April 2022

QIAGEN Digital Insights Admin Tool Quick Start Guide

Sample to Insight

QIAGEN

Contents

Introduction

QIAGEN Digital Insights Admin Tool (QDIAT) is a platform that allows you to:

1. Manage your users and monitor your license(s)/sessions/usage

2. Single Sign-on (SSO) configuration

This platform manages the access to the following products

- HGMD – Human Genetic Mutation Database - https://my.qiagendigitalinsights.com/bbp/

- HSMD – Human Somatic Mutation Database - https://my.qiagendigitalinsights.com/bbp/

- COSMIC – Catalogue of Somatic Mutations in Cancer - https://my.qiagendigitalinsights.com/bbp/

- PGMD - PharmacoGenomic Mutation Database - https://my.qiagendigitalinsights.com/bbp/

- ANNOVAR - https://my.qiagendigitalinsights.com/bbp/

- Genome Trax™ - https://my.qiagendigitalinsights.com/bbp/

- QCI – QIAGEN Clinical Insights – https://variants.ingenuity.com/qci

- IPA – Ingenuity Pathway Analysis – https://analysis.ingenuity.com/pa

QDIAT allows you to look up which licenses users have within your organization, control access to products by adding or removing users, look up who is currently logged in, and monitor when licenses expire.

Access to QDIAT

If you are a license coordinator for any of these products, log in at https://apps.ingenuity.com/iat with your username and password.

If you are the license coordinator and cannot access QDIAT please contact customer support via TS-Bioinformatics@qiagen.com and request a QDIAT license. Please note, a license to your

product can be managed by more than one administrator. If you wish to add/remove administrators, you must contact Customer Support. Administrators do not need to be members of the License Group (individual users that have access to a licensed product).

How to use QDIAT

License Administrator/License Coordinator: this is the administrator at the institution who is authorized to make changes to the licenses/users.

Once logged in, QDIAT displays on the home page the list of active licensing groups. From here you can administer more than one product license. To do this, you will need to choose which license you want to access after you log into QDIAT. In the example shown below, the license administrator can manage two different licenses, and must select one before continuing.
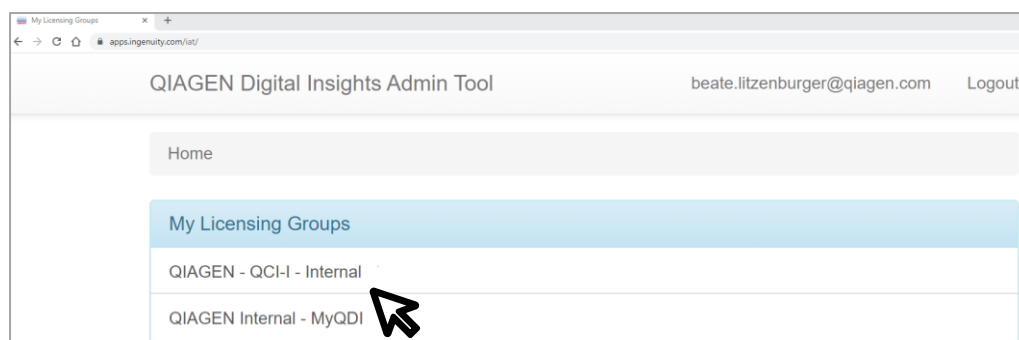
SSO Administrator: this is typically the buyer's IT person who configures and manages the institutions single sign-on with QDI's product offerings. To configure SSO for your institution reach out to TS-Bioinformatics@qiagen.com. We support multiple SSO Administrators.

The SSO Configuration tab allows the SSO Administrator to configure SSO for his/her company and to manage users by enabling/disabling the SSO process for them.
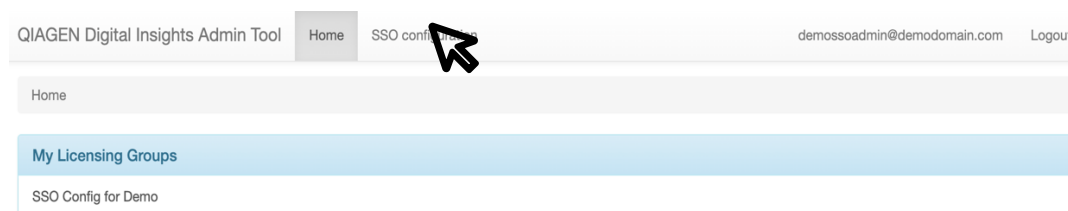
User Management

In the *Users* tab for QDIAT you will find 3 sections; (1) Administrators, (2) Add New Users to Licensing Group, and (3) Users in Licensing Group. These sections are described in more detail below.

