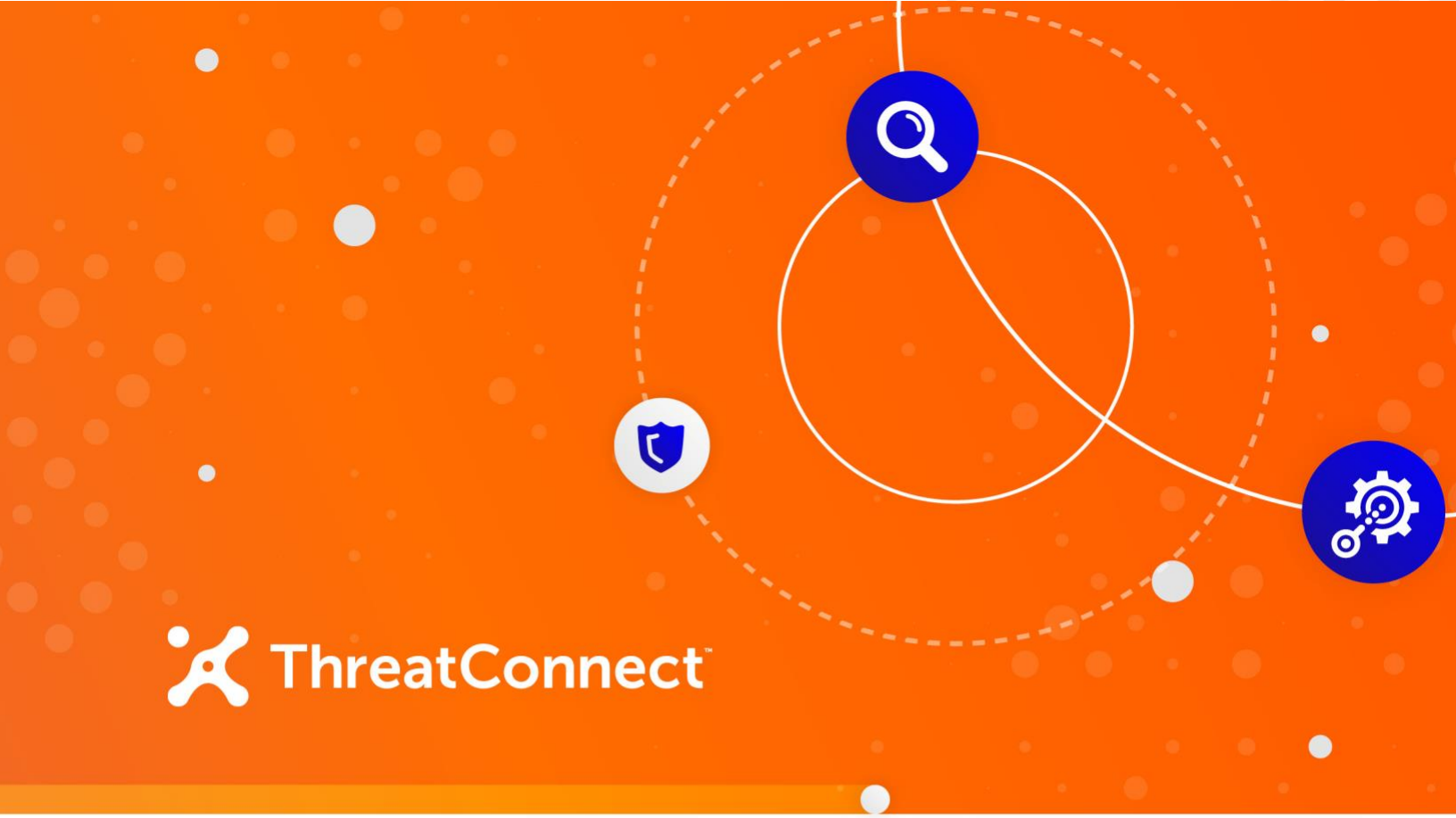

Security Features in ThreatConnect® Risk Quantifier

Administration Guide

Document Version 1.0

February 9, 2022

10025-01 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203
P: 1.800.965.2708 | F: 1.703.229.4489
www.ThreatConnect.com

Table of Contents

Overview

This document describes the main administrative and configuration-related security features of the ThreatConnect Risk Quantifier (RQ) platform. Administrators are recommended to review and set the configurable features in accordance with their organization's information security policies and guidelines.

Terms and Definitions

The following terms are used throughout the RQ platform:

- **Legal Entity**: A Legal Entity is an organization or business unit of a company for which risk data are being quantified in the RQ platform.
- **Enterprise**: The Enterprise level of an RQ instance provides access to multiple Legal Entities belonging to a company.
- **Portfolio**: Similar to an Enterprise, a portfolio contains information on all Legal Entities belonging to a company.
- **FAIR™**: Short for Factor Analysis of Information Risk, FAIR is a standard quantitative risk analysis model for information and operational risk.

Role-Based User Access

The RQ platform requires assignment of role-based access to users when creating user accounts so that least-necessary privilege can be provided to each user.

A user's role determines the capabilities and permissions that the user has in the RQ platform at the Enterprise level or within a Legal Entity. Table 1 defines the seven user roles from which administrators can select when creating user accounts. These roles may not be customized, and new user roles may not be created.

