

# 

OTCnet Participant User Guide

Table of Contents

[Overview, Topics, and Audience 1](#_Toc188538079)

[Overview 1](#_Toc188538080)

[Topics 1](#_Toc188538081)

[Audience 1](#_Toc188538082)

[Topic 1 The Purpose of Managing User Accounts 2](#_Toc188538083)

[Topic 2 Creating a User Identity in SailPoint IIQ 3](#_Toc188538084)

[Create a User Identity in SailPoint IIQ 3](#_Toc188538085)

[Create a User Identity in SailPoint IIQ 4](#_Toc188538086)

[Topic 3 Adding or Removing User Access in SailPoint IIQ 7](#_Toc188538087)

[Add User Access in SailPoint IIQ 7](#_Toc188538088)

[Add User Access in SailPoint IIQ 8](#_Toc188538089)

[Remove User Access in SailPoint IIQ 11](#_Toc188538090)

[Remove User Access in SailPoint IIQ 12](#_Toc188538091)

[Topic 4 Approving or Denying User Access Requests in SailPoint IIQ 15](#_Toc188538092)

[Approve or Deny User Access Requests in SailPoint IIQ 15](#_Toc188538093)

[Approve or Deny User Access Requests in SailPoint IIQ 16](#_Toc188538094)

[Topic 5 Importing User Identity to OTCnet 18](#_Toc188538095)

[Import User Identity to OTCnet 18](#_Toc188538096)

[Import User Identity to OTCnet 19](#_Toc188538097)

[Topic 6 Adding or Removing an Endpoint/Role for an OTCnet User 22](#_Toc188538098)

[Add an Endpoint/Role for an OTCnet User 22](#_Toc188538099)

[Add an Endpoint/Role for an OTCnet User 23](#_Toc188538100)

[Remove an Endpoint/Role for an OTCnet User 26](#_Toc188538101)

[Remove an Endpoint/Role for an OTCnet User 27](#_Toc188538102)

[Topic 7 Approving or Rejecting an Endpoint/Role (or the Removal of an Endpoint/Role) 29](#_Toc188538103)

[Approve or Reject an Endpoint/Role (or the Removal of an Endpoint/Role) 29](#_Toc188538104)

[Approve or Reject an Endpoint/Role (or the Removal of an Endpoint/Role) 30](#_Toc188538105)

[Summary 34](#_Toc188538106)

List of Figures

[Figure 1: Creating Identity in SailPoint IIQ 4](#_Toc188538107)

[Figure 2: Create Identity Screen 5](#_Toc188538108)

[Figure 3: Create Identity Request Submitted 5](#_Toc188538109)

[Figure 4: Manage Access/Manage User Access 8](#_Toc188538110)

[Figure 5: Select Users Screen 9](#_Toc188538111)

[Figure 6: Manage Access/Add Access Screen 9](#_Toc188538112)

[Figure 7: Review and Submit Add Access Screen 10](#_Toc188538113)

[Figure 8: Search Users Screen 12](#_Toc188538114)

[Figure 9: Remove User Access Screen 13](#_Toc188538115)

[Figure 10: Review and Submit Remove Access Screen 13](#_Toc188538116)

[Figure 11: Approval Awaiting the Approver's Action Screen 16](#_Toc188538117)

[Figure 12: Approve or Deny Screen 16](#_Toc188538118)

[Figure 13: Import OTCnet User Identity 19](#_Toc188538119)

[Figure 14: Enter User’s Email Address to Import User 19](#_Toc188538120)

[Figure 15: Import User Identity Confirmation Screen 20](#_Toc188538121)

[Figure 16: Search User Directory Screen 23](#_Toc188538122)

[Figure 17: Manage User Account Screen 23](#_Toc188538123)

[Figure 18: Add Endpoint/Role Screen 24](#_Toc188538124)

[Figure 19: Confirmation Screen on Adding Endpoint/Role Request Submitted 25](#_Toc188538125)

[Figure 20: Manage User Account Screen 27](#_Toc188538126)

[Figure 21: Select an Endpoint and Role to Remove Screen 28](#_Toc188538127)

[Figure 22: Confirmation Screen on Removing Endpoint/Role Request Submitted 28](#_Toc188538128)

[Figure 23: Manage OTCnet Users Screen 30](#_Toc188538129)

[Figure 24: Access Approval Request Screen 31](#_Toc188538130)

[Figure 25: Confirmation Screen on Approval/Rejection of the Access Request 32](#_Toc188538131)

Glossary

Select this [link](https://www.fiscal.treasury.gov/otcnet/training/wbt/content/course_OTC/glossary.htm) to access the full OTCnet Glossary.

## Overview, Topics, and Audience

### Overview

Welcome to *Managing User Accounts*. In this chapter, you will learn how to:

* Manage user accounts
* Create an identity for a user in SailPoint IIQ
* Add or remove user access in SailPoint IIQ
* Approve or deny user access requests in SailPoint IIQ
* Import a user identity to OTCnet
* Add or remove an endpoint/role for an OTCnet user
* Approve or reject an endpoint/role (or the removal of an endpoint/role) in OTCnet

### Topics

The topics in this chapter include the following:

1. The Purpose of Managing User Accounts
2. Creating an Identity for a User in SailPoint IIQ
3. Adding or Removing User Access in SailPoint IIQ
4. Approving or Denying User Access Requests in SailPoint IIQ
5. Importing a User Identity to OTCnet
6. Adding or Removing an Endpoint/Role for an OTCnet User
7. Approving or Rejecting an Endpoint/Role (or the Removal of an Endpoint/Role) in OTCnet

### Audience

The intended audience for the Managing User Accounts Participant User Guide includes:

* Primary Local Security Administrator (PLSA)
* Local Security Administrator (LSA)

## Topic 1 The Purpose of Managing User Accounts

As the **Primary Local Security Administrator (PLSA)** or **Local Security Administrator (LSA)** for your organization, you are authorized to manage the users who have access to OTCnet. Before a user can access OTCnet, they must have an identity and account created in SailPoint IIQ.

The **PLSAs**/**LSAs** assist with creating an identity for a user and/or requesting a High-Level Organization (HLO) or role access for them in SailPoint IIQ. This is the preferred method of registration for users in SailPoint IIQ, while the self-registration functionality is available to users as needed.

Managing a user’s account involves (in order):

* Registering users by creating an identity for a user in SailPoint IIQ
* Adding or removing user access in SailPoint IIQ
* Approving or denying user access requests in SailPoint IIQ
* Importing a user identity to OTCnet
* Adding or removing an endpoint/role for a user in OTCnet
* Approving or rejecting an endpoint/role (or the removal of an endpoint/role) for a user in OTCnet

The **User Provisioning** workflow includes the following high-level action steps:

1. The **PLSA** or **LSA** receives an authorized/approved request to add a new user (from their organization) to OTCnet.
2. The **PLSA** or **LSA** logs in to SailPoint IIQ, selects **Manage User Access**, and searches for the **email address** of the new user from the request in step 1.
   1. If the email address is not found, the **PLSA** or **LSA** selects **Manage Identity** and **Create Identity** from the menu options. They enter the authorized user’s email address and select **Submit**.
   2. If the email address is found, the **PLSA** or **LSA** continues with step 3.
3. The **PLSA** or **LSA** adds the authorized **role**/**HLO** or **role**/**Financial Institution** (**FI**) combinations to the identity.
4. Another **PLSA** or **LSA** approves (or denies) the request in SailPoint.
5. The **PLSA** or **LSA** imports the **email address** of a new user to OTCnet so that the user can be added to the OTCnet database. Then the **PLSA** or **LSA** assigns the authorized **endpoint(s)** and **role(s)** to the user.
6. Another **PLSA** or **LSA** approves (or rejects) the request in OTCnet. Then the user is informed that their OTCnet provisioning is complete.

