New AIM Certificate Process
Job Aid
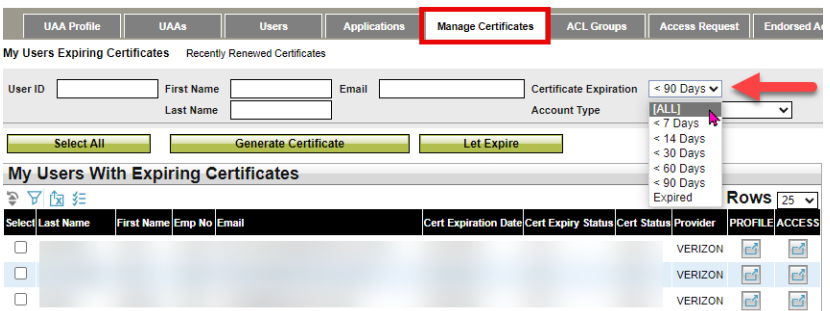
Please contact us at UAARequests@caiso.com if you have any issues or questions.
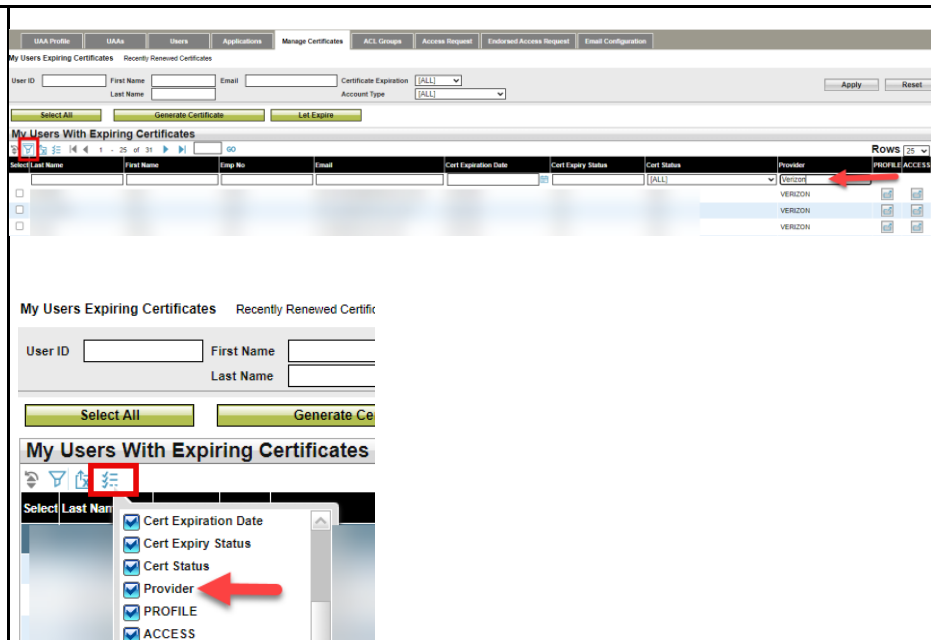
Table of Contents

Replacing a Verizon Certificate with an Entrust Certificate

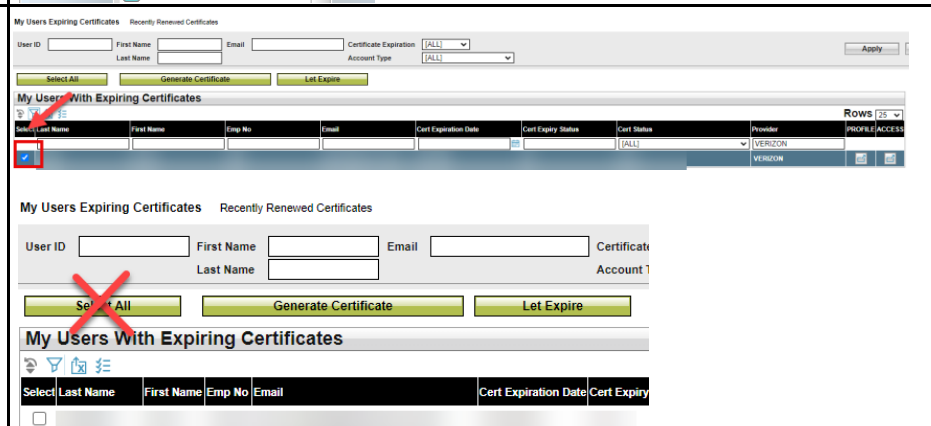|	
Navigate to the **Manage Certificates** tab and change the **Certificate Expiration** to filter for [ALL].	

| After filtering for [ALL], navigate to the filter icon on the table. In the **Provider** column, type **Verizon** and hit enter to filter.

