Customer and Asset Management System (CAMS)
User Guide for Company and Affiliate Maintenance

Version 1.14

2024

ISO New England Inc.

About this user guide

The Customer and Asset Management System (CAMS) User Guide is grouped into independent sections arranged by topic and user role. It is not necessary to read the guide from beginning to end.

You may:

- Select a topic from the How to: list on page 9
- Start with an Overview on page 10
- Select a CAMS Roles from the table of contents or from the list.

CAUTION

- Company names and any numerical values are fictitious and not to be associated with any actual market participant.
- Though we strive to maintain this guide current, the screen views in this guide may not fully reflect the current production environment.

Change Summary

Revision	Date	Comments
Version 1.0	August 3, 2012	Initial release
Version 1.1	October 23, 2013	Updated screen shots for CAMS 2013 upgrade; removed the Index section; added application and role descriptions for NX Application in the Reference Tables.
Version 1.2	March 7, 2014	Added Subaccount section. Made other revisions to describe new functionality in CAMS, particularly the Export Person Detail Report function.
Version 1.3	August 28, 2015	Additional updates made to the Subaccount information section.
Version 1.4	July 29, 2016	Added Banking Information section. Added Asset Ownership Share Transfers section.
Version 1.5	August 22, 2018	Updated information related to Ask ISO Manager.
Version 1.6	August 27, 2018	Updated customer service email hyperlink.
Version 1.7	April 9, 2019	Updated screens shots for CAMS Upgrade
Version 1.8	October 2, 2019	Updated screens shots for CAMS Upgrade Phase 2
Version 1.9	April 22, 2021	Remove contact type descriptions. Contact type descriptions will be maintained in CAMS. Remove application group role descriptions. Group role descriptions are maintained in the Customer Asset Management System Application Group Roles document.
Version 1.10	October 5, 2021	Asset Ownership Share Transfers section now points to Asset Registration webpage
Version 1.11	February 1, 2022	Updated Committee section for ELS project
Version 1.12	February 2, 2023	Updated for ELS Phase 3 release: Changes to Committees, Persons, Contacts New section for Mailing Lists

Version 1.13	July 28, 2023	Updated the roles and descriptions in section 3. Added information for managing international phone numbers (add person and update person). Removed fileshare section as they are now managed as application access. Added new process for delete person (reassign contacts screen).
Version 1.14	January 25, 2024	Updated for MIS Data Delivery: Changes to Add Person, Managing MIS Accounts, Person Subaccount Mapping

Table of contents

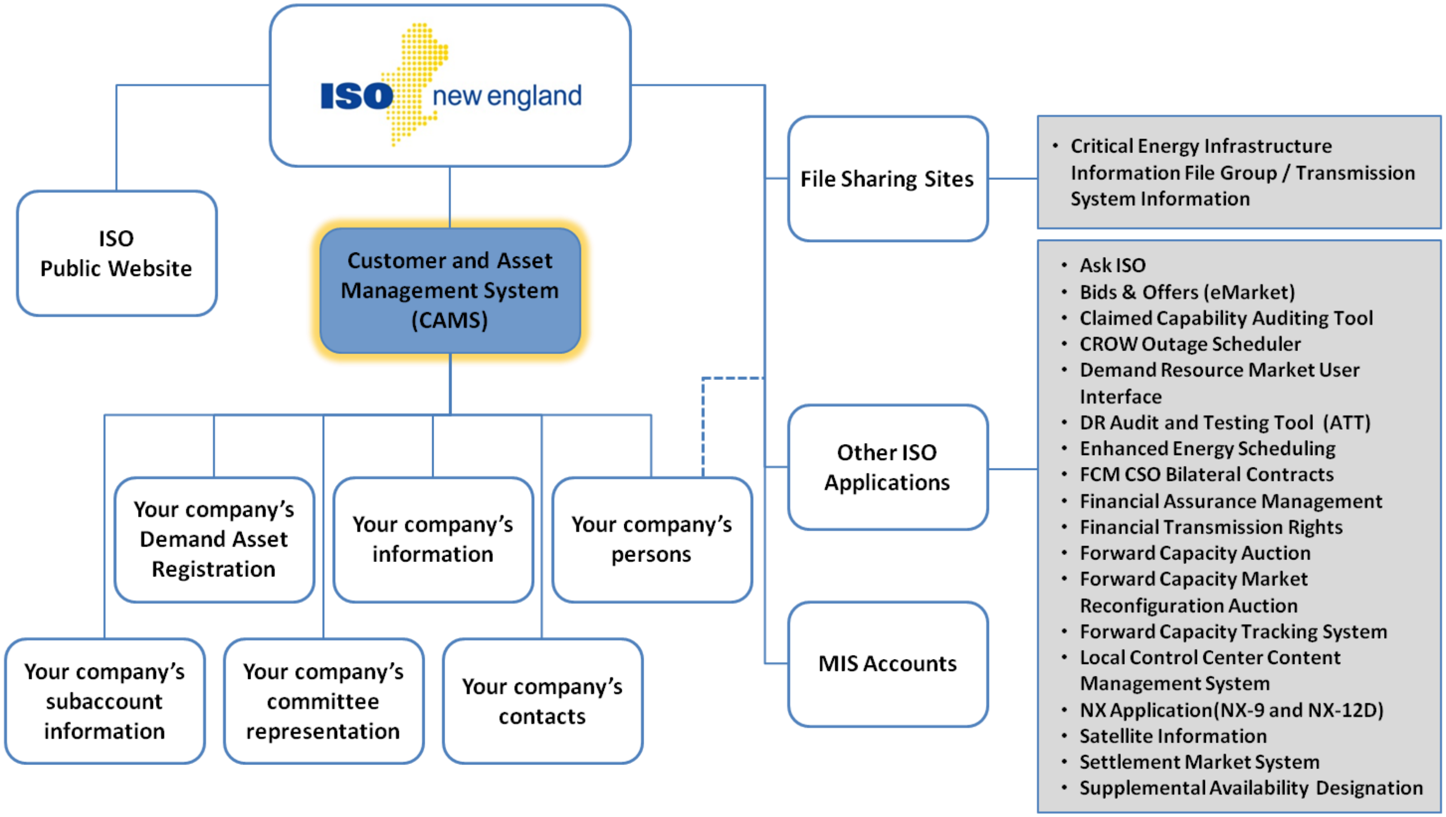
1 What is CAMS?

The Customer and Asset Management System (CAMS) is ISO New England's administrative database of record. It stores, maintains and manages all customer data and facilitates, as well as the registration of Demand Assets and Resources.

CAMS is available to customers as an internet-based tool for:

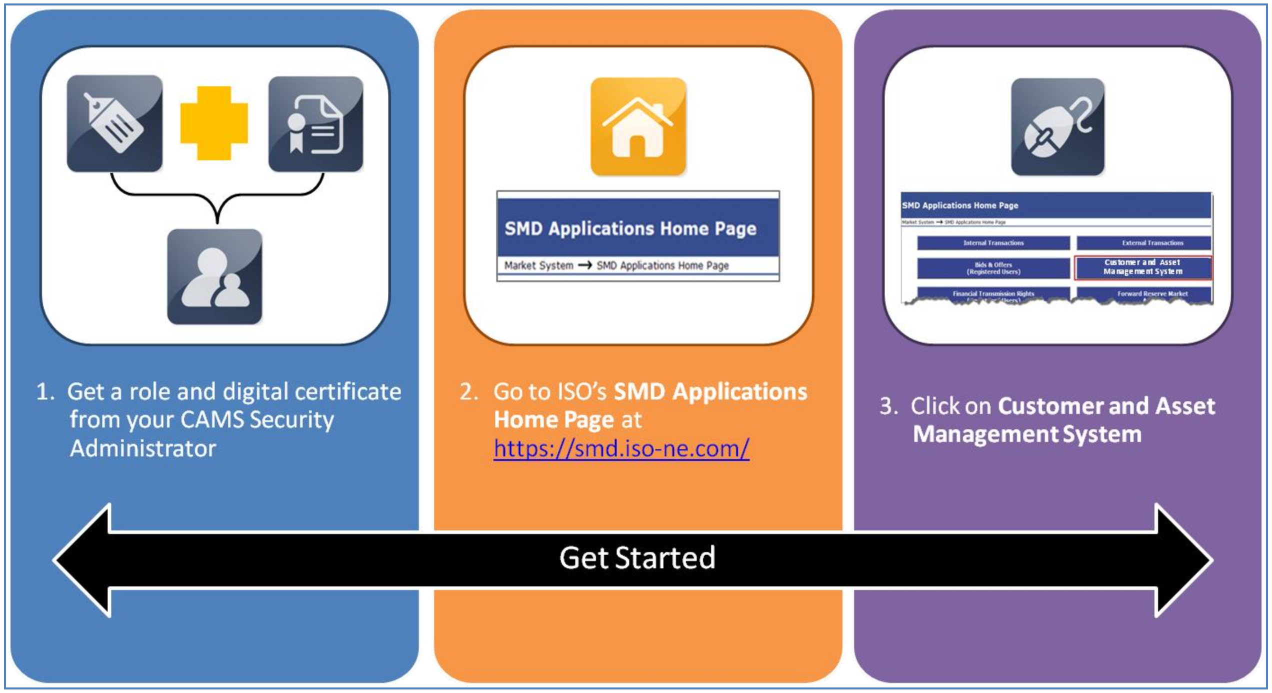
- Managing your company contacts (see "Contacts")

- Managing your committee representation (see "Committees")
- Granting users access to other ISO internet-based applications (see "Granting a person access to CAMS or another ISO application")
- Updating your company information (see "Manage your Company's Information")
- Managing your company's subaccounts (see "Subaccount information")



2 How to:

2.1 Get started



This section applies to the following CAMS roles:

✓ All roles

This section covers the following topics:

2.1.1 Overview

2.1.1.1 CAMS Security Administrators

- To use CAMS, a company must first designate at least one individual to be a CAMS Security Administrator (SA).
- New members designate an SA during the membership application process to ISO New England.
    - If your company does not have an SA, or would like to designate another SA, complete, notarize and return the *ISO New England Security Administrator Signatory Page* located on ISO New England's website at:

      https://www.iso-ne.com/static-assets/documents//support/custsvc/forms/iso_ne_security_admin_sig_page.pdf.
        - A company officer signs the form and it is notarized. Incomplete forms will not be processed. The original form, including notary stamp or seal, must be mailed to the address noted on the form.
- An SA is responsible for assigning roles in CAMS and issuing digital certificates to users. For details see the "Manage your company's persons" section on page 16.
    - For details on the SA role see "Security Administrator" on page 179.
    - For details on all roles in CAMS see Section 3.0 "CAMS Roles"

2.1.1.2 CAMS Persons and Roles

- Users are known in CAMS as "Persons".
- To access CAMS, a person must first be entered into the CAMS database by an SA. See "Adding persons to CAMS" on page 17.
- The person must then be assigned at least one role and issued a digital certificate by the company's SA.
    - A *role* is a defined set of allowable activities in CAMS or another ISO New England application.
    - A *digital certificate* is an electronic key to the ISO New England websites that host CAMS and other applications. A person cannot access any ISO application without a digital certificate.
    - Digital certificates are automatically issued the first time a person is assigned a role in CAMS.
        - For details on assigning roles and issuing digital certificates by Security Administrators, see "Manage your company's persons" on page 16.
        - Digital certificates must be renewed annually.
        - For further details including issuing, renewing, and installing digital certificates, see the CAMS User Guide for Digital Certificates which is available by contacting Participant Support.
- For details on all roles in CAMS see Section 3.0 "CAMS Roles"
- For details on roles in other ISO applications see the Tab: "Application Group Roles" in Customer Asset Management System Application Group Roles

2.1.1.3 Online CAMS Frequently Asked Questions

- See the "Customer and Asset and Management System (CAMS)" section on ISO New England's website FAQ page, located at https://www.iso-ne.com/participate/support/faq/cams.

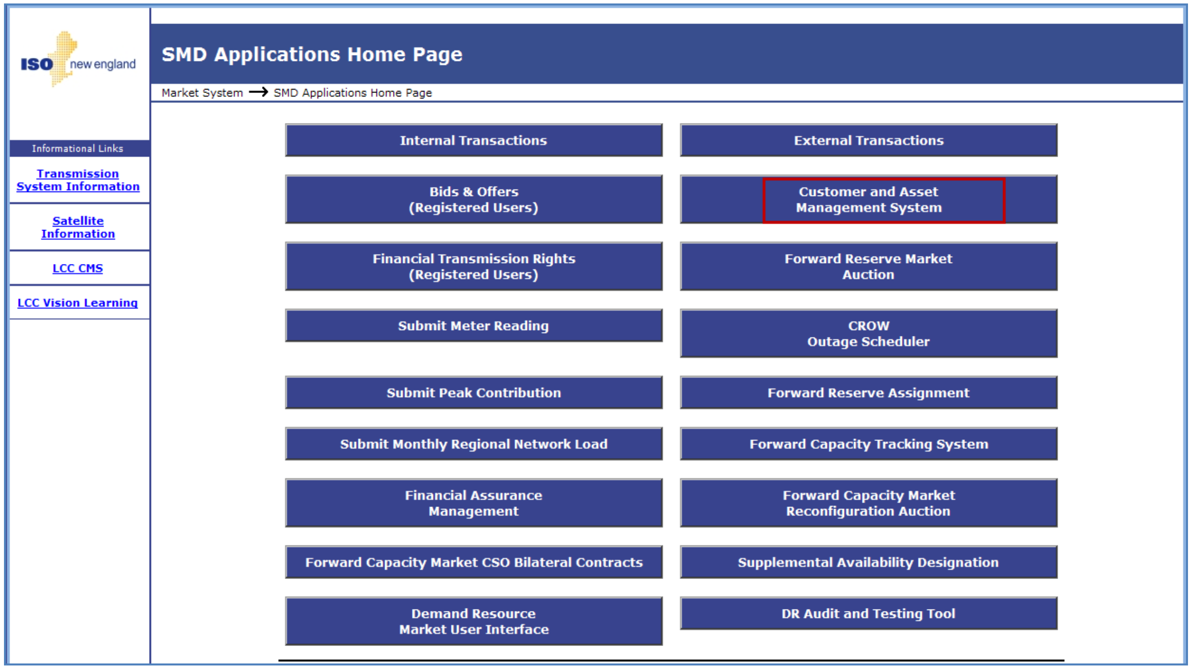
2.1.1.4 ISO New England Glossary and Acronyms

- For a full list of ISO New England terms and acronyms, see the Glossary and Acronyms listing on ISO New England's website at:
- https://www.iso-ne.com/participate/support/glossary-acronyms.

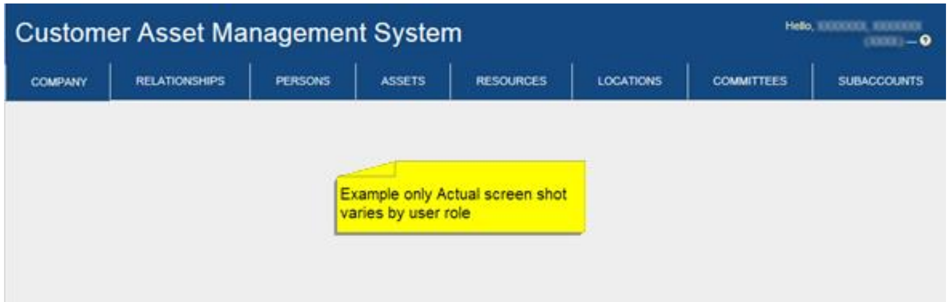
2.1.2 Accessing CAMS

I have a CAMS role and have installed my digital certificate. How do I access CAMS?

1. Navigate to the ISO SMD Applications Home Page at: https://smd.iso-ne.com/.
2. Click on "**Customer and Asset Management System**":



3. The CAMS homepage displays:



4. See the "How to:" list for details on the task you want to perform.

I do not have a CAMS role or have not installed a digital certificate. How do I access CAMS?

To get a CAMS role and digital certificate:

1. Contact your company's CAMS Security Administrator (SA) to request access to CAMS.

    a. To learn who at your company is an SA, contact ISO New England Participant Support at (413) 540-4220 or via email at **askiso@iso-ne.com**.

2. Your SA will assign you at least one specific role in CAMS. See the "CAMS Roles" section for details of each CAMS role.

3. Your SA will issue you a digital certificate if you do not already have one.

4. ISO New England will email you instructions for installing the certificate on your computer.

    a. See "Install a digital certificate" in the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA.

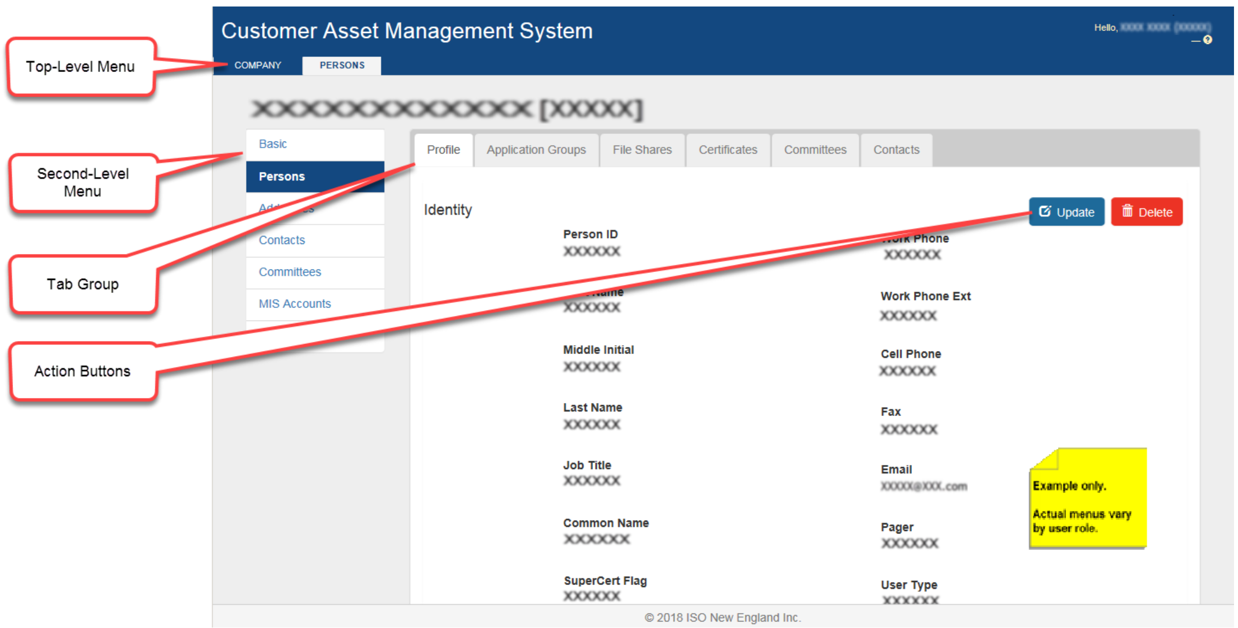
    b. You will need the "PIN #" or "Pickup Password" from your SA to complete the installation process.

5. After you have installed your digital certificate, go to the "Accessing CAMS" section.

IMPORTANT

❖ It may take up to two hours for the system to implement a new CAMS role.

2.1.3 CAMS User Interface



- The CAMS interface uses a hierarchical menu structure.

- Click on a *top-level menu* to reveal second-level menu options.
- Click on a *second-level menu* option to reveal additional *tab groups*, depending on the task you are intending to perform.
- *Action buttons* appear based on the application group roles that have been assigned.

- All menu selections are based on your individual user role or roles in CAMS.
- Menus and functionality that do not pertain to your role(s) will not be displayed.
- For details on the different CAMS roles, see the "CAMS Roles" section on page 179.

2.2 Manage your company's persons

This section applies to the following CAMS roles:

- ✓ Security Administrator
- ✓ External Person Maintainer
- ✓ External Person Viewer

This section covers the following topics:

2.2.1 Overview

- A "person" in CAMS is defined as:

- an individual who is associated with a company.
- an individual who has been granted access to CAMS, another ISO application, or a file sharing group.

- To perform any task related to a person, whether making the person a contact for your company or granting access to an ISO application, the person must be entered into the CAMS database (see "Adding persons to CAMS" on page 17).
- Only a Security Administrator (SA) can add a person to CAMS.
- Only an SA can grant a person access to CAMS, or another ISO application.
- Only an SA can create MIS accounts.

What if a person who is listed in CAMS leaves my company or is terminated?

The SA must take the following steps in the following order:

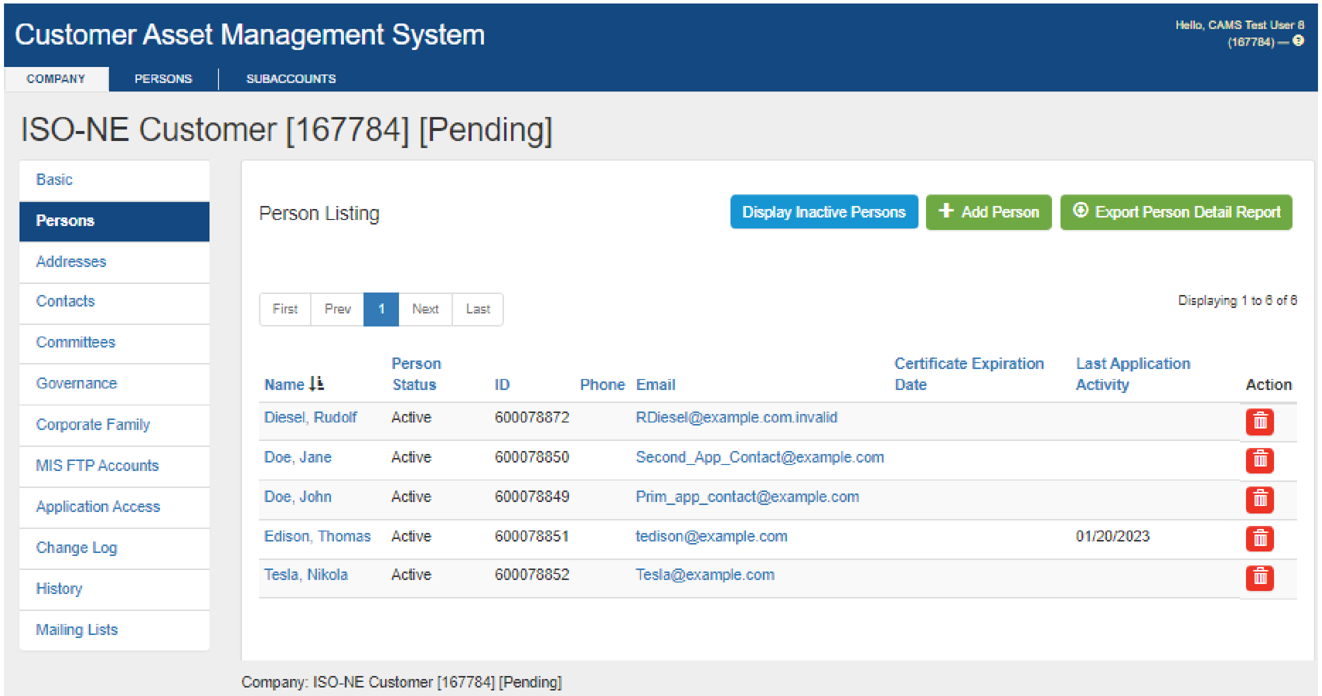
1. If applicable, remove the person's access to any ISO New England application.

   See "Removing or modifying a person's access to an application" on page 26. You do not need to take any action regarding the person's digital certificate.
2. If applicable, remove the person's contact listing. See "Delete contact information"
3. If the person has a committee assignment, remove the person's name from the committee. See "Update a committee" and "Delete individual committee assignment"
4. Delete the person from CAMS. See "Deleting persons"

2.2.2 Adding persons to CAMS

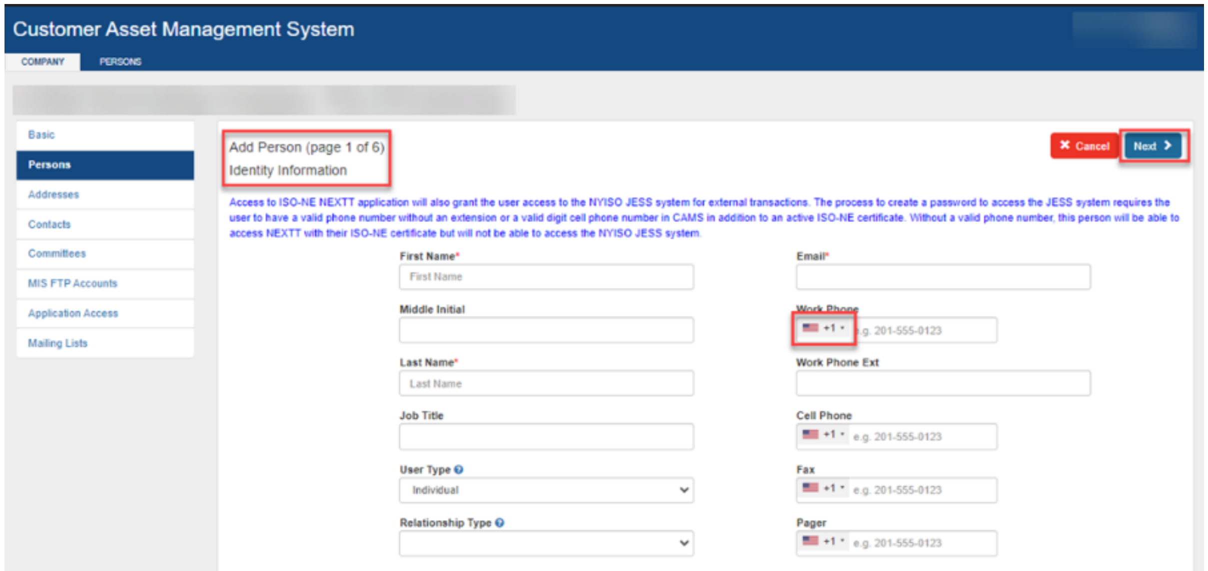
- Role that can perform this task:
  - Security Administrator

1. Launch the CAMS interface. See the "Accessing CAMS" section.
2. Click on the top-level "Persons" tab or on the second-level "Persons" tab if it is open.
3. The "Person Listing" screen displays:



4. Click the “Add Person” button.

5. The “Add Person – Identity Information” screen displays:



6. Enter the person’s information. First name, last name and email address are required. For phone numbers outside of North America, select the relevant country from the drop down then enter the phone number.Click “Next”.

7. Select the User Type to designate individual, desk or device. This indicates how the user and credentials will be used. Most CAMS person records should be individuals. Granting application access to specific individuals minimizes the risk of unauthorized access to digital certificates. The desk and device user types should be limited to those scenarios where a shared resource is needed.

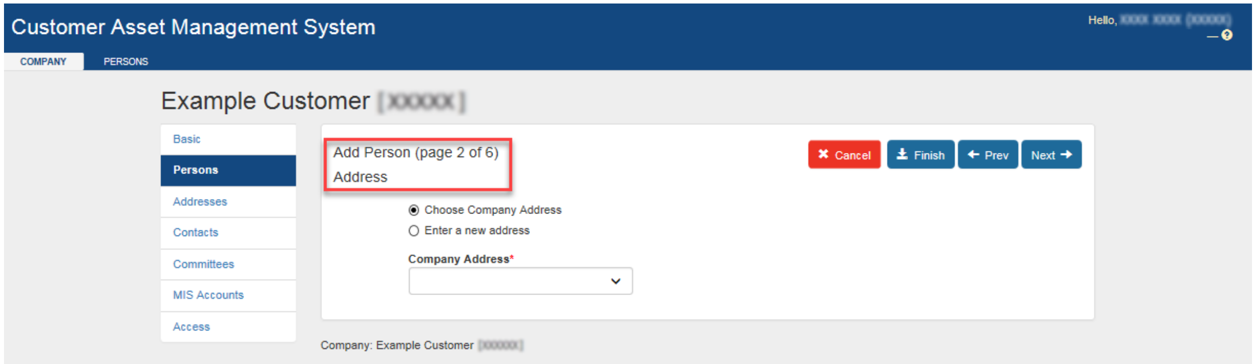
8. Select Relationship Type from the drop-down menu
   a. *Employee*: A person record that the participant directly manages. For individuals, this may include full-time, part-time, and contract (temporary) employees. The SA should select this relationship type for device/application or desk/department records where the participant directly manages the credentials.

   b. *Client*: A person record at an organization other than the participant's that uses the participant's products or services. They are usually only allowed access to specific subaccounts as assigned by the SA.

c. *Consultant*: A person who provides professional advice or services to the participant. An example is legal services, where a participant assigns the Legal Representation contact type to an individual from a law firm. Another example is a consultant who represents the participant at a committee and might be assigned a committee seat for that participant.

d. *Vendor*: A person at an organization that provides primarily software or application-based services to the participant. Adding this type of individual to CAMS is common for software or application services where a vendor needs credentials to configure the system for the participant (e.g., an application that downloads reports from the SMD Applications or the MIS FTP Server, or a system that supports a participant's bids and offers process). The entity type here may be individual, but it might also be a device/application if the credentials are used to configure the application on the server as a shared resource.

9. The "Add Person - Address" screen displays:



10. Choose an existing company address for the person from the drop-down box, or enter a new address by selecting the "Enter a new address" radio button.

11. If you want to grant the person access to CAMS or another ISO application, click "Next" and continue with the "Granting a person access to CAMS or another ISO application"

12. If you want to add the person without assigning an application role, click "Finish".

13. Review the information summary and click "Submit".

2.2.3 Granting a person access to CAMS or another ISO application

IMPORTANT

- ❖ To grant a person access to an ISO application the person must first be entered into the CAMS database. See "Adding persons to CAMS" on page 17.

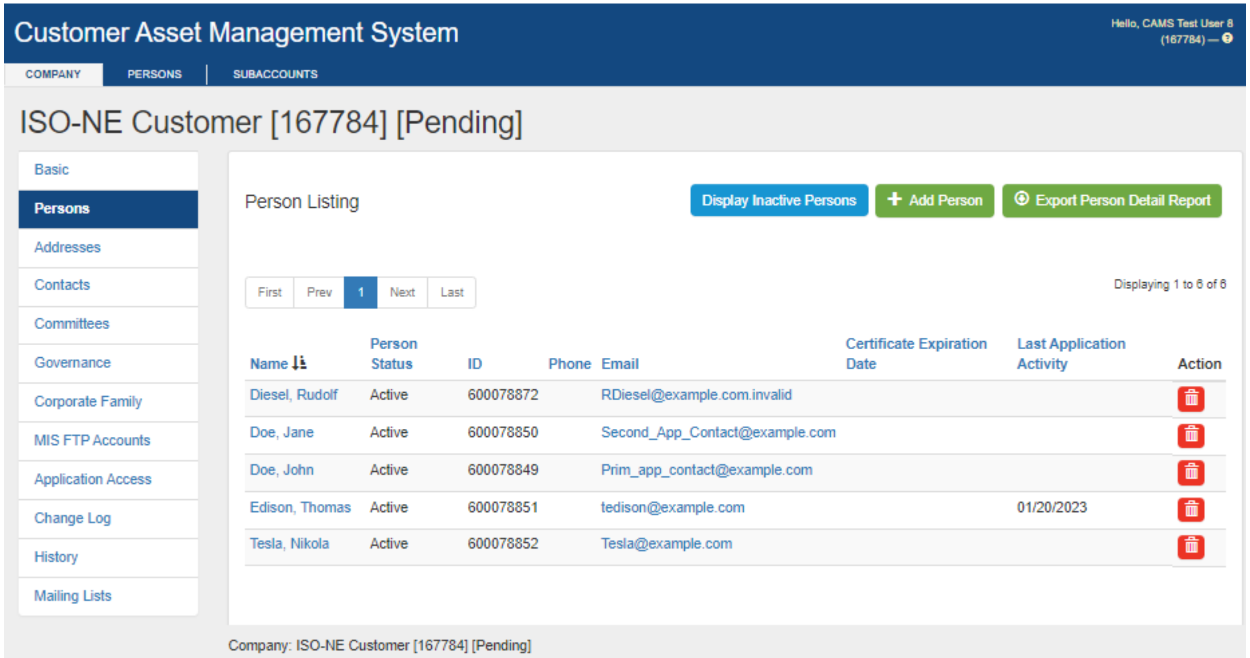
- Only a Security Administrator (SA) can grant a person access to ISO applications.
- An SA must assign the person at least one role in the application.
  - For details on all roles in CAMS see Section 3.0 "CAMS Roles"
  - For details on roles in other ISO applications see the Tab: "Application Group Roles" in Customer Asset Management System Application Group Roles
  - A person may have more than one role in an application, though there are some mutually exclusive roles.
- The person must have a digital certificate installed on his or her computer to access the site that hosts the particular ISO application.
- Digital certificates are automatically issued the first time a person is granted access to an ISO application.
  - See "Issue a digital certificate" in the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA.

To grant a user access to CAMS or another ISO application

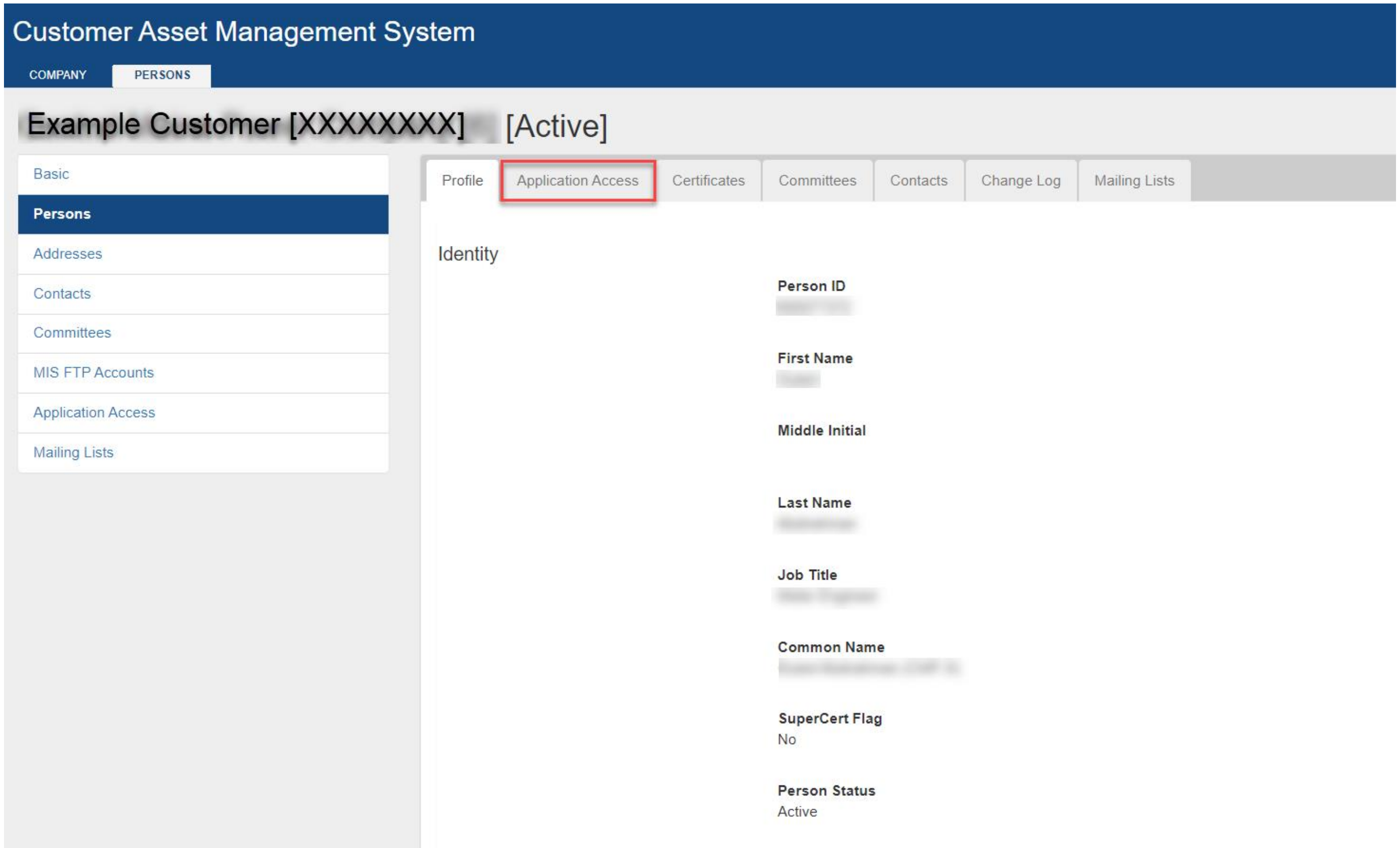
- Role that can perform this task:
  - Security Administrator

1. Launch the CAMS interface. See the "Accessing CAMS" section on page 11.

2. Click on the top-level “Persons” tab or on the second-level “Persons” tab if it is open.
3. The “Person Listing” page displays:

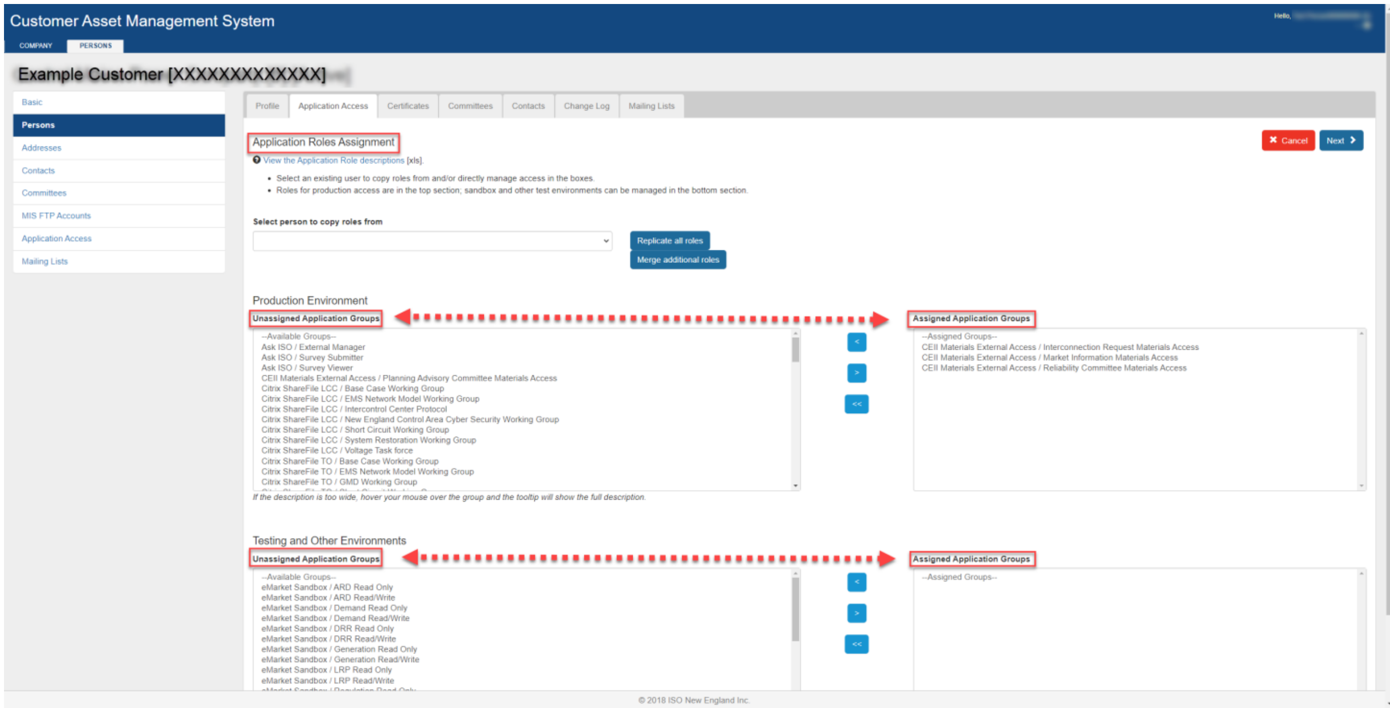


4. Click on the name of the person to whom you are granting access.
   a. If the person has not yet been entered into CAMS, and therefore does not appear in the list, you must first add the person by clicking “Add Person”. See “Adding persons to CAMS”
5. The “Profile” tab displays:



6. Click on the “Application Access” tab.
7. The “Person Application Access Listing” screen displays.
8. Click “Update” in the right corner of the screen.

9. The “Application Roles Assignment ” screen displays:



10. From the “Unassigned Application Groups” list boxes on the left, select the application group or groups you want to assign to the person. You may multi-select by holding down the shift key or the ctrl key while you click.

11. The CAMS roles are listed as “Customer Asset Management System / [role]”.

    a. For details on all roles in CAMS see Section 3.0 “CAMS Roles”
    b. For details on roles in other ISO applications see the Tab: “Application Group Roles” in Customer Asset Management System Application Group Roles

12. Click the Grant Access button between the two boxes to move your selections to the “Granted Access” box.

13. Click “Next”.
14. Enter the date you want the assignment(s) to take effect. The default is for the assignment(s) to be effective on the current day.
15. Click “Next”.
16. The “Application Access” tab displays showing the new assignments.
17. If the person has not already been issued a digital certificate, the new assignment(s) will initiate the process on the effective date entered. On that date, the person will receive an email from ISO New England with instructions for installing a digital certificate on his or her computer.
    a. As the Security Administrator, you will receive an email from ISO New England with a “PIN #” or “Pickup Password” for that person’s digital certificate.
    b. The user or person will need the “PIN #” or “Pickup Password” to complete the certificate installation.
    c. For details on installing a digital certificate see “Install a digital certificate” in the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA.
18. If the person has a valid certificate installed, instruct the person to navigate to the ISO New England site that hosts the application.
    a. For CAMS, go to https://smd.iso-ne.com/.
    b. For other applications, check Tab: “Application Application Access Information” in Customer Asset Management System Application Group Roles for the URL or Access Location.

IMPORTANT

- ❖ It may take up to two hours for the system to implement a new access and/or role(s).
- ❖ A person may have more than one role in a given application.
- ❖ Some roles are mutually exclusive, therefore granting greater access (i.e., to read/write or maintainer) or reducing access (i.e., to read-only or viewer) may require two steps: a removal of the current role and a subsequent addition of the new one.

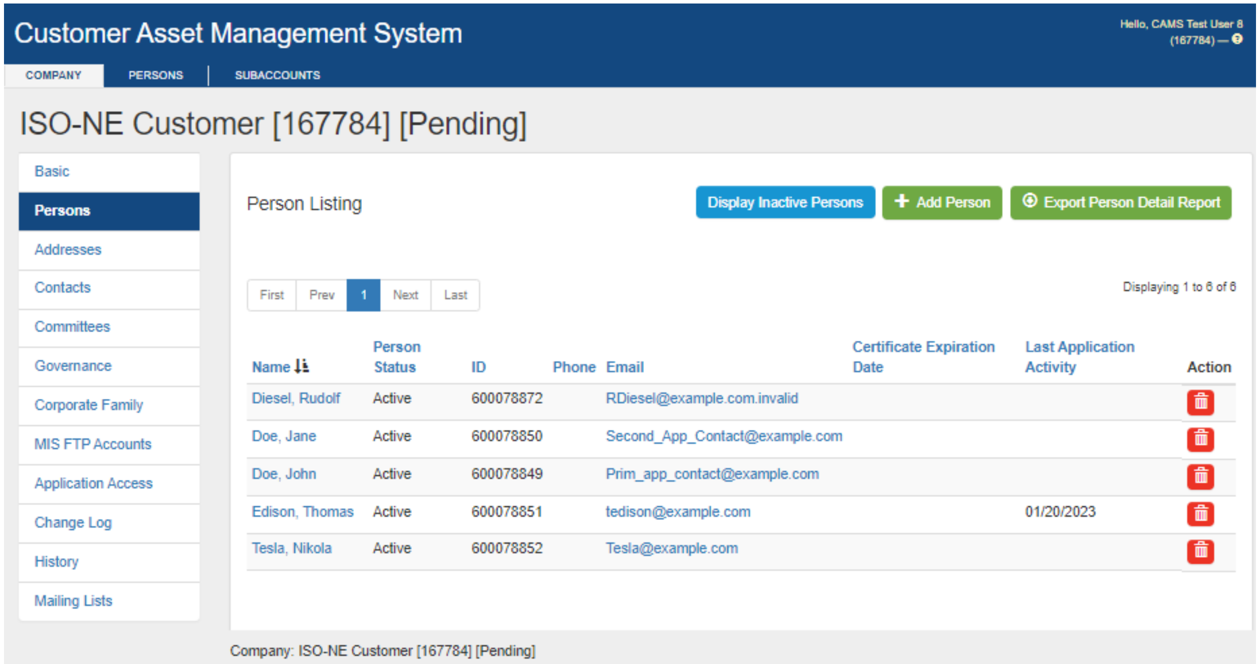
2.2.4 Removing or modifying a person's access to an application

To remove or modify a person's role and access to an application

- Role that can perform this task:
    - Security Administrator

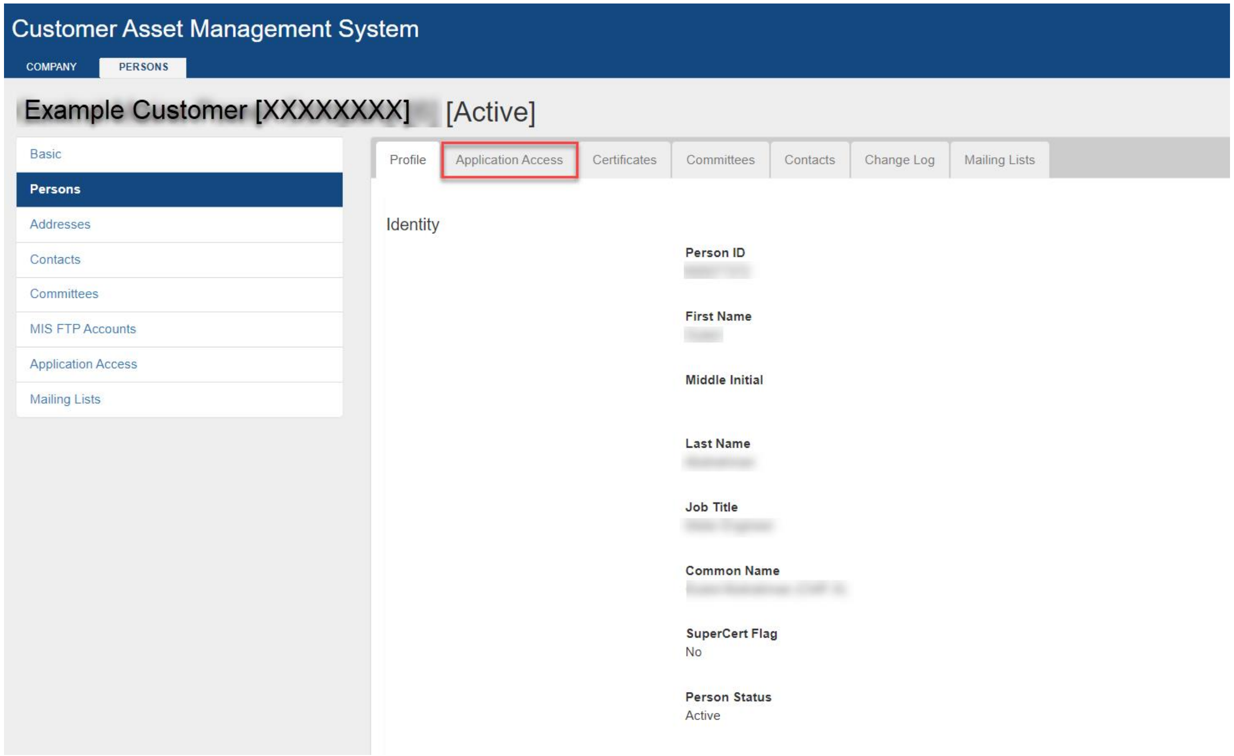
1. Launch the CAMS interface. See the "Accessing CAMS" section.
2. Click on the top-level "Persons" tab or on the second-level "Persons" tab if it is open.

3. The “Person Listing” page displays:

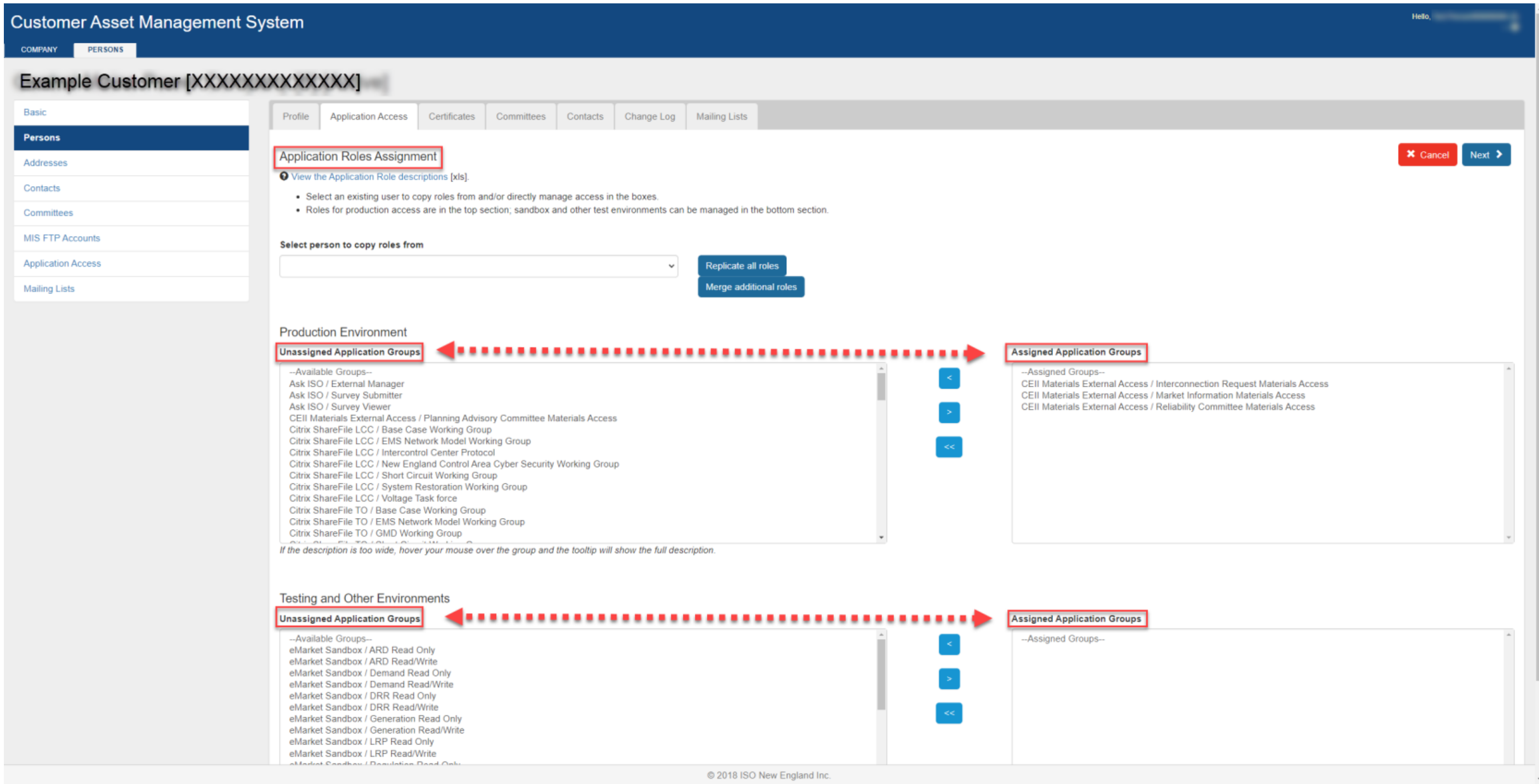


4. Click on the name of the person whose role you want to modify.

5. The “Person View” screen displays:



6. Click on the "Application Access" tab.
7. The "Person Application Access Listing" screen displays.
8. Click "Update" in the right corner of the screen.
9. The "Application Roles Assignment" screen displays:



10. From the “Assigned Application Groups” list boxes on the right, select the application group or groups that you want to remove. You may multi-select by holding down the shift key or the ctrl key while you click.

