

Access and Identity Management (AIM) User Guide

Document Owner: Customer Readiness



Access and Identity Management (AIM) User Guide

Effective Date:

01/29/2024

4.5

REVISION HISTORY

VERSION NO. (Must match header)	DATE	REVISED BY	DESCRIPTION
1.0	7/16/13	RMadrigal	Initial document created
1.1	8/29/13	RMadrigal	Supplemental edits
1.2	9/9/13	RMadrigal	Supplemental edits
1.3	9/17/13	RMadrigal	Updated screenshots
1.4	10/9/13	RMadrigal	Final edits
2.0	12/23/13	RMadrigal	Added release 2 functionality
2.1	3/5/14	RMadrigal	Added list of auto-provisioned applications. Added notes regarding certificate creation and renewal. Added note regarding requests for endorsed users.
2.2	7/1/14	RMadrigal	Updated with ACL functionality, weekly expiry email.
2.3	7/25/14	RMadrigal	Updated with new Create ACL Group button
2.4	1/14/16	LStoloski	Updated with new endorsed user enhancements and email configuration
2.5	2/10/16	LStoloski	Updated with new auto provisioned applications
2.6	4/20/16	LStoloski	Revised endorsed user step by step instructions
2.7	02/16/17	Mahmadi	Revised ACL Group function and replaced all POC with UAA. Improve flow of information for users.
2.8	10/18/18	Monica M.	 Ability to see the endorsement requestor(s) Visibility to other UAA's and their authorized "entities" and "contracts" within the same organization on the UAA Profile page Weekly Expiry Email option default to "Yes" Email auto generation when the UAA provisioning request(s) are rejected by CAISO Auto generated email notification message to both organization UAA's for each endorsement application request Added the Access Request Status section
2.9	09/10/19	Monica M.	Added clarification for OMS
2.10	04/08/20	Monica M.	Provided: - Modified Intro page - Best Practices - Clarification for ACL group
3.0	06/04/20	SDainard	Added item # 11 under the 'Best Practices' section regarding the conflicting roles for RIMS users.

California ISO		Technology	ISO Version:	4.5		
	Access and Ide	ntity Manageme	ent ((AIM) User Guide	Effective Date:	01/29/2024
3.1	06/10/20	SDainard	Ad Us	ded section to 'Best Practice er section regarding entering	s' and modified C an individual's e	reate New mail address.
3.2	06/16/20	Monica M.	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.			
3.3	01/20/21	SDainard	Re UA	placed screenshots to remov As. Edited document.	e POC and add r	new tab for
3.4	09/18/23	DVance	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			
3.5	10/06/23	DVance	Ad urls	ded two notes for downloadir	ng certificates and	dwhitelisting
3.6	10/16/23	DVance	Ad	ded section "Navigating to Al	M"	
3.7	11/16/23	DVance	Ad Pro bee wip	ded section "How to Reactive ofile". Also added a reminder en end dated, authorized cor ped out.	e Another UAA's that once a UAA htracts and entitie	Expired profile has s need to be
3.8	12/28/23	DVance	Up Re pro	dated verbiage to sections C quest, and Access Request cess.	reate New User, Status for certifica	Submit Access ation download
3.9	02/15/24	DVance	Up scr	dated the Renew a Certificate reenshots with the "Provider"	e section to inclu column.	de updated
4.0	03/05/24	DVance	Ad	ded a clarifying Step 5 to "Cro	eate New User" s	ection.
4.1	03/13/24	DVance	Up and Ad	dated language to Step 5 to ' d added clarifying language fo ded verbiage for downloading	Create a New Us or how to End Da g a certificate on	er Section" te a UAA. page 44.
4.2	10/10/24	DVance	Up Ad	dated broken link on page 8 f ministrator (UAA) Establishm	or ISO User Acc ient and Requirer	ess ments.
4.3	10/21/24	DVance	Re Hy use	arranged user guide for a mo perlinks have been added thr ers to different sections when	re efficient user e oughout the guid needed.	experience. le directing
4.4	11/19/24	DVance	Cla scr	arified steps in various proces eenshots for better user expo	ses and updated	overlapping

٦

	C	alifor	nia ISC	\mathbf{C}	Technology	ISO Version:	4.5
	Acce	ess and Idei	ntity Manageme	ent ((AIM) User Guide	Effective Date:	01/29/2024
4.	4.5 01/29/25 SCarlson Updated language in the note at the end of "How Revoke/Wipe a User's Access" on how to remearize the vokes and add new section for "How to Revoke and leave the User's Access intact".		t the end of "How on how to remed r "How to Revoke act".	to y unintended a Certificate			



Access and Identity Management (AIM) User Guide

01/29/2024

4.5

TABLE OF CONTENTS

Introduction	7
Navigating to AIM	7
Acknowledgement Message upon Login	8
Create New Users	8
How to Create New User	8
How to End Date a User and a UAA	9
Submit Access Request	10
How to Submit an Access Request	11
Access Request Status	14
Certificate Process	14
How to Create or Renew a Certificate	14
Downloading Email Templates with Attached Certificates	16
Downloading Only Certificates from AIM	17
Resending Customer Passwords for Certificates	18
Certification Status in AIM	19
How to Let a Certificate Expire	19
How to Revoke/Wipe a User's Access	20
How to Revoke a Certificate and leave the User's Access intact	21
How to Submit Endorse User Access	21
UAA Submits Initial Endorse User Access Request to another UAA	21
Endorsed User Request Email Notification	23
UAA to Grant Endorse User Access Request	23
Confirm Endorsement for Selected Users	26
UnEndorse Users Endorsed to Me	26
View Endorsed Access Request History	27
View List of Endorsed Users	27
Create ACL Groups	
How to Create a New ACL Group	
How to Add Assets to an ACL Group	
How to view an ACL Group	31

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	
Create New UAA			
How to Create New UAA			
How to Add Contract and Authorized	d Entities to Selected UA	A	
How to Reactivate Another UAA's E	xpired Profile		
UAA Profile – Landing Page			
Best Practices			35
Request History			
Check Status of an Access Request			
Email Configuration			
Features of User Interface			
Application Toolbar			
Filter Toolbar – User Access Tab			
Results Window			40
Multiple Column Sorting			40
Export Menu			41

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

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 13,000 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 <u>User Access Administrator Agreement</u> 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 / <u>Contact Us</u> 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: <u>https://portal.caiso.com</u>
- 2. Through the Market Participant Portal here: <u>https://mpp.caiso.com/</u>
- 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 <u>or</u> by reaching out to an existing UAA of your organization to create one. Please keep in mind only UAAs will have access to AIM.

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

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:

After the box is checked and the Submit button is clicked on. close the window and reopen the AIM application to begin using AIM.

California ISO Access and Identity Management COMPPOXO0

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 responsibility.
 All informations 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.
- Submit Please contact your client representative at 916-608-7320 with any guestions.

Create New Users

If you are creating a UAA from a user you have just created, please ensure that you have first downloaded and emailed the certificate to that user prior to the UAA creation process. Please see "Downloading Email Templates with Attached Certificates" section for instructions.

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:

- 1. **My Users** users who belong to the UAA's organization.
- 2. Users Endorsed to Us users of other organizations that are requesting to be endorsed to your organization
- 3. 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. Add new user, navigate to the Users tab and click the Create New User button.



California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

- 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. Click **Submit**.

Create New User	
First Name *	
Last Name *	
Email *	
Phone	
Address 1	
Address 2	
City	
State	Postal Code
Country	UNITED STATES 🗸
Account Type *	EXTERNALS 🗸
	EXTERNALS
	EXTERNALS_SYSTEM

4. <u>Newly Generated certificates will only be available to be downloaded by the UAA and</u> <u>emailed to the user for 5 days under the "Manager Certificates" tab</u>. For instructions, please go to the "Downloading Email Templates with Attached Certificates" section by <u>clicking here</u>. This step is required before submitting an Access Request and/or creating a new UAA from a New User

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 section "<u>Certification Status in AIM</u>."

