Iris™ media solutions

User Manual

Iris Admin

Version 9.6.0.197

GRAYMETA™

Contents

1 Introduction

1.1 Overview

Iris™ Server consists of a database and a web-based Server Tools GUI for management of the database and other Iris server-side tools.

This manual provides software installation instructions and an overview of the GrayMeta Iris Admin. For more information, please contact FAQ and support section on the GrayMeta website

Visit www.graymeta.com

- Product information and software download
- Manage user account and license
- Support center for enquiries and issue management

2 Installation

2.1 Installing GrayMeta Iris Admin

There are two ways to install Iris Admin. One option is to run the installer without specifying any parameters and it will bring up the GUI for an attended installation. The other option is to run the installer from the command line and specifying various parameters for an unattended install. An Iris Admin install will uninstall the previous version prior to installing the new version.

Optionally, the Postgres database server can be included in the install. By default, Postgres will be installed unless specified otherwise. If Postgres is excluded from the iris Admin install, then set up/upgrade of the database schema will take place via an existing Postgres database server (if the user chooses not to use the version of the Postgres database server included in the Iris Admin install and prefers to use an existing Postgres database server). If the user does choose to include Postgres database server in the Iris Admin installation, then the port number specified must not clash with the port number of any existing Postgres installations on the same machine, otherwise the install will fail. In fact, the chosen port number must be one that is not currently in use. If Postgres database server has been chosen and it already exists on the computer, then Iris Admin installer simply updates the existing database on that computer.

2.1.1 Migrate Database from an Older Version of Postgres to a Newer Version

If the Postgres database server installation has been chosen as part of the setup process, or alternatively a newer version of Postgres database server was manually installed, the data from a previous version of the Postgres database server can be migrated over to the newer Postgres database server.

The migration of data is a four-stage process that involves the backup of the database stored in the older Postgres database server, creating a new database in the new Postgres database server and restoring that data to the newly created database.

1. First of all, make sure the **original (older) PostgreSQL version** is the one currently running:
   - Open **Task Manager** → **Services** tab
   - Look for keyword **postgresql**
   - There would be two **postgresql** services (e.g. postgresql-x64-14 and postgresql-x64-17)
   - If a newer version is running instead, right-click on the newer service to stop and then start the older one.

To backup data from the older Postgres database server, run the pg_dump.exe utility, usually found in C:\Program Files\PostgreSQL\<version>\bin\pg_dump.exe where <version> is the version number of the Postgres database server you are **backing up from**.

The entire command will look like:

pg_dump.exe -f "<filename>" -p <port> -U "<username>" "Archimedia QC Player"

where <filename> is the name of the file to backup to, <port> is the port number and <username> is the username that is used to authenticate with the Postgres database server.

2. Then, make sure the **newer PostgreSQL version** is the one currently running (follow the steps similar to point 1).

   For the new version of Postgres database server, the existing database called “Archimedia QC Player” must be removed and a new blank database created (see next step). The command to create the new database is located in C:\Program Files\PostgreSQL\<version>\bin where <version> of the version number of the Postgres database server to **restore to**.

   dropdb.exe -h “<host>” -p <port> -U "<username>" "Archimedia QC Player"

   If this command fails with the error “database "Archimedia QC Player" is being accessed by other users” then use the -f flag to force the drop database:

   dropdb.exe -f -h “<host>” -p <port> -U "<username>" "Archimedia QC Player"

   Note that forcing the drop database will affect any users currently connected to the database and that **ALL DATA IN THE DATABASE “Archimedia QC Player” WILL BE DELETED**.

3. For the new version of the Postgres database server, a new database needs to be created. It must be named “Archimedia QC Player”. The command to create the new database is located in C:\Program Files\PostgreSQL\<version>\bin where <version> of the version number of the Postgres database server to **restore to**.

   createdb.exe -h “<host>” -p <port> -U "<username>" "Archimedia QC Player"

   where <host> is the IP address of the new Postgres database server, <port> is the port number and <username> is the username that is used to authenticate with the Postgres database server.

4. Now the new database “Archimedia QC Player” has been created, the restore process can take place by using the psql.exe command in C:\Program Files\PostgreSQL\<version>\bin where <version> of the version number of the Postgres database server to **restore to**:

   psql.exe -f "<filename>" -h "<host>" -p <port> -U "<username>" "Archimedia QC Player"

   where <host> is the IP address of the new Postgres database server, <port> is the port number and <username> is the username that is used to authenticate with the Postgres database server. These will all be the same as in step 2 above.

2.1.2 Unattended Install

To run the Iris Admin in unattended mode, execute the installer in the command prompt with the following parameters:

/S /INSTALLPOSTGRES=<Optional - 0/1 (default 1 if not specified)> /DATAFOLDER=<database folder location> /DBUSERNAME=<database username> /DBHOST=<Optional – database host name (default is localhost if no specified)> /DBPORT=<database port number> /DBPASSWORD=<database password> /ADMINUSERNAME=<web GUI admin username> /ADMINPASSWORD=<web GUI admin password>SERVERPORTHTTP=<web GUI HTTP port number> /SERVERPORTHTTPS=<web GUI HTTPS port number> /MAXCONNECTIONS=<Optional - Postgres max db connections> /SHAREDBUFFERS=<Optional - Postgres shared buffers>

Where:

/S = silent install

/INSTALLPOSTGRES = optional parameter that specifies whether to install Postgres database (0 = do not install, 1 = install). If this parameter is not specified, the default will be 1

/DATAFOLDER = location to store Postgres database

/DBHOST = Host IP of the Postgres database

/DBUSERNAME = username for Postgres connection

/DBPASSWORD = password for Postgres connection

/DBPORT = port number for Postgres connection

/ADMINUSERNAME = the username for logging into the Iris Admin web GUI

/ADMINPASSWORD = the password for logging into the Iris Admin web GUI

/SERVERPORTHTTP = The port number of the Iris Admin's HTTP web interface

/SERVERPORTHTTPS = The port number of the Iris Admin's HTTPS web interface

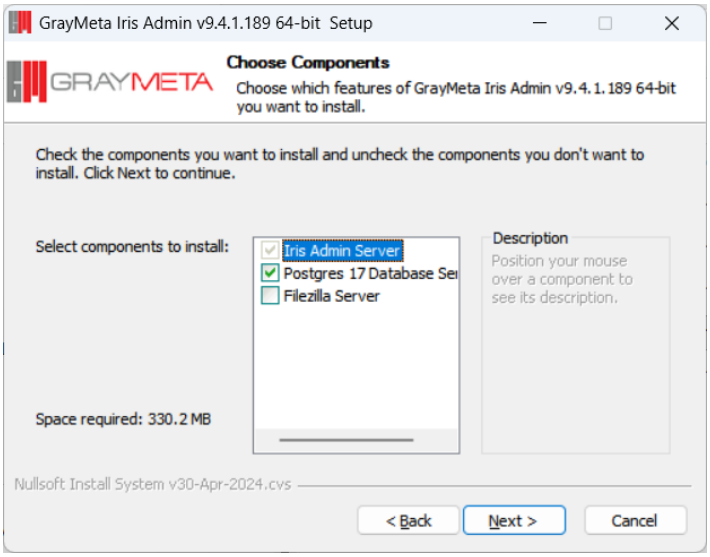
/MAXCONNECTIONS = Optional parameter that specifies the maximum number of concurrent connections to the database. This value has a default value of 100 if this parameter is not specified.

/SHAREDBUFFERS = Optional parameter that specifies the amount of memory the database server uses for shared memory buffers. This value has a default value of 128 if this parameter is not specified.

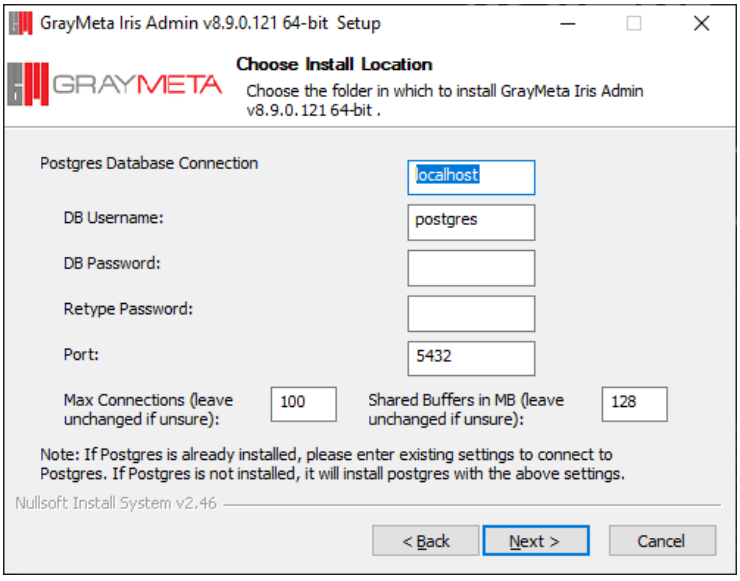
For further information on the MAXCONNECTIONS AND SHAREDBUFFERS settings, please refer to https://www.postgresql.org/docs/current/runtime-config-connection.html and https://www.postgresql.org/docs/9.1/runtime-config-resource.html

2.1.3 Attended Install

a) Firstly, select the components to install. By default, the Postgres database server is selected (see 2.1) and the Filezilla server is deselected. Filezilla server is required for transferring files between users during Iris collaboration sessions. After installation, set up the Filezilla server with the desired settings. To enable Iris to upload and download attachments, you will need to configure FTP Setup in the Server Tools GUI to use these settings. If you are hosting your own FTP Server or have no requirements to transfer files between users, you can uncheck the option to install Filezilla Server.



b) During install, you will be asked for database credentials, i.e. username, password, port number. The Max Connections setting determines the maximum number of connections to the database server and it is recommended to set this to 10x the number of concurrent signed in Iris QC Pro and/or Iris Anywhere users (eg. If there are 20 concurrent users signed in, set this value to 200). The Shared Buffers setting determines how much dedicated system memory to that Postgres will use for cache. According to Postgres documentation, it is recommended that 25% of the system RAM should be used. If unsure about these values, then leave them as default and in most cases the defaults shouldn't cause any issues.

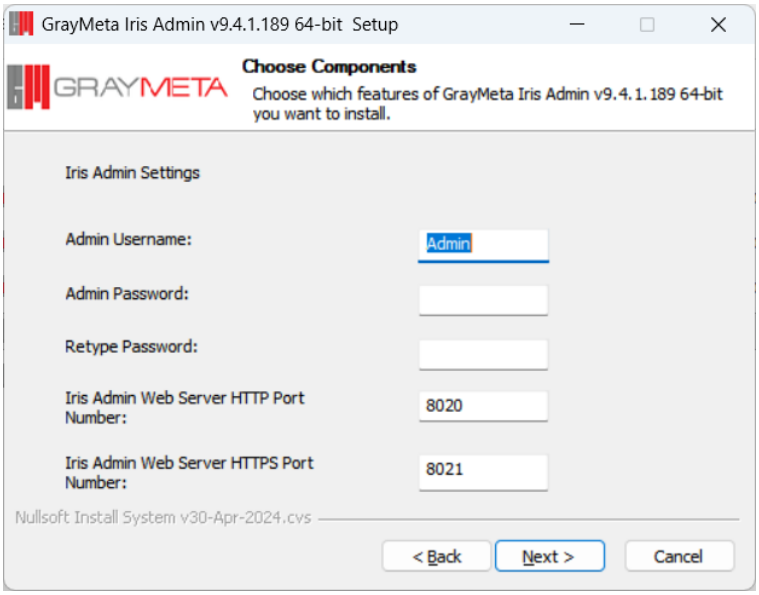


It is important that you do not lose the database username and password because this information will be required to be entered into Iris's options to allow it to connect to the database. Furthermore, it is also required when installing future versions of Iris Admin

where a database update may be necessary and these credentials will be required to proceed with the database update.

Note, the options to set Max Connections and Shared Buffers will only be shown when the user has chosen to install Postgres 17 from the previous page.

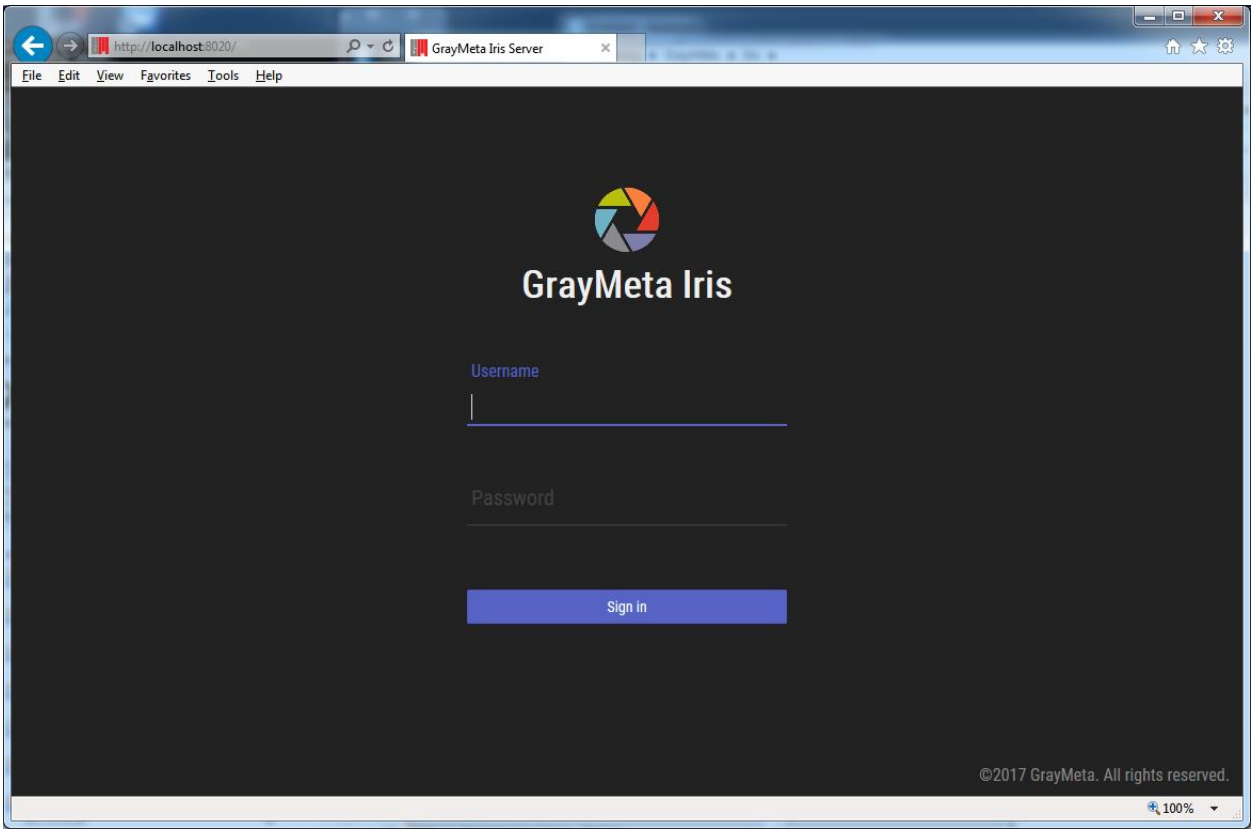
c) The next step is configuring the credentials to access the Server Tools GUI. Please enter the username and password that will be used to access the Server Tools GUI. The Iris Admin Web Server HTTP Port and Iris Admin Web Server HTTPS Port determines the port used to access Iris Admin's web-based GUI.