Table 1

User Role	Definition
RQ Enterprise Administrator	An **RQ Enterprise Administrator** has full administrative and editorial access over the Enterprise and within all Legal Entities in the Enterprise.
RQ Enterprise Read Only	An **RQ Enterprise Read Only** user has read-only access over the Enterprise. This role has no Legal Entity–level access.
RQ Pro Administrator	An **RQ Pro Administrator** has full administrative and editorial access within one or more Legal Entities. This role has no Enterprise-level access.
RQ Pro Editor	An **RQ Pro Editor** has full editorial, but no administrative, access within one or more Legal Entities. This role has no Enterprise-level access.
RQ Pro Read Only	An **RQ Pro Read Only** user has read-only access within one or more Legal Entities. This role has no Enterprise-level access.
RQ Fair Only	An **RQ Fair Only** user has read-only access within one or more Legal Entities, as well as the ability to run FAIR and semi-automated FAIR What If scenarios within those Legal Entities. This role has no Enterprise-level access.
RQ Export API	An **RQ Export API** user can only use API calls to retrieve information on one or more Legal Entities from the RQ platform. This role has no user interface (UI) access or Enterprise-level access.

Enterprise Level

The only user roles with Enterprise-level access are RQ Enterprise Administrator and RQ Enterprise Read Only. Table 2 defines the specific capabilities that users with the RQ Enterprise Administrator or RQ Enterprise Read Only role have on the **Portfolio Analysis** screen.

Table 2

User Role	View Portfolio Analysis	Edit Implementation Cost
RQ Enterprise Administrator	✓	✓
RQ Enterprise Read Only	✓	

NOTE: *Implementation Cost* ***is displayed in the table on the*** *Controls detailed list* ***card on the*** *Portfolio Analysis* ***screen.***

Table 3 defines the specific capabilities that users with the RQ Enterprise Administrator or RQ Enterprise Read Only role have on the **Legal Entities** screen.

Table 3

User Role	Create Legal Entity	Archive Legal Entity	Edit Legal Entity	Access Legal Entity
RQ Enterprise Administrator	✓	✓	✓	✓
RQ Enterprise Read Only				

NOTE: RQ Enterprise Read Only users may view the *Legal Entities* ***screen, but cannot make any changes to the Legal Entities in the Enterprise or access any of the Legal Entities from the screen.***

Table 4 defines the specific capabilities that users with the RQ Enterprise Administrator or RQ Enterprise Read Only role have on the **Data Export** screen.

Table 4

User Role	Export Data to CSV
RQ Enterprise Administrator	✓
RQ Enterprise Read Only	✓

Table 5 defines the specific capabilities that users with the RQ Enterprise Administrator or RQ Enterprise Read Only role have on the **Settings** screen.

Table 5

User Role	User Management				Preferences		Activity Log
	Create User	Edit Account	Reset Password	Deactivate/ Reactivate User	View	Edit	View
RQ Enterprise Administrator	✓	✓	✓	✓	✓	✓	✓
RQ Enterprise Read Only		✓	✓				

NOTE: RQ Enterprise Administrators may not edit the RQ instance administrator account (rq@threatconnect.com), reset the RQ instance administrator account's password, or deactivate the RQ instance administrator account.

NOTE: RQ Enterprise Read Only users will not be able to view other users on the** User Management **screen. They will see only their own account listed in the table. They may edit their own user name (by clicking** Edit Account**) and reset their own password.

Legal Entity Level

Table 6 defines the specific capabilities that all user roles have in the following areas of the RQ platform:

- **Risk Analysis**: screens for all options under the **Risk Analysis** menu
- **Configuration**: screens for all **Setup** options on the **Configuration** screen
- **Reports**: screen for the **Reports** menu
- **What If**: screen for the **What If** menu
- **Data Export**: screen for the **Data Export** menu

NOTE: The** Third Party **screen is not covered because its current functionality is only to provide a link to the** Configuration **screen.

NOTE: The RQ Export API user role is not covered because it has no UI access.

Table 6

User Role	Run Risk Analysis	All Configuration Setup Options	Generate Report	Build What If Analysis	Data Export to CSV
RQ Enterprise Administrator	✓	✓	✓	✓	
RQ Enterprise Read Only					
RQ Pro Administrator	✓	✓	✓	✓	✓
RQ Pro Editor	✓	✓	✓	✓	✓
RQ Pro Read Only		✓ (view only)	✓		
RQ Fair Only		✓ (view and edit **Legal Entity** and **Control Profiles** sections, including **Create Profile**)		✓	

Table 7 defines the specific capabilities that all user roles have on the **Settings** screen.

NOTE: The RQ Export API user role is not covered because it has no UI access.

Table 7

User Role	User Management				Model Tuning			Activity Log	Preferences		Model Insights
	Create User	Edit Account	Reset Password	Deactivate/ Reactivate User	View	Edit	Revert to Default	View	View	Edit	View
RQ Enterprise Administrator	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
RQ Enterprise Read Only											
RQ Pro Administrator	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
RQ Pro Editor					✔	✔	✔	✔	✔	✔	✔
RQ Pro Read Only					✔						✔
RQ Fair Only									✔	✔	

NOTE: All user types may view** License Details **information from the** Settings **screen.