Note: If the Provider column is not showing, please add this column by selecting the Adjust columns button. | |
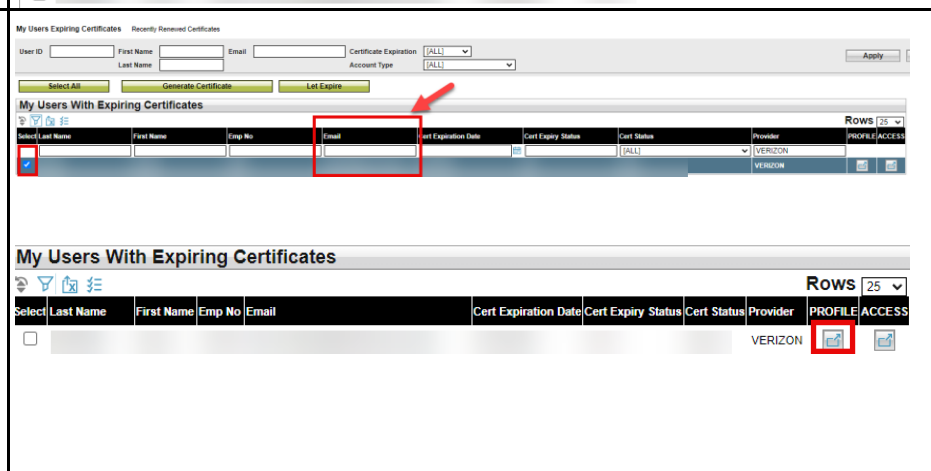| Now that only Verizon certificates are filtered, <u>**select one**</u> of the certificates.
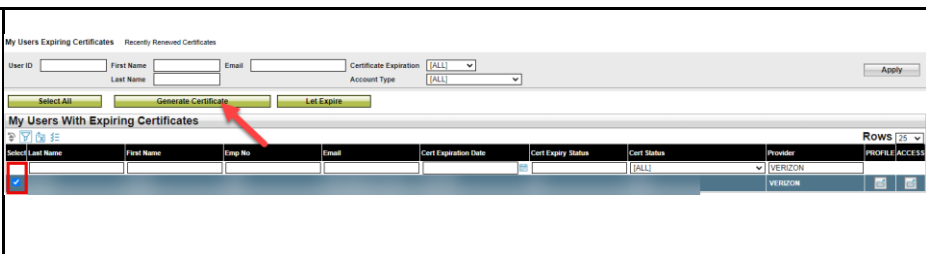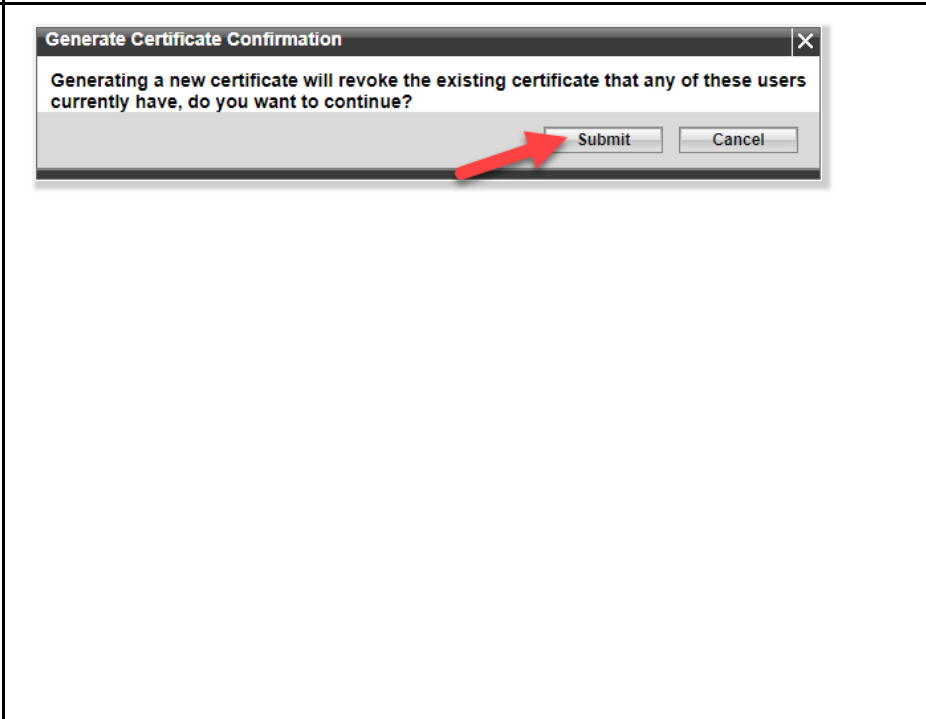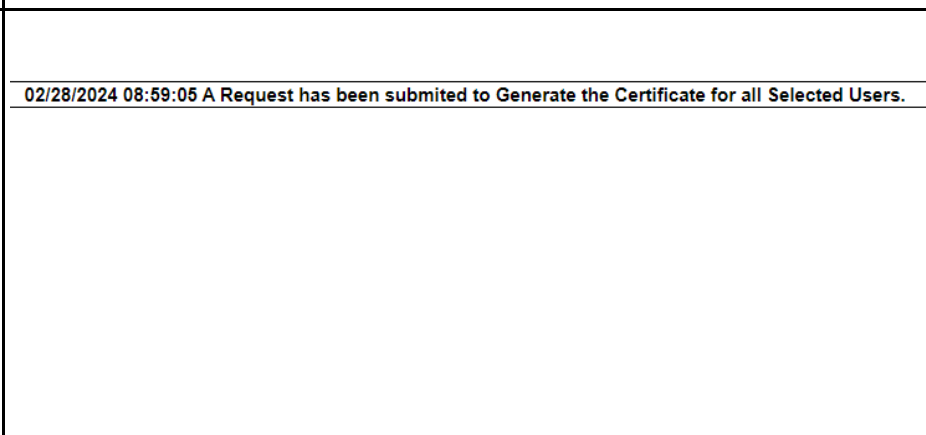
IMPORTANT TO NOTE: Do not hit the Select All feature. If you do, the system will select Entrust certificates as well. | |
| Please verify that the email address listed for the user is correct.