3 Iris Admin Tools

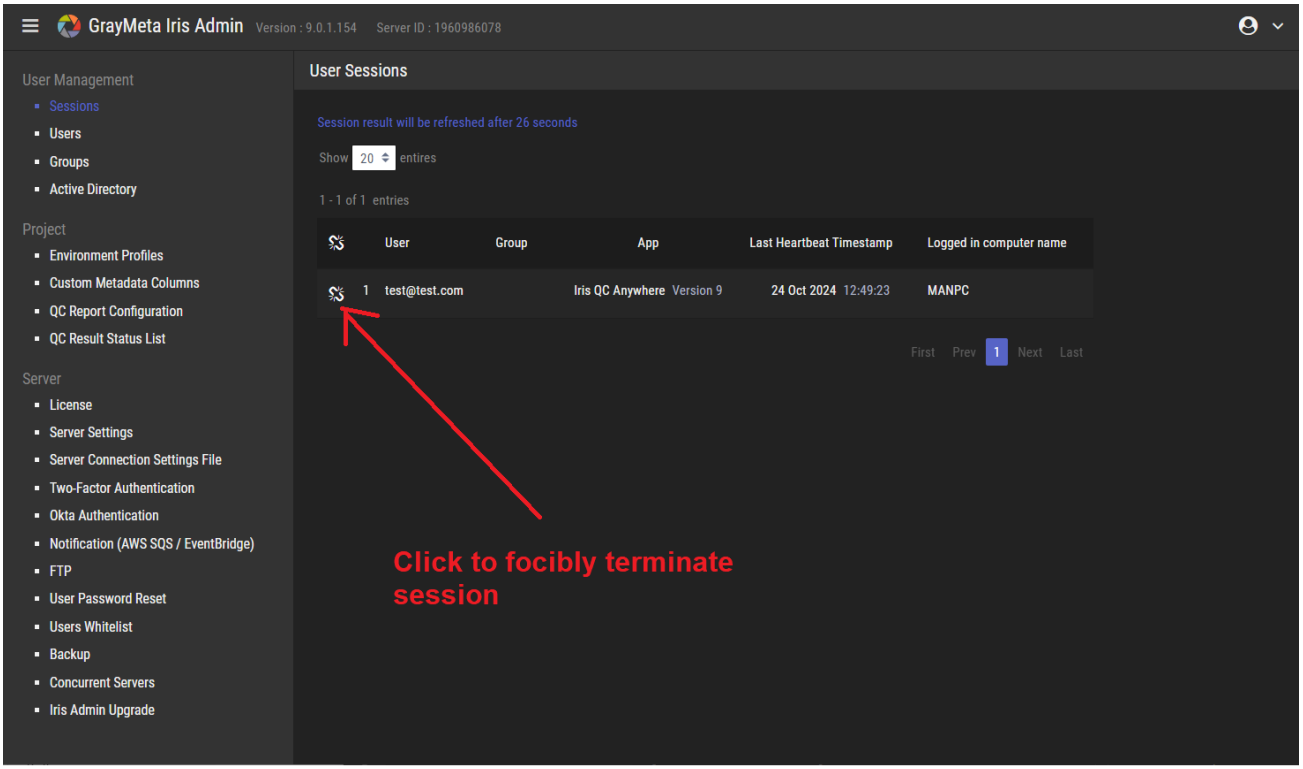
The Iris Admin web-based GUI that provides management of various resources such as user and group configuration, licensing, database settings, and so on.

Use of the Iris Admin require log in via the administrator account that was specified during the Iris Admin installation . To access Iris Admin, go to http://IrisServerMachine:aaaa or for https go to https://IrisServerMachine:bbbb where IrisServerMachine is the IP or hostname of the Iris Admin machine, aaaa is the port number for HTTP access (default is 8020) and bbbb is the port number for HTTPS access (default is 8021).



3.1 User Management

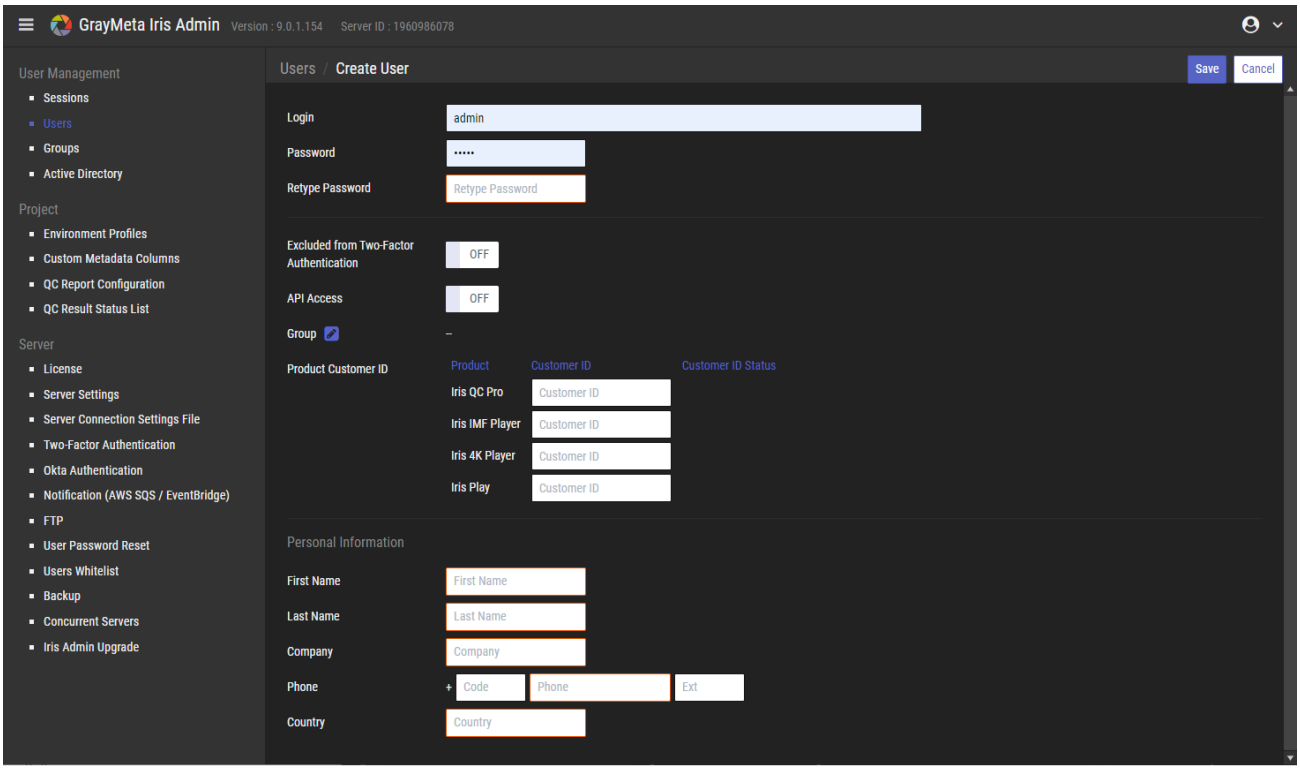
3.1.1 User Sessions



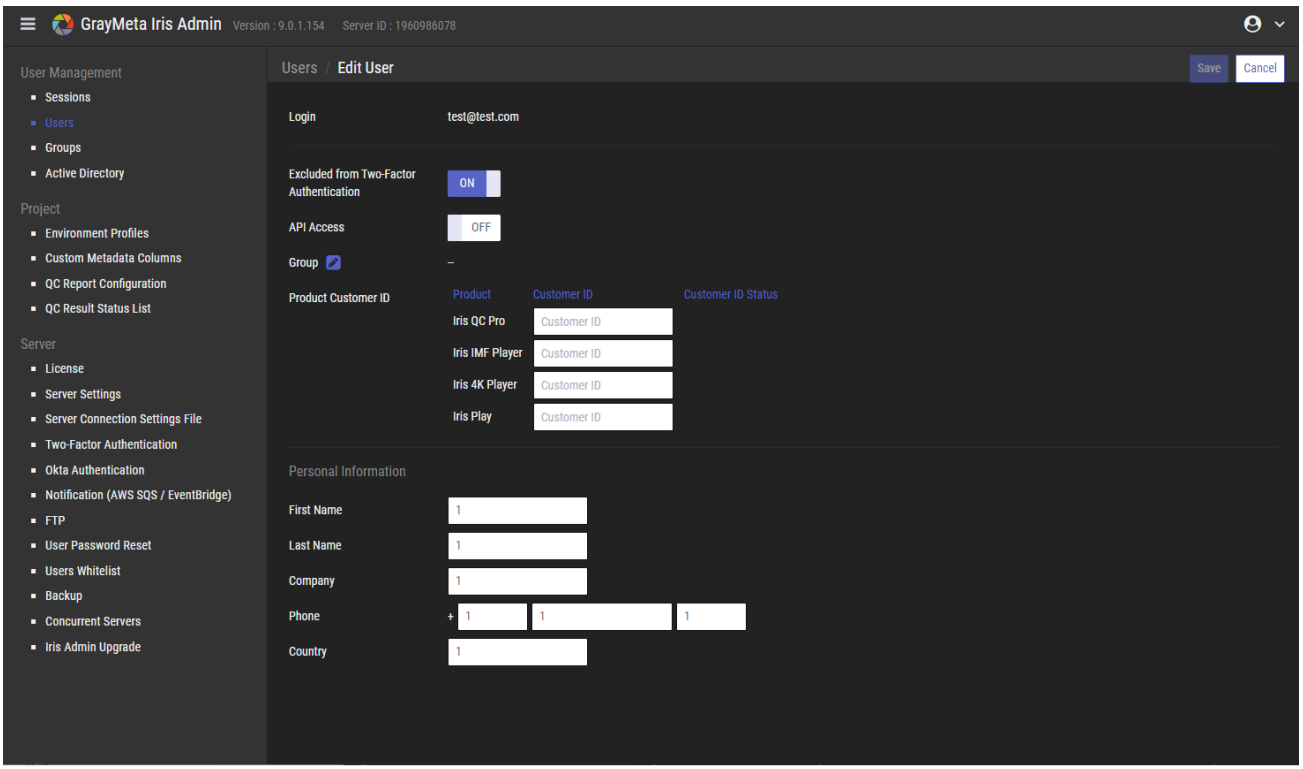
The list of users signed in to Iris is shown here. A session can be forcibly terminated by clicking on the “broken link” icon as shown above.

3.1.2 Users

The list of Iris users is shown here. A new user can be created here (as well as from within the Iris application). To create a new user, click the “Create” button located at the top right.

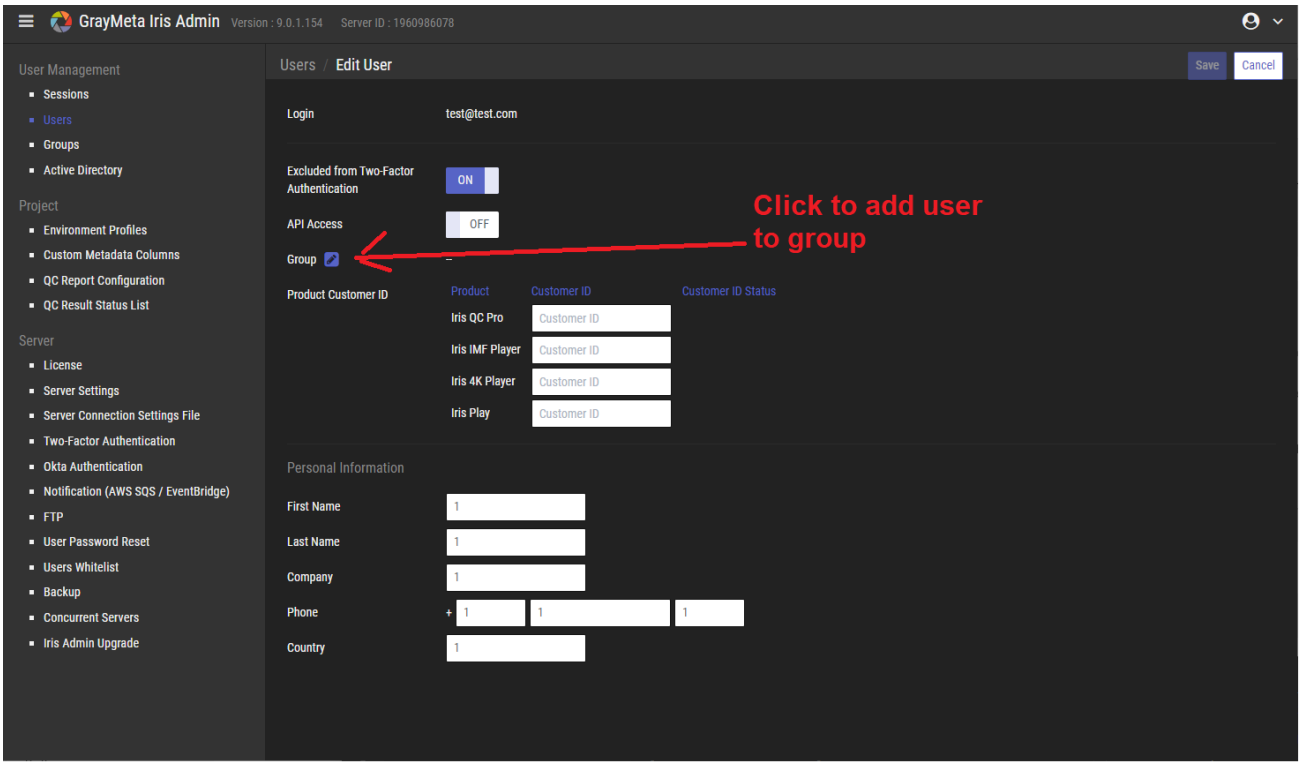


Each user can be edited or deleted. Click the pencil button to edit a user and the “-” button to delete a user. Note: if using Active Directory, this page does not show Active Directory users.