NOTE: The RQ Pro Administrator is the only RQ Pro account that may view other users on the** User Management **screen. All other RQ Pro users will see only their own account listed in the table. They may edit their own user name (by clicking** Edit Account**) and reset their own password. RQ Fair Only users will see only their own account listed in the table and may edit their own user name, but may not reset their own password.

Single Sign-On via OAuth

The RQ platform can be configured to leverage the customer's enterprise identity provider for user authentication using Single Sign-On (SSO). SSO is enabled via the Open Authorization (OAuth) protocol. Customers can request the SSO setup by emailing success@threatconnect.com.

Once SSO has been configured, users may log in via a SSO button that is displayed at the bottom of the main login screen (Figure 1).

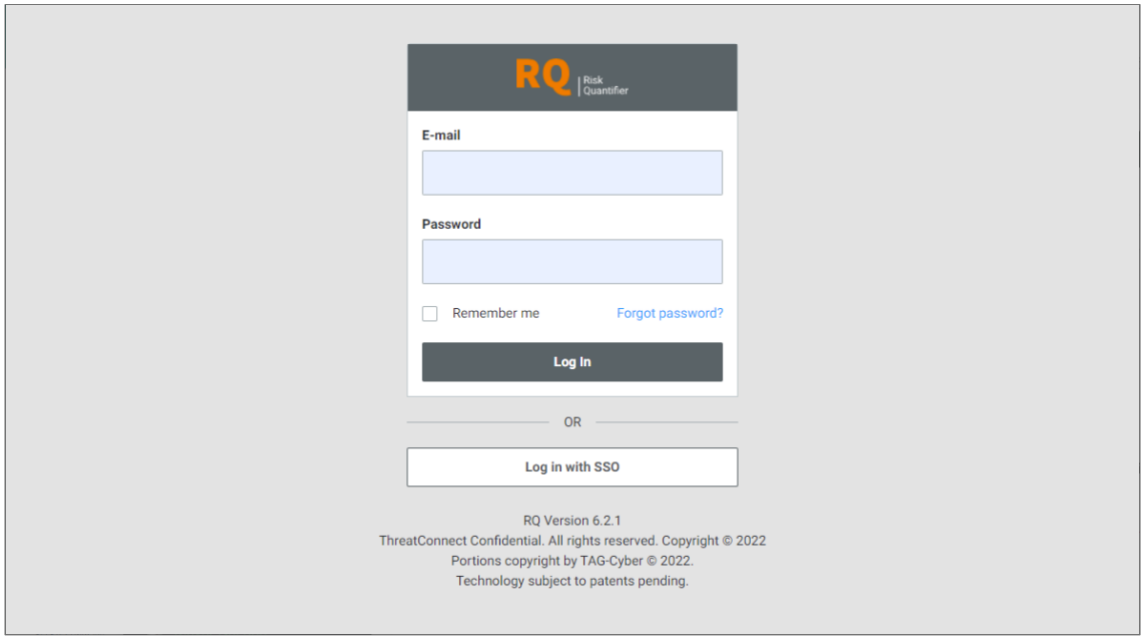

Figure 1

Currently, Ping Identity® and OKTA™ are the available methods for SSO.

Limiting Platform Access to IP Range

The customer instance of the RQ platform can be configured so that it can be accessed only from a range of specific IP addresses. To set up these limits, please open a ticket by emailing success@threatconnect.com.

Activation Link Email Expiration

When a user's RQ account is created, an email with a link to create their password is sent to the email address associated with their account. By default, the link included in the email expires after 60 minutes for security reasons. If a user clicks the link after 60 minutes have passed, they will be directed to an RQ screen with a message stating **Invalid or expired token**, and they will not be able to create their password (Figure 2).

