-F5 project)
Other Errors

• Make sure your organization whitelists downloads from the website “aim.caiso.com”
• White list 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 go into their spam folder.
Other Errors

- When downloaded, the certificates are in a .p12 extension.
- Your organization will need to allow internal email attachments with .p12 extensions.
  - Some organizations may restrict this type of attachment.
  - If this is not possible, you will need another method to share the certificates with the users.
- Some email systems may have issues sending these type of attachments (ex: Mozilla Thunderbird)
What You Need to Do

• Your AIM profile has been automatically updated with the new functionality.

• When you are ready to create or renew a certificate in AIM, use the quick reference guide located on the caiso.com learning center [here](#).
  – The job aid has also been added to the “Application access” webpage on caiso.com
  – AIM user guide has been updated

• Report any issues with the new process via CIDI ticket if you encounter them!
Thank you for your participation!

For clarification on anything presented in this training, send an email to: CustomerReadiness@caiso.com

For any other questions or stakeholder specific questions or concerns, please submit a ticket.

CustomerReadiness@caiso.com

www.caiso.com