When editing user details, the user can be added to an Iris group.

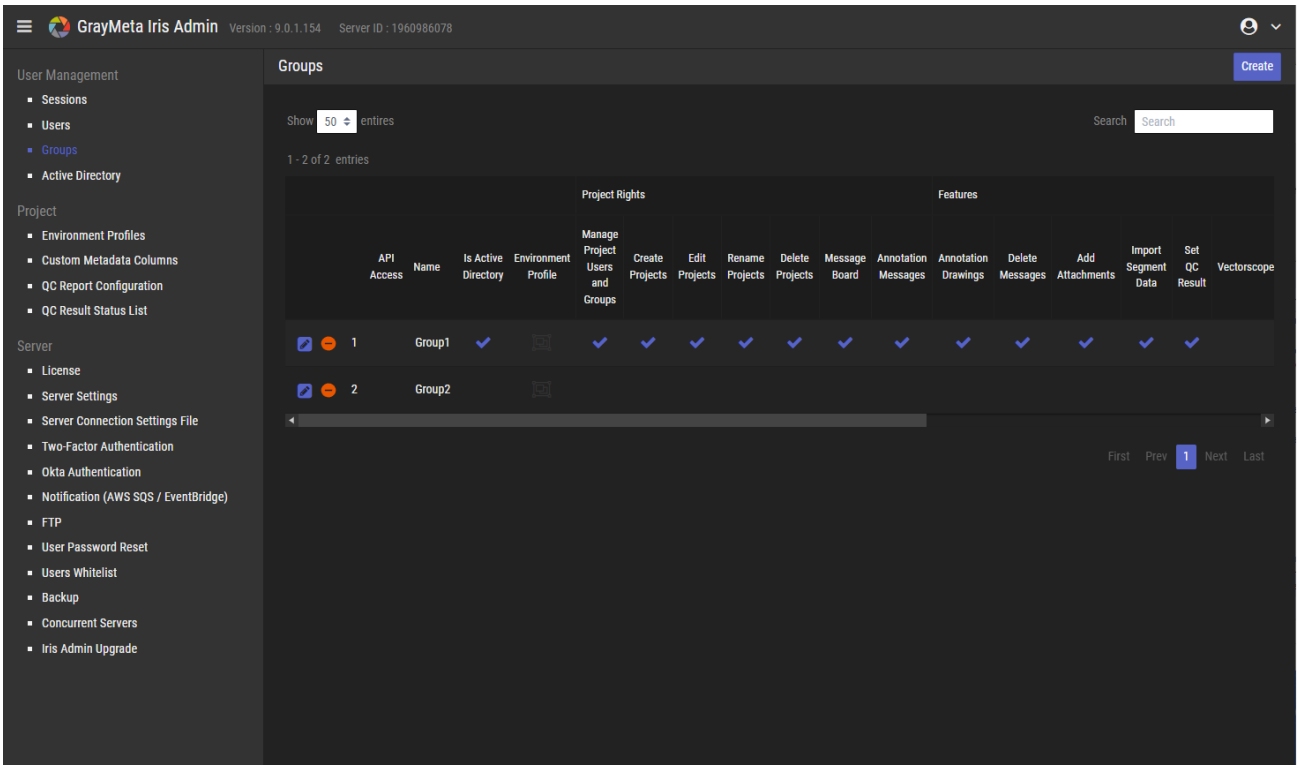
Version 9.6.0.197



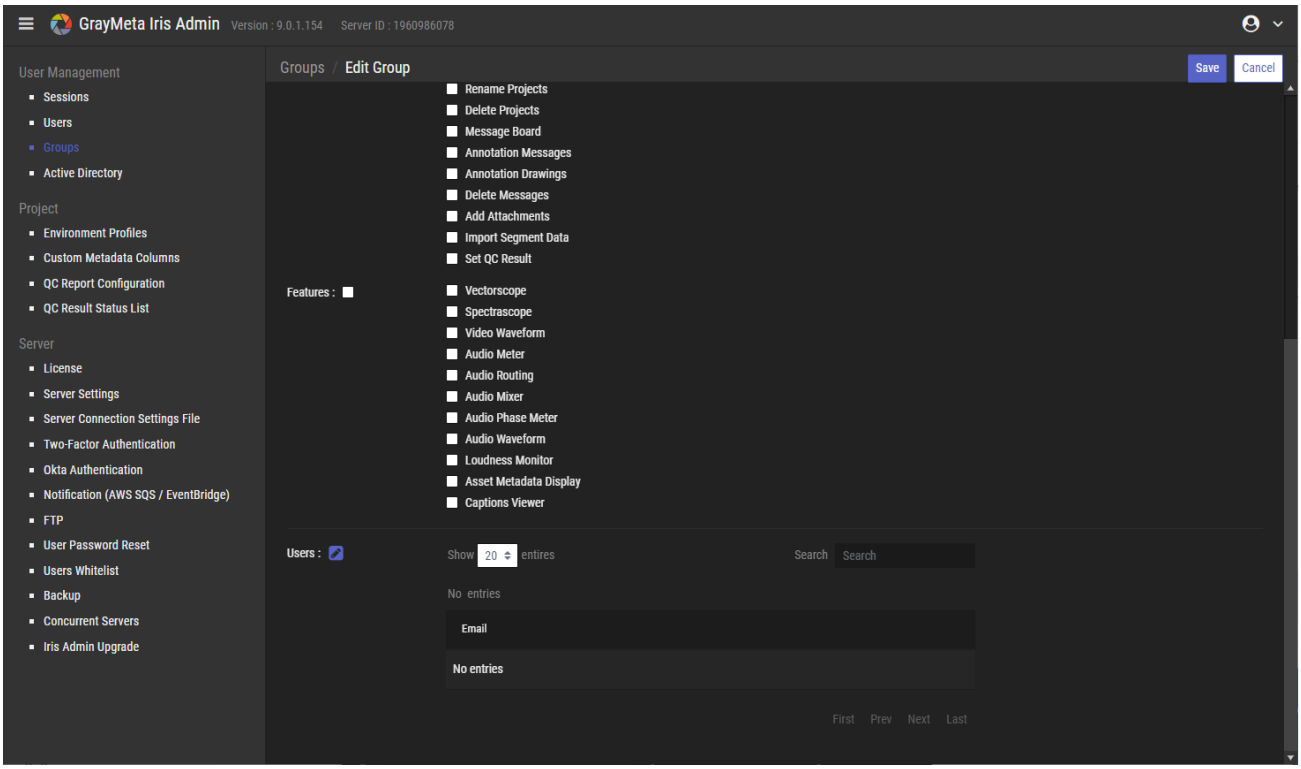
Each user has a setting to enable/disable access to the API and to be excluded from two-factor authentication. The default for both these settings are off.

3.1.3 Groups

Users can be placed into groups, of which they can be Active Directory groups (see 3.2) or Iris Groups. By placing users within groups, they can be assigned to share properties of that group, such as project rights or specific Iris features.



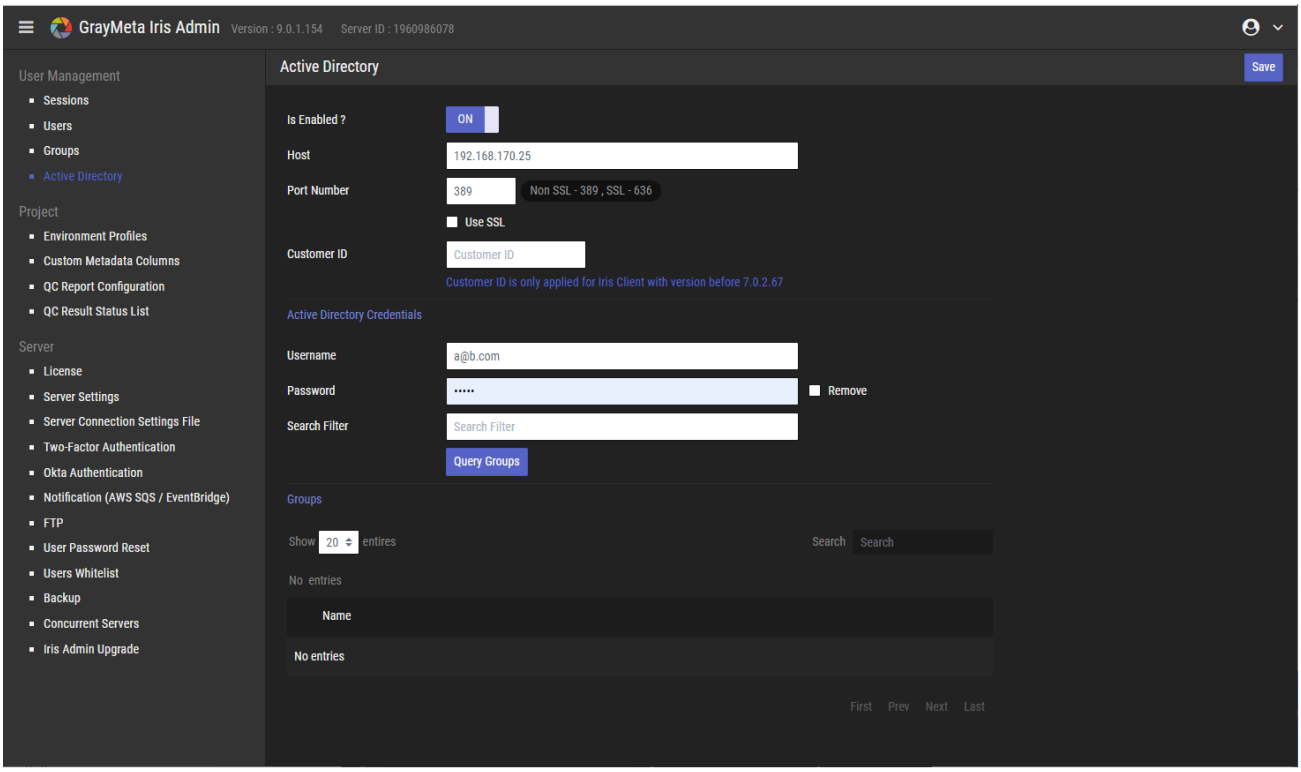
To specify group properties, click the edit button (blue pencil icon) and the following will be presented:



Choose the requisite features for the group. To add users to the group, click the blue pencil icon next to “Users” select each user for the group.

Each group can be associated with an Environment Profile. An Environment Profile consists of a set of Iris system-wide settings, tool window positions and sizes, and settings within tool windows and to specify the Environment Profile for a group, it must be exported from Iris first (as a .profile file) and re-imported by clicking the blue pencil icon next to Environment Profile. For more on Environment Profiles and how to export them, please consult the Iris user manual.

3.2 Active Directory



There are two ways to sign in to Iris. One option is to sign in using standard Iris accounts that were manually created in Iris Admin and the other way to sign in is to authenticate the user with an Active Directory Server. The Active Directory Server’s connection details can be specified by entering the Host, Port Number and SSL. Click Save on top right to save these settings. Additionally, the use of Active Directory server for signing in can be switched on or off. If it is switched off, then Iris users will sign in using a standard Iris account and if switched on, Iris users will sign in using Active Directory accounts.

For the purposes of using Iris Active Directory signing in, the only important details to be aware of is that an Active Directory server consists of a database that keeps track of user accounts and passwords and also the groups in which users belong to. For an Active Directory user to be allowed to sign in to Iris, that user must adhere to the following conditions:

- The user must be a member of an Active Directory Group

- The Active Directory Group in which a user is a member of must be enabled (see section 3.2.3)

It is important to realize that the permissions available to an Active Directory user are controlled by the group in which the user belongs to and not by the user's account itself. Therefore, the Active Directory setup of Iris Admin Tools allows for **configuration of permissions on a group basis rather than on an individual user basis**.

It is highly recommended that Iris users who require Active Directory sign in are placed into new groups created specifically for certain purposes and not built-in groups of the Active Directory Server. For example, for Iris users who have full access to everything, it makes more sense to place these users into a new group created specifically for Iris Admin users rather than place those users into the Active Directory's built-in group called "Administrators" since this may also contain non-Iris users as members of that group. This could pose a security issue as it allows unauthorized members of the built-in "Administrators" group to sign in to Iris via Active Directory authentication.

3.2.1 Use of Active Directory Credentials for OKTA SSO and Iris API

In the case of using Iris Anywhere to sign in via OKTA SSO and where Active Directory groups are required, the authentication is made with OKTA but the Active Directory group for the authenticated OKTA user has to be fetched from the Active Directory server. For this to work, Active Directory credentials are required to fetch the group from the server. The Active Directory Credentials described in Section 3.2 above will be used. The OKTA username will be used as the Active Directory user for which the groups will be fetched and the Active Directory Credentials will be used to authenticate with the Active Directory server in order to fetch the groups. For example, if signing in with the OKTA user john.smith@domain.com, then the Active Directory groups for john.smith@domain.com will be fetched using the settings for the Active Directory Credentials.

