



Iris[™] media solutions

User Manual
Iris Admin
Version 8.9.0.122



Contents

1	Introduction	3
1.1	Overview.....	3
2	Installation.....	4
2.1	Installing GrayMeta Iris Admin	4
2.1.1	Unattended Install.....	4
2.1.2	Attended Install	4
3	Iris Admin Tools	0
3.1	User Management	1
3.1.1	User Sessions.....	1
3.1.2	Users	1
3.1.3	Groups.....	3
3.2	Active Directory.....	5
3.2.1	Use of Active Directory Credentials for OKTA SSO and Iris API	6
3.2.2	Licensing	6
3.2.3	Configuring Group Permissions	6
3.3	Project	9
3.3.1	Environment Profiles.....	9
3.3.2	Custom Metadata Columns.....	10
3.3.3	QC Report Configuration	11
3.4	Server	13
3.4.1	License	13
3.4.2	Server Settings	14
3.4.3	Server Connection Settings File.....	15
3.4.4	Two-Factor Authentication	15
3.4.5	FTP Setup	16
3.4.6	User Password Reset	17
3.4.7	Users Whitelist.....	18
3.4.8	Curio API	19
3.4.9	Backup.....	19
4	Appendices	20
4.1	Appendix 1: Configuring Port Numbers	20

4.2 Appendix 2: Iris Admin Manager 21



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

2.1.1 Unattended Install

Run the installer from the command prompt with the following parameters:

```
/S /DATAFOLDER=<database folder location> /DBUSERNAME=<database username>  
/DBPORT=<database port number> /DBPASSWORD=<database password>  
/ADMINUSERNAME=<web GUI admin username> /ADMINPASSWORD=<web GUI admin  
password> /MIGRATEDB=0/1
```

Note that this will overwrite any previous Iris Admin installations.

/S = silent install

/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

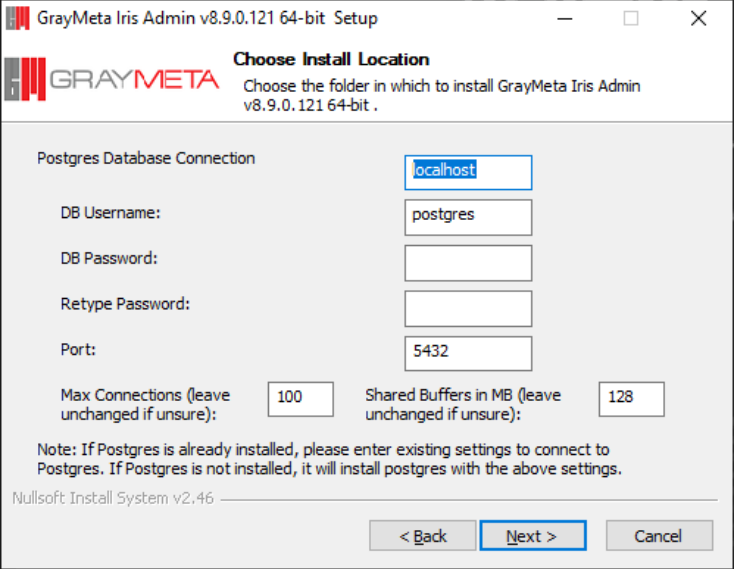
/SERVERPORTHTTP = The port number of the Iris Admin's HTTP web interface

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

2.1.2 Attended Install

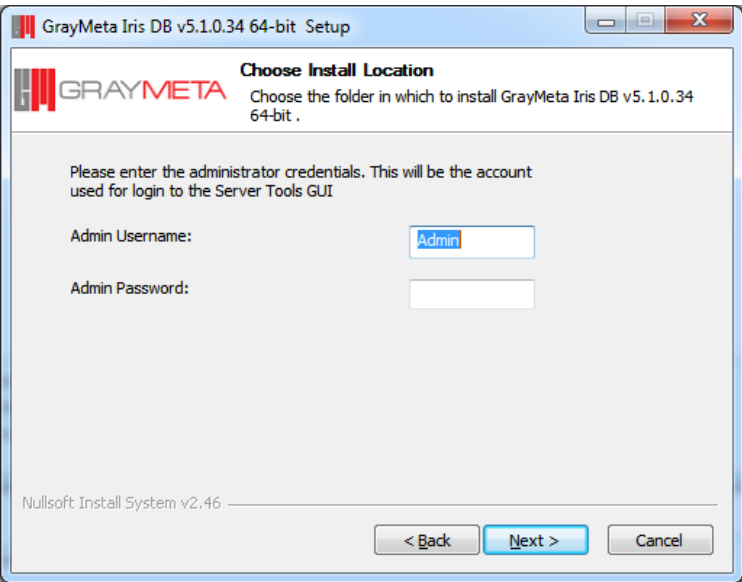
- a) If a previous version of Iris Admin is installed, you will be prompted to uninstall it first.
- b) During install, you will be asked for database credentials, i.e. username, password, port number. The Max Connections setting determines the maximum number of connections to the database server and 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.

