

# New AIM Certificate Process

## Job Aid

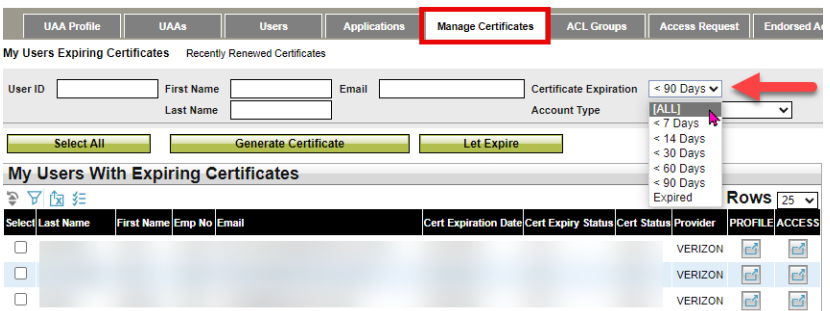
Please contact us at [UAARRequests@caiso.com](mailto:UAARRequests@caiso.com) if you have any issues or questions.

### Table of Contents

Replacing a Verizon Certificate with an Entrust Certificate .....	1
Create or Renew an Entrust Certificate .....	5
Downloading Email Templates with Attached Certificates (preferred method) .....	7
Downloading Only Certificates from AIM .....	8
Resending Customer Passwords for Certificates .....	10
Certification Statuses in AIM .....	11

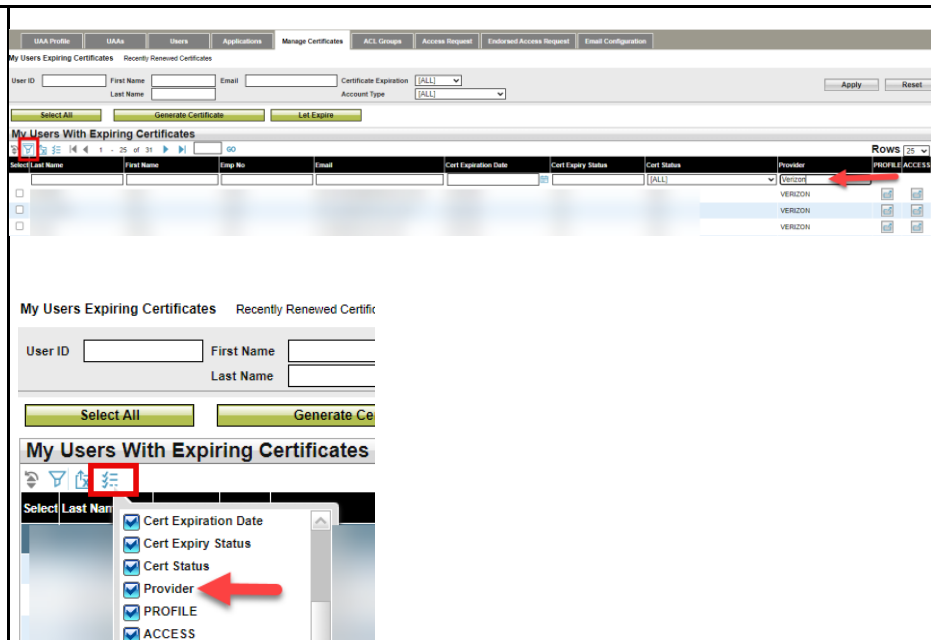
### Replacing a Verizon Certificate with an Entrust Certificate

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



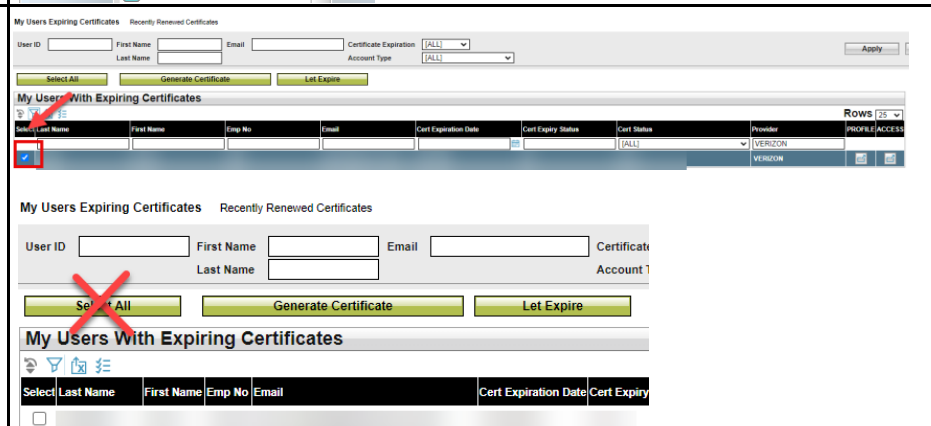
After filtering for [ALL], navigate to the filter icon on the table. In the **Provider** column, type **Verizon** and hit enter to filter.