11. Click the Deny Access button between the two boxes to remove your selections from the “Granted Access” box to the “No Access” box.

12. Click “Next”.

13. Enter the date you want the removal to take effect under the “Date Expires” column. The default is for the assignment to expire on the current day.

14. Click “Next”.

15. The “Application Access” tab displays, showing the revised assignments.

IMPORTANT

- ❖ It may take up to two hours for the system to implement the removal.
- ❖ The person’s digital certificate is not affected by the removal of any role/access. You may add access and roles in the future.

2.2.5 Managing MIS Accounts

- Market Information Server (MIS) accounts are secure FTP repositories for company settlement reports, financial information, forecast and operational information, tariff reports and World Wide Web reports. For details see https://www.iso-ne.com/static-assets/documents/support/tech/rpt_descriptions/report_descriptions.pdf.
  - MIS FTP accounts are used to access the secure FTP server (or system) to retrieve MIS Reports.
  - There are two MIS account types: Legacy accounts, and user-assigned accounts.
    - Legacy
      - The MIS FTP Accounts feature in CAMS enables a company to create accounts for their FTP sites. Legacy MIS account access is provided during the membership registration process.
      - New customers should see their mentoring letter from ISO New England for the FTP account location.
      - Customers are asked to limit the legacy MIS accounts to scenarios where a shared resource is needed (e.g., an automated process) and that process benefits from deleting files that have been retrieved from the server. User-assigned FTP accounts are view-only so the reports will be available subject to the retention policy for each report on

the FTP server. Most automated processes should not need to delete the files, so user-assigned accounts are recommended.

  - Legacy FTP accounts are managed by the Security Administrators. The account contact assigned for the SA is more for reference and troubleshooting. If the SA wants the individual to have direct access to the username and password, including the ability to manage/reset the password directly, then a user-assigned account should be assigned instead.
  - Prior to granting access to transmission reports, please refer to your company's policies on access to transmission-related information.

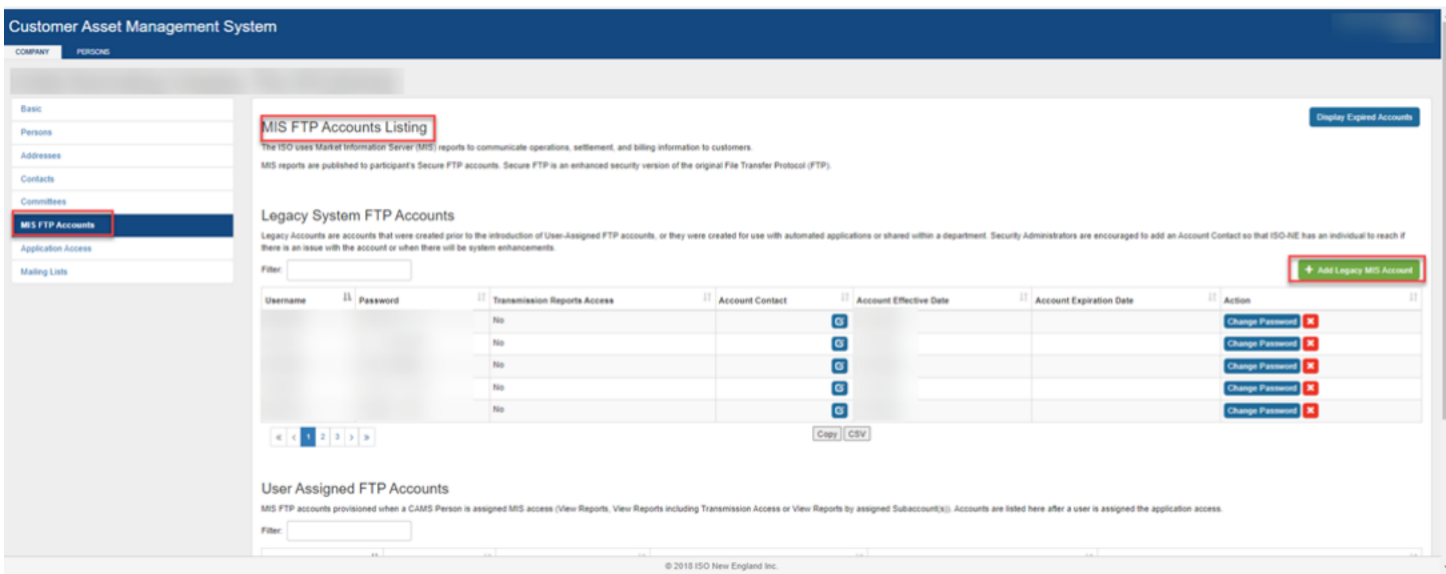
- User-assigned
  - User-assigned account access can be created at any time.
  - Create individual MIS FTP accounts specific to users; most of the time the CAMS Person will be an individual so this allows you to assign an MIS FTP account directly to an individual. Should there ever be an issue with an account, having directly assigned accounts makes resolving and troubleshooting issues easier.
  - The user-assigned access can view account information and change passwords.
  - Designed to afford the SA additional control and tracking, and reducing the need to share account information and passwords; less likely to result in interruption when an individual leaves. If the user had access to a legacy account, for example, a password change would have to be shared with everyone with access to that shared resource.
  - Three types of accounts that enable access to different information:
    - ***MIS/ View Reports including Transmission Access*** is unrestricted with transmission report access. This app group lets users see all subaccounts and transmission reports for their associated customers or assets.
    - ***MIS/ View Reports*** is unrestricted without transmission access. This app group allows users to see all reports in subaccount folders for their associated customer or asset but does not grant access to transmission reports.
    - ***MIS/ View Reports by Assigned Subaccount(s)*** restricts report access to specific subaccount access. This app group lets users see one or more folders containing subaccount reports. SAs map the authorized subaccount folders to the person.

2.2.5.1 To create a user ID and password for an MIS account

- Role that can perform this task:
    - Security Administrator

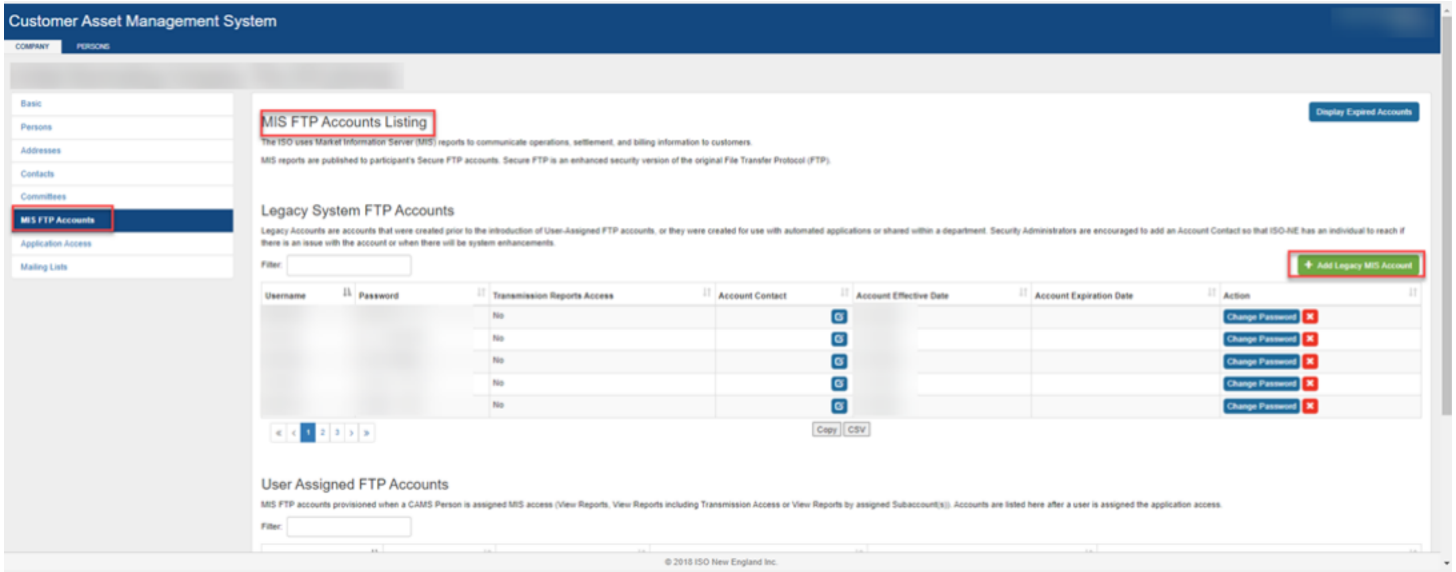
For Legacy MIS FTP Accounts:

1. Launch the CAMS interface. See the "[Accessing CAMS](#)"
2. Click on the "Company" tab to expose the second-level menu.
3. Click on the "MIS FTP Accounts" tab
4. The "MIS FTP Accounts Listing" page displays:



NOTE: If your company has access to transmission reports the "MIS FTP Accounts Listing" screen will also include a "Transmission Reports Access" column.

5. The "MIS – Account Insert" page displays:



6. Select an account contact from the dropdown. This contact will be notified if an issue is discovered with the account, or if upcoming upgrades may affect the account.
7. Enter the date you want the MIS Account to become active and click "Save".

NOTE: If your company has access to transmission reports, the "MIS – Account Insert" page will include a "Transmission Reports Access" check box.

a. When enabled, the following transmission reports are available:
   - Real Time Energy / Regulation (RTHS)
   - Special Real Time Metering Domain Report (RTUNMET)
   - Losses and External Tie Line Metering (OCLMETER)
   - Meter Adjustments (METERADJ)
   - Meter Domain (MTDOMAIN)

b. If you do not want this account to view transmission reports, leave the "Transmission Reports Access" check box clear.

8. The “MIS FTP Accounts Listing” page displays with the new accounts and passwords.
9. Distribute the user ID and password to staff at your company who require access to the MIS Accounts per your company’s IT guidelines or policies.

For user-assigned MIS accounts:

A. When adding a new person

Access the add person wizard:

1. On the Application Roles Assignment page (page 3), you can grant access to production or testing environments- select one.
2. Scroll down the list to app group MIS/___ (two access options will be available for all companies “view reports” and “view reports with transmission access.” If a company has active subaccounts in addition to the default subaccount, a third option will be available to assign “view reports by assigned subaccounts.” Select one. Only one active MIS application group can be assigned to a CAMS person at a time. Click next.
3. Set the effective date to today or a future date. Click next.
4. Create an MIS account username. User names must follow the requirements on screen.
5. The next screen (page 5) will vary based on access type.
6. For view reports or view reports by transmission access, the wizard will take you to the Add Contact Types screen next.
7. For view reports by assigned subaccount access, select at least one subaccount this entity is associated with. Proceed to the Contact Types screen. Click next.
8. Review the Summary page which displays all the data from the previous pages of the wizard. Verify all the information is correct.
9. Click Finish. This establishes a unique person account and will trigger an email from Global Sign to the email address entered for the new person.

B. When updating an existing person

1. Find the existing person’s profile.
2. Go to the Application Access tab. Click update.
3. In the Production Environment listing scroll down the list to app group MIS/__ (two access options will be available for all companies “view reports” and “view reports with transmission access.”
4. Select effective date of today or a future date.
5. Create a user name according to the parameters on the screen.
6. If appropriate based upon the application group assigned, select subaccounts.
7. Review the Summary page to verify all the information is correct.
8. Click Finish. A password is auto generated.

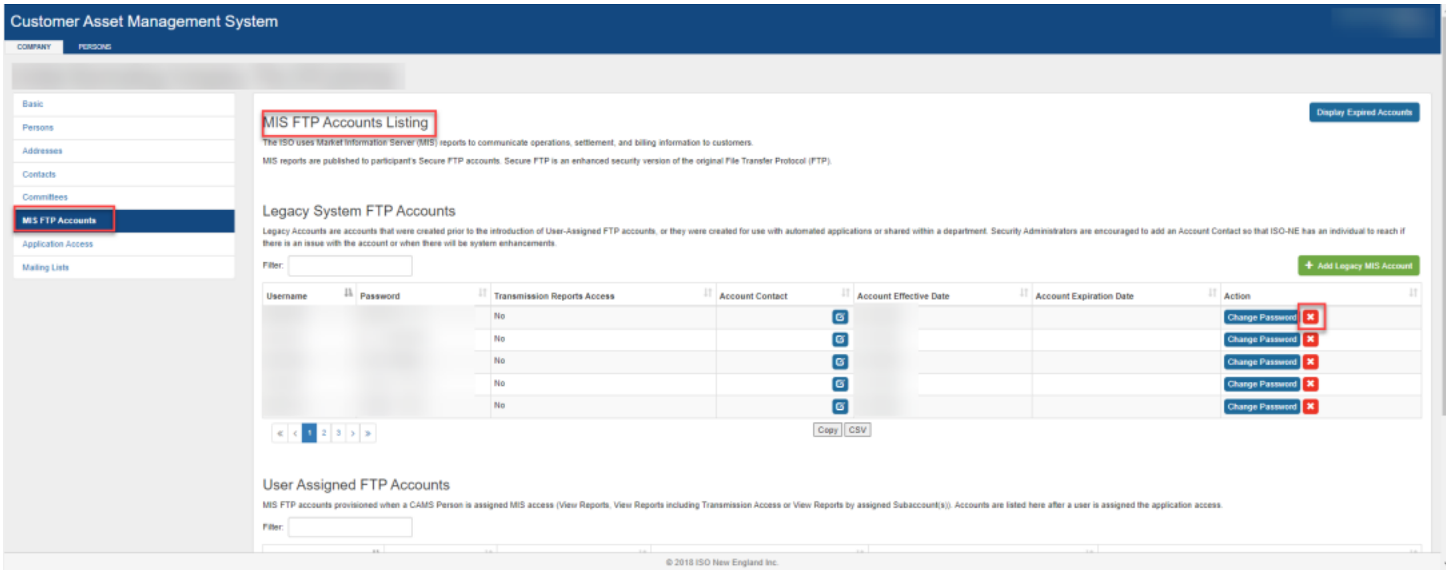
CAUTION

- ❖ Transmission reports contain sensitive data that only authorized and appropriate personnel at your company should view.
- ❖ Prior to granting access to transmission reports, please refer to your company's policies on access to transmission-related information.
- ❖ Once reports are deleted from a MIS account, they cannot be readily retrieved without having to be restored by ISO IT staff. Customers are encouraged to store copies of the reports and develop mechanisms to distribute the reports to all staff requiring access.

2.2.5.2 Delete a MIS account

- Role that can perform this task:
  - Security Administrator

1. Launch the CAMS interface. See the "Accessing CAMS" section.
2. Click on the "Company" tab to expose the second-level menu.
3. Click on the "MIS FTP Accounts" tab:



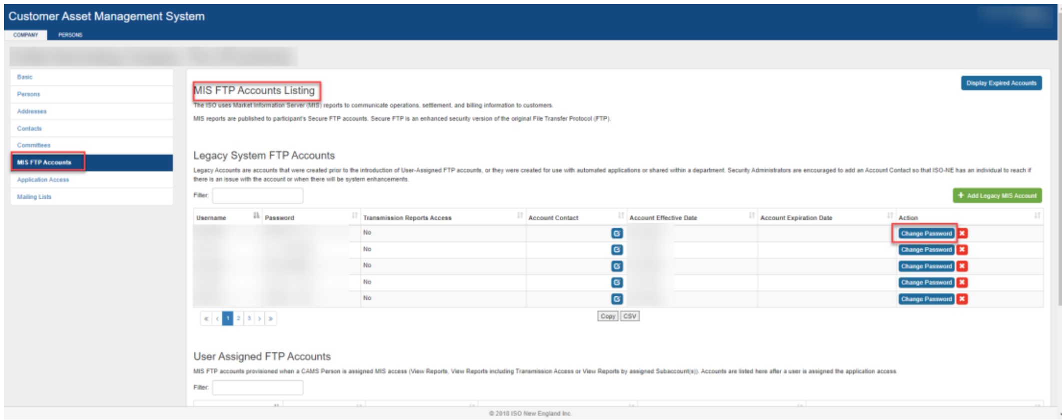
4. In the “MIS FTP Accounts Listing” page, click on the ‘**X**’ icon in the “Action” column for the appropriate user ID and password that needs to be deleted.
5. The “MIS – Account Expire” page displays.
6. Enter an expiration date for the user ID and password.
7. Click the “Submit” button.
8. The “MIS FTP Accounts Listing” page displays with the expiration date.

2.2.5.3 To change the password for an existing MIS account

- Role that can perform this task:
  - Security Administrator
  - CAMS Person, if given a user-assigned MIS FTP account

1. Launch the CAMS interface. See the “Accessing CAMS”

2. Click on the “Company” tab to expose the second-level menu.
3. Click on the “MIS FTP Accounts” tab:



4. In the “MIS FTP Accounts Listing” page, click on the “Change Password” button in the Action column for the appropriate user ID and password that needs to be modified.
5. The “MIS – Account Change Password” page displays.
6. Click “Generate New Password”.
7. The “MIS FTP Accounts Listing” page displays with the new system-generated password for the selected account.
8. Distribute the new password to appropriate staff at your company per your company’s IT guidelines or policies.

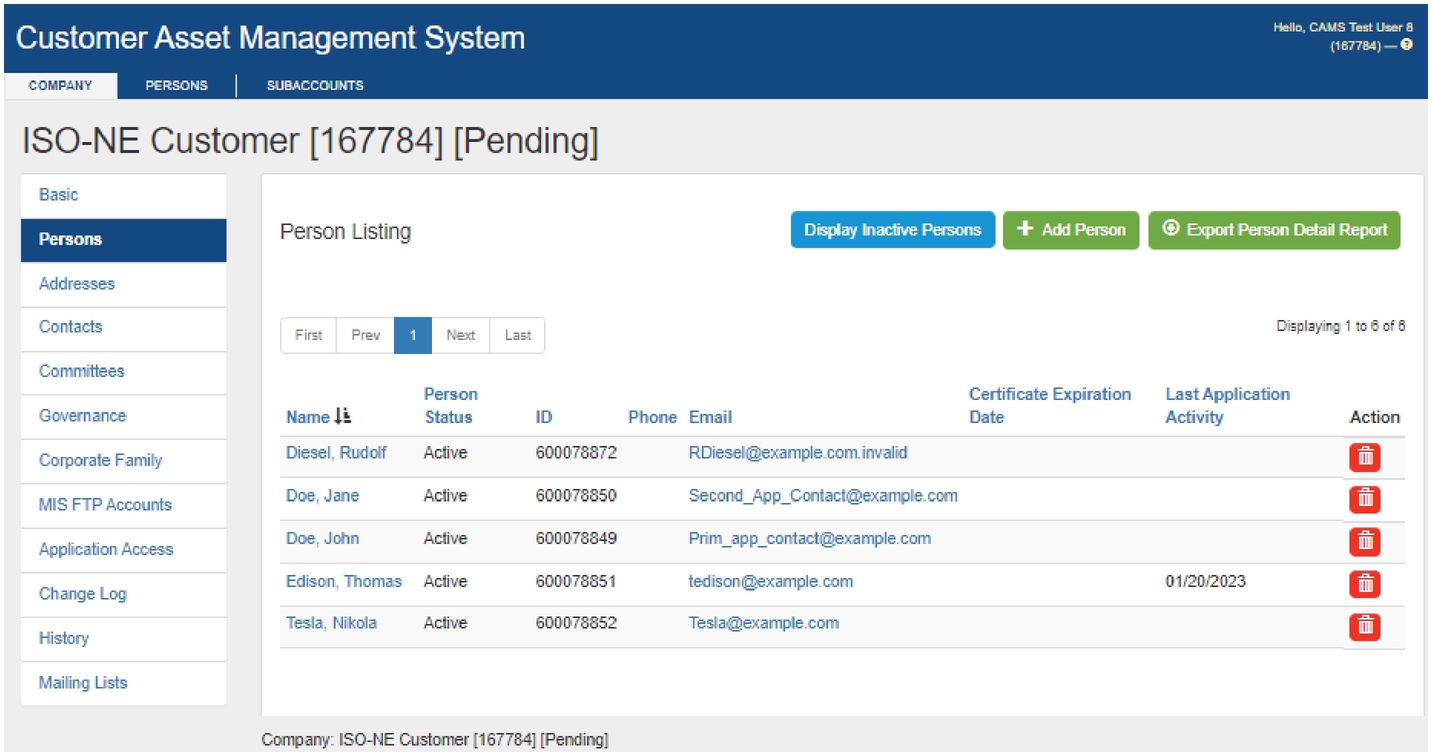
2.2.6 Viewing persons

- A customer’s person records can be viewd at the customer level or at the individual level.

2.2.6.1 View customer person listing

- Roles that can perform this task:
  - Security Administrator
  - External Person Maintainer
  - Exterma Person Viewer

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on the top-level "Persons" tab or on the second-level "Persons" tab if it is open.
3. The "Person Listing" page displays.



- The "Person Listing" page features the following actions and information:
  - Display inactive persons – a function that displays person records that have been deleted.
  - Add Person – see "Adding persons to CAMS"
  - Export Person Detail Report – see "Retrieving your company's person detail report"
  - View person details - see "View person detail"

- Email links – emails are displayed with mailto: links.
- Certificate expiration date – this sortable column provides a broad view of when user's certificates will expire – see "Granting a person access to CAMS or another ISO application".
- Last application activity – this sortable column provides the date on which the user last accessed an application in the Standard Market Design applications page (e.g., eMarket, NEXTT, IBT, Meter Readings).
- Delete Person – see "Deleting persons".

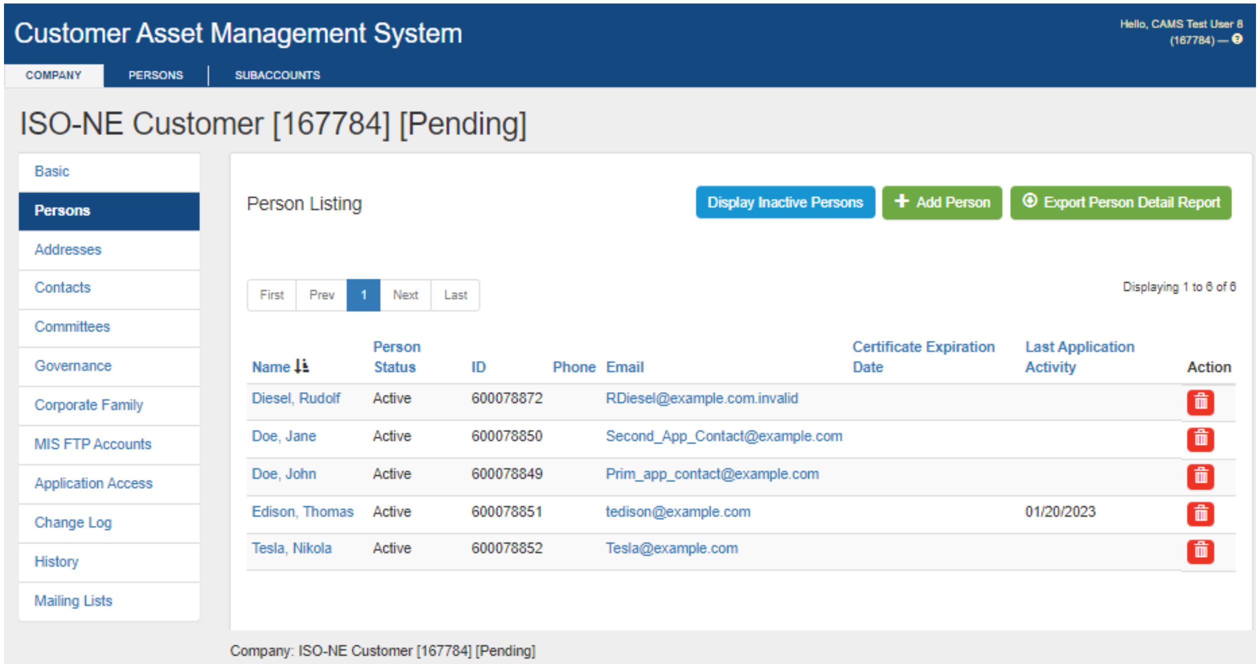
2.2.6.2 View person detail

To view person's information

- Roles that can perform this task:
  - Security Administrator
  - External Person Maintainer
  - External Person Viewer

1. Launch the CAMS interface. See the "Accessing CAMS" section.
2. Click on the top-level "Persons" tab or on the second-level "Persons" tab if it is open.

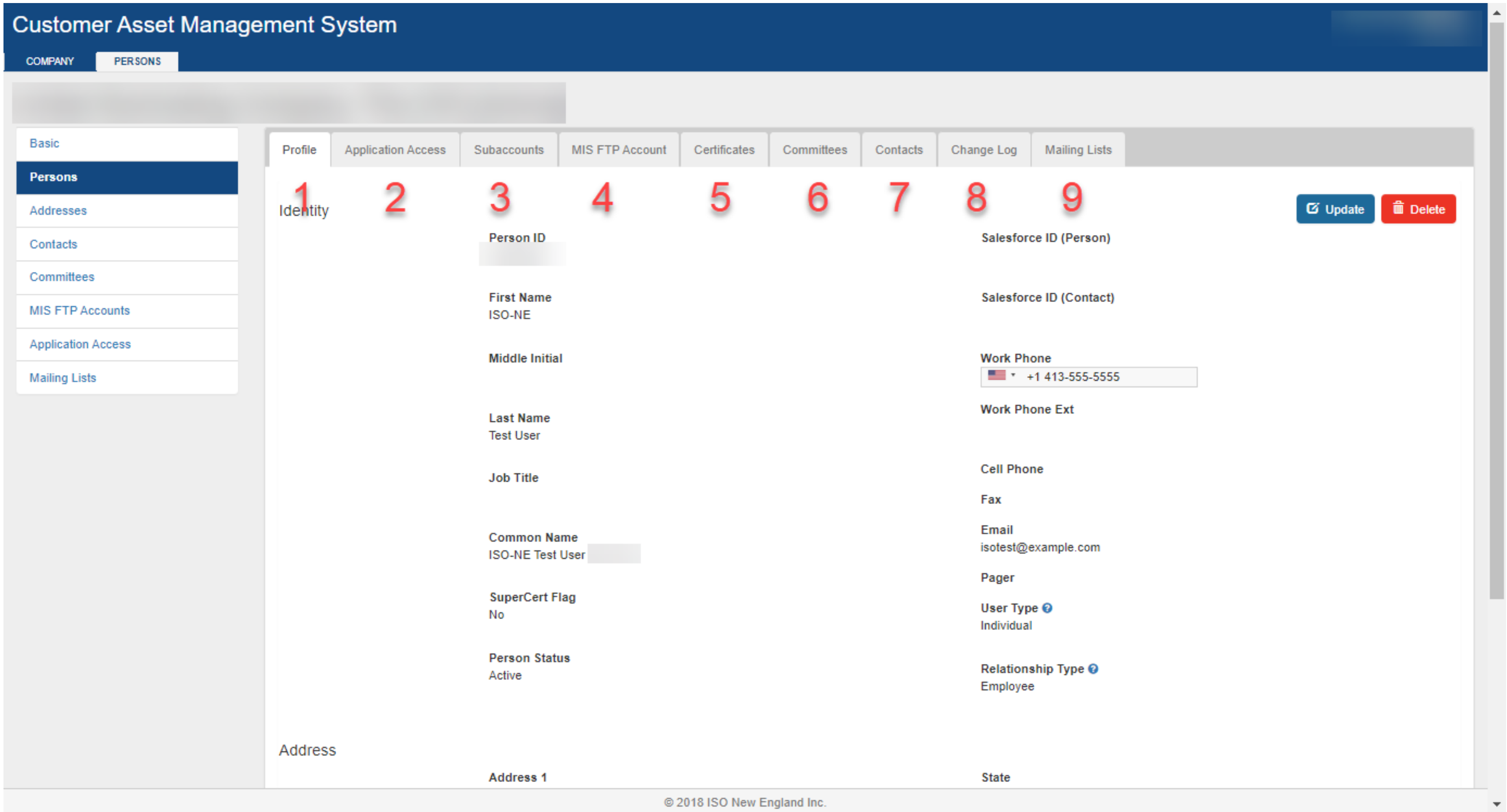
3. The “Person Listing” page displays:



4. Click on the name of the individual person whose record you wish to view.

Tab group summary

The person detail screen in CAMS contains seven tab groups, allowing you to perform a number of tasks, all from one screen:



1. Profile – displays general information specific to the person.

2. Application Access – view and manage person's access to ISO applications – see "Granting a person access to CAMS or another ISO application".

3. Subaccounts – view and manage person's Subaccount mappings – see "Person Subaccount Mapping"

4. MIS FTP Account – view and person's MIS FTP Account – see "Managing_MIS_Accounts For User-Assigned MIS Accounts"

5. Certificates – view and manage person's digital certificates – see "Granting a person access to CAMS or another ISO application".
6. Committees – view person's committee assignments and mailing list preference– see "Committees".
7. Contacts – view and manage contact assignments – see "Contacts".
8. Change Log – view historical changes to the person record.
9. Mailing Lists – view person's mailing list memberships – see "Mailing List".

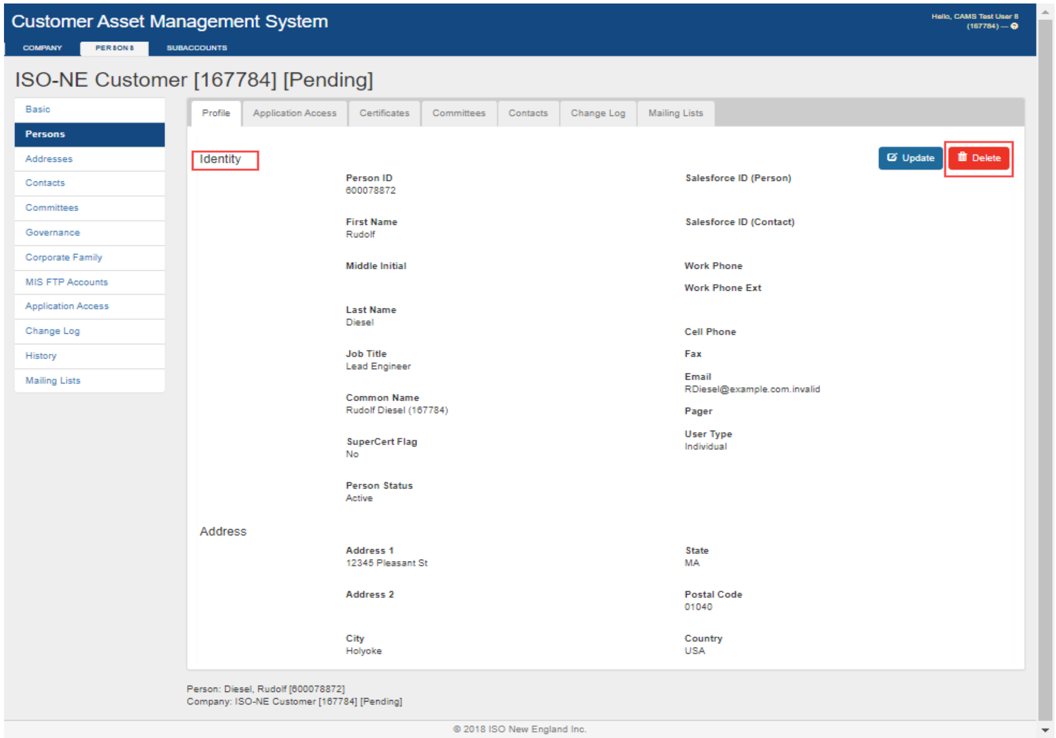
2.2.7 Deleting persons

To delete a person from CAMS

- Roles that can perform this task:
    - Security Administrator
    - External Person Maintainer

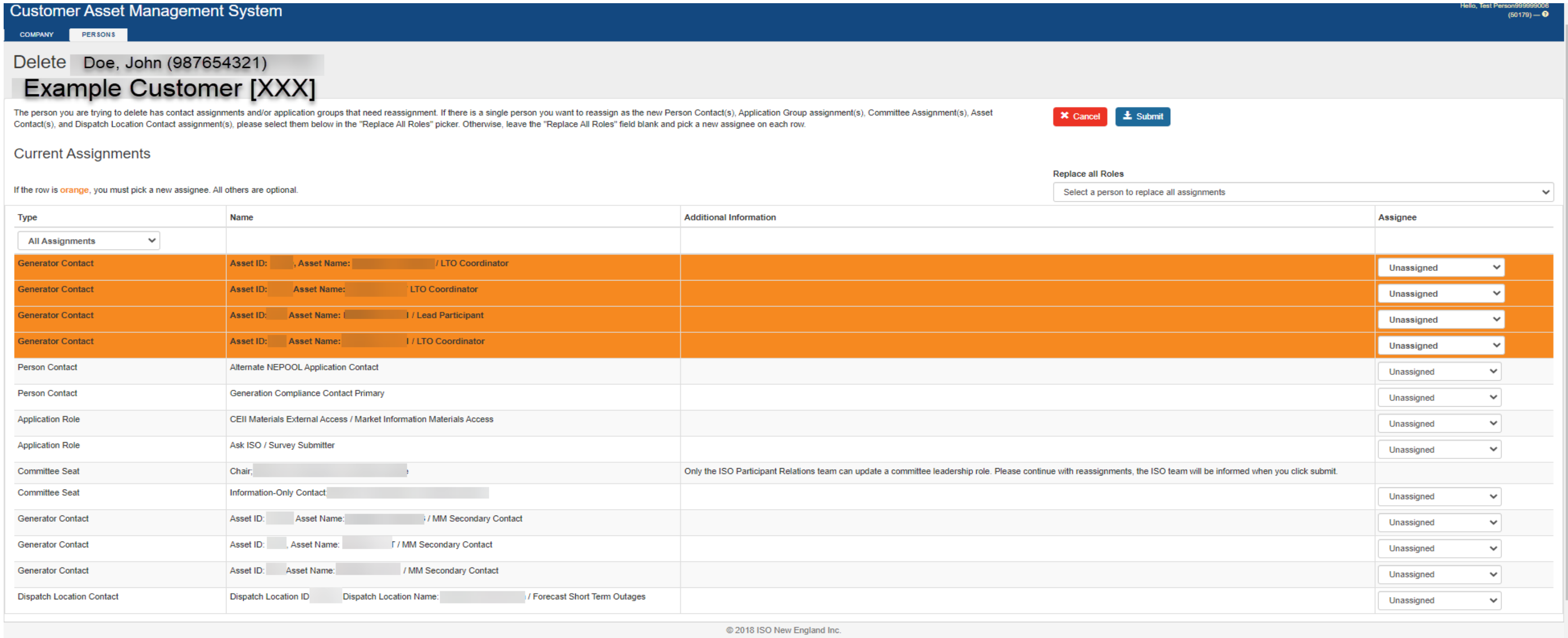
1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on the top-level "Persons" tab or on the second-level "Persons" tab if it is open.
3. The "Person Listing" page displays.
4. Click on the name of the person you want to delete.

5. The “Person View” screen displays:



6.Click the “Delete” button.

7.The contact reassignment screen displays all of the person contacts, application access, committee assignments, generator contacts and dispatch location contacts that are assigned to the person being deleted.



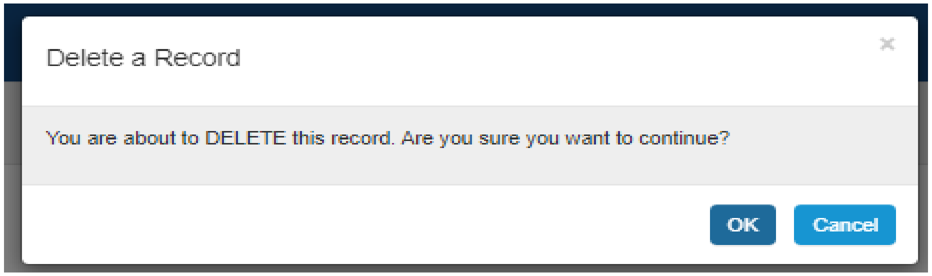
10. Select a person from the assignee dropdown to reassign a contact. Records highlighted in orange require replacement. Records not highlighted are optional. Instead of selecting individual assignees for each contact type, you can select one person from the "Replace all Roles" dropdown to reassign all the contacts to a person.

11. Click "Submit" once all required contacts have an assignee selected and any optional assignments are reassigned. Upon successful submittal, the reassignments will be assigned to the new assignee and the person will be deleted.

    Notes:

    - Application Access can only be reassigned by the External SA. If you are a Person Maintainer trying to delete a person with Application Access assignments, reach out to your SA to expire or reassign the access so you can proceede with person deletion.
    - Leadership can only be reassigned or expired by the ISO. Click "Submit" on the reassignment screen when leadership assignments exist. The ISO will be notified and help reassign or expire the leadership assignment so you can proceede with person deletion.

- If a person does not have any contacts assigned to them, then the reassignment screen will not display. Instead, a pop-up will appear asking to confirm that you want to proceede with person deletion. Click "OK" to continue with deletion.



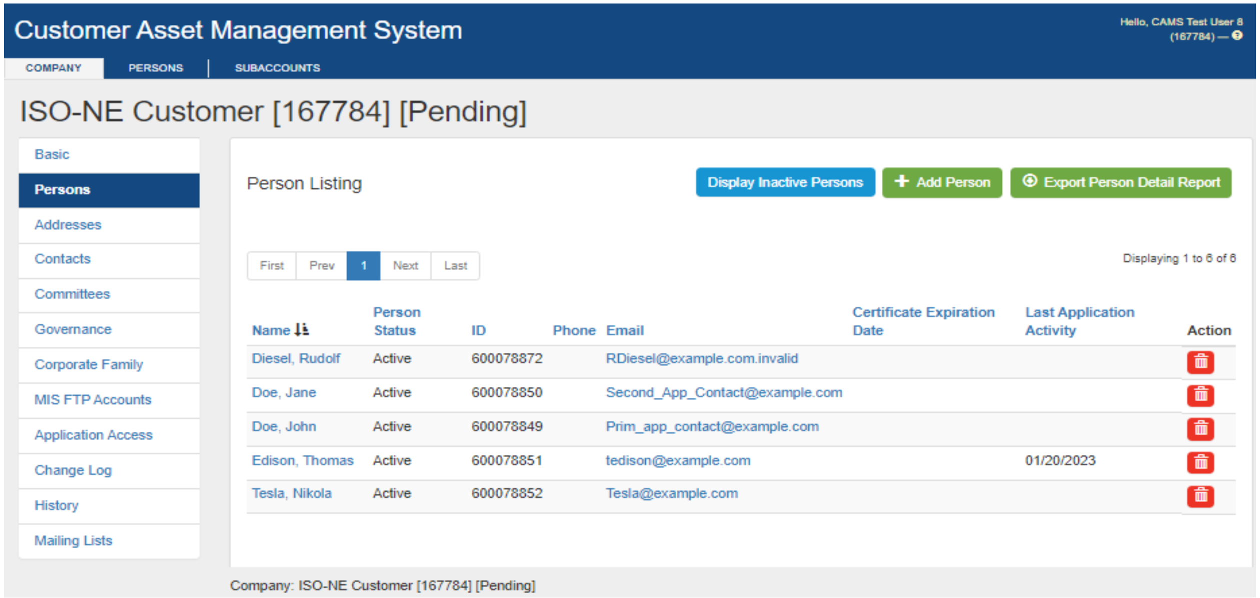
2.2.8 Update person's information

- Role that can perform this task:
    - Security Administrator

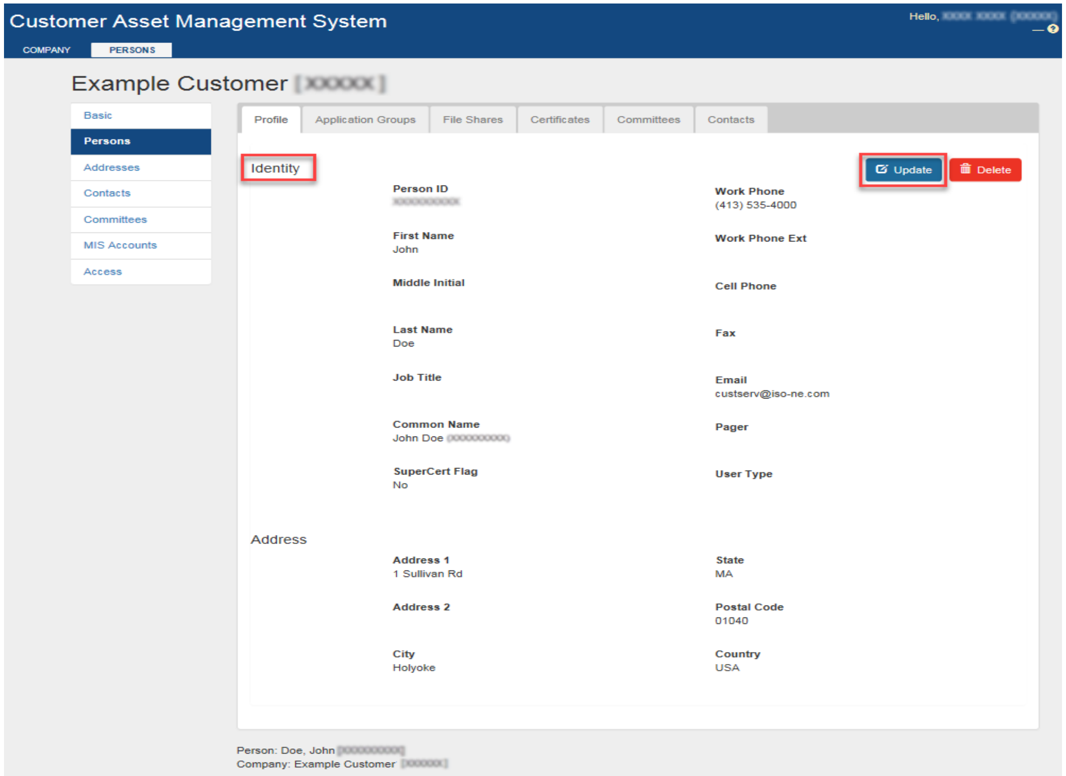
1. Launch the CAMS interface. See the "Accessing CAMS"

2. Click on the top-level "Persons" tab or on the second-level "Persons" tab if it is open.

3. The “Person Listing” page displays:

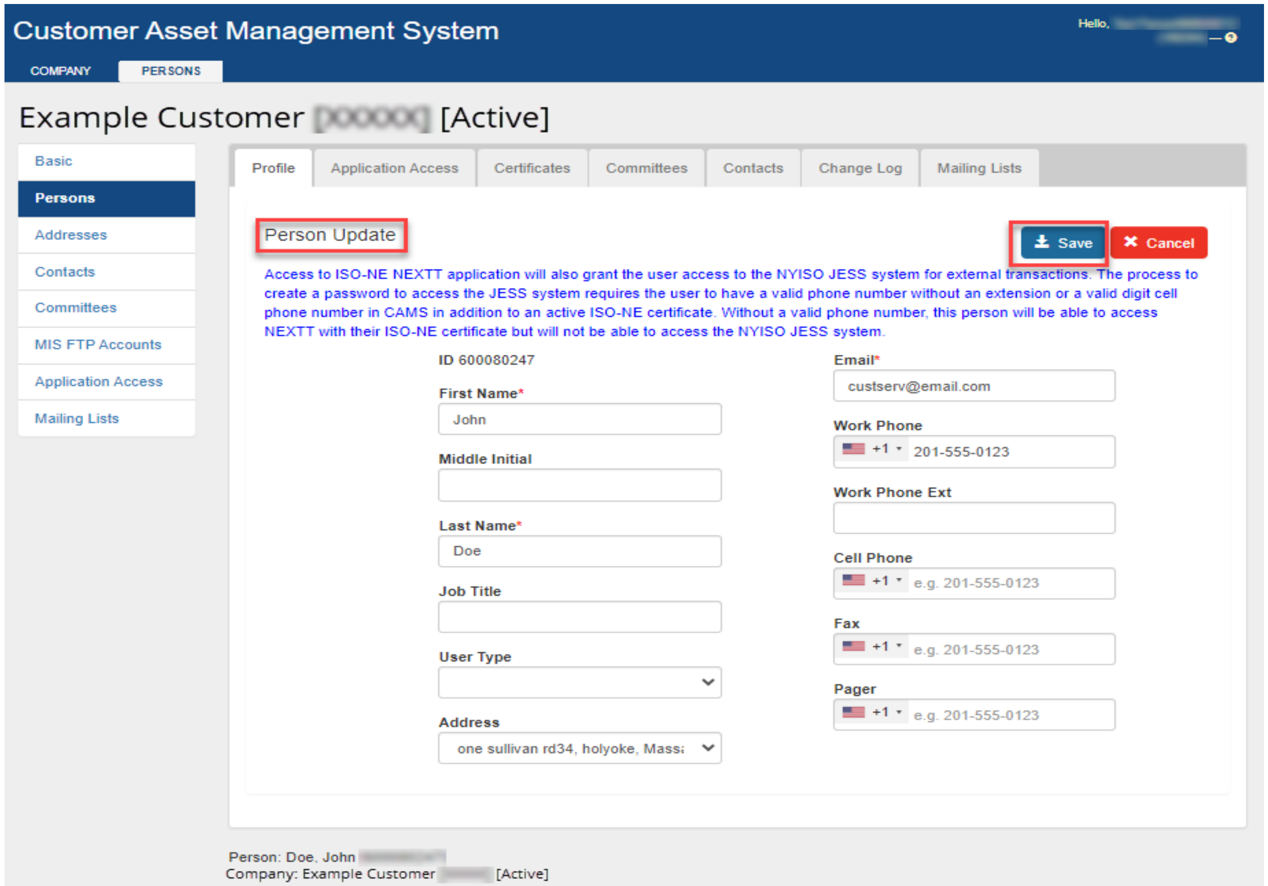


4. Click on the name of the person you want to delete.
5. The “Person View” screen displays:



6. Click the “Update” button.

7. The “Person Update” screen displays:



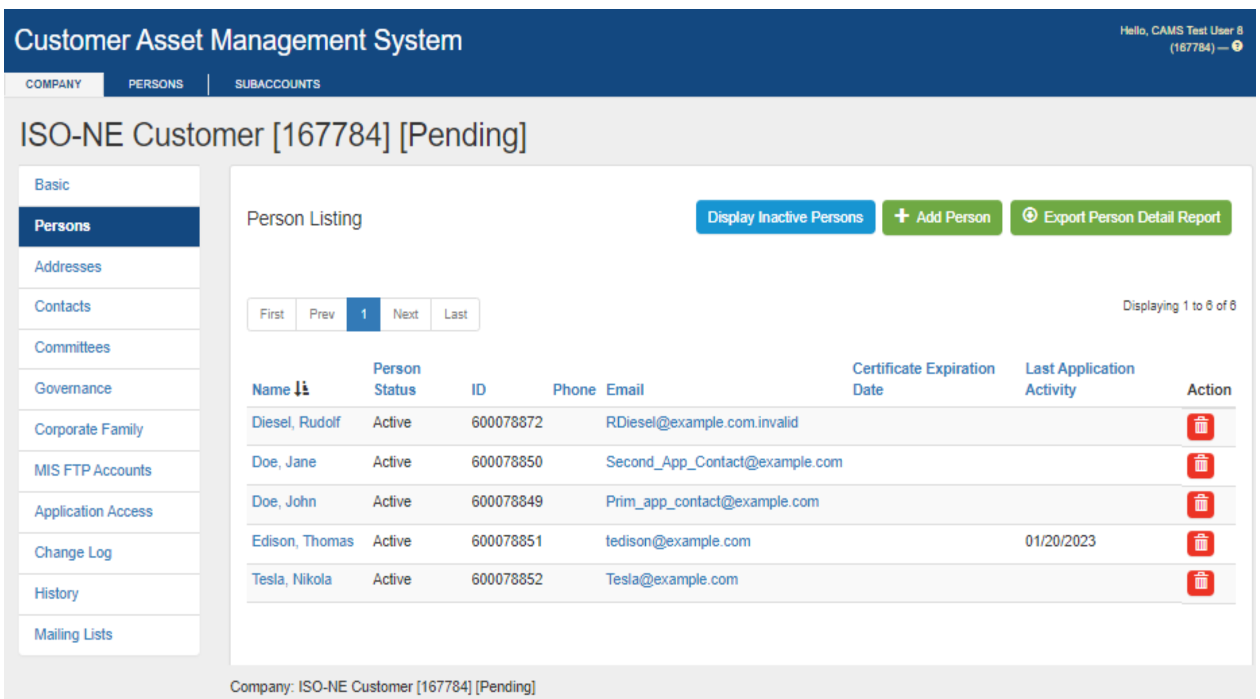
8. Update the information.First name, last name and email address are required. For phone numbers outside of North America, select the relevant country from the drop down then enter the phone number. Click on the “Save” button.

9. A confirmation message is displayed indicating the person was updated.

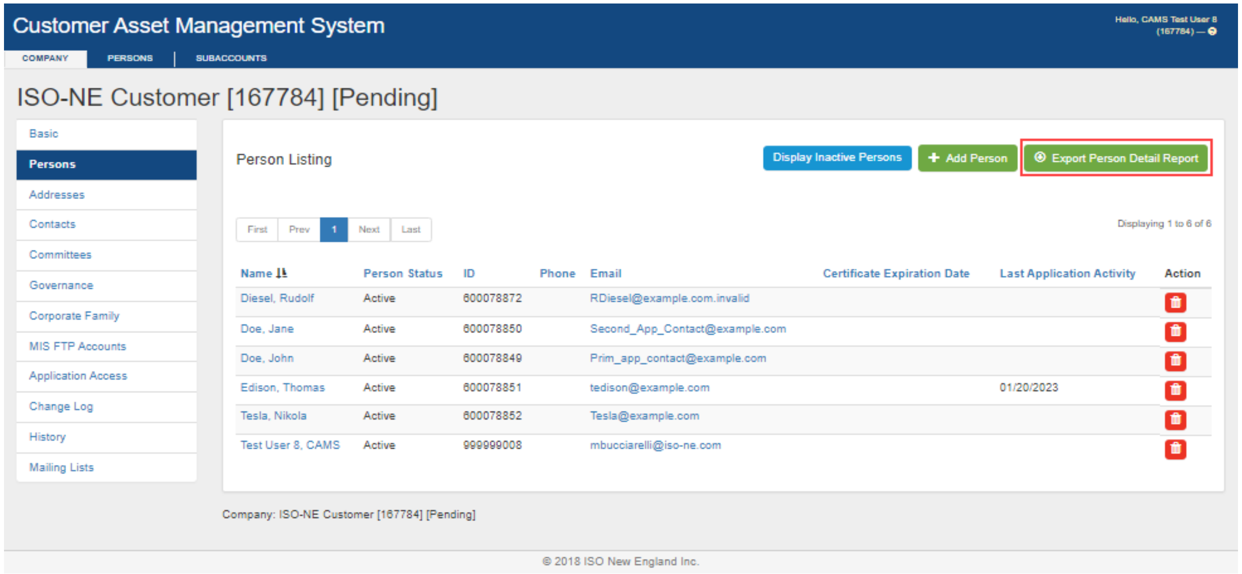
2.2.9 Retrieving your company's person detail report

- Role that can perform this task:
  - Security Administrator
  - External Person Maintainer
  - External Person Viewer

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on the top-level "Persons" tab or on the second-level "Persons" tab if it is open.
3. The "Person Listing" page displays:



4. Click on the “Export Person Detail Report” button.



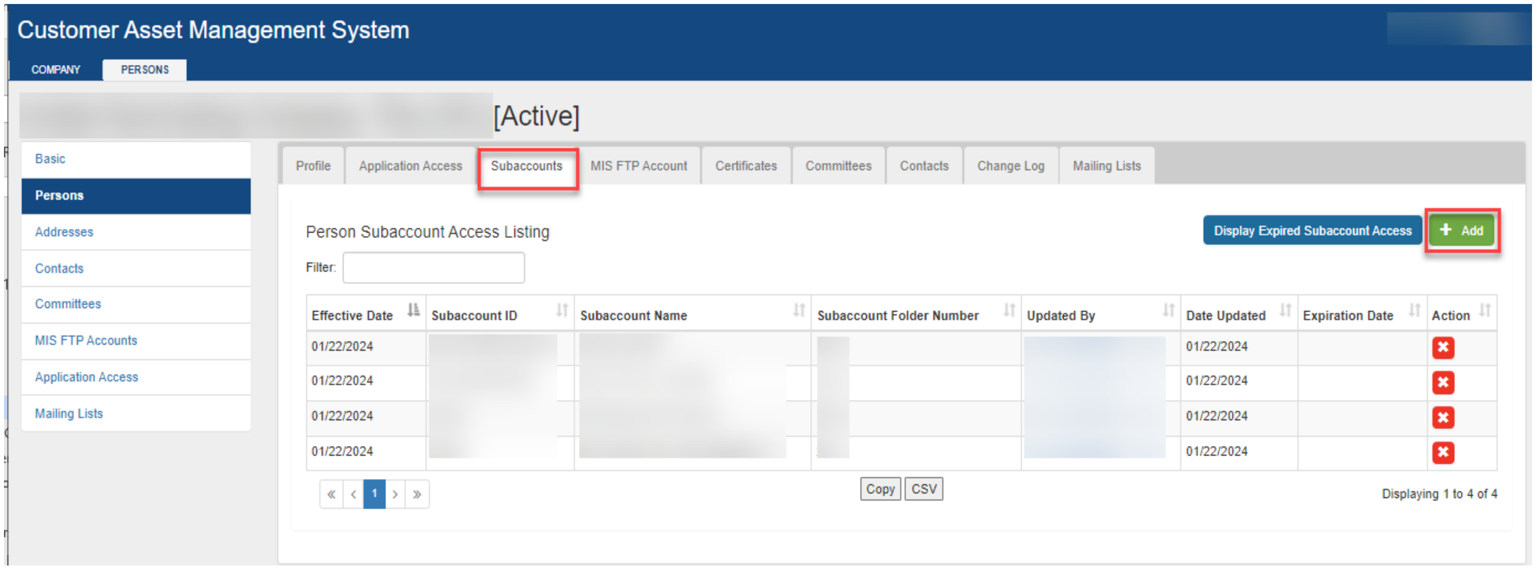
5. The Person Detail Report will be saved based on your settings. The Person Detail report is in XML format.