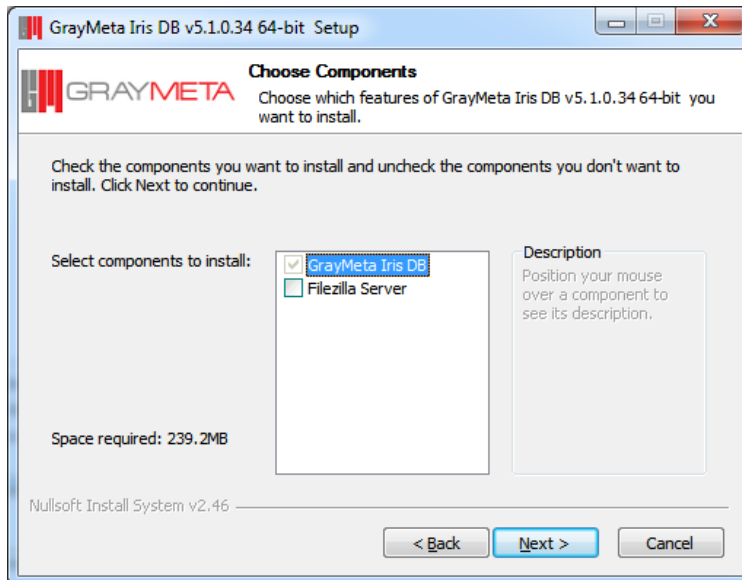


It is important that you do not lose the database username and password because this information will be required to be entered into Iris's options to allow it to connect to the database. Furthermore, it is also required when installing future versions of Iris Admin where a database update may be necessary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

- 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.



- d) The next stage is to select the components to install. One of the components is Filezilla Server and is optional.



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.

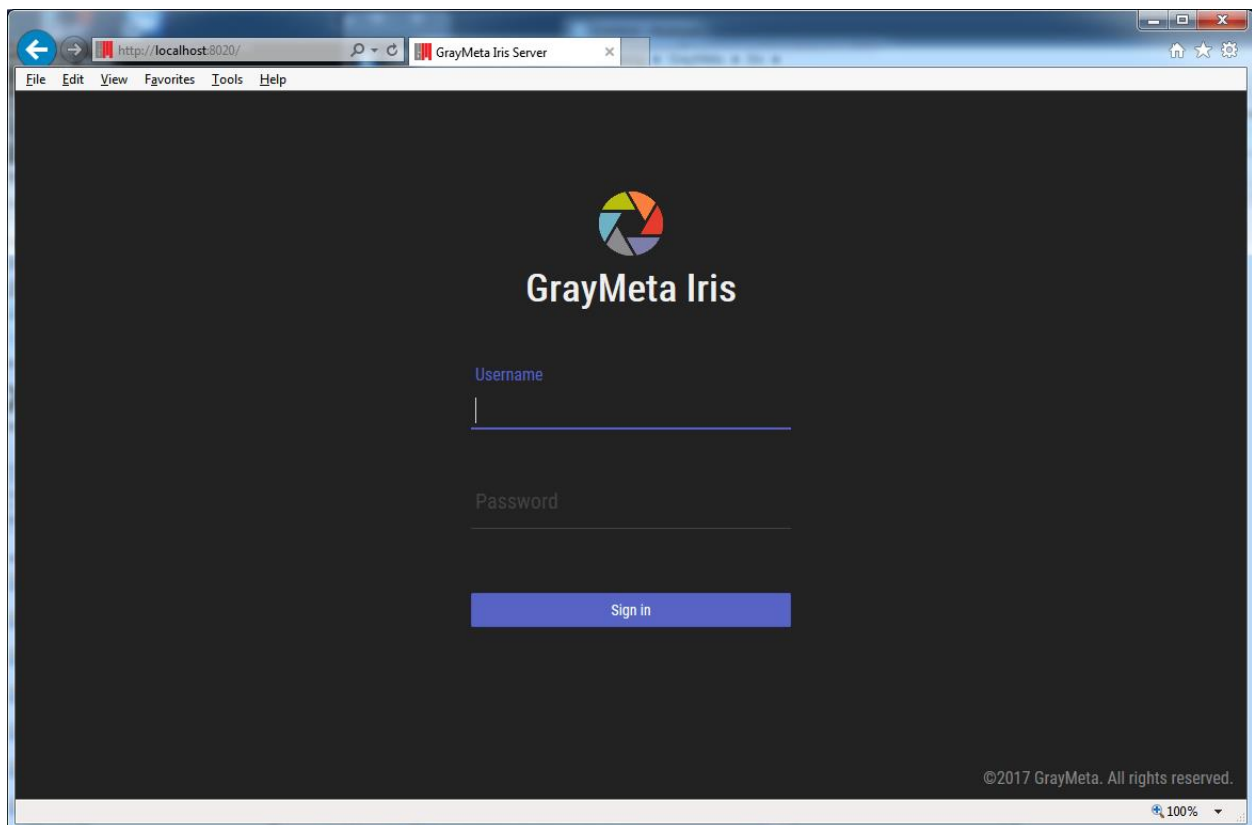
- e) Allow the installer to continue and when it is complete, the Iris Admin tools will be available on the desktop.