① Administators

Displays a list of administrators that can manage the access of users to the product. This list is managed by Customer Support. If you wish to add/remove administrators, you must contact Customer Support via TS-Bioinformatics@qiagen.com.

② Add New Users to Licensing Group

It is possible that users within your organization possess licenses for other QIAGEN Digital Insights products and are already registered within the QIAGEN licensing system. If this is the case, you can simply search in the "Add User to Group" section to see if the user has an account, as shown below. Note that in the screenshot below the search is performed using the organizational email address.

If the user exists within QIAGEN's licensing system a window will pop-up displaying the user details. You can then select the user to be added to this license group. Click on "Save Changes" to finalize the process and user will receive a "Welcome" email with a link to access this product.

If the user is not found, you can create a user account for that user. To add a user to your license group, click on "Create Account", fill in the required information, and click "Add to License".

When entering the Institution or Company name, suggestions will appear via autocomplete. Please try to use one of these names if applicable. If the institution or company is not listed, then type in the name.

Checking the *Enable SSO* checkbox will enable the account to login via the institution's Identity Provider. If the checkbox is in read-only mode, this means there is no SSO configured for your domain's institution.

After a moment, you will see a confirmation that the user was created and added to your license group. The user will then receive a "Welcome" email to activate account, set password and link to access this product.

(3a) Users in License Group

This section displays users in your license group for your product. The table is searchable by email, name, and the date they were added to the license.
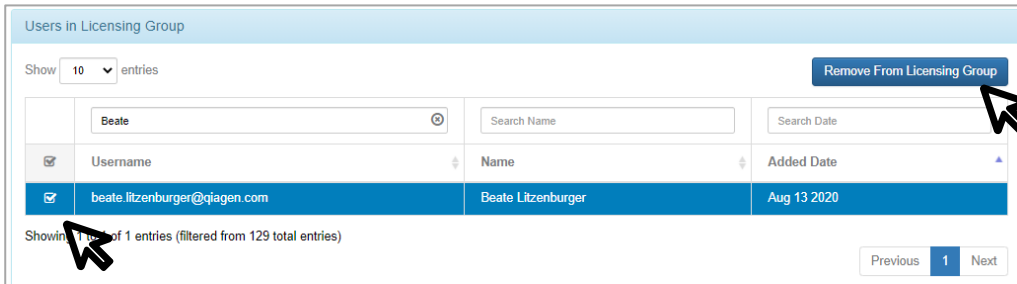

(3b) Remove Users from License Group to End Access.

To remove users from your license, first check the box to the left of the member(s) you wish to remove and then click on the "Remove From Licensing Group" button.

Once you remove a user from a specific licensed product, any active session for that person is immediately terminated and he or she will not be able to access this specific product.

License Management

The *Licenses* tab displays the start and end date of active license(s) for the license group.

If the license restricts usage from specific IP addresses, those will be listed. Then all sessions on this license must originate from these IP addresses. This is the institutional/building IP address as seen by the rest of the world. This is not the IP address on the user's computer.

Please note, only users from the specified domains can use your license, which are the email domains belonging to the institution that bought the license (e.g. qiagen.com).

Sessions

Viewing who is currently logged into your license group.

Go to the *Live Sessions* section, which provides a list of users who are currently logged into your license. You can see how long they have been using the license in the current session and you can terminate that session if necessary (see below). Note that all times listed are in the PST time zone.

Terminating an active session

In the *Live Sessions* section, you can click the terminate button to the right of the user whose session you wish to terminate. Please use this option only in urgent situations, as it will potentially interrupt the user's work. We recommend that you contact the user before terminating their session.

Viewing failed sessions

The *Failed Sessions* section provides a list of users who could not use the application. It states the cause why the user could not access the application.

Usage Monitoring

The *usage* tab allows users to review the Dataset Upload limit and consumption associated with your license. This tab Is divided into 2 sections that will be explained in more detail below.

(1) License Usage

This section shows you the activation and end date of your IPA license. If your IPA license is limited by consumption, its usage is noted in the table.   In the above example, the Group has a limit of 100 Dataset Uploads of which 2 have been consumed by some Group members.