*Note: If the Provider column is not showing, please add this column by selecting the Adjust columns button.*



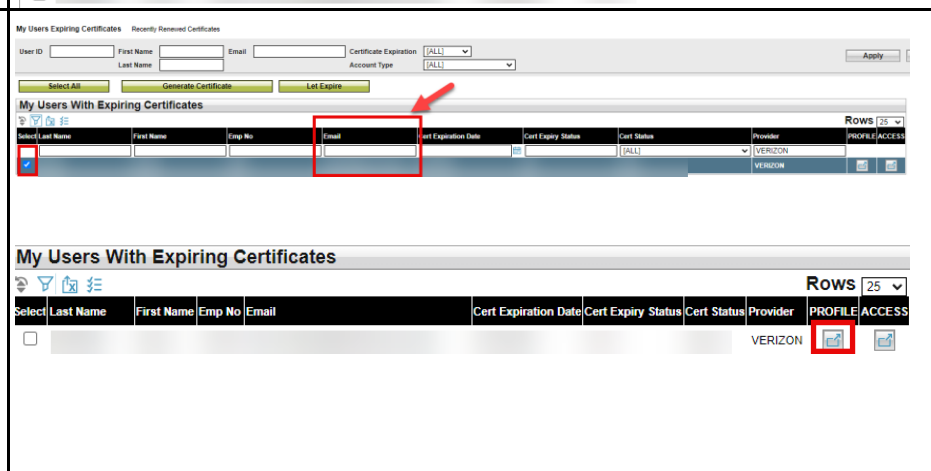
Now that only Verizon certificates are filtered, select one of the certificates.

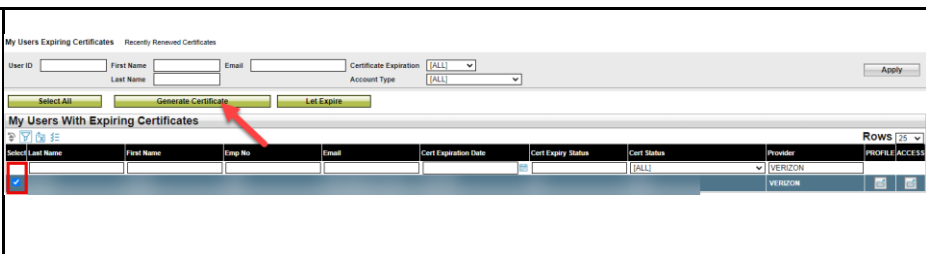
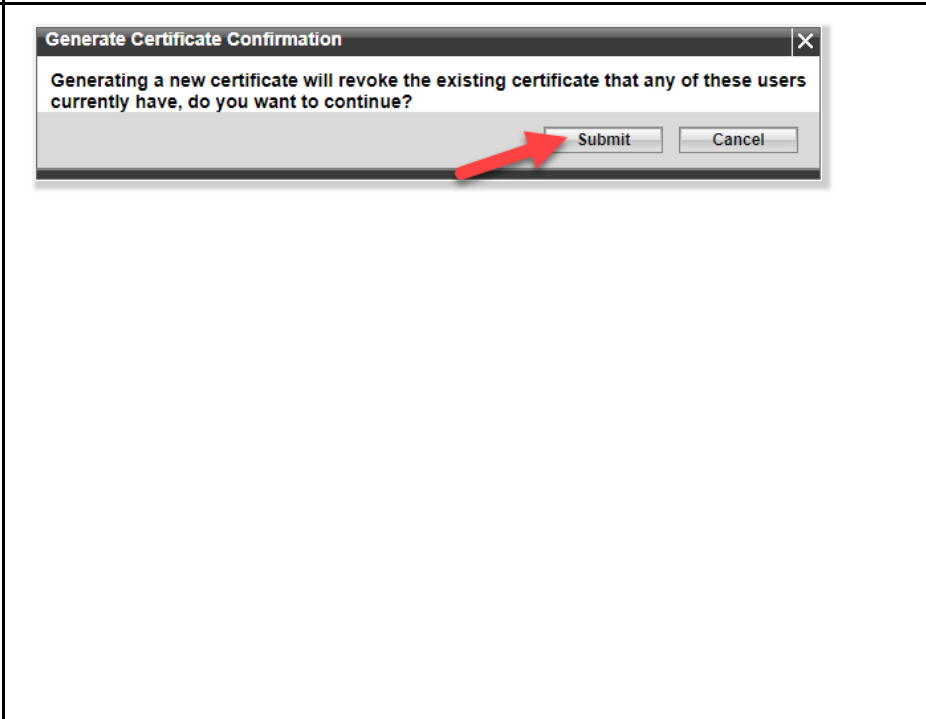
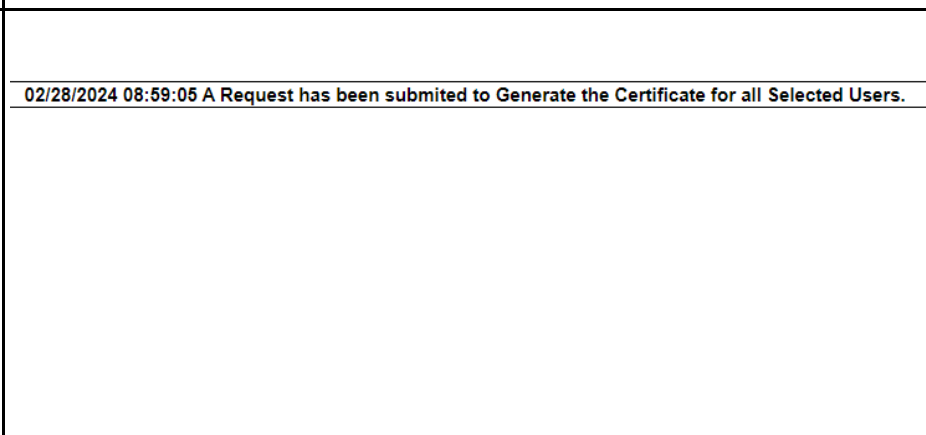
**IMPORTANT TO NOTE:**  
**Do not hit the Select All feature.** If you do, the system will select Entrust certificates as well.



