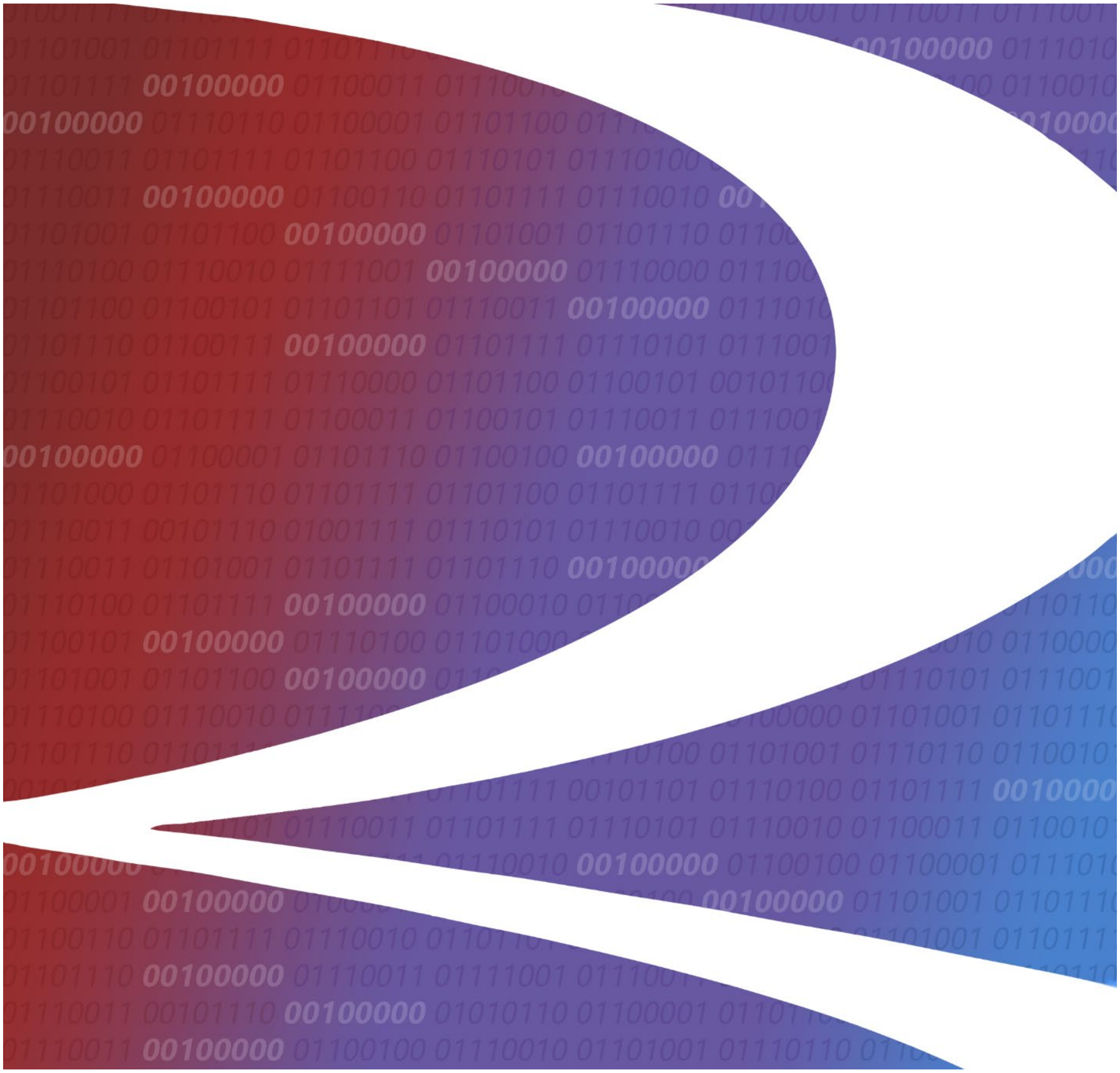


Single Sign-On and Launch Pad Administrator Guide

Last Updated: January 2021

Table of Contents

List of Exhibits

Using Single Sign-On and the Launch Pad for Company Admin Tasks

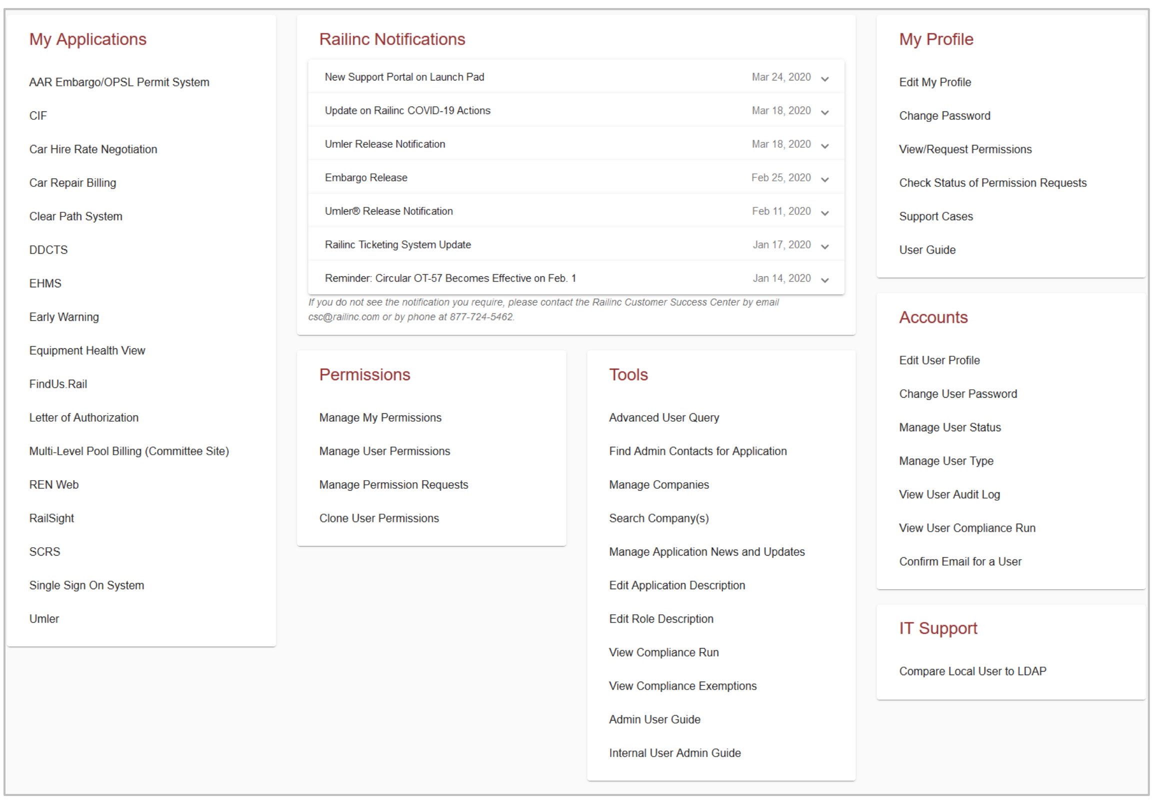
The Single Sign-On (SSO) system enables Railinc users to register for Railinc access, manage their user profile, and request and access Railinc applications. These functions are described in the *Railinc Single Sign-On User Guide*.