② User Usage for Sample Upload

This table displays the number of uploads consumed per user within the Group. From this table you can see the individual consumption rate.

SSO Configuration

Qiagen Digital Insights is an identity provider that offers authentication with security measures such as complex passwords, password expiration, 2 factor authentication. One user account in our identity store can access all QDI products as listed above in the Introduction.

Customers have the option to use their own identity provider for authentication through QDI's Single Sign-on (SSO). SSO allows you to login using your company credentials. Qiagen's SSO is based on SAML 2.0, more specifically, the Service Provider-Initiated SAML Flow.

Once SSO is configured, the SSO Administrator is responsible for all communication and authentication related issues/queries for their users.

Prerequisites

- Send a request to TS-Bioinformatics@qiagen.com

    o   with first name, last name, and email ID of the SSO Administrator

    o   list of domains for SSO

An SSO administrator will be created by the QDI customer support team and in order to gain access to the SSO configuration tab, a special license will be assigned.

Creating a new configuration

On the right side panel you can find detailed instructions on how to create and setup a new SSO configuration for your company.

On the left side panel, in the *My SSO Configs* section you will find a list of your current SSO configurations. You can click on the *Add new SSO config* to create a new one.

SSO configuration

My SSO Configs

demodomain.com

Add New SSO config

SSO instructions

Overview

Single sign-on allows you to login using your company credentials. Qiagen single sign-on (SSO) is based on SAML 2.0. Qiagen can map attributes to provision a user to different group with feature controls.

Qiagen acts as the Service Provider (SP), and it's capable of offering automatic user provisioning. In case auto-provisioning is enabled, then you do not need to register as a user in Qiagen. Once Qiagen receives a SAML response from the Identity Provider (IdP), Qiagen checks if this user exists. If the user does not exist, Qiagen creates a user account automatically with the received name ID.

This article covers:

- Configuring SSO
- Enabling SSO

Configuring SSO

First, enter your SSO information

- Domain name(s): <Domains for which you want to do SSO>
- Identity provider id: <ID of EntityDescriptor>
- Identity provider metadata xml: <Identity provider metadata xml> **Note: The metadata xml should be provided to you from the IT department of your company**
- Email attribute name: <Name of email attribute> **Note: The name of attribute should be provided to you from the IT department of your company**
- First attribute name: <Name of first name attribute> **Note: The name of attribute should be provided to you from the IT department of your company**
- Last attribute name: <Name of last name attribute> **Note: The name of attribute should be provided to you from the IT department of your company**

Enabling SSO

Second, download our metadata and enable SSO

- **Note** Once configured you'll have to download the SP metadata XML.
- Enable SSO

Enabling SSO users

Third, enable SSO login for existing users

- **Note** By default existing users will not be able to login with SSO. They have to be changed

There are three steps for setting up a new SSO configuration.

SSO Config: step 1

The configuration step requires you to choose one or multiple domain(s). The available domains are the ones setup by customer support at the time the SSO administrator was created. If you cannot find the domain you are looking for please reach out to customer support for any changes. Please observe the instructions on the right side panel for the information required in the form.

If the *Automatic user provisioning* is checked this means that all new users signing in to Qiagen via your company's identity provider will gain access to the Qiagen products by having accounts automatically created in the Qiagen system and added to your license group.

SSO Config: step 2

The 2nd step allows you to preview the configuration, choose the license group for auto provisioning and enable the SSO configuration. This is also the step from which an existing SSO configuration can be disabled by clicking on the *Disable* button. A right side panel is also available with more information on this.

SSO Config: step 3

The 3rd step allows you to move users between two lists: one that is SSO enabled – meaning that users will sign in using your company identity provider and the other which is SSO disabled meaning that users will continue to sign in via Qiagen system.

In order to do this, you need to click on the checkbox next to the username and then use the arrows highlighted below to submit the action. The left and right side lists will refresh automatically after this.

How to navigate between the *SSO configuration steps*

Use the arrows between the steps to move from one step to the other.

Changes to current support process for authentication related issues

When SSO is enabled, the SSO admin is responsible for all authentication related communication to their users.
Once QIAGEN assigns SSO admin for their domains/institution, QIAGEN will no longer reply/support authentication questions from those domains/institutions.