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.



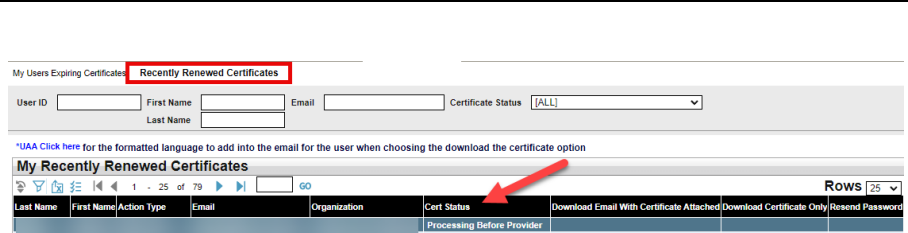
<p>Once the email is confirmed, click <b>Generate Certificate</b>.</p>	
<p>Clicking <b>Generate Certificate</b> will prompt a pop-up box if the certificate is 90 days or more from expiration warning that the older certificate will be revoked.</p> <p>This <b>WILL NOT</b> be the case for <b>Verizon</b> Certificates.</p> <p>For the purpose of replacing a Verizon Certificate to an Entrust Certificate, please disregard the pop-up by selecting <b>Submit</b>.</p>	
<p>At the bottom of the screen, users will see a text box indicating the request was submitted</p> <p><i>Note: Older Verizon certificates will remain available alongside newer Entrust certificates for roughly 14 days.</i></p>	

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.



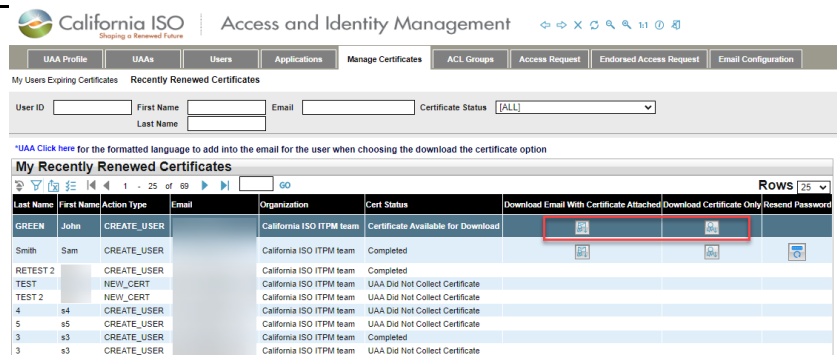
My Users Expiring Certificates **Recently Renewed Certificates**

User ID  First Name  Last Name  Email  Certificate Status [ALL] ▼

\*UAA Click [here](#) for the formatted language to add into the email for the user when choosing the download the certificate option

**My Recently Renewed Certificates**

Last Name	First Name	Action Type	Email	Organization	Cert Status	Download Email With Certificate Attached	Download Certificate Only	Resend Password
					Processing Before Provider			



California ISO | Access and Identity Management

UAA Profile | UAAs | Users | Applications | Manage Certificates | ACL Groups | Access Request | Endorsed Access Request | Email Configuration

My Users Expiring Certificates **Recently Renewed Certificates**

User ID  First Name  Last Name  Email  Certificate Status [ALL] ▼

\*UAA Click [here](#) for the formatted language to add into the email for the user when choosing the download the certificate option

**My Recently Renewed Certificates**

Last Name	First Name	Action Type	Email	Organization	Cert Status	Download Email With Certificate Attached	Download Certificate Only	Resend Password
GREEN	John	CREATE_USER		California ISO ITPM team	Certificate Available for Download			
Smith	Sam	CREATE_USER		California ISO ITPM team	Completed			
RETEST 2		CREATE_USER		California ISO ITPM team	Completed			
TEST		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
TEST 2		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
4	s4	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			
5	s5	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			
3	s3	CREATE_USER		California ISO ITPM team	Completed			
3	s3	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			