If the email is **NOT** correct, the UAA will need to edit the email address associated with the certificate by clicking the user's **Profile** button and updating. | |
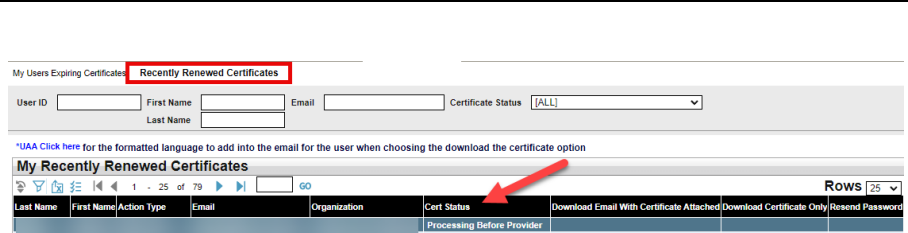
Once the email is confirmed, click **Generate Certificate**.	
Clicking **Generate Certificate** will prompt a pop-up box if the certificate is 90 days or more from expiration warning that the older certificate will be revoked. This **WILL NOT** be the case for **Verizon** Certificates. For the purpose of replacing a Verizon Certificate to an Entrust Certificate, please disregard the pop-up by selecting **Submit**.	**Generate Certificate Confirmation** ✕ Generating a new certificate will revoke the existing certificate that any of these users currently have, do you want to continue? Submit Cancel
At the bottom of the screen, users will see a text box indicating the request was submitted *Note: Older Verizon certificates will remain available alongside newer Entrust certificates for roughly 14 days.*	02/28/2024 08:59:05 A Request has been submitted to Generate the Certificate for all Selected Users.

It will take 5-10 minutes for certificates to generate. Navigate to the **Recently Renewed Certificates** tab. There, users will see the status of the new certificate that was generated.

Details on **Certification Statuses** column can be located on the last page.

It will take 3-5 minutes for the certificate download icon to show.

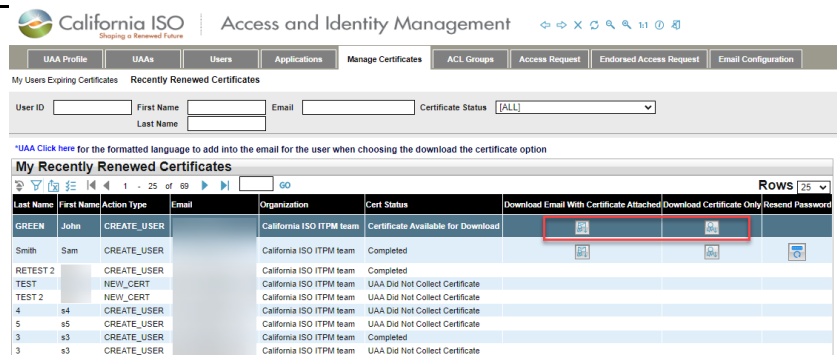If the certificate download icon is not showing, refer to the **Certification Status** column for the explanation.