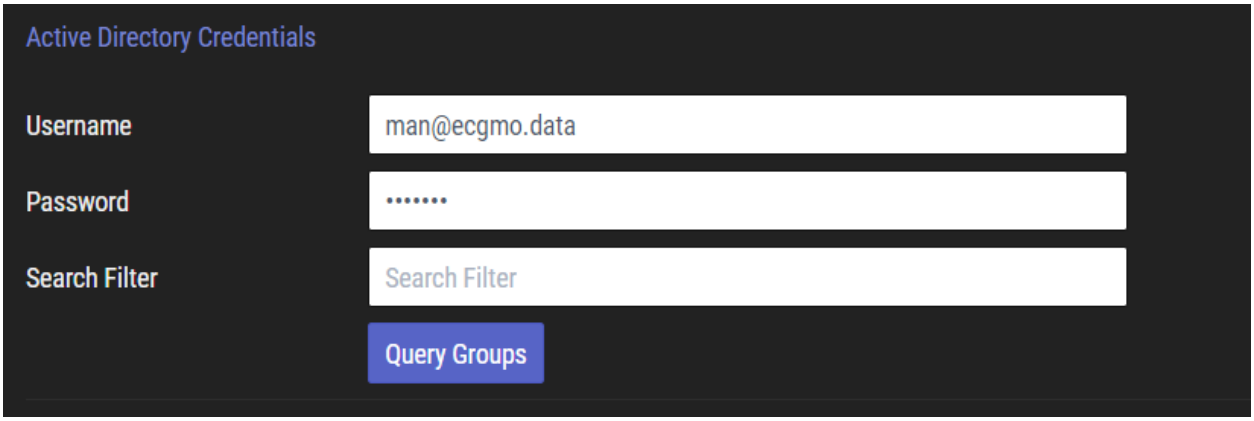
Similarly, when using the Iris API and Active Directory groups are required, the Active Directory Credentials provides the means to getting the Active Directory groups.

3.2.2 Licensing (only applies to Iris Clients prior to version 7.0.2.67)

For Iris Clients before version 7.0.2.67, each user who signs in using Active Directory sign in can use an Iris License by entering its customer ID on the Active Directory settings page. The Customer ID identifies the license to be used and is an alpha-numeric string that will be provided by GrayMeta.

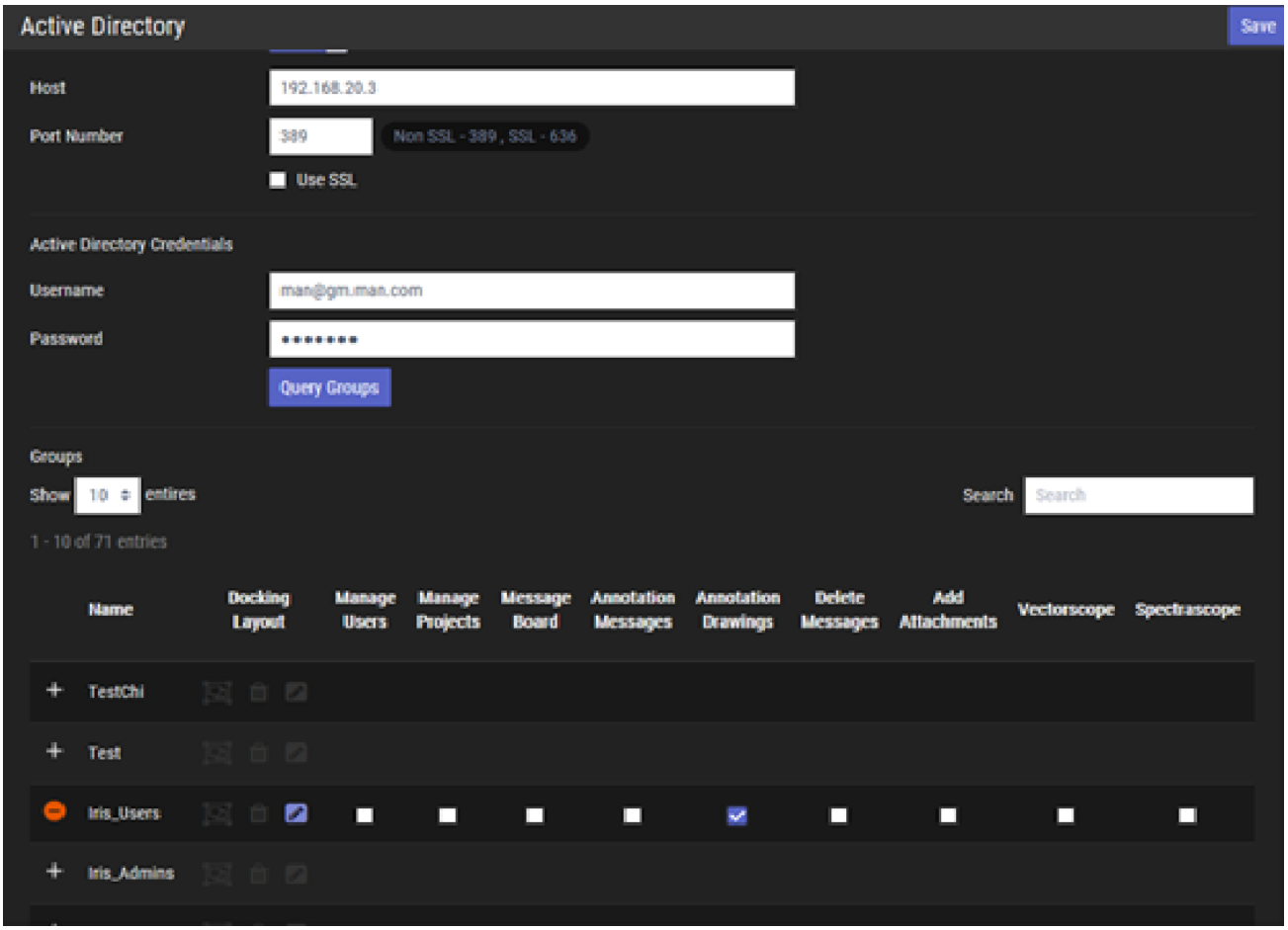
3.2.3 Configuring Group Permissions

In order to configure group permissions, they must be retrieved from the Active Directory server. An Active Directory account is required to retrieve the groups from the Active Directory server and this is required in the Active Directory Credentials:



The Search filter allows for access of groups that matches the filter. This can be used for narrowing down the number of groups retrieved in the Active Directory server, particularly if it contains a large number of groups.

If the groups are successfully retrieved from the Active Directory server, the display will be populated with a list of the groups as shown below:



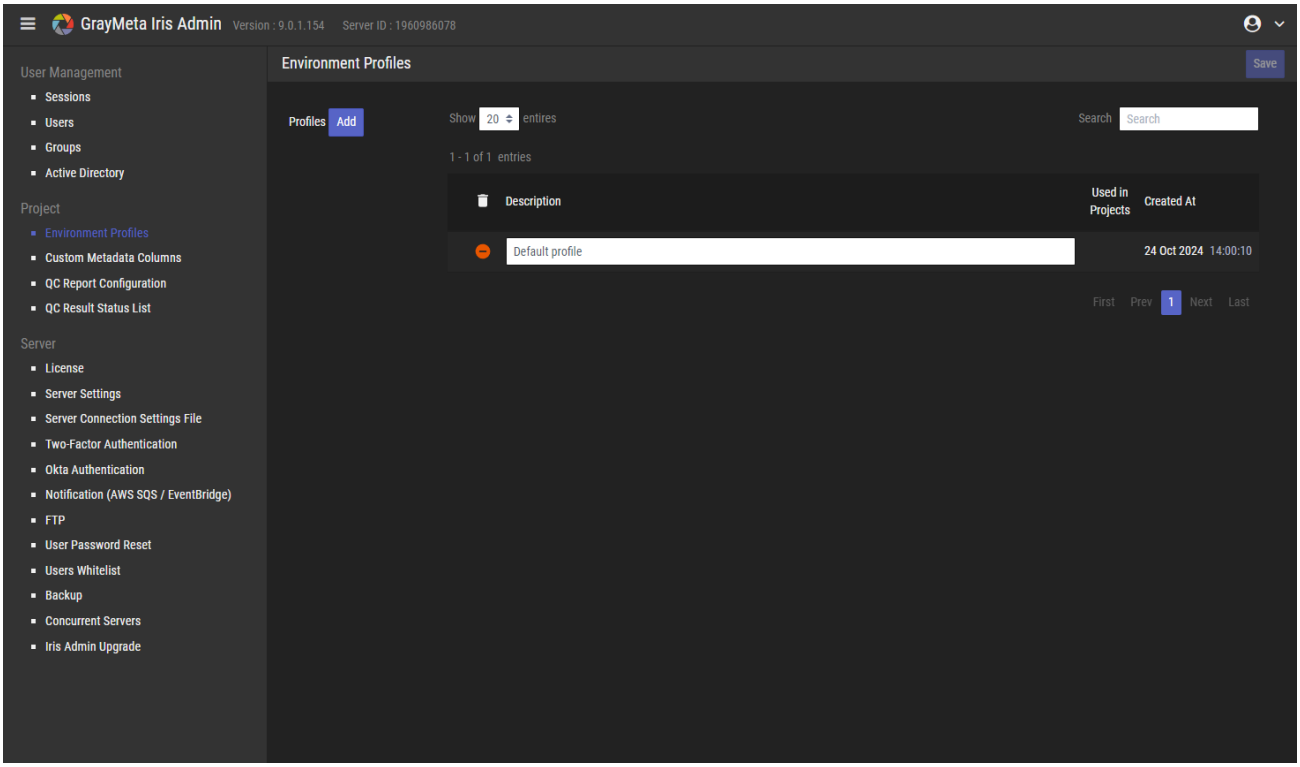
To enable a group, click the “+” button on the left and to disable it, click the same button. In the above screenshot, the Active Directory group called “Iris_Users” is enabled. This means that somebody who is a member of this group will inherit the group’s permissions. When a group has been enabled, each group permission can be toggled on or off. The group permissions can be saved by clicking the Save button on the top right.

Each group can be assigned an Iris user layout that determines the size and positioning of the windows in Iris. The benefit of this is to allow all users of the same group to share the same layout, for example, all users of a group that is responsible for work on audio could have the same layout with the audio tool windows already positioned in a specific location.

To assign a layout, it must be first exported to a .layout file in Iris (see the Iris user manual for details). The exported .layout file can then be assigned to the group by clicking the edit button. The trash bin button can be used to unassign the layout from the group. The changes can be saved by clicking the Save button on the top right.