## Topic 2 Creating a User Identity in SailPoint IIQ

SailPoint IIQ is an identity management solution utilized by the Department of the Treasury. It is being phased in through the Common Approach to Identity Assurance project, commonly referred to as CAIA.

### Create a User Identity in SailPoint IIQ

The **PLSAs** and **LSAs** assist with creating an identity for a user and/or requesting an **HLO** or **role** access for them in SailPoint IIQ. **This is the preferred method for registering users and requesting HLO and role access for users in SailPoint IIQ**.

To create a user identity, select **Create Identity** from the menu at the top left of the SailPoint IIQ application under **Manage Identity.** Thenenter their **email address** and select the **Submit** button.

Two notification emails will be sent out once an identity is created:

* One to the new identity holder, and
* One to the person who created the identity.

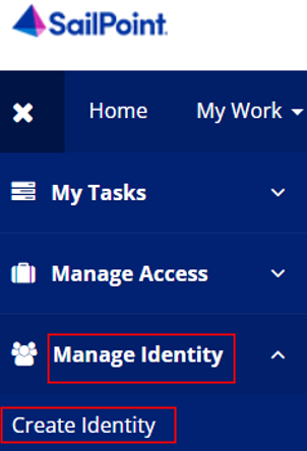
New users, not registered in SailPoint IIQ, will not be able to access OTCnet. Their identity will not be recognized. They may get a message that the email and/or password they entered is incorrect.

Create a User Identity in SailPoint IIQ

To create a user identity, complete the following steps:

1. At the top left of the SailPoint IIQ application, select the **Hamburger Menu** to display the available menu options.
2. Select the **Manage Identity** option, then select **Create Identity** as shown in Figure 1.

Figure 1: Creating Identity in SailPoint IIQ



1. SailPoint IIQ will route to the **Create Identity** screen as shown in Figure 2.

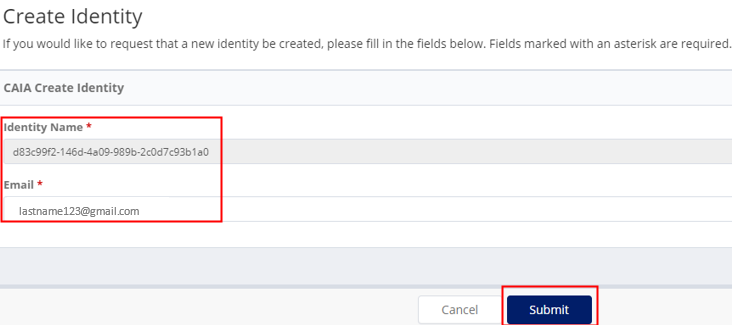
Application Tip



* There will be two fields available to fill out, **Identity Name** and **Email**.
* The **Identity Name** will be prepopulated as it is a unique identifier required by SailPoint IIQ.

1. Enter an **email address** for the identity you want to create and select **Submit** at the bottom of the page.

Figure 2: Create Identity Screen



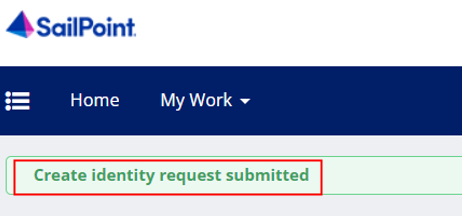
Application Tip



SailPoint IIQ will notify you if an identity with the email you provided already exists.

1. Once submitted, SailPoint IIQ will display the home page with a success message as shown in Figure 3.

Figure 3: Create Identity Request Submitted



Application Tip



* Due to system design, it may take up to a minute for the identity to be processed in SailPoint IIQ.
* Two notification emails will be sent out once an identity is created, one to the new identity holder and one to the person who created the identity.

## Topic 3 Adding or Removing User Access in SailPoint IIQ

There are two system administrator groups inside SailPoint IIQ, requestors and approvers.

* Requestors can request (or add access) on behalf of someone else. They can also remove user access.
* Approvers can approve or deny those requests. The application approvers will receive notification that there is an access request available to review.

After a **PLSA** or **LSA** requests access for a user, the application looks for other approvers for the organizational **HLO or role** selection and notifies them of the pending request.

In SailPoint IIQ, approvers are determined based on the HLO selections (approvers are security administrators with the same HLO assignments).

### Add User Access in SailPoint IIQ

To request/add OTCnet user access, select **Manage Access** from the main menu, then select **Manage User Access.** Search for the user by typing their **email address** and selecting the **Search** button. Then select the **checkmark** to the left of the user's email address in the returned search result and select **Next.**

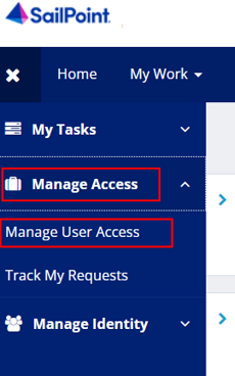
Make sure that **Add Access** is selected. In the search field, enter the **HLO or role** name to be assigned to the user. To select the **HLO or role** in the search results, select the **checkmark** to the left of the **HLO or role** name, then select **Next.** Review the requested role(s) and select the **Submit** button.

Add User Access in SailPoint IIQ

To request/add OTCnet user access, complete the following steps:

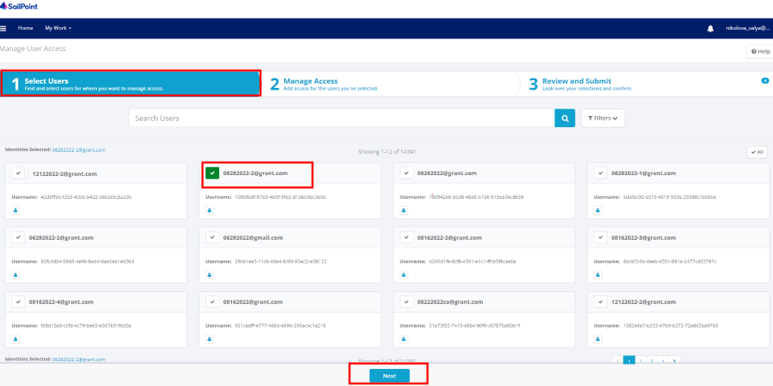
1. At the top left of left of the application, select the **Hamburger Menu** to display the options.
2. Select the **Manage Access** option, then select **Manage User Access** as shown in Figure 4.