2.2.10 Person Subaccount Mapping

- Role that can perform this task:
    - Security Administrator

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on the top-level “Persons” tab or on the second-level “Persons” tab if it is open.
3. Click on the “Subaccounts” tab to view the mapped subaccounts for the person

A. To add a new Subaccount mapping, click “Add”

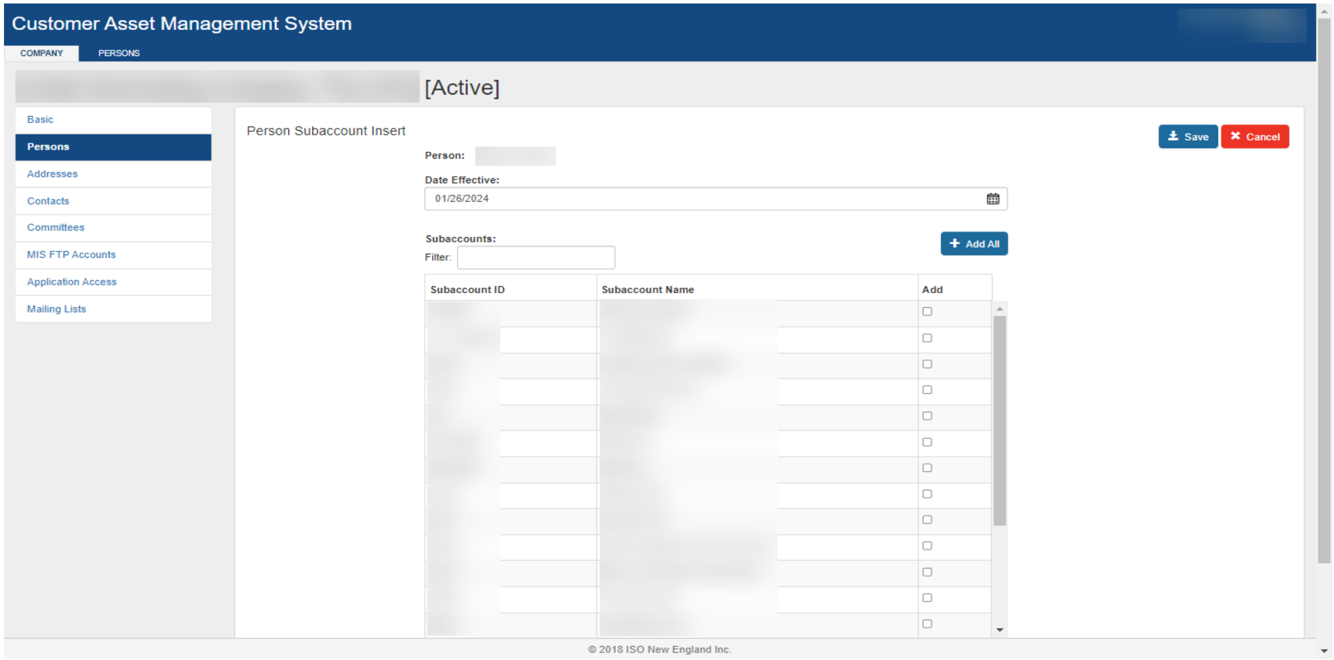


1. On “Person Subaccount Insert” screen

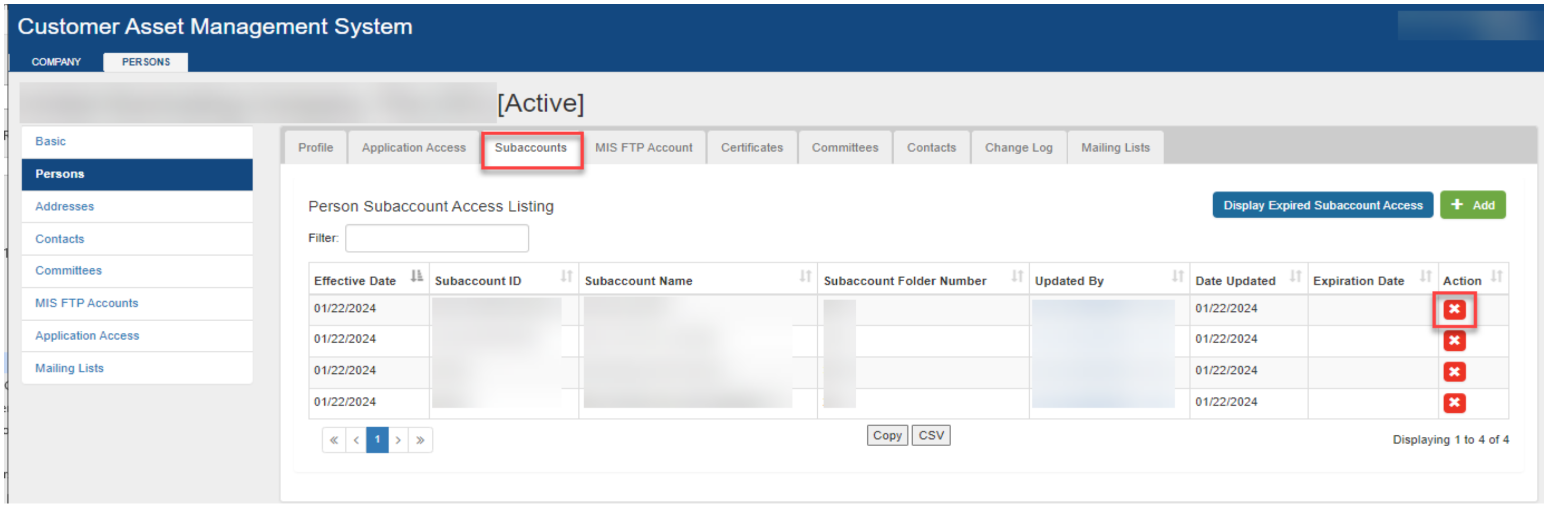
   a) Select Effective Date for the mapping (future date)

   b) Select one or more of the company’s active subaccounts

   c) Click “Save”


Customer Asset Management System
COMPANY
PERSONS
[Active]
Basic
Persons
Addresses
Contacts
Committees
MIS FTP Accounts
Application Access
Mailing Lists
Person Subaccount Insert
Save
Cancel
Person:
Date Effective:
01/26/2024
Subaccounts:
Add All
Filter:
Subaccount ID
Subaccount Name
Add
© 2018 ISO New England Inc.

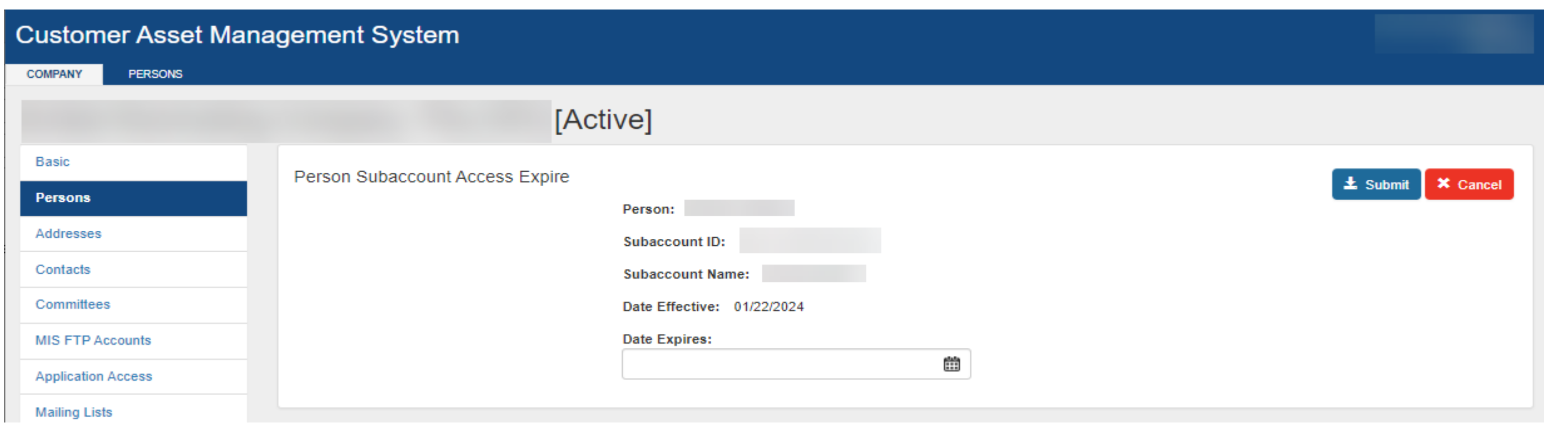
B. To delete a Subaccount mapping, click “X” in the action column for the subaccount you want to unmap from the person



1. On “Person Subaccount Access Expire” screen

 a) Select Expiration Date for the mapping (future date)

 b) Click “Submit”



2.3 Manage your Company's Information

This section applies to the following CAMS roles:

- External Customer Maintainer
- External Customer Viewer
- Security Administrator

This section covers the following topics:

- Roles that can perform this task:
    - External Customer Maintainer
    - Person Maintainer
    - Security Administrator

1. Launch the CAMS interface. See the "Accessing CAMS"
1. Click on "Company" in the top-level menu.
2. The "Basic" screen displays.

2.3.1 Overview

Company information stored and maintained in CAMS is grouped into the following categories:

- General customer information
    - Attributes about your company and its relationship to ISO New England
    - Found on the “Basic” tab
- DUNS information
    - Your company’s Data Universal Numbering System (DUNS) with Dun and Bradstreet
        - Can be modified
    - Found on the “Basic” tab
- Trading
    - Your company’s public trading information
        - Can be modified
    - Found on the “Basic” tab
    - See “Trading information”
- Addresses
    - Your company’s main office, billing addresses
        - Can be modified
    - Found on the “Addresses” tab
    - See “Update company address”
- Contacts
    - See “Contacts”
- Committees
    - See “Committees ”
- Corporate Family

- See “Corporate Family”

External Customer Maintainers and External Customer Viewers have access to the following:

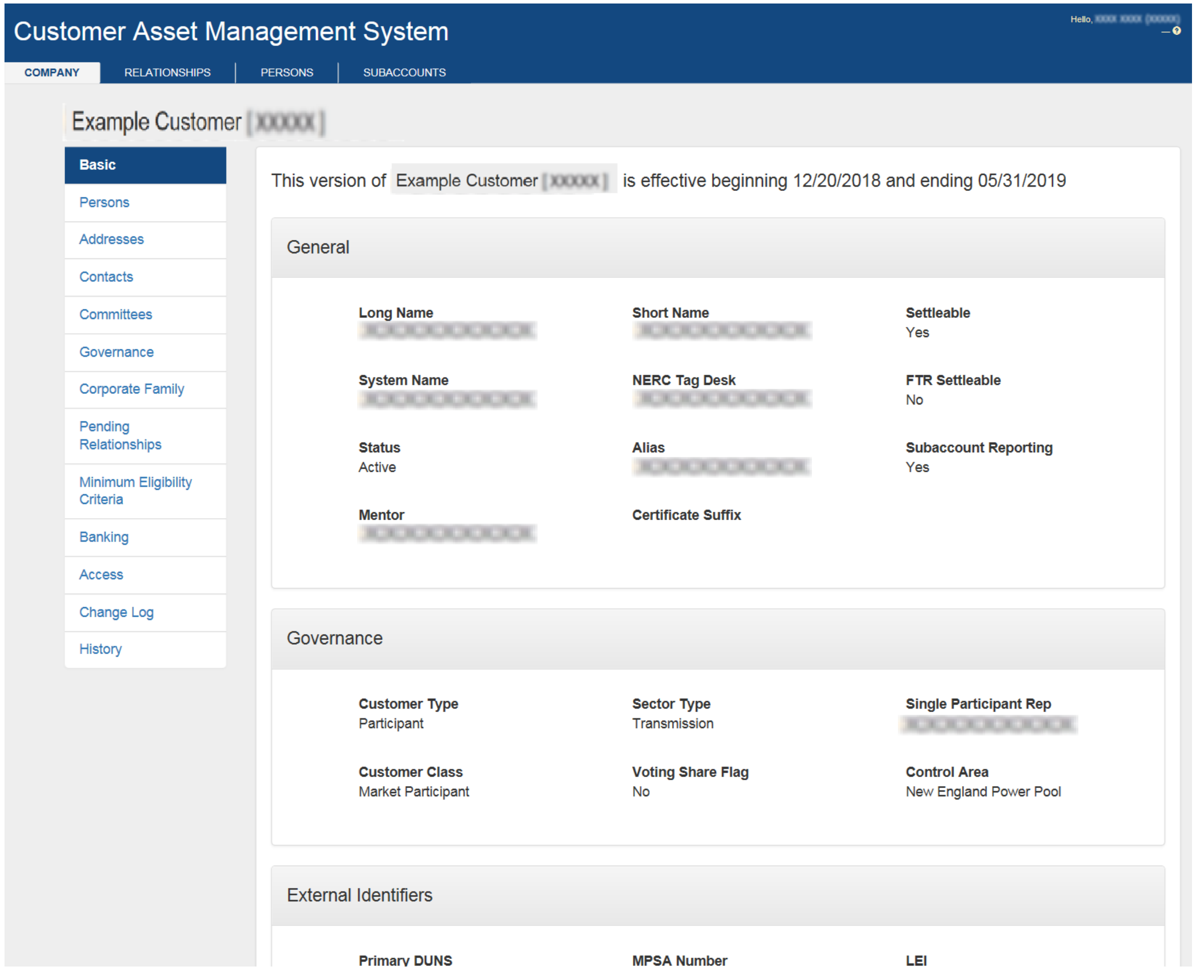
- History
  - The “History” tab displays a list of time periods in the past. Each period is a snapshot of company information as it appeared in CAMS at that time. A new snapshot increment is created each time your company information is updated or changed.
  - Click on the “History” tab, and then click on the selected time period. Your company information as of that time period is displayed.
- Change Log
  - The Customer Change Log is an audit trail showing what company information was changed, when and by whom.
- Governance
  - The “Governance” tab displays any governance relationships your company has with other companies in CAMS.

2.3.2 Customer

2.3.2.1 View customer information

- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer
  - Security Administrator

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Company” in the top-level menu.
3. The Customer’s Basic information screen displays:


Customer Asset Management System
COMPANY
RELATIONSHIPS
PERSONS
SUBACCOUNTS
Example Customer
Basic
Persons
Addresses
Contacts
Committees
Governance
Corporate Family
Pending Relationships
Minimum Eligibility Criteria
Banking
Access
Change Log
History
This version of Example Customer is effective beginning 12/20/2018 and ending 05/31/2019
General
Long Name
Short Name
Settleable
Yes
System Name
NERC Tag Desk
FTR Settleable
No
Status
Active
Alias
Subaccount Reporting
Yes
Mentor
Certificate Suffix
Governance
Customer Type
Participant
Sector Type
Transmission
Single Participant Rep
Customer Class
Market Participant
Voting Share Flag
No
Control Area
New England Power Pool
External Identifiers
Primary DUNS
MPSA Number
LEI

2.3.3 Addresses

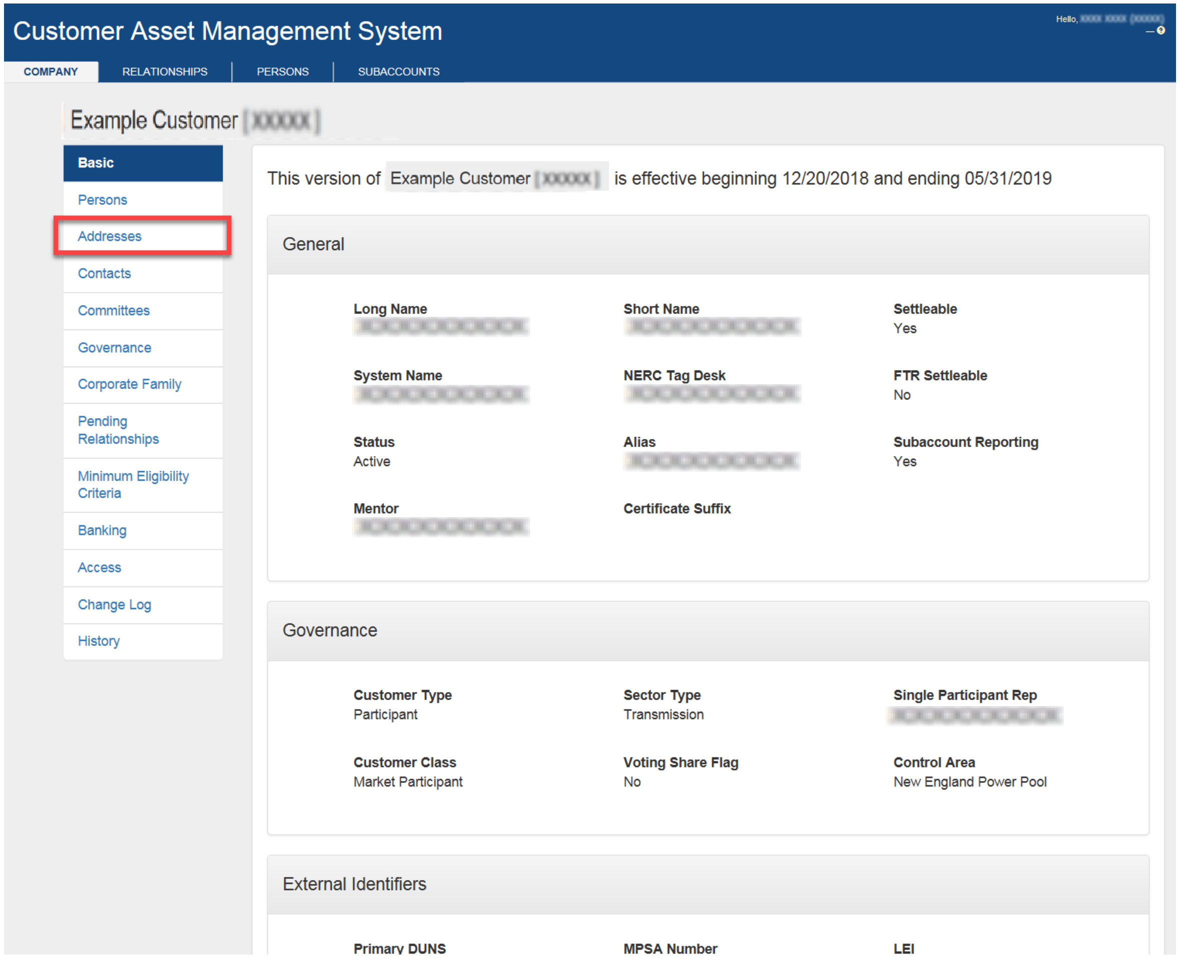
IMPORTANT

- ❖ Your company's "Main Office" (headquarters) address is initially entered into CAMS during the membership application process.
- ❖ Your company must always have one accurate "Main Office" address designated in CAMS.
- ❖ Your company can only have one "Main Office" address.

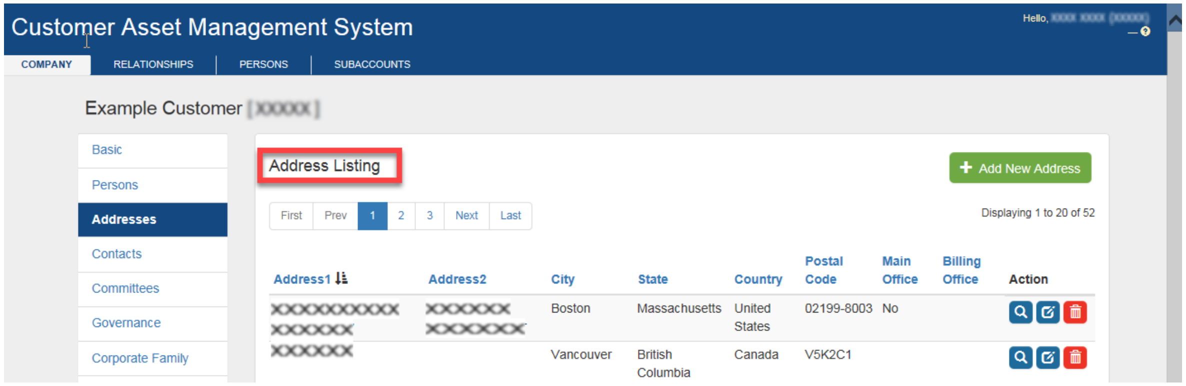
2.3.3.1 Add company address

- Role that can perform this task:
    - External Customer Maintainer

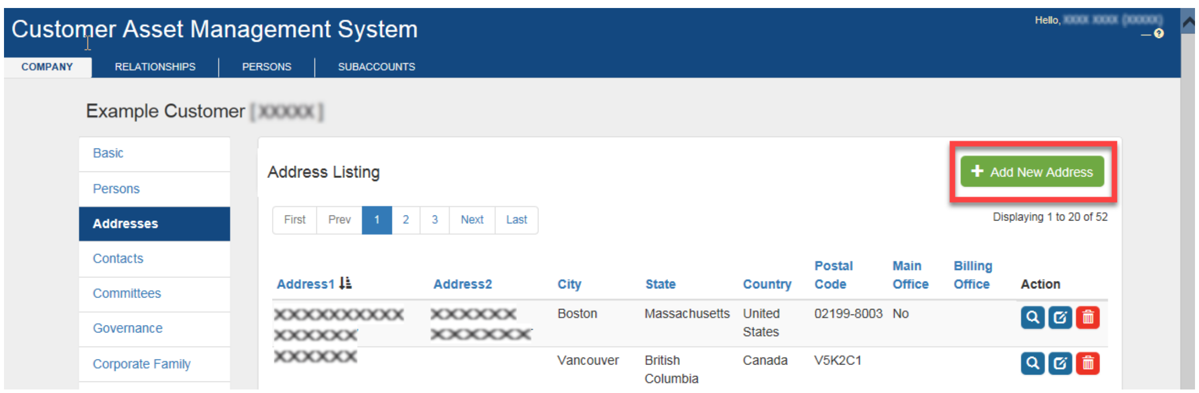
1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The Customer's Basic screen displays:



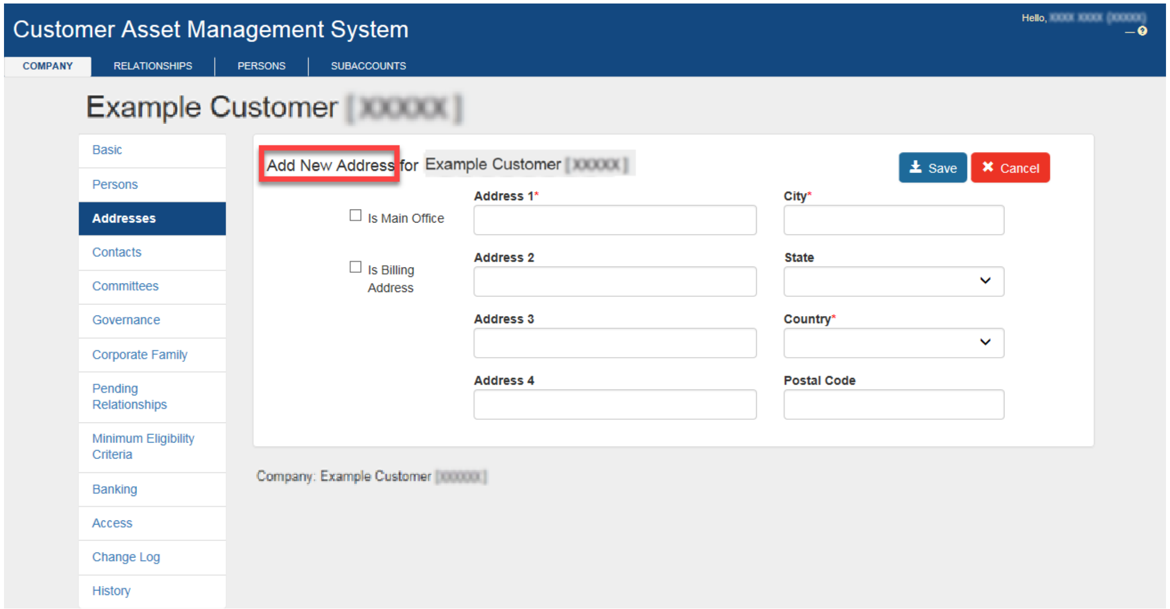
4. Click on the “Addresses” tab in the second-level menu.
5. The Company “Address Listing” screen displays:



6. Click the “Add New Address” button.



7. The Company “Add New Address” screen displays:

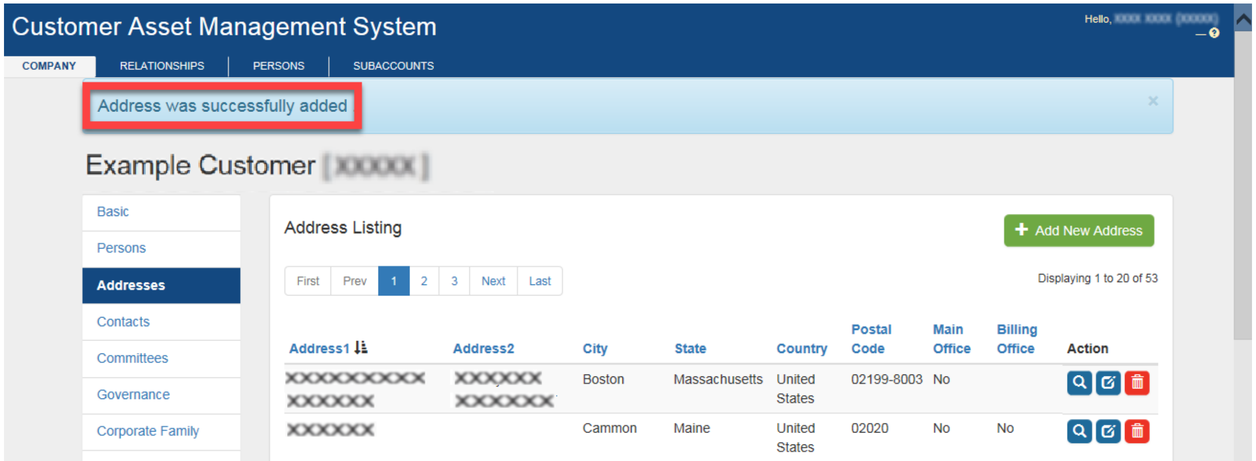


8. Enter the address and related information in the fields provided. Address, city, state, country, and postal code are required.
9. Click the “Save” button.

IMPORTANT

❖ There can be only one Billing address and one Main Office address for the company.

10. A confirmation message displays:

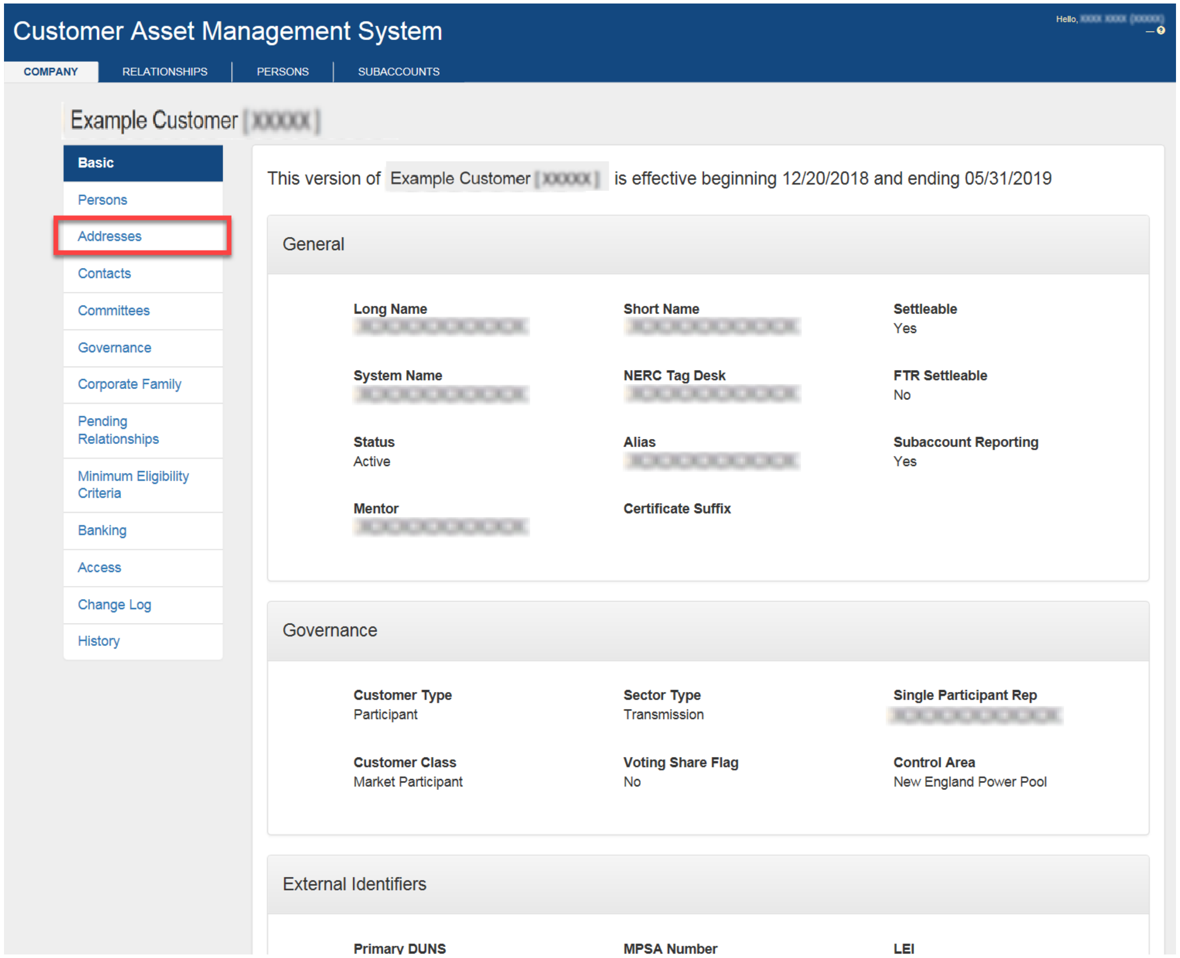


2.3.3.2 Update company address

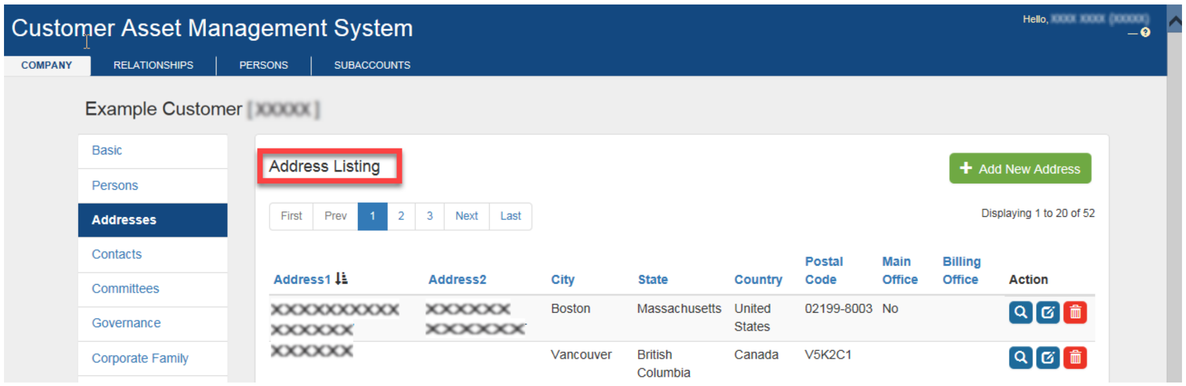
- Role that can perform this task:

- External Customer Maintainer

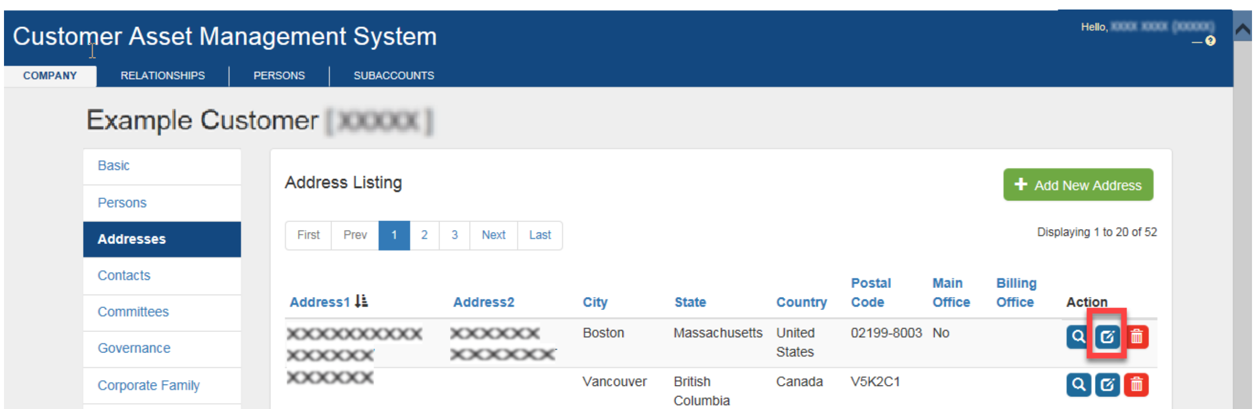
1. Launch the CAMS interface. See the "[Accessing CAMS](#)"
2. Click on "Company" in the top-level menu.
3. The Customer "Basic" screen displays:



4. Click on the “Addresses” tab in the second-level menu.
5. The “Address Listing” screen displays:



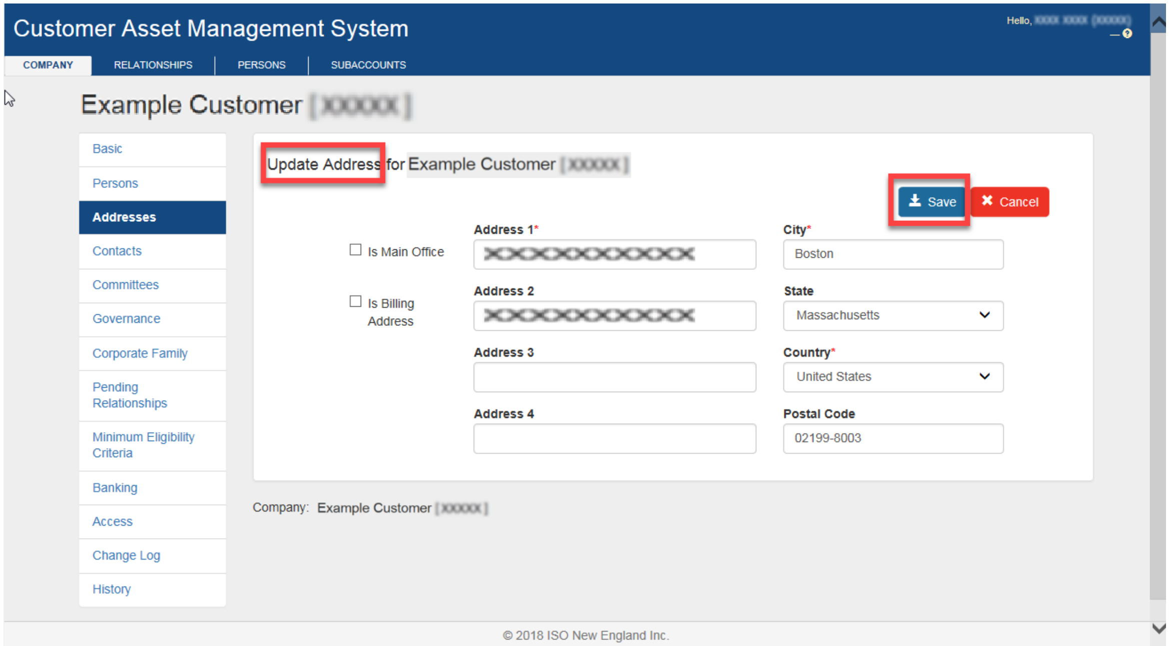
6. Locate the record you want to update and click on the Pencil icon in the “Action” column for the address for that row:



IMPORTANT

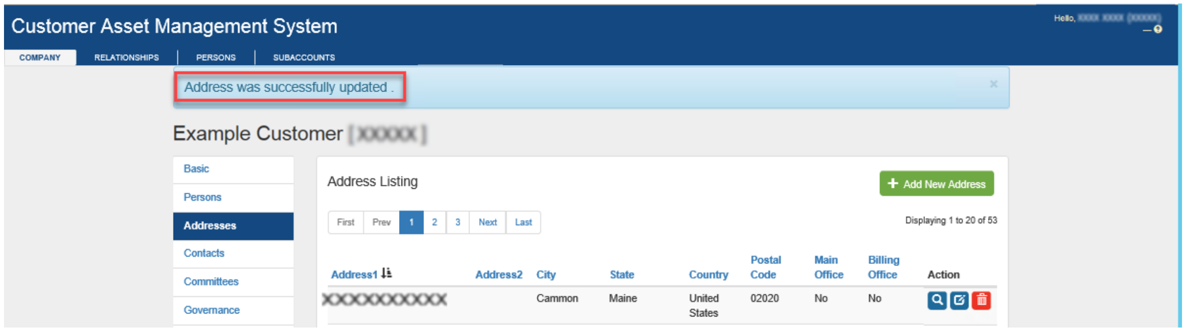
- Main Office address and the Billing Address can be updated.

7. The “Company Address Update” screen displays:



8. Enter the address and related information in the fields provided. Address, city, state, country, and postal code are required.
9. Click “Save”

10. The confirmation message displays:



2.3.3.3 Delete company address

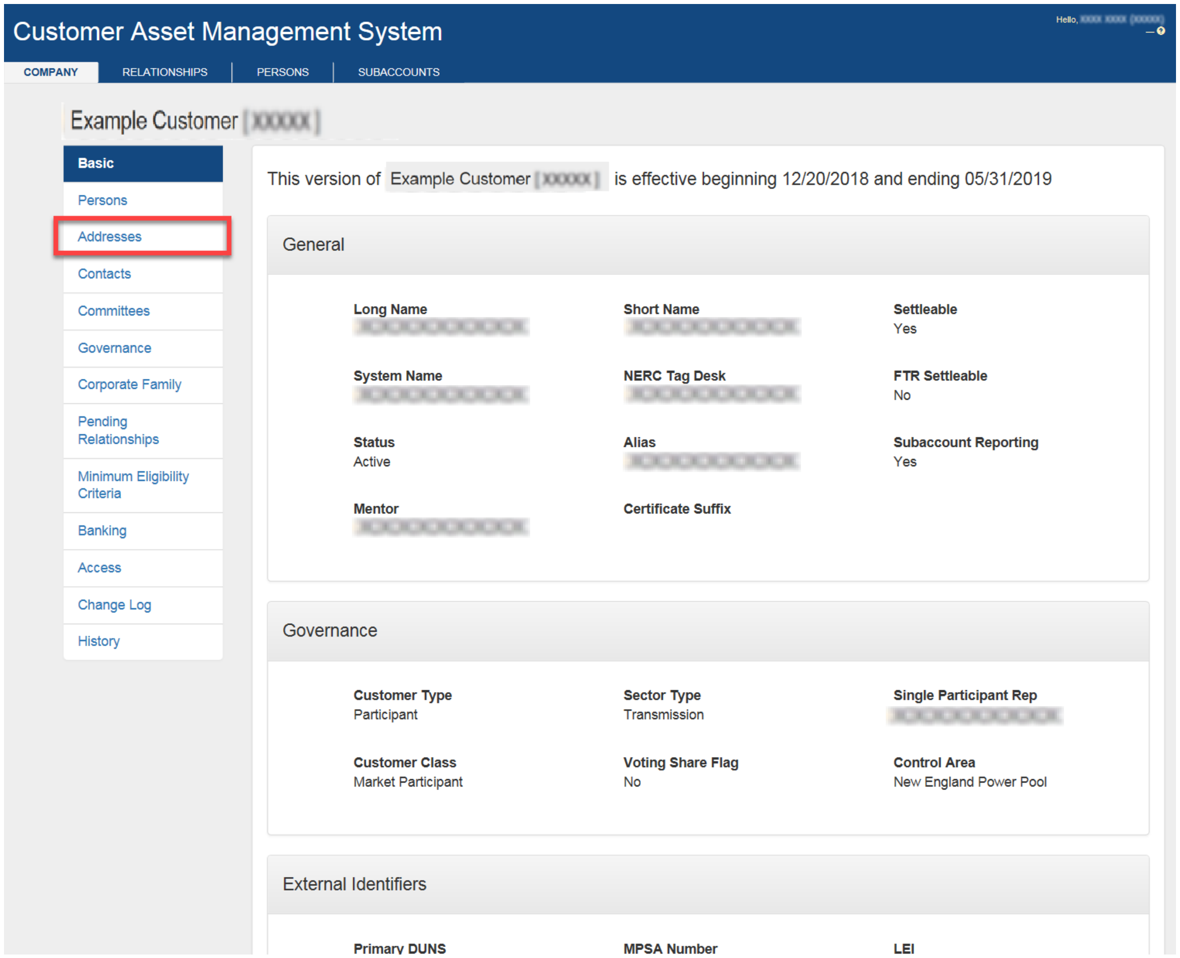
- Role that can perform this task:
    - External Customer Maintainer

IMPORTANT

- ❖ You cannot delete an address if it is associated with any person.
- ❖ Main Office address and the Billing Address can be deleted if they are not associated to any person.

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.

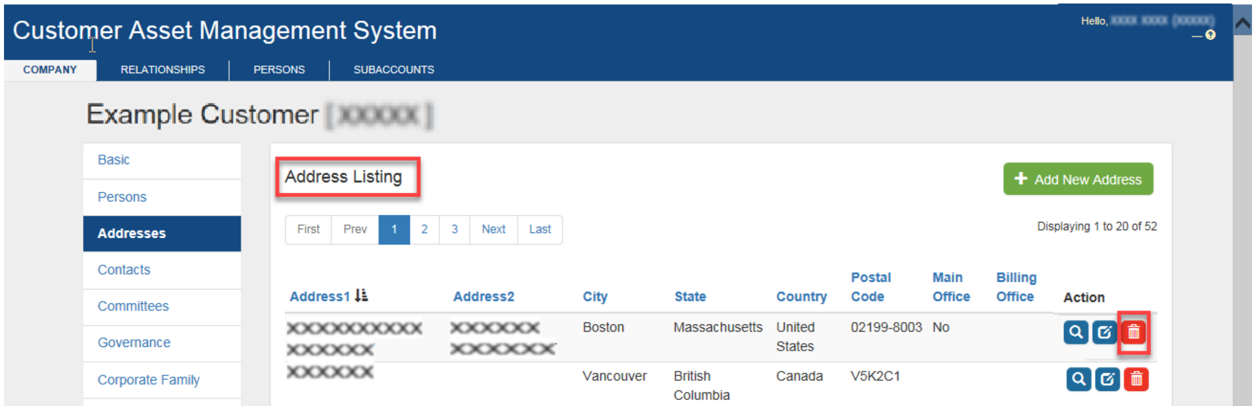
3. The “Customer View” screen displays:



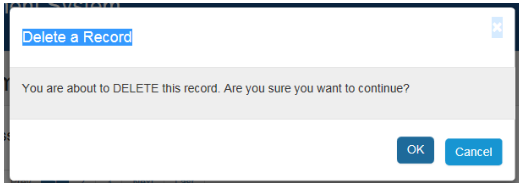
4. Click on the “Addresses” tab in the second-level menu.

5. The “Company Address Listing” screen displays.

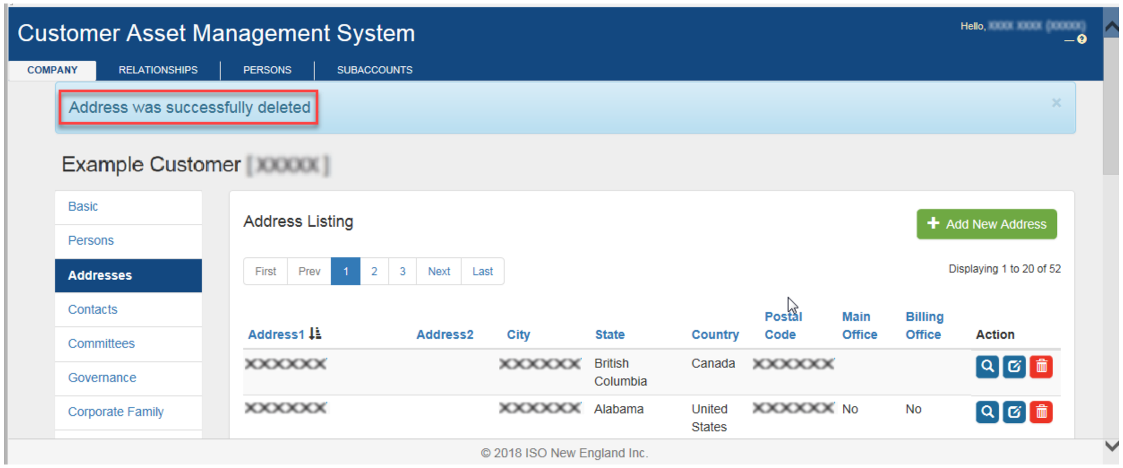
6. Locate the record you want to delete and click the “ ” icon in the “Action” column for that row:



7. A pop up message is displayed asking for user confirmation to delete or not.



8. Click “OK” to delete.
9. A confirmation message displays:



IMPORTANT

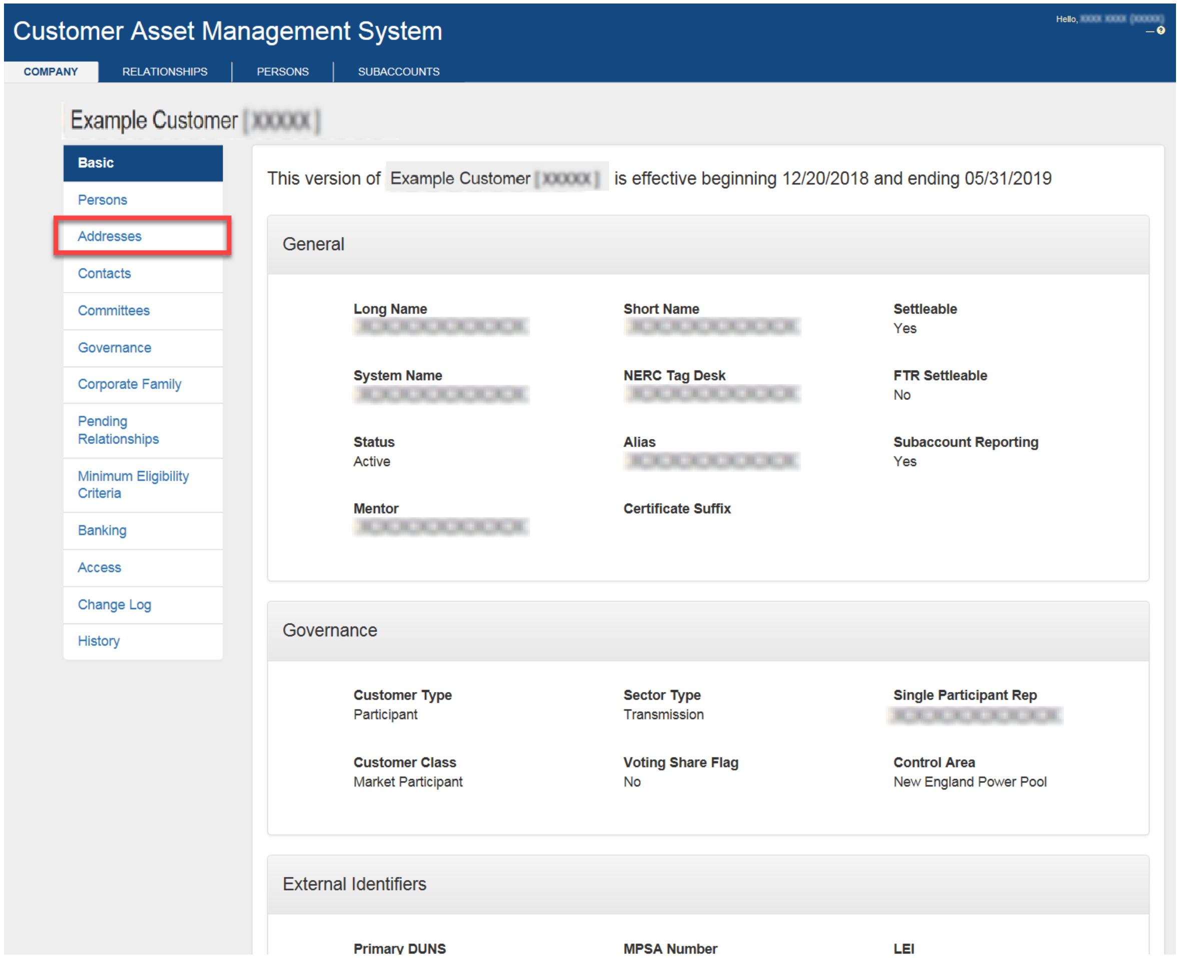
- ❖ Your company must always have one accurate "Main Office" address designated in CAMS.

