
June 2024

QIAGEN Digital Insights Admin Tool Quick Start Guide

Contents

Introduction	3
Access to QDIAT	3
How to use QDIAT	4
Administrators	5
Add New Users to Licensing Group	5
Users in License Group	8
Remove Users from License Group to End Access	8
Sessions	10
Viewing who is currently logged into your license group	10
Terminating an active session	10
Viewing failed sessions	11
Usage Monitoring	11
License Usage	12
User Usage for Sample Upload	12
SSO Configuration	13
Prerequisites	13
SSO Config: step 1	15
SSO Config: step 2	15
SSO Config: step 3	16
How to navigate between the <i>SSO configuration steps</i>	17
Changes to current support process for authentication related issues	17
When SSO is enabled, the SSO admin is responsible for all authentication related communication to their users	17

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.qiagenbioinformatics.cn/qci/>
- IPA – Ingenuity Pathway Analysis – <https://analysis.qiagenbioinformatics.cn/pa/installer/select>

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

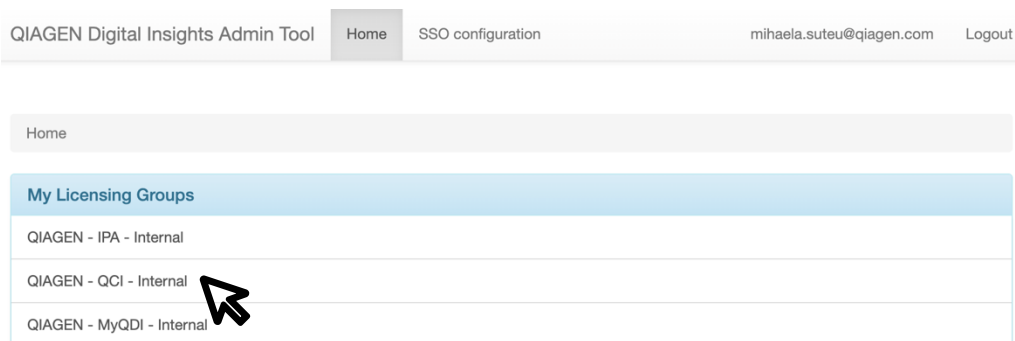
If you are a license coordinator for any of these products, log in at <https://apps.qiagenbioinformatics.cn/iat/> with your username and password.

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).

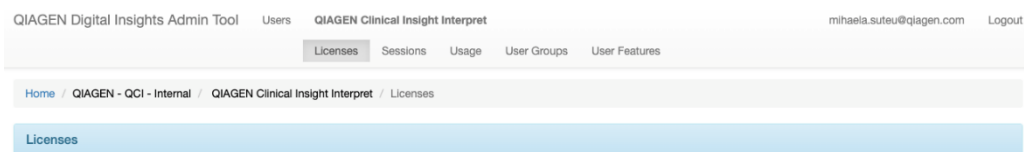
How to use QDIAT

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.



Once a license group is selected, the top menu will display the following tabs: Users and "QIAGEN Digital Insights" with the following submenu: Licenses, Sessions, Usage, User Groups and User Features.



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.

QIAGEN Digital Insights Admin Tool | Users | About | mihaela.suteu@qiagen.com | Logou

Home / QIAGEN - QCI - Internal

All users listed in the Users tab belong to the license groups and have access to all applications shown.

Add Users to Licensing Group (2)

Search Users | Create Account

Search and add existing accounts to the licensing group.

User account email address or addresses

Enter one or more email addresses or search on one partial address.

Search

Administrators (1)

Username	Name	Admin Type
christine.bueno@qiagen.com	Christine Bueno	SSO
cristian.balint@qiagen.com	Cristian Balint	SSO
mihaela.suteu@qiagen.com	Mihaela Suteu	License
roslen.anacieto@qiagen.com	Roslen Anacieto	SSO
sachin.pattanshetty@qiagen.com	Sachin Pattanshetty	SSO
stuart.tugendreich@qiagen.com	Stuart Tugendreich	SSO

Users in Licensing Group (3)

Show only users with SSO | Export users as: XLS | XLSX

Show 10 entries

Search Username	Search Name	Search Date
Username	Name	Added Date
<input type="checkbox"/> aaron.mandel@qiagen.com	Aaron Mandel	May 19 2020
<input type="checkbox"/> aarthi.goverdhan@qiagen.com	Aarthi Goverdhan	Apr 25 2023
<input type="checkbox"/> aavishkar.ghosh@qiagen.com	Aavishkar Ghosh	Sep 20 2022
<input type="checkbox"/> alexandra.matei@qiagen.com	Alexandra Matei	Jan 26 2023

<https://apps-pdm.ingenuity.com/iat/app/users/view/338426>

1 Administrators

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.