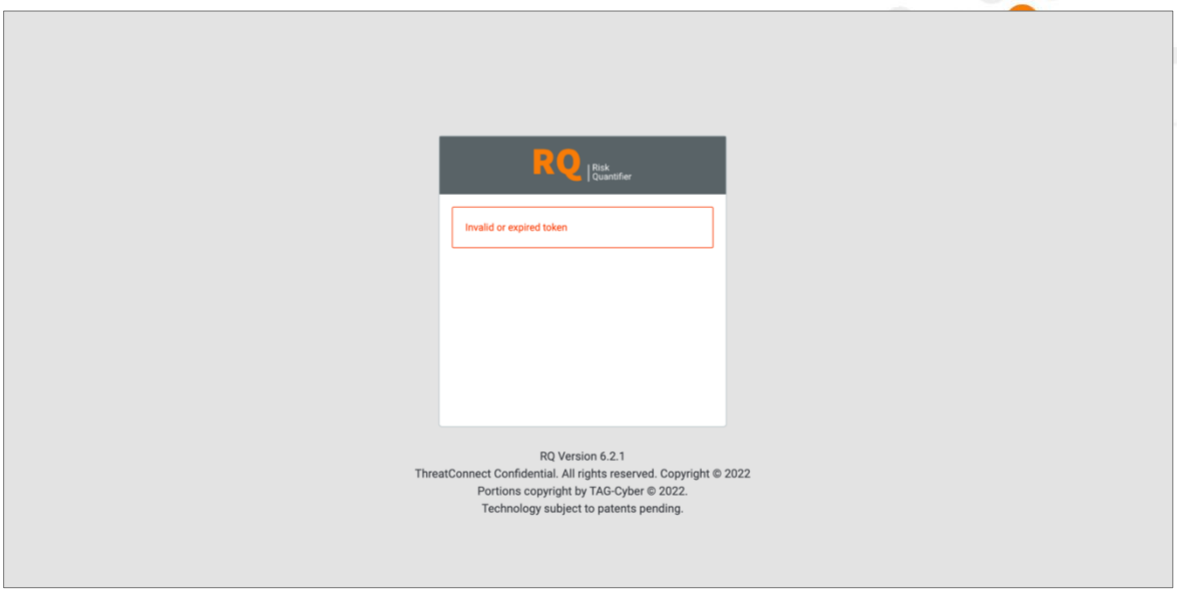

Figure 2

NOTE: The 60-minute time limit cannot be changed in the RQ interface. Administrators may request a change to this time limit by emailing success@threatconnect.com**.**

To reset the expired account, a user can go to the main login screen for their RQ instance and click the **Forgot password?** link (Figure 1). A new activation email will be sent to the user automatically. Alternatively, the user can ask their administrator to reset their password, which will result in a new activation email being sent.

Password Complexity Requirements

A user's RQ password must meet specific criteria, such as length and complexity. These criteria are not configurable and cannot be changed. Specifically, RQ passwords must meet the following criteria:

- Be between 8 and 64 characters long;
- Contain at least one uppercase letter;
- Contain at least one lowercase letter;
- Contain at least one number;
- Contain at least one special character;
- Not be a common password (e.g., 12345, abcde).

Users can view these criteria in two locations when resetting their password:

- In the password reset email they receive;
- On the RQ screen where they reset their password (Figure 3) by hovering over the **question mark** ⓘ icon to the right of the **New Password** label.

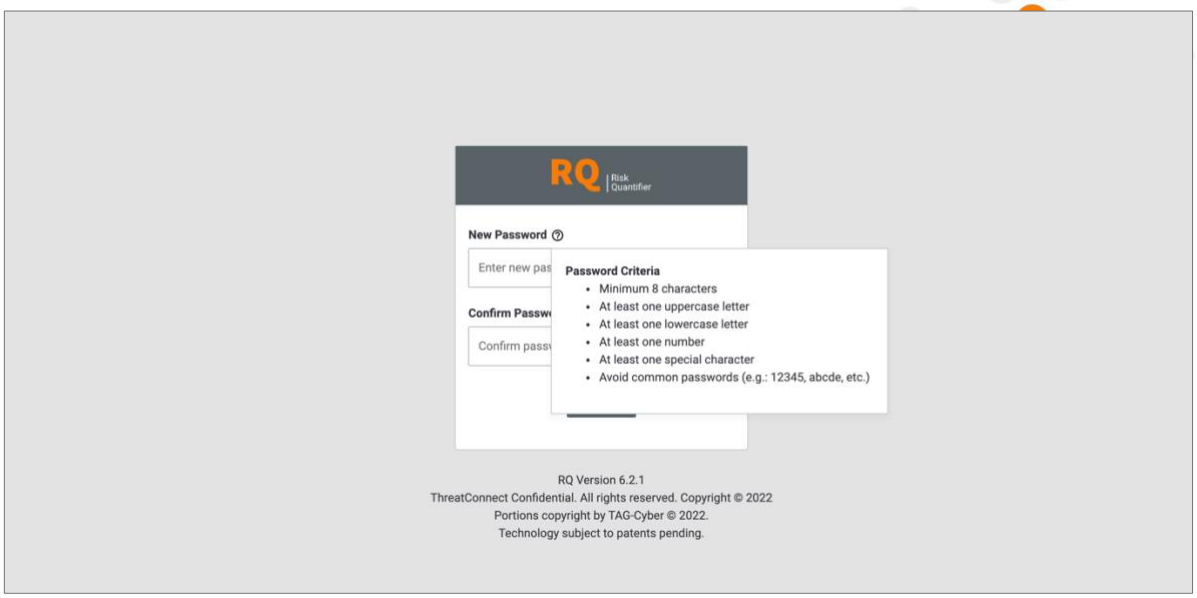

Figure 3

Deactivation of User Accounts

The RQ platform allows administrators to deactivate and reactivate user accounts as necessary to investigate or prevent unauthorized activities.

Users with a user role of RQ Enterprise Administrator or RQ Pro Administrator can deactivate and reactivate user accounts via the **Settings** screen (Figure 4 for Enterprise and Figure 5 for Legal Entity).