Figure 4: Manage Access/Manage User Access



1. Search for the user (recipient of the access) by typing their **email address** and selecting the **Search** button (blue magnifying glass) as shown in Figure 5.
2. Select the **checkmark** to the left of the user's **email address** in the returned search result, then select **Next** at the bottom of the page.

Figure 5: Select Users Screen



1. Select **Add Access** as shown in Figure 6.In the search field, enter part or all of the **HLO or role** name to be assigned to the user. For example, enter “customer.”

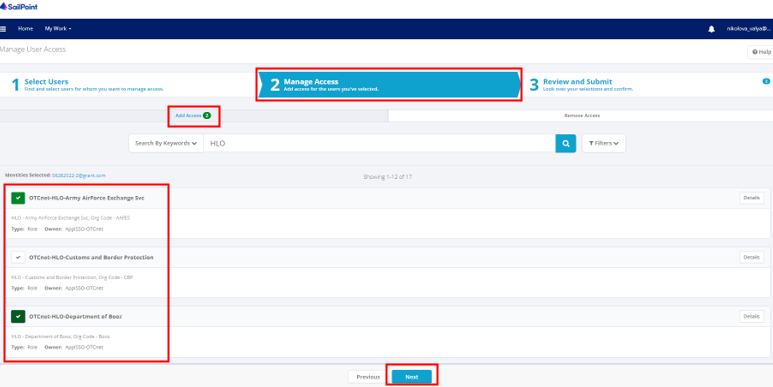
Application Tip



If you are unsure of the **HLO or role** name, simply select the **Magnifying Glass** button to return all roles that you as a requestor are authorized to provision to users.

1. Select an **HLO or role** by selecting the **checkmark** to the left of the **HLO or role** name. Select **Next** at the bottom of the page.

Figure 6: Manage Access/Add Access Screen



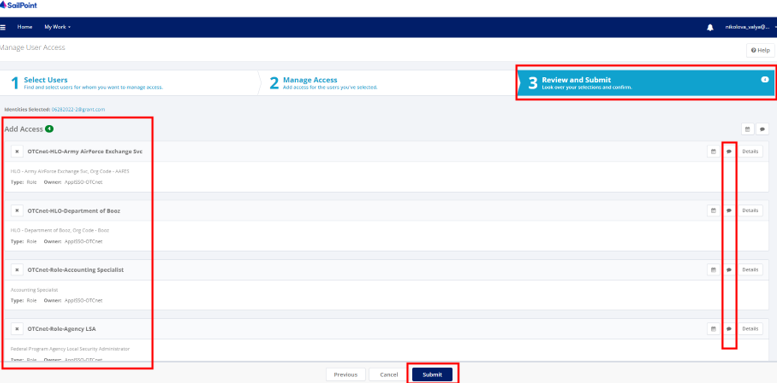
Application Tip



Multiple **HLOs or roles** can be selected.

1. Review the requested **HLOs or role(s)** as shown in Figure 7. Select the **voice bubble** on the right side to add any comments on the **HLO or role**, as needed. Then select the **Submit** button when finished.

Figure 7: Review and Submit Add Access Screen



1. A confirmation message will appear. You will also receive an **email** confirmation. The request is now pending approval.

### Remove User Access in SailPoint IIQ

To remove user’s access, select **Manage Access** from the main menu, then select **Manage User Access.** Search for the user by typing their **email address** and selecting the **Search** button. Then select the **checkmark** to the left of the user's **email address** in the returned search result and select **Next.**

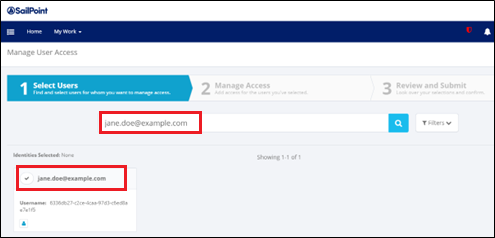
Make sure **Remove Access** is selected and then select the **Magnifying Glass** Icon to the right of the text box to return all currently assigned **HLOs or roles** for the selected user. If everything is correct, select the **Submit** button to confirm the changes. If the information is incorrect, select the **Previous** button to modify the removal.

Remove User Access in SailPoint IIQ

To remove OTCnet user access, complete the following steps:

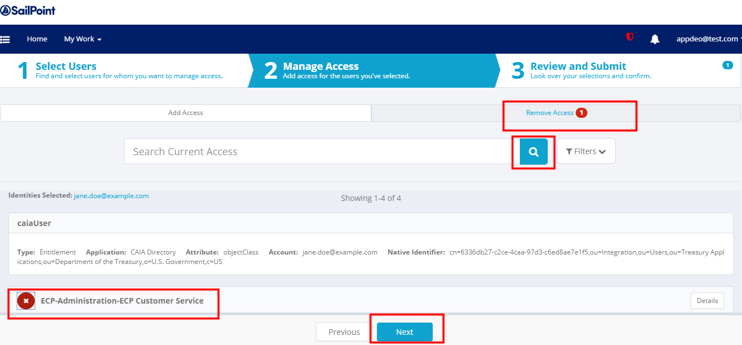
1. At the top left of the application, select the **Hamburger Menu** to display the options.
2. Select the **Manage Access** option, then select **Manage User Access.**
3. Search for the user by typing their **email address** and selecting the **Search** button (blue magnifying glass) as shown in Figure 8.
4. Select the **checkmark** to the left of the user's **email address** in the returned search result, then select **Next** at the bottom of the page.

Figure 8: Search Users Screen



1. Select **Remove Access** as shown in Figure 9.Then select the **Magnifying Glass** iconto the right of the text box to return all currently assigned **HLOs or roles** for the selected user. Select **Next**.

Figure 9: Remove User Access Screen



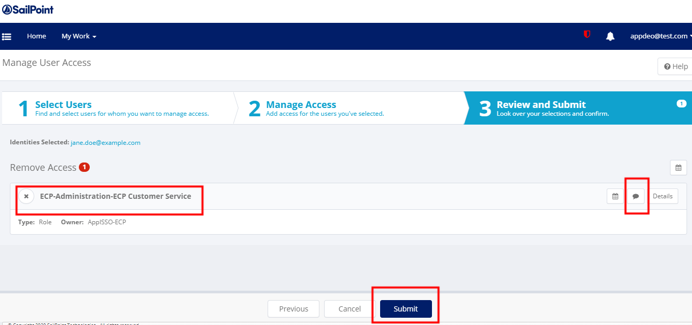
Application Tip



The requestor will only be able to remove **HLOs or roles** that they are authorized to manage.

1. Review the information to confirm the removal as shown in Figure 10. You may add any comments using the **voice bubble** on the right side. Then select the **Submit** button to confirm the changes.

Figure 10: Review and Submit Remove Access Screen



Application Tip



If the information is incorrect, select the **Previous** button to modify the removal.

## Topic 4 Approving or Denying User Access Requests in SailPoint IIQ

A **PLSA** or **LSA** assigns **HLOs or roles** to a user; approvers of these requests are determined based on the **HLO** org selections. They are security administrators with the same HLO assignments. An approver logs in to SailPoint IIQ and approves (or denies) the request(s).