The 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.

Please proceed to the downloading certificates portions of this Job Aid (page 7 and 8).

Create or Renew an Entrust Certificate

Create new user via the **Users** tab. OR Renew a current user's certificate on the **Manage Certificates** tab. Click the box next to the user(s) and click the **Generate Certificate** button.	To create a new user: To renew a certificate for a current user:
Once you have created the new user (or renewed the certificate of a current user), navigate to the **Manage Certificates** tab.	
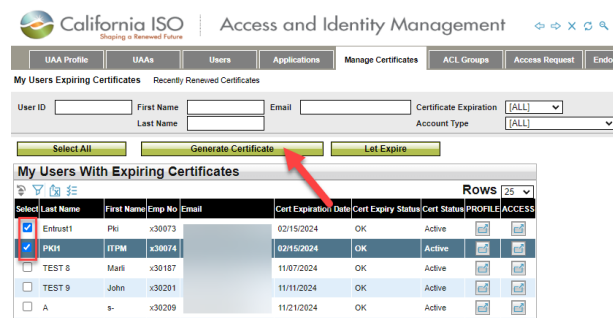
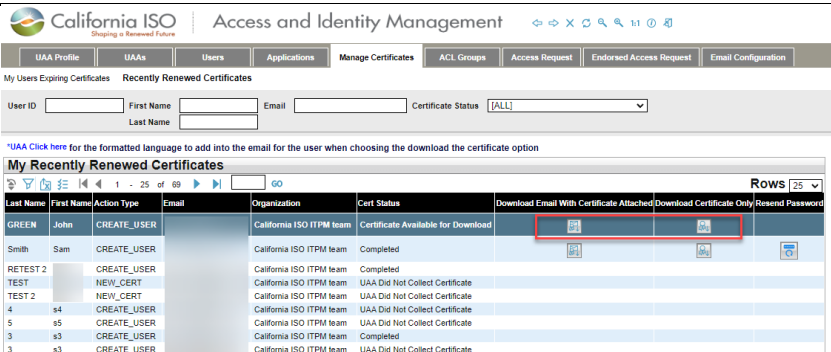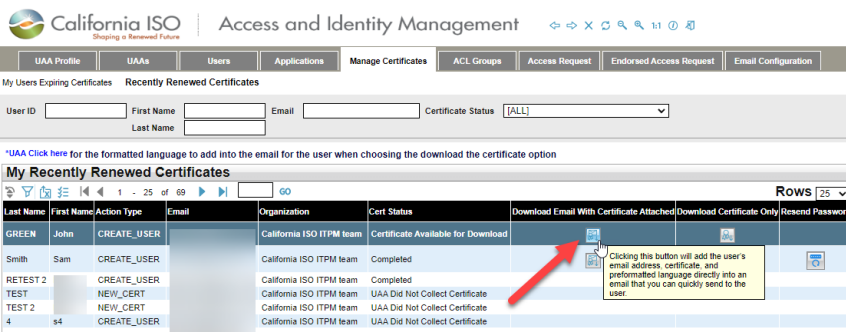|	
Click on the **Recently Renewed Certificates** link.	
Navigate to the newly created (or renewed) user. *Note: It can typically take 5-10 minutes for new or renewed users to show on the Recently Renewed Certificates list after creating or renewing a user. If the user name does not show, please check back after a few minutes.*	
The certificate download icons will now show next to the user's name. *Note: If you do not see icons available and have just created the user, please wait 3-5 minutes for processing. If the icons still do not show, please review the listed certification status for reason.*	

Downloading Email Templates with Attached Certificates (preferred method)