If you are a *company administrator* for a Railinc application, you have access to additional Permissions and Tools tasks, which are listed in the Administrator functions of the Launch Pad (Exhibit 1). This Administrator Guide describes these administrator tasks.

Your authorized tasks and applications can be accessed from the **Launch Pad**. To access the **Launch Pad**, enter the following link in your browser:

https://www.railinc.com/rsso/ Log in at the prompt.

Exhibit 1. Launch Pad (Company Admin)



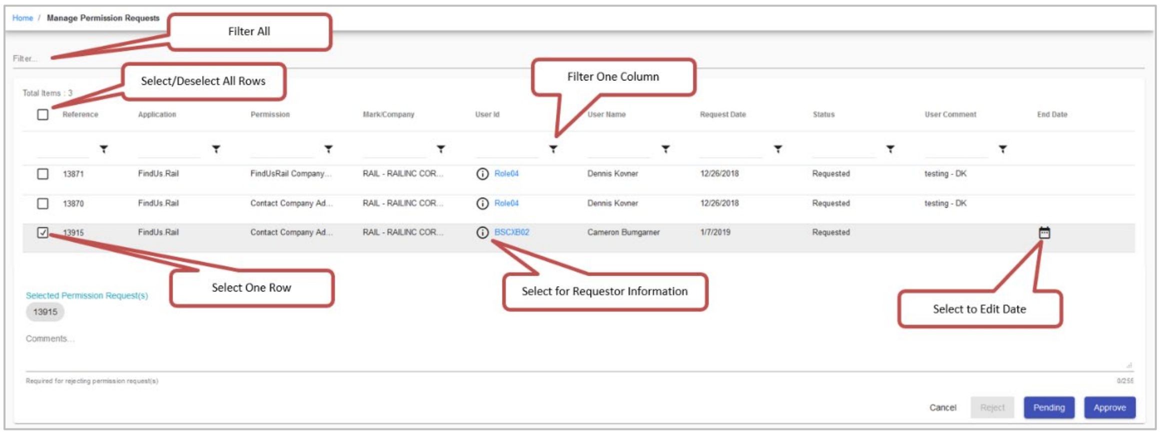
Approving and Rejecting Permission Requests

The company administrator is responsible for responding to requests for access to a specific application. The following sections describe how to approve or reject application access requests.

Individual Requests

1. Log into SSO as described in the *Railinc Single Sign-On User Guide*. The **Launch Pad** is displayed.
2. Select **Manage Permission Requests** in the **Permissions** portlet. The **Manage Permission Requests** page is displayed (see Exhibit 2).

Exhibit 2. Manage Permission Requests



3. Review the requests:

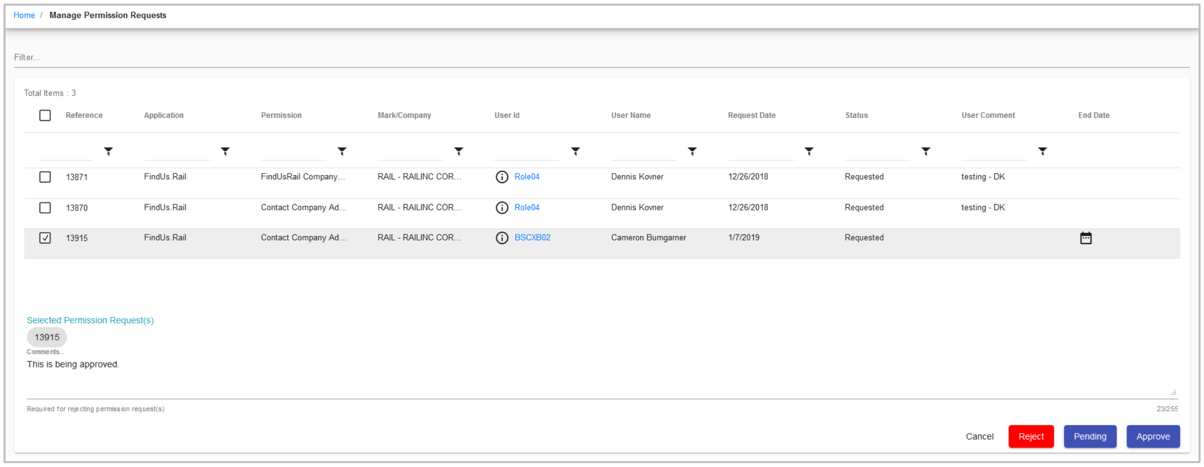
   a. As needed, select the user ID hyperlink to open the Manage User Permissions function (see Managing User Permissions).

   b. As needed, select the information icon ( ) to open a pop-up window with SSO user information about the requester. Click outside the pop-up window to return to the **Manage Permissions Requests** page.

   c. Read the **User Comments** the requester might have written to clarify the need for access.

4. To approve or reject individual requests, select the checkbox to the left of the request. To approve or reject all requests, select the checkbox at the top of the form.
5. To reject one or more requests, enter **Comments** explaining why the request is being rejected. The **Reject** button becomes available once a comment has been entered.
6. (Optional) For approvals, you have the option to use the calendar icon ( ) to add an **End Date** for access as appropriate. The start date begins the day the request is approved.
7. (Optional) Enter **Comments** as appropriate (see Exhibit 3 for an example). This entry is included in the notification email.

Exhibit 3. Manage Permission Requests Example for Approve/Reject



8. Select one of the following options:

   Approve—Approves the request for the specified period, sends an approval email to the user, and makes the application link available on the user's Launch Pad. Request status is set to **Approved**.

   Reject—Rejects the request, sends a rejection email to the user. The application link is NOT available on the user's Welcome page and the request status is set to **Rejected**.

   Pending—Pends the request, sends an email to the user. The application link is NOT available on the user's Welcome page. Use Pending when a determination about the access cannot be made without further investigation or information. The request status is set to **Pending**.

   Cancel—Returns to the **Launch Pad** (Exhibit 1). The request status is **Cancelled**.

Note: Requests that have been approved or rejected are removed from the **Manage Permission Requests** page. Those that are **Pending** remain in the list.