**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:



California ISO | Access and Identity Management

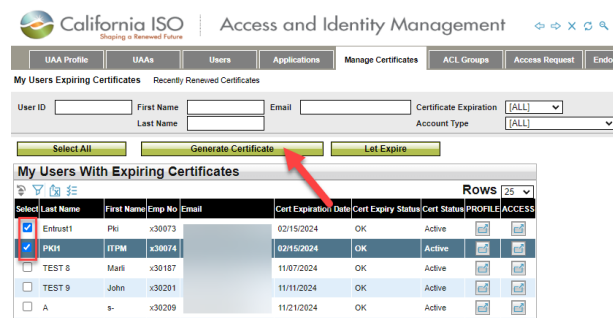
UAA Profile | UAAs | **Users** | Applications | Manage Certificates | ACL Groups | Access Request | Endors

Create New User

First Name \*  
Last Name \*  
Email \*  
Phone  
Address 1  
Address 2  
City  
State  
Postal Code  
Country: UNITED STATES  
Account Type: EXTERNALS

Submit Cancel

To renew a certificate for a current user:



California ISO | Access and Identity Management

UAA Profile | UAAs | Users | Applications | **Manage Certificates** | ACL Groups | Access Request | Endors

My Users Expiring Certificates | Recently Renewed Certificates


User ID: First Name: Last Name: Email: Certificate Expiration: [ALL] Account Type: [ALL]

Select All Generate Certificate Let Expire

My Users With Expiring Certificates

Select	Last Name	First Name	Emp No	Email	Cert Expiration Date	Cert Expiry Status	Cert Status	PROFILE	ACCESS
<input checked="" type="checkbox"/>	Entrust1	PKI	x30073		02/15/2024	OK	Active		
<input checked="" type="checkbox"/>	PKI1	ITPM	x30074		02/15/2024	OK	Active		
<input type="checkbox"/>	TEST 8	Mark	x30187		11/07/2024	OK	Active		
<input type="checkbox"/>	TEST 9	John	x30201		11/11/2024	OK	Active		
<input type="checkbox"/>	A		x30289		11/21/2024	OK	Active		

Once you have created the new user (or renewed the certificate of a current user), navigate to the **Manage Certificates** tab.



California ISO | Access and Identity Management

UAA Profile | UAAs | Users | Applications | **Manage Certificates** | ACL Groups | Access Request | Endors

My Users Expiring Certificates | Recently Renewed Certificates

User ID: First Name: Last Name: Email: Certificate Expiration: [ALL] Account Type: [ALL]

Select All Generate Certificate Let Expire

My Users With Expiring Certificates

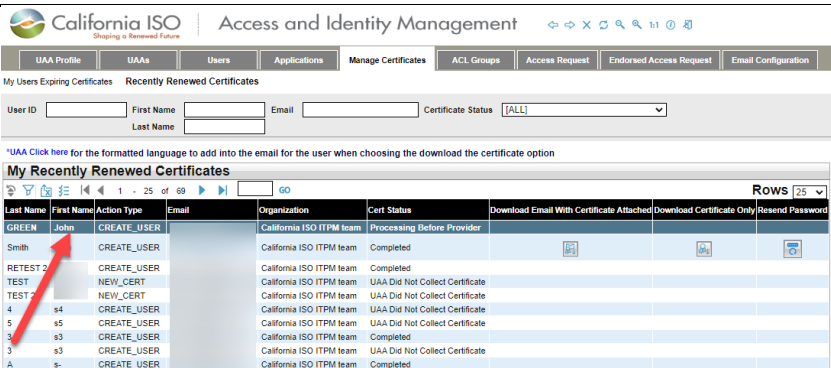
Select	Last Name	First Name	Emp No	Email	Cert Expiration Date	Cert Expiry Status	Cert Status	PROFILE	ACCESS
No Data found									

Click on the **Recently Renewed Certificates** link.



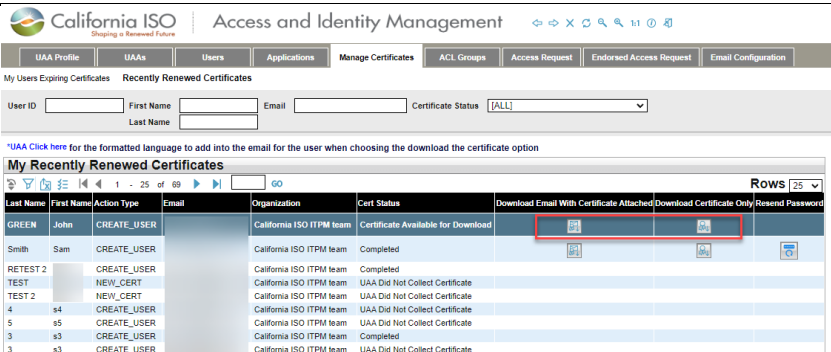
Navigate to the newly created (or renewed) user.