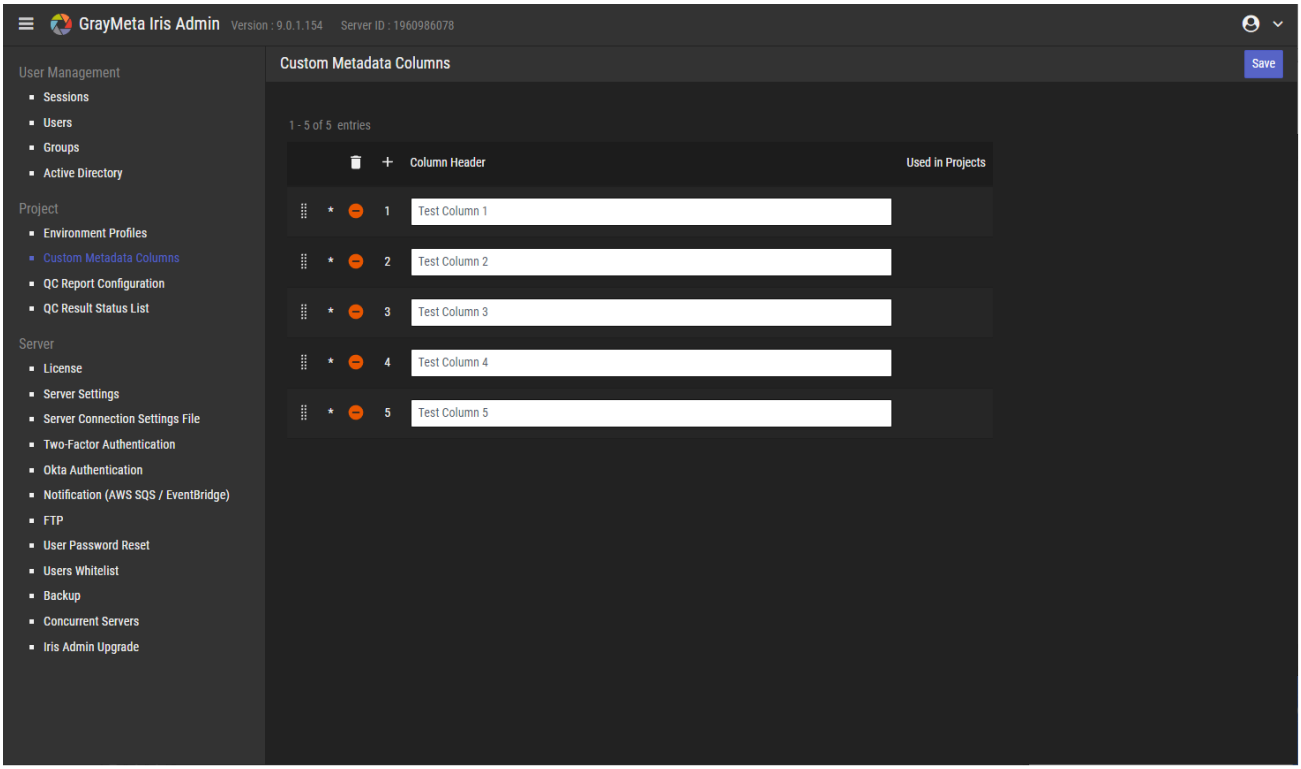
3.3 Project

3.3.1 Environment Profiles



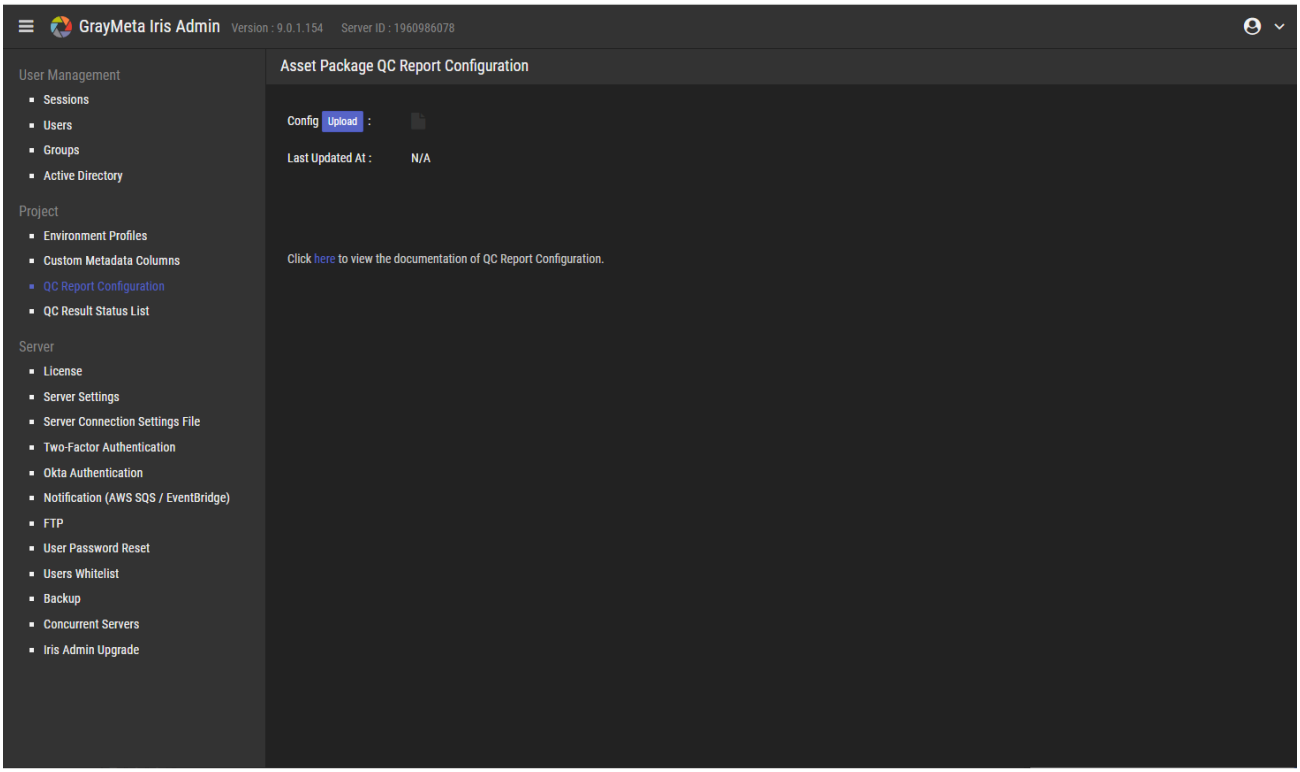
Here, a list of Environment Profiles data files can be uploaded and stored in Iris Admin. Environment Profiles data files are exported from Iris client and have the .profile file extension. The environment profiles stored in Iris Admin are used for asset packages in Iris Client. Each asset package can be associated with an Environment Profile, therefore opening the asset package will apply an environment profile associated with it.

3.3.2 Custom Metadata Columns



This enables the creation of extra metadata columns for each asset package that is shown in Iris. By default, each asset package in Iris will be associated with metadata such as frame rate, resolution, and so on. Extra customized metadata can also be added by creating new columns of data. The metadata for each custom metadata column can be set for each asset package through the API and displayed in Iris.

3.3.3 QC Report Configuration

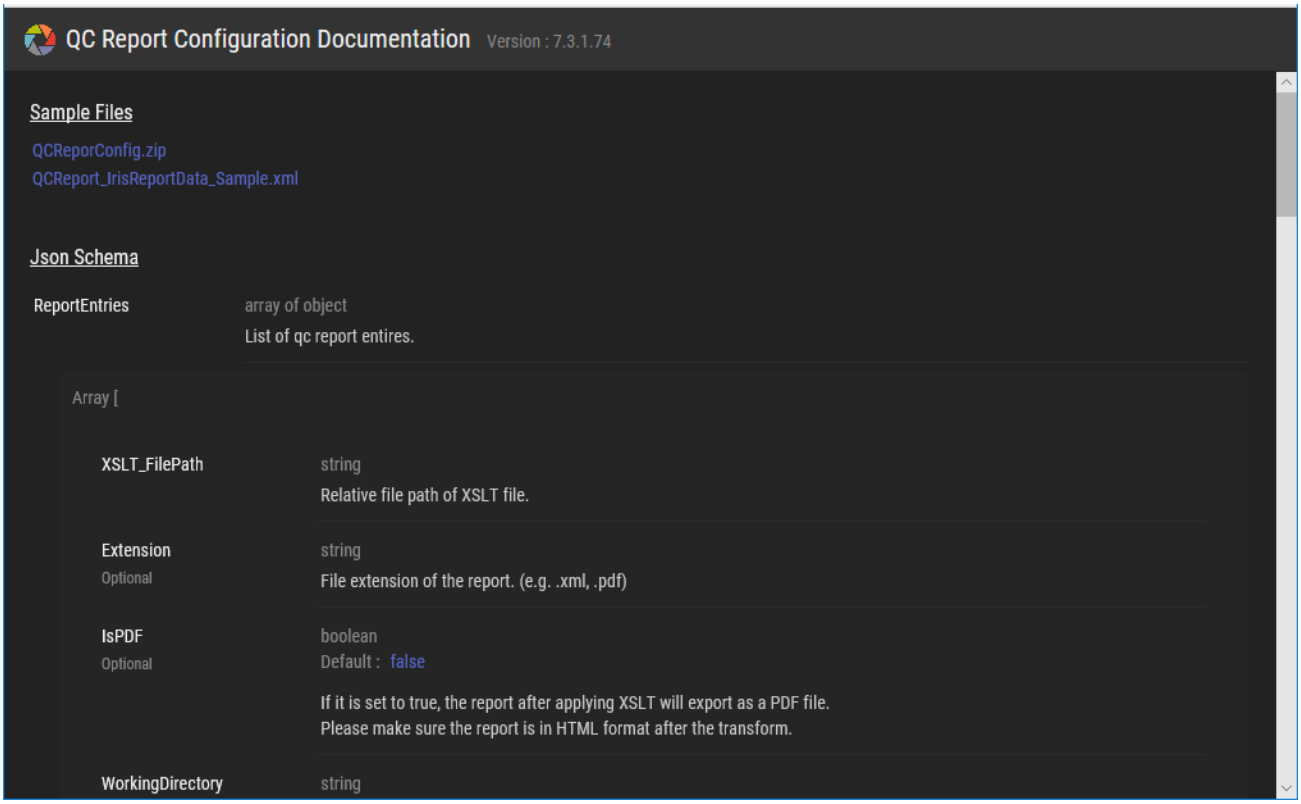


QC Reports are generated via a combination of an XML Report File and a QC Report Config File. The XML file contains metadata stored in XML format and the QC Report Config File contains information on how to transform the data of the XML Report File into another format such as PDF.

The first step that is required is to import the QC Report Config file in Iris Admin. Note that this will replace any previous config files. The files are in .zip format and contain .json and .xslt files to customize the metadata in the QC Report XML files that are generated in Iris Admin. For example, this can be used to transform the Iris-generated XML file into a PDF file.

By default, Iris Admin will have a sample QC Report Config file already imported which means that a PDF report can already be generated from within Iris Client, based on this sample QC Report Config file. For customized QC Report Config files, these can be provided by GrayMeta on a bespoke basis or by user modification of the sample QC Report Config file.

The sample QC Report Config file can be downloaded by going to the QC Report Configuration section of Iris Admin, clicking on the link to view the QC Report documentation:



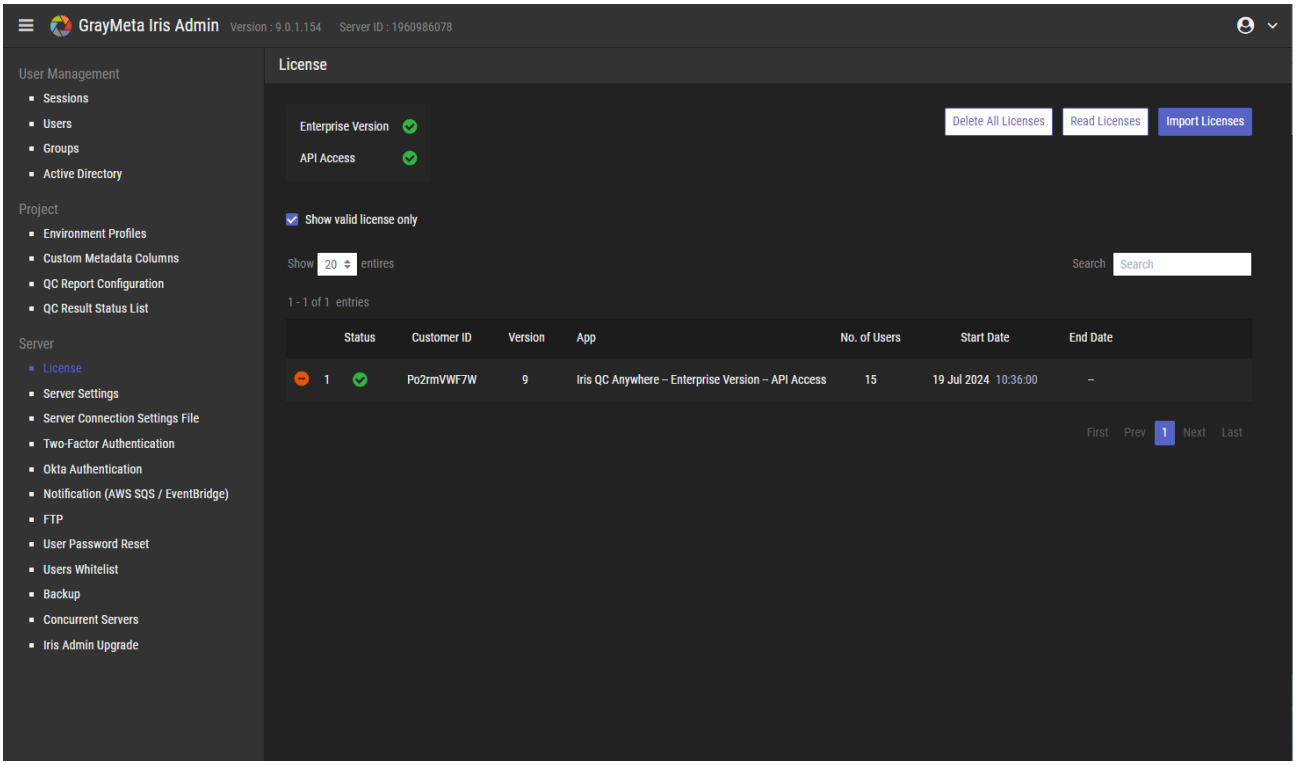
Also available for download is a file called QCReport_IrisReportXml_Sample.xml. This sample contains all possible parameters available and serves as a guide for the user to create their own QC Report Config file.

The steps involved in customizing the default QC Report is:

- Generate the report XML file in Iris Client (see the Iris Client User Manual for details on how they are generated).
- Upload a QC Report Config file into Iris Admin.
- Once this has been uploaded successfully, the “Generate QC Report” context menu in iris Client will show new entries that allows generation of QC reports. These reports will be generated based on the xslt transformations contained within the QC Report Config file.

3.4 Server

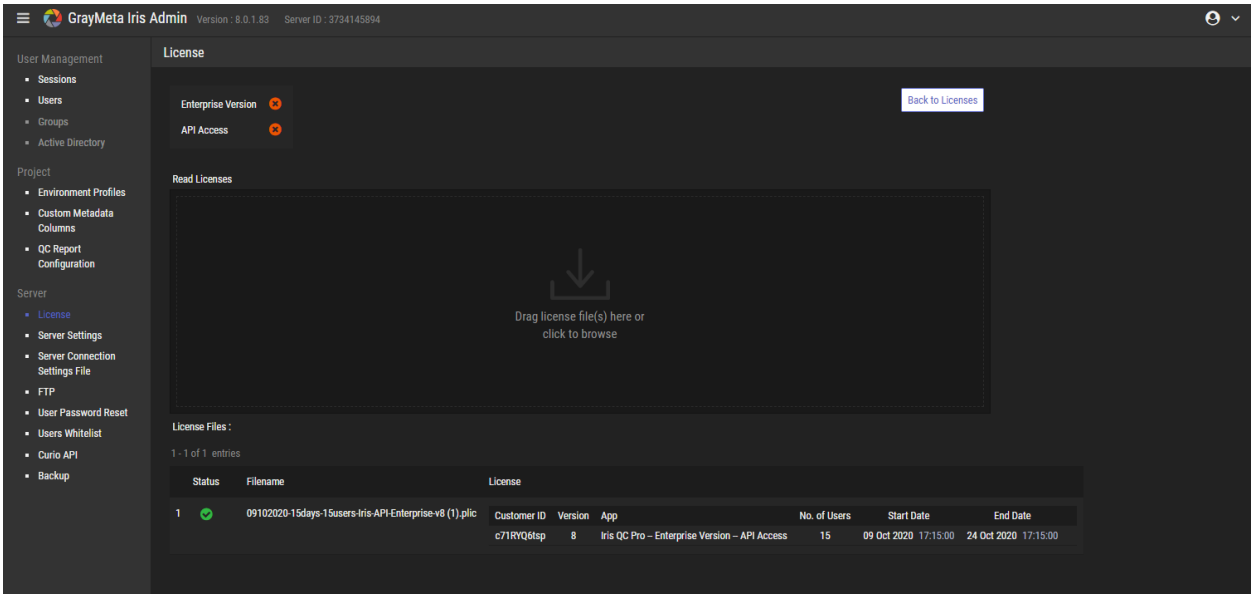
3.4.1 License



This screen shows a current list of Iris Licenses that have been successfully registered in Iris Admin. To import an Iris Admin license (with the extension .plic), click the Import License button and either:

- Drag and drop the .plic license file into the drop zone
- Click the drop zone to select the .plic license file to import

The Read License option operates in the same way as Import License but its function is to read the license file without performing an import and displaying details of the license file:

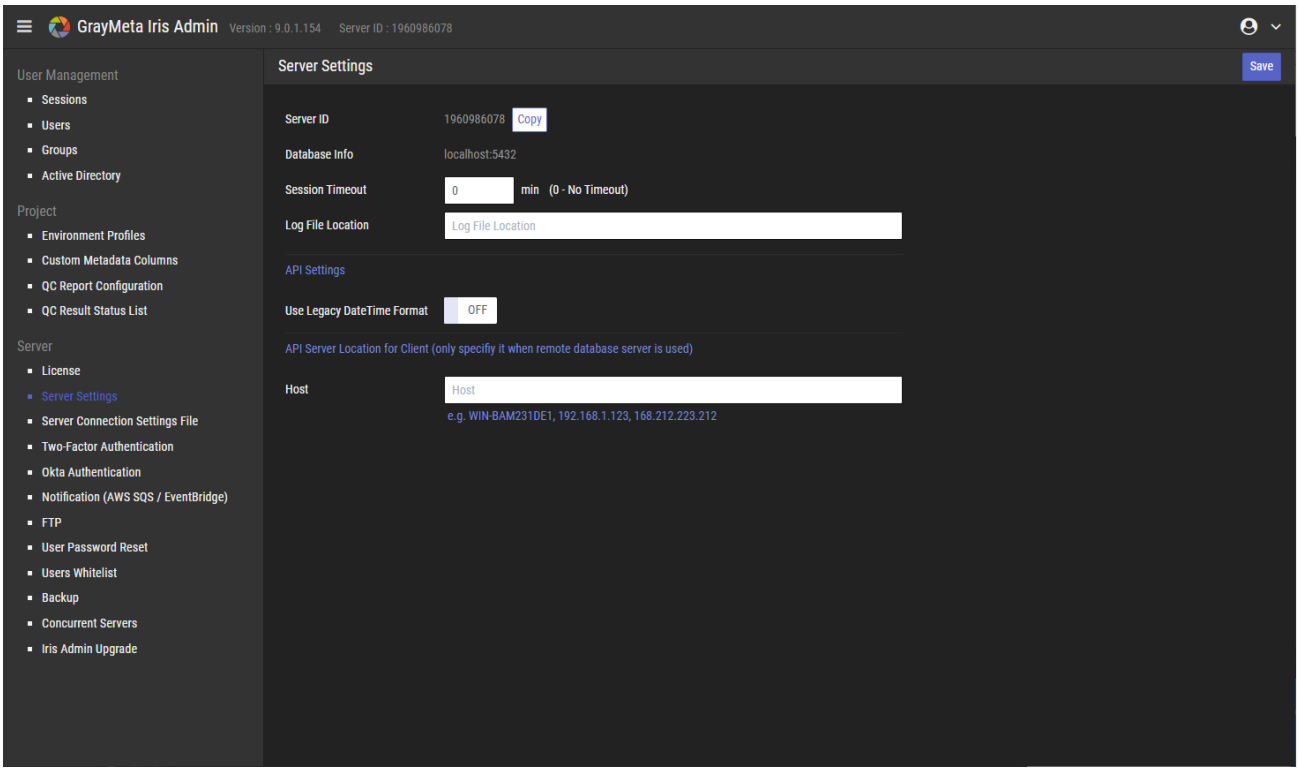


3.4.1.1 Auto Import Licenses

As well as importing licenses from the web interface, .plic license files can also be placed in the directory **C:\Users\Public\Documents\GrayMeta\Iris Server\License\ForImport**

Once a user attempts to sign in, Iris Admin will pick up the .plic files and import them automatically. The .plic files will be moved to **C:\Users\Public\Documents\GrayMeta\Iris Server\License\Imported**

3.4.2 Server Settings



This page shows server side information and settings.

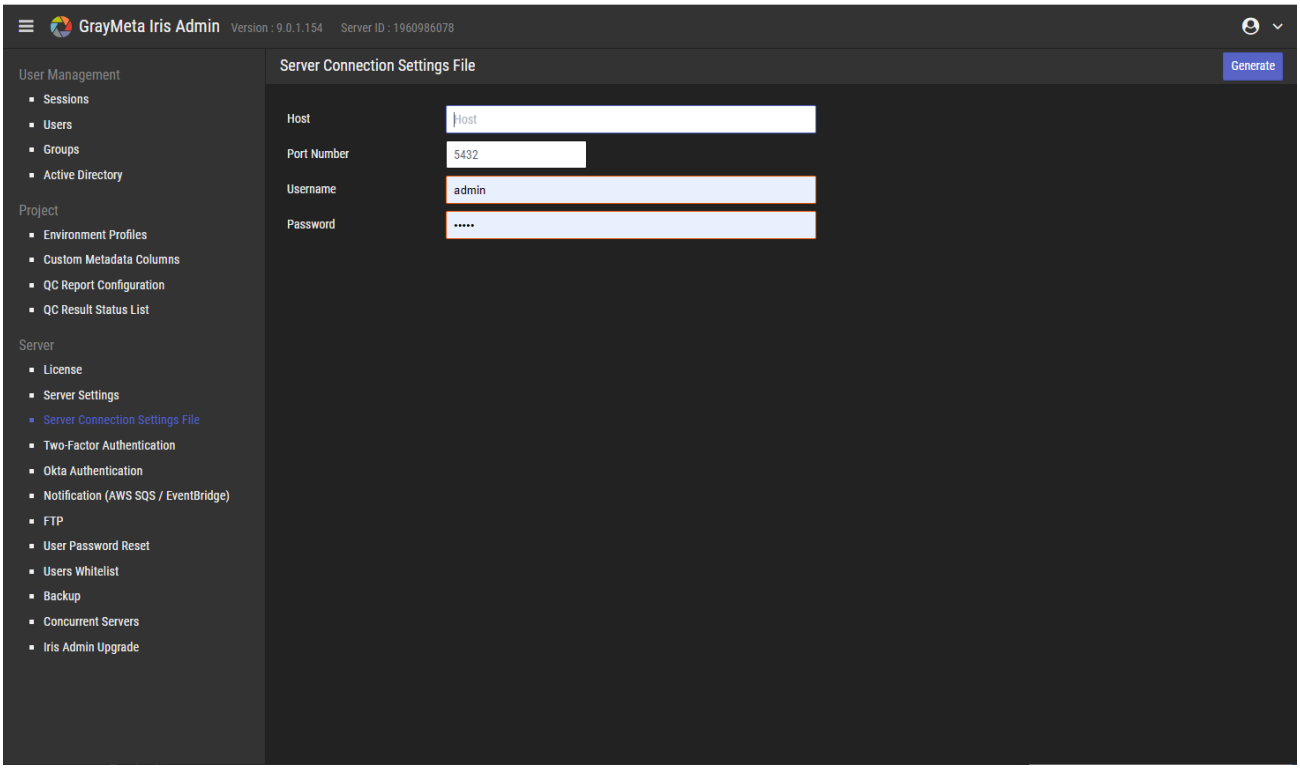
The Server ID is a value that uniquely identifies the machine in which the server is running. This ID is required by GrayMeta when generating server licenses that are to be imported (see 3.4.1 for information on importing licenses). From version 7, all Iris Admin licenses requests to GrayMeta will require the Server ID to be provided.

The Session Timeout option allows a user to specify the number of minutes of inactivity before Iris automatically logs out the user. Choose a value of 0 to disable this.

Log File Location specifies where log files will be stored (if not specified, the default will be in C:\Users\Public\Documents\GrayMeta\Iris Server\logs). See Appendix 2 for more information on the log files.

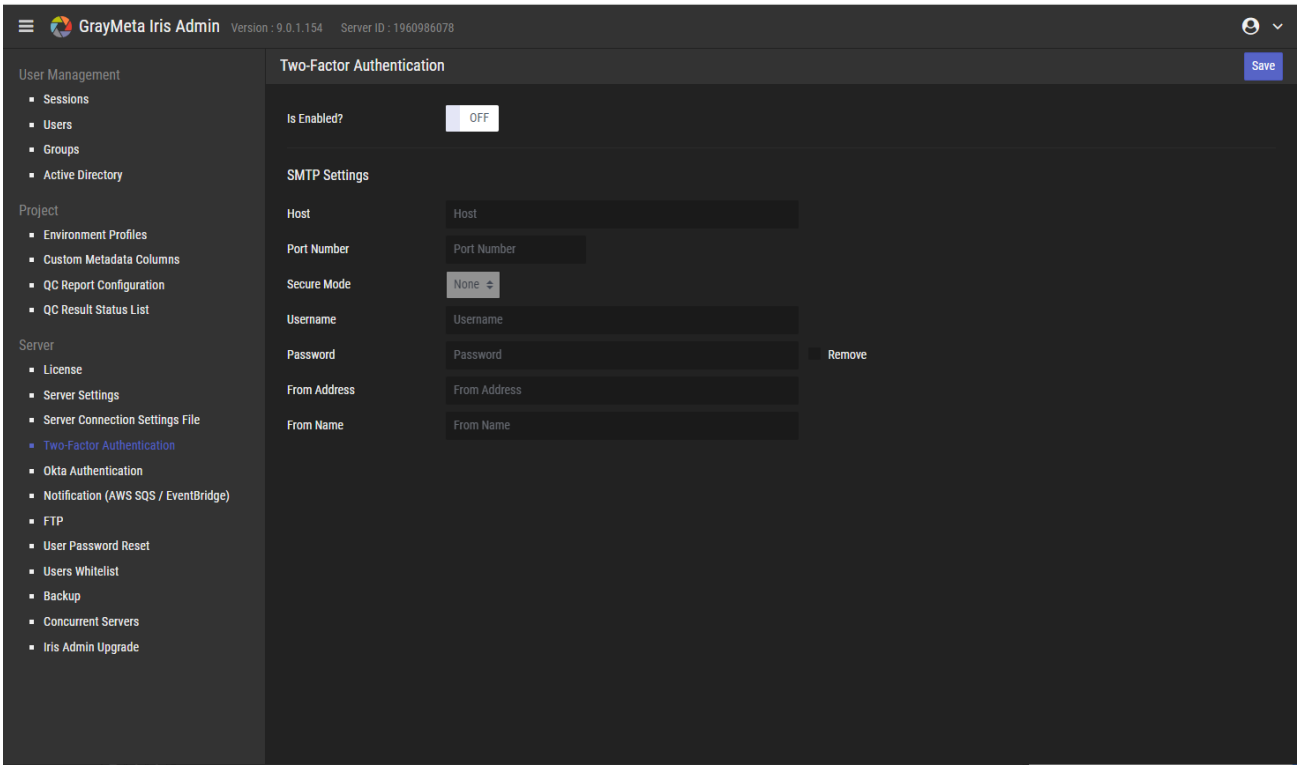
The setting for API location for client is used to specify the host name of the database in which the API needs to connect to. This is only required where the database is not located on the same machine as the Iris Admin server.

3.4.3 Server Connection Settings File



When logging in as a user in Iris or when using an Iris Admin License, Iris needs to make a connection to the Iris Admin database. The database connection settings can be entered here and generated as a .dbs file. This file can then be imported from Iris via Options -> Server Settings.