Managing User Permissions

The Manage User Permissions function enables the company administrator to grant access that has not officially been requested. You can use this function to quickly grant application accesses to new personnel whose SSO access has been established. You can also quickly remove access when it is no longer needed.

Adding a Permission

1. Log into SSO as described in the *Railinc Single Sign-On User Guide*. The **Launch Pad** is displayed.

2. Select **Manage User Permissions** in the **Permissions** portlet. The **User Search** page is displayed (Exhibit 4).

Exhibit 4. User Search

3. There are multiple ways to search for users to manage their permissions:

   a. Enter the **User ID** and select **Search**.

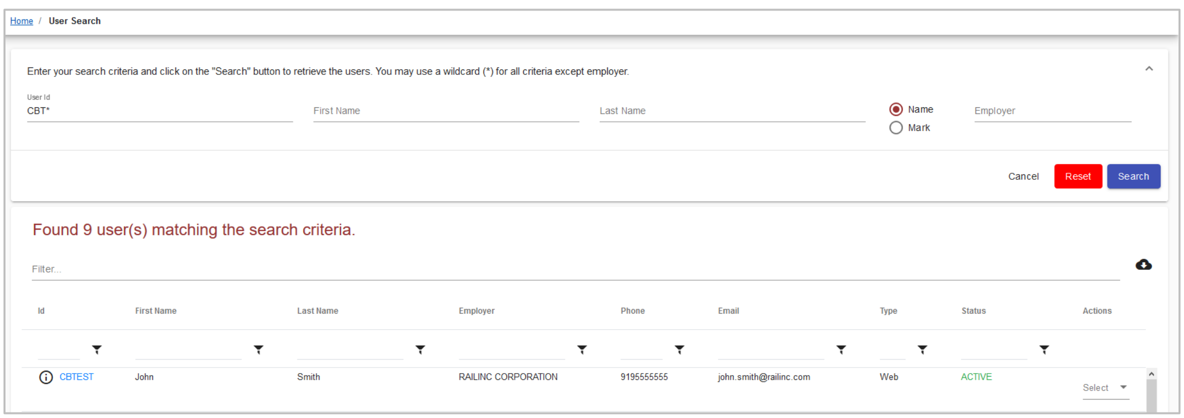
   b. Begin entering the **User ID** and select the appropriate ID from the drop-down list and select **Search**.

   c. Enter part of the **User ID**, **First Name** or **Last Name** using asterisk (*) for a wildcard and select **Search** (see Exhibit 5).

Note: Select the arrow (˅) in the top right corner to view or hide your search criteria.

4. Select **Search**. Results are listed in the table.

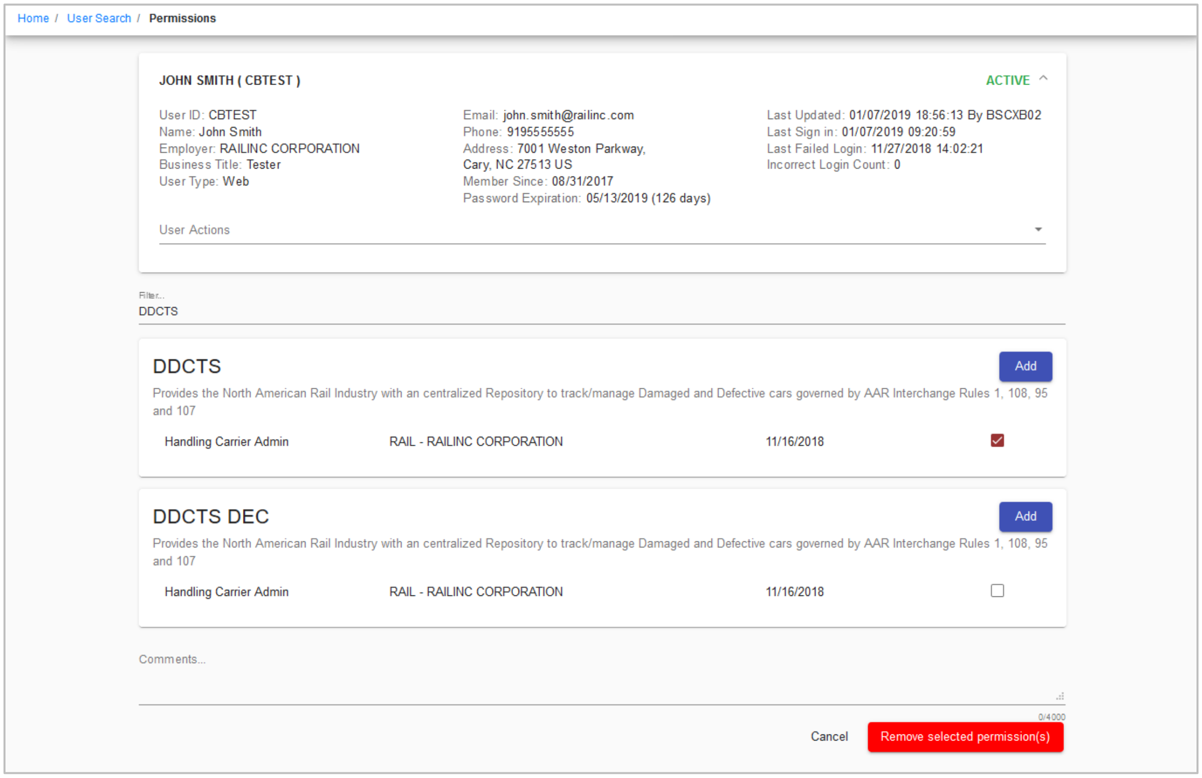
Exhibit 5. User Search with Criteria and Results



Note: If the first name begins with Eve, enter **eve*** in the field for the query. Case is ignored. Enter ***eve*** to show users named Steve, Beverly, or other names that contain **eve**. You can use wildcards for partially-known fields, or when internal characters are unknown. For example, typing **joh*ns*on** finds Johnson, Johanson, Johansson, and Johnston.

5. Select the link of the desired **User ID**. Links are available only for active user IDs. The user's **Permissions** page is displayed (see Exhibit 6).