*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.

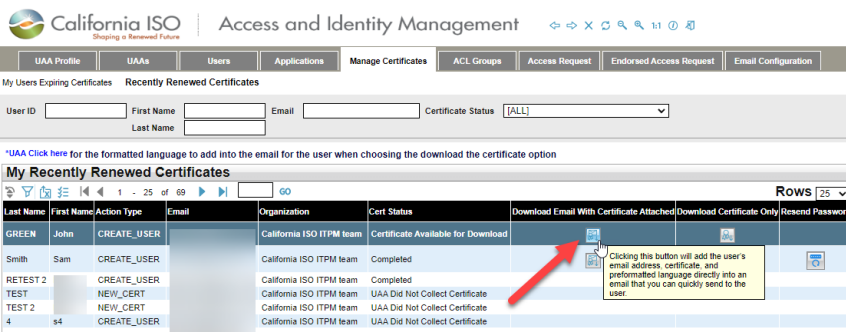
*Note: If you do not see icons available and have just created the user, please wait 3-5 minutes for processing. If the icons still do not show, please review the listed certification status for reason.*



## 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.

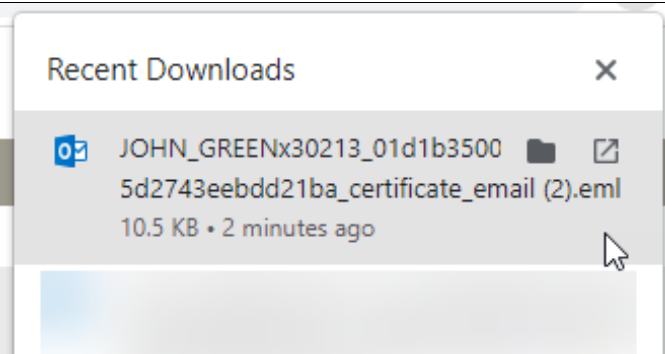
*Note: You can roll your mouse over an icon to view a short description of what that icon does.*



Last Name	First Name	Action Type	Email	Organization	Cert Status	Download Email With Certificate Attached	Download Certificate Only	Reset Password
GREEN	John	CREATE_USER		California ISO ITPM team	Completed			
RETEST 2		CREATE_USER		California ISO ITPM team	Completed			
TEST 2		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
TEST 2		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
4	s4	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			
5	s5	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			

An email will be created using your default email program with the certificate attached.

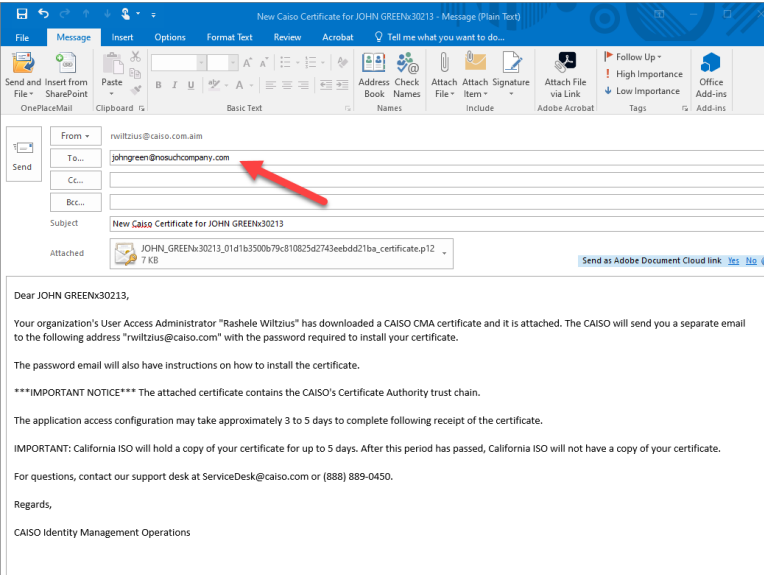
*Note: If you do not receive an email popup, check your browser's Recent Downloads folder.*



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.*



From: rwtizius@caiso.com.aim  
To: john.green@nosuchcompany.com  
Subject: New CAISO Certificate for JOHN GREENx30213  
Attachments: JOHN\_GREENx30213\_01d1b3500b79c810825d2743eebdd21ba\_certificate.p12 (7 KB)

Dear JOHN GREENx30213,

Your organization's User Access Administrator "Rashele Wiltzius" has downloaded a CAISO CMA certificate and it is attached. The CAISO will send you a separate email to the following address "rwtizius@caiso.com" with the password required to install your certificate.

The password email will also have instructions on how to install the certificate.

\*\*\*IMPORTANT NOTICE\*\*\* The attached certificate contains the CAISO's Certificate Authority trust chain.

The application access configuration may take approximately 3 to 5 days to complete following receipt of the certificate.