How to End Date a User and a UAA

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

California ISO Shoping a Renewed Future Access and Identity Manag							
UAA Profile	UAAs	Users		utions	Manag	je Certificat	es A(
User ID	First Name Last Name		Email Status	Active	~		Certifica Account
Users (Last Refreshed on:) Create New User	Users Endor	sed To Us (Last Refre	eshed or	i:) User	s Endors	sed By Us	
My Users						D	
♣' ¥ IX 3= Last Name First Name Email			Status	Cert Expira	tion Date	PROFILE	25 V
			Active	12/15/2024			

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

2. Click the pencil icon under **User Profile**. From there, go to the **End Date** section and put the desired date – click **Update** when complete.

			User ID:	Emp No:	User Name:
User ID:	Emp No:	User Name:		3	
			User Prof		
			Update	Cancel 💦	
			Emp No x	26004	
Licor Profile		Lisor Cortificatos	Emp type	EXTERNALS	
User Prome	-	User Certificates	First Name		
1			Last Name		
			Organization		
Emp No		Common Name	Email		
Emp Type			Phone Number		
User ID			Address 1		
First Name			Address 2		
act Name			City		
Last Name			State		
Organization			Postal Code		
Email			Country	JNITED STATES	
Phone Number			Start Date 11	1/20/2023	
Address 1			End Date 0	03/04/2025	2
			Status /	Active	•
			Updated By		

- 3. Similar to the steps above, to end date a UAA navigate to the **UAA** tab and click the UAA's profile button to initiate a new pop-out window.
- 4. Navigate to the UAA Profile section and select the pencil icon. From there, go to the **End Date** section and put the desired date click **Update** when complete.

User Profile	UAA Profi	UAA Profile		file UAA Profile	UAA Profile		
0	0			5 Update	Cancel 💦		
INDE NO	UAAID	Manual Voters		UAA ID	4725		
np Type	Weekly Expiry Em	sail Yes	imp Type	Weekly Expiry Ema	I Yes 🗸		
ser ID rst Name	Notes UAA Agreement U	new backup IRL	her ID	Notes	new backup		
st Name	Start Date	03/23/2022	irst Name	UAA Agreement UR	8.		
ganization tail	End Date	12/31/2099	rganization	Start Date	03/23/2022		
one Number	Updated Date	04/12/2022 16 52	mail	End Date	12/31/2099 1		
ldress 2 ly	User Certi	ficates	thone Number iddress 1 iddress 2	Updated By Updated Date	AUX_APP 04/12/2022 16:52		

Note: 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".

Authorized Col	tracts:
Contract Type	
Authorized En	No.
Authorized En	ities:
Authorized En	ities:

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. <u>Access requests will be rejected for new</u> <u>certificates if a UAA has not first downloaded and emailed the new certificate to the new user.</u>

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

How to Submit an Access Request

1. Navigate to the **Access Request** tab. Click the pencil icon to add a new request – this will allow you to either add a new row, update, or cancel.

Californi	ia ISO	Access and I	dentity Man	agement	⇔⇒×;	ु ९ ९ १:१ () ही
UAA Profile	UAAs Use	rs Applications	Manage Certificates	ACL Groups	Access Request	indorsed Access Requ
New Request Request Histor	ry					-
New Access Requ	est					
Ø Y						
Req. 0 Description	1 × N	Upd: Io Data found	ated By Updated Da	te		
Access request for applicatio Requests without approved le	ons CRR, CRRFNM, MMD/ egal documents will be R	Protected Data and Transmis ejected.	sion Planning(TP) requires	ISO Legal departmen	t approval before acc	ess request submittal.
Select Users Select Applica	ations and Roles Copy	Current User Access				
Available Users ⇒ ▽ ≸≣ Last Name → First Name → U	Jser1D	Selected Users	S			

2. Click the **New Row** button.

🌏 Ca	lifornia ISC Shaping a Renewed Futur	Acce	ess and la	lentity	Manag	ement	\$\$X \$\$
UAA Profile	UAAs	Users	Applications	Manage Ce	rtificates A	CL Groups	Access Request
New Request R	equest History						
New Acces	s Request						
New row	Update Ca	ancel 🔒					
Request ID	Description		Updat	ed By	Updated Date		

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

California ISO Shoping a Renewed Future Access an	d Identity Management
UAA Profile UAAs Users Appli New Request Request History New Access Request	Enter a description and click Update
Update Cancel	
Request ID Description	Updated By Updated Date
× No Data found	
Testing for User Guide	XATRAININGPOC140071

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

4. 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).



Note: 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.

- 5. Click on the Select Applications and Roles tab.
- 6. Click on the desired application and role and click the **Green Add** button. (Note: Use "**Ctrl + click**" or "**Shift + click**" to select multiple applications).
- 7. (Optional) To remove access, click on the drop-down button in the **Action** column in the Selected Applications/Roles section to change the selection from **ADD** to **REMOVE**.

Select Users	Select Applications and Roles Copy	Current User Access	
For Endorse	d Users, ADS provisioning at the resource	level (ACL groups) and A	Applications not listed b
Available	e Applications/Roles		
ATUILUDI	e Applications/toles		
\$,			
Application Application	Application Name	Role	
ADS	Automated Dispatch System	EXTERNAL READ	-ONLY
ADS	Automated Dispatch System	EXTERNAL READ	-WRITE
BAAOP	Balancing Area Authority Operator Porta	EXTERNAL BAA C	PERATOR
BSAP	Base Schedule Aggregation Portal	EXTERNAL BSC R	EAD-ONLY
BSAP	Base Schedule Aggregation Portal	EXTERNAL BSC R	EAD-WRITE
BSAP	Base Schedule Aggregation Portal	EXTERNAL EIM E	NTITY READ-ONLY
BSAP	Base Schedule Aggregation Portal	EXTERNAL EIM E	NTITY READ-WRITE
CIDI	Customer, Inquiry, Dispute and Informat	ion EXTERNAL SDS R	EAD-WRITE
CIDI	Customer, Inquiry, Dispute and Informat	ion EXTERNAL IMS R	EAD-WRITE
CMRI	Customer Market Results Interface	EIM ENTITY REPO	ORTS
CMRI	Customer Market Results Interface	EIM TO OPERATO	R
CMRI	Customer Market Results Interface	EIM NON TO REP	ORTS
MASTERFILE	Master File (MFRD)	EXTERNAL OPER	ATOR
MASTERFILE	Master File (MFRD)	EXTERNAL READ	-ONLY
MPP	Market Participant Portal	GENERAL MPP O	NLY
MRI-S	Market Results Interface Settlements	EXTERNAL READ	ONLY
MRI-S	Market Results Interface Settlements	METER DATA REA	AD-WRITE
WEBOMS	Outage Management System (OATI)	EXTERNAL READ	-WRITE
WEBOMS	Outage Management System (OATI)	EXTERNAL READ	-ONLY

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

- 8. (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).

Note: You will only be able copy access that comes from your own Organization. If the selected user has endorsed access that endorsed access will not be copied to the new user.

9. After all users, applications, roles, and environments are selected, click the **Update** button in the **Access Request** panel.

Note: The normal provision for users is either PRODUCTION or MAP STAGE. The STAGE environment is rarely used.