Add Users to Licensing Group

Search User [Create Account](#)

Search and add existing accounts to the licensing group.

Dominic.John@qiagen.com

Enter one or more email addresses or search on one partial address.

Search

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.

Add Users To Licensing Group

Select the users that will be added to the licensing group **QIAGEN Internal - MyQDI**

Show 10 entries

<input type="checkbox"/>	Username	Name
<input checked="" type="checkbox"/>	dominic.john@qiagen.com	Dominic John

Showing 1 to 1 of 1 entries

Previous 1 Next

Cancel **Save Changes**

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".

Add Users to Licensing Group

[Search Users](#) [Create Account](#)

Create new account and add it to the licensing group.

Institutional Email Address

First Name

Last Name

Institution or Company Name

The license does not have a domain or the user's domain is not configured for SSO. Select a value from autocomplete dropdown.

Enable SSO

[Add to License](#) [Reset](#)

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.

Add Users to Licensing Group

Search Users
Create Account

The new account was successfully created and added to the licensing group. ✕

Create new account and add it to the licensing group.

Institutional Email Address

First Name

Last Name

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. A filter can be applied to view only the users in the license group having SSO enabled.

If an account has SSO enabled, a key icon will be displayed near the username.

The list of users can be exported in a xls or xlsx file format.

Users in Licensing Group 3

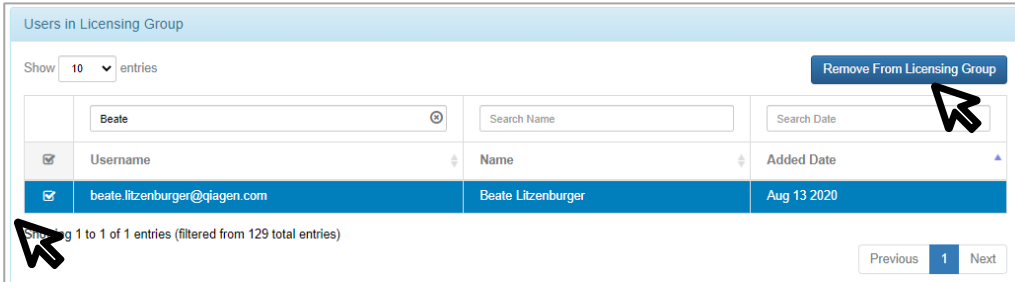
Show only users with SSO
Export users as: [XLS](#) | [XLSX](#)

Show: 10 entries

	Search Username	Search Name	Search Date
<input type="checkbox"/>	Username	Name	Added Date
<input type="checkbox"/>	aarthigoverdhan@qiagen.com	Aarthi Goverdhan	Nov 04 2021
<input type="checkbox"/>	aavishkarghosh@qiagen.com	Aavishkar Ghosh	Sep 20 2022
<input type="checkbox"/>	ada.ceen@contractor.qiagen.com	Ada Ceen	Nov 19 2020

3b Remove Users from License Group to End Access.

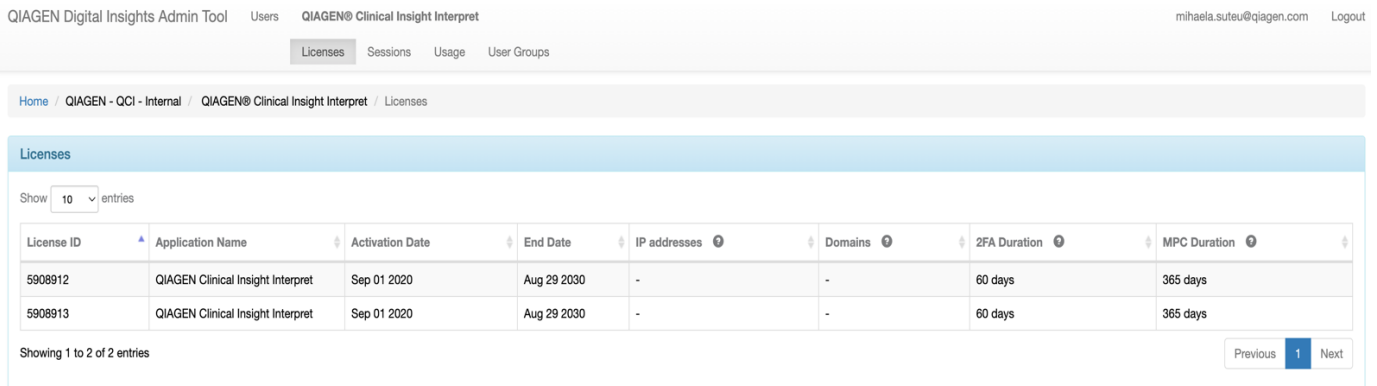
To remove users from your license, first check the box to the left of the member(s) you wish to remove and then click on the "Remove From Licensing Group" button.