Most actions within SailPoint IIQ will require at least one level of approval.

### Approve or Deny User Access Requests in SailPoint IIQ

To approve or deny user access requests, first notice a **red number notification** next to the **Bell** icon in the upper right-hand corner of the main SailPoint IIQ dashboard. Select the **Approvals** (or **Notifications**) box or the **Approvals** option under the **Bell** icon.

On the right side of the screen containing the details about the request, you will have the option to approve or deny the request. Select **Approve** or **Deny** and you will see a confirmation pop-up window.

Approve or Deny User Access Requests in SailPoint IIQ

To approve or deny user access requests, complete the following steps:

1. Notice a **red number notification** next to the **Bell** icon in the upper right-hand corner of the main SailPoint IIQ dashboard as shown in Figure 11.

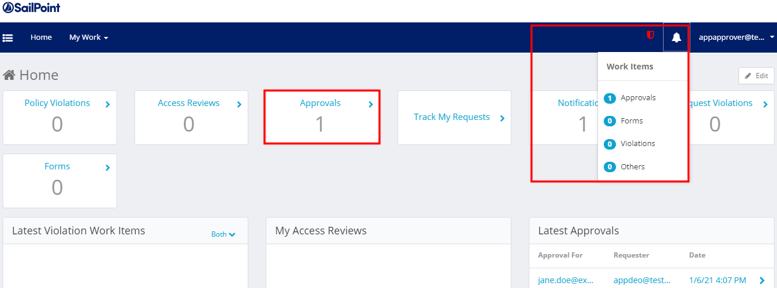
Application Tip



You may also receive an email notification about the approval request.

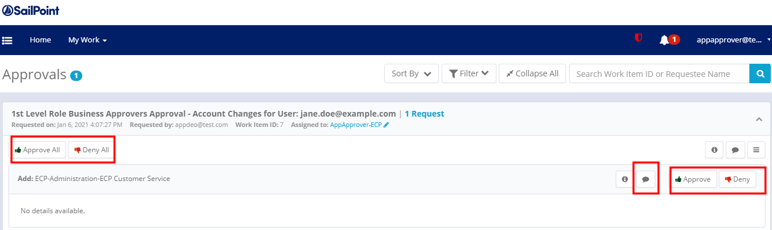
1. Select the **Approvals** (or **Notifications**) box, or the **Approvals** option under the **Bell** icon on the home page.

Figure 11: Approval Awaiting the Approver's Action Screen



1. You will be redirected to a screen containing the details about the request as shown in Figure 12.
2. Add any comments using the **voice bubble** on the right side of the screen. Then select the **Approve** or **Deny** button. A confirmation pop-up window will appear.

Figure 12: Approve or Deny Screen



Application Tip



You may select the **Approve All** or **Deny All** button on the left if you want to approve or deny multiple requests.

Application Tip



If the first-level approver denies the request, any additional levels of approval will not occur.

## Topic 5 Importing User Identity to OTCnet

Security administrators (PLSAs and LSAs) will import the **email address** of a new user to OTCnet so that the user can be added to the OTCnet database without having to wait for the user to log in.

### Import User Identity to OTCnet

PLSAs/LSAs can import the user identity to OTCnet:

* After creating an identity for a user and requesting user access for them in SailPoint, and
* After the user access request is approved by another PLSA/LSA.

Then the PLSA or LSA will add the authorized endpoint(s) and role(s) to the user in OTCnet.

To import a user identity to OTCnet: from the **OTCnet Home page**>**Administration**>**Manage Users,** select the **Import OTCnet User Identity** tab. On the **Import OTCnet User Identity** page, enter one or more **email addresses** (separated by a space, comma, semicolon, or a new line) of the user whose identity will be imported. Select the **Import User** button.

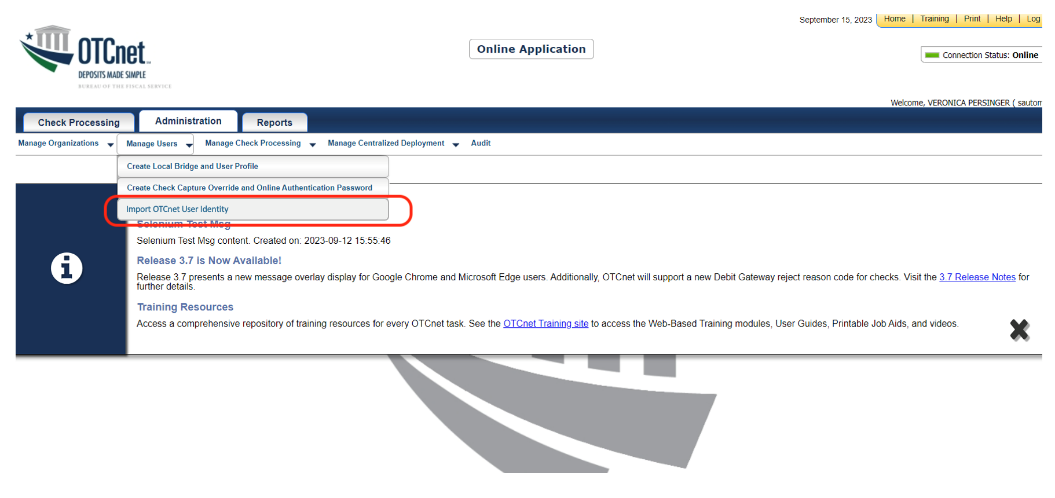
A confirmation page displays, alerting you that the user identity has been imported and/or if there are errors. Select the **OK** button on the confirmation page to return to the OTCnet home page or the **Fix Errors and Reimport** button to navigate back to the Import OTCnet User Identity page to fix the errors.

Import User Identity to OTCnet

To import an OTCnet user identity to OTCnet, complete the following steps:

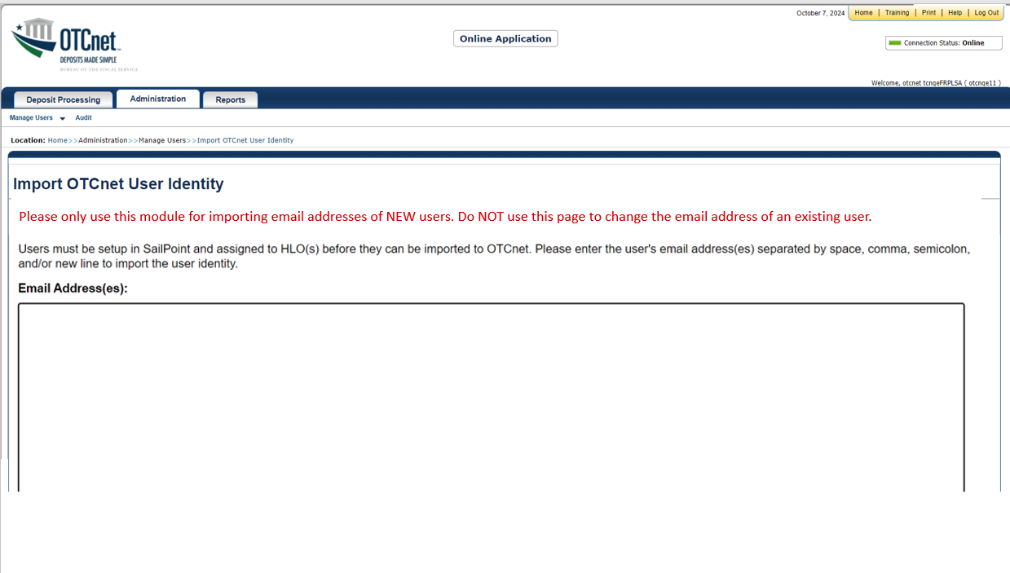
1. From the **OTCnet Home page**>**Administration**>**Manage Users,** select the **Import OTCnet User Identity** tabas shown in Figure 13.