2.3.3.4 View persons associated to a company address

- Roles that can perform this task:
  - External Customer Maintainer

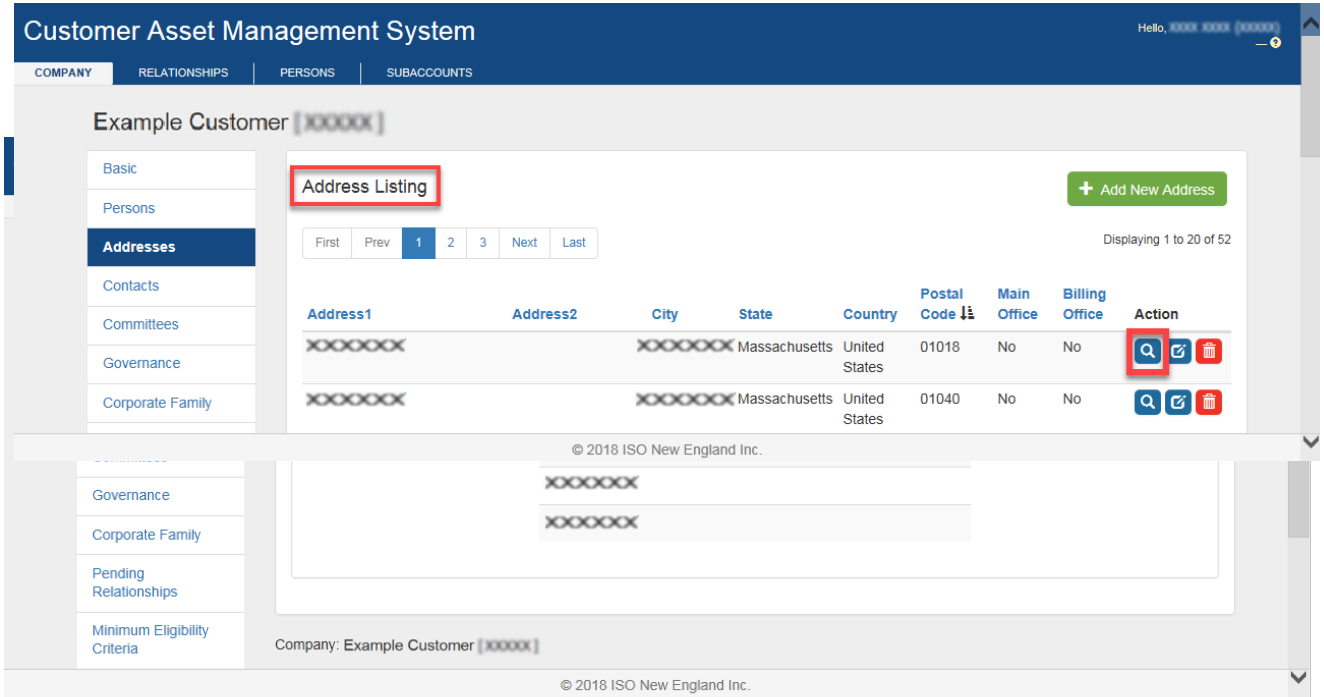
- External Customer Viewer

1. Launch the CAMS interface. See the “[Accessing CAMS](#)”
2. Click on “Company” in the top-level menu.
3. The “Customer View” screen displays:



4. Click on the “Addresses” tab in the second-level menu.
5. The “Company Address Listing” screen displays.
6. Locate the address for the person associations you want to view.

7. Click on the look up icon in the “Action” column for that row:



8. The “Company User Address Listing” screen displays.

IMPORTANT

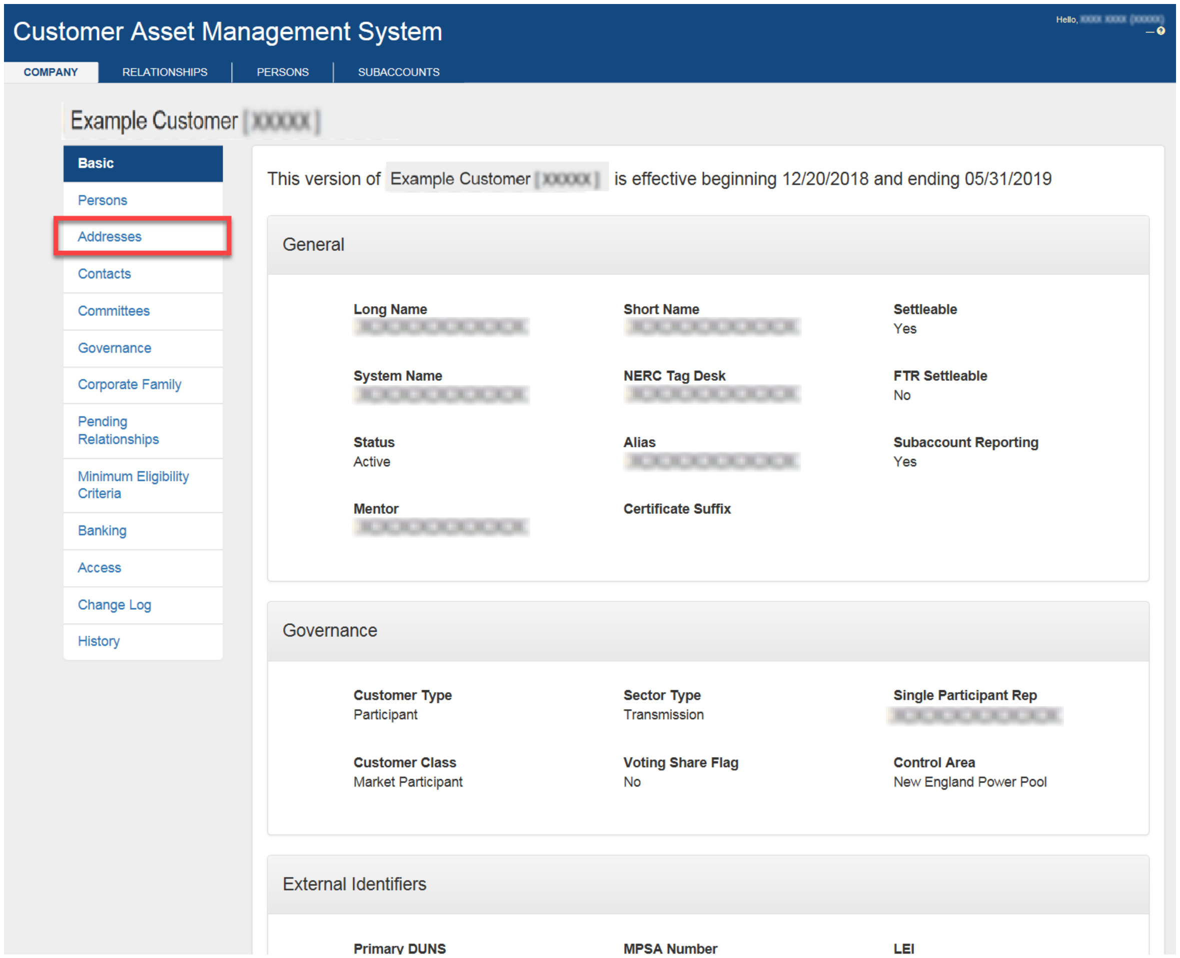
- ❖ You will not be able to view the individual record of the persons listed. Only a Security Administrator, External Person Maintainer or External Person Viewer has access to Person details.

2.3.3.5 View company address listing

- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer

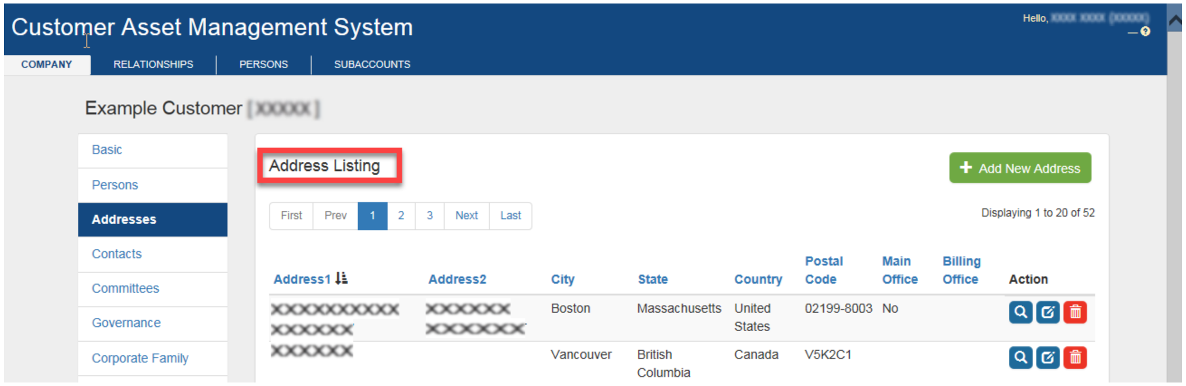
1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.

3. The “Customer View” screen displays:



4. Click on the “Addresses” tab in the second-level menu.

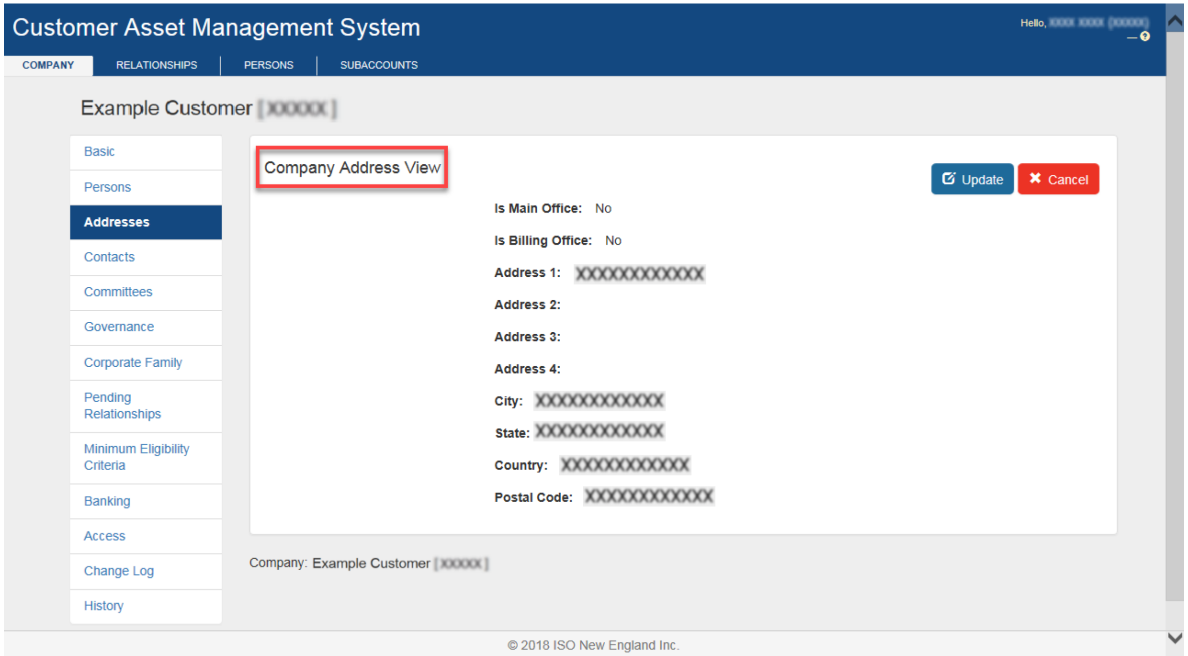
5. The “Company Address Listing” screen displays:



2.3.3.6 View company address information

- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Customer View" screen displays:
4. Click on the "Addresses" tab in the second-level menu.
5. The "Company Address Listing" screen is displayed:
6. Click on the hyperlink in the "Address 1" column to view the address information.
7. The "Company Address View" screen displays:



2.3.4 History

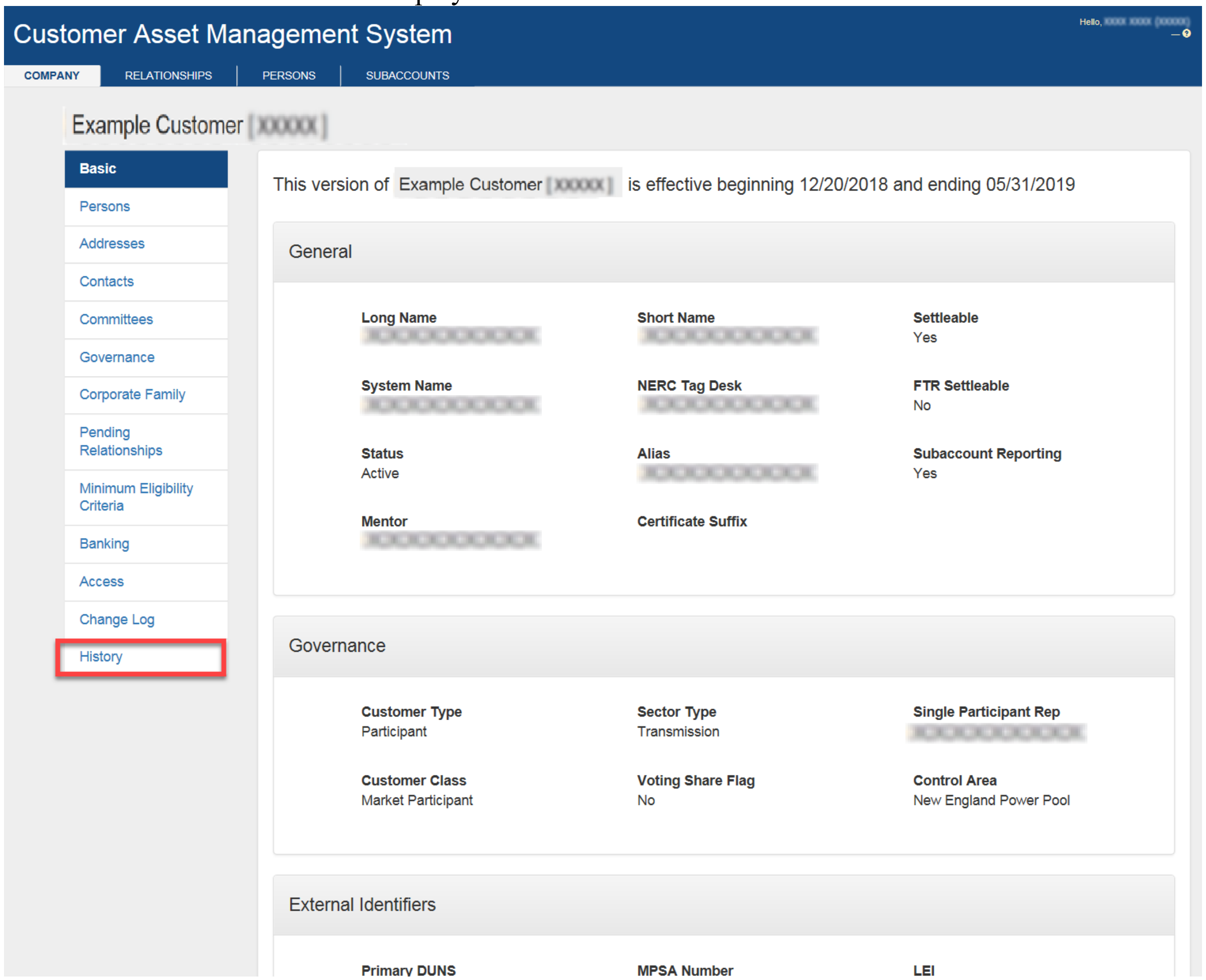
- The "History" tab displays a list of time periods in the past. Each period is a snapshot of company information as it appeared in CAMS at that time. A new snapshot increment is created each time your company information is updated or changed.

2.3.4.1 View history information

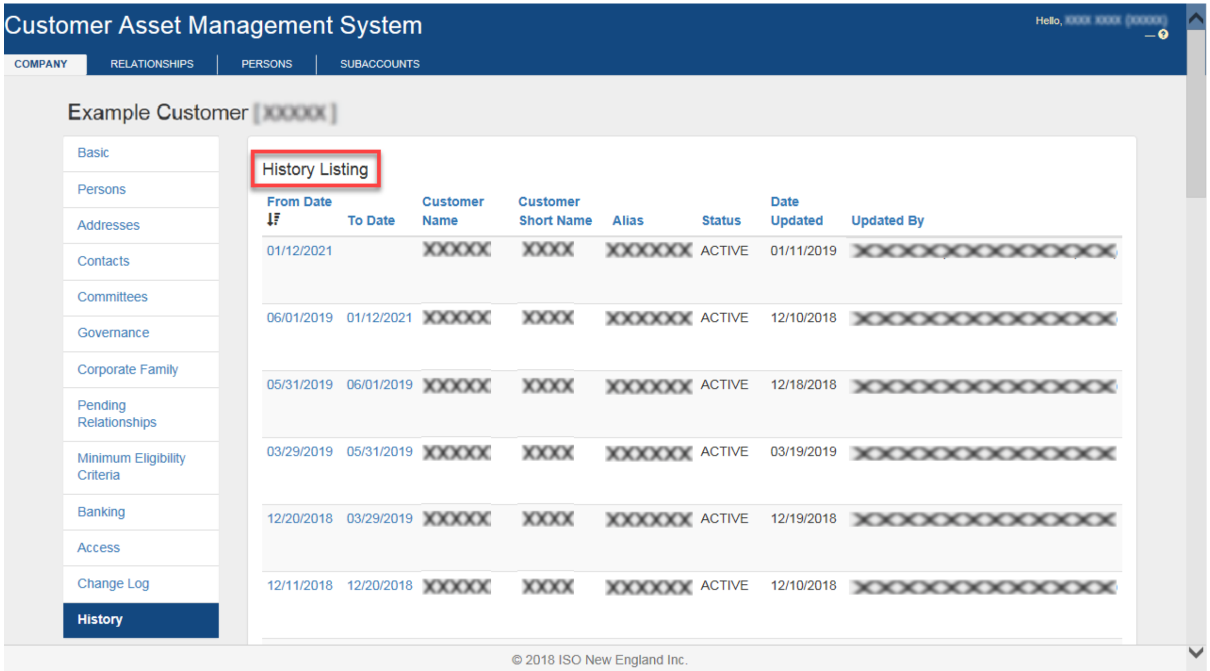
- Roles that can perform this task:
    - External Customer Maintainer
    - External Customer Viewer

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.

3. The “Customer View” screen displays:



4. Click on the “History” tab in the second-level menu.
5. The “Customer History Listing” screen displays:



6. Click on a time period. Your company information as of that selected time period displays.

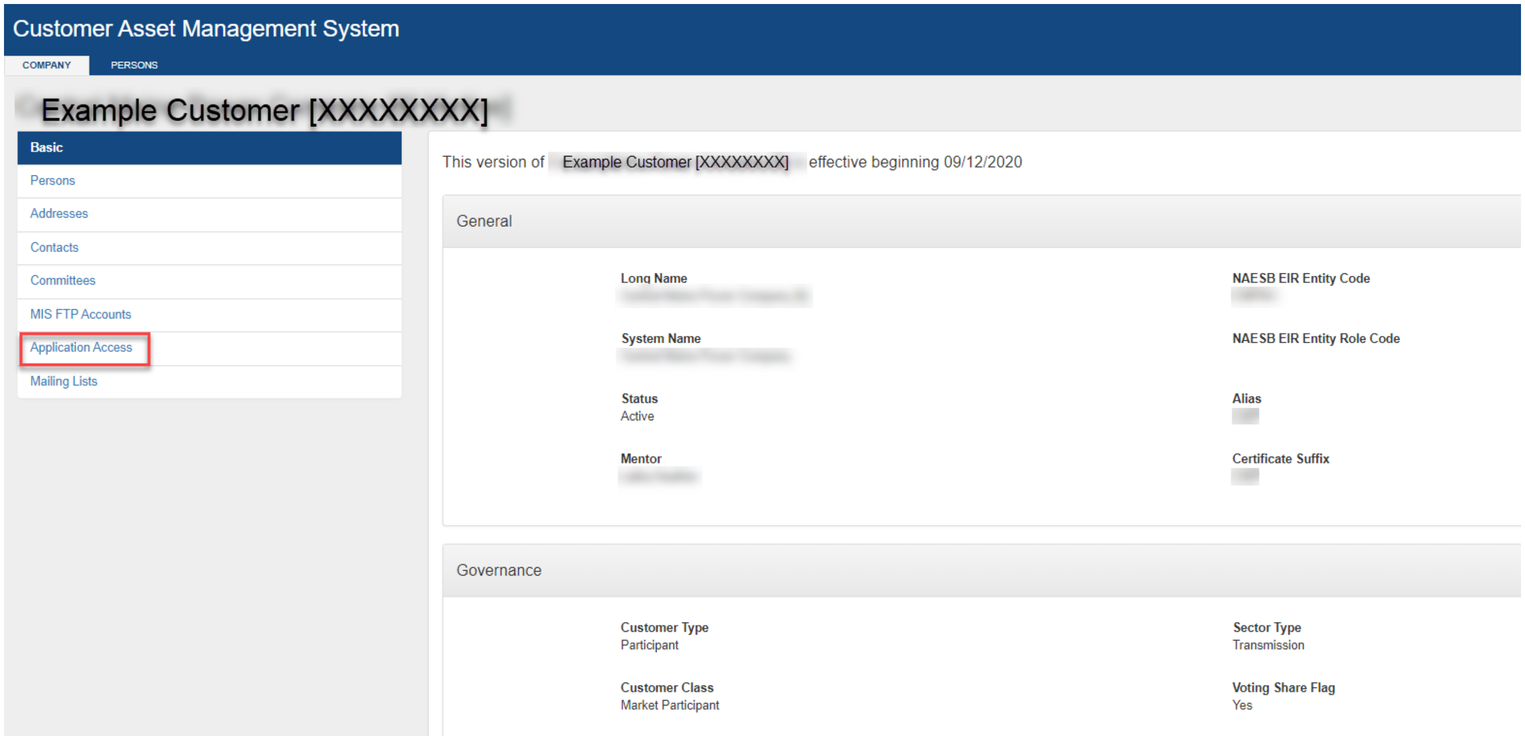
2.3.5 Applications

2.3.5.1 View customer application information

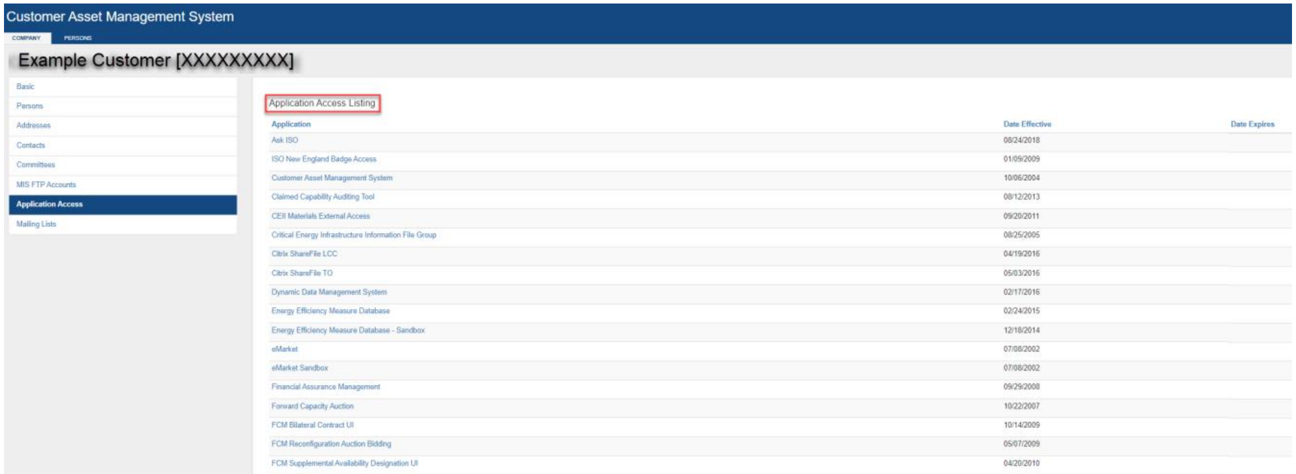
- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer
  - Security Administrator

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.

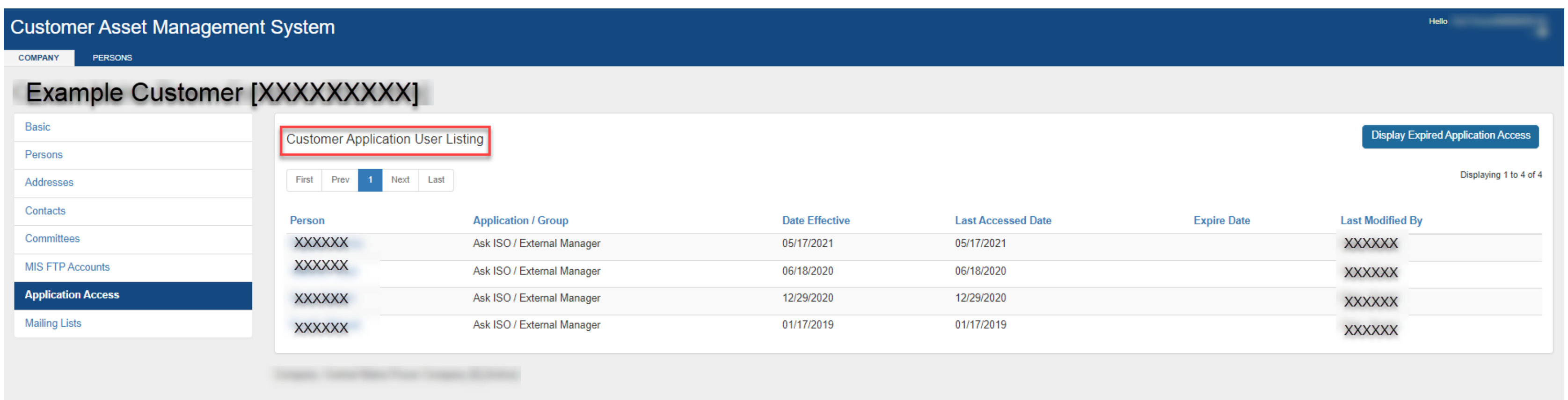
3. The “Customer View” screen displays.



4. Click on the “Application Access” tab in the second-level menu.
5. “Application Access Listing” screen displays:



6. Click on the hyperlink in the "Application" column to view which person has access to a particular application.
7. "Customer Application User Listing" screen is displayed:



IMPORTANT

- ❖ A *digital certificate* is an electronic key to the ISO New England websites that host CAMS and other applications. A user cannot access any ISO application without a digital certificate.

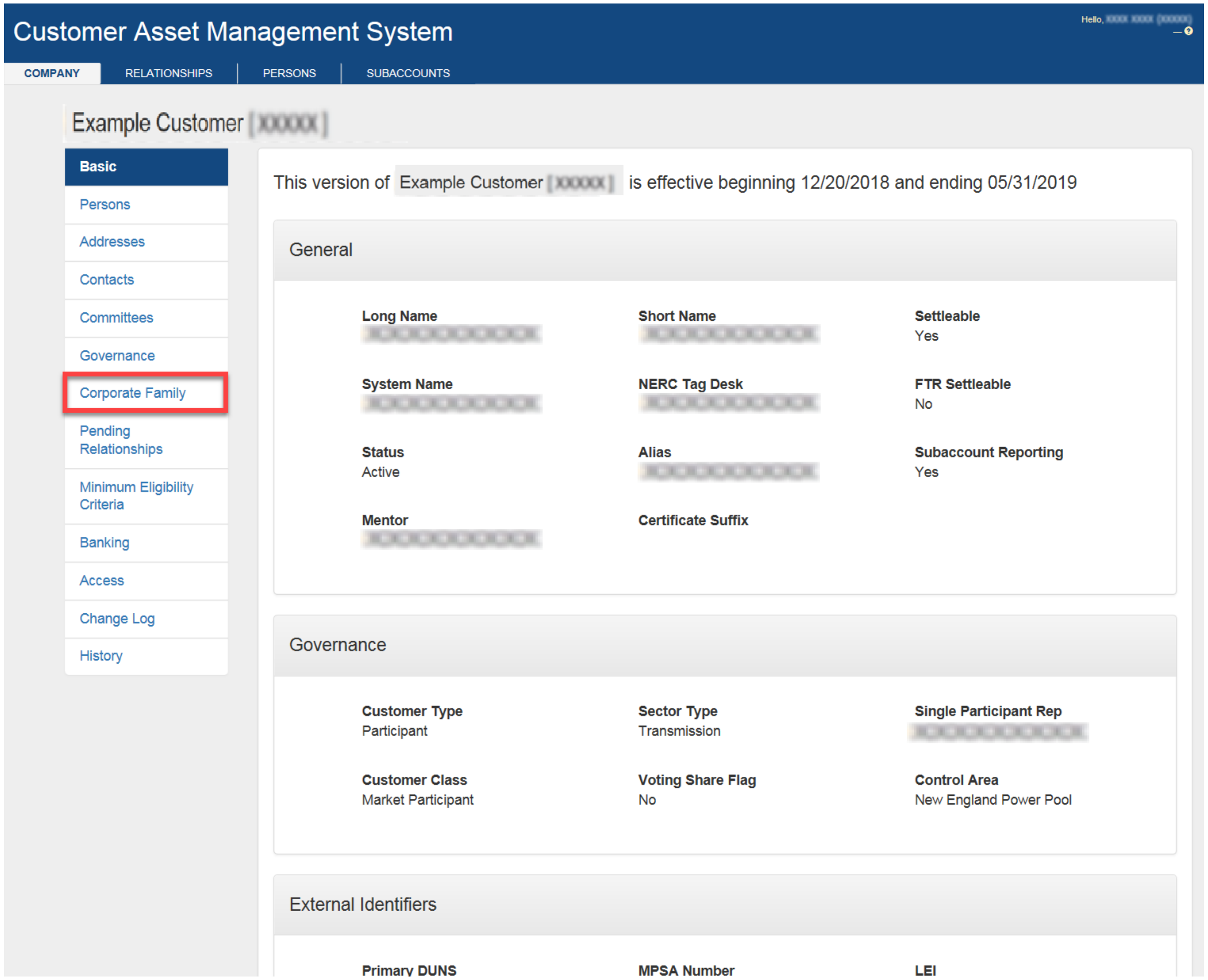
2.3.6 Corporate Family

- A customer's corporate family consists of direct and indirect relationships from the ultimate parent to the ultimate child.

2.3.6.1 View corporate family information

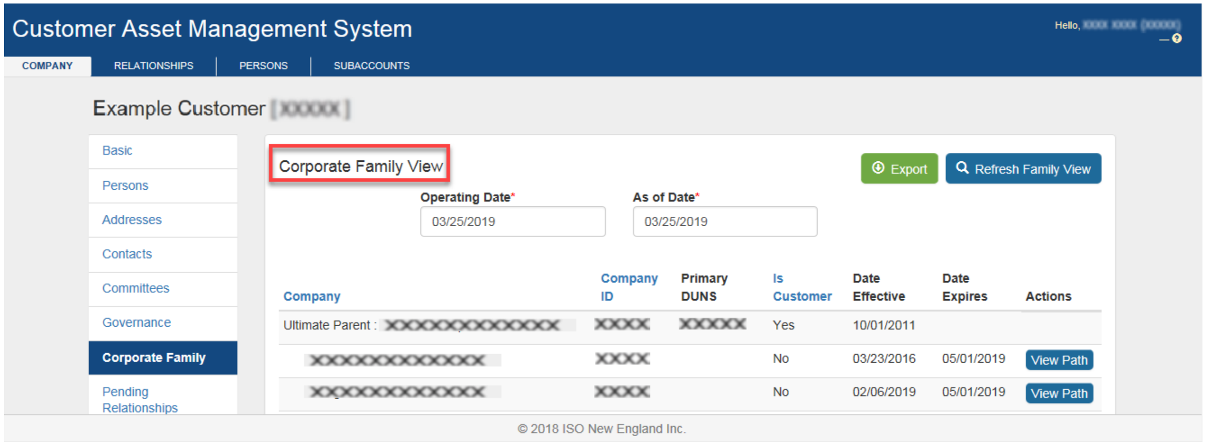
- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Customer View" screen displays:



4. Click on the “Corporate Family” tab in the second-level menu.

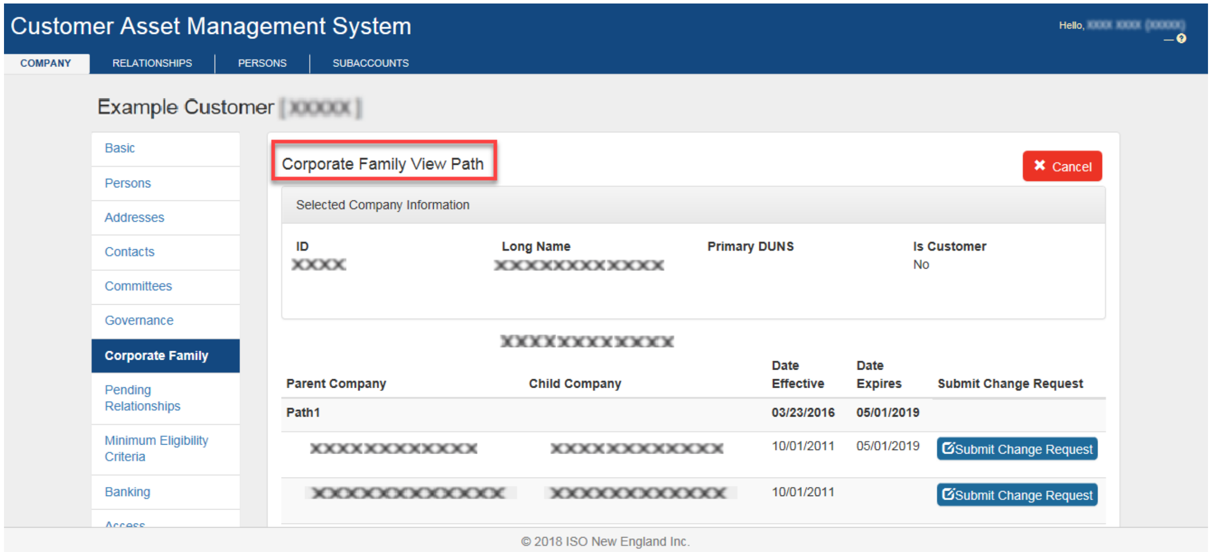
5. “Corporate Family View” screen displays:



2.3.6.2 View company path information

- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on the “Corporate Family” tab in the second-level menu.
3. The “Corporate Family View’ screen displays.
4. Click on “View Path” in the Actions column for the company to be viewed.
5. The “Path Details” screen displays:



NOTE: The "Path Details" pop-up is displayed on top of the Corporate Family View screen.

2.3.7 Contacts

- A "contact" is an individual or an entity (such as a "Service Desk" or distribution list) authorized to receive notifications and correspondence from ISO New England relevant to the specific "contact type".
- "Contact types" are ISO New England-defined groupings based on the information and communication needs of the activity.
- Your company's contact types in CAMS should be kept up-to-date at all times. ISO New England distributes important information to contacts. If a person at your company is no longer the appropriate contact, update CAMS as soon as possible with the new individual.
- "Contact types" do not give the assigned person any additional privileges or roles. To add permissions and roles for CAMS or another application, see "Granting a person access to CAMS or another ISO application"
- A company may designate multiple contacts for each contact type.

CAUTION

- ❖ Keep your company's contact types up-to-date in CAMS at all times. ISO New England distributes important and time-sensitive information to contacts.

2.3.7.1 Add contact information

- Roles that can perform this task:
    - External Customer Maintainer
    - External Customer Viewer
    - Security Administrator

1. Launch the CAMS interface. See the "Accessing CAMS"

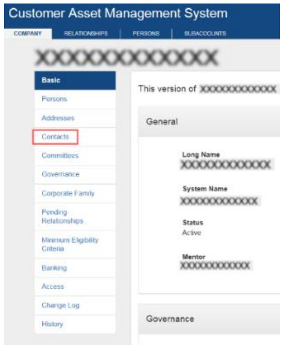
IMPORTANT

- ❖ You may add a contact through the second-level "Contacts" menu (as described below) or by selecting an individual person from the "Persons" menu tab and then clicking the "Contacts" tab that appears.

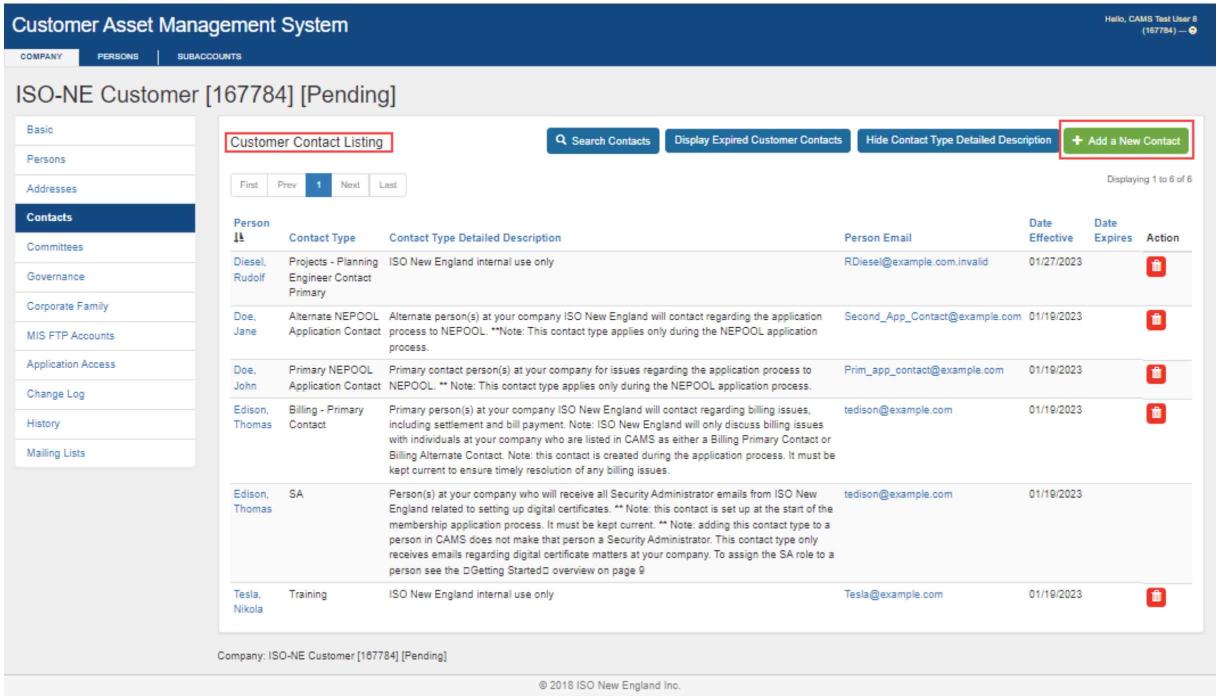
2. Click on "Company" in the top-level menu.

3. The "Basic" screen displays.

4. Click on the "Contacts" tab in the second-level menu:

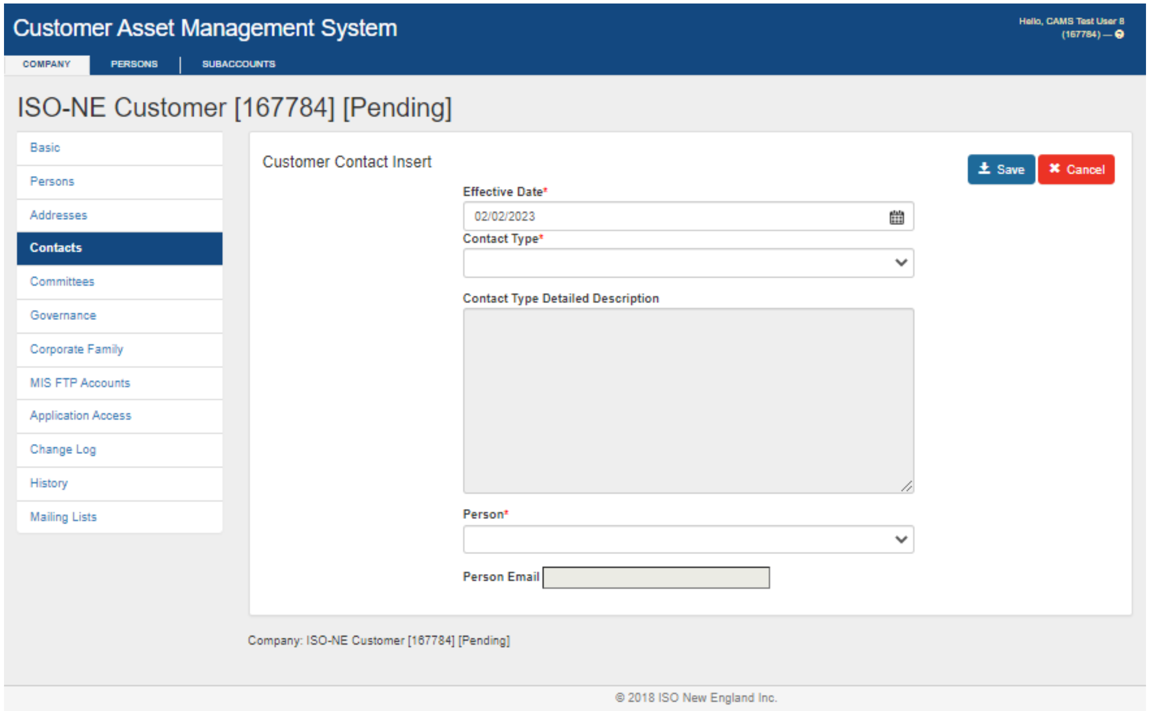


5. The “Customer Contact Listing” page displays:



6. Click the “Add a New Contact” button.

7. The “Customer Contact Insert” screen displays:



8. Select the “Contact Type” from the drop-down box.

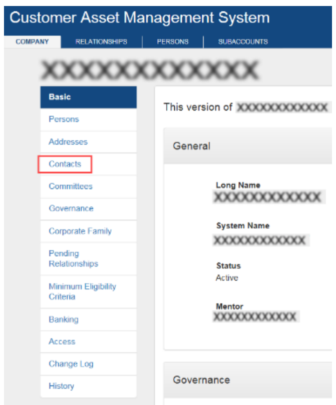
9. Select the name of the person you want to designate as the contact for that type.

10. Click the “Save” button.

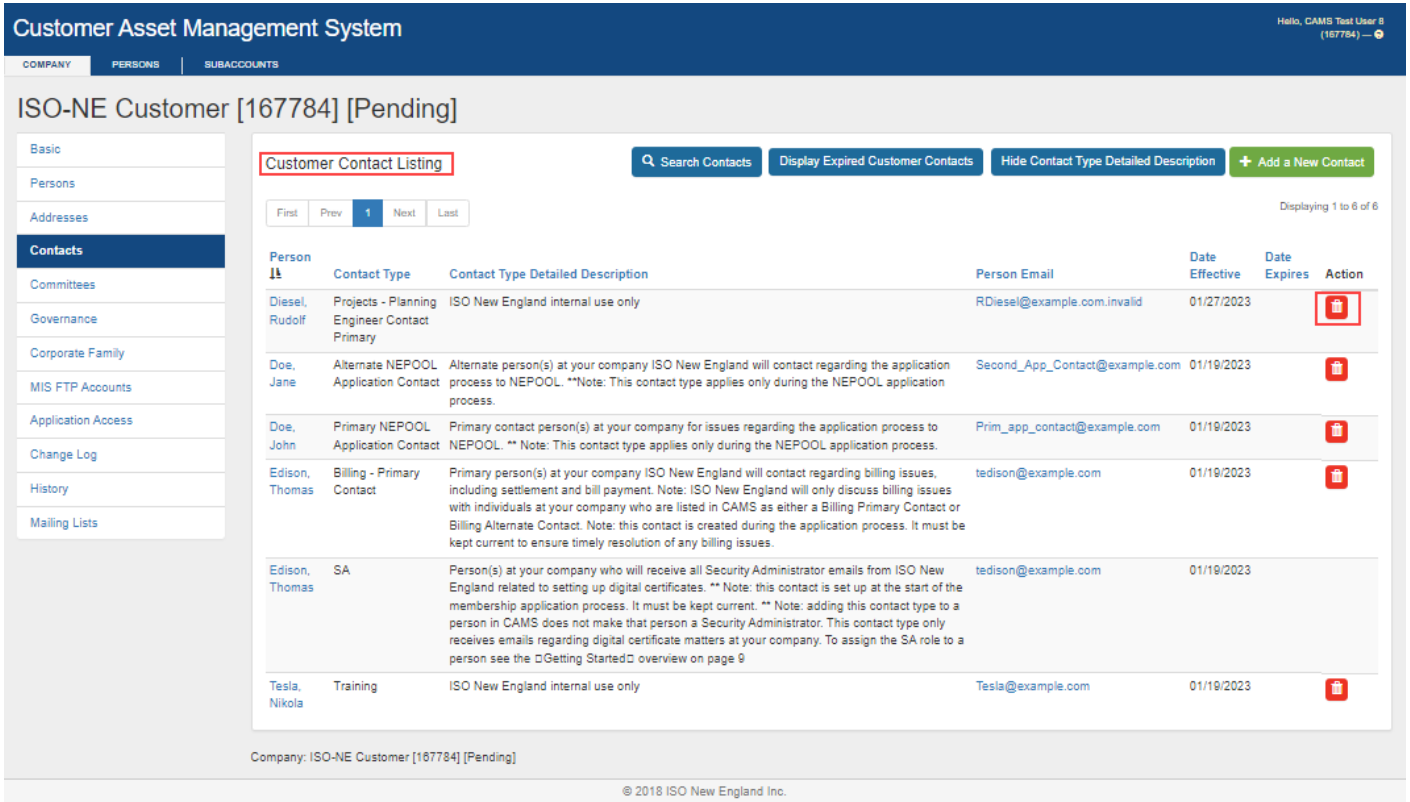
2.3.7.2 Delete contact information

- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer
  - Security Administrator

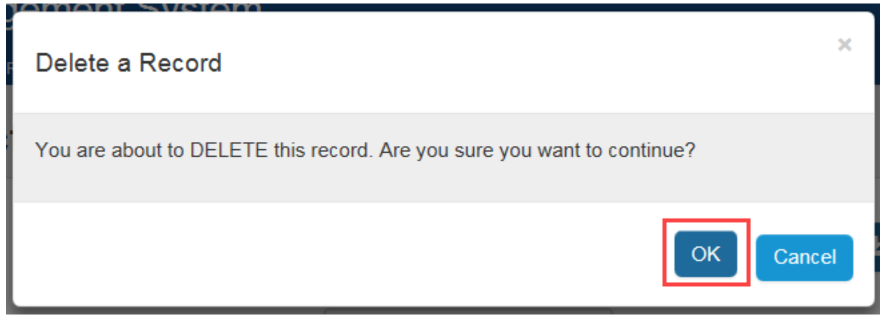
1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Basic" screen displays.
4. Click on the "Contacts" tab in the second-level menu:



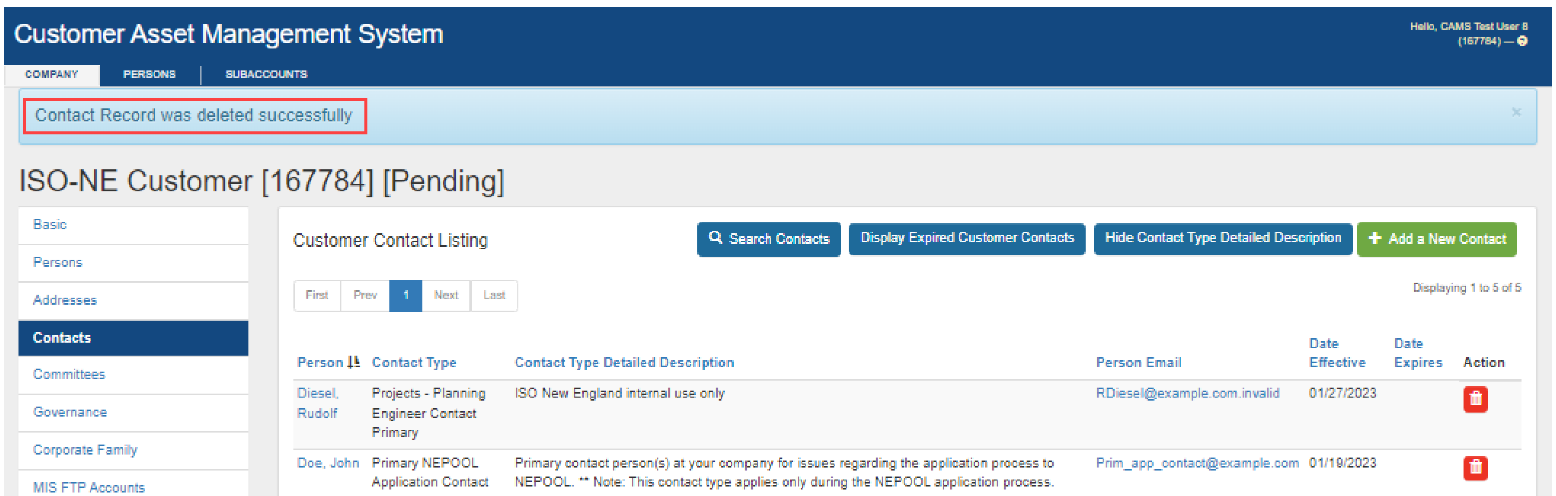
5. The "Customer Contact Listing" page displays.
6. Find the name of the person you want to delete as a contact.
7. Click the red delete icon in the "Action" column.



8. A pop up message is displayed asking for user confirmation to delete or not.



9. Click "OK" button to delete the record.
10. Message is displayed confirming the contact type was deleted:

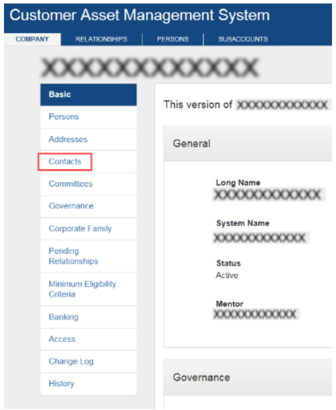


2.3.7.3 View contact information

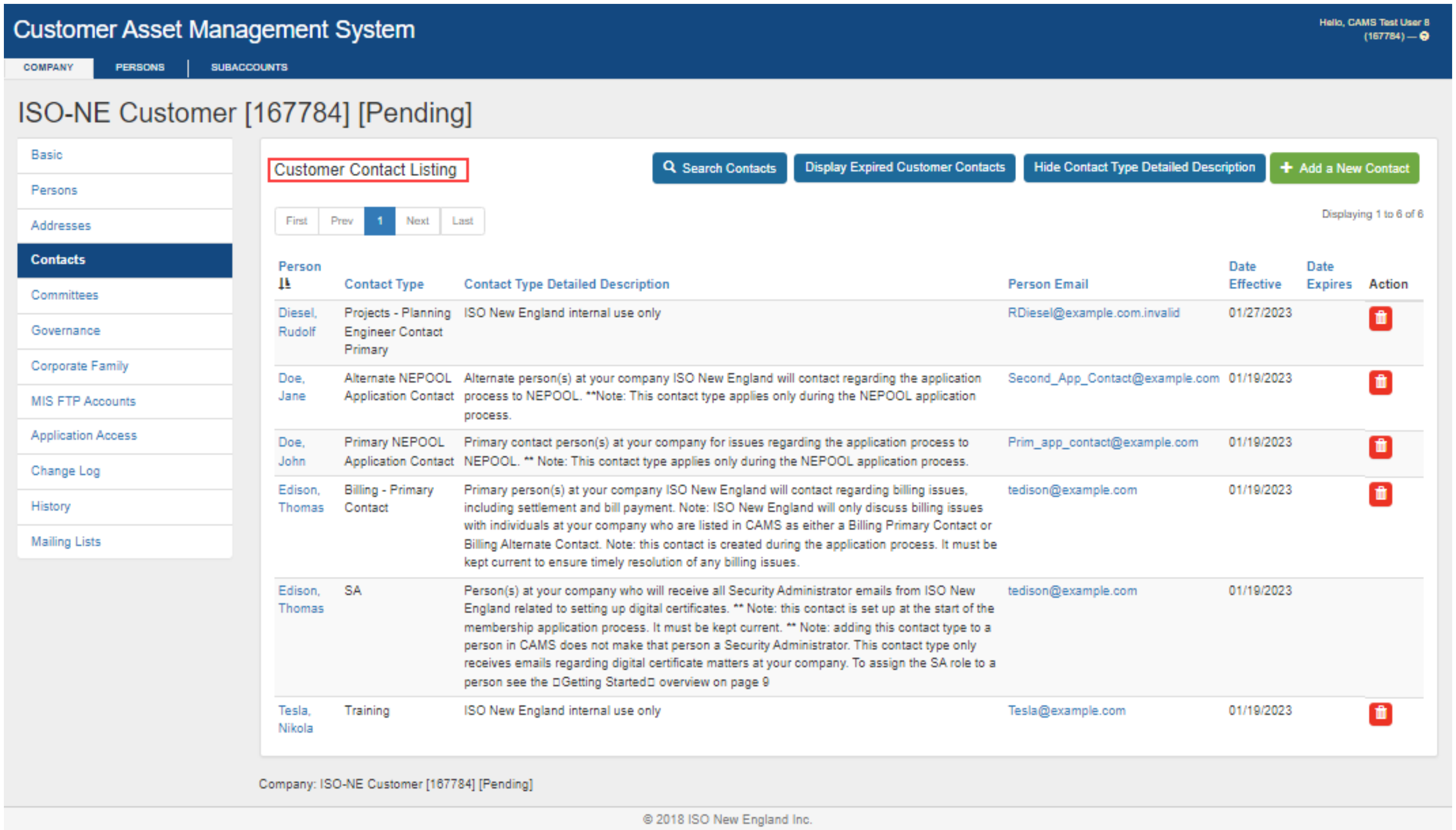
- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer
  - External Person Maintainer

- External Person Viewer
- Security Administrator

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Basic" screen displays.
4. Click on the "Contacts" tab in the second-level menu:



5. The “Customer Contact Listing” page displays:



2.3.8 Committees

- ISO New England has formed specialized committees to assist in ensuring fair and efficient wholesale electricity markets and a reliable bulk power generation and transmission system for the region.
- To learn more about the different committees, see the ISO New England website at https://www.iso-ne.com/committees
- In CAMS a company may:

- designate a primary and/or an alternate member for each committee.
- designate proxy assignments to NEPOOL committees.
- designate information-only contacts to receive correspondence related to the committee

- In CAMS, a company may set mailing list preference for primary, alternate, and proxy committee members. The ISO may use this indicator to exclude primary, alternate and proxy committee members from certain committee related communications. The mailing list preference is set individually for each committee assignment. An update to the mailing preference may take time to be reflected in the corresponding lists.
- Persons must first be entered into the CAMS database before being added to a committee. See "Adding persons to CAMS"

CAUTION

- Individuals listed in CAMS as your company's committee members will also be listed on ISO New England's website at:

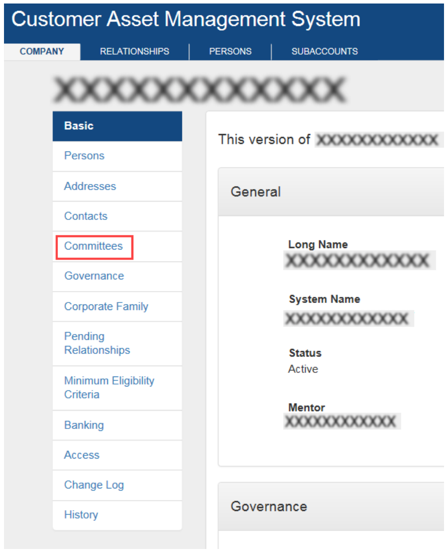
  https://www.iso-ne.com/participate/participant-asset-listings/directory.