IMPORTANT: California ISO will hold a copy of your certificate for up to 5 days. After this period has passed, California ISO will not have a copy of your certificate.

For questions, contact our support desk at ServiceDesk@caiso.com or (888) 889-0450.

Regards,  
CAISO Identity Management Operations

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 below 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>.

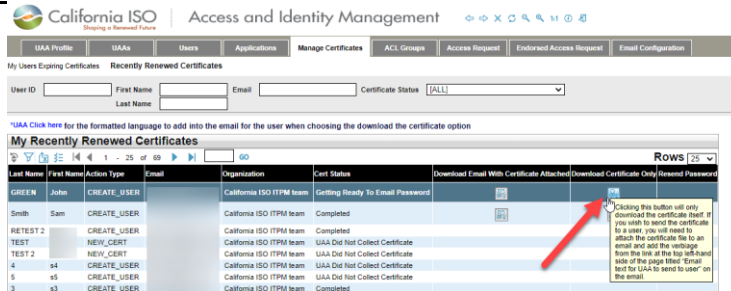
If you have any further questions, please contact our support desk at [HelpDesk@caiso.com](mailto:HelpDesk@caiso.com) or (888) 889-0450.

**UAs 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.

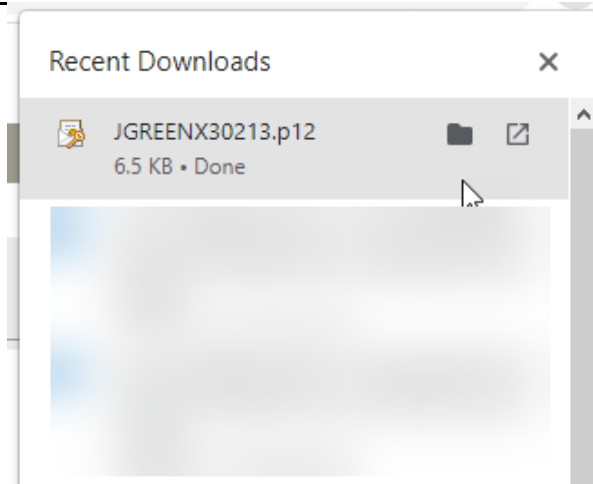
*Note: You can roll your mouse over an icon to view a short description of what that icon does.*



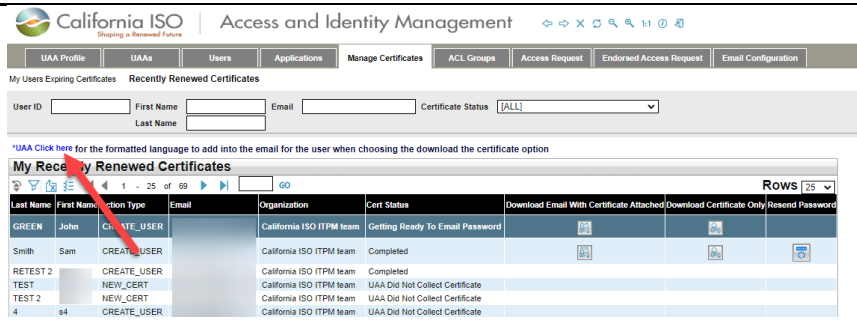
Last Name	First Name	Action Type	Email	Organization	Cert Status	Download Email With Certificate Attached	Download Certificate Only/Reset Password
GREEN	John	CREATE_USER		California ISO ITPM team	Getting Ready to Email Password		
Smith	Sam	CREATE_USER		California ISO ITPM team	Completed		
RETEST 2		CREATE_USER		California ISO ITPM team	Completed		
TEST		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate		
TEST 2		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate		
4	44	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate		
5	45	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate		
3	43	CREATE_USER		California ISO ITPM team	Completed		

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.



California ISO | Access and Identity Management

UAA Profile | UAAs | Users | Applications | **Manage Certificates** | ACL Groups | Access Request | Endorsed Access Request | Email Configuration

My Users Expiring Certificates | Recently Renewed Certificates

User ID:  First Name:  Last Name:  Email:  Certificate Status: [ALL]

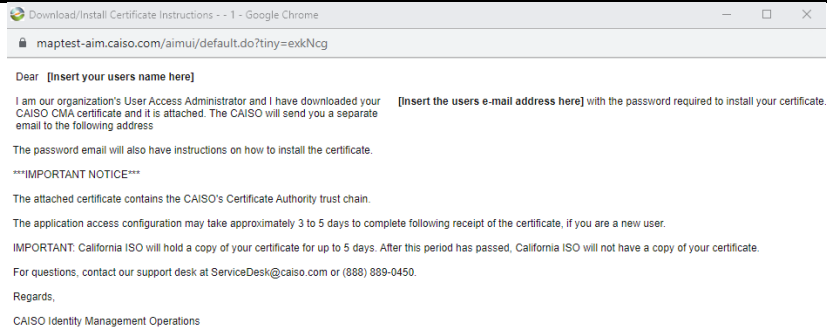
[UAA Click here](#) for the formatted language to add into the email for the user when choosing the download the certificate option

**My Recently Renewed Certificates**

Last Name	First Name	Creation Type	Email	Organization	Cert Status	Download Email With Certificate Attached	Download Certificate Only	Reset Password
GREEN	John	CREATE_USER		California ISO ITPM team	Getting Ready To Email Password			
Smith	Sam	CREATE_USER		California ISO ITPM team	Completed			
RETEST 2		CREATE_USER		California ISO ITPM team	Completed			
TEST 2		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
TEST 2		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
4	94	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			

Copy the wording from the popup.