Exhibit 6. Permissions



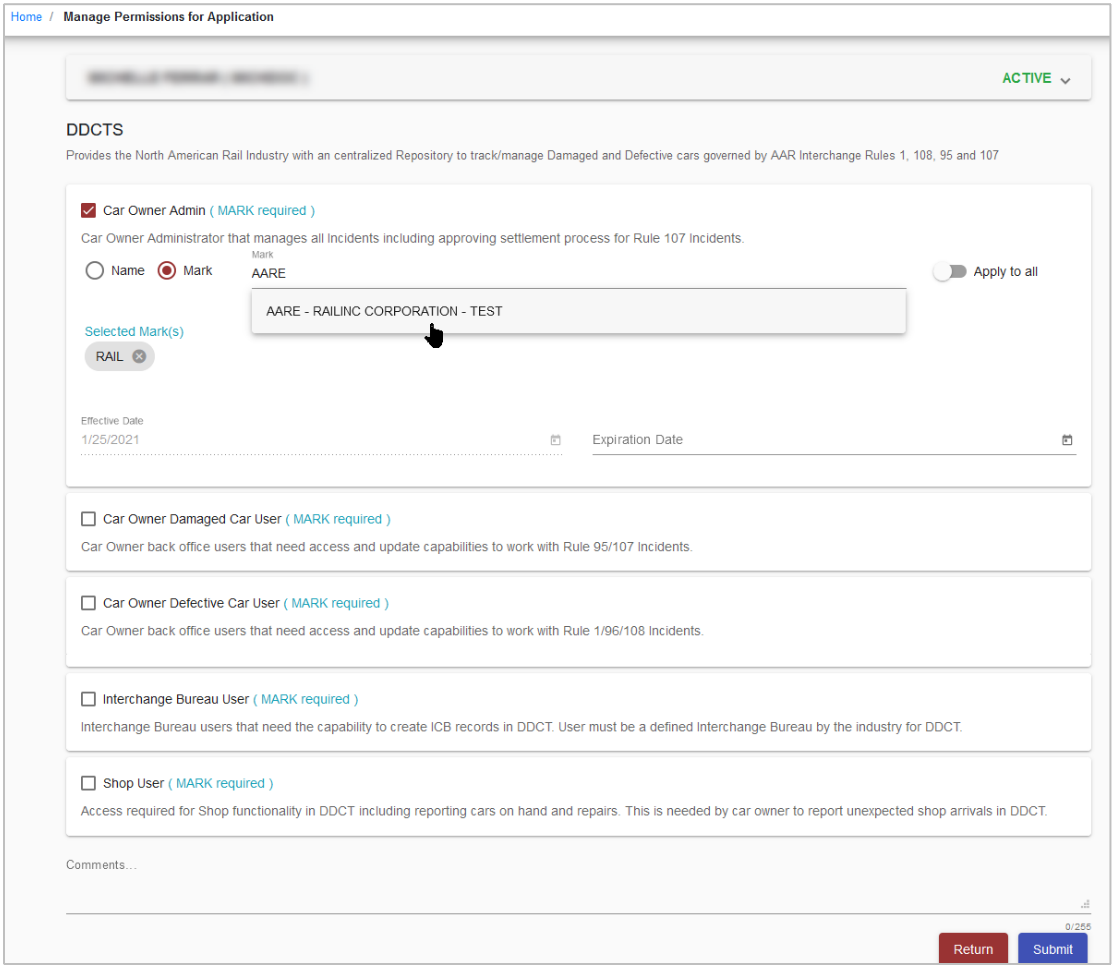
Note: The only applications listed on this page are those the administrator is authorized to administer.

6. Select **Add**. The **Manage Permissions for Application** page is displayed (Exhibit 7).

7. Select the checkboxes for the appropriate roles.

8. If required, select the appropriate **Name** or **Mark** (Company ID). Multiple marks can be entered and selected one at a time, so that they appear in the **Selected Mark(s)** section.

Exhibit 7. Manage Permissions for Application



9. Click **Apply to All** to apply the Name or Mark(s) to all selected roles.

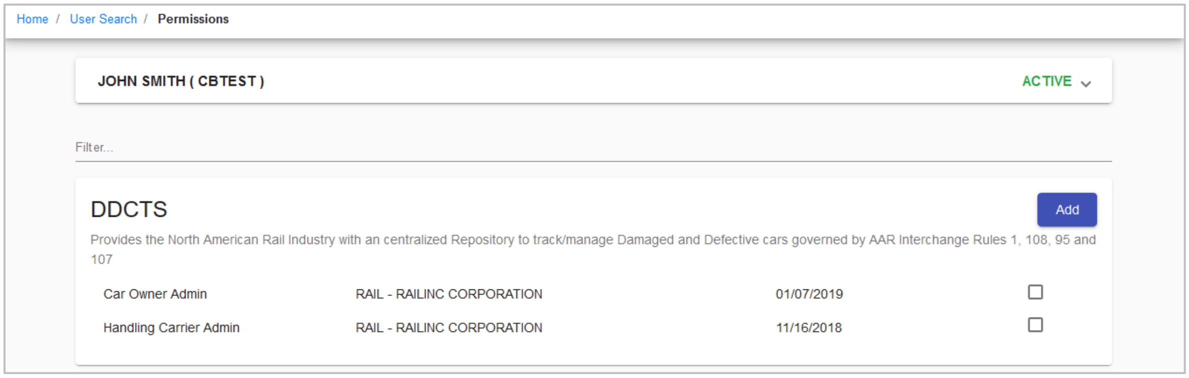
10. Enter or use the calendar icon to select the **Effective Date** and **Expiration Date**. The default **Effective Date** is today. You have the option to leave the **Expiration Date** field blank or enter it as needed.

11. Scroll to the bottom of the page.

12. (Optional) Enter **Comments**.

13. Select **Submit**. The **Permissions** page is redisplayed with the added permission (Exhibit 8).

Exhibit 8. Permissions Example of Added Role



14. If other listed application permissions are needed, select **Add** to repeat the process.

15. Otherwise, select **Cancel**. The **Launch Pad** is displayed (Exhibit 1).

Removing a Permission

This function enables an administrator to remove access for a specified user ID. To remove application access:

1. Log into SSO as described in the *Railinc Single Sign-On User Guide*. The **Launch Pad** is displayed.

2. Select **Manage User Permissions** in the **Permissions** portlet.

   The **User Search** page is displayed (Exhibit 4).

3. There are multiple ways to search for users to manage their permissions:

   a. Enter the **User ID** and select **Search**.

   b. Begin entering the **User ID** and select the appropriate ID from the drop-down list and select **Search**.