New Acces	s Reques	st				
28						
lequest ID	Description		Updated By	Updated Date		
1978	Testing for U	ser Guide	XATRAININGPOC140071 12/24/2020 09:30 Preview		Select one or more	
Access request for Requests without	or applications t approved lega	CRR, CRRFNM, MMD/Protected Dat I documents will be Rejected.	a and Transmission Planning(TP) r	requires ISO Legal dep	artment approval bef	add them to the request
Select Users Se	elect Applicatio	ns and Roles Copy Current User	Access			
Current U	sers		Current User Acces	s Current Us	er Access:	Se Applications/Roles
多 及 窪			\$∋ ≸⊟			
Last Name	🕈 First Name	🛧 UserID	Application Role 📌	Entity 👇 Enviror	nment 🕈	Jon Application Role Environment Entity Conflicting R
Training UAA	AIM	xatrainingpoc140071				
Training User1	AIM	xatraininguser1140072	L			
Training User10	AIM	xatraininguser10155123				Add
Training User2	AIM	xatraininguser2140073				
Training User3	AIM	xatraininguser3140074				Demonst
Training User4	AIM	xatraininguser4140075				Remove
Training User5	AIM	xatraininguser5155118				

- 10. Review the request to ensure that it is accurate.
- 11. Click the **Submit** button in the **Access Request Preview** window to submit the request. Please 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.

Cal	ifornia ISO Shoping a Renewed Future	Acce	ss and	Identity Ma	anageme	ent ⇔⇔	X C Q Q	1:1 () 4	
UAA Profile	UAAs	Users	Applications	Cartificanto Docom	ACL Groups	Access Reque	st Endorsed	Access Request	Email Configuration
New Request Re	s Request							Click Pr	review to be request
Request ID	Description		Up	dated By	Updated Date			~	
5978	Testing for User Guide		XA	TRAININGPOC140071	12/24/2020 09:30	Preview	Cancel		

12. After reviewing the request, click the **Submit** button to complete the request.

Access R	equest F	Previe	Clin comple	ck submi ete the re	t to equest	Submit
Last Name 🛛 📍	First Name 🕈	Action 🕈	Eh			🕈 Entity
Training UAA	AIM	ADD	PROD	CIDI	EXTERNAL IMS READ-WRITI	E TRAINING
Training User1	AIM	ADD	PROD	CIDI	EXTERNAL IMS READ-WRITE	TRAINING
Training User10	AIM	ADD	PROD	CIDI	EXTERNAL IMS READ-WRITE	TRAINING
Training User2	AIM	ADD	PROD	CIDI	EXTERNAL IMS READ-WRITE	TRAINING

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

Access Request Status

To check on the status of the application request, go to **Access Request** and then select **Request History.**

California ISO Shoping a Renewed Future Access and Identity Management	⇔⇔хҫ۹ҹ
UAA Profile UAAs Users Applications Manage Certificates ACL Groups Acce	ss Request
New Request History	
Request ID Request By (UserId): From Updated Date:	
Access Request History	

Provisioning access in AIM typically takes 1 - 1&1/2 hours to transpire, but may take up to 24-48 hours to complete for certain applications requiring verification.

• 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.

New Request Requ	st History										
Request ID From Updated Date:	31	Request By (Userl To Updated Date:	d):	Organization [A	LL]				~	Apply	Reset
Access Req	est History										
Req ID Requested E	Description Upda	ed Date 🔍 Requ	uest Tyre Statu	IS							0
114545 JSMITH	MRI-S 10/22	2018 08:09	PRO	CESSED							
Access Req	est Details										
* T 🖻 🗄		En deserved	A V	D-1-		5-14	Ctature.	Netes			
SMITH J	HN ADD	MAP-STAGE	MRI-S	EXTERNAL READ ONLY	app_mristlmt_ro_ext	ABCI	ON_HOLD	On hold for CAISO approva			

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.

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

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.

Califo	rnia ISO	Acce	ess and Ic	lentity Ma	nagemen	t ⇔⇒×	ୁ ୦ ୦ ୦ 1:1		
UAA Profile	UAAs	Users	Applications	Manage Certificates	ACL Groups	Access Request	Endorsed Ac		
My Users Expiring Certificates Recently Renewed Certificates									
User ID	First Name Last Name		Email	(Certificate Expiration Account Type	< 90 Days 🗸	~		
Select All My Users With	Expiring Cer	Generate Certific	cate	Let Expire					
> ४ छ ≇						R	ows 25 🗸		
Select Last Name F	irst Name Emp No E	mail		Cert Expiration Date	Cert Expiry Status Cer	t Status Provider	ROFILEACCESS		
 ✓ ✓ 	-	_		-	-	-			

3. 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 $\Rightarrow \Rightarrow X \heartsuit @ $ 11									
UAA Profile UAAs Users Applications	Manage Certificates ACL Groups Access Request Endorsed Ac								
My Users Expiring Certificates Recently Renewed Certificates									
User ID First Name Email	Certific Expiration 90 Days Account Type [ALL]								
Select All Generate Certificate	Let Expire								
My Users With Expiring Certificates									
● ▼ 囟 涯	Rows 25 V								
Select Last Name First Name Emp No Email	Cert Expiration Date Cert Expiry Status Cert Status Provider PROFILE ACCESS								
	e e								

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

UAA Profile	UAAs	Users	Applications	Manage Certificates	ACL Groups	Access Reque	st Endorsed Ac
My Users Expiring C	ertificates Recentl	y Renewed Certificates					
User ID	First Name Last Name		Email	Cer Acc	tificate Expiration count Type	< 90 Days 🗸	~
Select All		Generate Certific	ate	Let Expire			
My Users Wit	h Expiring Co	ertificates					
📚 🖌 🖄 🖅							Rows 25 🗸
Select Last Name	First Name Emp No	Email		Cert Expiration Date Cer	t Expiry Status Cert	Status Provider	PROFILE ACCESS

5. Navigate to the newly created (or renewed) user. The certificate download icons will show next to the user's name. It may take 5 minutes for the icon to appear, please refresh your page until the icon is present. **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.

-									
My Users Exp	iring Certificates Recently F	Renewed Certificates							
User ID	First Nam Last Nam	ne	Email	Certificate	Status [ALL]				
*UAA Click h	*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								
	≸ ≣				Rows [100~]				
Last Name	First Name Action Type	Email	Organization	Cert Status	Download Email With Certificate Attached Download Certificate Only Resend Password				
1									
				15					

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

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.

California ISO Stoping & Barnewel Future Access and Identity Management $\Rightarrow \Rightarrow X \odot @ @ 11 @ 13$								
UAA Profile UAA	s Users	Applications	Manage Certificates	ACL Groups	Access Request	Endorsed Access Request	Email Configuration	
My Users Expiring Certificates Recently Renewed Certificates								
User ID First Name Email Certificate Status [ALL]								
Las	t Name							
*UAA Click here for the formatted	language to add into the	e email for the user w	hen choosing the dov	vnload the certifica	ate option			
My Recently Renewed	d Certificates							
🗟 🖌 这 🤮	ছি 🕅 🕅 🕫 🕅 🕹							
Last Name First Name Action Ty	pe Email	Organization	Cert Status	Do	wnload Email With Ce	rtificate Attached Download Cer	tificate Only Resend Password	
						<u>e</u>		
				-		6		

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.

	n ⇔ ↑	🕴 💲 🔹 New Caiso Certificate for JOHN GREEN/x30213 - Message (Plain Text)					
File	Message	Insert Options Format Text Review Acrobat 👰 Tell me what you want to do					
Send and File * OnePla	Insert from SharePoint aceMail	Pate A A E E E E A A E E E E A A E E E E A A A E E E E A A A E E E E A A A A E A E A					
	From +	rvviltzius⊜caiso.com.aim					
Send	То	johngreen@nosuchcompany.com					
	Cc						
	Bcc						
	Subject	New Calco Certificate for JOHN GREEN/30213					
	Attached	JOHN_GREENv30213_01d1b3500b79c810825d2743eebdd21ba_certificate.p12 _ Send as Adobe Document Cloud link Yes No					
Dear JC Your or to the f The pas	OHN GREENX rganization's following add ssword emai PORTANT NC	30213, User Access Administrator "Rashele Wiltzius" has downloaded a CAISO CMA certificate and it is attached. The CAISO will send you a separate email dress "wiltzusgeaioo.com" with the password required to install your certificate. Il will also have instructions on how to install the certificate. 2TICE*** 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 que	estions, cont	act our support desk at ServiceDesk@caiso.com or (888) 889-0450.					
Regard	s,						
CAISO	Identity Man	agement Operations					

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

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*)."