*Note: You can right click and use the “copy” function or use Ctrl+C.*



Download/Install Certificate Instructions - 1 - Google Chrome

maptest-aim.caiso.com/aimui/default.do?tiny=exkNcg

Dear [Insert your users name here]

I am our organization's User Access Administrator and I have downloaded your CAISO CMA certificate and it is attached. The CAISO will send you a separate email to the following address [Insert the users e-mail address here] with the password required to install your certificate.

The password email will also have instructions on how to install the certificate.

\*\*\*IMPORTANT NOTICE\*\*\*

The attached certificate contains the CAISO's Certificate Authority trust chain.

The application access configuration may take approximately 3 to 5 days to complete following receipt of the certificate, if you are a new user.

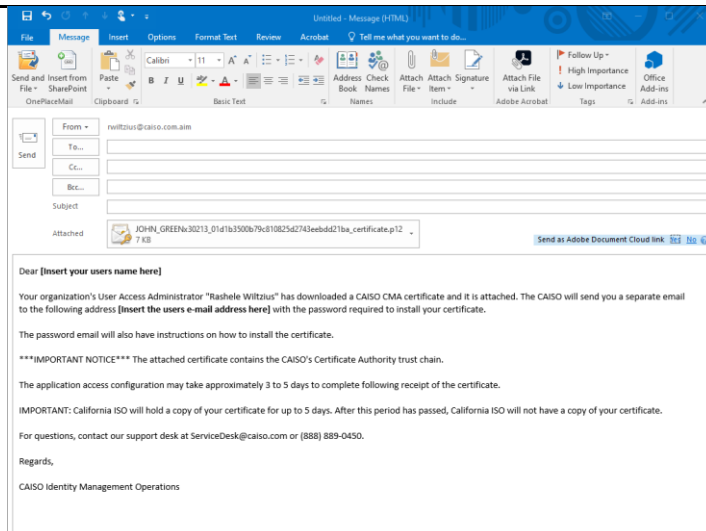
IMPORTANT: California ISO will hold a copy of your certificate for up to 5 days. After this period has passed, California ISO will not have a copy of your certificate.

For questions, contact our support desk at ServiceDesk@caiso.com or (888) 889-0450.

Regards,

CAISO Identity Management Operations

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



File | Message | Insert | Options | Format | Text | Review | Acrobat | Tell me what you want to do...

Send and Insert from File | SharePoint | OnePlaceMail | Clipboard | Basic Text | Names | Attach | Attach Signature | Attach File | Attach Item | Attach File via Link | Follow Up | High Importance | Low Importance | Office Add-ins

From: nwilltzius@caiso.com.aim

To:

Cc:

Bcc:

Subject:

Attached: JOHN\_GREEN-30213\_01d1b3500b79c810825d2743eebd421ba\_certificate.p12 7 KB

Send as Adobe Document Cloud link

Dear [Insert your users name here]

Your organization's User Access Administrator "Rashele Wiltzius" has downloaded a CAISO CMA certificate and it is attached. The CAISO will send you a separate email to the following address [Insert the users e-mail address here] with the password required to install your certificate.

The password email will also have instructions on how to install the certificate.

\*\*\*IMPORTANT NOTICE\*\*\* The attached certificate contains the CAISO's Certificate Authority trust chain.

The application access configuration may take approximately 3 to 5 days to complete following receipt of the certificate.

IMPORTANT: California ISO will hold a copy of your certificate for up to 5 days. After this period has passed, California ISO will not have a copy of your certificate.

For questions, contact our support desk at ServiceDesk@caiso.com or (888) 889-0450.

Regards,

CAISO Identity Management Operations

**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.**

## Resending Customer Passwords for Certificates

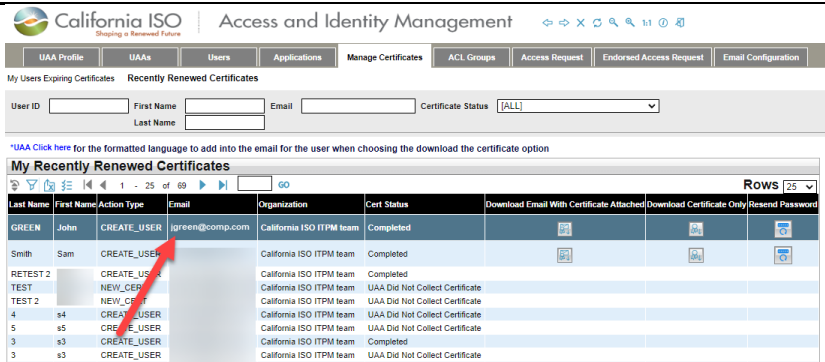
Navigate to the **Managing Certificates** tab and ensure that the customer's email address is correct.