2.3.8.1 Add committee memberships

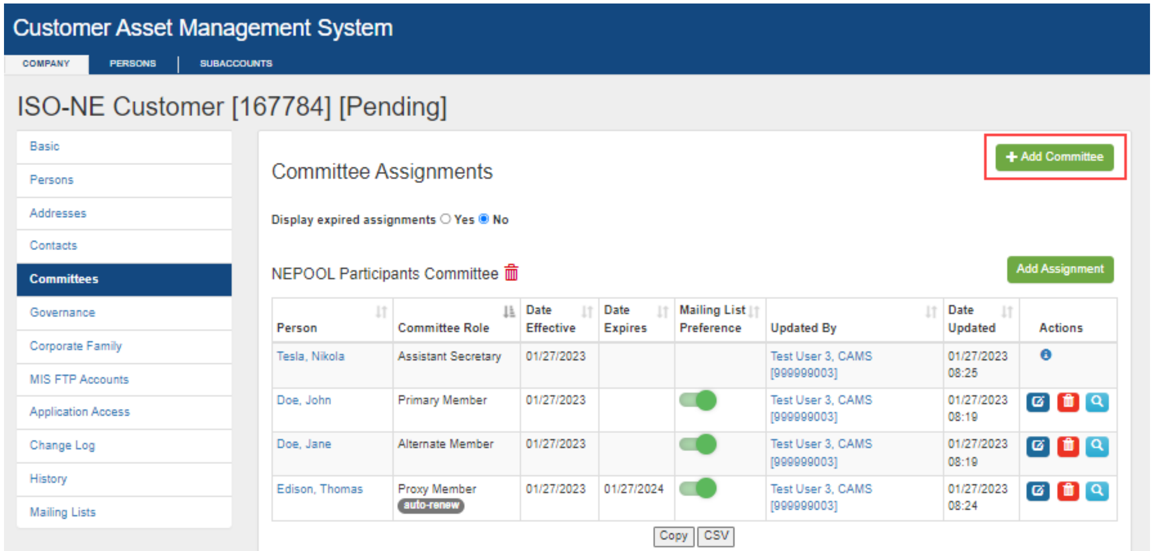
- Roles that can perform this task:
  - External Customer Maintainer
  - Person Maintainer
  - Security Administrator

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Basic" screen displays.

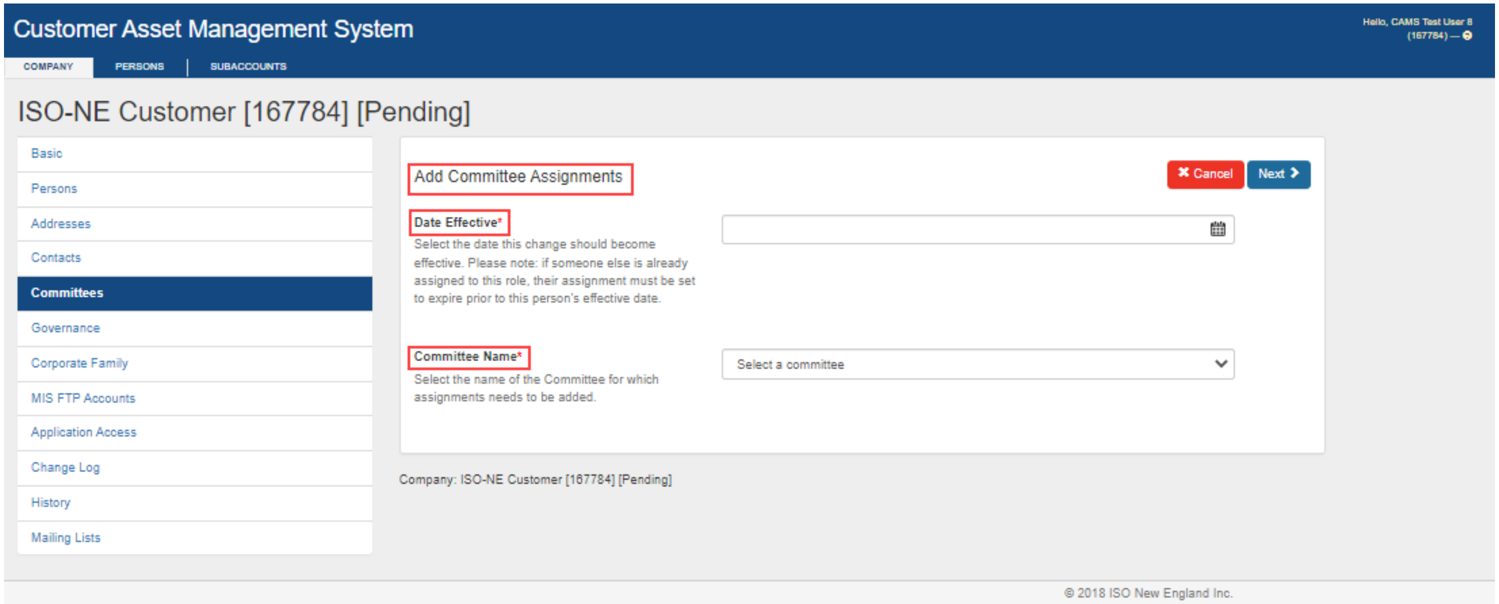
4. Click on the “Committees” tab in the second-level menu:



5. The “Committee Assignments” page displays.



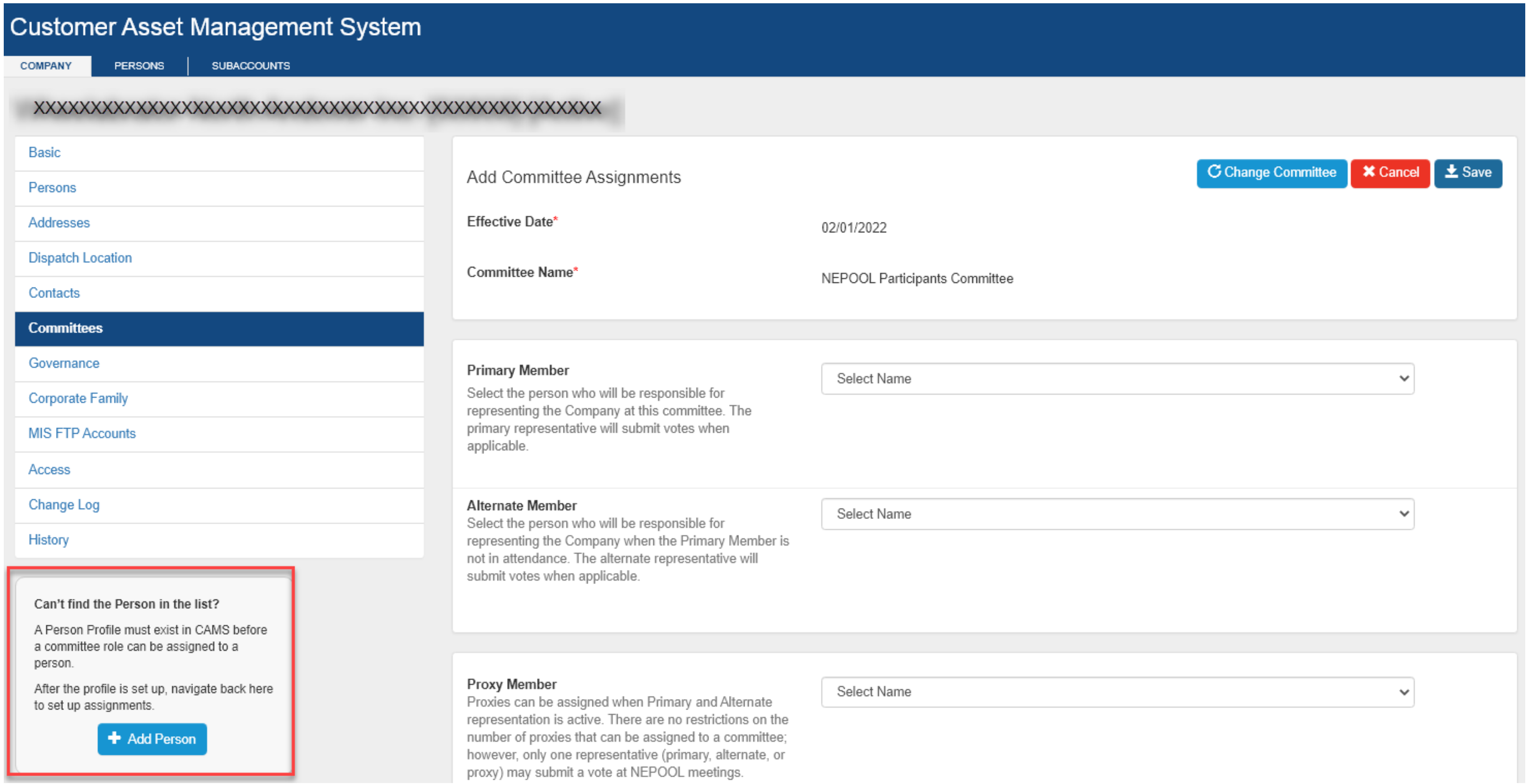
6. The “Add Committee Assignments” screen displays:



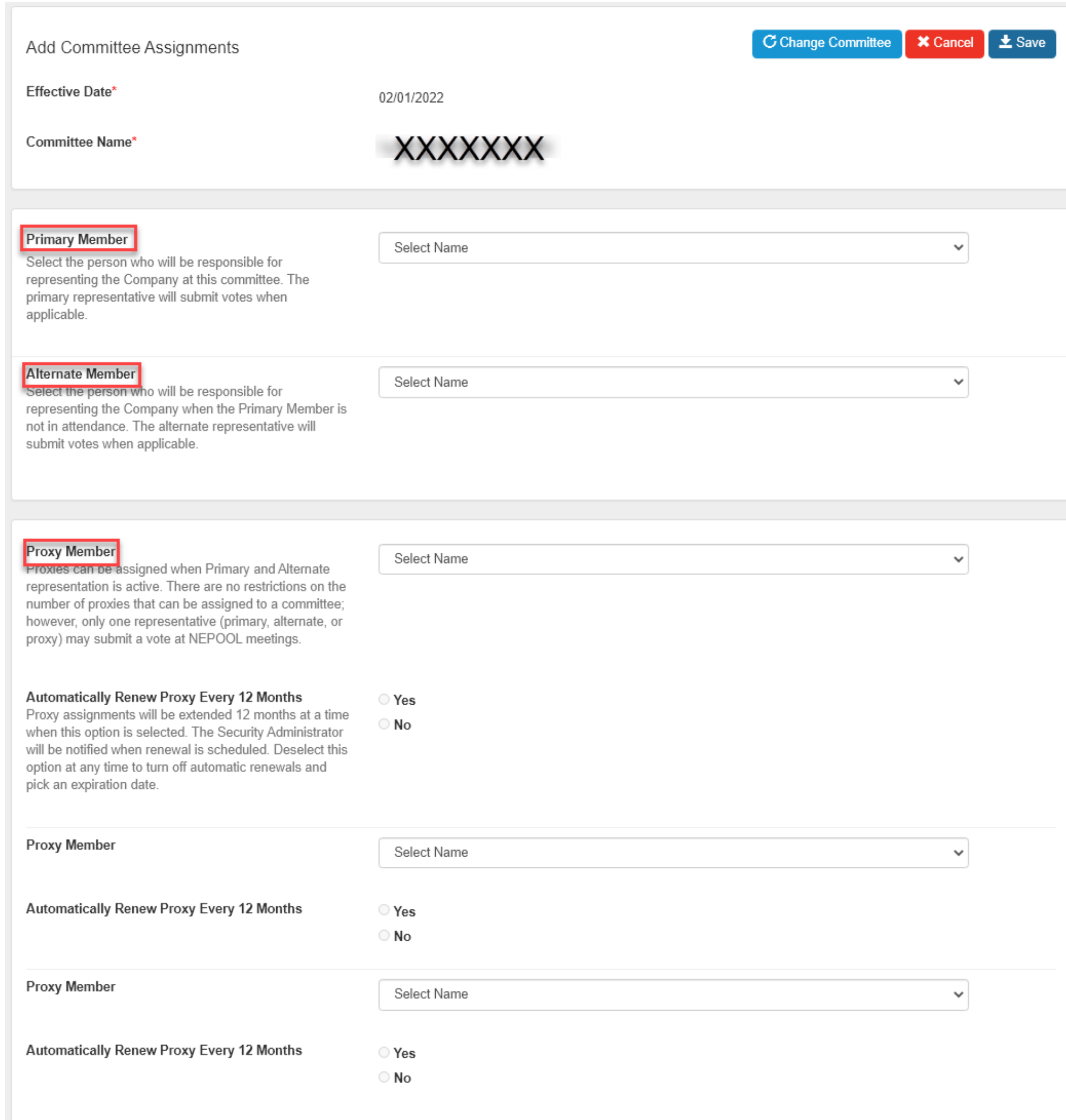
7. Enter the “Date Effective” that the changes will become effective.
8. Select the committee you want from “Committee Name” drop-down box. Click Next.
9. For an explanation of the different committees, see ISO New England’s website at https://www.iso-ne.com/committees/comm_wkgrps/index.html.
10. Select the primary member, alternate member, proxy members or information-only contacts you want to assign from the dropdowns.

Note:

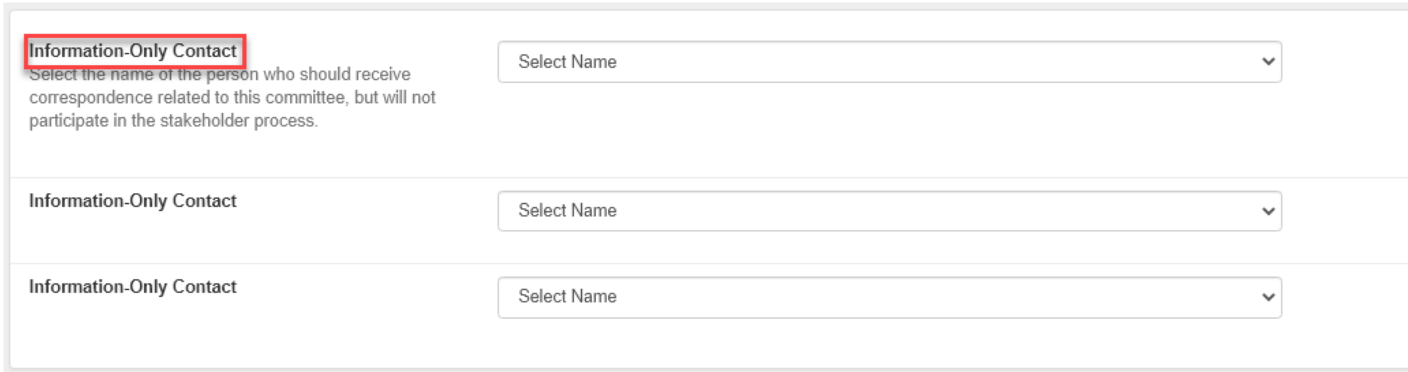
- Primary member, alternate member, and proxy members must be unique from each other.
- A primary or alternate must be assigned before assigning a proxy member.
- You may select “Yes” to automatically renew a proxy every 12 months or select “No” to enter a specific expiration date.
- If the person has not yet been added to CAMS, you must first see “Adding persons to CAMS”



Customer Asset Management System
COMPANY
PERSONS
SUBACCOUNTS
Basic
Persons
Addresses
Dispatch Location
Contacts
Committees
Governance
Corporate Family
MIS FTP Accounts
Access
Change Log
History
Can't find the Person in the list?
A Person Profile must exist in CAMS before a committee role can be assigned to a person.
After the profile is set up, navigate back here to set up assignments.
Add Person
Add Committee Assignments
Change Committee
Cancel
Save
Effective Date*
02/01/2022
Committee Name*
NEPOOL Participants Committee
Primary Member
Select the person who will be responsible for representing the Company at this committee. The primary representative will submit votes when applicable.
Select Name
Alternate Member
Select the person who will be responsible for representing the Company when the Primary Member is not in attendance. The alternate representative will submit votes when applicable.
Select Name
Proxy Member
Proxies can be assigned when Primary and Alternate representation is active. There are no restrictions on the number of proxies that can be assigned to a committee; however, only one representative (primary, alternate, or proxy) may submit a vote at NEPOOL meetings.
Select Name



Add Committee Assignments
Change Committee
Cancel
Save
Effective Date*
02/01/2022
Committee Name*
XXXXXXX
Primary Member
Select the person who will be responsible for representing the Company at this committee. The primary representative will submit votes when applicable.
Select Name
Alternate Member
Select the person who will be responsible for representing the Company when the Primary Member is not in attendance. The alternate representative will submit votes when applicable.
Select Name
Proxy Member
Proxies can be assigned when Primary and Alternate representation is active. There are no restrictions on the number of proxies that can be assigned to a committee; however, only one representative (primary, alternate, or proxy) may submit a vote at NEPOOL meetings.
Select Name
Automatically Renew Proxy Every 12 Months
Proxy assignments will be extended 12 months at a time when this option is selected. The Security Administrator will be notified when renewal is scheduled. Deselect this option at any time to turn off automatic renewals and pick an expiration date.
Yes
No
Proxy Member
Select Name
Automatically Renew Proxy Every 12 Months
Yes
No
Proxy Member
Select Name
Automatically Renew Proxy Every 12 Months
Yes
No



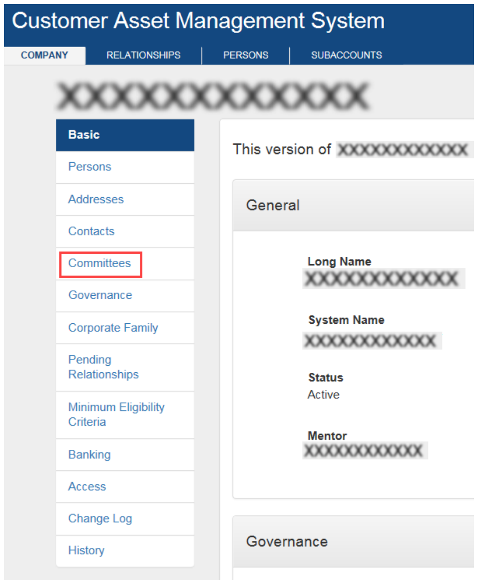
11. Click the “Save” button.

2.3.8.2 Add individual assignments

- Roles that can perform this task:
  - External Customer Maintainer
  - Person Maintainer
  - Security Administrator

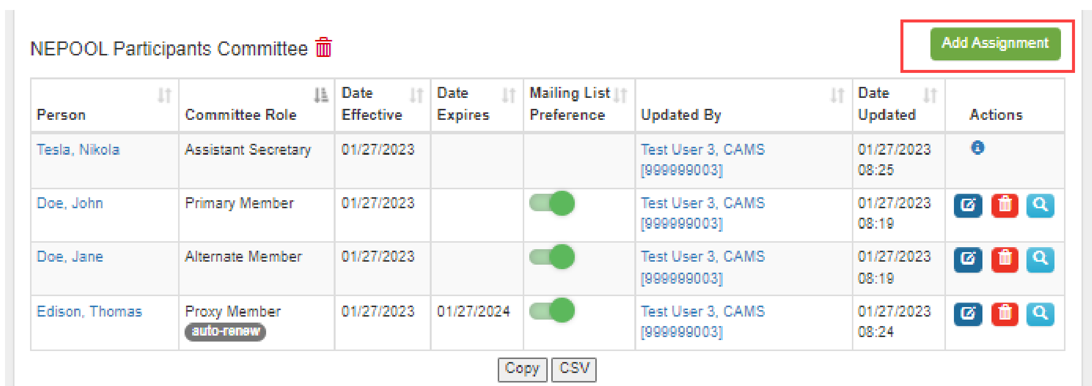
1. Launch the CAMS interface. See “Accessing CAMS”
2. Click on “Company” in the top-level menu.
3. The “Basic” screen displays.

4. Click on the “Committees” tab in the second-level menu:



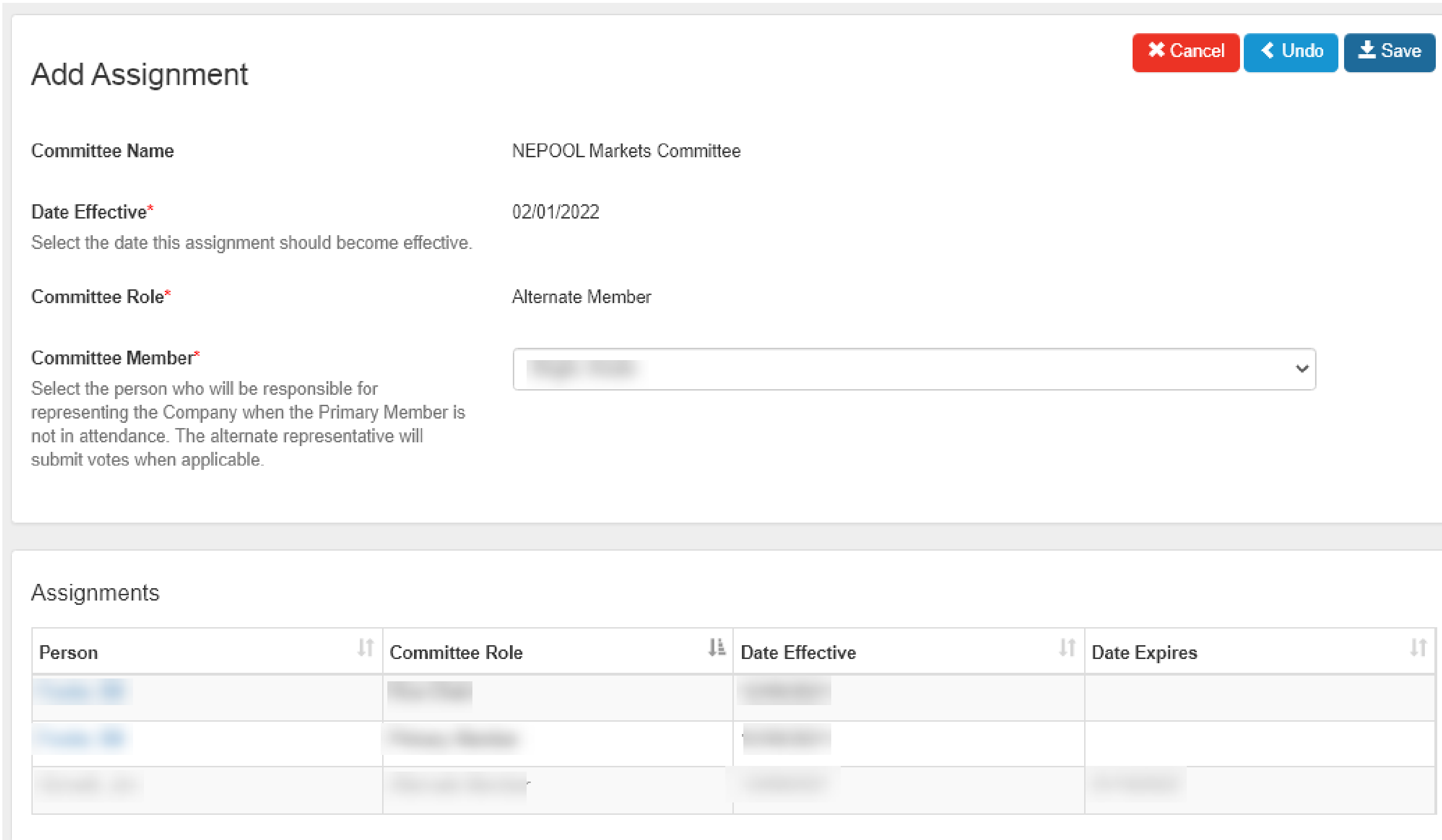
5. The “Committee Assignments” page displays.

6. Click “Add Assignment” next to the committee you want to add an assignment to.



7. Select the “Date Effective” the assignment will become effective. Click “Next”.

8. Select the “Committee Role” you are adding to the committee. Click “Next”.
9. Select the “Committee Member” you are adding to the committee from the drop-down. Click “Save”. (Note: You can see the active “Assignment” already on the committee under the “Add Assignment” section of the screen.)

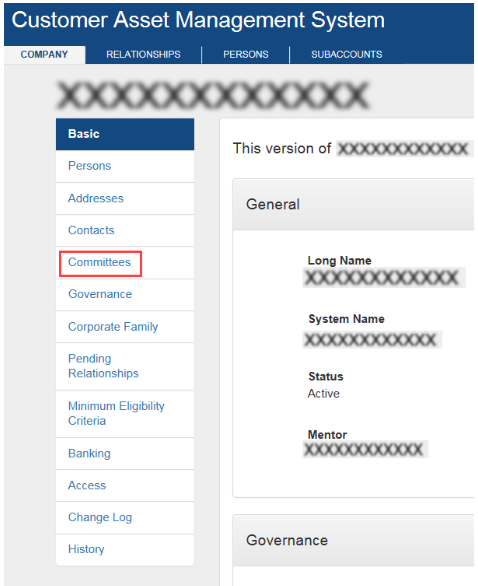


2.3.8.3 Update a committee assignment

- Roles that can perform this task:

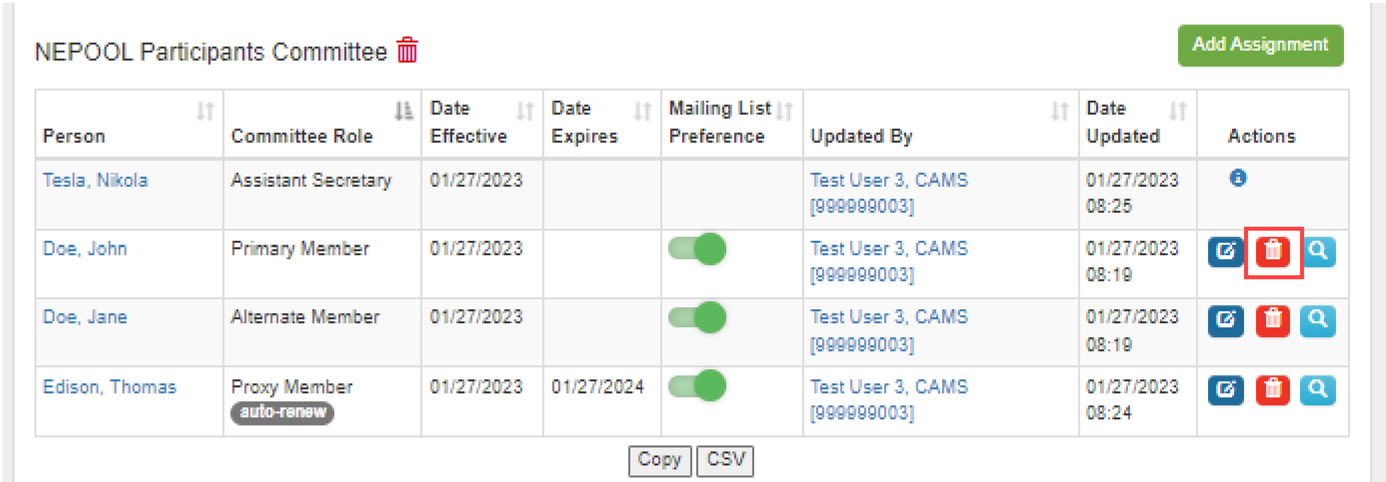
- External Customer Maintainer
- Person Maintainer
- Security Administrator

1. Launch the CAMS interface. See "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Basic" screen displays.
4. Click on the "Committees" tab in the second-level menu:

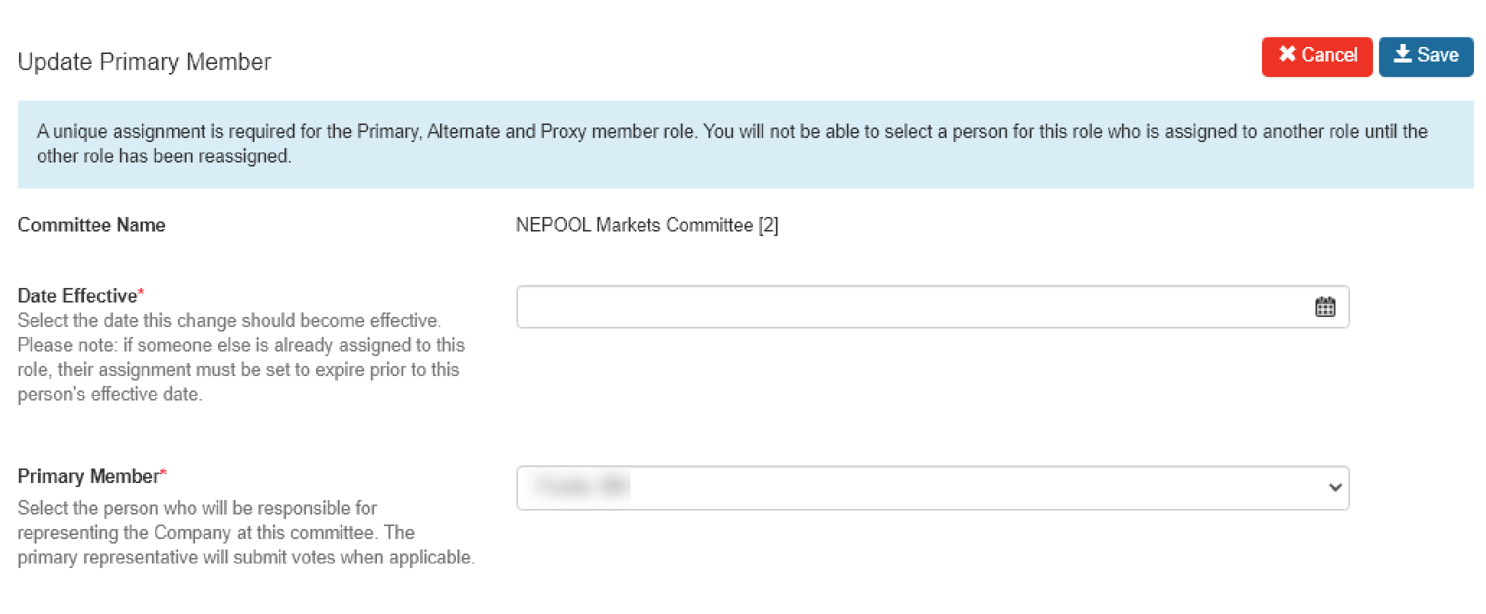


5. The "Committee Assignments" page displays.
6. Find the committee assignment you wish to modify in the list.
   a. If there is a proxy assignment and you are attempting to modify the only member assigned to the committee you must expire the proxy assignment first, then modify the member, and add the proxy back to the committee, if applicable.

7. Click the pencil icon in the “Action” column for that row:



8. The “Update Member” screen displays.



9. Select the "Date Effective" this update will become effective.
10. Use the drop-down box to select a different person.
11. Click "Save".
12. Message is displayed confirming the committee assignment was updated:

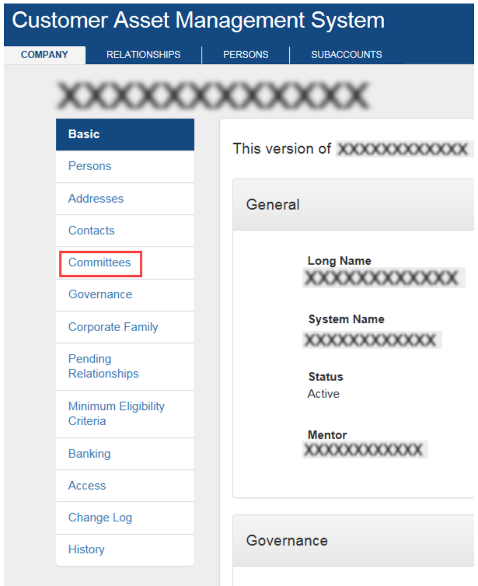
2.3.8.4 Delete a committee

- Roles that can perform this task:
    - External Customer Maintainer

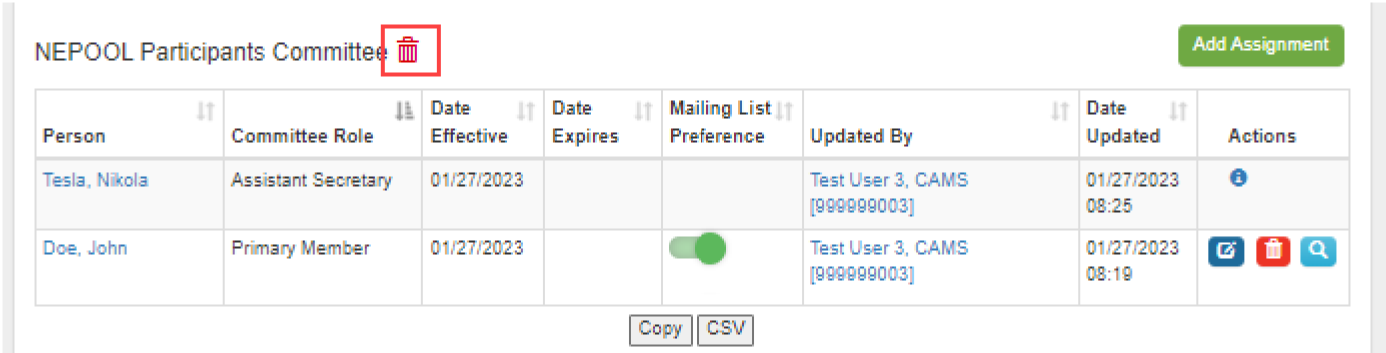
- Person Maintainer
- Security Administrator

NOTE: This action will delete the committee entirely. You can add it again at any time.

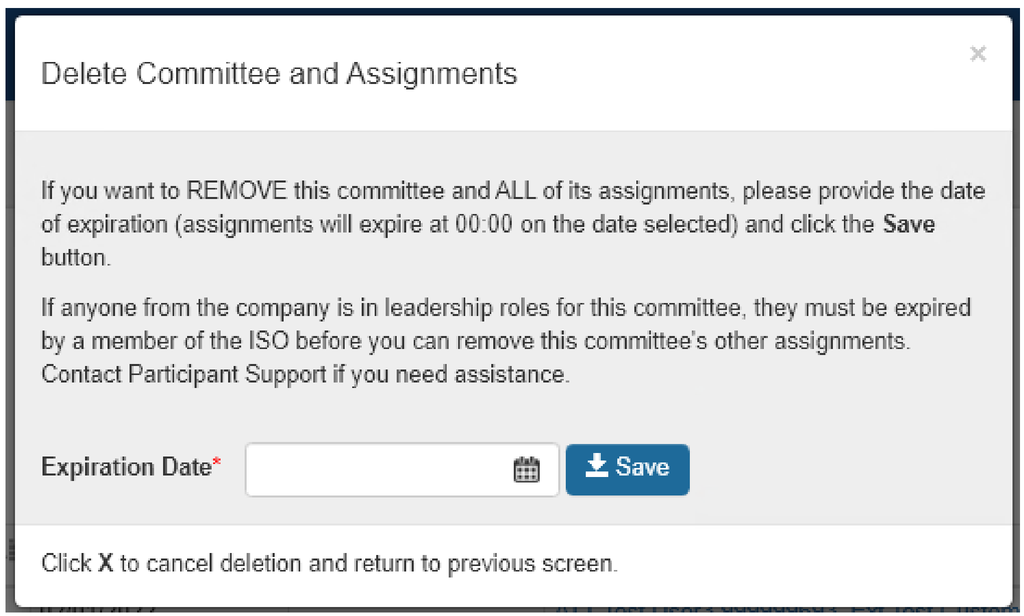
1. Launch the CAMS interface. See "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Basic" screen displays.
4. Click on the "Committees" tab in the second-level menu:



5. The "Committee Assignments" page displays.
6. Locate the committee you wish to delete.
7. Click on the "**Trash Can**" icon next to the committee you wish to delete.



8. A pop up message is displayed asking for the "Expiration Date" which the committee and its assignments will be deleted. Enter the Expiration Date in which you want the deletion to occur.



9. Click "Save" to delete the committee.

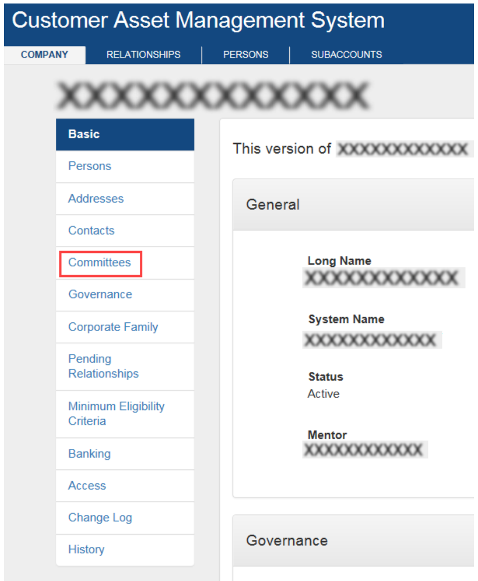
10. Message is displayed confirming the committee was deleted:

2.3.8.5 Delete individual committee assignment

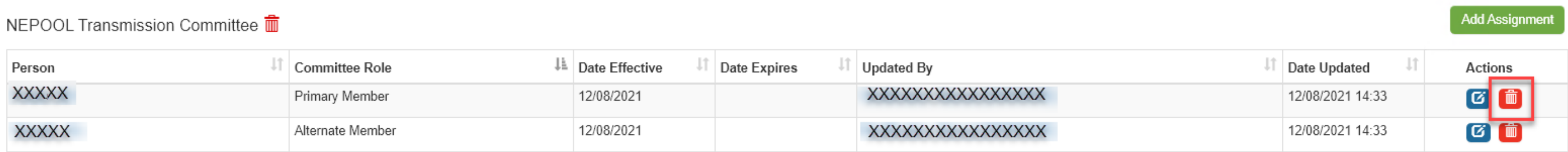
- Roles that can perform this task:
  - External Customer Maintainer
  - Person Maintainer
  - Security Administrator

1. Launch the CAMS interface. See "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Basic" screen displays.

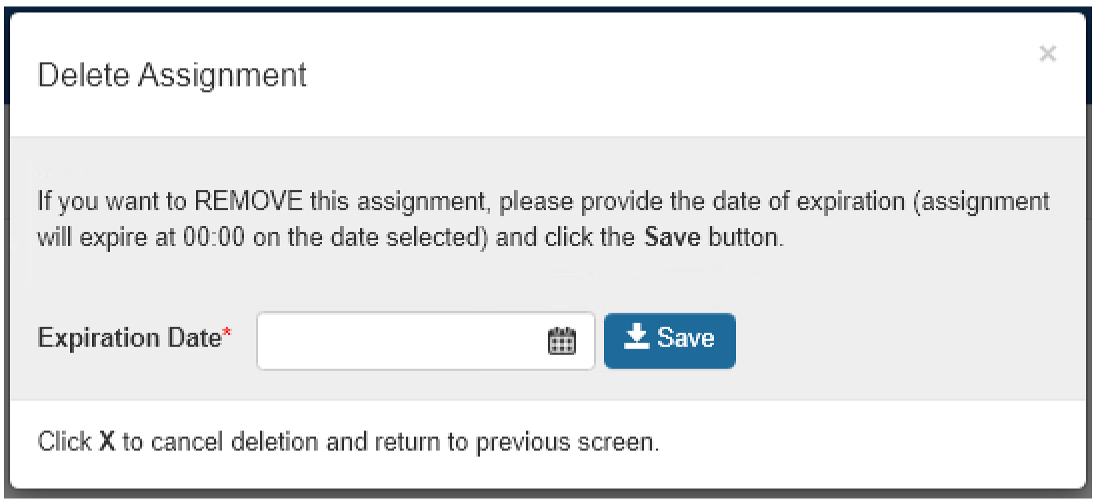
4. Click on the "Committees" tab in the second-level menu:



5. The "Committee Assignments" page displays.
6. Locate the record you want to delete.
    a. If there is only one member assigned to the committee and a proxy exists, expire the proxy first. If a new member is added, you can add a proxy again.
    b. If there are two members assigned to the committee and a proxy exists, expire one member and add its replacement, then expire the other member and add its replacement. In this case you do not need to expire the proxy because one member is active throughout the the process.
7. Click on the "**Trash Can**" icon next to the assignment you wish to delete.



8. A pop up message is displayed asking for the "Expiration Date" which the assignment will be deleted. Enter the Expiration Date in which you want the deletion to occur.

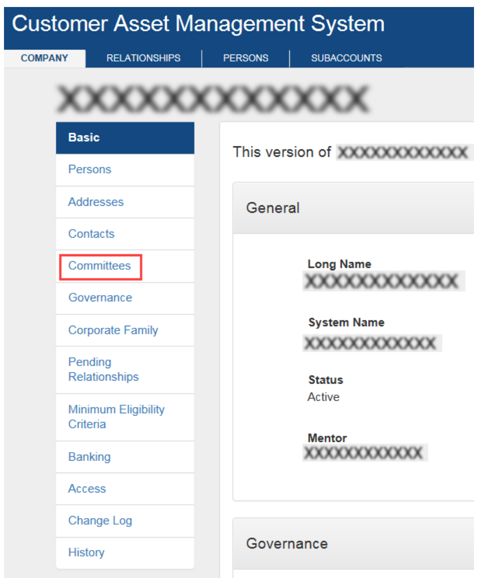


9. Click "Save" to delete the committee assignment.
10. Message is displayed confirming the committee assignment was deleted:

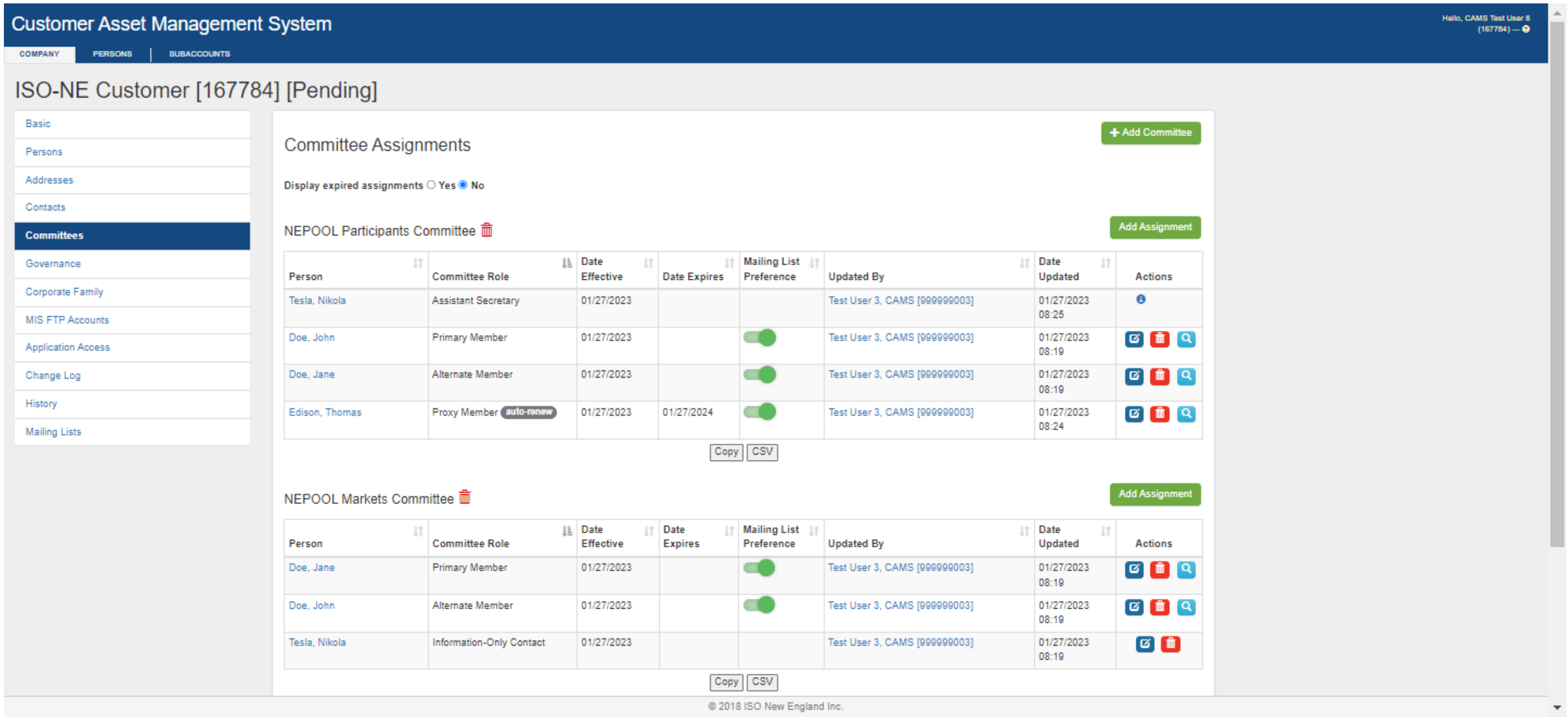
2.3.8.6 View committee listings

- Roles that can perform this task:
    - External Customer Maintainer
    - External Customer Viewer
    - External Person Maintainer
    - External Person Viewer
    - Security Administrator

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Basic" screen displays.
4. Click on the "Committees" tab in the second-level menu:



5. The “Customer Committee Listing” page displays:



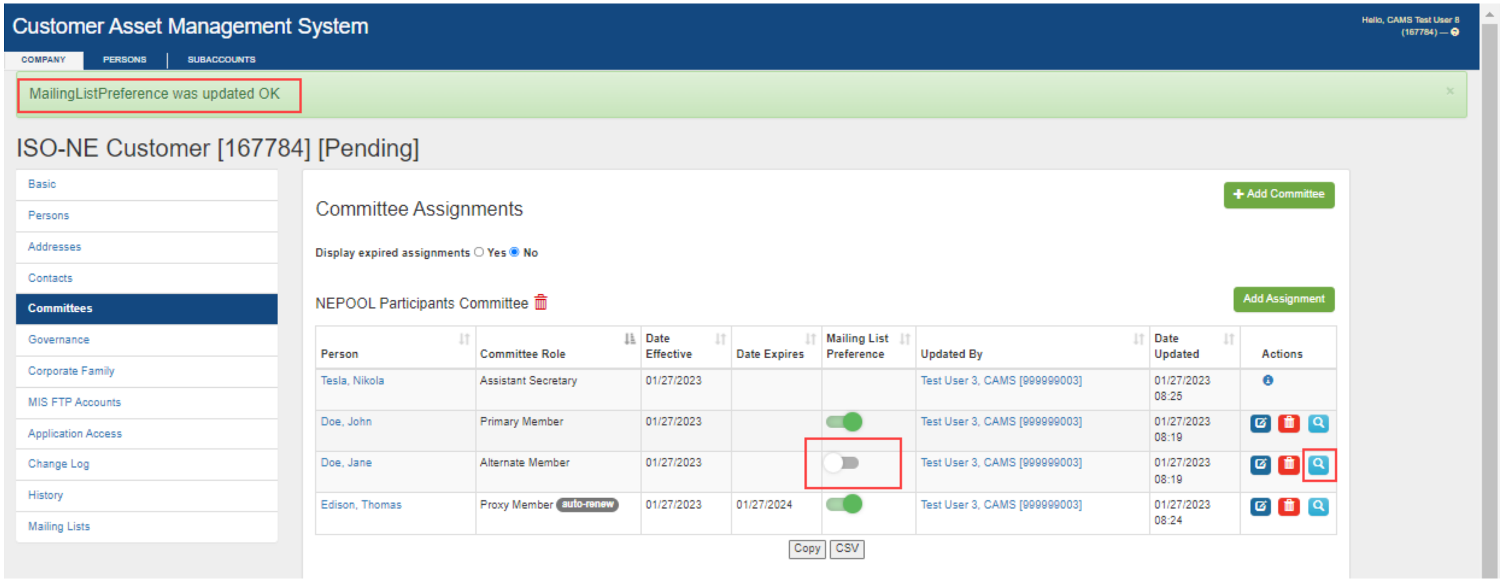
6. The “Customer Committee Listing” shows any committees in which your company currently has membership.

2.3.8.7 Manage mailing list preference

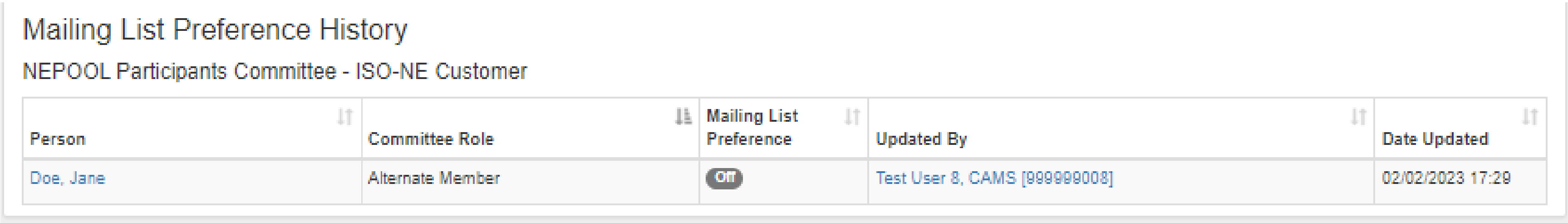
- Roles that can perform this task:
    - External Customer Maintainer
    - Person Maintainer
    - Security Administrator

1. Launch the CAMS interface. See the “[Accessing CAMS](#)”

2. Click on “Company” in the top-level menu.
3. The “Basic” screen displays.
4. Click on the “Committees” tab in the second-level menu:
5. Click the toggle for the committee member you wish to change the mailing list preference setting on. A success message is displayed, indicating an update has taken place.