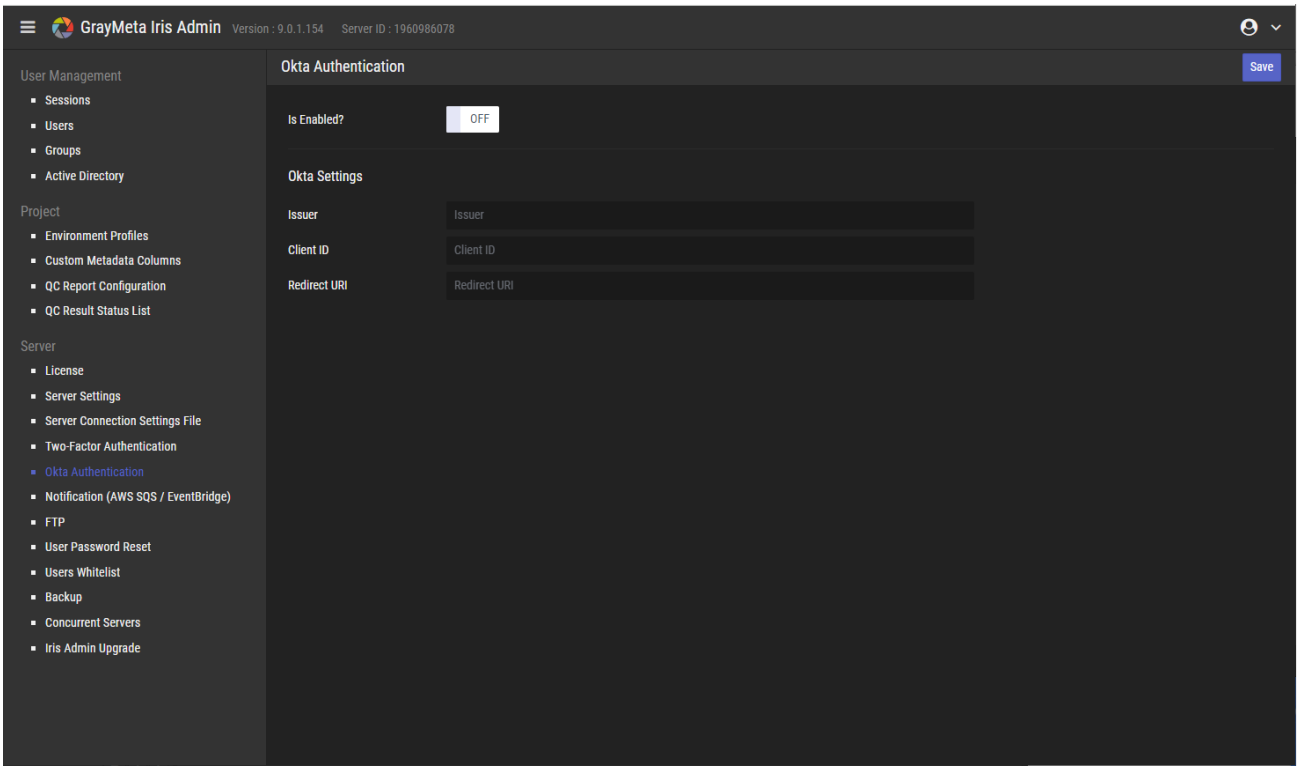
3.4.4 Two-Factor Authentication



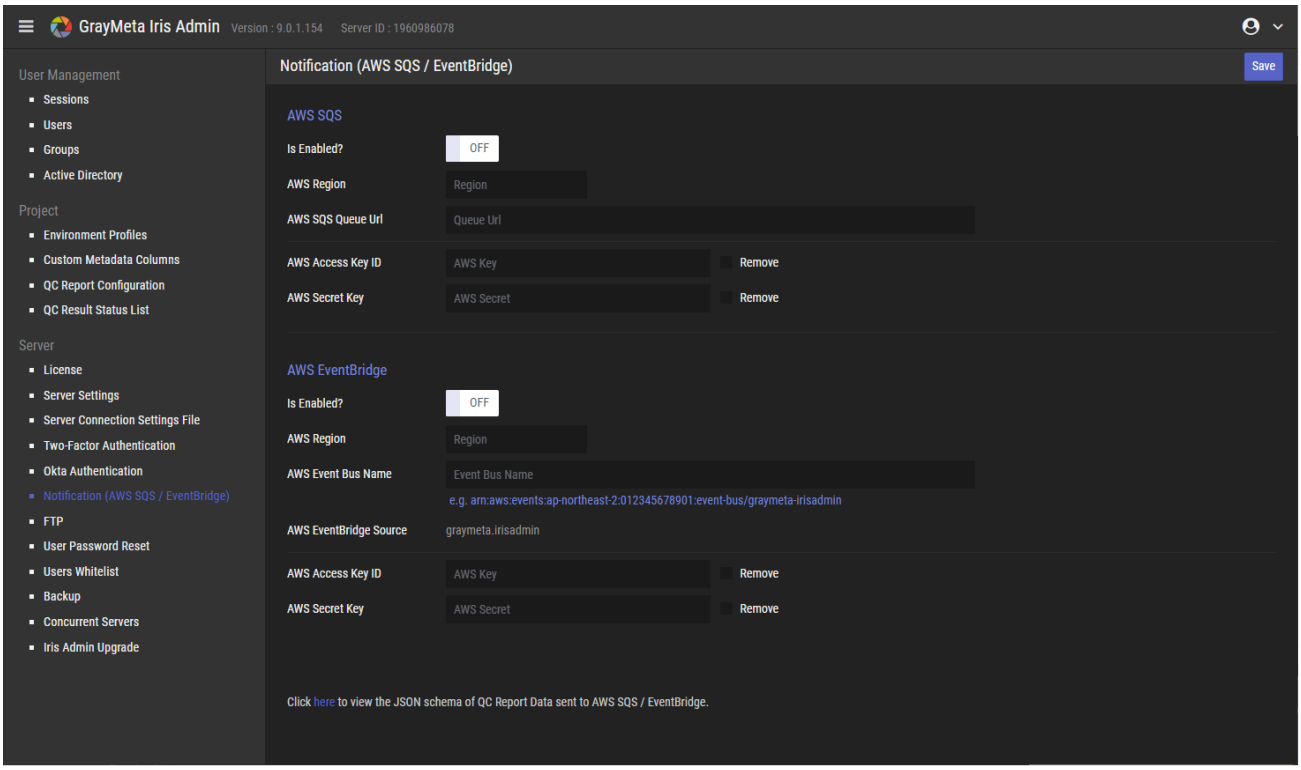
This page allows two-factor authentication to be switched on/off. Since two-factor authentication requires sending of a code via email, the email SMTP settings must be set up here to enable two-factor code to be sent.

3.4.5 Okta Authentication

This page allows Okta authentication to be enabled or disabled, along with the settings for Okta.

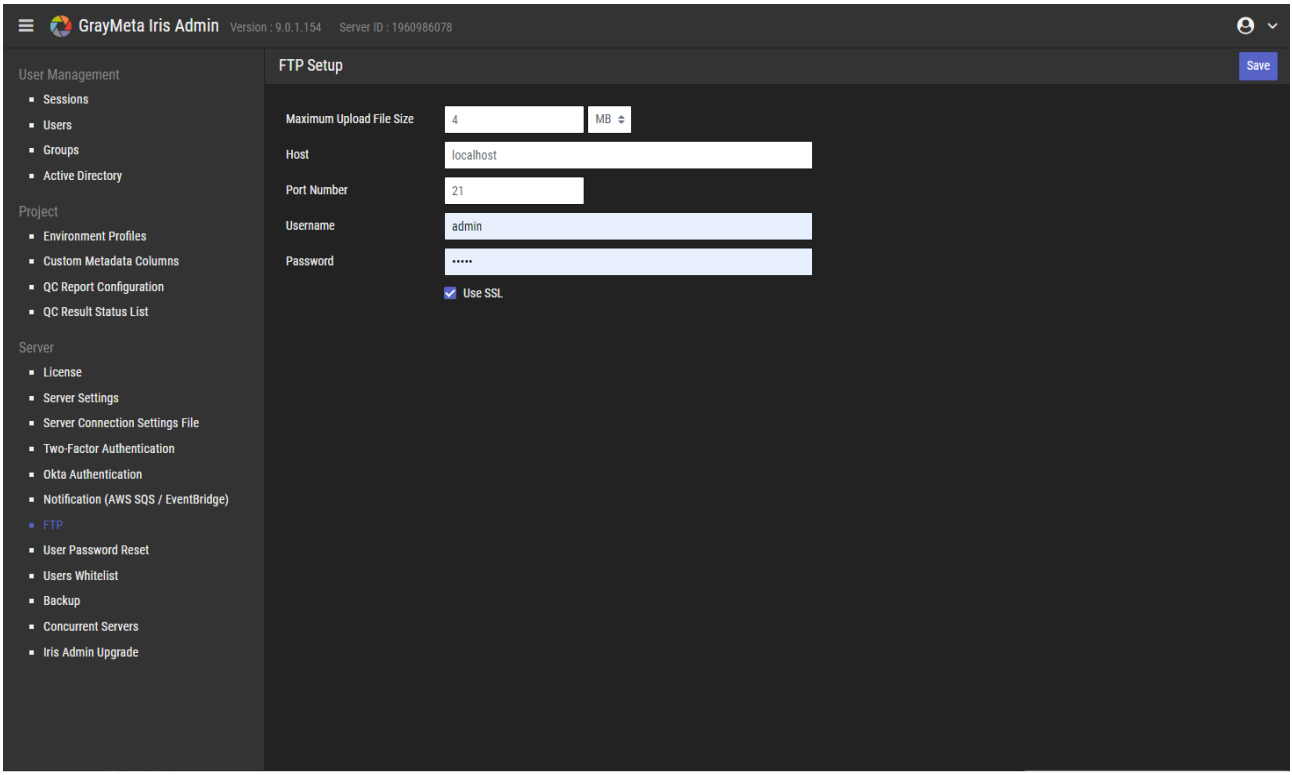


3.4.6 Notification (AWS SQS / EventBridge)



Within Iris Client, there is the ability to generate reports and to specify results for the reports. It is possible to send these results to AWS SQS and AWS EventBridge. This page provides the necessary settings to configure AWS SQS and AWS EventBridge services.

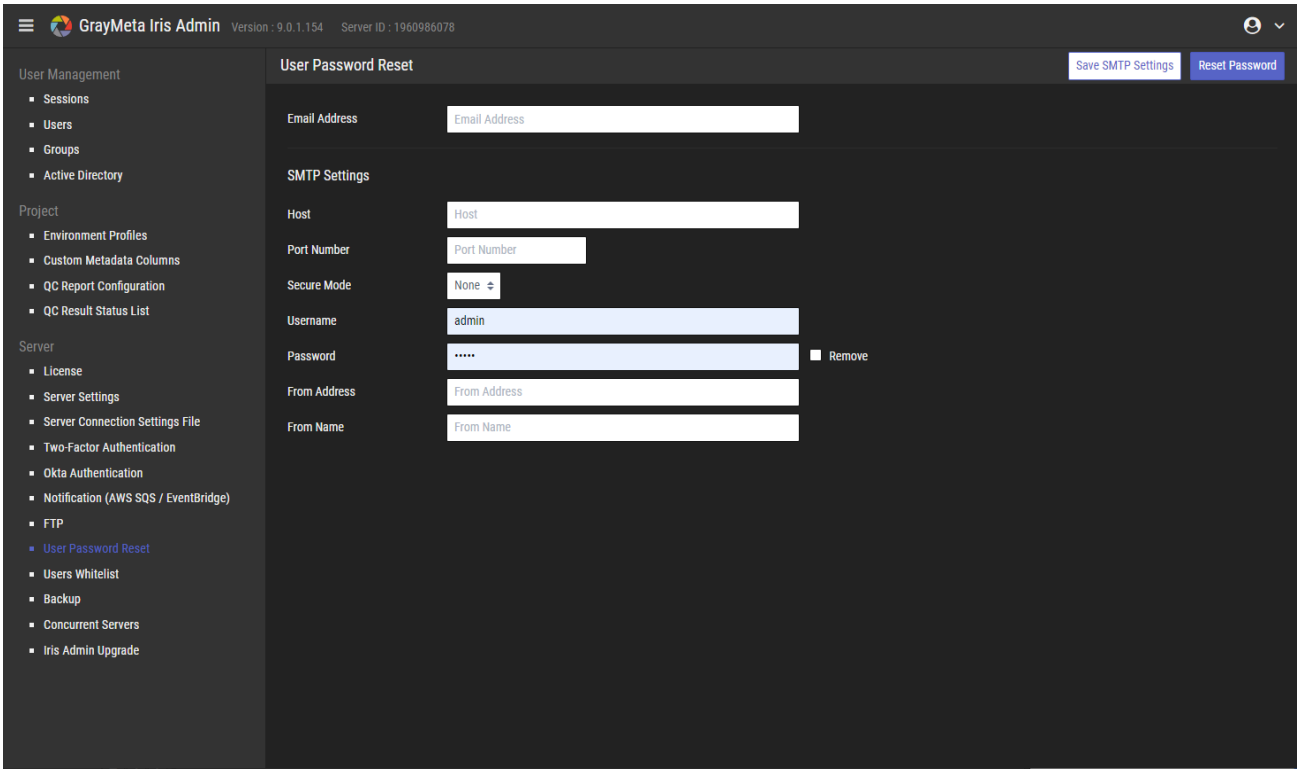
3.4.7 FTP Setup



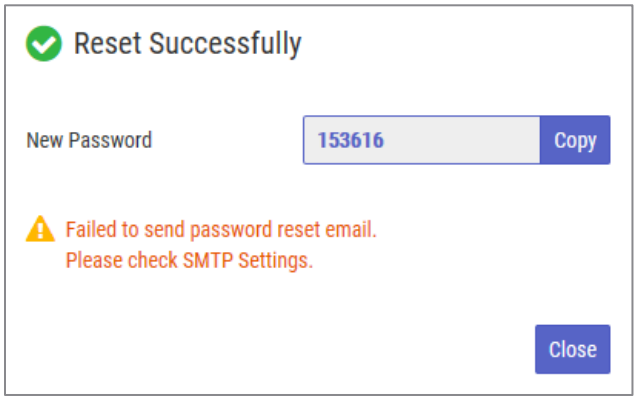
If you wish to send attachments during an Iris collaboration session, you will need to point Iris to the Filezilla FTP server that will be used to handle the upload and download of attachments. In FTP Setup, enter the Host, Port Number, Username, Password to connect to the Filezilla FTP Server. Specify SSL if the connection is to be SSL encrypted and Filezilla Server has been configured to use a valid SSL certificate. The size of file uploads can be controlled via the Maximum Upload File Size setting. Click the Save button on the top right to save the settings.

Note: if the Filezilla Server was installed from the Iris Admin installer, the port number will have been pre-defined to be 6021 and SSL will be enabled.

3.4.8 User Password Reset

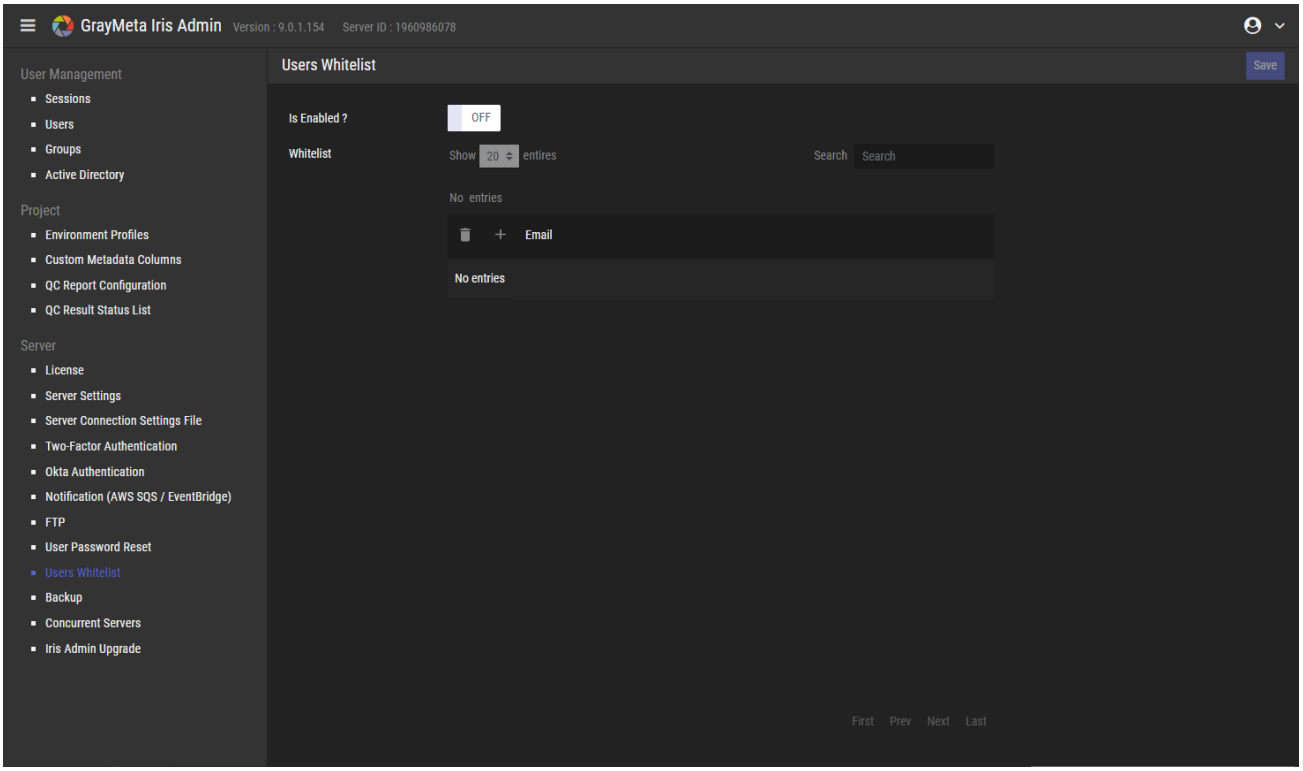


In order to reset a user's password, enter the email and click Reset Password. The new password will be shown:



In the above screenshot, the password could not be emailed to the recipient. If you want the password to be automatically emailed then the email SMTP settings are required.