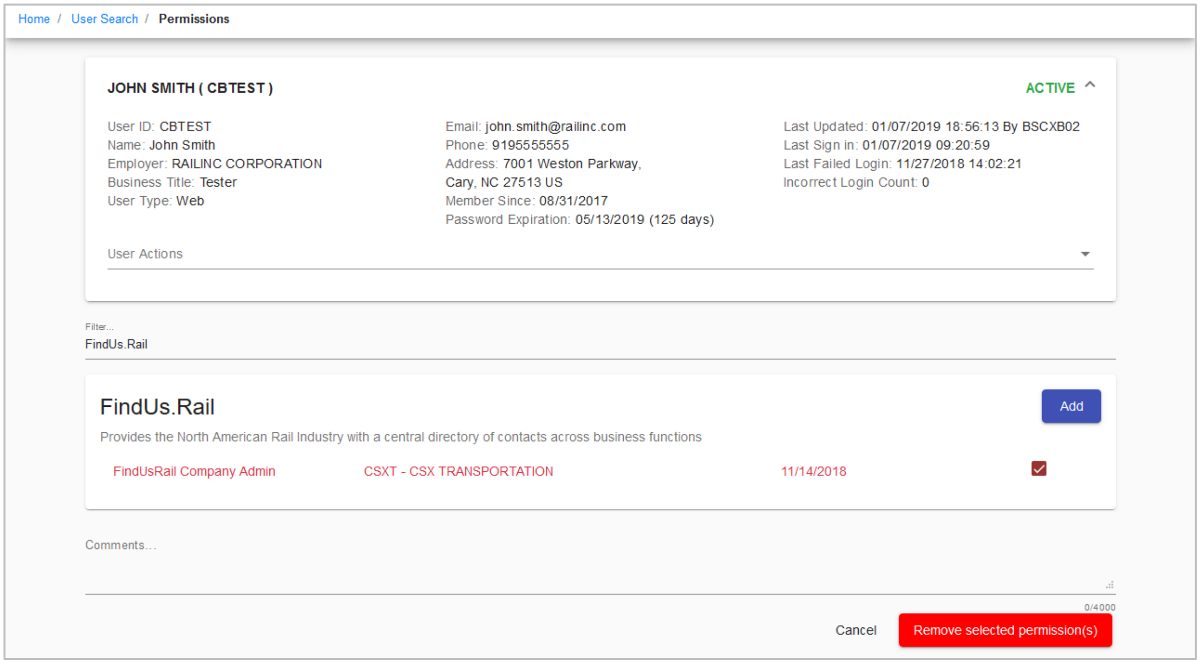
   c. Enter part of the **User ID**, **First Name** or **Last Name** using asterisk (*) for a wildcard and select **Search** (Exhibit 5).

Note: Select the arrow ( ) in the top right corner to view or hide your search criteria.

4. Select **Search**. Results are listed in the table (Exhibit 5).

5. The **Permissions** page is displayed (Exhibit 9).

Exhibit 9. Remove Permissions



6. Scroll to the permission/role to be removed and select the checkbox to the right of the specific permissions to be removed.

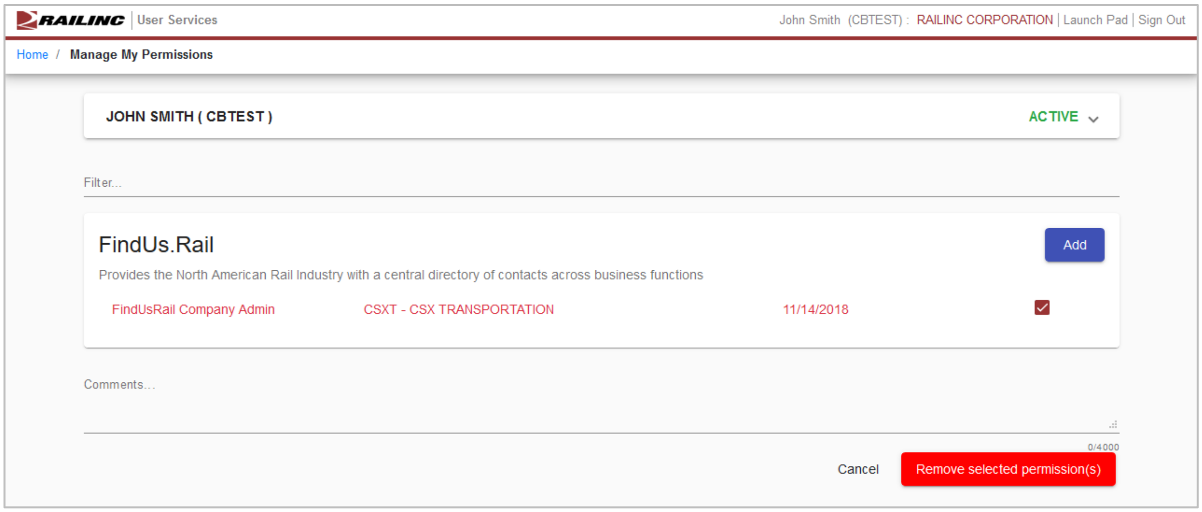
7. Select **Remove Selected Permission(s)** at the bottom of the page. The **Permissions** page is redisplayed showing only the remaining permissions.

8. Select **Cancel** to return to the **Launch Pad** (Exhibit 1).

Managing Your Own Permissions

An administrator can manage their own personal permissions for authorized applications. When an administrator selects **Manage My Permissions**, the **Manage My Permissions** page is displayed (Exhibit 10).

Exhibit 10. Manage My Permissions



The administrator can add or remove permissions as described in the previous sections. Unauthorized applications must be requested by selecting **View/Request Permissions** as described in the *Railinc Single Sign-On User Guide*.

Select **Cancel** when finished with permission. The **Launch Pad** is displayed (Exhibit 1).

Performing an Advanced User Query

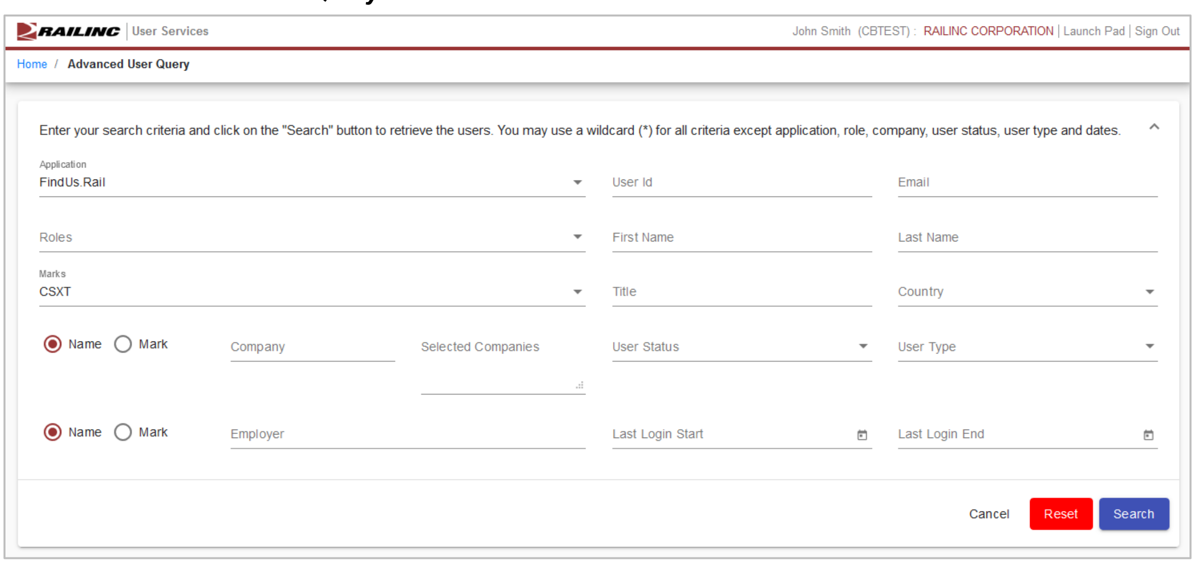
The **Advanced User Query** enables company administrators to locate specific users of specific applications. Criteria can include:

- Application
- Roles
- User ID
- Email
- First Name/Last Name
- Title
- Country
- User Status (active, inactive, etc.)
- User Type
- Name/Mark (company for specific Roles)
- Mark
- Company
- Employer
- Last Login Start Date
- Last Login End Date

To find a user using a query:

1. Log into SSO as described in the *Railinc Single Sign-On User Guide*. The **Launch Pad** is displayed.
2. Select **Advanced User Query** in the **Tools** portlet. The **Advanced User Query** page is displayed (Exhibit 11).

Exhibit 11. Advanced User Query



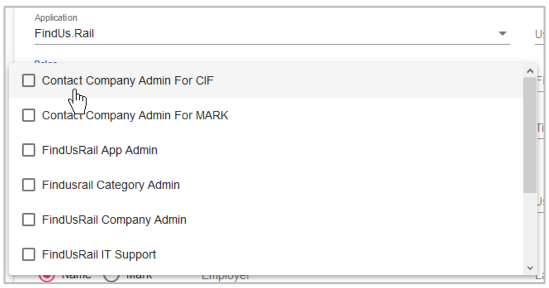
Hint: At least ***one*** criteria must be specified to produce a successful search. Always use the minimum, optimal criteria for efficient searches. First and last names together generally produce a short results list (unless the last name is common–like Smith). Other unique criteria include user IDs. Specifying too many criteria can result in no match found. Use asterisks (*) as wildcards to overcome spelling variations. For example, entering *JOHNS*N* finds the names Johnson, Johnsen, Johnston, Johnsten, etc.

3. Select the **Application** for the user from the drop-down.

Note: If the administrator has only one authorized application, then only one application will appear in the drop-down list.

The **Roles** drop-down list populates with applicable roles (Exhibit 12) for the application selected.

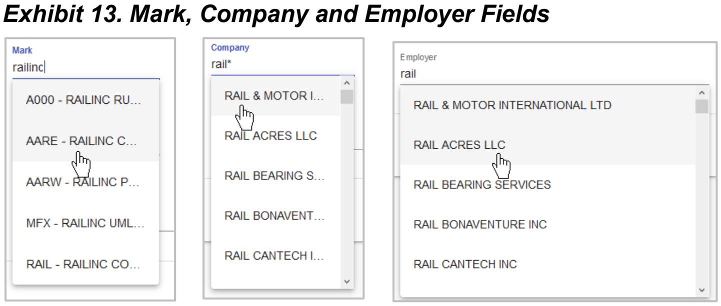
Exhibit 12. Application Selected (with Roles drop-down list displayed)



4. Select one or more **Roles** for the user by clicking inside more than one checkbox. Click again to unselect.
5. Begin entering a **Mark** and a drop-down list appears with possible selections to choose from. One or more marks can be selected and will appear to the right of the field. Entries can be removed by deleting them from **Selected Marks**.
6. Begin entering a **Company** and a drop-down list appears with possible selections to choose from. One or more companies can be selected and will appear to the right of the field. Entries can be removed by deleting them from **Selected Companies**.
7. Begin entering an **Employer** and a drop-down list appears with possible selections to choose from. Entry can be removed from the **Employer** field at any time.

Note: The **Mark** and **Company** fields are the mark and the name of the company for which the user is authorized to act, not necessarily the user's employer. **Employer** is the user's employer as shown in their User Profile.

Exhibit 13. Mark, Company and Employer Fields



8. Enter the **User ID**, **Email**, **First Name**, **Last Name** and **Title** fields as appropriate to add them to the query. Remove entries by deleting them.

> **Note:** Use an asterisk (*) as a wildcard for a partially-known field. For example, if the first name begins with Nel, type nel* in the field for the query. Case is ignored. Surrounding the string with asterisks on both sides is recommended for internal strings. Date fields ***cannot*** have wildcards.

9. Select **Country** from the drop-down list.

10. Select **User Status** from the drop-down list by clicking inside the checkbox(es). If no status is specified, all statuses are used as the default. Valid values for status include:
    - Active
    - Non-Recoverable (cannot be activated; must be recreated)
    - Hard Locked
    - Inactive
    - Password Expired
    - Locked
    - Suspended

11. Select **User Type** from the drop-down list. Valid values for type include:
    - System User
    - Web User
    - Ghost User

12. Enter the **Last Login Start** and **Last Login End** dates in the MM/DD/YYYY format or click the calendar ( ) icon to select dates.

13. When you have specified one or more search criteria, select **Search**. The **Advanced User Query** page redisplays with a table of search results. See Viewing Query Search Results. If no users are found, remove some of the search criteria and search again.

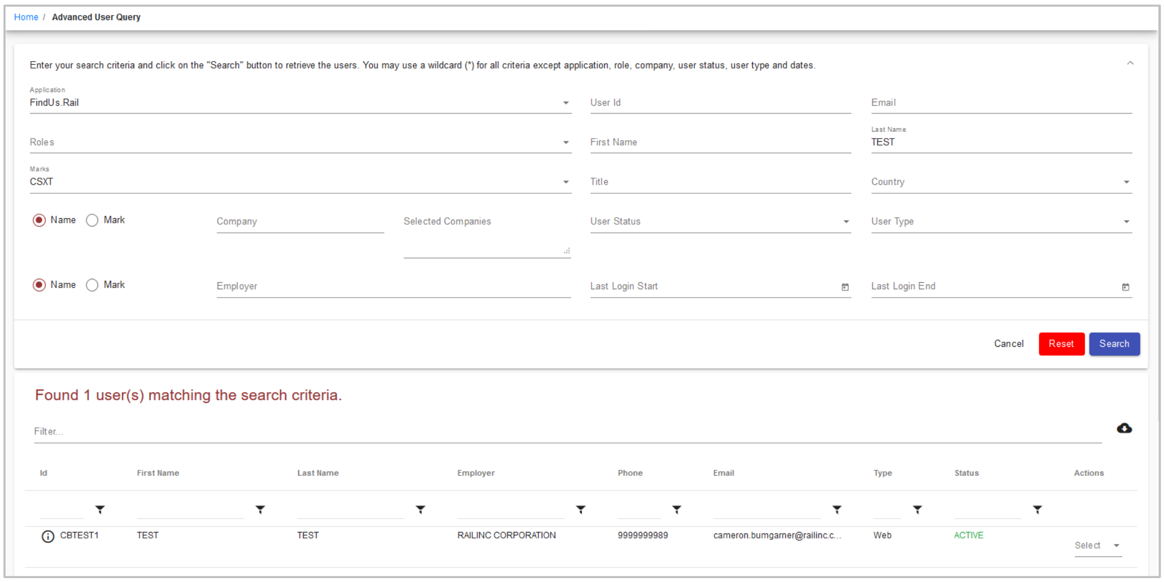
Viewing Query Search Results

When you execute a successful user search, the results are displayed in a table at the bottom of the **Advanced User Query** page. The following sections show samples of various types of queries and a detailed description of the Search Results table navigation and tasks.