Figure 13: Import OTCnet User Identity



1. On the **Import OTCnet User Identity** page, enter one or more **email addresses** (separated by a space, comma, semicolon, or a new line) of the user whose identity will be imported.
2. Select the **Import User** button as shown in Figure 14.

Figure 14: Enter User’s Email Address to Import User



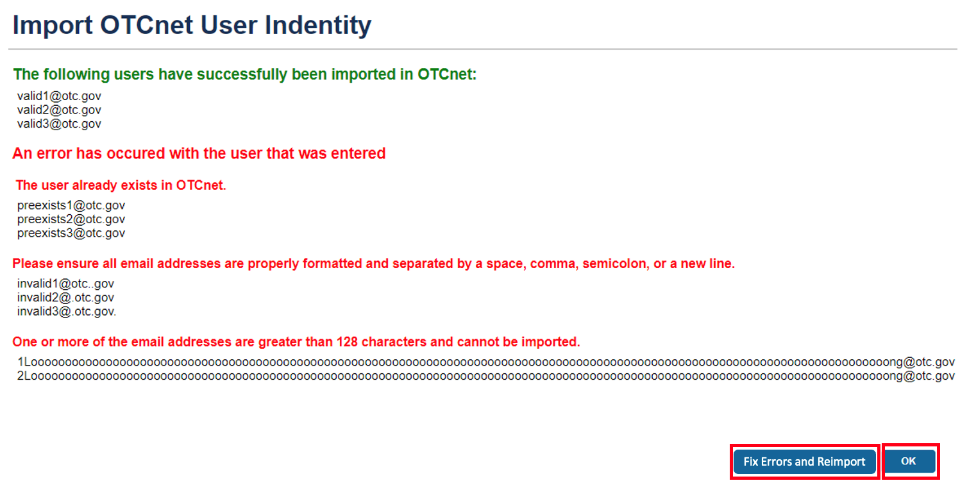
Application Tips



* Please only use this module for importing emails for **NEW** users. **Do NOT** use this screen to update an email for an existing user.
* If you select the **Import User** button without entering an email address, an error message will display, notifying you that at least one email address should be entered.
* When you select the **Cancel** button, you will be returned to the home page.

1. A confirmation page displays, alerting you that the user identity has been imported and/or if there are errors as shown in Figure 15.
2. Select the **OK** button on the confirmation page to return to the OTCnet home page or the **Fix Errors and Reimport** button to navigate back to the Import OTCnet User Identity page to fix the errors.

Figure 15: Import User Identity Confirmation Screen



Application Tips



Error messages may include:

* The email address already exists in the OTCnet database.
* The email address has an invalid format. Ensure all email addresses are properly formatted and separated by a space, comma, semicolon, or a new line.
* The email address is greater than 128 characters and cannot be imported.

Ensure that you enter the **correct email address** for the user. If you import an incorrect email address, another entry in the database will be created and the user will not be able to access the application.

Application Tip



* OTCnet automatically recognizes when an existing user logs in with a **new email address**. The database is updated to reflect the user’s new email address, preventing them from receiving a blank screen upon login.
* As a reminder, PLSAs and LSAs are responsible for **updating the user email** associated with the user's identity in **SailPoint** and verifying that the user is assigned the correct roles and endpoints associated with their **new email address** in SailPoint.

## Topic 6 Adding or Removing an Endpoint/Role for an OTCnet User

There are two types of user provisioning access requests in OTCnet:

* Adding an endpoint/role
* Removing an endpoint/role

In OTCnet, **PLSA/LSA** users log in to select specific **endpoint(s)/role(s)** for fine-grained access under the HLO(s) and role(s) selected and approved in SailPoint IIQ for a user.

### Add an Endpoint/Role for an OTCnet User

To add an **endpoint**/**role** for an OTCnet user, select the **Search User Directory** button from the **OTCnet Home page>Administration>Manage Users>Manage OTCnet Users** screen. In the search field, type the user **email address.** Then under **Manage User Account**, select **View Account**.

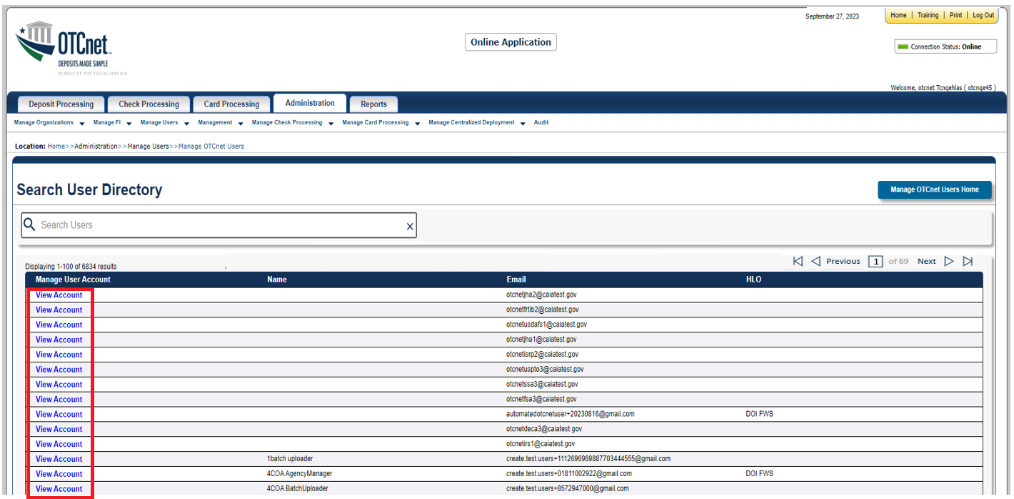
From the **Manage User Account** screen, select the **Add Endpoint/Role** button. From the **Add Endpoint/Role** screen, select a **role** from the **Choose a Role** dropdown. Then select the associated **level(s)** from the dropdown options. There can be many levels to select depending on the HLO/endpoint hierarchy. Finally, select the **Submit** button to submit your request. Review the confirmation page that appears and select the **OK** button to return to the **Manage OTCnet Users** home screen.