Ready to submit access? <u>Click here</u>. Need to Create New UAA? <u>Click here</u>.

Downloading Only Certificates from AIM

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

California ISO Access and Identity Management $\Rightarrow \Rightarrow \times o e $ In () &									
UAA P	rofile U/	LAs	Users	Applications	Manage Certificates	ACL Groups	Access Request	Endorsed Access Request	Email Configuration
My Users Expiri	ng Certificates Re	cently Rene	wed Certificates						
User ID	F	irst Name		Email	Ce	tificate Status [/	ALL]	~	
	L	ast Name							
*UAA Click he	re for the formatte	d language	to add into the en	nail for the user w	hen choosing the dow	nload the certific	ate option		
My Rece	ently Renew	ed Certi	ficates						
≥ 7 🖄 :	}≡			_					Rows 100 -
Last Name	First Name Action	Type En	mail	Organization	Cert Status	De	ownload Email With Ce	rtificate Attached Download Cer	tificate Only Resend Password
							6		

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 **Manage 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.

My Users Expiring Certificates	Recently Re	newed Certificates									
User ID	First Name Last Name		Email	Certificate Status	s [ALL]						
*UAA Click here for the for My Recevy Ren	*UAA Click here for the formatted language to add into the email for the user when choosing the download the certificate option My Receive Renewed Certificates										
🦻 🏹 🖄 🚝 📐 📢	1 - 25 of (59 🕨 🕨	GO								
Last Name First Name Ac	n Type Err	ail	Organization	Cert Status	Download Email With Certificate Attached Downlo						

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

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

	Onwnload/Install Certificate Instructions - · 1 - Work - Microsoft Edge
	https://maptest-aim.caiso.com/aimui/default.do?tiny=QjrbPA
	Dear [Insettyour users name here]
ľ	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 certificat
	The password email will also have instructions on how to install the certificate.
ľ	**IMPORTANT NOTICE**
ľ	The attached certificate contains the CAISO's Certificate Authority trust chain.
ł	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.
ł	For questions, contact our support desk at ServiceDesk@caiso.com or (888) 889-0450.
	Regards,
	CAISO Identity Management Operations
- U	

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

Note: This action can only be accomplished if done within 5 days of the certificates generation.

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

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 Contificates Recently Renewed Certificates									
User ID First Name Email Certificate Status [ALL] V Last Name									
*UAA Click	here for th	e formatted lang	uage to add into the	email for the user when c	hoosing the download the co	ertificate option			
My Re	cently	Renewed C	ertificates						
ə 🖓 🖄	≸≣ 4	🖣 1 - 25 o	n 69 🕨 🔰 📃	60			F	Rows 25 V	
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		2	2	
Smith	Sam	CREATE_USER		California ISO ITPM team	Completed	<u>67</u>	Bu	7	
RETEST 2		CREATE_US		California ISO ITPM team	Completed				
TEST		NEW_CER		California ISO ITPM team	UAA Did Not Collect Certificate				

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

Rece	ent Downloads	×	;
3	JGREENX30213.p12 6.5 KB • Done	Ø	î

3. Click on the icon in the **Resend Password** column.

*WA 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 Image: Second S										
Last N	ame Firs	st Name	Action Type	Email	Organization	Cert Status	Download Email With Certificate Attached	Download Certificate Ont	Resend Password	
GREE	N Job	h	CREATE_USER		California ISO ITPM team	Getting Ready To Email Password	5	2		
Smith	Sar	m	CREATE_USER		California ISO ITPM team	Completed		a .	D	
RETE	ST 2		CREATE_USER		California ISO ITPM team	Completed			Note: T	
TEST			NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			emailed	
TEST	2		NEW_CERT		California ISO ITPM team	UAA Did Not Collect Certificate			downloa	
4	54		CREATE_USER		California ISO ITPM team	UAA Did Not Collect Certificate				

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

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.



Certification Status in AIM

Cert Status	Definition
Active	AIM has just started processing the certificate.
Getting Ready To Email	The certificate has been dow nloaded and AIM is about to send the password
Password	to the user.
Certificate Available for Download	The certificate has been created and is ready to be dow nloaded by the UAA.
UAA Did Not Collect Certificate	After the certificate w as ready to be dow nloaded, the UAA did not dow nload 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.

How to Let a Certificate Expire

- 1. To let a certificate expire, navigate to the Manage Certificates tab.
- 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.

🍣 Calife	ornia ISO	Acce	ess and lo	lentity Mar	nagemen	t ⇔⇔x¢
UAA Profile	UAAs	Users	Applications	Manage Certificates	ACL Groups	Access Request
My Users Expiring Ce	rtificates Recently	Renewed Certificates	5			
User ID	First Name		Email	Ce	rtificate Expiration	< 90 Days 🗸
	Last Name			Ac	count Type	[ALL]
Select All		Generate Certifi	cate	Let Expire	⊶	
My Users With	n Expiring Ce	rtificates				
🗟 🖌 🖄 🛠						Rows 25 🗸
Select Last Name First N	Name Emp No Email		Cert Expirat	ion Date Cert Expiry Stat	us Cert Status Provi	der PROFILE ACCESS
			19			

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

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/Wipe a User's Access

1. To revoke a user's certificate, navigate to the **User** tab. Find the correct user and click on the button in the **Profile** column.

California ISO Shoping a Renewed Future Access and Identity Manag										
UAA Profile	JAAs	Users		utions	Manag	e Certificat	es A(
User ID	First Name Last Name		Email Status	Active	~		Certifica Account			
Users (Last Refreshed on:) Create New User	Users (Last Refreshed on:) Users Endorsed To Us (Last Refreshed on:) Users Endorsed By Us Create New User									
My Users										
€ ▼ 弦 差						Rows	25 🗸			
Last Name First Name Email			Status	Cert Expira	tion Date	PROFILE /	ACCESS			
			Active	12/15/2024	1					

2. From the **User Profile** screen, click the **Revoke User** button.

User ID: Emp No:	User Name:					
		_	\rightarrow	Revoke Us	er	
User Profile	User Certifica	ates				
Ø						
Emp No Account Type	Common Name	Serial Number	Valid From	Valid To	Cert Status	Cert Action
User ID			03/23/2022	03/27/2025	Active	
First Name			09/14/2020	12/14/2023	Inactive	RENEW
First Name			09/14/2020	12/14/2	023	023 Inactive

- 3. 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."
- 4. Click **OK** to revoke the user's certificate.
- 5. 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, there are two ways to resolve. (1) The quickest way to fix the loss in access would be to create a new user, download and email the certificate to the individual, and then provision that new user all need access. (2) If you wish to keep the user ID as is, 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

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

UAA to add access back. Please mind that if user was a UAA, a UAA Agreement will need to be submitted for this user to regain AIM access.

How to Revoke a Certificate and leave the User's Access intact

There may be a situation when a certificate have been compromised or is malfunctioning, but the user the certificate is intended for still needs application access. Please mind that the following action will only work for certificates with expiration dates greater than 90 days from the current date. In order to revoke a certificate only and keep the users access intact, please...

1. Start on step 2 of the "<u>How to Create or Renew a Certificate</u>" section above. However, once you have navigated to the Manage Certificate tab, please change the Certificate Expiration filter from "<90 Days" to "[ALL]", then click the "Apply" button.



- 2. After clicking the Generate Certificate button, you should see a pop up message warning that by continuing, the older certificate will be revoked. (This message will not appear if the certificate you are generating a replacement expires within 90 days. In that scenario, the older certificates will remain intact until the expiration date.)
- 3. By clicking submit, the older certificate will be revoked and a new replacement certificate will become available to download and send to the intended certificate user. For those instructions see the "Download Email Template with Attached Certificates" above.