*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*



California ISO | Access and Identity Management

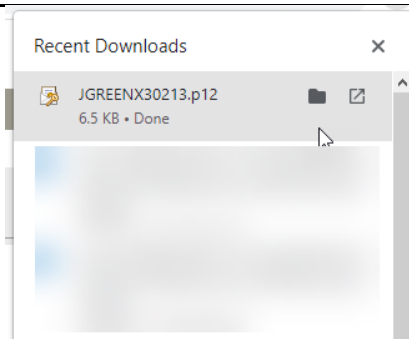
My Users Expiring Certificates Recently Renewed Certificates

User ID:  First Name:  Last Name:  Email:  Certificate Status: [ALL]

\*UAA Click here for the formatted language to add into the email for the user when choosing the download the certificate option

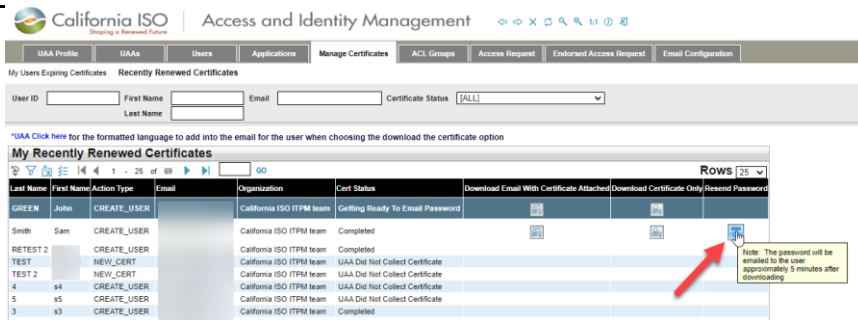
My Recently Renewed Certificates

Last Name	First Name	Action Type	Email	Organization	Cert Status	Download Email With Certificate Attached	Download Certificate Only	Resend Password
GREEN	John	CREATE_USER	jgreen@comp.com	California ISO ITPM team	Completed			
Smith	Sam	CREATE_USER		California ISO ITPM team	Completed			
RETEST 2		CREATE_USER		California ISO ITPM team	Completed			
TEST 1		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
TEST 2		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
4	s4	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			
5	s5	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			
3	s3	CREATE_USER		California ISO ITPM team	Completed			
3	s3	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			



Recent Downloads

JGREENX30213.p12  
6.5 KB • Done



California ISO | Access and Identity Management

My Users Expiring Certificates Recently Renewed Certificates

User ID:  First Name:  Last Name:  Email:  Certificate Status: [ALL]

\*UAA Click here for the formatted language to add into the email for the user when choosing the download the certificate option

My Recently Renewed Certificates

Last Name	First Name	Action Type	Email	Organization	Cert Status	Download Email With Certificate Attached	Download Certificate Only	Resend Password
GREEN	John	CREATE_USER		California ISO ITPM team	Getting Ready To Email Password			
Smith	Sam	CREATE_USER		California ISO ITPM team	Completed			
RETEST 2		CREATE_USER		California ISO ITPM team	Completed			
TEST 1		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
TEST 2		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			
4	s4	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			
5	s5	CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate			
3	s3	CREATE_USER		California ISO ITPM team	Completed			

Note: The password will be emailed to the user approximately 5 minutes after downloading

<i>certificate has expired.</i>	
By design, password emails will not be sent until approximately 5 minutes <i>after</i> certificates have been downloaded. If the user still has not received the email, please call the Service Desk for assistance.	<p>Dear User [REDACTED]</p> <p>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.</p> <p>Password : 7d6MD#TmPV ←</p> <p>* 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.</p> <p>For instructions on how to install your certificate, visit: <a href="https://www.caiso.com/informed/Pages/Notifications/Default.aspx">https://www.caiso.com/informed/Pages/Notifications/Default.aspx</a>.</p> <p>If you have any further questions, contact our support desk at <a href="mailto:ServiceDesk@caiso.com">ServiceDesk@caiso.com</a> or (888) 889-0450.</p> <p>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: <a href="http://www.caiso.com/participate/Pages/ApplicationAccess/Default.aspx">http://www.caiso.com/participate/Pages/ApplicationAccess/Default.aspx</a></p> <p>By requesting access to ISO applications or tools, you may occasionally receive emails specific to that tool, such as notifications, outages or reminders.</p> <p>Regards,</p> <p>CAISO Identity Management Operations  <a href="mailto:CertificateRequests@caiso.com">CertificateRequests@caiso.com</a></p>

## Certification Statuses in AIM

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

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