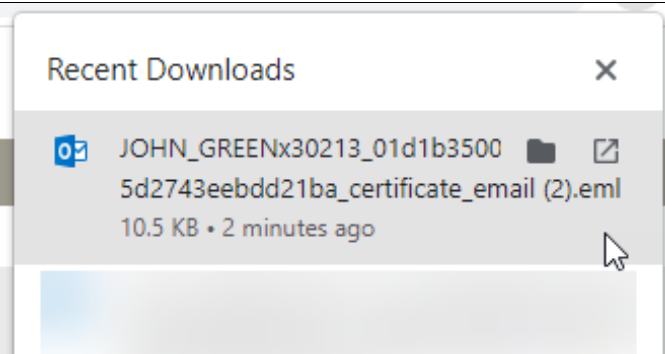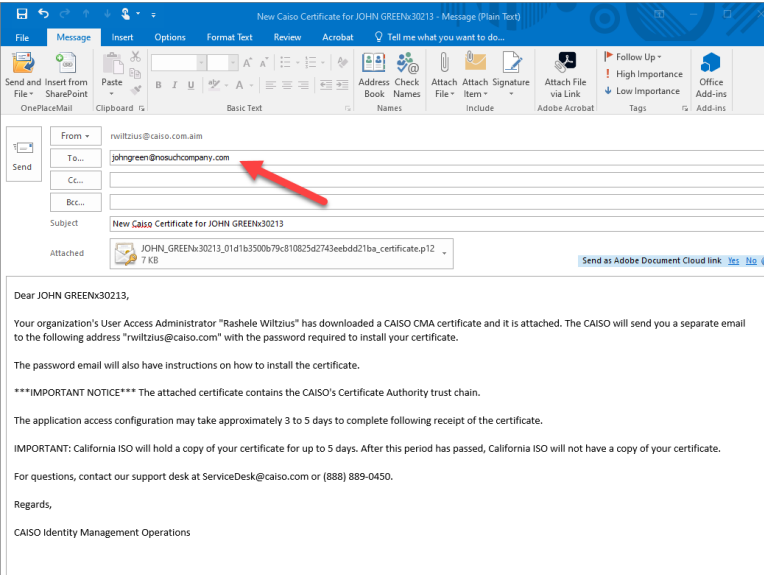|	
Click the icon on the **Download Email with Certificate Attached** column next to the selected user's name. *Note: You can roll your mouse over an icon to view a short description of what that icon does.*	
An email will be created using your default email program with the certificate attached. *Note: If you do not receive an email popup, check your browser's Recent Downloads folder.*	
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: When downloaded, the certificates are in a .p12 extension. Your organization will need to allow internal email attachments with .p12 extensions.*	

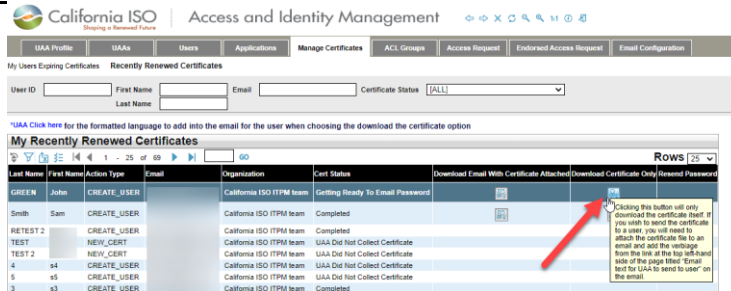|	
Users will receive a separate email directly from AIM with the certificate password. *Note: Make sure your organization whitelists downloads from the website "aim.caiso.com" and "caiso.com"*	Dear User "SALLY JANE 2x30171", We have given bellow the password to be used to install your California ISO CMA Certificate. The certificate will be provided to you by "MUAAX23863" from within your organization. Password : &amO78qeB_ For instruction on how to install your certificate please visit https://www.caiso.com/informed/Pages/Notifications/Default.aspx. If you have any further questions, please contact our support desk at HelpDesk@caiso.com or (888) 889-0450.

UAAs generating an Entrust certificate to replace a Verizon certificate for a user, please follow-up with the email recipient of the new Entrust certificate to ensure their certificate is installed.