How to Submit Endorse User Access

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 <u>My</u> <u>Users</u>. The top section is My Users to be Endorsed and the bottom section is My Users to be UnEndorsed.

UAA Submits Initial Endorse User Access Request to another UAA

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

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

_							
🍣 Calif	ornia ISC Shaping a Renewed Futur	Acc	ess and la	dentity Man	agement	⇔ ⇔ X	💭 🔍 🍳 1:1 🕧 💐
UAA Profile	UAAs	Users	Applications	Manage Certificates	ACL Groups	Access Request	Endorsed Access Request
Endorse/UnEndorse M	My Users UnEndo	rse Users Endorsed t	o Me Add/Remove E	Endorsed User Access Er	dorsed Access Reque	st History	
,							
Endorse My Users							
Available Us	sers			Conf	irm Endorse	ment For Sel	ected Users
> ∀ 🖄 結 ।	4 4 1 - 8 a	of 8 🕨 ▶	GO	UserID	Last Name	Firs	st Name
UserID	Last N	lame First	Name			× No Data found	
				Remove			

- 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).
- 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.
- 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. Click the **Endorse Selected Users** button.

E	ndorse/UnEndorse My Users	UnEndorse Users E	ndorsed to Me Add/R	emove Endorsed User A	ccess Endorsed Acces	s Request History	
	▼Endorse My Users						
	Available Users				Confirm End	orsement For Sel	ected Users
	> ∀ 🕱 ≸≣ ┥ ┥ 1	- 6 of 6 🕨	▶ G0	Add	UserID	Last Name	First Name
	UserID	Last Name	First Name				
				Remove			
				Remove All			
	Select an Organization:			~			
	Enter a comment (required	d):					
						h	
	Endorse Selected Users						

Key Reminders

- 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.

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

Example:

Name	User ID	Action	Environment	Application	Role	Entity
OMSTester05	OTESTER05x812	ADD	MAP-TEST	ADS	EXTERNAL READ-ONLY	PCG2
on 10/02/2018	occarejected by Car	so person	u	v/similar short	d and for the second	CHIS

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

For a high-level overview, consider checking out this quick training walkthrough here!

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

Under the **UAA Profile** section, in the **Endorsed Users without Access** box, UAAs may see users from other organizations waiting for approval. If a user(s) are listed here, that is the indicator for the UAA to go to the **Endorsed Access Request** tab for approval/disapproval of their access request.



1. Under the **Endorsed Access Request** tab, navigate to the **Add/Remove Endorsed User Access** sub-tab. The granting UAA will click on the pencil icon to add a new request.

California ISO Shaping o Renewed Future Acces	ss and Identity Mc	inagement	् ् 1:1 () ही
UAA Profile UAAs Users	Applications Manage Certificate:	s ACL Groups Access Requine	Endorsed Access Request
Endorse/UnEndorse My Users UnEndorse Users Endorsed	Add/Remove Endorsed User Access	Endorsed Access Request History	
New Endorsed Access Request			
Request 3 Description	Updated By Update	d Date	
× No Data fou	ind		
Select Endorsed Users Select Applications and Roles Copy	Current User Access		_
Available Users Endorsed to Me	Sele	cted Users	
🂱 🏹 搅 🚝 ┥ 🖉 - 0 of 0 🕨 🕨 🗌	60 🗙 😓	∀ 4 0 - 0 of 0 ▶ ▶	
Endorsing Org UserID Last Name First Name Is Provisio	oned A Endorsi	ng Org UserID Last Name First Name	
× No Data found		× No Data found	

2. The UAA will then click on the **New Row** button, type a description for the request and click the **Update** button.

Endorse/UnEndorse	My Users	UnEndorse Use	ers Endorsed to Me	Add/Remov	e Endorsed U	ser Access	Endorsed	l Access
New End	- Ja Ac	cess Rec	uest					
Update	Cance	el 💦						
Request ID	Description	on			Updated By	Updated	d Date	
			Хнов		1			
	Testing F	Purpose						
C-1+ C		.1 &		C				

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

 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).

Palast Cadana di Jawa	O de et de estile							
Select Endorsed Users	Select Applica	ations and Ro	copy Current User Ad	ccess				
Available Use	rs Endors	sed to M	e		Selected L	sers		
>∀ 🖄 🚝 ┥	€ 0 - 0	of 0 🕨	▶ GO		X 🕭 📐 利	۰	- 0 of 0	
Endorsing Org User	iD Last Name	First Name	Is Provisioned		Endorsing Org	UserID	Last Name	First Name
	× No Dat	a found				× No E	ata found	

4. 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).

Select Endorsed Users Select Applications and Roles	Conv Current User Access	
Available Applications/Roles		Selected Applications/Roles
New Endorsed Access Request		
◊ ₽		
equest ID Description	Updated By	Updated Date
× No E	Data found	
Select Endorsed Users Select Applications and Roles	Copy Current User Access	
Available Applications/Roles		Selected Applications/Roles
۲		New row Update Cancel 😋
Application Application Name Role		Action Application Role Environment Entity Conflicting Rol
WEIMPORTAL Western EIM Portal site ENTITY READ C	ONLY EXTERNAL	ADD V WEIMPORTAL V ENTITY READ ONLY EXTERNAL V PROD V
	Add	ADD letter foles will be highlighted in yellow if roles conflicts with each other, did or remove the conflicting roles to continue with the access request.
	Remove	

- 5. (Optional) To remove access, click on the drop-down button in the **Action** column to change the selection from **ADD** to **REMOVE**.
- 6. (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.
 - a. Click a name in the **Current Users** panel to view that user's access in the **Current User Access** panel.
 - b. 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).

S	elect Endorsed Users	Select Application	ns and Roles Copy Cu	rrent User Acce	88						
Users Endorsed to Me			Current Use	r Acces	ss Curre	ent User Access:		Selected Applications/Roles			
	Endorsing Org		UserID	Last Name	First Name	Application	Role	Entity	Environment		Action Application Role Environment Entity Conflicting Role?
										Add	
										Remove	

7. After all users, applications, roles, and environments are selected, click the **Update** button in the **Access Request** panel.

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

- 8. Review the request to ensure that it is accurate.
- 9. 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.)

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

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.

1. Click on the **Endorsed Access Request** tab and then the **UnEndorse Users Endorsed to Me** sub-tab.

	$\bigotimes_{\text{Shapping a Renewed Future}} \text{Access and Identity Management} \Leftrightarrow \Rightarrow \times \ \square \ \P \ \P$									
	UAA Profile UAAs Users Applications Manage Certificates ACL Groups Access Request Endorsed Access Request Email G							quest Email Co		
Er	ndorse/UnEndorse My Users	Jorse/UnEndorse My Users UnEndorse Users Endorsed to Me Add/Remove Endorsed User Access Endorsed Access Request History								
	Users Endorse	d to Me			Add	1 S	Selected Use	rs For U	nEndorse	
		1 - 10 of	313 ViserID	GO Last Name	First Name	Ē	A Y IX 3 = I¶ ndorsing Org	I - UserID	0 of 0 🕨 🖡	First Name

- 2. From the list of users in the User Endorsed to Me box, select the applicable user.
- 3. Click the **Add** button. This will move the selected user from left box to the right box **Selected Users For UnEndorse**.

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

4. Click on the **Un Endorse Selected Users** button on the bottom of the left box. This will UnEndorse the selected user.