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).

Security settings defined on the license are also displayed here. These can be custom defined values or default ones provided by the system.

The two factor authentication duration column lists the duration for which a 2FA token is valid for, it applies to users that are not on SSO. If the license group contains both users that are on

SSO login and users that are not on SSO, then the 2FA setting will be displayed as a combination.

The mandatory password change duration column lists the duration for which a password is valid for, after which the system will request to be changed with a new one. It applies to users that are not on SSO. If the license group contains both users that are on SSO login and users that are not on SSO, then the MPC setting will be displayed as a combination.

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.

QIAGEN Digital Insights Admin Tool Users QIAGEN Clinical Insight Interpret mihaela.suteu@qiagen.com Logout

Licenses **Sessions** Usage

Home / QIAGEN - QCI - Internal / QIAGEN Clinical Insight Interpret / Sessions

License Details

License ID: 956531
Max. Concurrent Users: 2147483647

Live Sessions

Show 10 entries

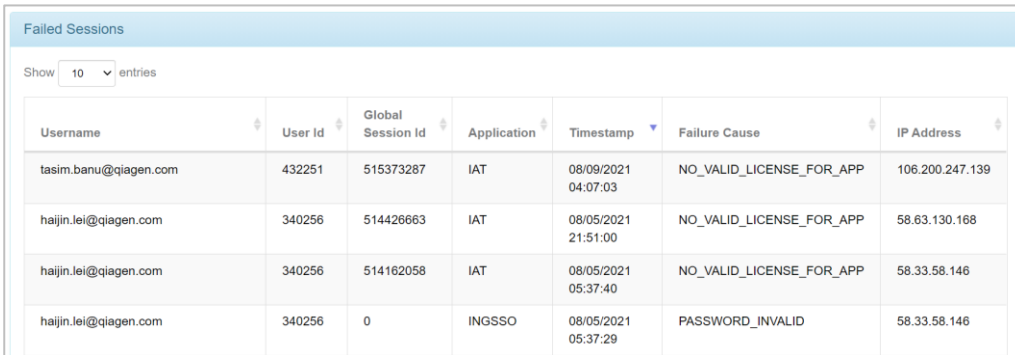
Username	Session Id	Start Time	Last Request	Duration	Inactivity Timeout	IP Address	Geo Location	Action
mihaela.suteu@qiagen.com	18710129	Aug 31 2023, 16:22:02	Aug 31 2023, 18:17:56	1h 55m	1h 0m	10.32.45.46	Rotterdam,South Holland,Netherlands	Terminate
ionel.marincas@qiagen.com	18710129	Aug 31 2023, 16:22:02	Aug 31 2023, 18:17:56	1h 55m	1h 0m	10.32.45.46	Rotterdam,South Holland,Netherlands	Terminate

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.



The screenshot shows a table titled "Failed Sessions" with a "Show 10 entries" dropdown. The table has seven columns: Username, User Id, Global Session Id, Application, Timestamp, Failure Cause, and IP Address. There are four rows of data.

Username	User Id	Global Session Id	Application	Timestamp	Failure Cause	IP Address
tasim.banu@qiagen.com	432251	515373287	IAT	08/09/2021 04:07:03	NO_VALID_LICENSE_FOR_APP	106.200.247.139
haijin.lei@qiagen.com	340256	514426663	IAT	08/05/2021 21:51:00	NO_VALID_LICENSE_FOR_APP	58.63.130.168
haijin.lei@qiagen.com	340256	514162058	IAT	08/05/2021 05:37:40	NO_VALID_LICENSE_FOR_APP	58.33.58.146
haijin.lei@qiagen.com	340256	0	INGSSO	08/05/2021 05:37:29	PASSWORD_INVALID	58.33.58.146

Usage Monitoring

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

License Usage ①

License ID: 4293077
 Application Name: QIAGEN Clinical Insight Interpret
 Activation Date: Aug 31 2020
 End Date: Aug 28 2030