Performing a Simple Last Name Query

The query in Exhibit 14 shows how to find users with the last name of "TEST".

Exhibit 14. Last Name Only Query Results



In this example, only one user has the last name of TEST. For a description of the search results table, see Working with Search Results.

From the **Select** drop-down in the **Actions** column of the table, select **Manage Permissions** to see all the selected user's active permissions on the **Manage Permissions** page.

Exhibit 15. Select Manage User Permissions in Actions Column

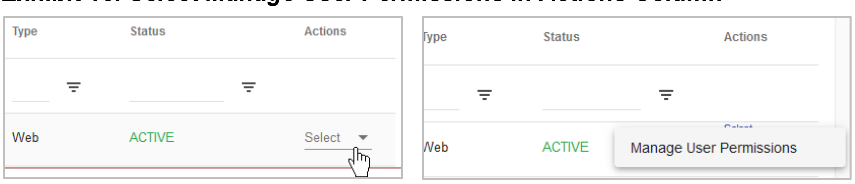
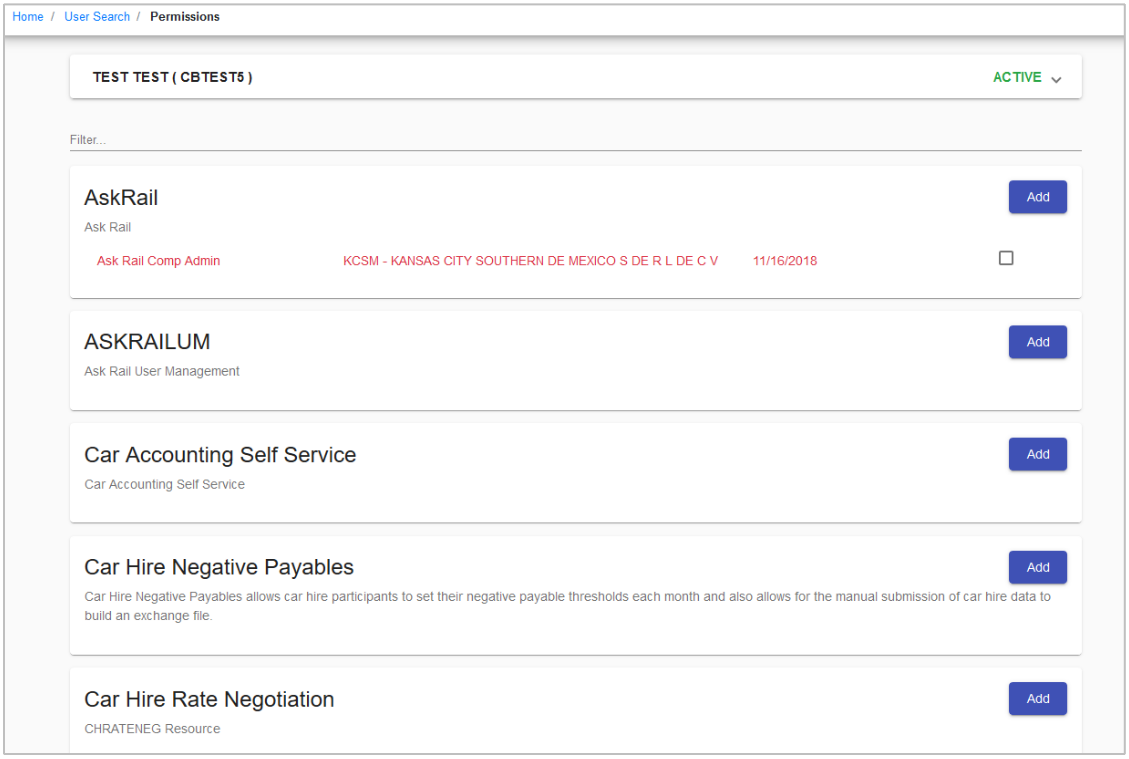


Exhibit 16. Manage Permissions



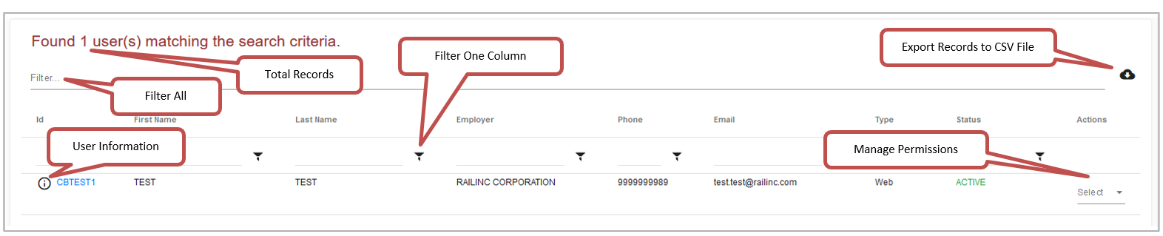
The same user with the last name of "TEST" is shown with all active permissions. For a description of the search results table, see Working with Search Results.

Working with Search Results

The search results table is a fixed size and has a scroll bar at the right for viewing records. Each results record is divided by a horizontal line.

Tables are sorted by selecting the links in the table headings. The default sort is by **User ID**. Move columns around by dragging the header of a column to a new place.