Endorse/UnEndorse My Users	UnEndorse Users Endorsed to Me	Add/Remove Endorsed Us	er Access Endorsed	Access Request History	
	1 - 1				
Users Endorsed	to Me			Selected Users Fo	or UnEndorse
> ∀ 🖄 ﷺ 🛯 ◄	1 - 10 of 311 🕨 🔰	GO	Add	🖓 🖄 🚝 ┥ 🖣 1	- 2 of 2 🕨 🌬 😡
Endorsing Org	UserID	Last Name First Name		Endorsing Org	UserID Last Name First Name
			Remove		
			Remove All		
Un Endorse Selected Us	sers				

View 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.

- 1. Click on the **Endorsed Access Request** tab and then click on the **Endorsed Access Request History** sub-tab.
- 2. The Access Request History shows you a list of your recent access requests.
- 3. 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.
- 4. 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.

Californ	California ISO Access and Identity Management $\Rightarrow x o q q to 0$							
UAA Profile	UAAs Users	Applications	Manage Certificates	ACL Groups	Access Request	Endorsed Access Reques	st E	
Endorse/UnEndorse My Users	UnEndorse Users Endorsed to Me	Add/Remove Endorse	ed User Access Endors	sed Access Request H	listory			
Request ID					A	pply Reset		
Access Request	History							
Ø 🖗 🖓 🚝 ┥ ♦	1 - 10 of 258 🕨 📔	GO						
Req ID Requested By	Description		Updated Date	T Status	j			
Access Request	Details							
多 🖌 🖄 🖅								
Last Name 🛖 First Name 🛖 C	N User ID A	ction Environment	Application Role		Entity	Status Notes		

View List of Endorsed Users

There is a sub tab under the **Users** tab called **Users Endorsed to Us**. This 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).

Owner: Customer Readiness

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

- 1. Click on the **Users** tab and then click on **Users Endorsed to Us**.
- 2. Please allow time for users from other organizations to show up under **Users Endorsed to Us**. This is just a view display.

Califc	ornia ISC haping a Renewed Futur	Acce	ss and la	dentity Ma	nagemen	nt ⇔⇒×	(C Q Q 1
UAA Profile	UAAs	Users	Applications	Manage Certificates	ACL Groups	Access Request	Endorsed /
User ID	First Name Last Name		Email Status Active	✓ .	Certificate Expiration Account Type	[ALL]	~
Users (Last Refreshed o	on:) Users Endo	orsed To Us (Last Refr	eshed on:) Use	ers Endorsed By Us			
Users Endorse	ed to Us						
🗟 🕅 🔯 🖉	🖣 1 - 25 of 3	333 🕨 🔰	GO				
Last Name First Name	Email		User Organizat	tion	Status	Cert Expiration Date E	Endorsement Da

QUICK REFERENCE GUIDE TO ENDORSED ACCESS REQUEST SUB TABS

- 10. Endorse/UnEndorse My Users: This sub tab is for <u>REQUESTING UAA only</u>. The users reflected under this sub tab belong to your organization.
- 11. **UnEndorse Users Endorsed to Me**: This sub tab is for <u>GRANTING UAA only</u>. The users reflected under this sub tab do NOT belong to your organization.
- 12. Add/Remove Endorsed User Access: This sub tab is for <u>GRANTING UAA only</u>. The users reflected under this sub tab do NOT belong to your organization.
- 13. Endorsed Access Request History: This sub tab is for <u>GRANTING UAA only</u>. 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

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	(AIM) User Guide	Effective Date:	01/29/2024

1. Click the **ACL Groups** tab and then click the **Create ACL Group** button to create an ACL group.

Califor	rnia ISO	Acce	ess and la	entity	Man	agemen	t ⇔ ⊰	×
UAA Profile	UAAs	Users	Applications	Manage Ce	rtificates	ACL Groups	Access Req	uest
Entity Type [ALL]	Entity Name		Group Name		Enviro	onment [ALL]	✓ Statu:	s Pr
Create ACL Group	\leftarrow							
ACL Groups					Asset	s		
🖉 🖗 🖓 🗊 🗲			Row	S 25 ✔	€71	א ≹≡		
Entity Name Entity Type En	nvironment Group Nam	ne Description St	art Date End Date St	atus Count	Asset Nam	ne 🕇 Asset Type Ma	sterFile Start Da	te 축 M

2. Select the **Environment** and enter a **Description** for the ACL group. 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.

Create New ACL Gr	oup	
Entity Type	SCID	~
Entity Name	[None]	~
Environment		Remember: State Date
Description		may be set to a past date.
Start Date		
End Date	t	
	Submit	ncel

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 <u>does not</u> 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

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

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

UAA	Profile	UAAs	Users	Applications	i Certif	icate Renewa	ACL Gro	oups	Access Reques	t Endorsed Acce	
Entity Type	Entity Type [ALL] V Entity Name Group Name Environment [ALL] V Status Provisionable										
Create AC	Create ACL Group Select the ACL Group name and click on the Pencil icon										
1 2 7	Rows 25 V										
Entity Name	Entity Type	Environment	Group Name	up Name Description		End Date	Status	Count			
TRAINING	SCID	PROD	EXC_TRAINING_186	Resources 1 2 & 3	12/01/2015	12/31/2028	Provisionable	0	Edit	Delete	

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.

UAA	Profile	UAAs	Users	Арр	lications	Manage Certi	ficates	ACL Groups	Acce	ss Requ	est Endorsed	Access Request
Entity Type Create AC	[ALL]	C Entity M	lame	Nov "Descri	w you o ption" a of the J	an cha and "S ACL Gr	inge the tatus'' fi oup	e ields	Status	s Provisionable		
Update	2	Cancel 🗧	a	_								
Entity Name	Entity Type	Environment	Group Name	Description		Start Date	End Date	Status 🗸		Count		
TRAINING	SCID	PROD	EXC_TRAINING_186	Resources	12&3	12/01/2015	12/31/2028	Provisionabl	e 🗸	0		
TRAINING	SCID	MAP-STAGE	EXC_TRAINING_185	Resource 3	only	12/01/2015	12/30/2017	Provisionable		0	Edit	Delete

How to Add Assets to an ACL Group

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

UAA Profile UA		UAA	8	Users	Applications	s Mana	ge Certificates	ACL Groups	Access Request
UAA Profile UA			8	Users	Applications	s Mana	ge Certificates	ACL Groups	Access Request
Entity Type	[ALL]	✓ Entity	Name		Group Name		Envir	onment [ALL]	✓ Status Provi
Create AC	CL Group		Fi	rst select the	ACL Gro	up then			
ACL G	ACL Groups			ck on "Edit"	to add res	ources			
	囟 绐								Rows 25 🗸
Entity Name	Entity Type	Environmer	t Group	Name Descript	tion Start Date	End Date	Stau. C	Count	
BARC	SCID	MAP-TEST			08/16/2023	08/31/2023	Provisionable	4 Edit	Delete
BARC	SCID	MAP-TEST			08/16/2023	11/29/2023	Provisionable	0 Edit	Delete

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

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 <u>PERMANENTLY</u> 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.

W	A Profile	UAAs	Users	Application	s Mana	ige Certifica	ACL G	iroups	Access Requ	est Endorsed A	Access Request Email Configuration
Entity Ty	e [ALL]	C Entity P	Name	Group Name		E	nvironment	[ALL]	✓ Status	Provisionable	\checkmark
Create	ACL Group										
ACLO	Groups										Assets
/ 🖗 🛛	了囟狂									Rows 25 🗸	€ ∀ 🖄 ﷺ
Entity Nan	e Entity Type	Environment	Group Name	Description	Start Date	End Date	Status	Count			Asset Name 🕈 Asset Type MasterFile Start Date 🕈
TRAINING	SCID	PROD	EXC_TRAINING_186	Resources 1 2 & 3	12/01/2015	12/31/2028	Provisionable	0	Edit	Delete	×Nc
TRAINING	SCID	MAP-STAGE	EXC_TRAINING_185	Resource 3 only	12/01/2015	12/30/2017	Provisionable	0	Edit	Delete	
TRAINING	SCID	MAP-STAGE	EXC_TRAINING_184	Resource 3 only	12/01/2015	12/31/2017	Provisionable	0	Edit	Delete	
											Click on an ACL Group to
											view the list of Assets
											displayed here

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

Create New UAA

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

If you are creating a New UAA from a <u>newly created User</u>, please ensure you have downloaded and emailed the certificate to the user prior to Creating the New UAA. <u>Click here</u> for instructions.