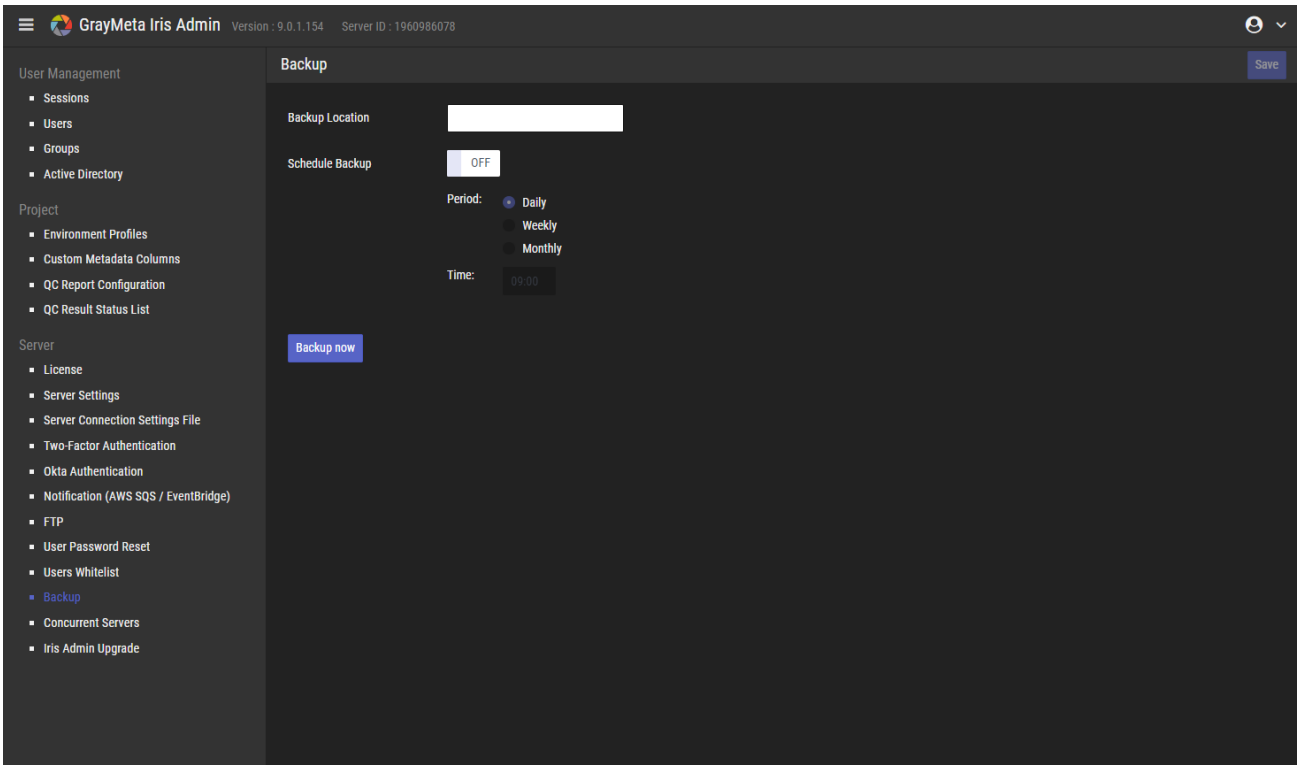
3.4.9 Users Whitelist



When the whitelist is enabled, only users specified in the whitelist can use the collaboration features of Iris. Everyone who is not in the whitelist will be blocked. The Users Whitelist section of Iris Admin Tools provides options to add and remove users from the whitelist. The whitelist can be switched on or off. Click the Save button on the top right to save the settings.

3.4.10 Backup

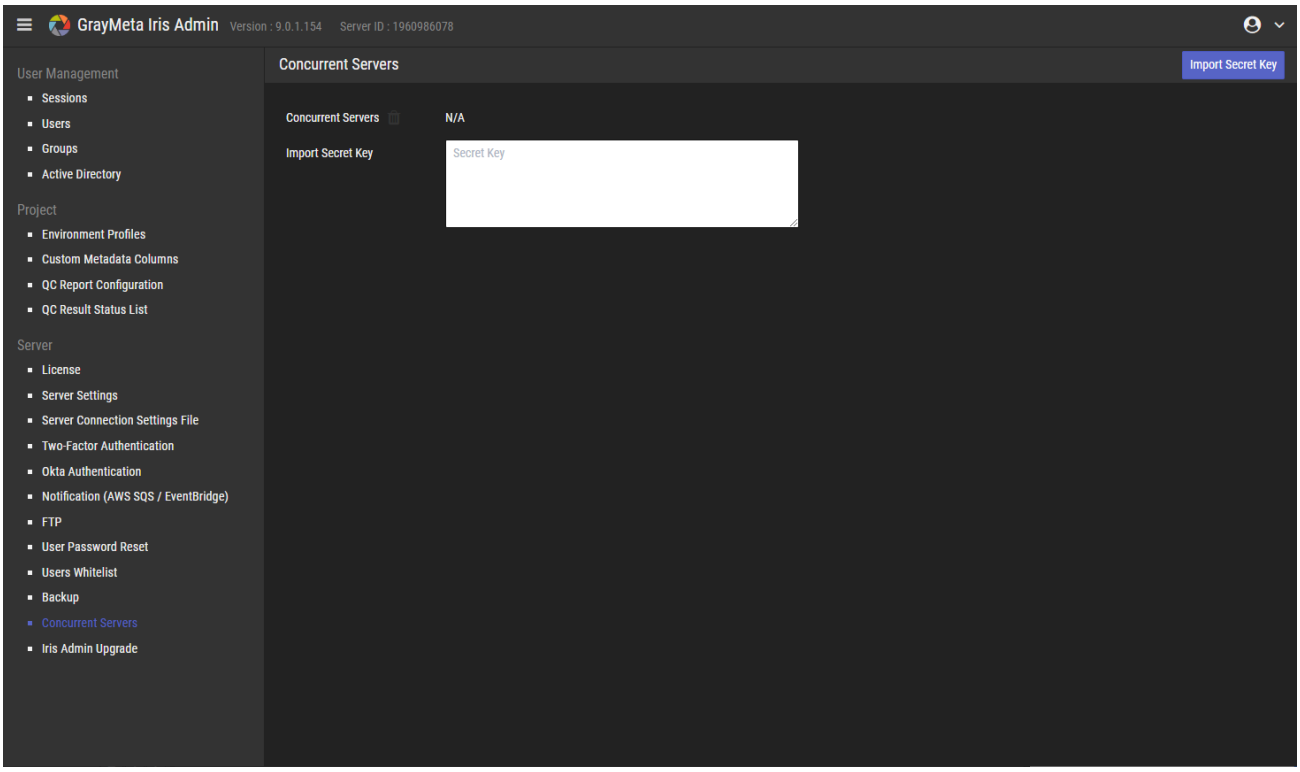
This option allows the database to be backed up either on demand or at scheduled intervals.



To back up the database on demand, click the “Backup Now” button. To schedule a backup, enable the “Schedule backup” button and select the backup interval (Daily, Weekly or Monthly) followed by the time in 24 hour format.

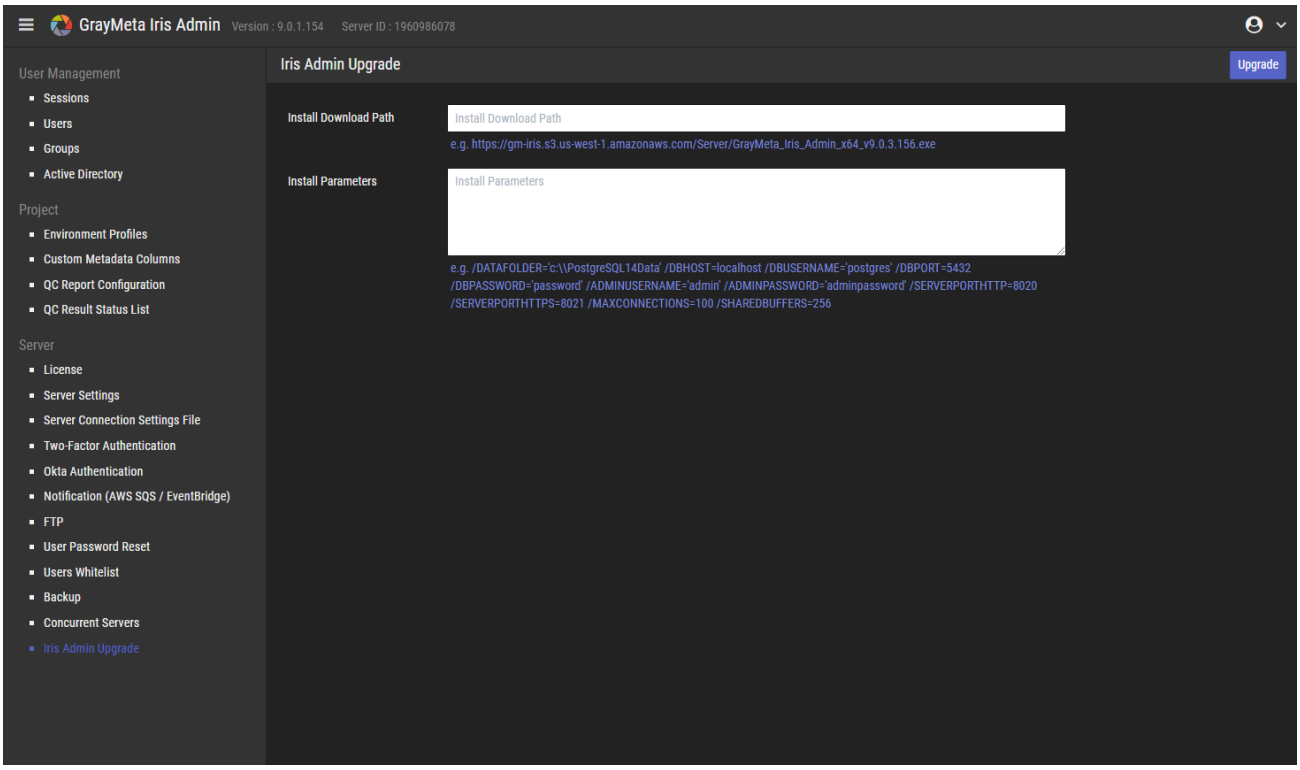
The last backup can be downloaded by clicking “Download Last File”. It is also possible to access all previous backups by going to the folder location **%public%\Documents\GrayMeta\Iris Server\Backup**

3.4.11 Concurrent Servers



For multiple Iris Admin servers connected to the same database, a secret key is required to allow this type of deployment. The secret key is available from GrayMeta upon request.

3.4.12 Iris Admin Upgrade



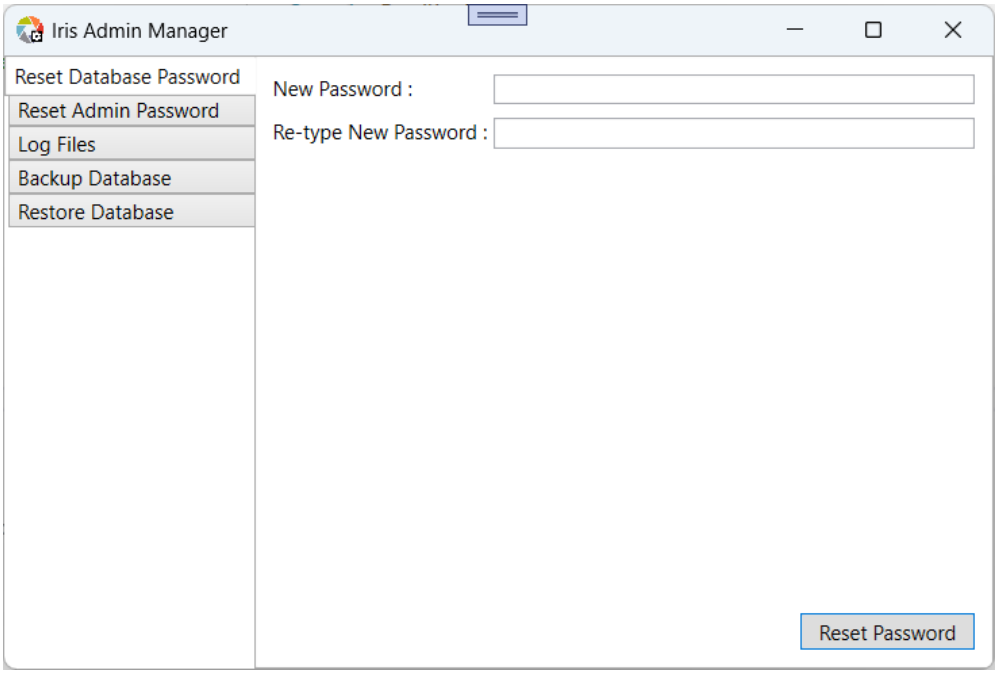
It is possible to update Iris Admin to newer versions from this page. By entering the url of the download path and specifying the required installation parameters, Iris Admin can be automatically downloaded and installed using the specified parameters.

4 Appendices

4.1 Appendix 1: Configuring Port Numbers

There are 2 ports that are used for the Iris Admin web interface and these are specified during the install. Both of these ports can be modified in the nginx.conf file that exists in C:\Program Files\GrayMeta\GrayMeta Iris DB\Postgres\IrisWebServer\nginx\conf. It is a text file that can be opened in Notepad. After the nginx.conf file has been modified, restart the Windows service “GrayMeta Iris Web Server”

4.2 Appendix 2: Iris Admin Manager



Iris Admin Manager provides administrative tools for Iris Admin. This application allows

- The database password to be reset
- The admin password to be reset
- View and export log files
- Backup the database
- Restore the database

The Iris Admin installer does not create a shortcut for Iris Admin Manager. The application is called IrisAdminManager.exe and has to be run the installed location.