Exhibit 17. Search Results

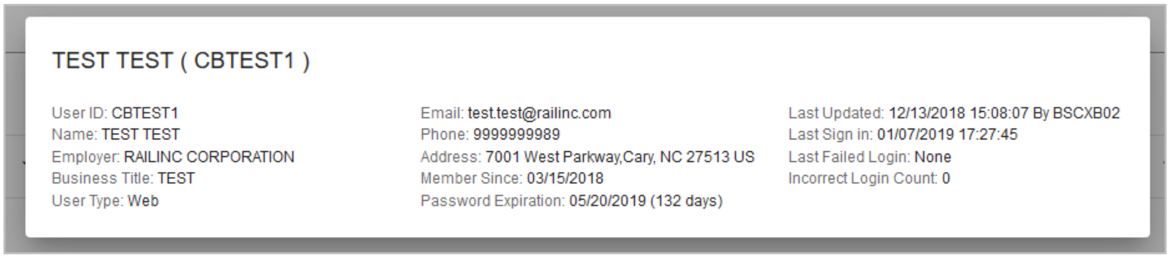


Select the cloud ( ) icon at the upper right to export the query results to a comma separated value (CSV) file that can be opened in Microsoft Excel for printing.

In the Actions column, click **Select** and **Manage Permissions** to view the available user actions. For company administrators, the only available user action is **Manage User Permissions**. See Managing User Permissions for more information.

Select the information icon (ⓘ) to open a view only pop-up window with the user's **User Profile** (see Exhibit 18). Click outside the window to close it when finished viewing.

Exhibit 18. User Information



Finding Administrator Contacts for Applications

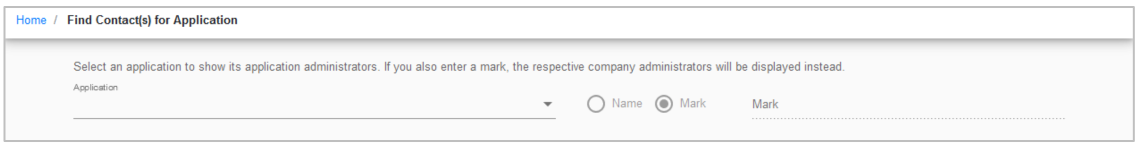
The **Find Admin Contacts for Application** function enables administrators to determine who is an administrator for specific Railinc applications.

1. Log into SSO as described in the *Railinc Single Sign-On User Guide*. The **Launch Pad** is displayed.

2. Select **Find Admin Contacts for Application** in the **Tools** portlet.

   The **Find Contact(s) for Application** page is displayed (Exhibit 19).

Exhibit 19. Find Contact(s) for Application



3. Select an application from the **Application** drop-down list. Matches will appear below the selection. When no company is provided, only application administrators are displayed.

4. (Optional) Choose the **Name** or **Mark** radio button to search on the name or mark (company ID) and start entering a name or a mark in the **Mark** field. A drop-down list matching your entry appears. Select a Mark from the list. Matches will appear below the selection. When a company is provided, only company administrators are displayed.

5. The **Find Contact(s) for Application** page is redisplayed with a list of administrators:

   - Exhibit 20 shows Railinc application administrators only. No company was specified in the search.

   - Exhibit 21 shows results when a Company ID is added to the search. The list shows administrators for the RAIL company.

   Information shown includes phone numbers and email addresses for the administrator contacts. Tables are sorted by selecting the links in the table headings.

Exhibit 20. Find Contact(s) for Application (with AskRail Application Administrators

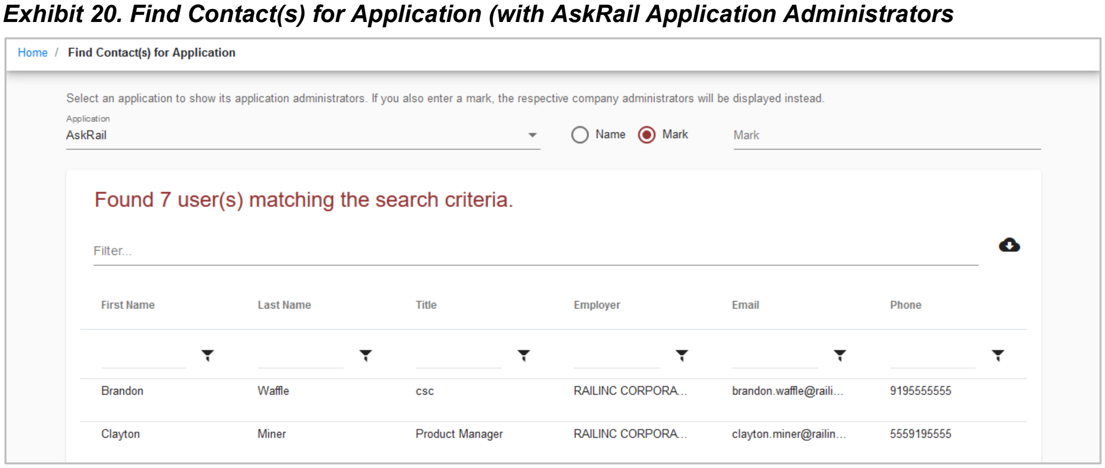
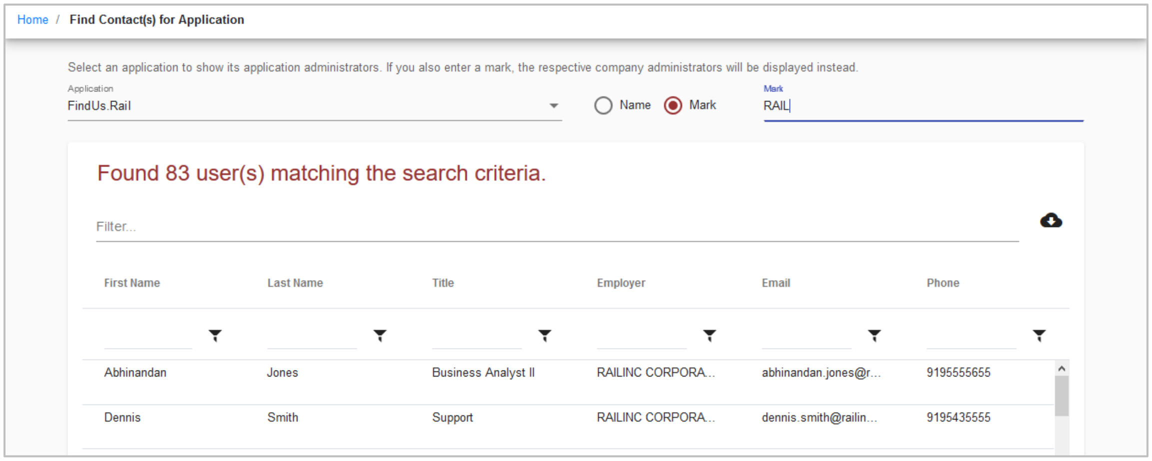


Exhibit 21. Find Contact(s) for Application (with Company Administrators)



Viewing the SSO and Launch Pad Admin User Guide

Select the **Admin User Guide** link to open the *SSO and Launch Pad Administrator Guide* in a new tab or window.

Index