How to Create New UAA

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

California ISO Access and Identity Management $\Rightarrow x$										
UAA Profile	UAAs	Users	Applications	Manage Certificates	ACL Groups	Access Request				
First Name		Last Name		Email	Sta	tus Active 🗸				
Create New UAA Pro	ofile	-								
User Access A	dministrato	rs								
> ∀ 岔 注										
Last Name 🦰 First Name	User Id	Notify AIM Org Sho	rt Name Organizatio	n Email	Sta	rt Date End Date				

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

Create New UAA Profile									
User *	AIM Training User10 - xatraininguser10155123 🗸								
UAA Notes									
Environment	TEST 🗸								
Start Date *	i i i i i i i i i i i i i i i i i i i								
End Date *	i								
	Submit Cancel								

The new UAA will be able to access AIM as a UAA after about 30 minutes.

To add what applications and what organizations this newly created UAA needs to be allowed to provision/endorse access to, please proceed to <u>How to Add Contract and Authorized Entities to</u> <u>Selected UAA</u>.

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.

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

- 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.

UAA Profile UAAs Users Applicati	tions Manage Certificates ACL Groups Access Request Endorsed Access Request Email Configuration	
First Name Last Name	Email Status Active 🗸	
Create New UAA Profile		
User Access Administrators		
● ▼ 協 結	Rows	10 🗸
Last Name – First Name User Id Notify AIM Org Short Name Orga	ganization Email Start Date End Date Status Cert Expiration Date Modified By Modified Date PROFILE AC	CESS
TRAINING UAA UTRAININGx16238		2
Note: Please assign required Contracts and Entities to t	the other UAA's using following 'Contracts' and 'Entities' drop down options	
VIAA Authorized Contracts		
Provisionable Contracts: WESTERN EIM PORTAL - ENTITY - Western EIM	M Portal for EIM Entity SC V Add Contract to Selected UAA	
Authorized Contracts: UAA TRAININGx16238	Authorized Contract Associated Applications:	
×	5 注	
Contract Type	Application Application Name Role Entity Type	
WESTERN EIM PORTAL - ENTITY - Western EIM Portal for EIM Entity SC	WEIMPORTAL Western EIM Portal site ENTITY READ ONLY EXTERNAL	
VIAA Authorized Entities	_ /	
Provisionable Entities: Add Entity to Selected U		
Authorized Entities: UAA TRAININGx16238	OM_ENTITY_NAME: PACE_TO	
έX	多 Δ 淮	
Entity Entity Type	ACL Group Name Description Environment Start Date End Date Status Assets	

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. Please not that automated notifications are not sent when a UAA Profile is approaching Expiration.

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

California ISO Stoping a Receved Fatre												
UAA Profile	UAAs	Users	Applications	Manage Certificates	ACL Groups	Access Reque	st Endor:	ed Access Requ	est Email Configuration	on		
First Name		Last Name		Email		Status Active	•					
Create New UAA Profile												
User Access Administrators												
多 🖌 🖄 注											Rows	10 🗸
Last Name First N	ame User Id	Notify All	Org Short Name Or	ganization	Email	Start Date	End Date	Status Cert Exp	piration Date Modified By	Modified Date	PROFILE /	ACCESS
							12/31/2023	Active				
							02/15/2024	Active			6	C2
							10/27/2024	Inactive			ß	C2

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

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

User Profile	UAA Profile
Emp No	UAA ID
Account Type	Weekly Expiry Email
User ID	Notes
First Name	Start Date
Last Name	End Date
Organization	Undeted By
Email	opdated by
Phone Number	Updated Date
Address 1	
Address 2	User Certificates

3. Extend the date as deemed appropriate and select update to save changes.

User Profile	UAA Profile
Ø	Update Cancel 😋
Emp No	UAAID
Account Type	Weekly Expiry Email
User ID	Notes
First Name	07/07/0000 tt
Last Name	Start Date 0//2//2023
Organization	End Date 10/27/2024
Email	Updated By
Phone Number	Undated Date
Address 1	
Address 2	User Certificates
City	User Gertineates

UAA Profile – Landing Page

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

Shaping a	Renewed Future		emeni			
UAA Profile	UAAs Users Ap	plications Manage Certificates A	CL Groups Access Reques	t Endorsed Access Request	Email Configuration	
erence to the AIM User Guide		Link to AIM User Gui	de			
AA Status	Contact Info	Organization				
1	Ø	Ø				
A ID	User ID First Name	Org Short Name				
ekly Expiry Email Yes	Last Name	Address1				
t Date	Organization	Address2				
	Phone Number	State				
Default to "Ves"		Postal Code				
Delault to Tes		Phone				
ndorsed Users w	/ithout Access		Endorsed l	Jser(s) waiting for acc	ess	
) 🖓 🖄 📒 🔰 🖣 1	- 0 of 0 🕨 🕨 🔼 🤇	50 L				
ndorsing Org UserID Last Nar	me First Name Comment Requester Name	Requester Email Requester Phone				
	× No Data found					_
	-		Authorized Con	tracts shows UAA wh	at they can provision	
uthorized Contra	cts	2 3 -			at any samplement	
ntract Type		Application Application Name	Role	Entity Type		
ESTERN EIM PORTAL - ENT	ITY - Western EIM Portal for EIM Entity 9	C WEIMPORTAL Western FIM Portal s				
		TEIMI ONTAL TRACTICIMIT ONUT				
uthorized Entity	Entity:		Rims Projects	s Entity:		
≸⊟	多人 祥		Project Code Pro	oject Name F	Project Type Queue Number IC	Legal En
tity Type	ACL Group Name Description Environ	ment Start Date End Date Status A	ssets	مراجع والمعار والمعار والمعار		
	×	No Data found		rofile will display othe	er UAAs and their	
			A	luthorized Entities an	d Contracts	
Other UAAs In My	Organization	Authorized Entities for	the UAA	Authorized Contract	s for the UAA	
२४ फि ा = ¶ ¶ 1	- 0 of 0 🕨 🕨	io ≥ ∀ 🗧 🖣 🖣 0 - 0 of	0 0 00	≥∀☆ = 4 4 0 -	0 of 0 🕨 🕨 😡	
	- FT			* * LA - 14 4		
irst Name as	t Name - Email	Entity 🔶	Type 🔶	Contract Type		
rst Name Las	st Name 🔶 Email	Entity 2	lype	Contract Type		
rst Name Las	st Name Email	Entity 🚖	Гуре	Contract Type		

Customer Services and Stakeholder Affairs

California ISO	Technology	ISO Version:	4.5
Access and Identity Management (AIM) User Guide		Effective Date:	01/29/2024

Best Practices

- 1. Must review the ISO User Access Administrator Establishment and Requirements.
- 2. Organizations <u>should</u> 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 <u>not</u> 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 <u>must</u> 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.

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

12. A RIMS application user can only have <u>one</u> role type per environment.

Roles	Roles for Application: New Resource Interconnection Management System					
🥖 🗙 :	✓ X ☆ Y 函 < < 1 - 10 of 12 < >					
Role ID	Display Name 🖉	Description	External	Agreement Check?	Role Conflicts With	
292	EXTERNAL AFFECTED SYSTEM READ-WRITE	External Affected System Read- Write	Yes	No		
295	EXTERNAL IC READ-ONLY	External IC Read-Only	Yes	No	INTERNAL ADMIN EXTERNAL IC READ-WRITE	
294	EXTERNAL IC READ-WRITE	External IC Read-Write	Yes	No	INTERNAL ADMIN EXTERNAL IC READ-ONLY	

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.