6. To view mailing list preference history click the magnifine glass icon on the far right of the committee assignment record.



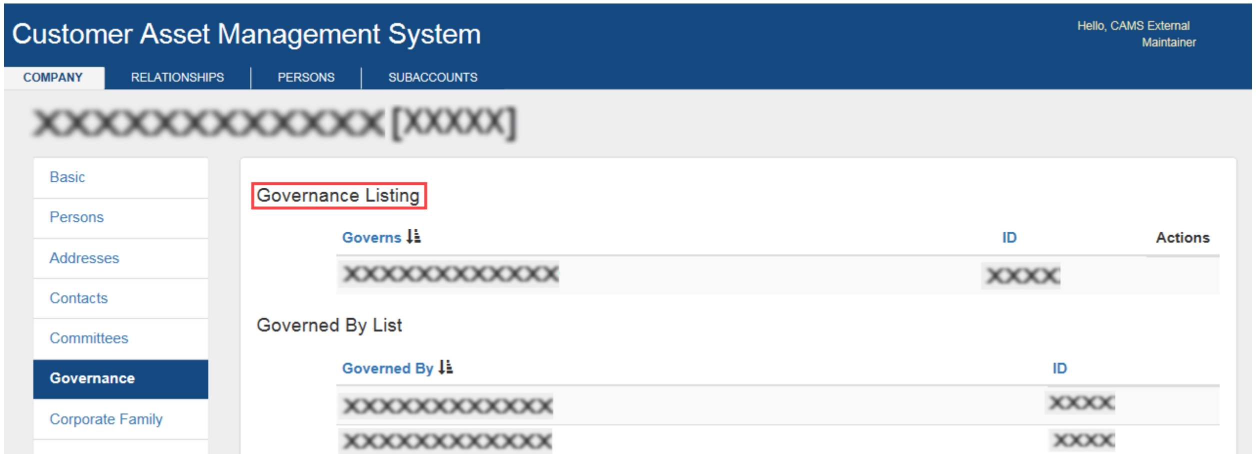
2.3.9 Governance

- The “Governance” tab displays any governance relationships your company has with other companies in CAMS.

2.3.9.1 View Governance Listing

- Roles that can perform this task:
    - External Customer Maintainer
    - External Customer Viewer
    - External Person Maintainer
    - External Person Viewer
    - Security Administrator

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Company” in the top-level menu.
3. The “B” screen displays.
4. Click on the “Governance” tab in the second-level menu.
5. “Governance Listing” and “Governed By List” displays:



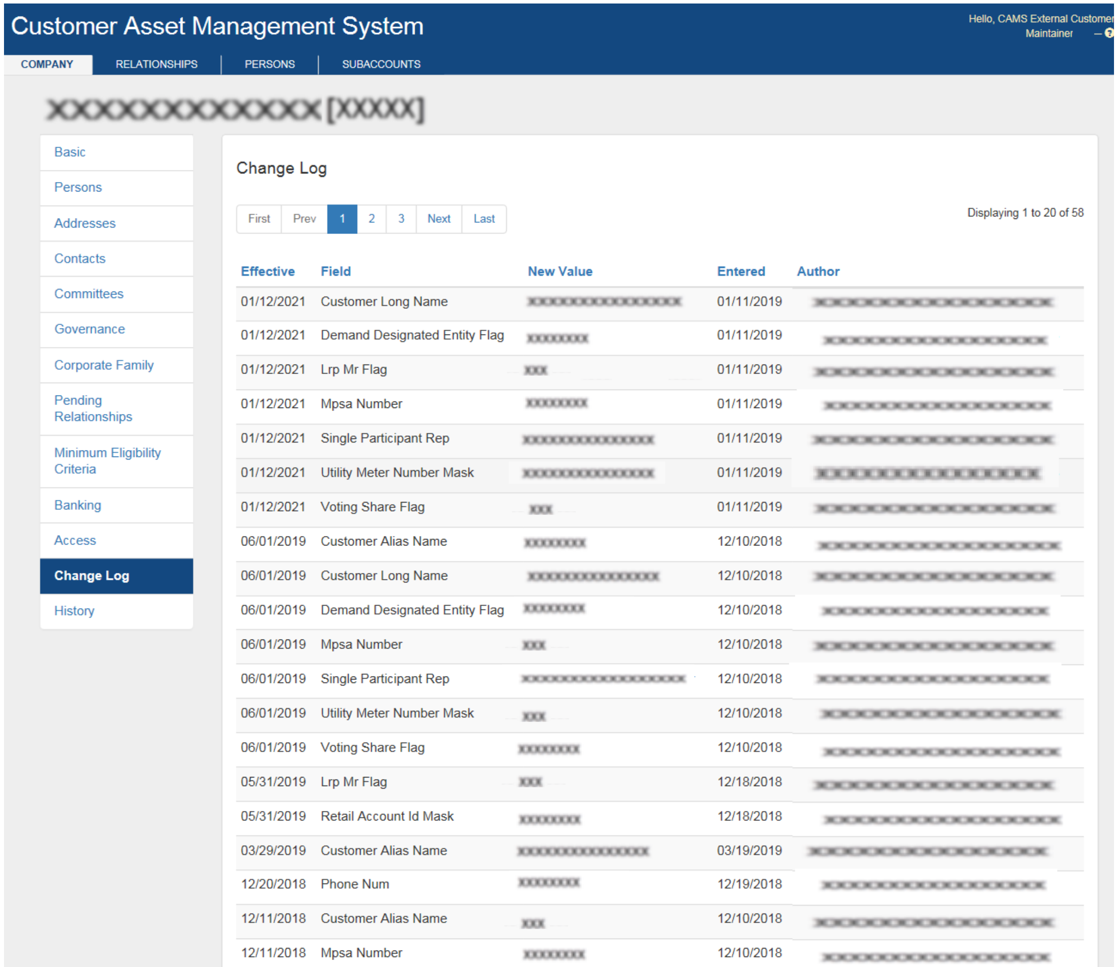
2.3.10 Change Log

- The Change Log is an audit trail showing what company information was changed, when and by whom.

2.3.10.1 View change log listing

- Roles that can perform this task:
    - External Customer Maintainer
    - External Customer Viewer
    - External Person Maintainer
    - External Person Viewer
    - Security Administrator

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Company” in the top-level menu.
3. The “Basic” screen displays.
4. Click on the “Change Log” tab in the second-level menu.
5. “Customer Change Log” screen displays:



2.3.11 Mailing List

- Mailing Lists is a menu item that displays mailing list memberships for your company's persons.
- ISO New England uses an application to manage mailing lists used for communicating with customers and stakeholders. Lists fall into two broad categories, "Managed" and "Subscribable".

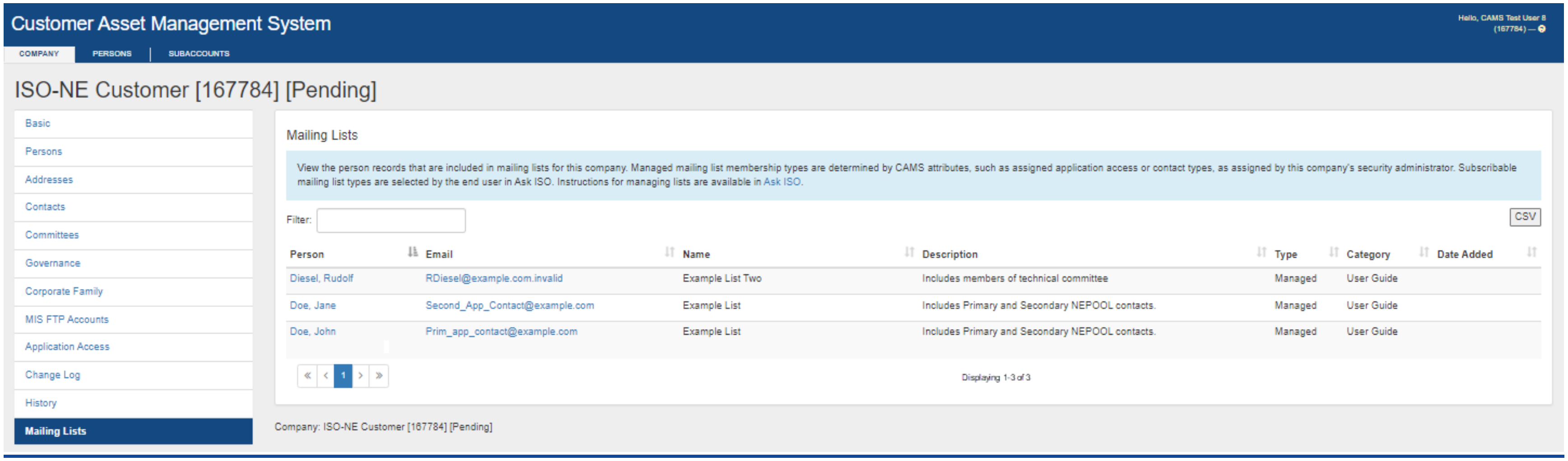
- Managed lists are comprised of users who are identified by various attributes on the person record in CAMS or other data sources. These attributes include committee assignments, the various contact types on a CAMS Person record, being a contact managed in FCTS in connection to a project, or being an ISO-TEN user who has registered for training. Your company's security administrator (SA) can subscribe or unsubscribe you from a managed list by managing the underlying attribute that dynamically added you to a list.
- Subscribable lists allow individuals to take action on their subscriptions in Ask ISO. This replaces the subscription options from Mailing Lists page from the ISO New England website.

- List mebership is displayed in CAMS based on visibility settings set by the ISO and the type of list. Members of visibile lists that are dynamically assigned will be displayed if they meet the list criteria based on attributes associated to your company. Members of Subscribable lists are displayed if they have a CAMS person record for your company and ther email domain is assigned to your company.
- Managed lists typically provide a detailed description of the attributes used to dynamically assign membership. Actions taken to modify such attributes might not be immediately reflected in list membership. The next time the list is compiled changes will be reflected.

2.3.11.1 View Mailing List information

- Roles that can perform this task:
  - External SA
  - External Customer Maintainer
  - External Customer Viewer
  - External Person Maintainer
  - External Person Viewer

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Company" in the top-level menu.
3. The "Basic" screen displays in the Basic tab.
4. Click on the "Mailing List" tab in the second-level menu.
5. "Mailing List" screen displays:



2.3.12 Data Universal Numbering System (DUNS)

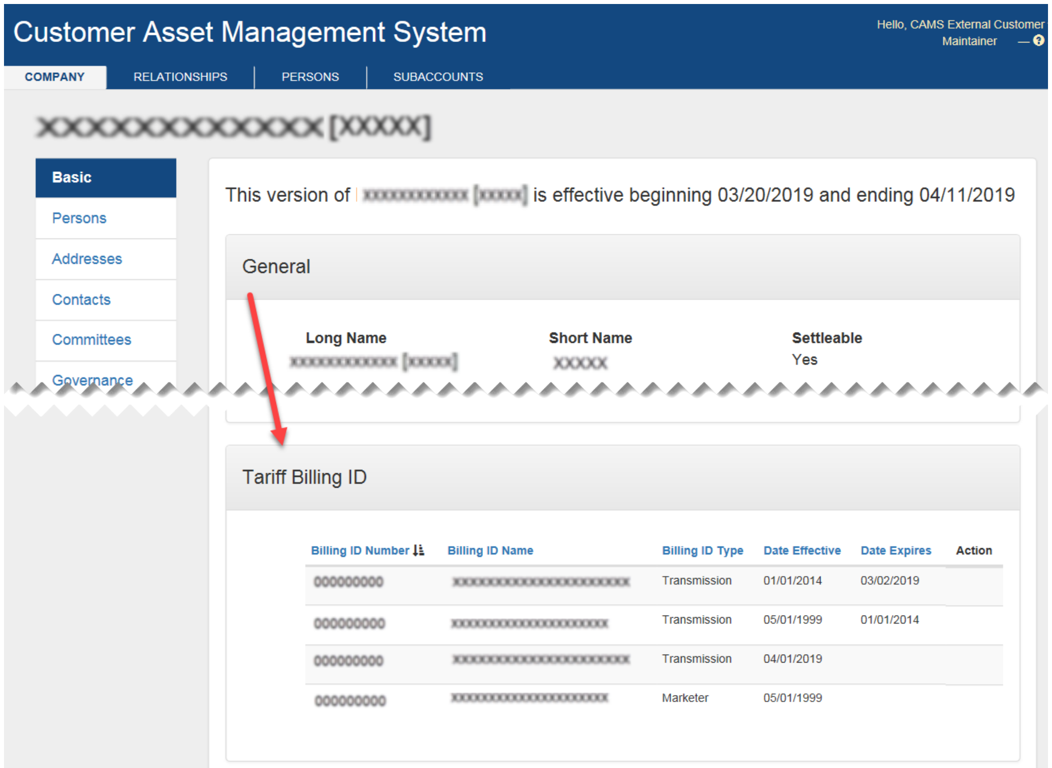
- See the Dun and Bradstreet website for details on DUNS numbers at https://www.dnb.com/.

2.3.12.1 View DUNS information

- Role that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Company” in the top-level menu.

3. The “Basic” screen displays in the Basic tab:
4. Scroll down, the “DUNS” information is displayed in the “Tariff Billing ID” table.

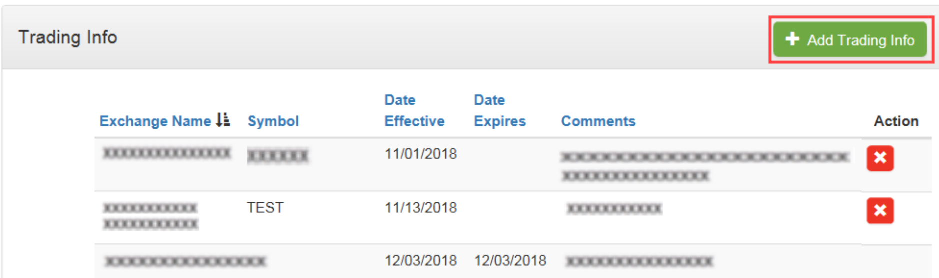


2.3.13 Trading information

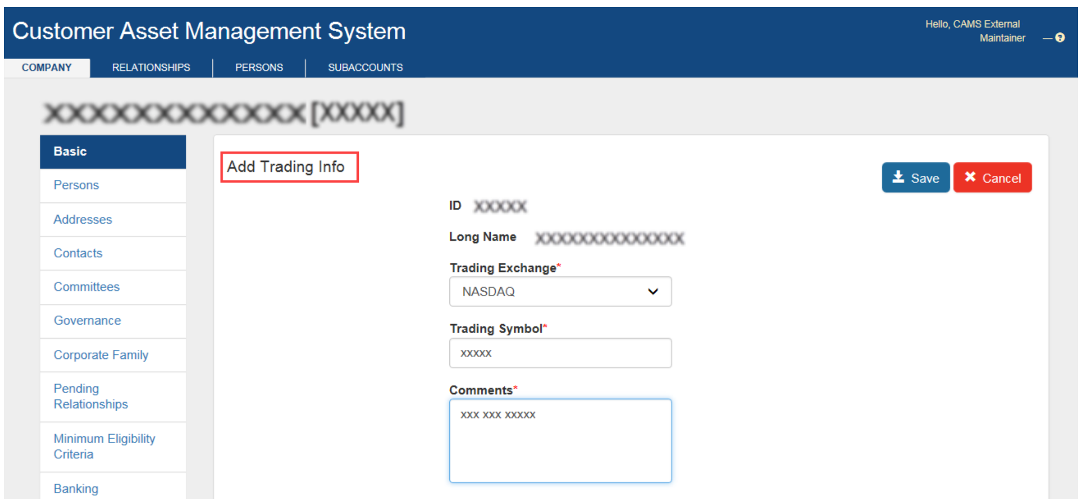
2.3.13.1 Add trading information

- Role that can perform this task:
    - External Customer Maintainer

6. Launch the CAMS interface. See the "Accessing CAMS"
7. Click on "Company" in the top-level menu.
8. The "Basic" screen displays in the Basic tab.
9. Click on the "Add Trading Info" button in the "Trading Info" section:



10. The "Add Trading Info" screen displays:

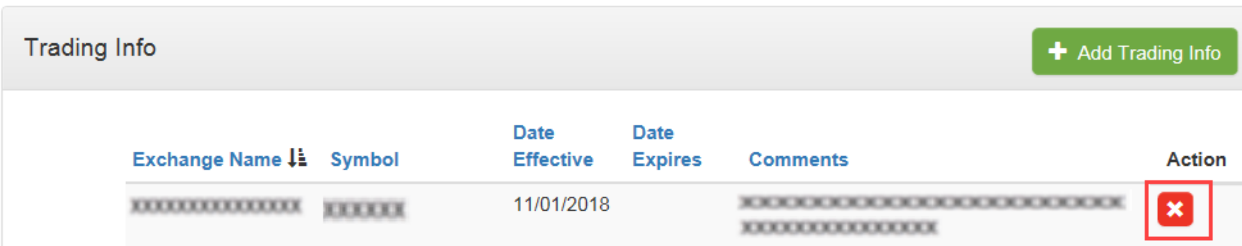


11. Enter the required fields.
12. Click "Add" button.

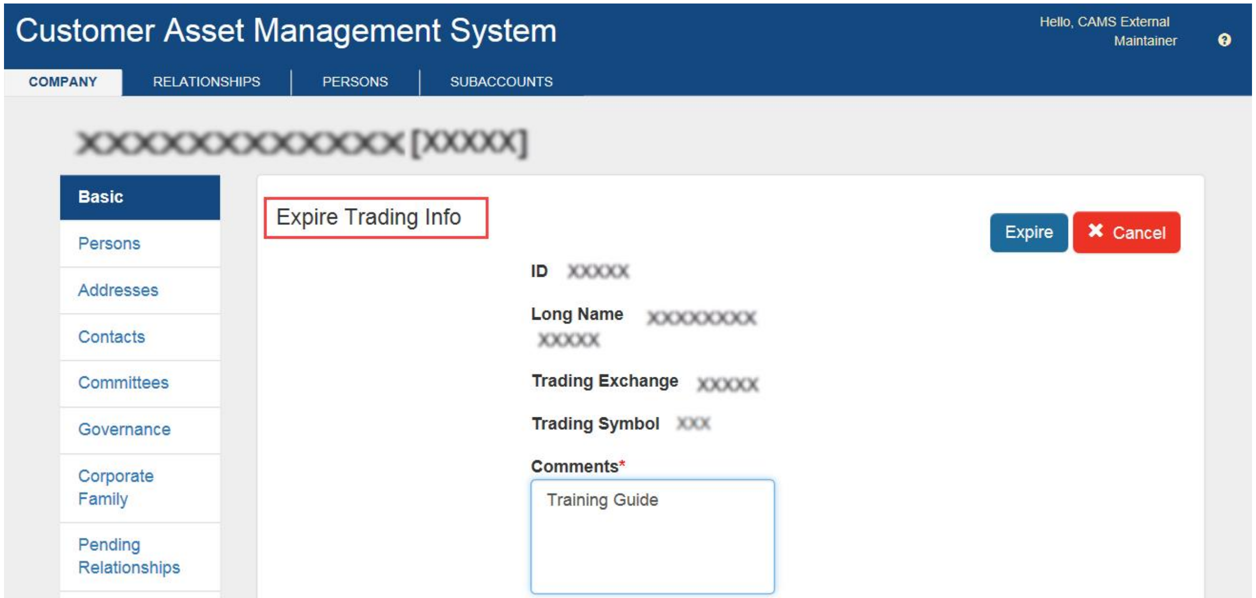
2.3.13.2 Delete trading information

- Role that can perform this task:
  - External Customer Maintainer

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Company” in the top-level menu.
3. The “Customer View” screen displays in the Basic tab.
4. Locate the entry you want to delete in the “Trading Info” table.
5. Click the “**X**” icon in the “Action” column for that row:



6. The “Expire Trading Info” screen displays:

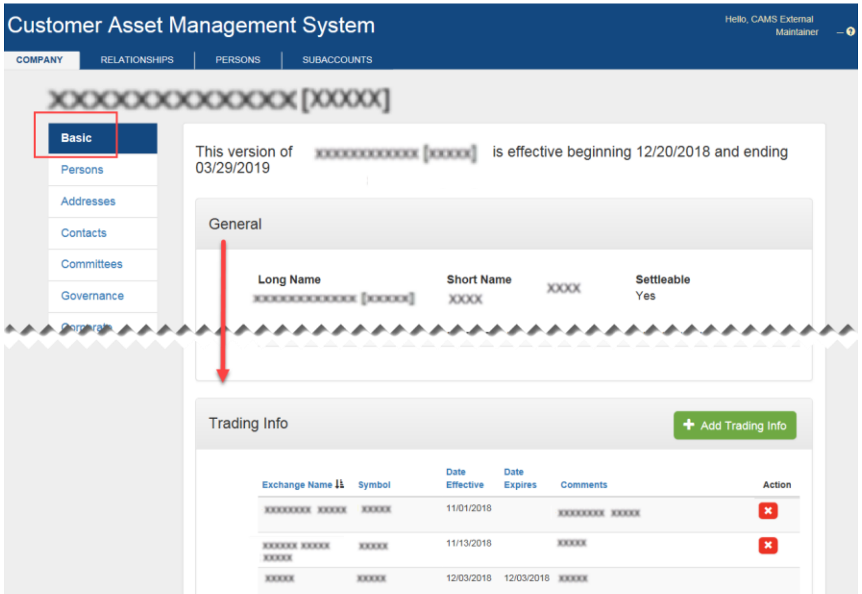


7. Enter a comment to substantiate the deletion.
8. Click on “Submit” to delete the selected trading information.

2.3.13.3 View trading information

- Roles that can perform this task:
    - External Customer Maintainer
    - External Customer Viewer

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Company” in the top-level menu.
3. The “Basic” screen is displayed:

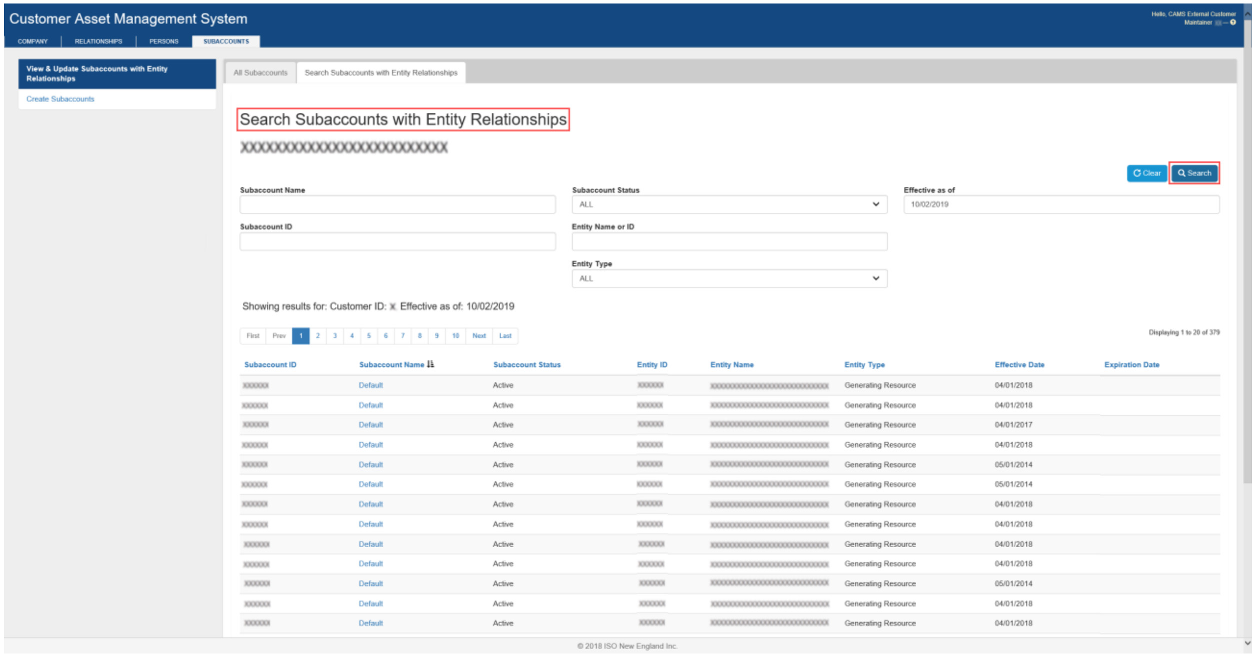


4. The "Trading Info" section displays the trading information.

2.3.14 Subaccount information

Divisional accounting allows customers to assign market activity to a subaccount or division for settlement reporting. Assets or “entities”, such as generators, load assets, asset-related demand (ARD), demand assets, resources, and network loads can be assigned to a subaccount and have the charges and credits of those entities separated by subaccount in the settlement reporting. Customers are not required to enable subaccount reporting (see “Click on “Search Subaccounts with Entity Relationships” in the second-level menu.

1. The “Search Subaccounts with Entity Relationships” screen displays:

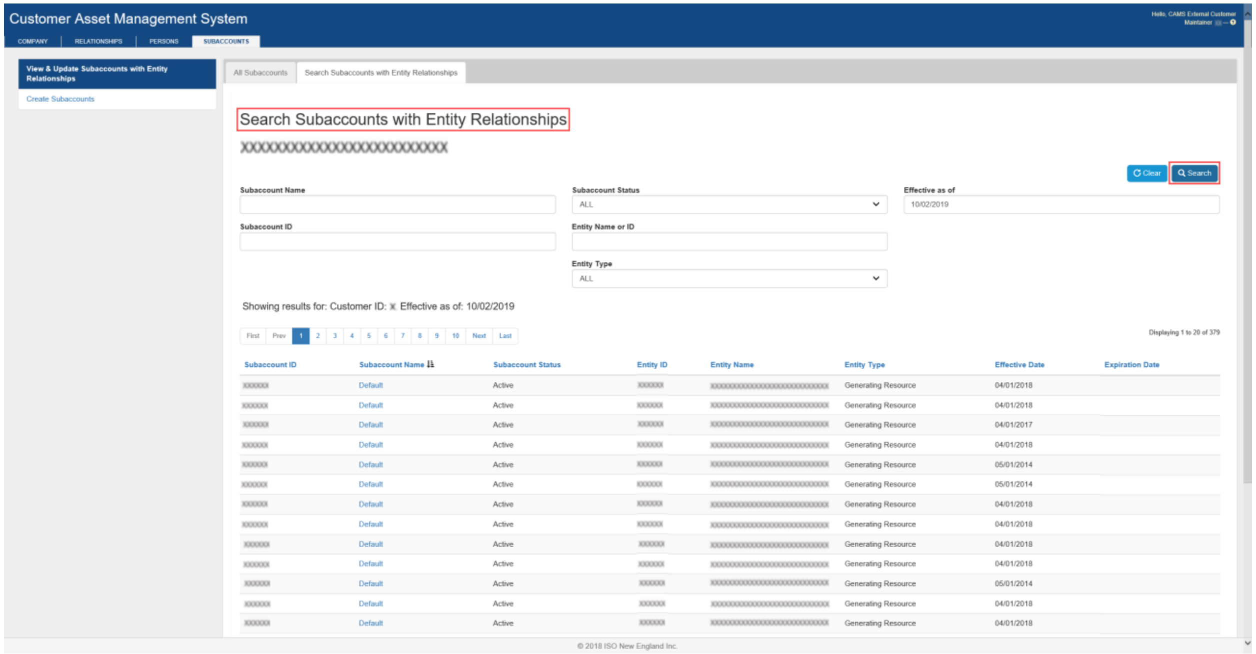


2. Refine the search by entering a Subaccount Name, Subaccount ID, Subaccount Status, Entity Name or ID, Entity Type, or Effective as of date.
3. Click the "Search" button.
4. The "Subaccounts with Entity Relationships Search" results are displayed at the bottom of the screen.

Enable subaccount settlement reporting"); however, every customer is automatically given a "default" subaccount with the ID and Name of "Default". When subaccount reporting is enabled, any entity or market activity that is not assigned to a subaccount is reported in the default subaccount.

Market activities that are not associated with assets, such as demand bidding and internal bilateral tranactions, can be assigned to a subaccount at the activity entry point. A subaccount created in CAMS will be available for selection in the Bids & Offers (eMarket) and the Internal Transactions applications for Operating Days where the subaccounts are effective, independent of the subaccount reporting status (see "Click on "Search Subaccounts with Entity Relationships" in the second-level menu.

5. The "Search Subaccounts with Entity Relationships" screen displays:



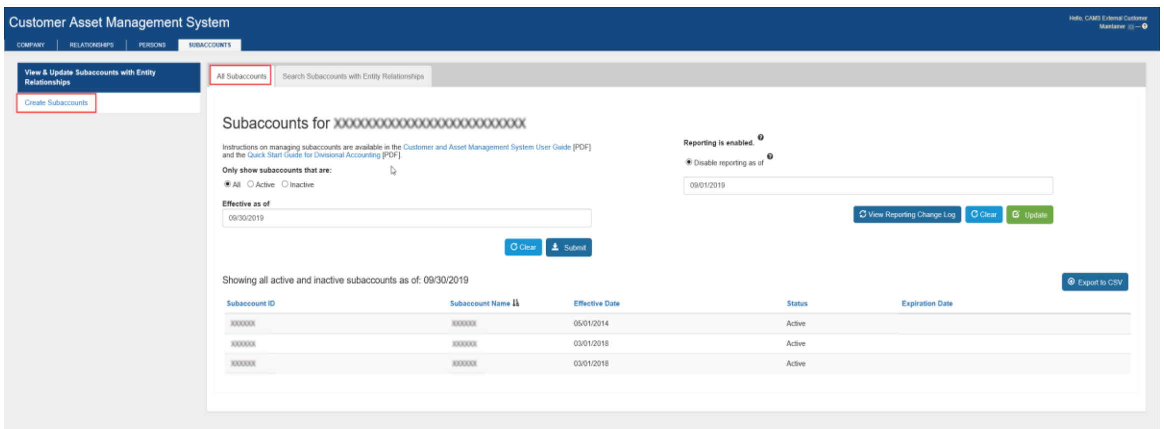
6. Refine the search by entering a Subaccount Name, Subaccount ID, Subaccount Status, Entity Name or ID, Entity Type, or Effective as of date.
7. Click the “Search” button.
8. The “Subaccounts with Entity Relationships Search” results are displayed at the bottom of the screen.

Enable subaccount settlement reporting” for instructions for changing the subaccount reporting status).

2.3.14.1 Create subaccount

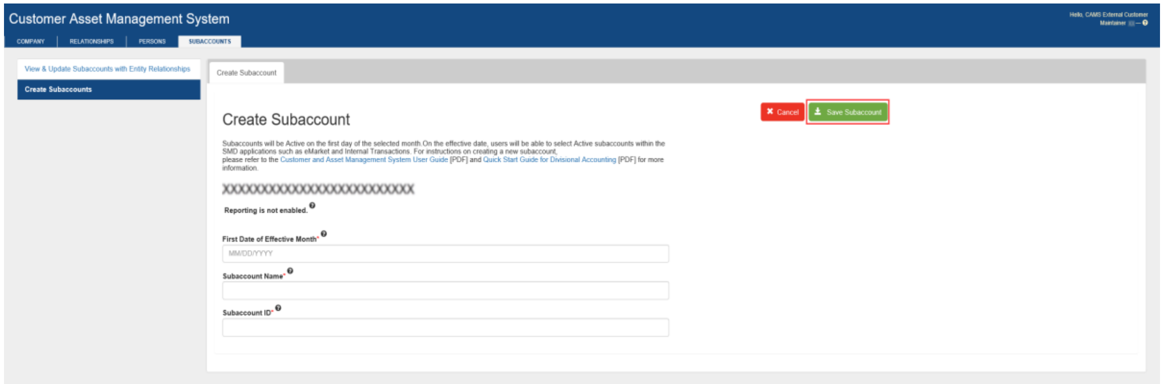
- Role that can perform this task:
  - External Customer Maintainer

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Subaccounts” in the top-level menu.
3. The “All Subaccounts” screen displays:



4. Click on “Create Subaccount” in the second-level menu.

5. The “Create Subaccount” screen displays:



6. Enter the required fields.

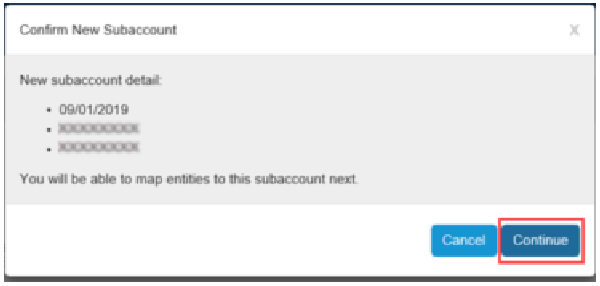
   - “Date Effective” must be the first day of a month.

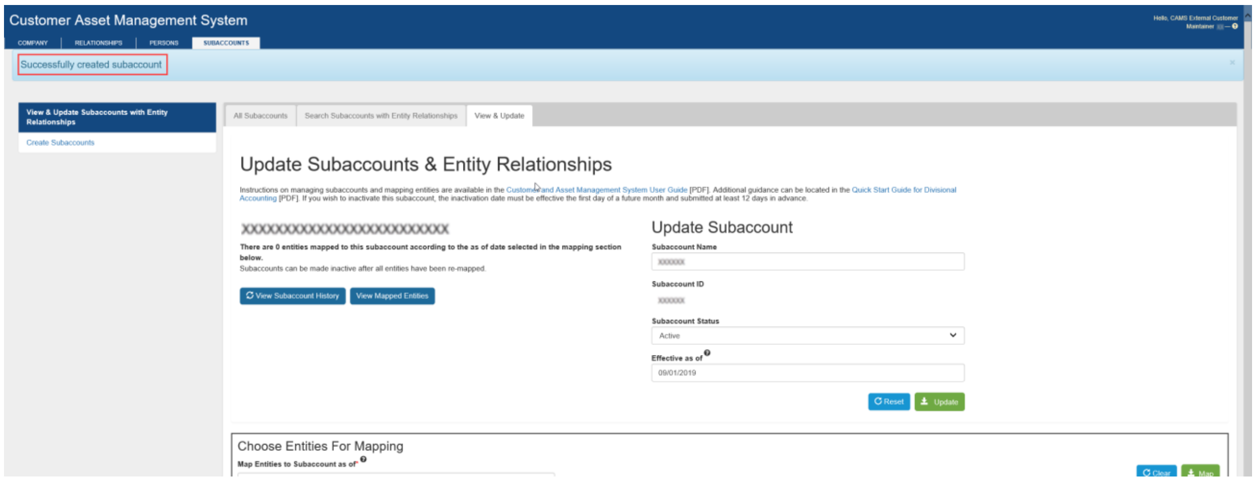
     NOTE: A subaccount will be available for selection in the eMarket and Internal Transactions applications on this effective date. If this is the initial use of the subaccount functionality, the start date should be set far enough in the future to allow for successful testing of eMarket and Internal Transactions communications in the corresponding sandbox environments. Because data in the sandbox environment generally mirrors the production environment, please contact ISO New England Participant Support at (413) 540-4220 or via email at **askiso@iso-ne.com** to make arrangements for testing your communication processes.

   - “Subaccount ID” may have between 1 and 20 alpha-numeric characters, hyphens and underscores. Spaces are not allowed.
   - “Subaccount Name” may contain between 1 and 50 characters. Spaces are allowed.
   - Each subaccount created must have a unique ID and Name. Duplicate subaccounts are not allowed.

7. Click “Save Subaccount” button.

8. A pop up confirmation message is displayed when the action is successful:



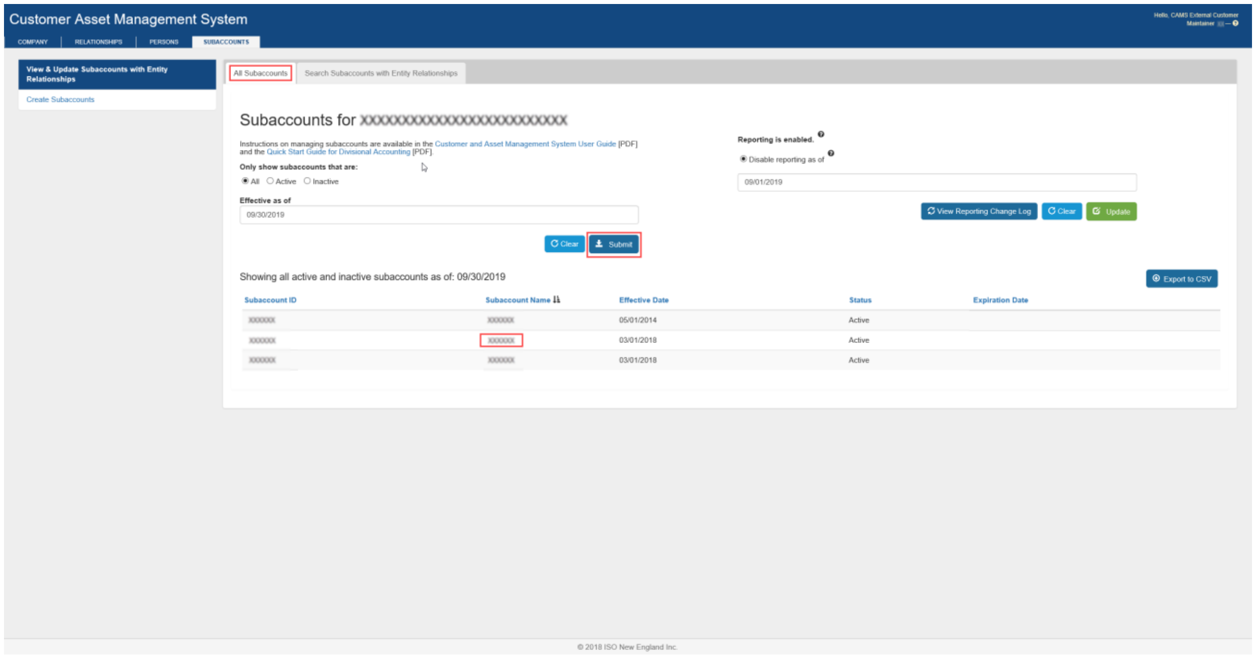


2.3.14.2 Edit subaccount information

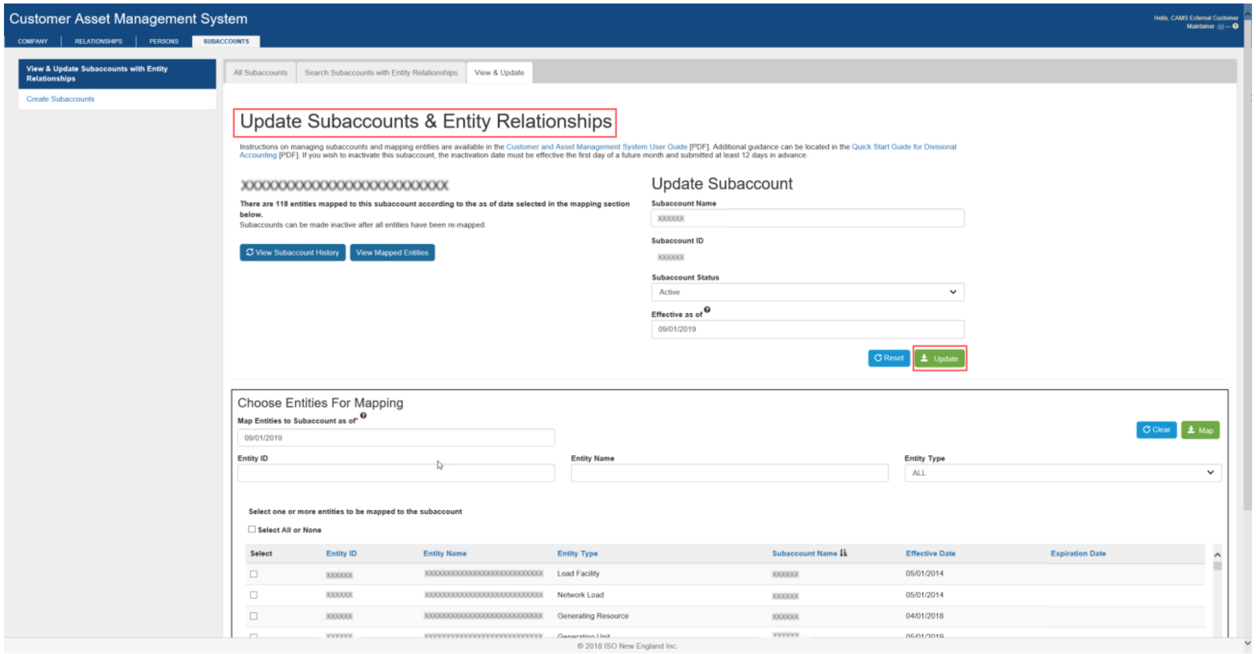
- Roles that can perform this task:
    - External Customer Maintainer

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on "Subaccounts" in the top-level menu.

3. The “All Subaccounts” screen displays:

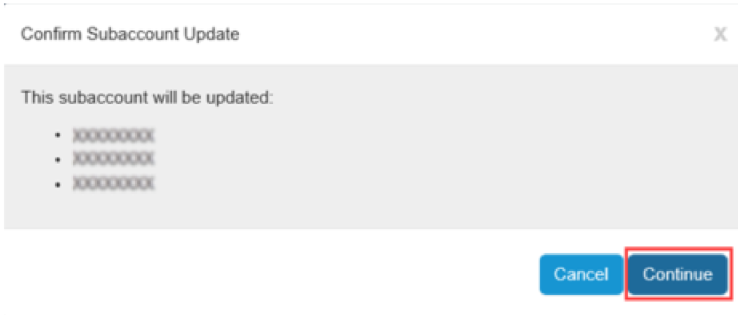


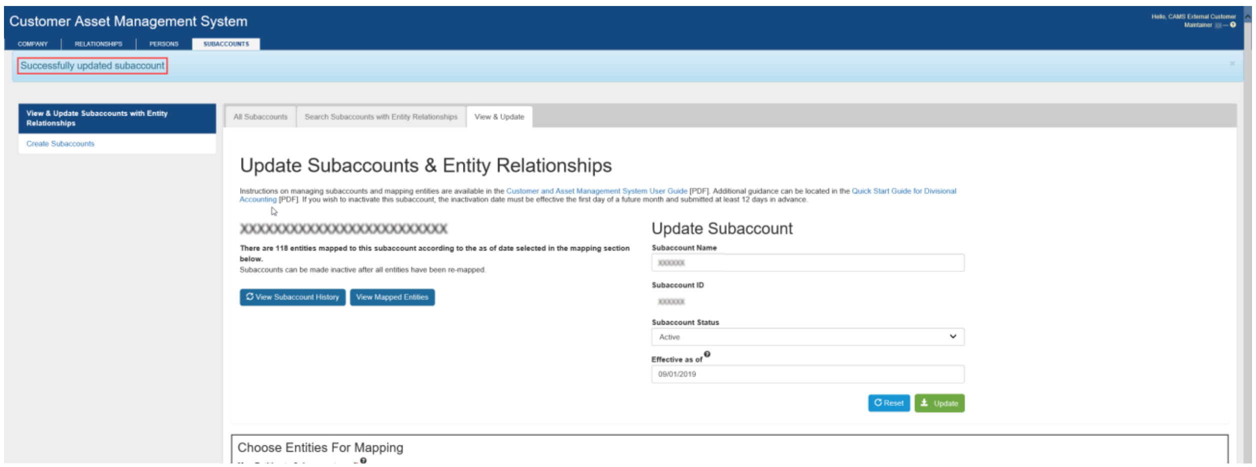
4. Enter subaccount search criteria, click “Submit” button.
5. Select the subaccount to be edited, shown in the Search Results section at the bottom of the screen.
6. The “Update Subaccounts & Entity Relationships” screen displays:



7. Enter the required fields.
   - “Date Effective” must be the first day of a month.
   - “Subaccount Name” may contain between 1 and 50 characters. Spaces are allowed.
   - Each subaccount created must have a unique ID and Name. Duplicate subaccounts are not allowed.

8. Click “Update” button.
9. A pop up confirmation message is displayed when the update is successful:



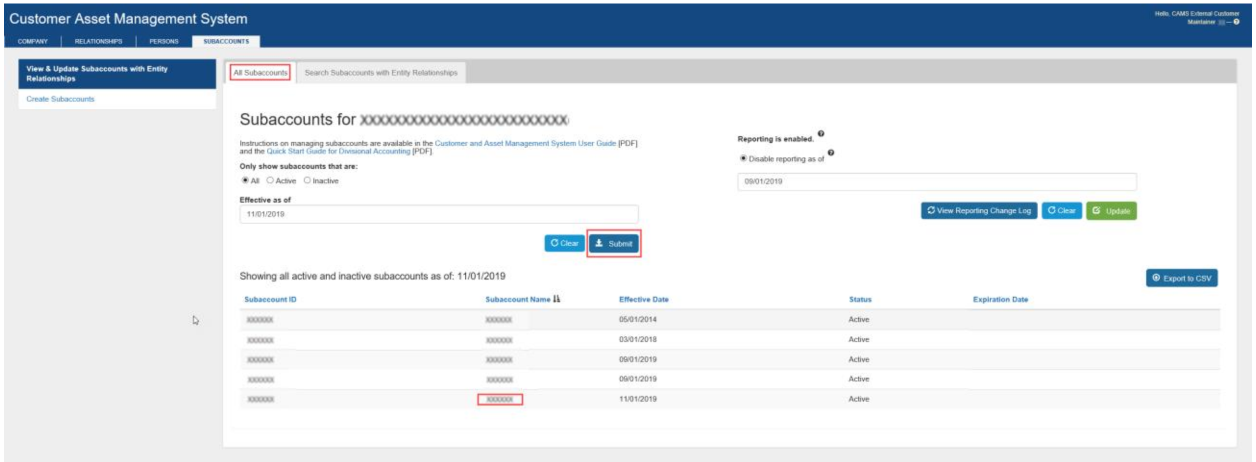


2.3.14.3 Delete subaccount

- Roles that can perform this task:
    - External Customer Maintainer

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Subaccounts” in the top-level menu.

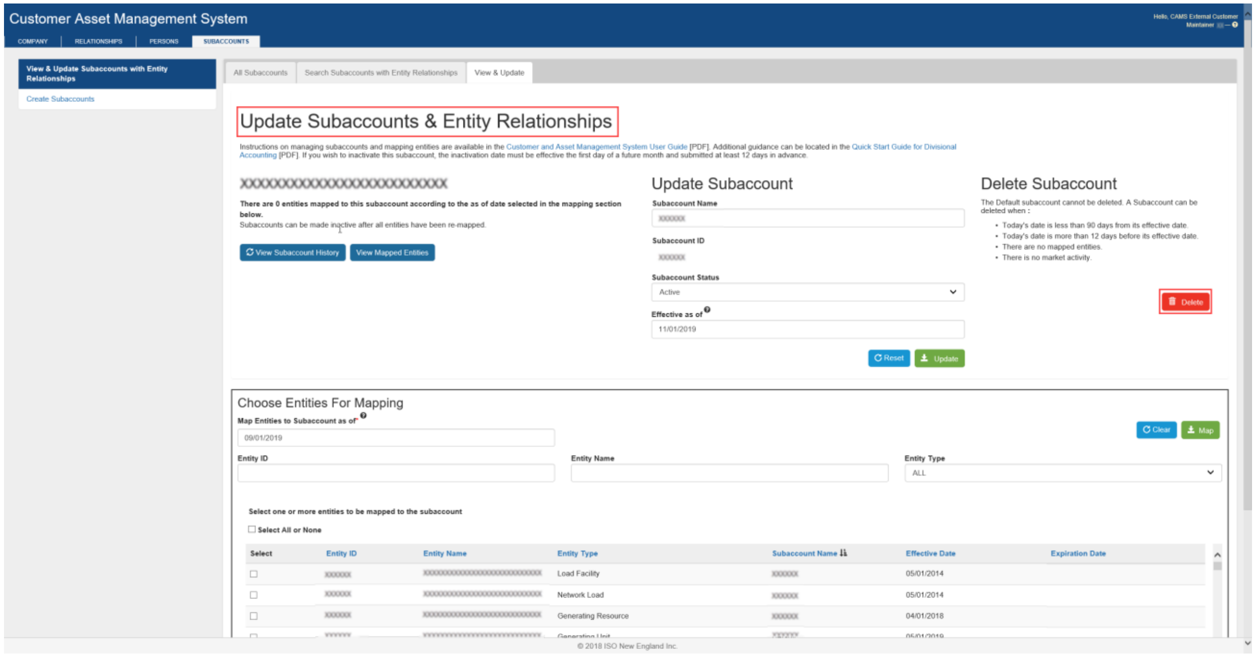
3. The “All Subaccounts” screen displays:



4. Enter subaccount search criteria, click “Submit” button.

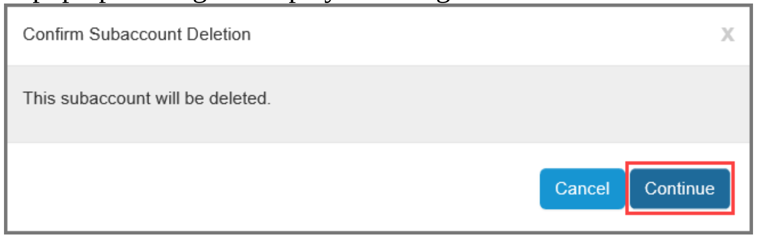
5. Select the subaccount to be deleted, shown in the Search Results section at the bottom of the screen.

6. The “Update Subaccounts & Entity Relationships” screen displays:



7. Click on the “Delete” button.

8. A pop up message is displayed asking the user to confirm the deletion or not:



9. Click the“Continue” button to delete the subaccount.

CAUTION

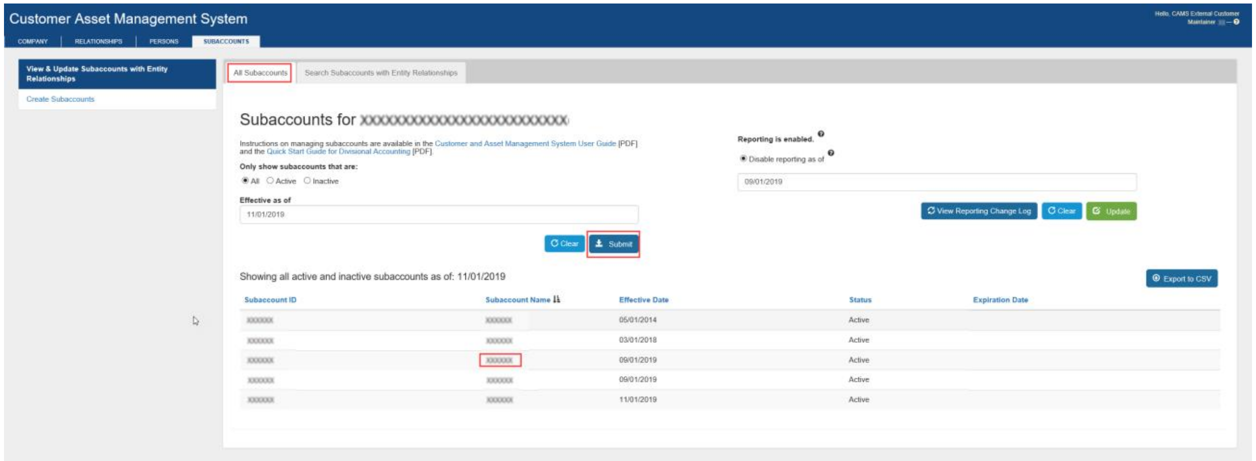
- ❖ The delete subaccount feature is meant to help with initial setup of subaccounts in the event an error is made during setup.
- ❖ CAMS restricts deletion of a subaccount under certain conditions, one being if the subaccount has a history of activity.