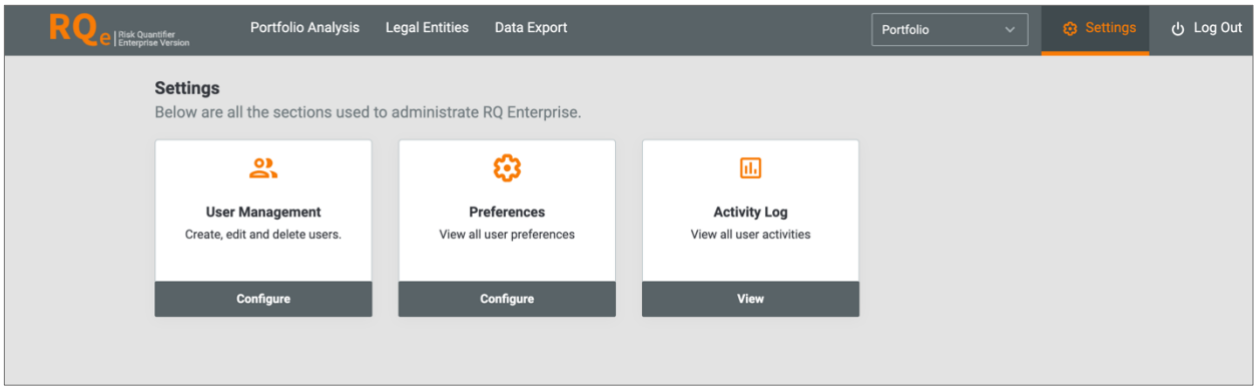

Figure 4

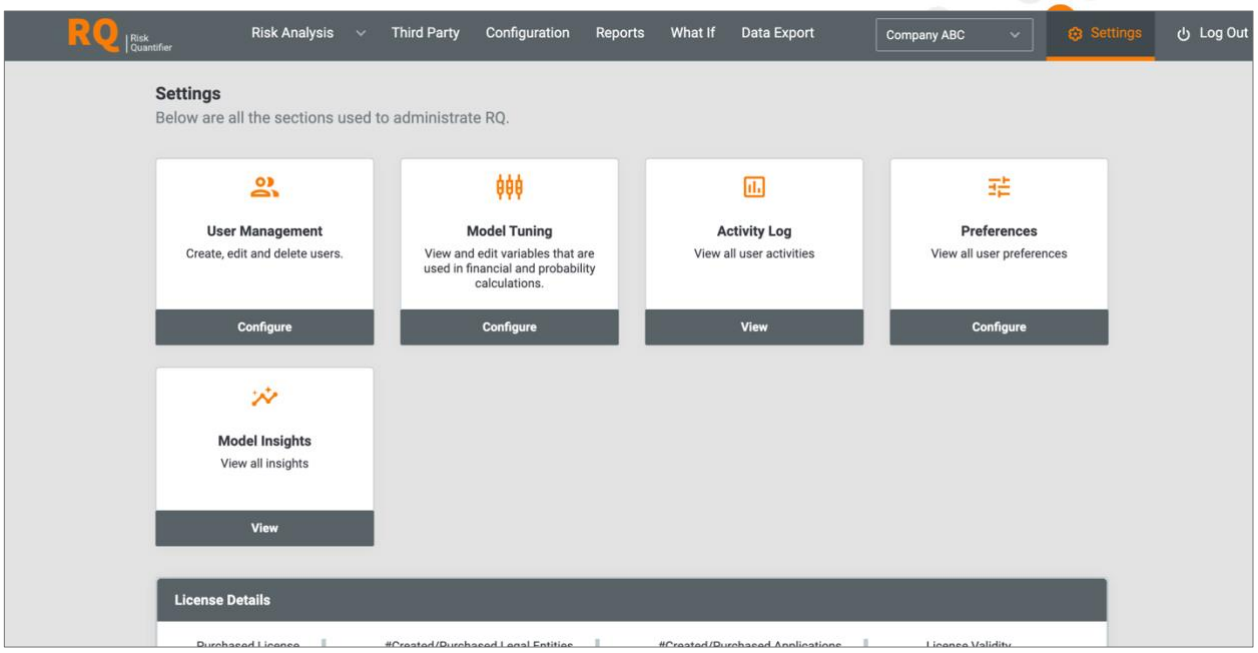

Figure 5

On the **Settings** screen, click the **Configure** button on the **User Management** card. The **User Management** screen will be displayed (Figure 6 for Enterprise and Figure 7 for Legal Entity).