Add an Endpoint/Role for an OTCnet User

To add an **endpoint**/**role** for an OTCnet user, complete the following steps:

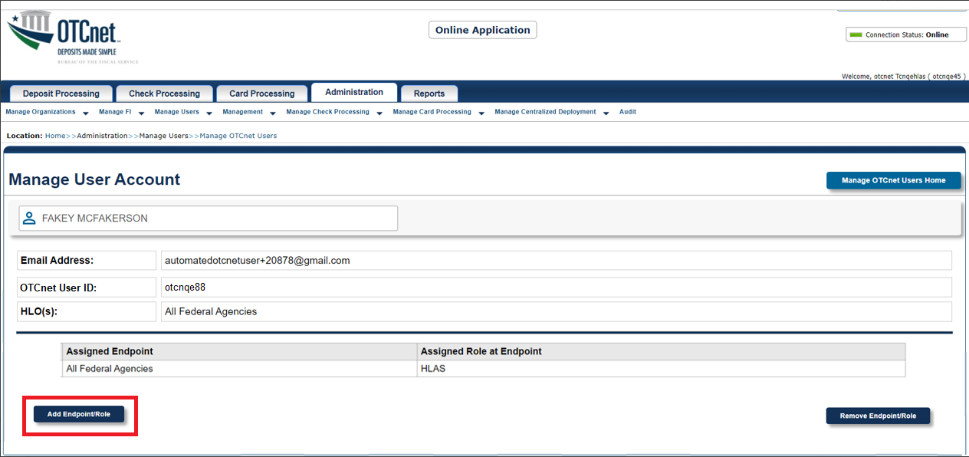
1. From the **OTCnet Home page**>**Administration**>**Manage Users**>**Manage OTCnet Users** screen, select the **Search User Directory** button.
2. In the search field, type the user’s **email address.**
3. Under **Manage User Account**, select **View Account** for the desired useras shown in Figure 16.

Figure 16: Search User Directory Screen



1. The **Manage User Account** screen displays as shown in Figure 17.
2. Review the read-only information, including the current endpoint/role assignments listed for the user. Select the **Add Endpoint/Role** button.

Figure 17: Manage User Account Screen



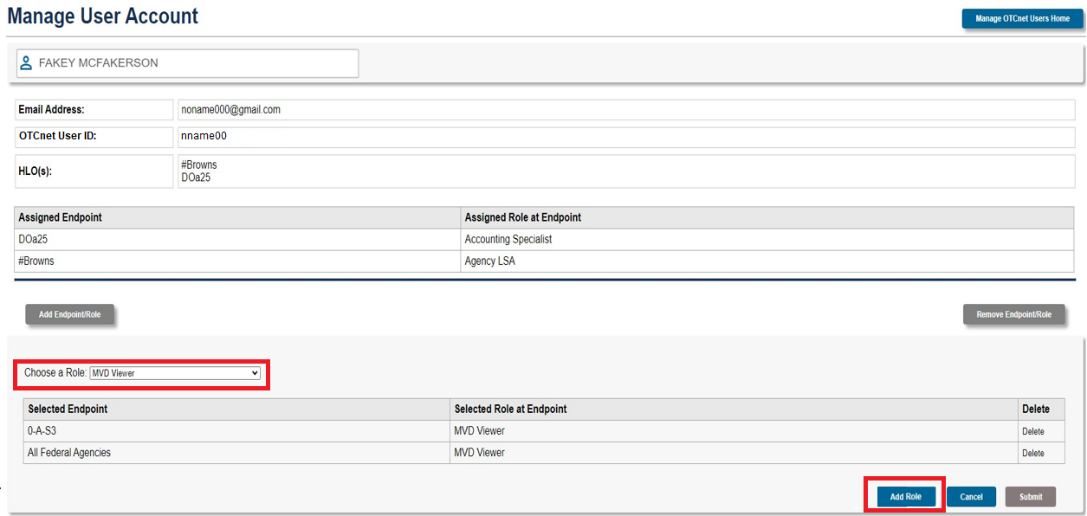
1. The **Add Endpoint/Role** screen displays as show in Figure 18.
2. Select a **role** from the **Choose a Role** dropdown, choosing from the options provisioned for the specific OTCnet user.
3. Then select the associated **level(s)** from the dropdown options (each one is based on the previous selection and may be prepopulated). There can be many levels to select depending on the HLO/endpoint hierarchy.
4. As needed, use the **Add Role** button to select additional roles. Once you select a role, it will be added to the *Selected Role at Endpoint* field as illustrated in Figure 18.

Application Tips



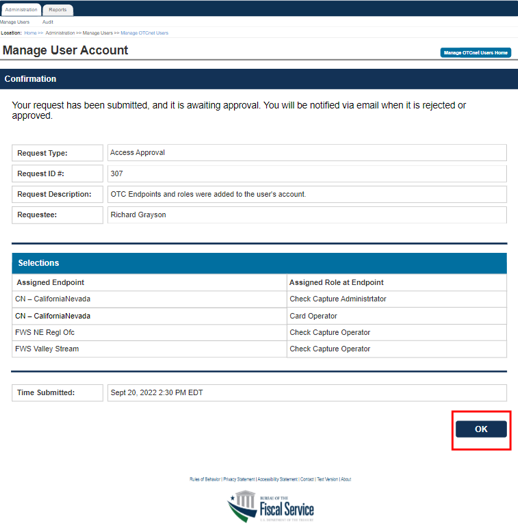
* You can select up to **10 roles** per request. After 10 role additions, the **Add Role** button is disabled. To add additional roles, you must repeat the process by submitting a new request.
* If a user changes their **email address**, security administrators should verify that the user is assigned the correct roles and endpoints associated with their **new email address** through the **Manage OTCnet Users** module.

Figure 18: Add Endpoint/Role Screen



1. Once you have selected all necessary roles, select the **Submit** button to submit your request.
2. The confirmation page appears as shown in Figure 19.
3. Select the **OK** button to return to the **Manage OTCnet Users** screen.

Figure 19: Confirmation Screen on Adding Endpoint/Role Request Submitted



Application Tip



You will be notified via email when the request is approved or rejected by another PLSA/LSA.

Application Tip



* Ensure that users log in to OTCnet **at least once every 120 days** (or four months). After the four-month period of inactivity, the user’s OTCnet entitlements will be systematically removed from their **SailPoint** identity.
  + To restore their account, users must contact the **Customer Support Team** to begin the process.
  + Customer Support will reach out to **PLSAs** and **LSAs** and require permission to restore the user’s account.
  + **PLSA/LSAs** must confirm all the previously assigned roles that were associated with the user’s identity before they can be added back.

### Remove an Endpoint/Role for an OTCnet User

To remove an endpoint/role for an OTCnet user, select the **Search User Directory** button from the **OTCnet Home page>Administration>Manage Users>Manage OTCnet Users** screen. In the search field, type the user’s **email address.** Then under **Manage User Account**, select **View Account**.