2.3.14.4 Map Entity to subaccount

- Roles that can perform this task:
    - External Customer Maintainer

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Subaccounts” in the top-level menu.

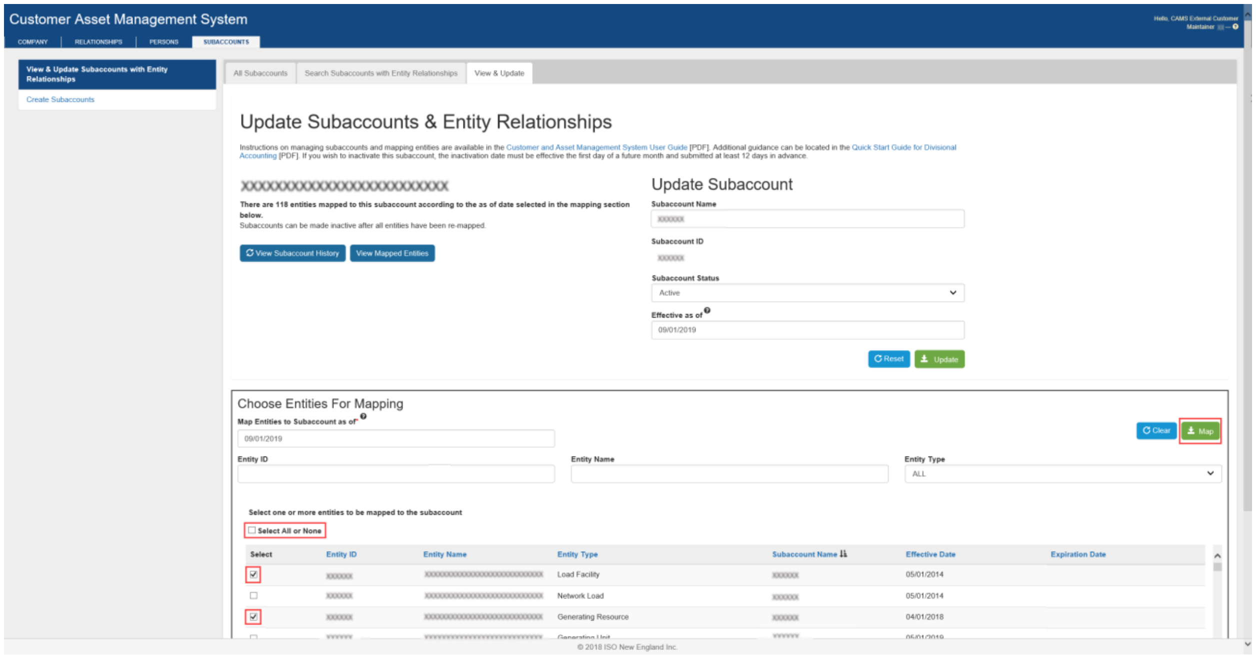
3. The “All Subaccounts” screen is displayed:



4. Enter subaccount search criteria, click “Submit” button,

5. Select the applicable subaccount, shown in the Search Results section at the bottom of the screen.

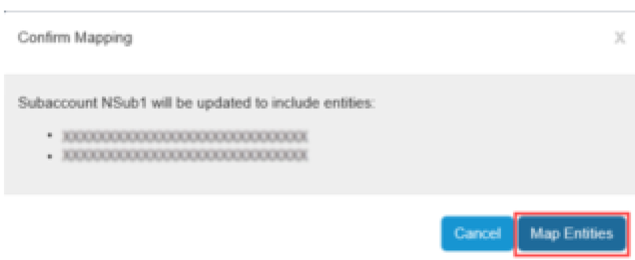
6. The “Update Subaccounts & Entity Relationships” screen displays:



7. In the “Choose Entities For Mapping” section enter the effective date in the “Map Entities to Subaccount as of” field, then click the check boxes in the “Select” column, or the “Select All or None” check box shown above, to map the selected entites to this subaccount.

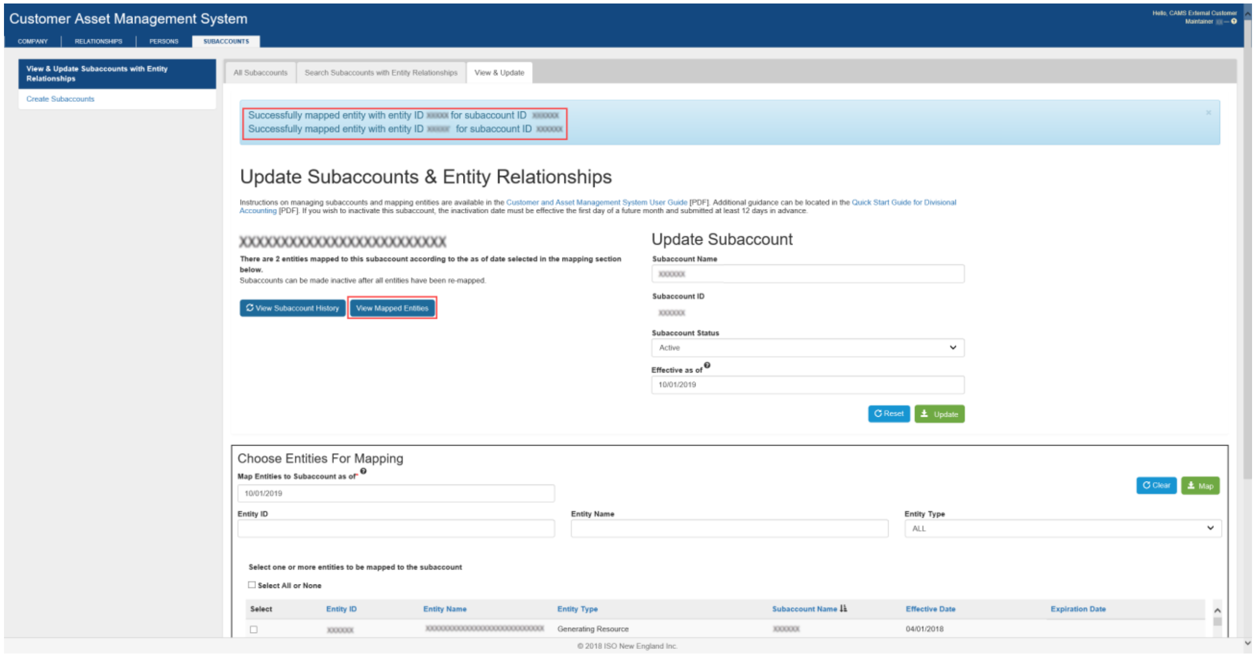
8. Click on the “Map” button.

9. The Confirm Mapping dialog is displayed with the entities to be mapped:

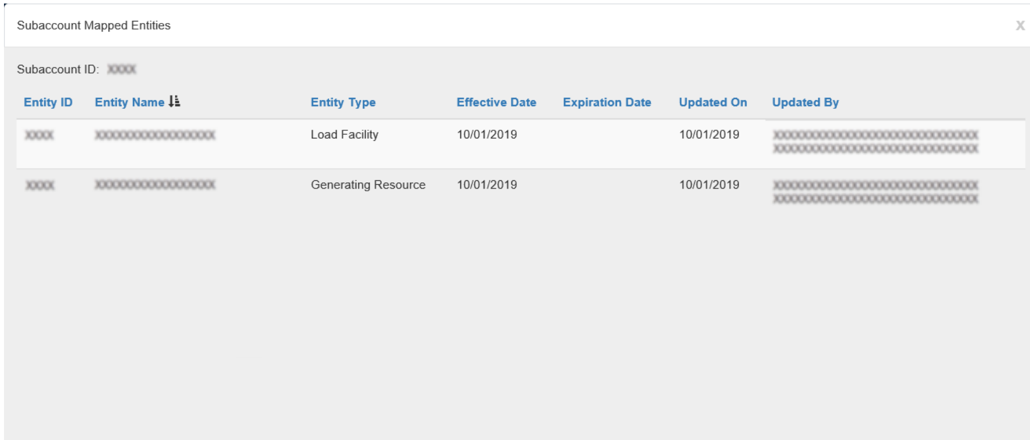


10. Click “Map Entities”

11. The “Update Subaccounts & Entity Relationships” screen displays with a success message and the “Choose Entities For Mapping” showing the as of the date selected.:



12. The “View Mapped Entities” tab displays the entities mapped to the selected subaccount as of the “Map Entities to Subaccount as of” date:

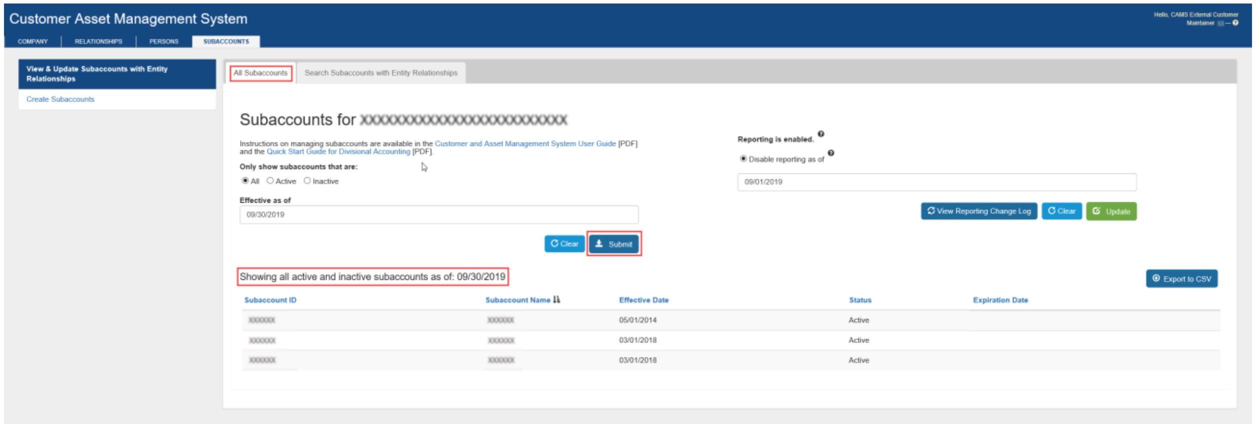


2.3.14.5 Search for a subaccount

- Roles that can perform this task:
    - External Customer Maintainer
    - External Customer Viewer

1. Launch the CAMS interface. See the “Accessing CAMS”
2. Click on “Subaccounts” in the top-level menu.

3. The “All Subaccounts” screen displays:



4. Enter subaccount search criteria, click “Submit” button,

5. The “All Subaccounts” screen displays the search results at the bottom of the screen.

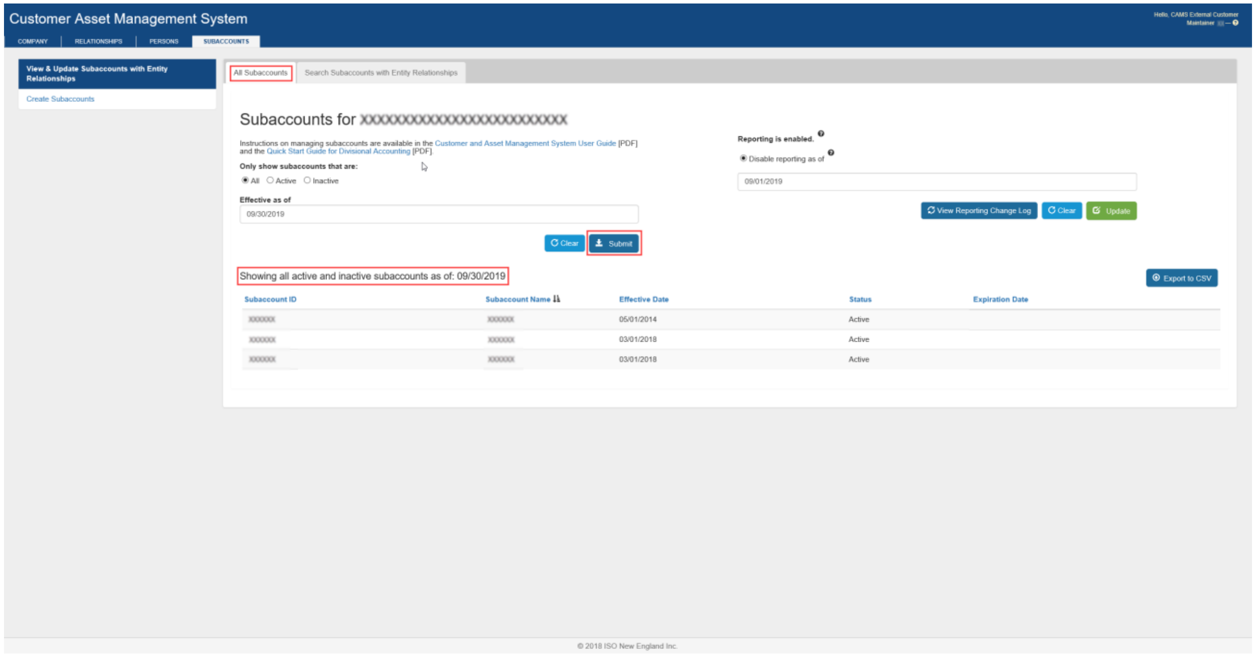
2.3.14.6 Search for Entity Relationship

- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer

9. Launch the CAMS interface. See the “Accessing CAMS”

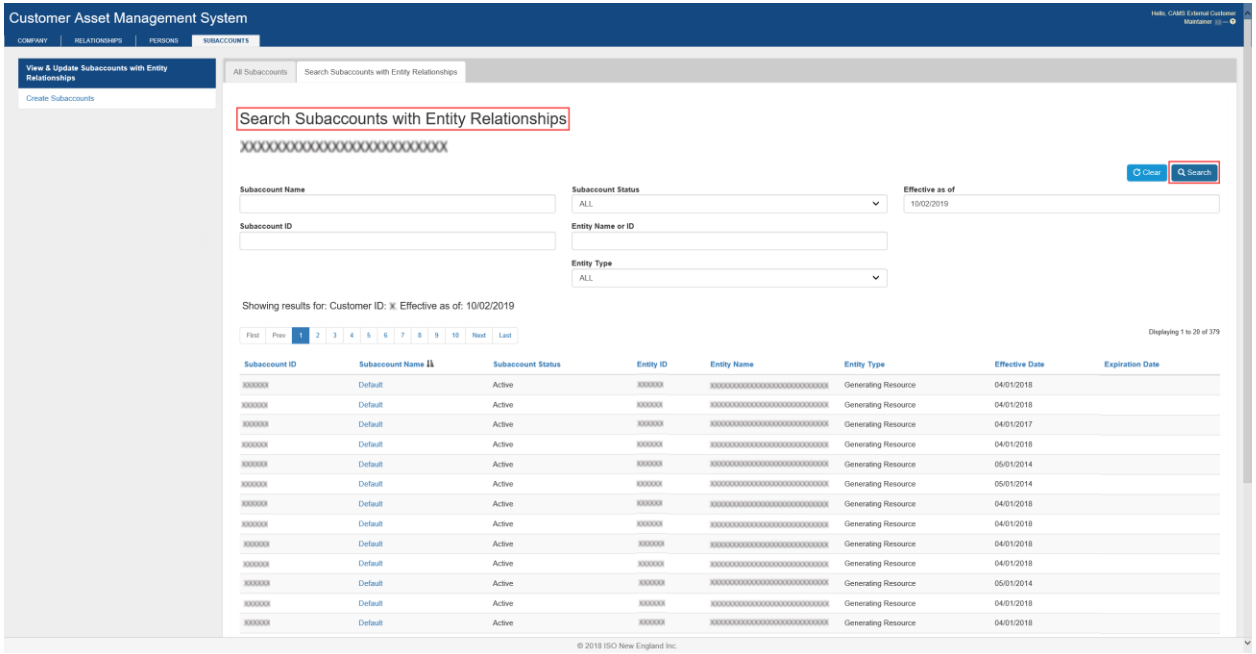
10. Click on “Subaccounts” in the top-level menu.

11. The “All Subaccounts Search” screen displays:



12. Click on “Search Subaccounts with Entity Relationships” in the second-level menu.

13. The “Search Subaccounts with Entity Relationships” screen displays:



14. Refine the search by entering a Subaccount Name, Subaccount ID, Subaccount Status, Entity Name or ID, Entity Type, or Effective as of date.

15. Click the “Search” button.

16. The “Subaccounts with Entity Relationships Search” results are displayed at the bottom of the screen.

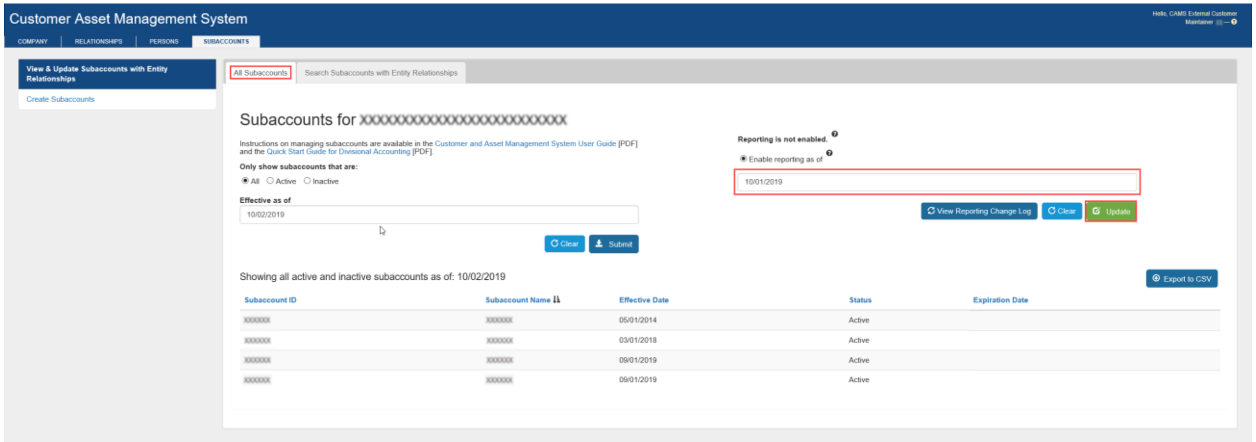
2.3.14.7 Enable subaccount settlement reporting

- Roles that can perform this task:
  - External Customer Maintainer

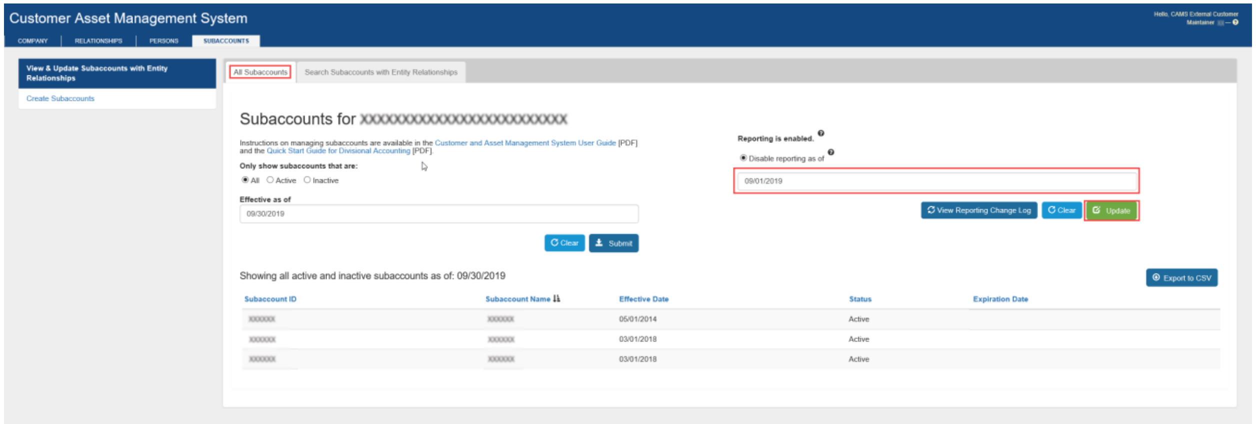
1. Launch the CAMS interface. See the “Accessing CAMS”

2. Click on “Subaccounts” in the top-level menu.

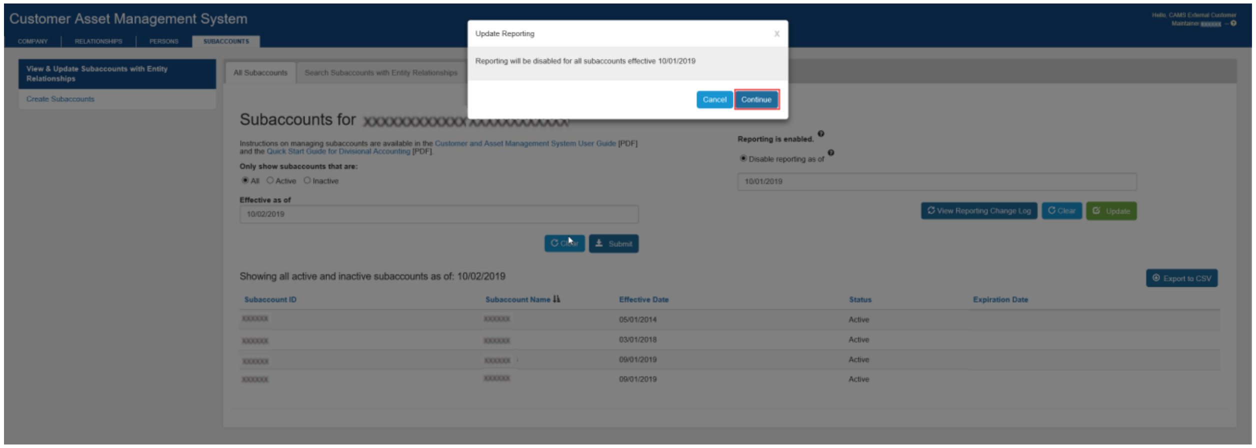
3. The “All Subaccounts” screen displays.
4. To enable settlement subaccount reporting enter an effective date in the field under the “Enable reporting as of radio button, then click the “Update” button:

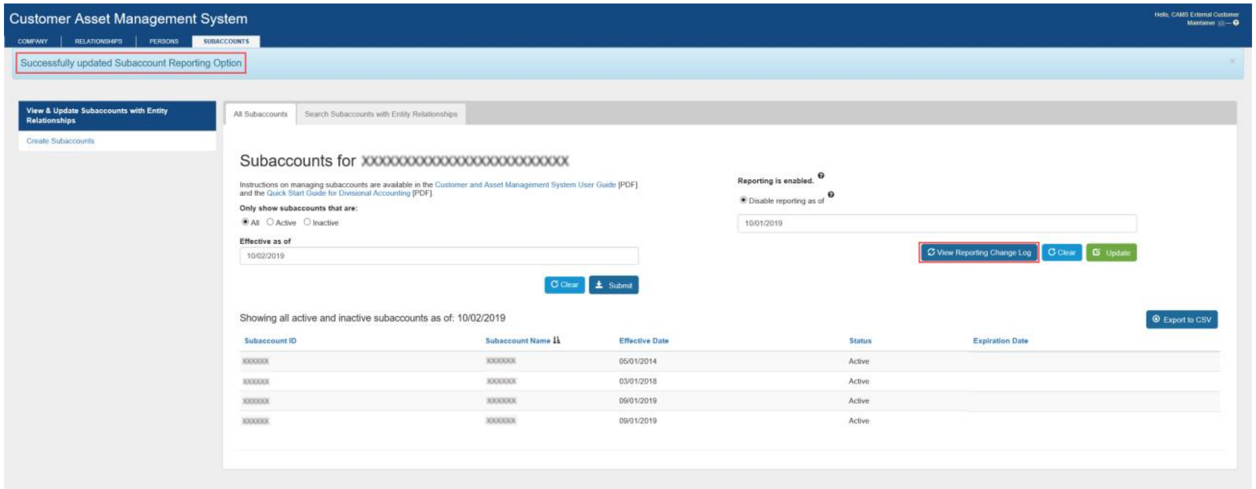


5. To disable settlement subaccount reporting enter an effective date in the filed under the “Disable reporting as of” radio button, then click the “Update” button:

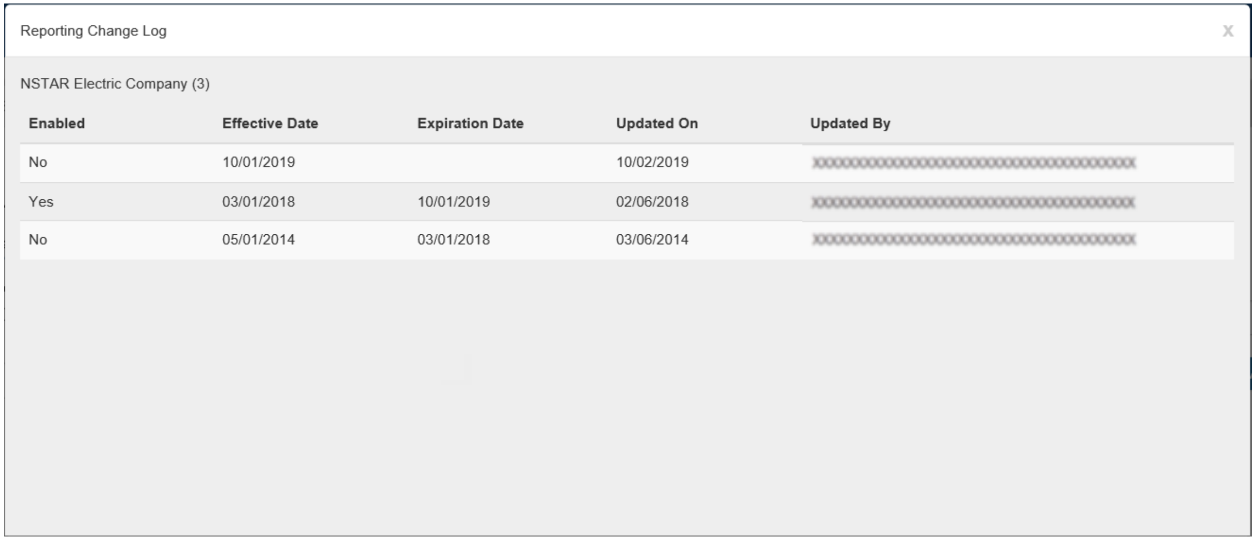


6. A confirmation message is displayed when the selected action is confirmed and successful:





7. The “View Reporting Change Log” popup displays all actions taken pertaining to reporting:



Reporting Change Log

NSTAR Electric Company (3)

Enabled	Effective Date	Expiration Date	Updated On	Updated By
No	10/01/2019		10/02/2019	[illegible]
Yes	03/01/2018	10/01/2019	02/06/2018	[illegible]
No	05/01/2014	03/01/2018	03/06/2014	[illegible]

NOTE: A subaccount remains active and available for selection in the eMarket, NEXTT, and Internal Trasactions applications until the subaccount's status is changed to "Inactive" in CAMS. In order to suspend all divisional accounting activity, all subaccounts should be changed to "Inactive" status in conjunction with the disabling of subaccount reporting. Individual subaccount status changes can only be done on a future monthly boundary.

2.3.15 Asset Ownership Share Transfers

To transfer ownership share of an asset, the Lead Market Participant of the asset must initiate the transfer in the Customer and Asset Management System (CAMS); please reference the brief training video (10 min video) found on the Asset Registration webpage

2.3.16 Banking information

2.3.16.1 Contact type and banking role assignment

1. New applicants will be assigned the “Billing – Primary Contact” contact type and both the “External Banking Admin” and “External Banking Approver” application group roles during the application process.
    a. For most market participant applications, the primary contact provided in the New Member Credit Application is used to assign the “Billing – Primary Contact” contact type and both the “External Banking Admin” and “External Banking Approver” application group roles in CAMS.
    b. The market participant’s System Administrator can grant the “External Banking Approver” role if the market participant chooses to separate the role from the “External Banking Admin” role.
    c. Some application types, such as the Data-Only member, must provide the contact via email to the billing department and the membership coordinator during the application process.
2. Active market participants may update the “Billing – Primary Contact” contact type in CAMS
    a. Launch the CAMS interface. See the “Accessing CAMS” section.
    b. Refer to the “Contacts” section of this guide for the detailed process steps to add contacts.
    c. Assign the “Billing – Primary Contact” contact type to the individual that will be notified when new banking information has been submitted.
        i. Only one primary billing contact is allowed.
        ii. To change the primary contact, select the existing contact first and click on the red “X” next to the existing contact.
        iii. The Primary Billing Contact Delete screen is displayed.
        iv. Select the new “Billing – Primary Contact” from the Person drop down by clicking the down arrow.
        v. Click submit to replace the existing “Billing – Primary Contact” with the new contact.

   d. The person(s) assigned the “Billing – Primary Contact” contact type or the “External Banking Admin” application group role will receive automated banking-related email notifications from CAMS.

3. The Security Administrator must assign the banking application group roles
   a. Refer to the Granting a person access to CAMS or another ISO application section of this guide for the steps to add application access to a user.
   b. Assign banking roles as needed.
      i. External Banking Admin (only one person may have this role assigned)
      ii. External Banking Viewer
      iii. External Banking Approver

IMPORTANT

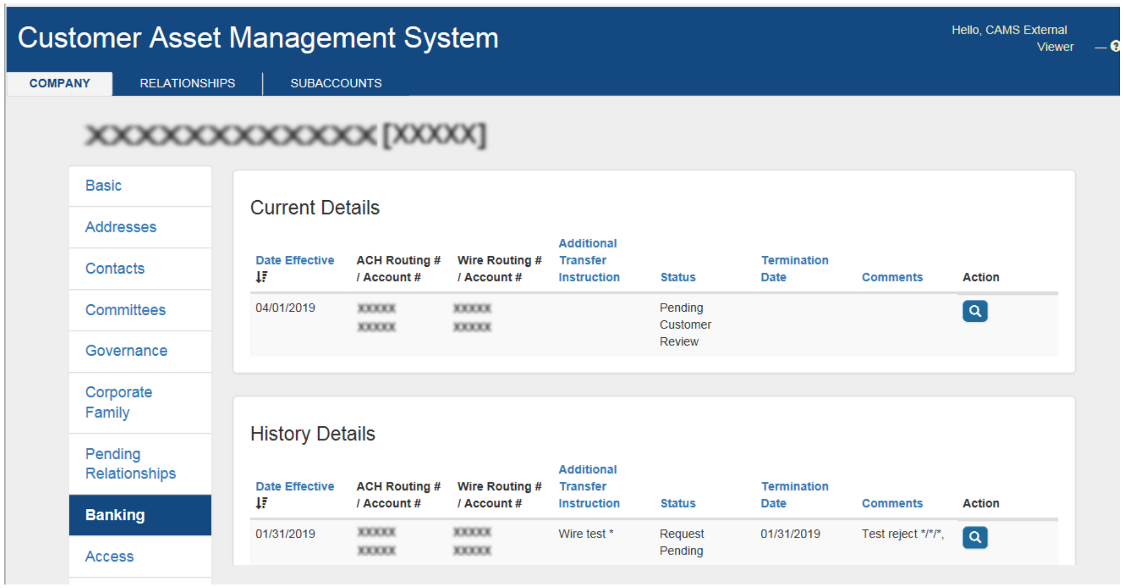
- Banking information must be maintained directly in CAMS by the person assigned the External Banking Admin application group role.
- ISO personnel cannot process banking changes submitted via email, phone, or fax and **do not have access** to maintain banking data on behalf of customers.

2.3.16.2 View the Banking tab

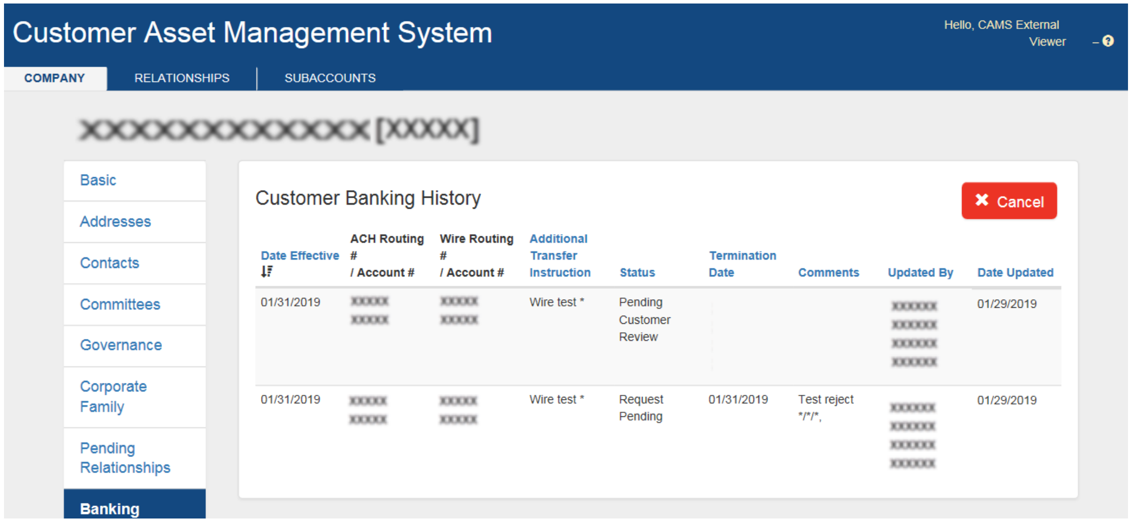
- Roles that can perform this task:
  - External Banking Admin
  - External Banking Viewer
  - External Banking Approver

1. Launch the CAMS interface. See the “Accessing CAMS” section.

2. Click on the “Banking” tab in the side menu.
3. The Customer Banking Listing screen is displayed containing two sections, the Current Details section and the History Details section.



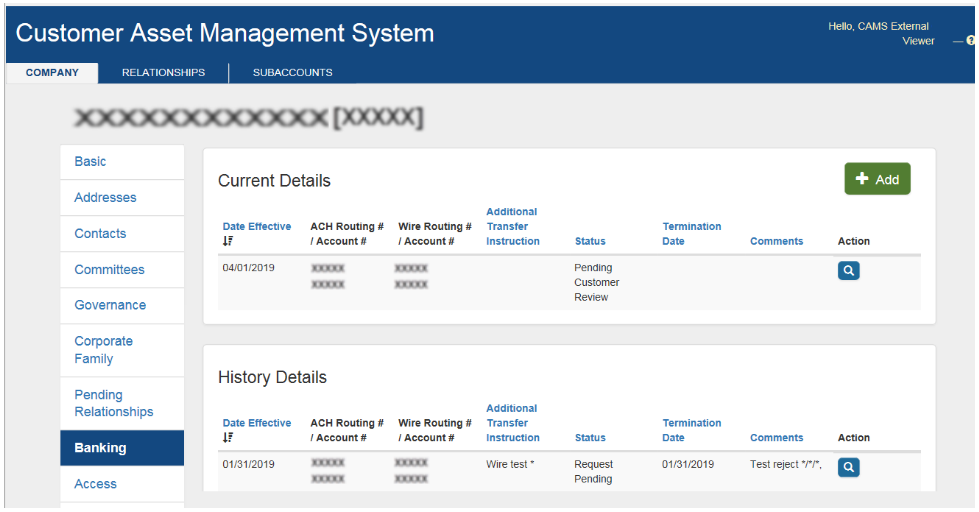
4. The External Banking Viewer role may view the details in each section by clicking on the magnifying glass icon. The bank account number will be partially masked.
5. The External Banking Admin and the External Banking Approver roles may view the details in each section by clicking on the magnifying glass icon. The bank account number will be fully displayed.



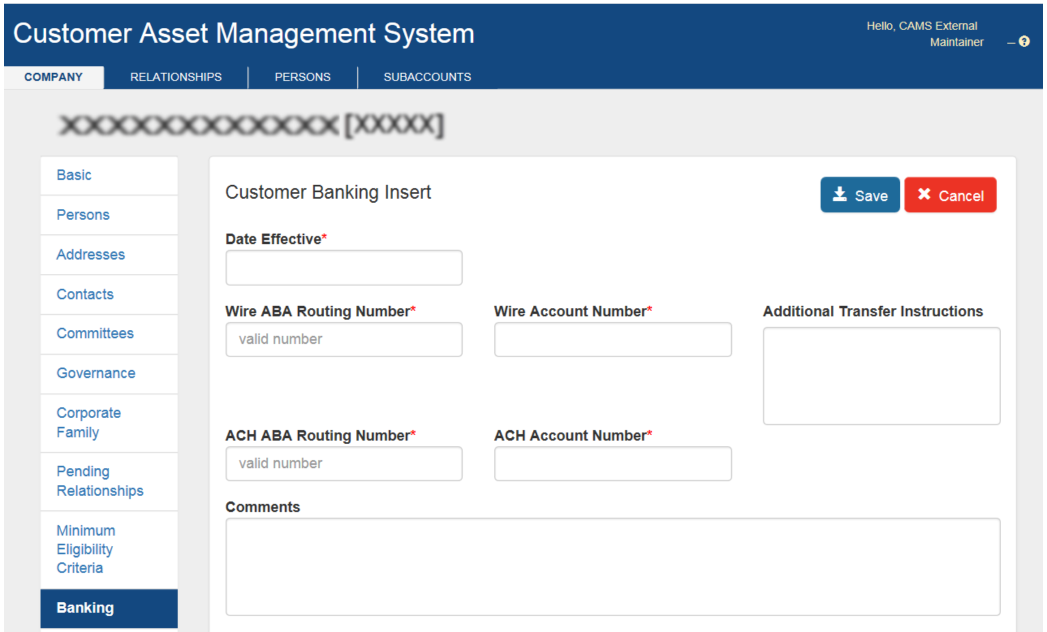
2.3.16.3 Submit new banking information

- Roles that can perform this task:
  - External Banking Admin

1. Launch the CAMS interface. See the "Accessing CAMS" section.
2. Click on the "Banking" tab in the side menu.
3. The Customer Banking Listing screen is displayed.
4. To add new banking information the person assigned the External Banking Admin role clicks the "Add" button.



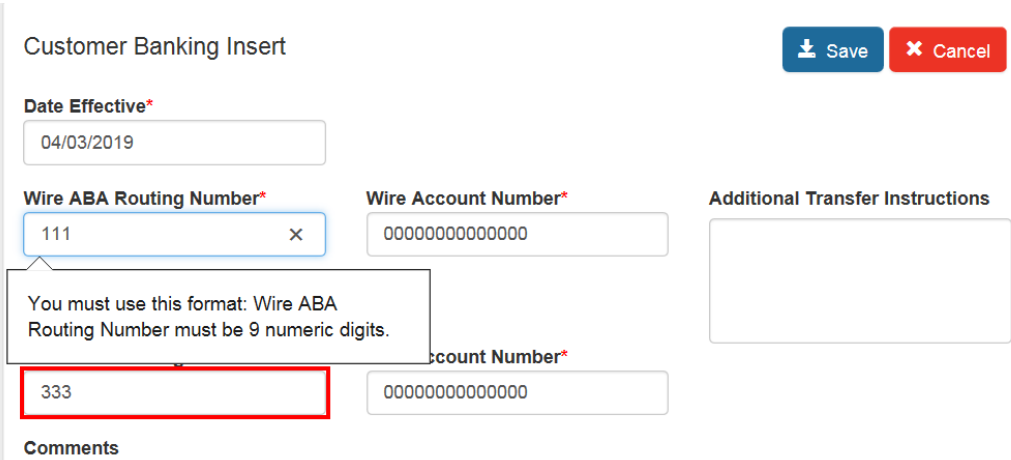
5. The Customer Banking Insert screen is displayed.



6. The External Banking Admin must provide the data identified with a red asterisk.
    a. The effective date must be in the future. Effective dates must be a minimum of two business days in the future or a maximum of ten business days in the future.
    b. The Wire ABA Routing Number is a numeric field and must be nine digits.
    c. The Wire Account Number is an alpha numeric field with a minimum of four digits and a maximum of thirty-four digits with no special characters or spaces.
    d. The Additional Transfer Instruction field is optional with a maximum of three hundred characters.
    e. The ACH ABA Routing Number is a numeric field and must be nine digits. If unable to accept ACH due to bank account requiring additional transfer instructions, must use all nines for ABA number.
    f. The ACH Account Number is an alpha numeric field with a minimum of four digits and a maximum of thirty-four digits with no special characters or spaces. If unable to accept ACH due to bank account requiring additional transfer instructions, must use all nines for Account number.
    g. The Comments field is optional.

Please Note: ISO Billing Department requires both Wire and ACH information. However, if you do NOT have ACH, please enter 999999999 for the ACH ABA and ACH Account Numbers.

7. When the required banking information has been provided click “Save.”



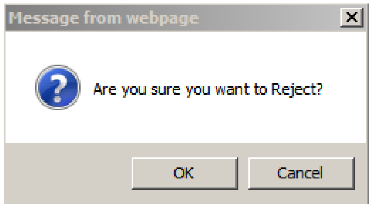
8. A success message is displayed or an error message with details is provided.
9. A successful banking information submittal moves to the “Pending Customer Review” status.

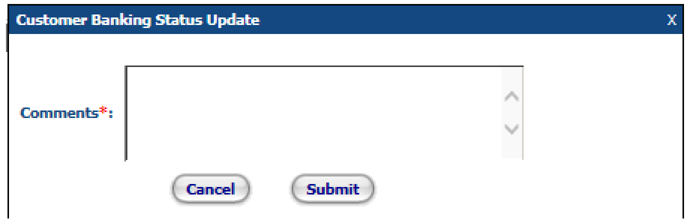
2.3.16.4 Approving banking information

- Roles that can perform this task:
  - External Banking Approver

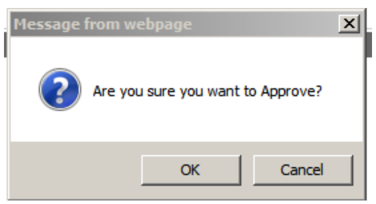
1. Launch the CAMS interface. See the “Accessing CAMS” section.
2. Click on the “Banking” tab in the side menu.
3. The Customer Banking Listing screen is displayed.
4. The External Banking Approver will see the option to accept or rejected the submitted changes.
   a. To Reject the banking information – click the × button
      i. Select Ok to confirm you want to reject the banking change.

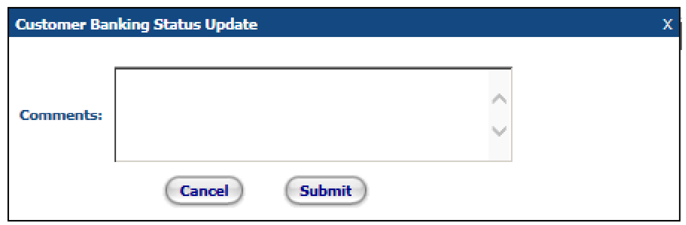
ii. Enter a comment for the rejected banking information and click submit.
iii. Banking information will be available for the External Banking Admin to make the required changes and resubmit.





b. To Approve Banking information – click the ✓ button
   i. Select Ok to confirm you want to approve the banking change.
   ii. Enter a comment (optional) and click submit.
   iii. Banking Information will be sent to ISO for approval.





5. An automated email notification is sent from CAMS to the person assigned the “Billing – Primary Contact” contact type that new banking information has been submitted.

6. A success message is displayed or an error message with details is provided.
7. A successful banking information submittal moves to the “Pending ISO Review” status.

2.3.16.5 ISO review

1. The ISO may approve or reject banking information submittals in the “Pending ISO review” status.
2. Changes that are approved become effective as of the submitted effective date and an automated email notification is sent to the person assigned the External Banking Admin role.
3. Changes that are rejected are moved to the ‘Pending Customer Action” status and an automated email notification is sent to the person assigned the External Banking Admin role.
    a. The person assigned the External Banking Admin must access CAMS to edit the banking information and resubmit.
    b. The effective date field is not editable.
    c. The reason for the rejection will display in the Comments field.

IMPORTANT

- ❖ If the banking information is not resubmitted by the two business day minimum before the effective date the banking submission moves to the “Terminated” status and a new banking information submittal must be generated.

2.4 Manage your company's Affiliates Information

This section applies to the following CAMS roles:

- ✓ External Customer Maintainer
- ✓ External Customer Viewer

This section covers the following topics:

2.4.1 Overview of affiliates

- Market Participants use CAMS to update their participant affiliation information mandated by the Federal Energy Regulatory Commission (FERC) Order 741, *Credit Reforms in Organized Wholesale Electric Markets*, and described in the ISO New England Financial Assurance Policy (FAP). The Participant Support department collects and maintains affiliate information on all active customers of ISO New England. The affiliate information is used for:
    - NEPOOL's determination of participant voting responsibilities
    - Determination of financial assurance
    - Day-Ahead Net Commitment Period Compensation (NCPC) settlements

    - ISO New England code of conduct compliance

- Section 1.3.5 of the Transmission, Markets and Services Tariff (Tariff) requires each Market Participant to:
    - Regularly review its corporate family on an ongoing basis
    - Promptly update CAMS with any additions, expirations, and/or corrections to the corporate family

- Affiliates reporting will support the following functions:
    - The FAP:
        - Limits the amount of unsecured credit extended to participants and their affiliates
        - Places restrictions on the provision of letters of credit from a bank that is an affiliate
    - Market Rule 1 allocates NCPC using affiliate information
    - Code of conduct provisions prohibit the ISO directors, officers, employees and their spouses from having a financial interest in a Market Participant or its affiliates
    - Participants Agreement governance arrangements entitle participants and their related persons to join only one sector and have only one vote on each principal committee
- Roles that can access this information:
    - External Customer Maintainer - Allows viewing capabilities
    - External Customer Viewer - Allows viewing capabilities

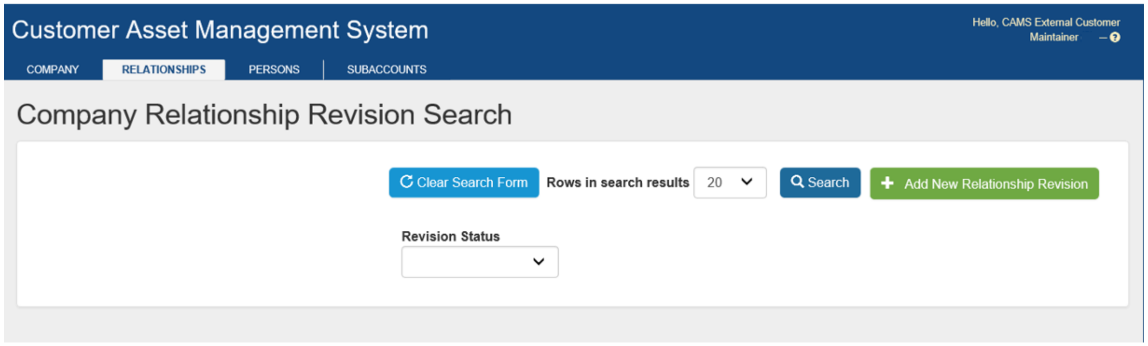
2.4.2 Summary of the affiliate process

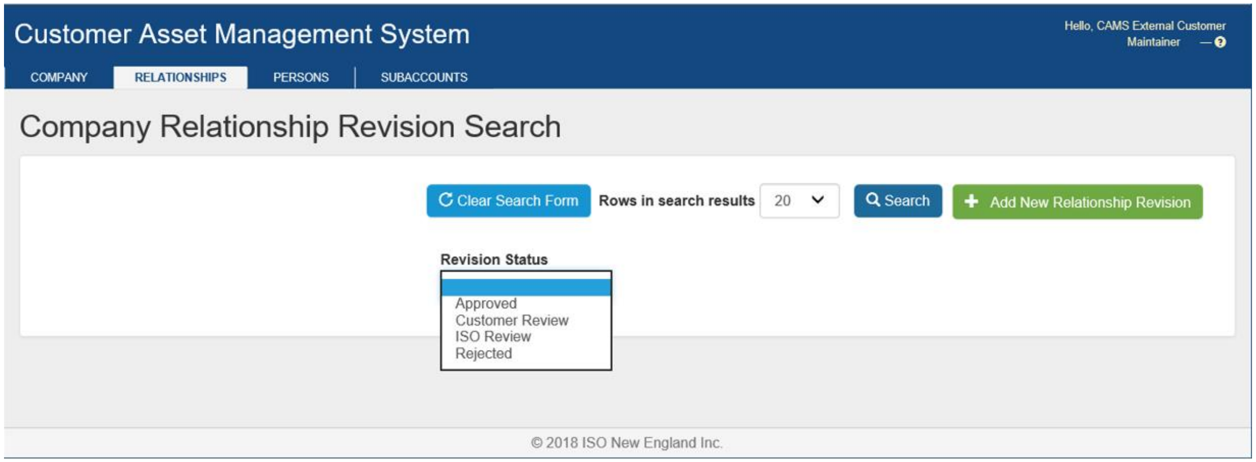
- An applicant or existing participant provides affiliate information to the ISO Membership Coordinator (MC)
- MC will review a current participant's CAMS corporate family or an applicant's affiliate submission as well as external sources, if available (i.e. customer's website, Hoover's Dun and Bradstreet) for the direct affiliates in identifying the corporate family tree
- In the case of an existing participant the new affiliate information is compared to the current corporate family. MC reviews the information and requests additional information from the customer when necessary
- Once a relationship change is approved by MC, the status changes to "Customer Review" until the approval date is reached and can be viewed on the Pending Relationships tab
- Additional changes to the corporate family must be submitted as a separate request

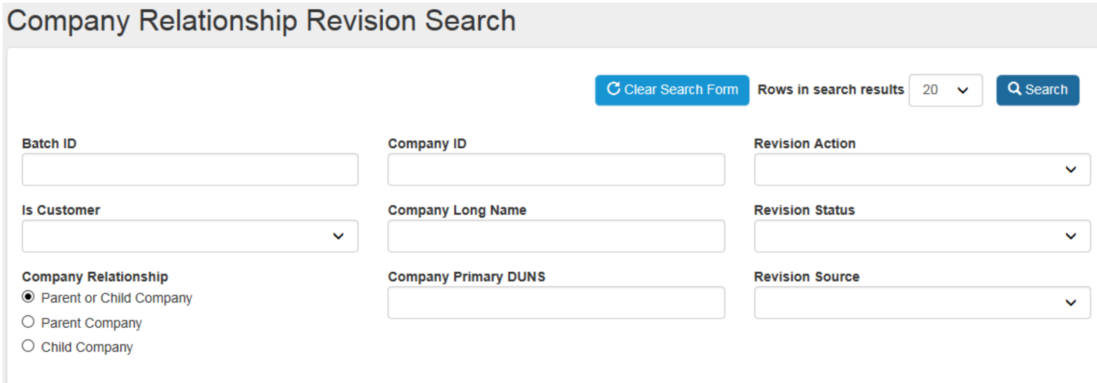
2.4.3 Search for and view a company relationship revision

- Roles that can perform this task:
    - External Customer Maintainer
    - External Customer Viewer

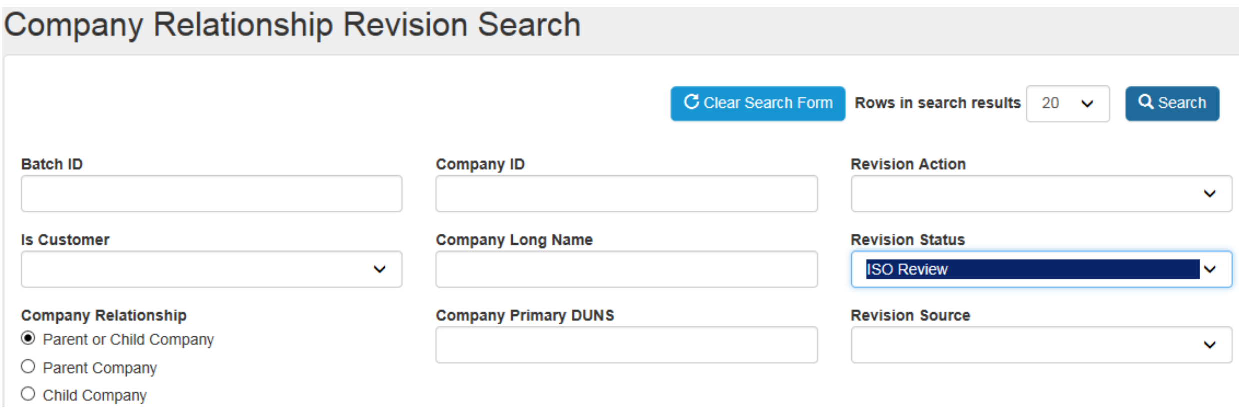
1. Launch the CAMS interface. See the "Accessing CAMS" section
2. Click on the "Relationships" tab in the top-level menu
3. The "Company Relationship Revision Search" screen displays:



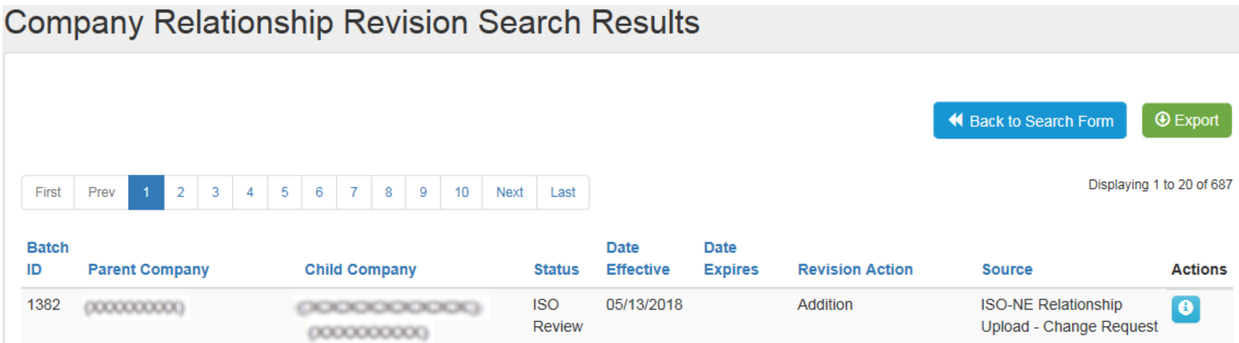




4. Select the “Revision Status” option (Approved, Customer Review, Duplicate, ISO Review, Superceded, or Rejected) from the drop-down menu and click “Search”:



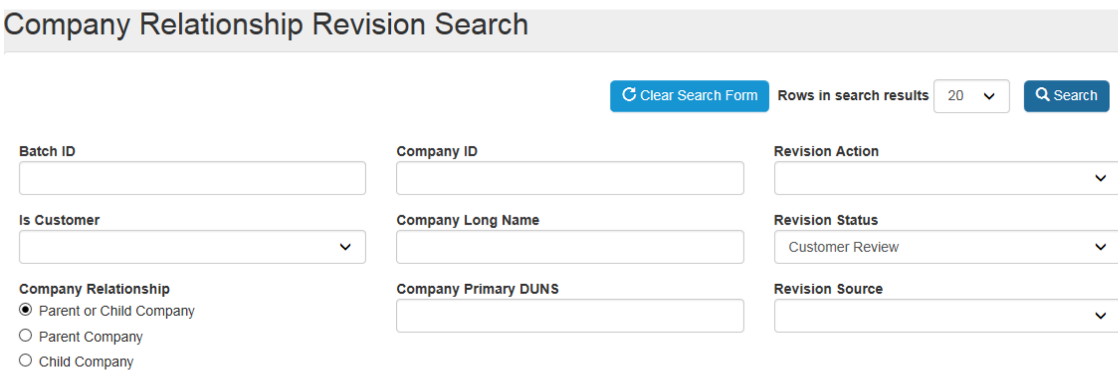
The “Company Relationship Revision Search Results” screen displays:



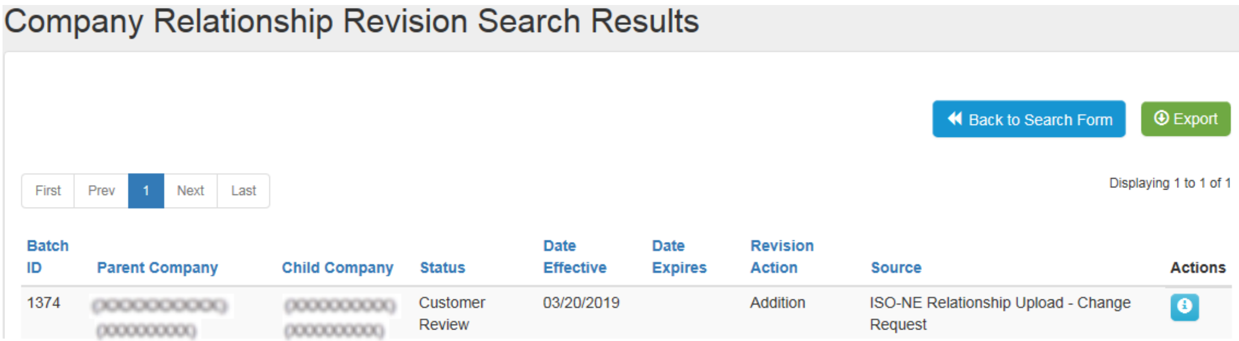
2.4.4 View company relationship revision information

- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer

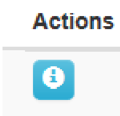
1. Launch the CAMS interface. See the "Accessing CAMS" section
2. Click on the "Relationships" tab in the top-level menu
3. The "Company Relationship Revision Search" screen displays:



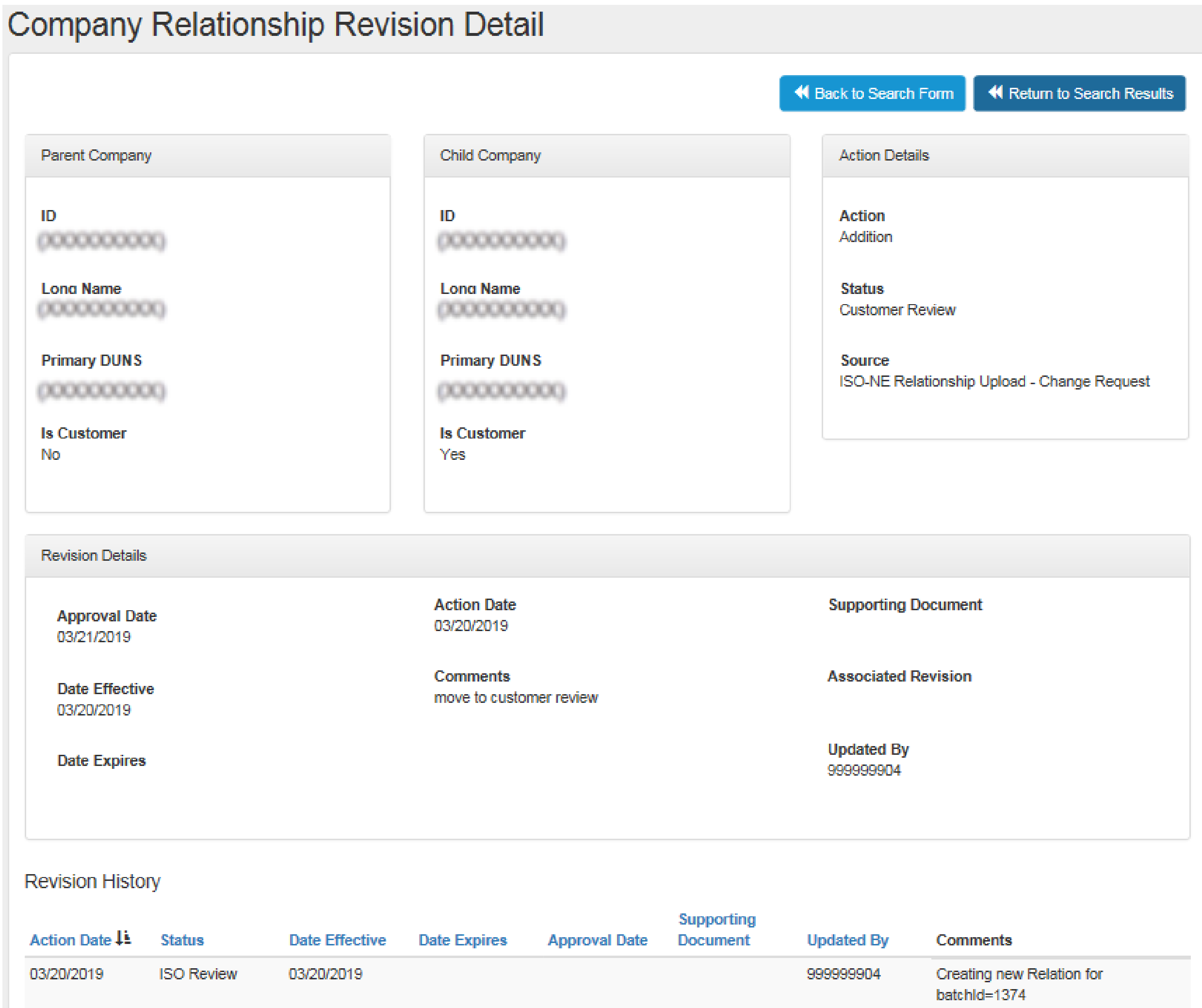
4. Select the "Revision Status" option from the drop-down menu and click "Search".
5. The "Company Relationship Revision Search Results" screen displays:



6. To view the details of the revision, click on the information icon in the “Actions” column.



7. The “Company Relationship Revision Detail” screen displays:


Company Relationship Revision Detail
Back to Search Form
Return to Search Results
Parent Company
ID
Long Name
Primary DUNS
Is Customer
No
Child Company
ID
Long Name
Primary DUNS
Is Customer
Yes
Action Details
Action
Addition
Status
Customer Review
Source
ISO-NE Relationship Upload - Change Request
Revision Details
Approval Date
03/21/2019
Date Effective
03/20/2019
Date Expires
Action Date
03/20/2019
Comments
move to customer review
Supporting Document
Associated Revision
Updated By
999999904
Revision History
Action Date
Status
Date Effective
Date Expires
Approval Date
Supporting Document
Updated By
Comments
03/20/2019
ISO Review
03/20/2019
999999904
Creating new Relation for batchId=1374

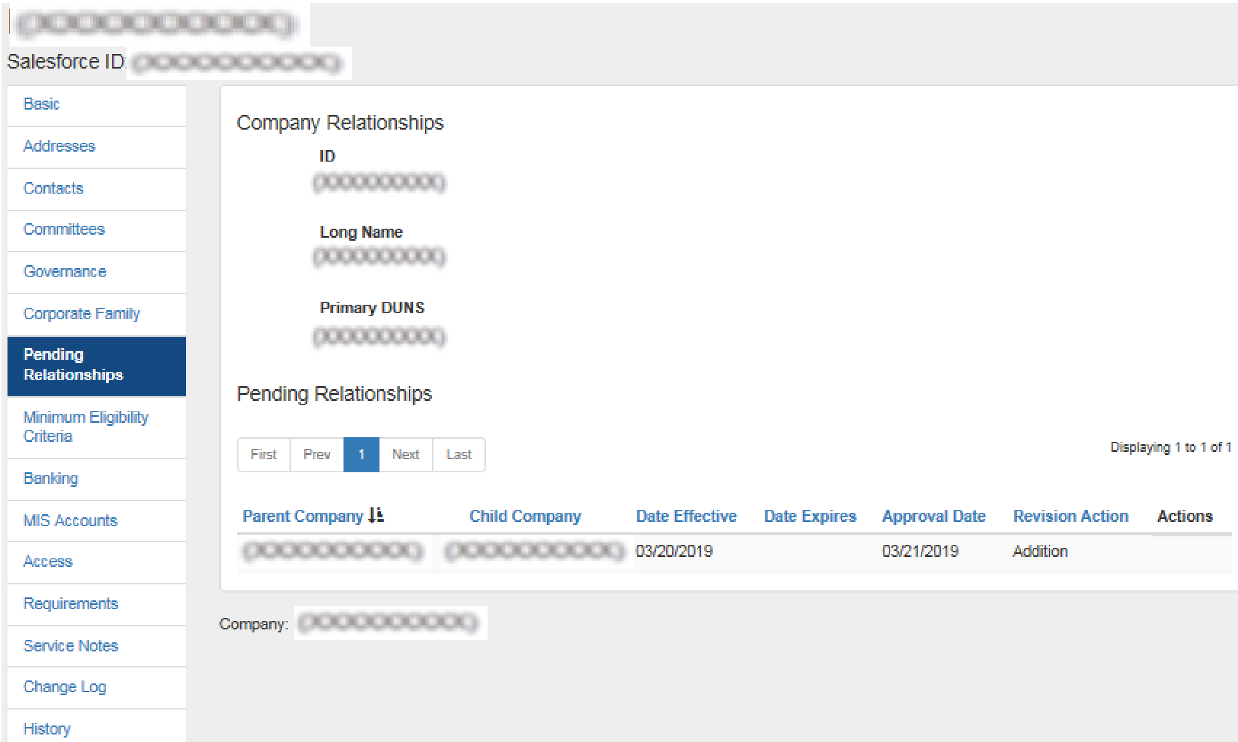
IMPORTANT

❖ The “Approval Date” is the As of Date needed to view the corporate family in its revised state.

2.4.5 View a pending company relationship

- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer

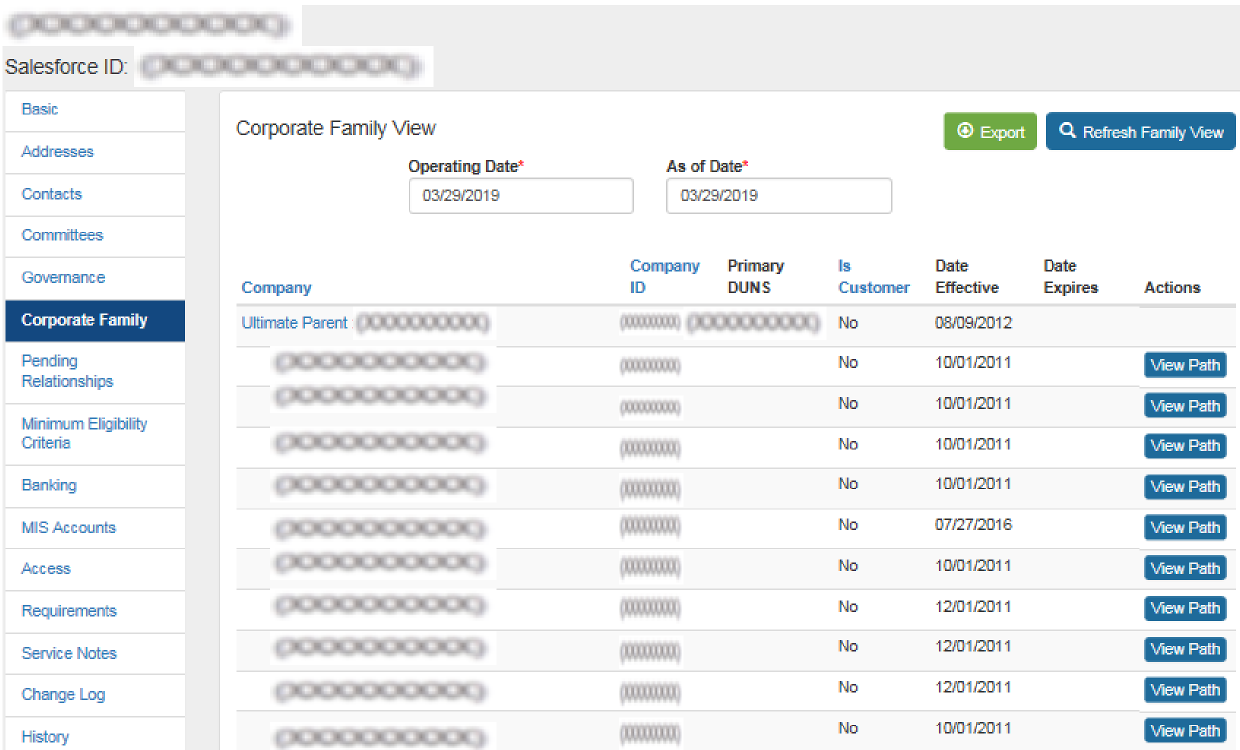
1. Launch the CAMS interface. See the “Accessing CAMS”.
2. Click on the “Company” tab in the top-level menu.
3. Click on the “Pending Relationships” tab in the second-level menu
4. The “Company Relationships” screen displays:



2.4.6 View a corporate family

- Roles that can perform this task:
  - External Customer Maintainer
  - External Customer Viewer

1. Launch the CAMS interface. See the "Accessing CAMS".
2. Click on the "Corporate Family" tab in the second-level menu.
3. The "Corporate Family View" screen displays:



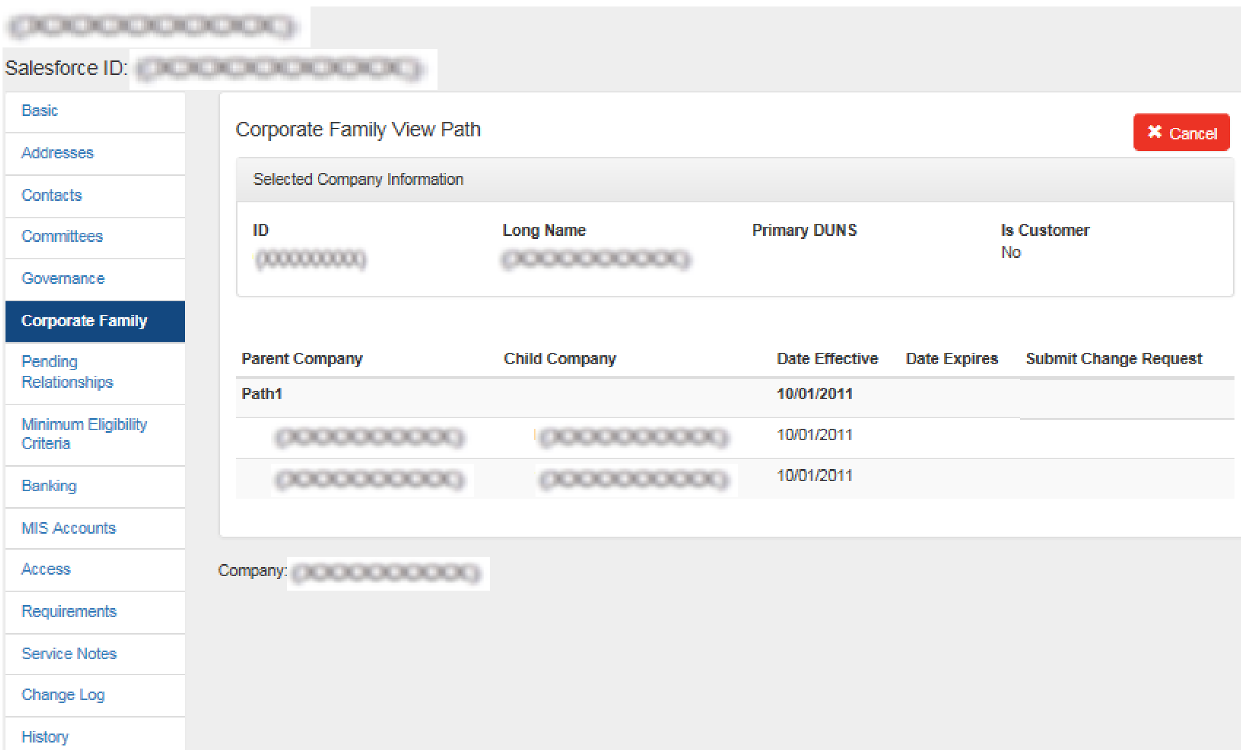
2.4.7 View a company path detail

- Roles that can perform this task:
    - External Customer Maintainer
    - External Customer Viewer

1. Launch the CAMS interface. See the "Accessing CAMS" section.
2. Click on the "Corporate Family" tab in the second-level menu.
3. The "Corporate Family View" screen displays.

4. Click on “View Path” in the “Actions” column to determine how a company is related to the Corporate Family.

5. The “Corporate Family View Path” screen displays:



2.5 Manage your company's minimum eligibility criteria information

This section applies to the following CAMS roles:

- ✓ External MEC Maintainer
- ✓ External MEC Viewer

This section covers the following topics:

- ❖ Overview of minimum eligibility criteria (page 119)
- ❖ Add minimum eligibility criteria information (page 119)
- ❖ View minimum eligibility criteria information (page 123177)

2.5.1 Overview of minimum eligibility criteria

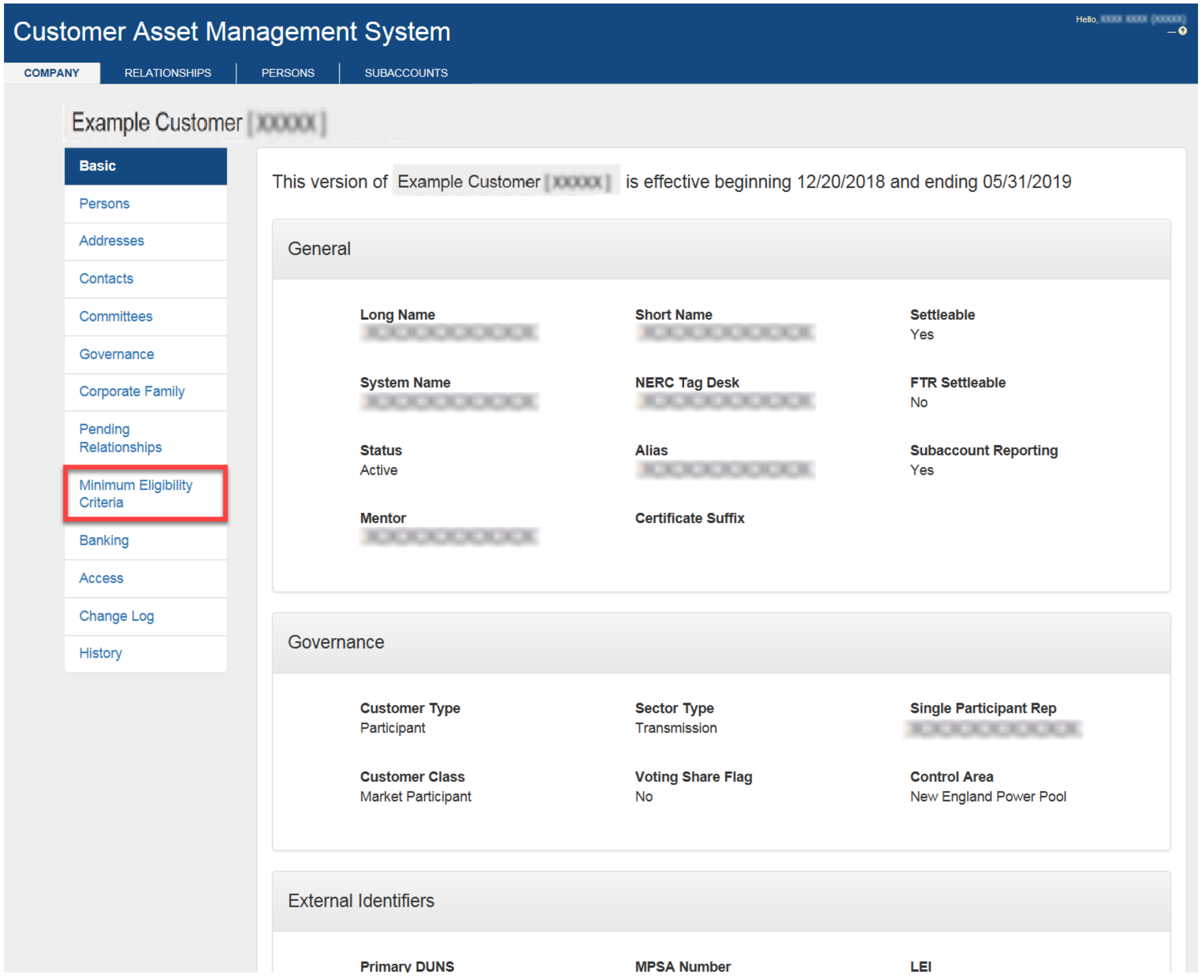
- Market Participants must use CAMS to update their minimum eligibility requirements mandated by the Federal Energy Regulatory Commission (FERC) Order 741, *Credit Reforms in Organized Wholesale Electric Markets*, and described in the ISO New England Financial Assurance Policy.
- CAMS provides customers with the functionality to upload Minimum Eligibility Criteria (MEC) documentation.
- Effective February 29, 2012, customers are required to submit the following documentation to ISO New England via CAMS:
    - Communications and Risk Management Officer's Certificate
    - Information Disclosure

2.5.2 Add minimum eligibility criteria information

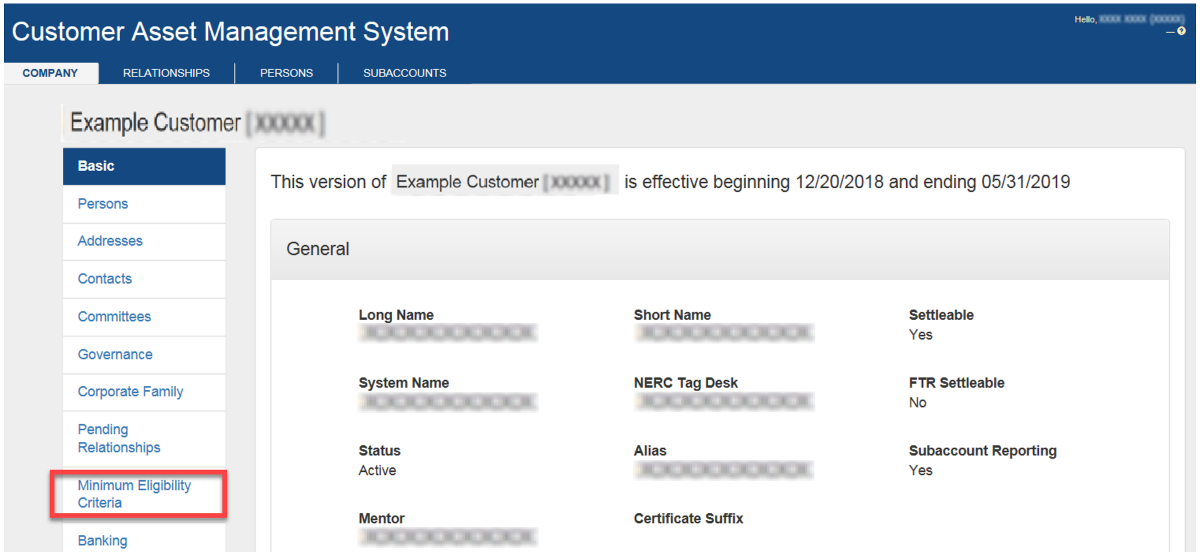
- Role that can perform this task:
    - External MEC Maintainer

1. Launch the CAMS interface. See the "Accessing CAMS"

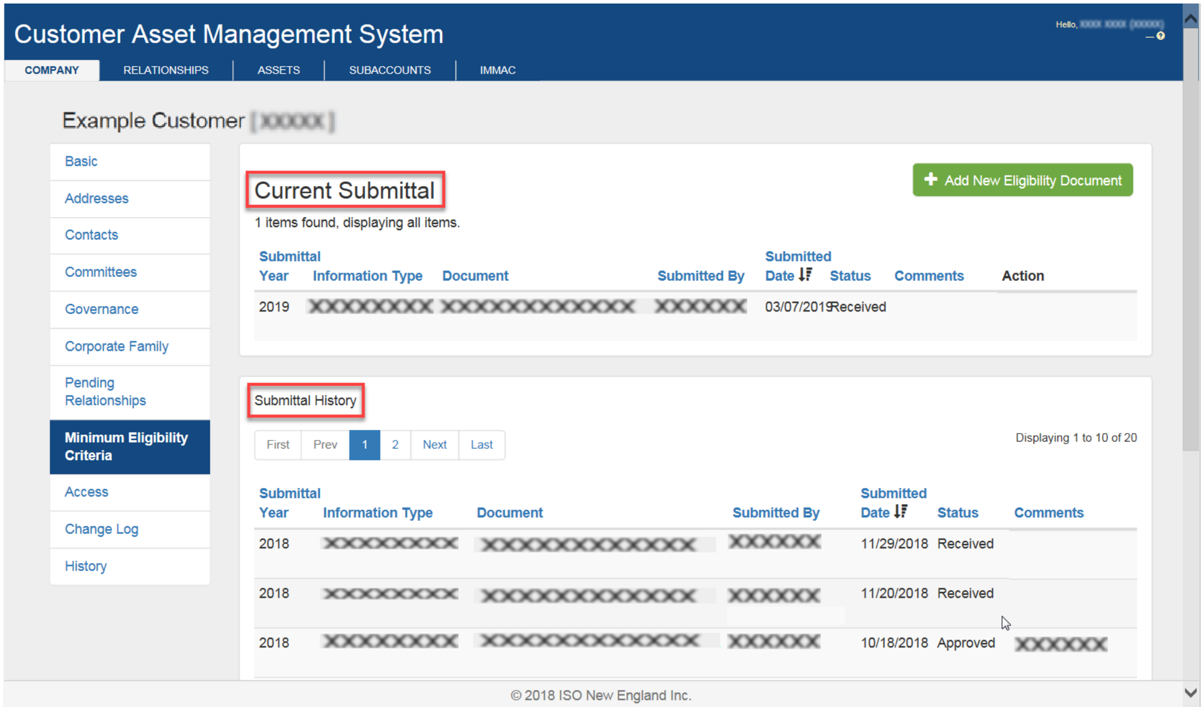
2. The Customer "Basic" information screen displays:



3. Click on the “Minimum Eligibility Criteria” tab in the second-level menu.

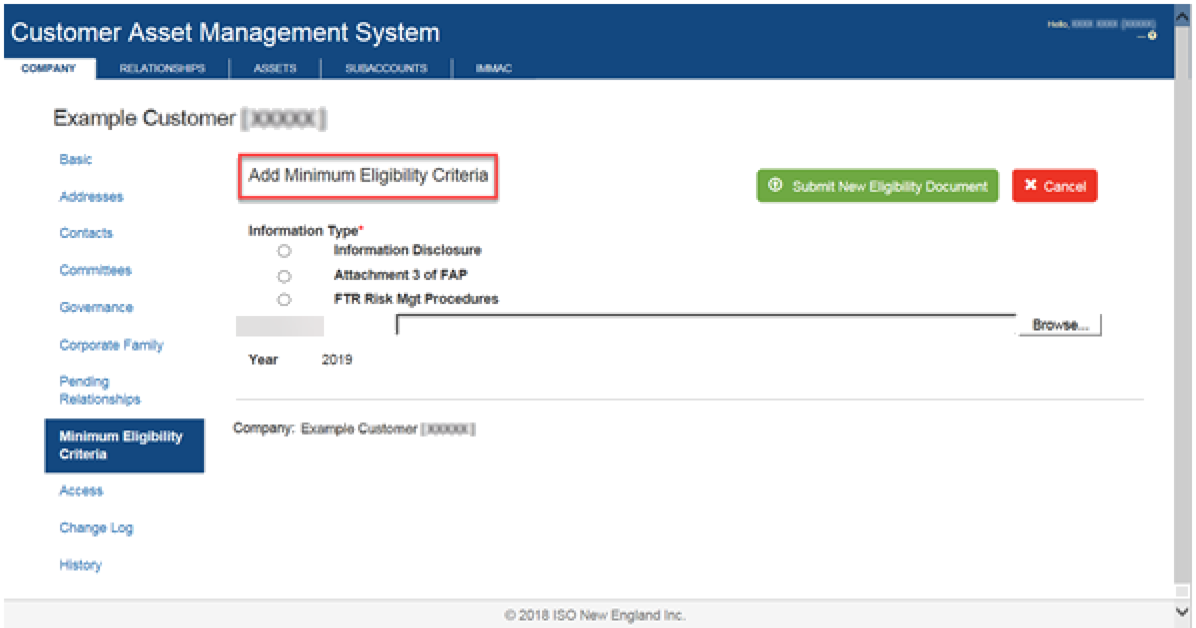


4. The "Current Submittal" and "Submittal History" screen displays:



5. Click on the “Add New Eligibility Document” button.

6. The “Add Minimum Eligibility Criteria” screen displays:

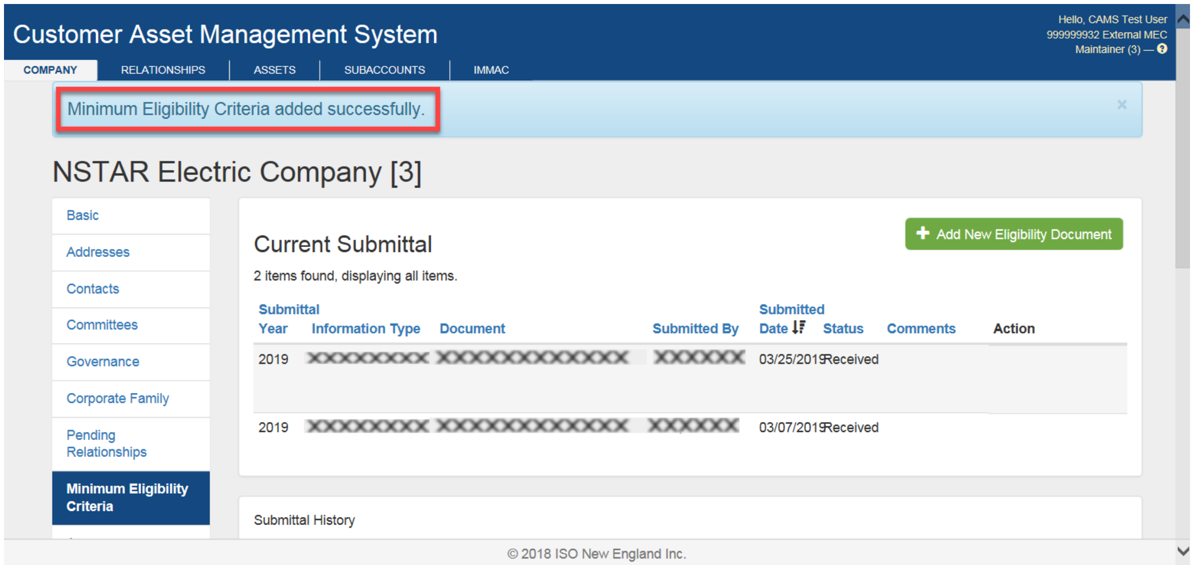


7. Select the “Information type”, browse through the document that needs to be submitted and click on “Submit New Eligibility Document” button to upload new MEC documentation.

IMPORTANT

- ❖ Information Type section is the type of document that is uploaded.
- ❖ Only the following file-type extensions are allowed to be attached as supporting documents:
    - .pdf
- ❖ The Year defaults to the current year.

8. A confirmation message displays when the Minimum Eligibility Criteria is created successfully:


Customer Asset Management System
Hello, CAMS Test User
999999932 External MEC
Maintainer (3) —
COMPANY
RELATIONSHIPS
ASSETS
SUBACCOUNTS
IMMAC
Minimum Eligibility Criteria added successfully.
NSTAR Electric Company [3]
Basic
Addresses
Contacts
Committees
Governance
Corporate Family
Pending Relationships
Minimum Eligibility Criteria
Current Submittal
Add New Eligibility Document
2 items found, displaying all items.
Submittal Year
Information Type
Document
Submitted By
Submitted Date
Status
Comments
Action
2019
03/25/2019
Received
2019
03/07/2019
Received
Submittal History
© 2018 ISO New England Inc.

IMPORTANT

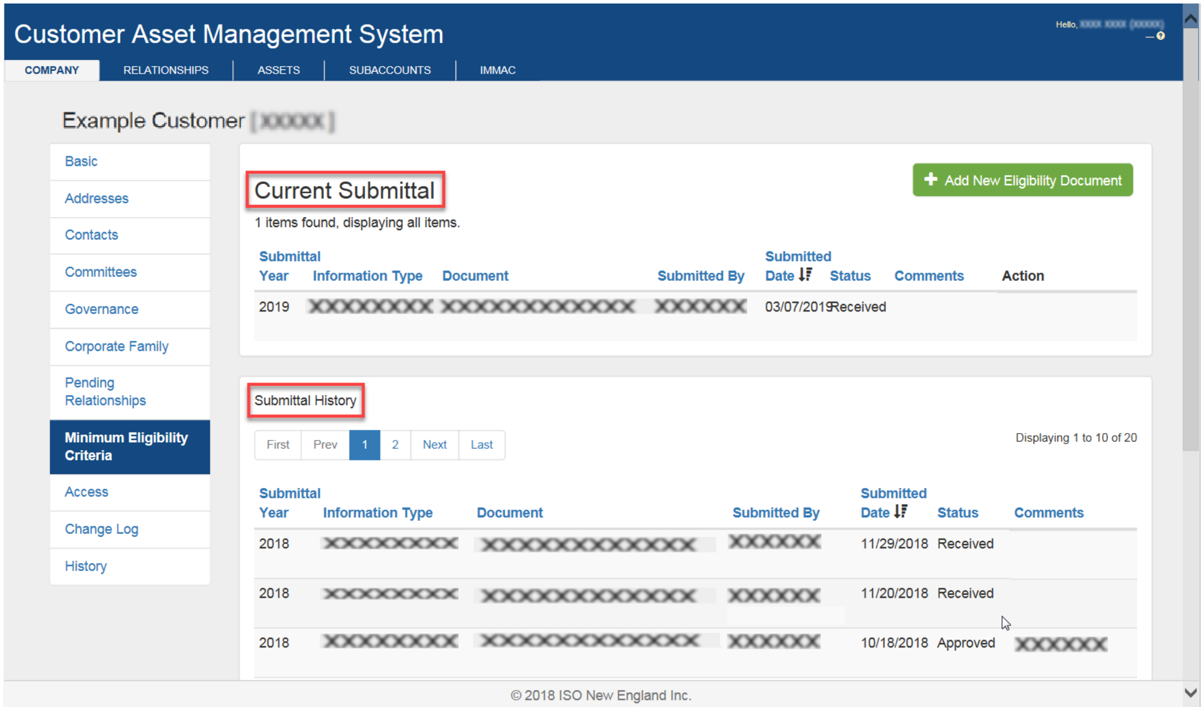
- ❖ The current year's submittals are displayed under the Current Submittal section.
- ❖ All documents for each year are seen under the Submittal History section.
- ❖ The Information Type column displays the most recent document for each Information Type.
- ❖ The Submitted Date column displays the most recent document for each Submitted Date.

2.5.3 View minimum eligibility criteria information

- Roles that can perform this task:
  - External MEC Maintainer

1. Launch the CAMS interface. See the "Accessing CAMS"
2. Click on the "Company" tab in the top-level menu.
3. Click on the "Minimum Eligibility Criteria" tab in the second-level menu.

4. The “Minimum Eligibility Criteria Listing” screen displays:



5. Click on hyperlink under the Document column to view the documents.

3 CAMS Roles

3.1 Security Administrator

- A Security Administrator (SA) is a person authorized by your company to manage users in CAMS.
- The SA is responsible for creating users in CAMS, granting users access rights to ISO New England's Standard Market Design (SMD) Applications, and managing committee assignments, contacts and MIS accounts.
    - For additional information, see the following sections in this user guide:
        - "Get Started"
        - "Manage your company's persons"
        - "Issue a digital certificate" (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
        - "Install a digital certificate" (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company must have at least one SA to use CAMS.
- Designation of an SA is normally completed as part of a company's membership application process to ISO New England.
- If your company does not have an SA—or would like to designate another SA, complete, notarize and return the *ISO New England Security Administrator Signatory Page* located on the ISO website at: https://www.iso-ne.com/static-assets/documents/support/custsvc/forms/iso_ne_security_admin_sig_page.pdf
    - The form must be signed by a company officer and notarized. Incomplete forms will not be processed. The original form, including notary stamp or seal, must be mailed to the address noted on the for.:

3.2 External Customer Maintainer

- An External Customer Maintainer has read/write access to your company's general information stored in CAMS.
- For companies that are a Demand Designated Entity (DDE), the External Customer Maintainer manages the RTU-to-Demand Resource mappings.
- This role does not have access to any "persons" information.

- For additional information see the following sections in this user guide:
  - "Get Started"
  - "Manage your company's information"
  - DDE companies only: "Manage your Demand Resources and Demand Assets" (see the CAMS User Guide for Asset and Resource Maintenance)
  - "Install a digital certificate" (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Customer Maintainers.
- Only a Security Administrator may assign the External Customer Maintainer role to a person.

3.3 External Customer Viewer

- An External Customer Viewer has read-only access to the company's general information stored in CAMS. This role does not have access to any "persons" information.
  - For additional information see the following sections in this user guide:
    - "Get Started"
    - "Manage your company's information"
    - DDE Companies only: "Manage your Demand Resources and Demand Assets" (see the CAMS User Guide for Asset and Resource Maintenance)
    - "Install a digital certificate" (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Customer Maintainers.
- Only a Security Administrator may assign the External Customer Maintainer role to a person.

3.4 External Person Maintainer

- An External Person Maintainer has read and write access to the company's Persons section in CAMS.

- An External Person Maintainer can update existing person information, but cannot add a person to the CAMS database or grant access or roles to existing persons in the database. Only a Security Administrator can add persons and grant persons access to ISO applications.
    - For additional information see the following sections in this user guide:
        - "Get Started"
        - "Manage your company's persons"
        - "Install a digital certificate" (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Person Maintainers.
- Only a Security Administrator may assign the External Person Maintainer role to a person.

3.5 External Person Viewer

- An External Person Viewer has read-only access to the company's Persons section in CAMS.
    - For additional information see the following sections in this user guide:
        - "Get Started"
        - "Manage your company's persons"
        - "Install a digital certificate" (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Person Viewers.
- Only a Security Administrator may assign the External Person Viewer role to a person.

3.6 External Demand Resource Maintainer

- An External Demand Resource Maintainer is responsible for managing the company's Demand Resource information and resource mappings.
    - For additional information see the following section in this user guide:
        - "Get Started"
        - "Manage your Demand Resources and Demand Assets" (see the CAMS User Guide for Asset and Resource Maintenance)

        - “Install a digital certificate” (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Demand Resource Maintainers.
- Only a Security Administrator may assign the External Demand Resource Maintainer role to a person.

3.7 External Resource Viewer

- An External Resource Viewer has read-only access to the company’s Generator, Demand and Import Resource information in CAMS.
    - For additional information see the following sections in this user guide:
        - “Get Started”
        - “Manage your Demand Resources and Demand Assets” (see the CAMS User Guide for Asset and Resource Maintenance)
        - “Install a digital certificate” (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Resource Viewers.
- Only a Security Administrator may assign the External Resource Viewer role to a person.

3.8 External Demand Asset Maintainer

- An External Demand Asset Maintainer is responsible for managing the company’s Demand Assets in CAMS, including:
    - enrolling measures
    - maintaining measure information
    - creating and maintaining asset information
    - mapping assets to resources
- For additional information see the following sections in this user guide:
    - “Get Started”
    - “Manage your Demand Resources and Demand Assets” (see the CAMS User Guide for Asset and Resource Maintenance)

        - "Install a digital certificate" (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Demand Asset Maintainers.
- Only a Security Administrator may assign the External Demand Asset Maintainer role to a person.

3.9 External Demand Asset Viewer

- An External Demand Asset Viewer has read-only access to the company's Demand Asset information.
    - For additional information see the following section in this user guide:
        - "Get Started"
        - "Manage your Demand Resources and Demand Assets" (see the CAMS User Guide for Asset and Resource Maintenance)
        - "Install a digital certificate" (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Demand Asset Viewers.
- Only a Security Administrator may assign the External Demand Asset Viewer role to a person.

3.10 External Demand Host Participant Viewer

- An External Demand Host Participant Viewer has read-only access to information and mappings for all Demand Assets that have been registered within the Host Participant's metering domain.
    - See the following section in this user guide:
        - "Get Started"
        - "Manage your Demand Resources and Demand Assets" (see the CAMS User Guide for Asset and Resource Maintenance)
        - "Install a digital certificate" (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Demand Host Participant Viewers.
- Only a Security Administrator may assign the External Demand Host Participant Viewer role to a person.

3.11 External Demand Meter Reader Viewer

- An External Demand Meter Reader Viewer has read-only access to information and mappings for Demand Assets assigned to the company.
    - The role grants the user access to CAMS metering information for Demand Assets to which the company has been assigned.
- This role should not be confused with the “LRP Meter Reader” contact type, which provides the user with email correspondence, notifications, and service notes about any Demand Assets that are assigned to the company.
    - For additional information see the following section in this user guide:
        - “Get Started”
        - “Manage your Demand Resources and Demand Assets” (see the CAMS User Guide for Asset and Resource Maintenance)
        - “Install a digital certificate” (see the CAMS User Guide for Digital Certificates which is available by contacting ISO-NE Participant Support or your SA)
- A company may have multiple External Demand Meter Reader Viewers.
- Only a Security Administrator may assign the External Demand Meter Reader Viewer role to a person.

3.12 External Asset Maintainer

- Read/write access to submit and/or approve new settlement only generator and load assets, submit and/or approve asset relationship changes (ownership, lead participant, meter reader), and submit and/or approve asset retirements. New asset, relationship change, and asset retirement requests are initiated by the asset’s Lead Participant. This role will not provide read/write access to demand assets (request External Demand Asset Maintainer)
- A company may have multiple External Asset Maintainers.
- Only a Security Administrator may assign the External Asset Maintainer role to a person.

3.13 External Asset Viewer

- Read-only access allows the user to view and download asset information for modeled generator, settlement only generator, load, alternative technology regulation resource, asset related demand and non-energy assets for assets which the user's company has one or more associations with the asset (Lead Participant, Asset Owner, Meter Reader, Host Participant). This role will not provide view access to demand assets

(request External Demand Asset Viewer)

- A company may have multiple External Asset Viewers.
- Only a Security Administrator may assign the External Asset Viewer role to a person.

3.14 External MEC Maintainer

- An External Minimum Eligibility Criteria (MEC) Maintainer has read and write access to their company's Minimum Eligibility Criteria information stored in CAMS.
    - For additional information see the following sections in this user guide:
        - "Overview of Minimum Eligibility Criteria"
        - "Add minimum eligibility criteria information"
        - "View minimum eligibility criteria information"
- A company may have multiple External MEC Maintainers.
- Only a Security Administrator may assign the External Minimum Eligibility Criteria Maintainer role to a person.

3.15 External MEC Viewer

- An External Minimum Eligibility Criteria (MEC) Viewer has read-only access to the Minimum Eligibility Criteria information stored in CAMS.
    - For additional information see the following sections in this user guide:
        - "Overview of Minimum Eligibility Criteria"
        - "Add minimum eligibility criteria information"
        - "View minimum eligibility criteria information"
- A company may have multiple External MEC Viewers.
- Only a Security Administrator may assign the External Minimum Eligibility Criteria Viewer role to a person.

4 Participant Support

4.1 By Internet

https://www.iso-ne.com/about/contact/participant-support

4.2 By Telephone

Hours and Days of Operation can be found on the ISO New England website

For emergency inquiries dial: **(877) 226-4814**

4.3 By Email

askiso@iso-ne.com

4.4 Ask ISO Manager

Ask ISO is available to anyone that wants to submit an inquiry or information to ISO New England. The Ask ISO Manager role is managed in CAMS and is granted access to users by their company security administrator. This role allows the user to view all cases for all users within their organization. Ask ISO can be accessed by clicking the link on the ISO New England Participant Support landing page or for those with active digital certificates via a link at the left of the SMD homepage. See "Granting a person access to CAMS or another ISO application"

4.5 NEPOOL Membership Questions

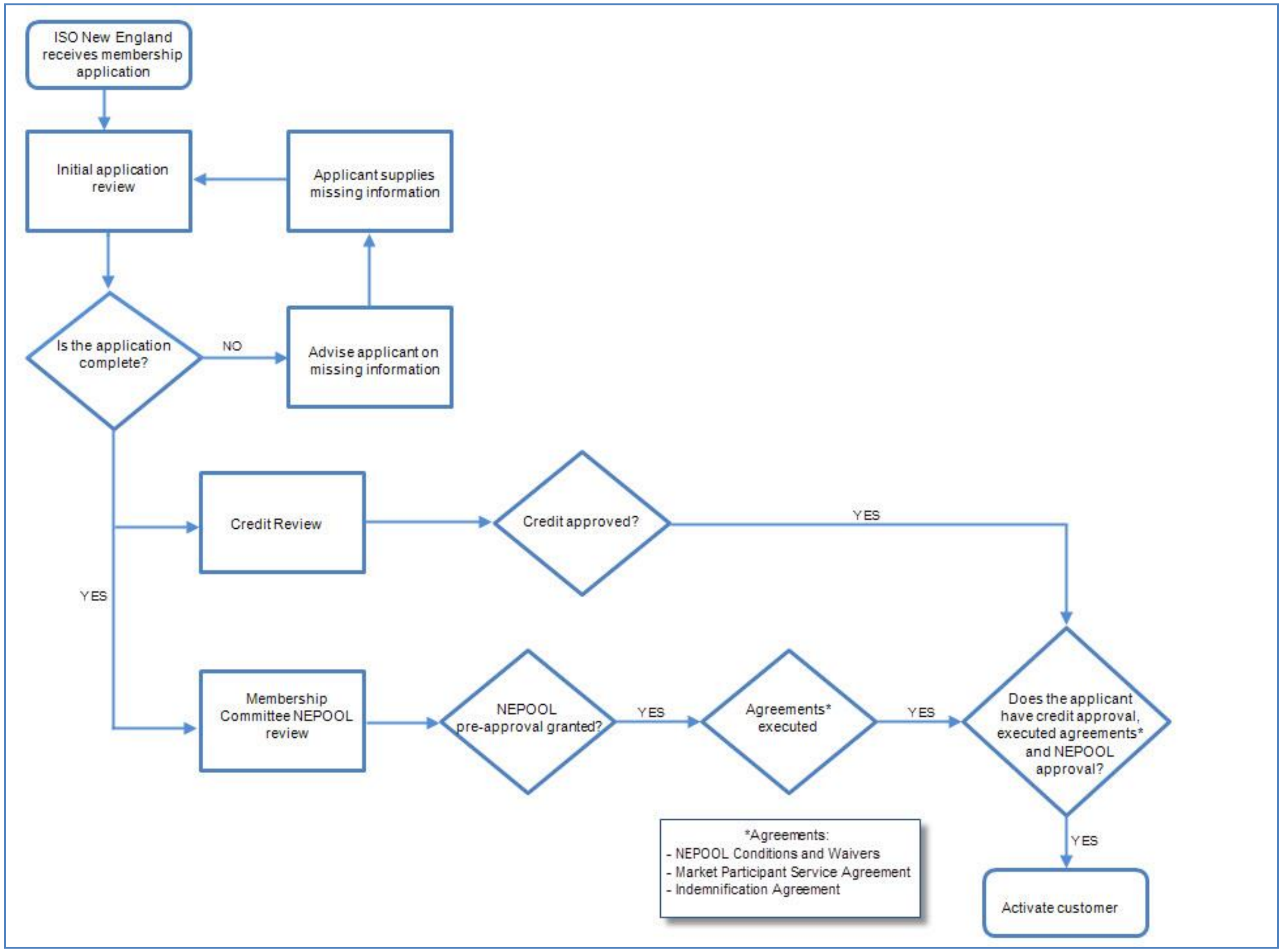
On the web:
https://www.iso-ne.com/participate/support/faq/membership

Inquiries related to NEPOOL membership may be directed to:
memcoord@iso-ne.com.

4.6 Financial Assurance Questions

Financial Assurance margin call (80%, 90%, 100% Notices) inquires may be directed to:
(413) 540-4400

4.7 Membership Application Process



5 Links

5.1 ISO New England Security Administrator Signatory Page

https://www.iso-ne.com/static-assets/documents/support/custsvc/forms/iso_ne_security_admin_sig_page.pdf

5.2 ISO New England Training Page

https://www.iso-ne.com/participate/training

5.3 ISO New England FAQ Page

https://www.iso-ne.com/participate/support/faq

5.4 SMD Site for ISO Applications

https://smd.iso-ne.com/

5.5 SMD Site for ISO Sandbox Applications

https://sandboxsmd.iso-ne.com/

5.6 ISO New England Glossary and Acronyms

https://www.iso-ne.com/participate/support/glossary-acronyms