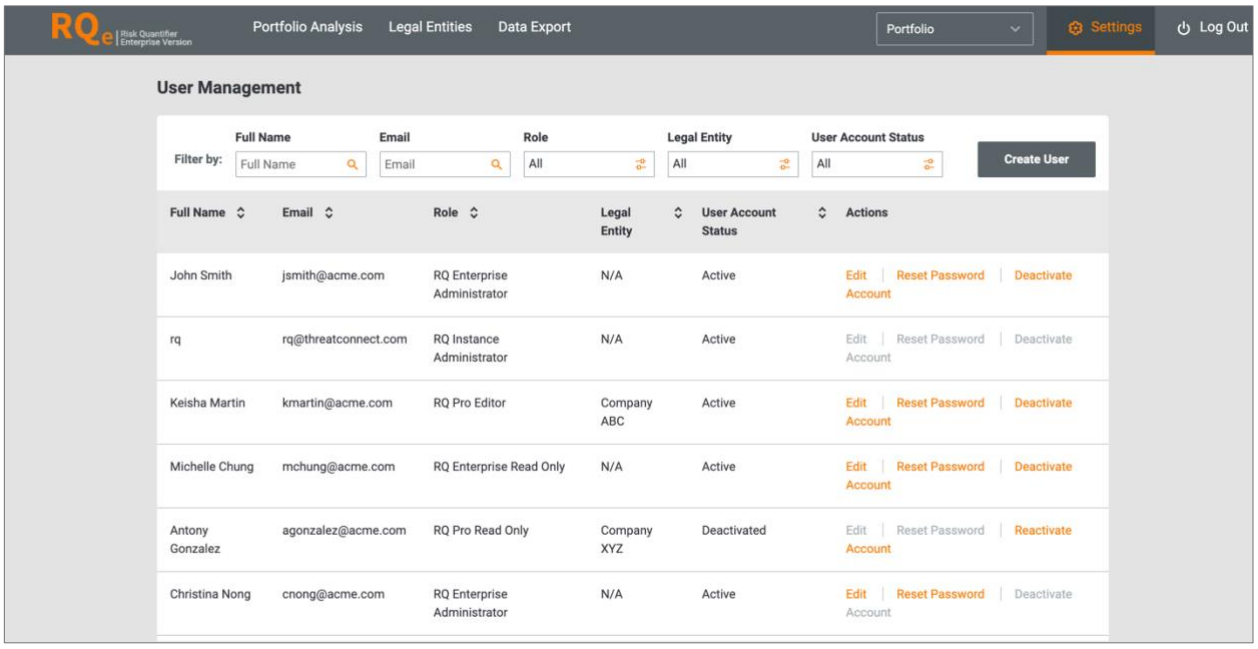

Figure 6

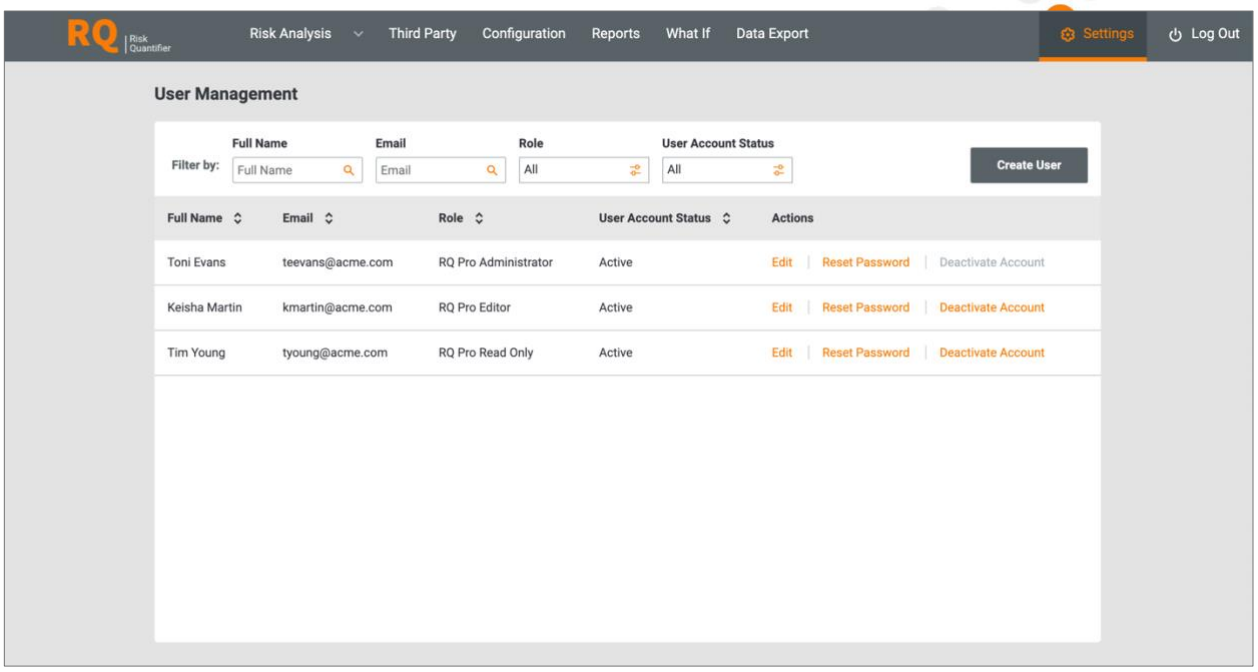

Figure 7

Select **Deactivate Account** in the **Actions** column for the RQ user account you want to deactivate. After a user account is deactivated, its entry in the **User Account Status** column will change from **Active** to **Deactivated**.

To reactivate a RQ user account that is deactivated, select **Reactivate Account** in the **Actions** column for that account (Figure 6). After a user account is reactivated, its entry in the **User Account Status** column will change from **Deactivated** to **Active**.

NOTE: The Enterprise-level RQ instance administrator account (rq@threatconnect.com) may not be deactivated.

User Activity Logs

Users with a user role of RQ Enterprise Administrator or RQ Pro Administrator can review user activity logs in their RQ instance via the **Settings** screen (Figure 4 for Enterprise and Figure 5 for Legal Entity).

On the **Settings** screen, click the **View** button on the **Activity Log** card. The **Activity Log** screen will be displayed (Figure 8 for Enterprise and Figure 9 for Legal Entity).