05/21/2020 09:09:11	
Employee:	Application: RIMS; Environment: Map-Stage; Role EXTERNAL IC READ-ONLY and EXTERNAL IC READ-WRITE are conflicting. Please remove one to continue.

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.

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.

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

- 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.

UAA Profile UAAs Users Applications Manage Certificates ACL Groups Access Request Endorse	d Access Request	Email Confi
New Request History		
Request ID Request By (UserId): From Updated Date: To Updated Date:		
Access Request History		
Req ID Requested By Requested By User Id Description Updated Date Status		
PROCESSED		
Access Request Details		
多 ▲ 図 注	_	
Queue ID Last Name 🛧 First Name 🛧 CN User ID Action Environment Application Role Entity	Status No	otes
	COMPLETED	
	COMPLETED	

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:

California ISO	Technology	ISO Version:	4.5
Access and Identity Management (Effective Date:	01/29/2024	

1. Please click on the **Email Configuration** tab. Select applicable Certificate Events. Example in screen shot below is "Application Access Request." Then click on the pencil icon under the **Email List semicolon separated** panel.

UAA Profile UAAs	Users Applications Manage Certificates ACL Gro	ps Access Request	Endorsed Access Request	Email Configuration
Email Notification Events				
Y 1				
Scenario	Description			
APPLICATION_ACCESS_REQUEST_CONTENT	Application Access Request			
CERT_RENEWAL_CONTENT	Certificate Renewal from UI			
RENEW_USER_CERT_CONTENT	Renew User Certificate from UI			
REVOKE_USER_CERT_CONTENT	Revoke User Certificate from UI			
CREATE_NEW_USER_CONTENT	Submit a New User from UI			
AIM_USERS_CERT_EXPIRY_CONTENT	Notification for certs expiring within 30 days, 60 days, 90 days and new users			
REVOKE_USER_CERT_CONTENT	Automatic User Revocation Email			
Email List semicolon separat / · · · · · · · · · · · · · · · · · · ·	ed			

2. Click the **New Row** button under the **Email List semicolon separated** box.

UAA Profile UAAs	Users	Applications Manage Certificate	S ACL Groups	Access Request	Endorsed Access Request	Email Configuration
Email Notification Even	ts					
🗟 🖌 😰						
Scenario	Description					
APPLICATION_ACCESS_REQUEST_C	ONTENT Application Access Re	equest				
CERT_RENEWAL_CONTENT	Certificate Renewal	from UI				
RENEW_USER_CERT_CONTENT	Renew User Certificat	te from UI				
REVOKE_USER_CERT_CONTENT	Revoke User Certifica	ate from UI				
CREATE_NEW_USER_CONTENT	Submit a New User fr	rom UI				
AIM_USERS_CERT_EXPIRY_CONTEN	T Notification for certs e	expiring within 30 days, 60 days, 90 da	ys and new users			
REVOKE_USER_CERT_CONTENT	Automatic User Revo	cation Email				
Email List semicolon se	parated					
New row Update	Cancel Ca					
Additional EMails						

- 3. A free text field will be activated. Please list applicable email recipients separated by semicolon in this field.
- 4. When your list is finalized, please click on the **Update** button under the **Email List semicolon separated** panel.

UAA Profile	UAAs	Users	Applications	Manage Certificates	ACL Groups	Access Request	Endorsed Access Request	Email Configuration		
Email Notifica	Email Notification Events									
€ 7 🕅										
Scenario		Description								
APPLICATION_ACCESS	S_REQUEST_CONTE	NT Application Acce	ess Request							
CERT_RENEWAL_CON	ITENT	Certificate Ren	ewal from UI							
RENEW_USER_CERT_	CONTENT	Renew User Ce	rtificate from UI							
REVOKE_USER_CERT	CONTENT	Revoke User Ce	ertificate from UI							
CREATE_NEW_USER_	CONTENT	Submit a New U	Iser from UI							
AIM_USERS_CERT_EX	PIRY_CONTENT	Notification for o	erts expiring within 3	0 days, 60 days, 90 days a	nd new users					
REVOKE_USER_CERT	CONTENT	Automatic User	Revocation Email							
Email List semicolon separated Update Cancel X No Data found										
				38						

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

 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 <u>on your</u> <u>keyboard</u>. 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.

	◆ → २ ₽ →
ŧ	Goes to the previous display in browsing history
	Goes to the next display in browsing history
STOP	Stops loading the current display
3	Refreshes the display in the current window
Q	Zoom out
÷	Zoom in
1	Log out

Filter Toolbar – User Access Tab

The filter toolbar contains the account filtering options.

User ID		First Name Last Name	Email Status	[ALL]	_	Certificate Expiration Account Type	[ALL] [ALL]	V	Apply	Reset
	Apply		Refreshes user da	ta with	the filte	rs				
	Reset		Restores filters to	defaul	t setting:	6				
* wildcard search Use the asterisk (*) wildcard symbol to search for user information. (Enter Chris * in the First Name field and click the Apply button to d list of users whose first names begin with "Chris". The search results display users who are named Chris, Christopher, Christine, etc.) To that you see all records meeting your search criteria, add the "*" at the display multiple records.					n. (e.g. o displa ults will To ensu it the er	ay a ure nd to				

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

Results Window

	★ ▼ 🖷 🖶
×	Restore sort to default setting (removes user-created multiple column
- *	sorting, which is described in detail on the following page)
Y	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 *UAA* or UAA will provide the same results.)
	Exporting (to Excel, Word, CSV)

Results Window – Multiple Pages

	【 ▲ 101 - 200 of 225 ▶ ▶				
M	Navigate to the first page of data				
•	Navigate to the previous page of data				
•	Navigate to the next page of data				
	Navigate to the last page of data				
	Go to specific line item entered in search box				

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: 1. The following icon appears in the second column: 2. 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: 3.
- Click the same column again. The data is sorted in descending order. The icon in the column header is changed to: ³ .
- Continue to click column headers to deselect and then reprioritize the sorting order.

California ISO	Technology	ISO Version:	4.5
Access and Identity Management	Effective Date:	01/29/2024	

The following image shows the example explained above:

Users 🖈 🍸 🗎 (-					
Last Name	1 First Name	🔶 UserID	<mark>- 3</mark> Email	Status	Cert Expiration Date	PROFILE ACCESS
Training POC	AIM	xatrainingpoc1	40071 TNgo@caiso.com	Active	10/31/2014	
Training User1	AM	xatraininguser11	40072 TNgo@caiso.com	Active	10/31/2014	C C
Training User2	AIM	xatraininguser21	40073 TNgo@caiso.com	Active	10/31/2014	
Training User3	AIM	xatraininguser31	40074 TNgo@caiso.com	Active	10/31/2014	d d
Training User4	AIM	xatraininguser41	40075 TNgo@caiso.com	Active	10/31/2014	

Export Menu

	Export All		
	Export Page		
	Export Wizard		
Export All	All data points will be exported to Excel		
Export Page	The current page will be exported to Excel		
Export Wizard	The user can customize the data export		

Export Wizard

The Export Wizard enables the user to export data in the following three file types:

- Export Excel
- Export CSV
- Export Word

Export Type Export E	xcel 🚽 Export			
Grid 1: Users Export C	scel SV			
Column Name	Vord visplay Name	Visible	Column Width	
Last Name	Last Name	v	84	
First Name	First Name	1	84	
UserID	UserID	1	67	
Email	Email	1	127	
Organization	Organization	1	127	
Status	Status	1	42	
Cert Expiration Date	Cert Expiration Date	1	63	
Account Type	Account Type	\checkmark		Rows to Export All Rows 💌

California ISO	Technology	ISO Version:	4.5
Access and Identity Management (AIM) User Guide		Effective Date:	01/29/2024

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.