Downloading Only Certificates from AIM

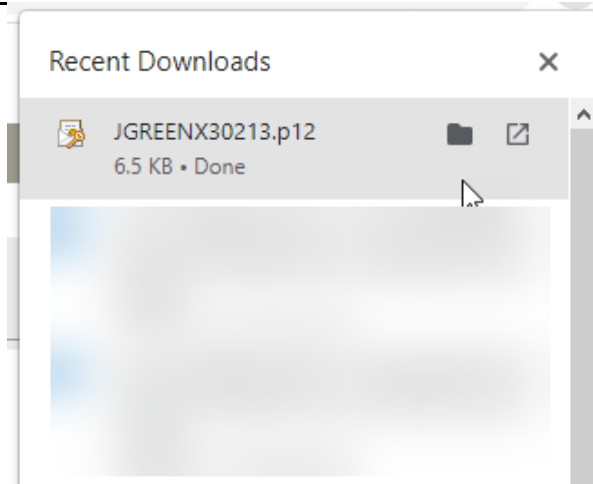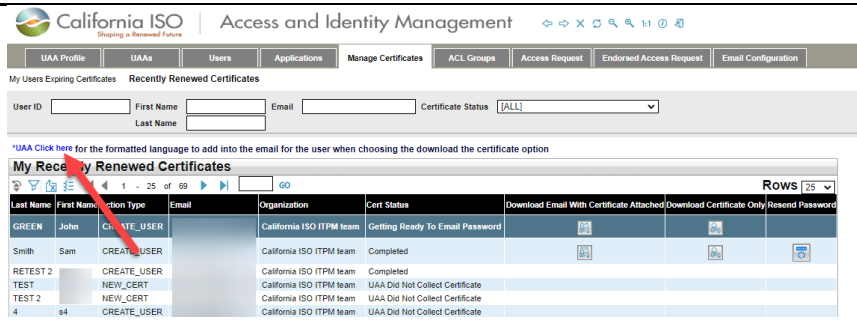|	
Click the icon on the **Download Certificate Only** column next to the selected user's name. *Note: You can roll your mouse over an icon to view a short description of what that icon does.*	
The certificate "bundle" (zip file) will be downloaded to your computer and can be found in your browser's **Recent Downloads** folder. *Note: When downloaded, the certificates are in a .p12 extension. Your organization will need to allow internal email attachments with .p12 extensions.*	

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.	
Copy the wording from the popup. *Note: You can right click and use the "copy" function or use Ctrl+C.*	
Paste the wording from the pop-up into an email (using your default email application) and attach the certificate bundle.	

<p style="color:red">UAAs generating an Entrust certificate to replace a Verizon certificate for a user, please follow-up with the email recipient of the new Entrust certificate to ensure their certificate is installed.</p>

Resending Customer Passwords for Certificates
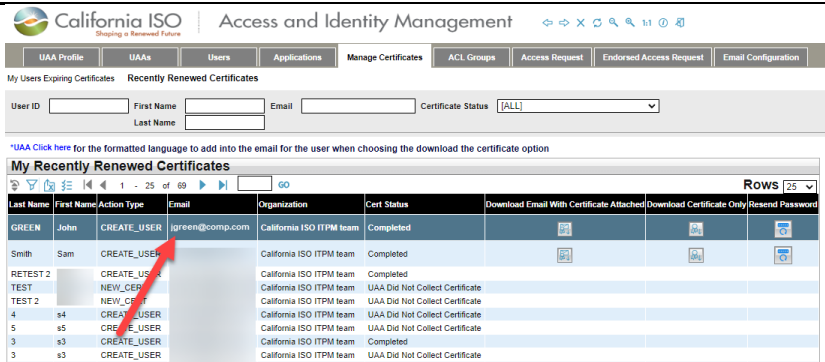
Navigate to the **Managing Certificates** tab and ensure that the customer's email address is correct. *Note: If not correct, adjust the user's email address on the user's profile under the Users tab.*	
Ensure that you have downloaded the certificate and send it to the user.	
Click on the icon in the **Resend Password** column. *Note: if the icon is not viewable, click the **Apply** button. If the icon is still not viewable, the password email may not yet been sent, the certificate process has been completed, or the*	

certificate has expired.	
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 ▓▓▓▓▓▓ 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 : 7d6MD#TmPV ⟵ * 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. 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, outages or reminders. Regards, CAISO Identity Management Operations CertificateRequests@caiso.com

Certification Statuses in AIM

Cert Status	Definition
Active	AIM has just started processing the certificate.
Getting Ready To Email Password	The certificate has been downloaded and AIM is about to send the password to the user.
Certificate Available for Download	The certificate has been created and is ready to be downloaded by the UAA.
UAA Did Not Collect Certificate	After the certificate was ready to be downloaded, the UAA did not download it. *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.*
Completed	The certificate process has completed.
Something Went Wrong – Certificate	There was failure while trying to process the certificate. If this status has not change after approximately 2 hours, contact customer support.
Invalid Cert Request	The certificate request was deemed to be invalid. This is a very rare occurrence. Please contact customer support to determine why this occurred.

Password Emailed to User	The password has been emailed to the user.
Processing Before Provider	CAISO is processing the certificate request.
Processing At Provider	The certificate is being processed by the certificate provider.