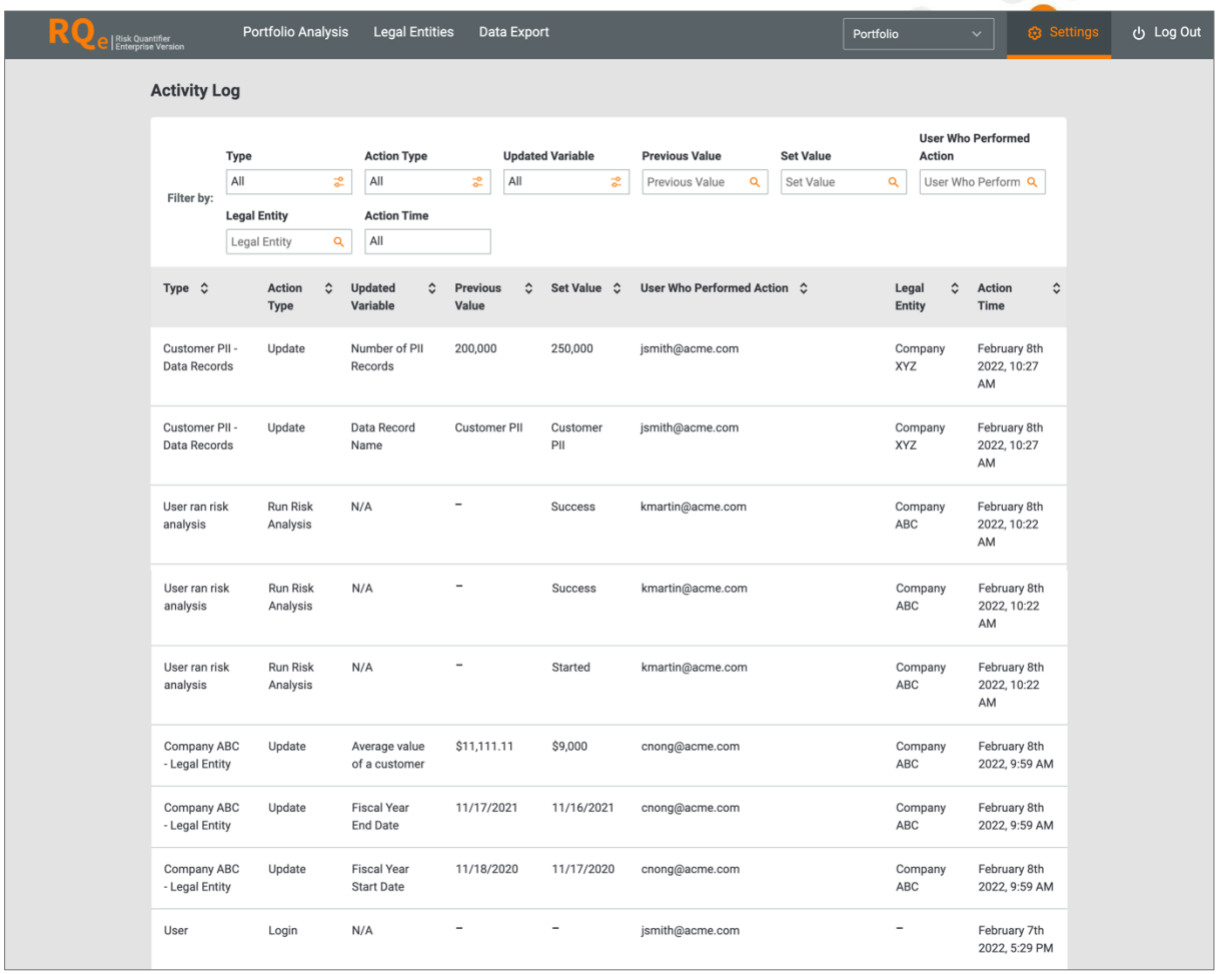
RQe Risk Quantifier Enterprise Version
Portfolio Analysis
Legal Entities
Data Export
Portfolio
Settings
Log Out
Activity Log
Filter by:
Type
All
Action Type
All
Updated Variable
All
Previous Value
Previous Value
Set Value
Set Value
User Who Performed Action
User Who Perform
Legal Entity
Legal Entity
Action Time
All
Type
Action Type
Updated Variable
Previous Value
Set Value
User Who Performed Action
Legal Entity
Action Time
Customer PII - Data Records
Update
Number of PII Records
200,000
250,000
jsmith@acme.com
Company XYZ
February 8th 2022, 10:27 AM
Customer PII - Data Records
Update
Data Record Name
Customer PII
Customer PII
jsmith@acme.com
Company XYZ
February 8th 2022, 10:27 AM
User ran risk analysis
Run Risk Analysis
N/A
–
Success
kmartin@acme.com
Company ABC
February 8th 2022, 10:22 AM
User ran risk analysis
Run Risk Analysis
N/A
–
Success
kmartin@acme.com
Company ABC
February 8th 2022, 10:22 AM
User ran risk analysis
Run Risk Analysis
N/A
–
Started
kmartin@acme.com
Company ABC
February 8th 2022, 10:22 AM
Company ABC - Legal Entity
Update
Average value of a customer
$11,111.11
$9,000
cnong@acme.com
Company ABC
February 8th 2022, 9:59 AM
Company ABC - Legal Entity
Update
Fiscal Year End Date
11/17/2021
11/16/2021
cnong@acme.com
Company ABC
February 8th 2022, 9:59 AM
Company ABC - Legal Entity
Update
Fiscal Year Start Date
11/18/2020
11/17/2020
cnong@acme.com
Company ABC
February 8th 2022, 9:59 AM
User
Login
N/A
–
–
jsmith@acme.com
–
February 7th 2022, 5:29 PM