Show 10 entries

Feature Id	Feature Name	Feature Description	Feature Current Usage / Limit
23237	QCIT Upload	QCIT Upload	19 / 10000

Showing 1 to 1 of 1 entries

Previous 1 Next

User Usage for QCIT Upload ②

Show 10 entries

User Id	Username	Name	Individual Usage
58215	jean-noel.billaud@qiagen.com	Jean-Noel Billaud	0 / 10000
73412	aaron.mandel.qcit@qiagen.com	aaron.mandel.qcit	0 / 10000
165582	vcs_selenium_qcit_autouser@qiagen.com	VCS Selenium QCIT Auto User	0 / 10000
244360	tim@demo.com	Tim Demo	0 / 10000
244361	dong@demo.com	Dong Demo	0 / 10000
244419	james@demo.com	James Demo	0 / 10000
247936	shawn@demo.com	Shawn Demo	0 / 10000
260324	rafael@demo.com	Rafael Filippelli	0 / 10000
260325	ruth@demo.com	Ruth Burton	0 / 10000
260352	beta.ngs.qcit.automation@qiagen.com	BETA NGS QCIT	0 / 10000

Showing 1 to 10 of 32 entries

Previous 1 2 3 4 Next

① License Usage

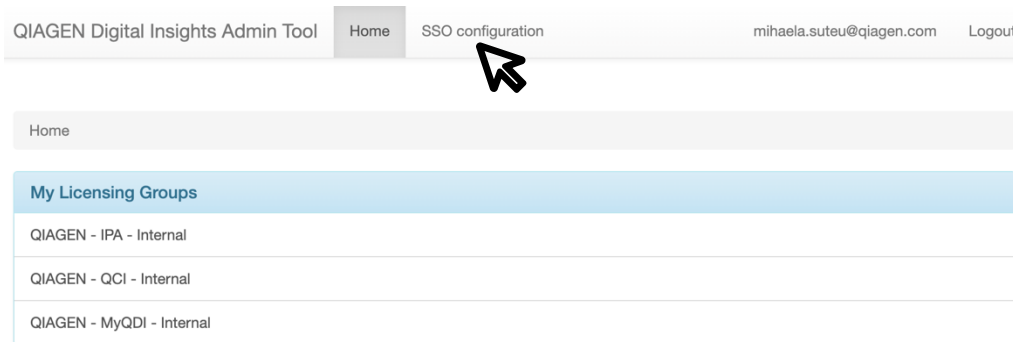
This section shows you the activation and end date of your QCI Interpret Translational license. Your QCI Interpret Translational license consumption limit and usage is noted in the table above. In the example, the Group has a limit of 10000 samples of which 19 samples have been consumed by all Group members.

② User Usage for Sample Upload

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

SSO Configuration

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.



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.

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

There is also a table that lists all the administrators defined on the group.

The screenshot displays the SSO configuration interface. On the left, the 'My SSO Configs' section shows a list of configurations: ion.com, keycloak.com, and qiagen.com contractor.qiagen.com. Below this is a blue button labeled 'Add New SSO config' with a mouse cursor pointing to it. The 'Administrators' section contains a table with the following data:

Username	Name	Admin Type
diana.stanila@qiagen.com	Diana Stanila	SSO
gabriel.padurean@qiagen.com	Gabriel Padurean	SSO
ionel.marincas@qiagen.com	ionel Marincas	License, SSO
suteum@qiagen.com	Miha Suteu	SSO

On the right, the 'SSO instructions' panel provides an overview and detailed steps for configuring and enabling SSO.

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

You can download QIAGEN service provider public certificate used for SAML signing from [here](#)

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.

The screenshot shows the 'SSO configuration' page in the 'QIAGEN Digital Insights Admin Tool'. The user is logged in as 'demossoadmin@demodomain.com'. The page is titled 'SSO configuration / Create SSO Config'. There are three numbered steps: 1. Configure SSO (highlighted with a mouse cursor), 2. Enable SSO configuration, and 3. Enable SSO users.

Step 1: Create SSO configuration for domain(s)

Domain Name(s)

demodomain.com

- demodomain.com
- test.com
- qiagen.com
- contractor.qiagen.com
- keycloak.com

Email attribute name

Eg: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Enter name of attribute for email address sent in SAML response.

First name attribute name

Eg: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

Enter name of attribute for first name sent in SAML response.

Last name attribute name

Eg: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

Enter name of attribute for last name sent in SAML response.

Automatic user provisioning

When this will be checked users will be automatically assigned to unlimited site licenses.