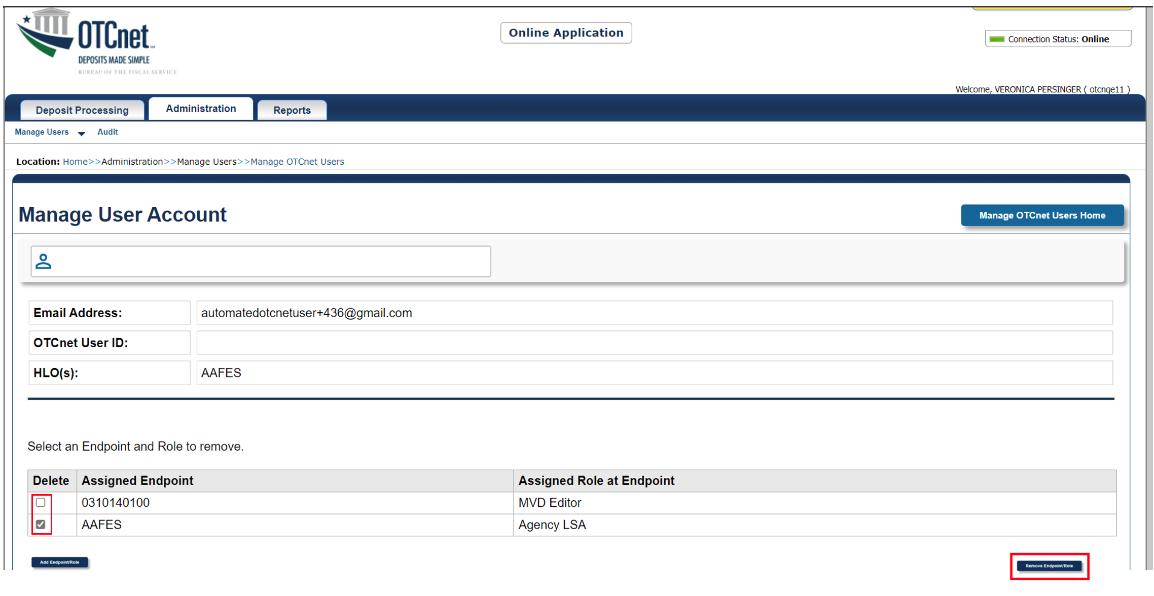
From the **Manage User Account** screen, select the **Remove** **Endpoint/Role** button. From the **Select an Endpoint and Role to Remove** screen, select the **Delete** checkbox next to the specific **Assigned Endpoint** or **Assigned Role at Endpoint** item. Then select the **Submit** button to submit your request. Review the confirmation page that appears and select the **OK** button to return to the **Manage OTCnet Users** home screen.

Remove an Endpoint/Role for an OTCnet User

To remove an endpoint/role for an OTCnet user, complete the following steps:

1. From the **OTCnet Home page**>**Administration**>**Manage Users**>**Manage OTCnet Users** screen, select the **Search User Directory** button.
2. From the **Search User Directory** screen, type the user’s **email address** in the search field.
3. Under **Manage User Account**, select **View Account**.
4. The **Manage User Account** screen displays as shown in Figure 20. Review the read-only information, including the current endpoint/role assignments listed for the user.
5. Select the **Remove** **Endpoint/Role** button.

Figure 20: Manage User Account Screen



1. The **Select an Endpoint and Role to Remove** screen displays as show in Figure 21.
2. Select the **Delete** checkbox next to the specific **Assigned Endpoint** or **Assigned Role at Endpoint** item.

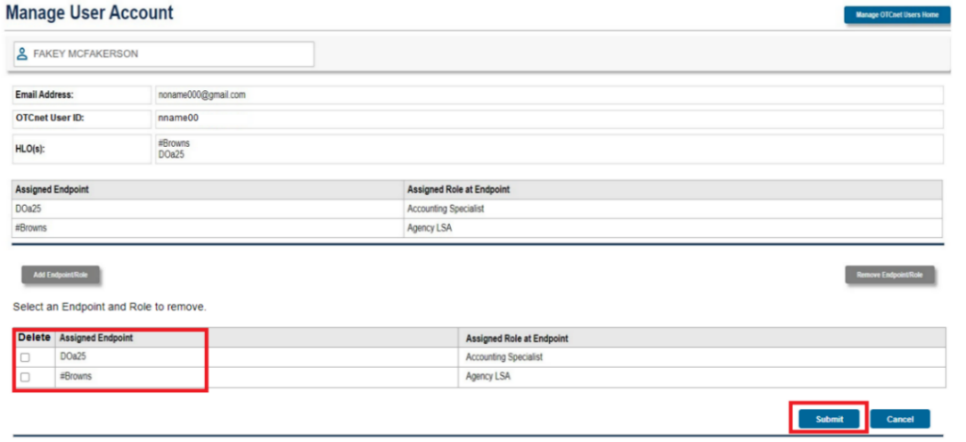
Application Tip



You can select multiple **checkboxes** to remove multiple assigned endpoints/roles.

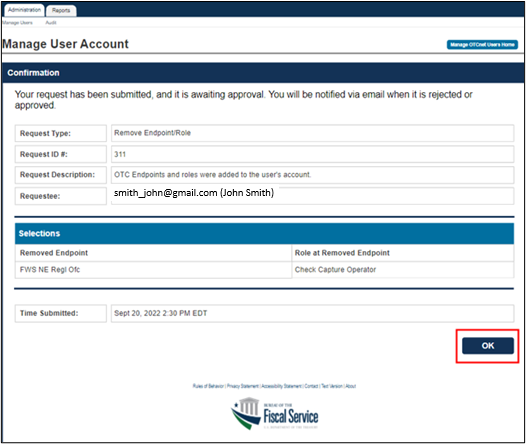
1. Then select the **Submit** button to submit your request.

Figure 21: Select an Endpoint and Role to Remove Screen



1. The confirmation page appears as shown in Figure 22.
2. Select the **OK** button to return to the **Manage OTCnet Users** screen.

Figure 22: Confirmation Screen on Removing Endpoint/Role Request Submitted



Application Tips



* You will be notified via email when the request is approved or rejected by another PLSA/LSA.
* When a role is successfully removed it is logged in the **Audit log**.

## Topic 7 Approving or Rejecting an Endpoint/Role (or the Removal of an Endpoint/Role)

In OTCnet, approvers are determined based on the **endpoint** selections.

* An access request is sent to all **PLSAs** and **LSAs** at the same level or above the selected endpoints within the same hierarchy.
* An approver logs in and approves (or rejects) the submitted request.

As a **PLSA** or **LSA** you are authorized to approve or reject an endpoint/role (or to remove an endpoint/role) for an OTCnet user. You can approve or reject a request *after* another **PLSA** or **LSA** within the same OTC endpoint or hierarchy generates the request (adds or removes an endpoint/role for a user in OTCnet).

After the request is approved, the user to whom the OTCnet request applies receives an email notification containing information about the approval of the request. If you reject the request, the **PLSA** or **LSA** who created the request receives a notification of the rejection.

For **new users** who have not logged in to OTCnet yet, both the **User Name** and **User ID** values will be empty in the database and displayed as blank values on the screen.