Figure 8

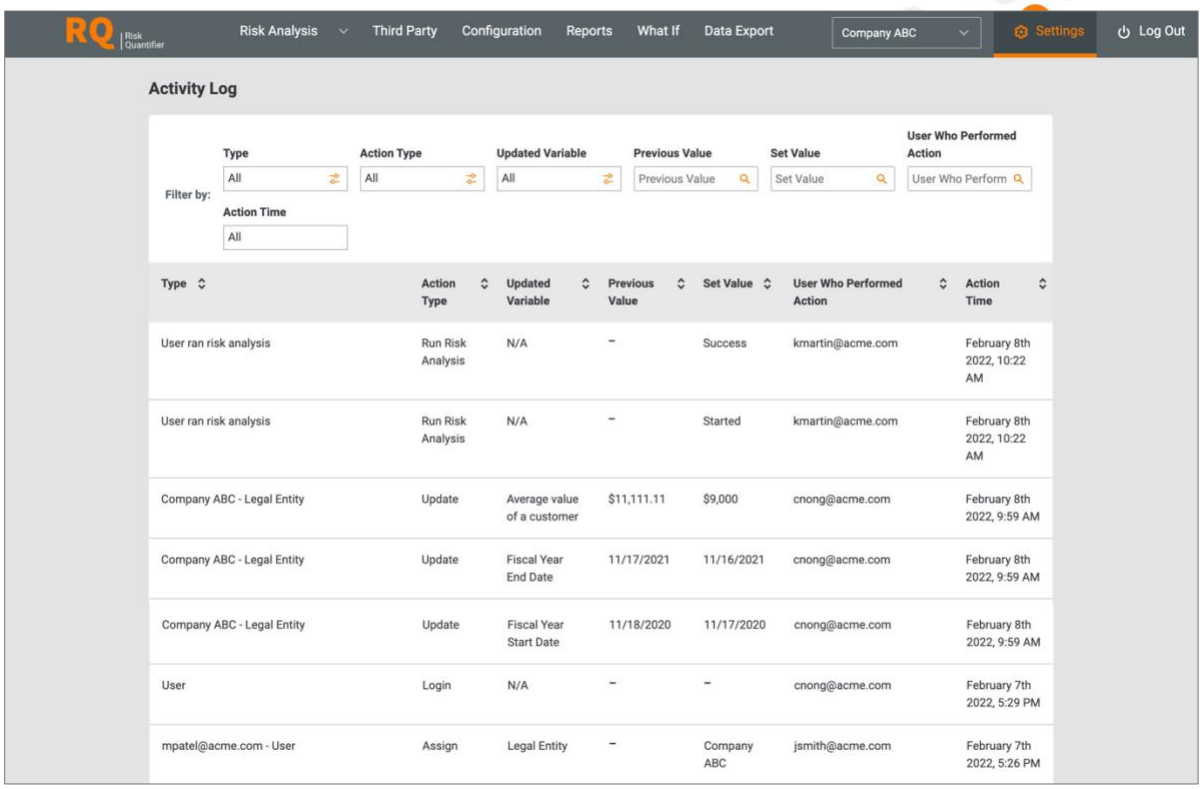

Figure 9

By default, all activities in the user's RQ instance will be displayed. The following filters can be used to limit the activities displayed on the **Activity Log** screen:

- **Type**: Select one or more activity types that were performed.
- **Action Type**: Select one or more action types that were performed.
- **Updated Variable**: Select one or more variables that were updated.
- **Previous Value**: Enter a value that was previously assigned to a variable. Note that this value depends on the variable and type of value it accepts (e.g., the **Fiscal Year Start Date** variable accepts a date as its value, but the **Legal Entity Name** variable accepts a text-based entry as its value).

  NOTE: Enter at least two letters in this field. Entries to be filtered on do not have to be typed in their entirety.
- **Set Value**: Enter a value currently assigned to a variable. Note that this value depends on the variable and type of value it accepts (e.g., the **Fiscal Year Start Date** variable accepts a date as its value, but the **Legal Entity Name** variable accepts a text-based entry as its value).

  NOTE: Enter at least two letters in this field. Entries to be filtered on do not have to be typed in their entirety.
- **User Who Performed Action**: Enter the email address of a user in your instance.

  NOTE: Enter at least two letters in this field. Entries to be filtered on do not have to be typed in their entirety.

- **Legal Entity**: Enter the name of a legal entity in your instance. This column is displayed only on the Enterprise level (Figure 8).

  NOTE: Enter at least two letters in this field. Entries to be filtered on do not have to be typed in their entirety.
- **Action Time**: Select the period of time when activities were performed.

User Account Lockout

By default, user accounts are locked after 10 failed login attempts in order to protect against brute-force attacks. This default cannot be changed in the RQ interface. Users who have been locked out of their account will receive an email message instructing them to contact their administrator to unlock the account. Administrators can unlock locked user accounts from the **User Management** screen, where the **Reset Password** option will be replaced with an **Unlock Account** option for locked accounts.