Step 2: Configuring SSO

First step

Enter your SSO information here

- 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**

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. After selecting the domain(s) a service provider metadata URL will get displayed and it will allow for the QIAGEN metadata data file to be downloaded locally. 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.

QIAGEN Digital Insights Admin Tool Home SSO configuration Users ionel.marincas@qiagen.com Logout

SSO configuration / demodomain.com

1 Configure SSO 2 Edit SSO configuration 3 Enable SSO users

View SSO configuration for domain(s)

Domain Name(s)
demodomain.com

Download QIAGEN service provider metadata

Entity Id
demodomain.com

Identity metadata xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntitiesDescriptor
  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  Name="http://ingenuity.com"
  xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata oas:names:tc:SAML:2.0:metadata_2.0.xsd" />
```

Choose file No file chosen

Email attribute name
email

Enter name of attribute for email address sent in SAML response.

First name attribute name
firstname

Enter name of attribute for first name sent in SAML response.

Last name attribute name
lastname

Enter name of attribute for last name sent in SAML response.

Automatic user provisioning

When this will be checked users will be automatically assigned to unlimited site licenses.

Show 10 entries

<input type="checkbox"/>	License group name	Application name
<input type="checkbox"/>	Demo - IPA and My Findings	Ingenuity Views and Reports
<input type="checkbox"/>	Demo Findings Internal Group	Ingenuity Views and Reports
<input checked="" type="checkbox"/>	SSO Config for Demo	Ingenuity Views and Reports

Showing 1 to 3 of 3 entries Previous 1 Next

Save

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

You can download QIAGEN service provider public certificate used for SAML signing from [here](#)

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

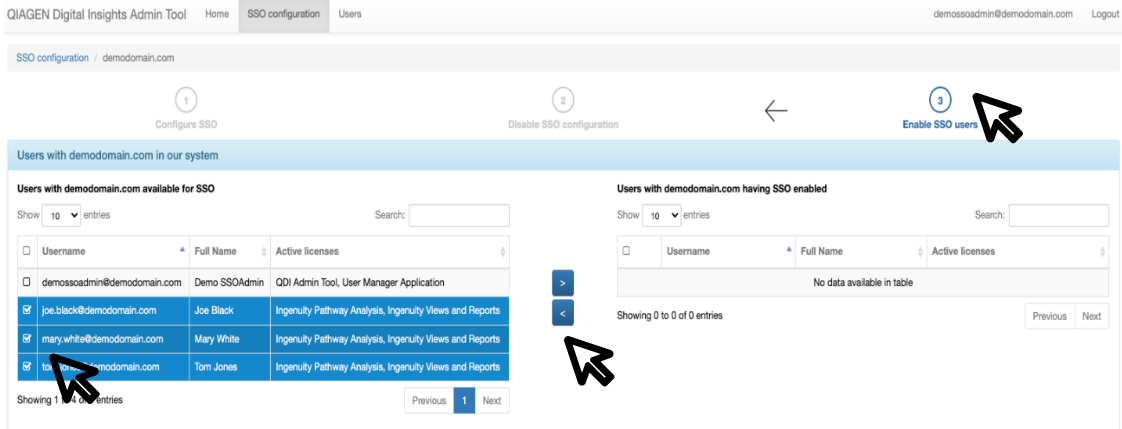
Third, enable SSO login for existing users

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

SSO Config: step 3

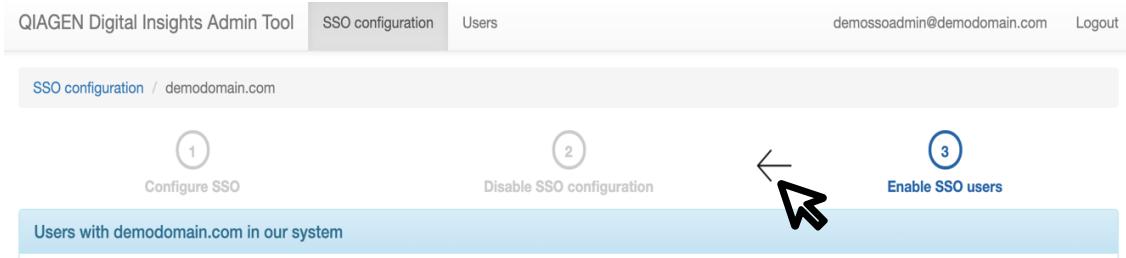
The 3rd step allows you to move users between two lists: one that is SSO enabled – meaning that users will sign in using your company identity provider and the other which is SSO disabled meaning that users will continue to sign in via Qiagen system.

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.