### Approve or Reject an Endpoint/Role (or the Removal of an Endpoint/Role)

To approve or reject an endpoint/role, log in to OTCnet and select **Administration>Manage Users>Manage OTCnet Users** from the home page**.** You will notice your **Pending Requests** list. Select the **View Details** link to view a specific request. Review the read-only information and enter any approval or rejection comments in the **Approver Comments** field. Select the **Approve** or **Reject** button. Review the read-only information on the confirmation page and select **OK** to return to the **Manage OTCnet Users** page.

To approve or reject a **removal** of an endpoint/role, follow the same process and steps as for approving or rejecting an endpoint/rolerequest, starting with selecting the **View Details** link from the **Manage OTCnet Users** page for a **Remove Endpoint/Role** type of request.

Approve or Reject an Endpoint/Role (or the Removal of an Endpoint/Role)

To approve an endpoint/role for an OTCnet user, complete the following steps:

1. Log in to OTCnet and from the **Administration** tab**,** select **Manage Users,** and then **Manage OTCnet Users**.
2. From the **Manage OTCnet Users** screen, notice the **Pending Requests** list (**Your To-Do list**) as shown in Figure 23.

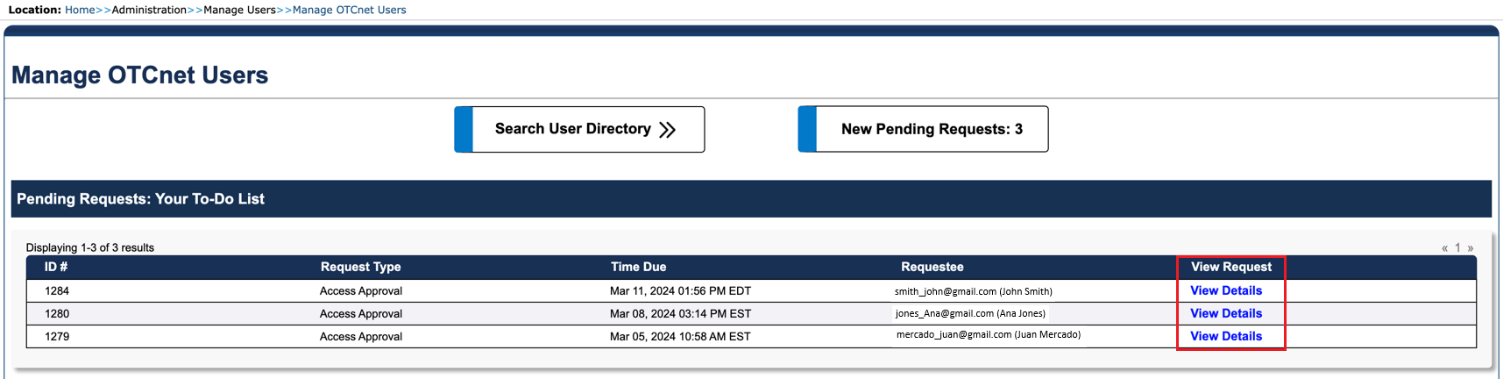
Application Tips



* You will receive an email notification regarding a new user provisioning request awaiting review when a provisioning request is made and added to your **pending requests list**, to alert you when a user needs your verification.
* For each request, notice the **Request Type**, **Time Due**, and **Requestee.**
* Notice two request types, for **Access Approval** and **Remove Endpoint/Role**. Each selection will take you to the appropriate workflow for access approval or access removal, respectively.

1. Select the **View Details** link for a specific **access approval** request.

Figure 23: Manage OTCnet Users Screen



1. The **Access Approval Request** screen displays as shown in Figure 24.
2. Review the read-only information and enter any approval or rejection comments in the **Approver Comments** field.

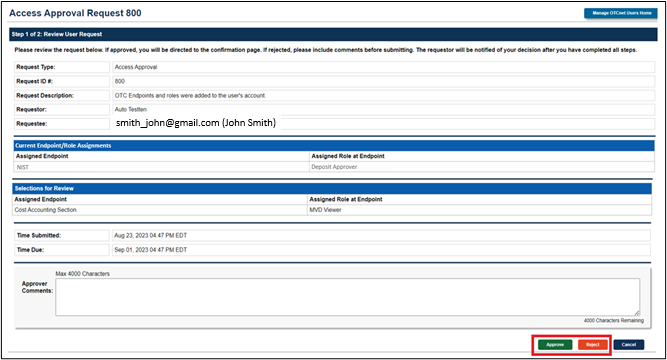
Application Tips



* If you reject the request, you **must** provide comments in the specified field. Otherwise, you will get an error message and will not be able to continue until you provide comments.
* You can enter a **maximum** amount of 4000 characters.

1. Select the **Approve** or **Reject** button.

Figure 24: Access Approval Request Screen



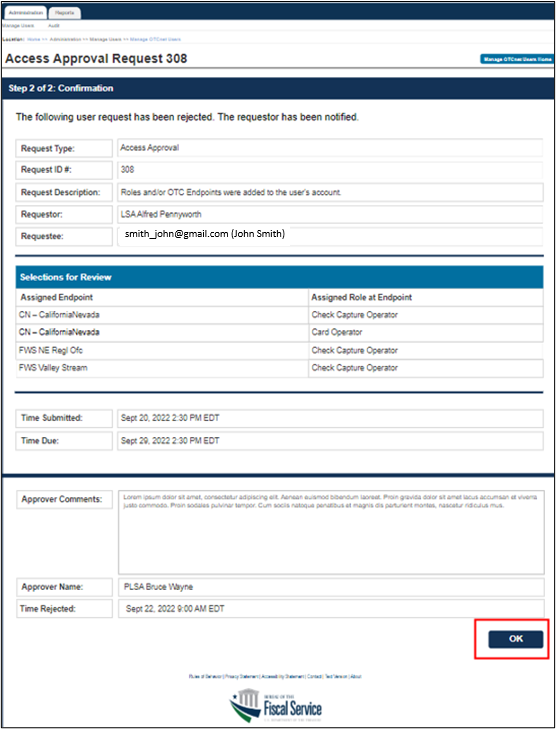
Application Tip



* Selecting **Cancel** will cancel the approval process.
* If you select **Reject**, you will get a notification: “Are you sure if you want to reject this request?” Select **Reject** or **Cancel**.

1. A confirmation page about the approval/rejection of the access request will display as shown in Figure 25.
2. Review the read-only information and select **OK** to return to the **Manage OTCnet Users** page.

Figure 25: Confirmation Screen on Approval/Rejection of the Access Request



Application Tip



Requestors will be notified via email when a request is approved or rejected.

Application Tip



* To approve or reject a **removal** of an endpoint/role, follow the same process and steps as for approving or rejecting an endpoint/role request.
* Start with selecting the **View Details** link from the **Manage OTCnet Users** page for a **Remove Endpoint/Role** request.

## Summary

In this chapter, you learned how to:

* Manage user accounts
* Create an identity for a user in SailPoint IIQ
* Add or remove user access in SailPoint IIQ
* Approve or deny user access requests in SailPoint IIQ
* Import a user identity to OTCnet
* Add or remove an endpoint/role for an OTCnet user
* Approve or reject an endpoint/role (or the removal of an endpoint/role) in OTCnet