3 Iris Admin Tools

The Iris Admin Tools is a web-based GUI that provides management of the following:

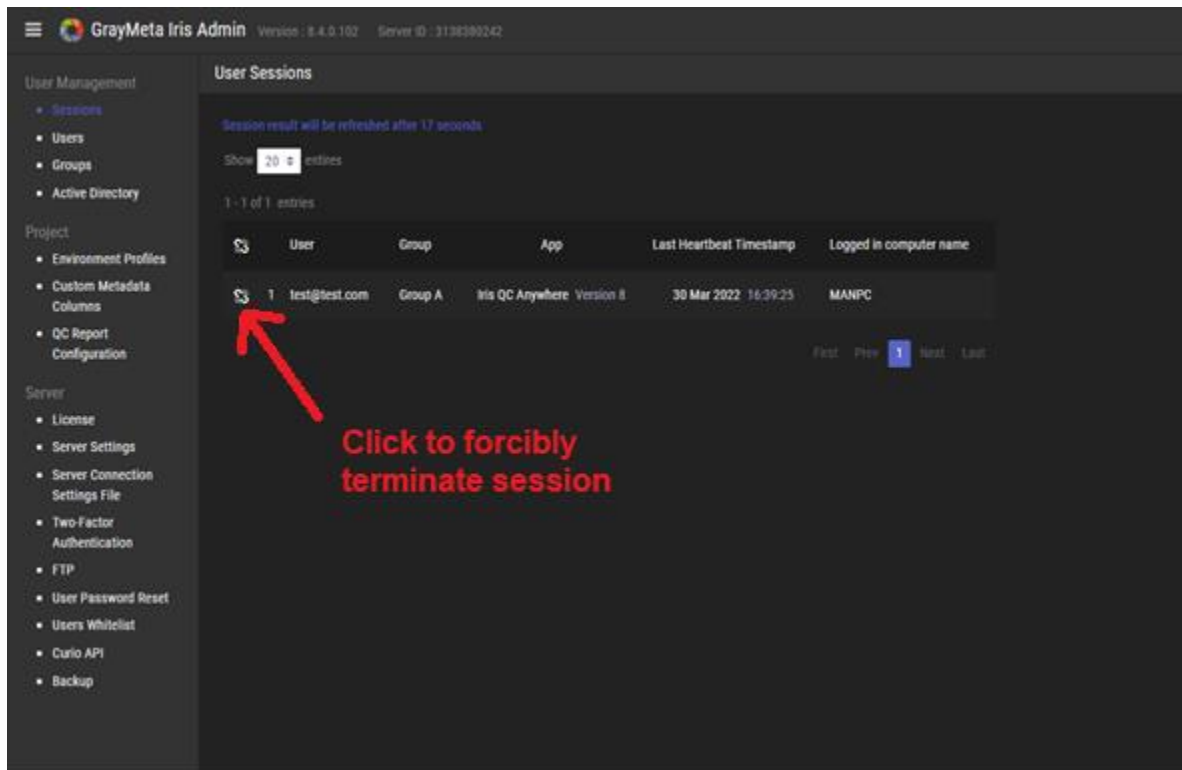
- Iris License Importer
- Password Reset
- FTP Setup
- User Whitelist Configuration
- Active Directory
- Users and Groups
- QC Reports
- Database connection settings

Use of the Iris Admin Tools require log in via an account that is specified during the Iris Admin installation. To access the Iris Admin Tools, 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



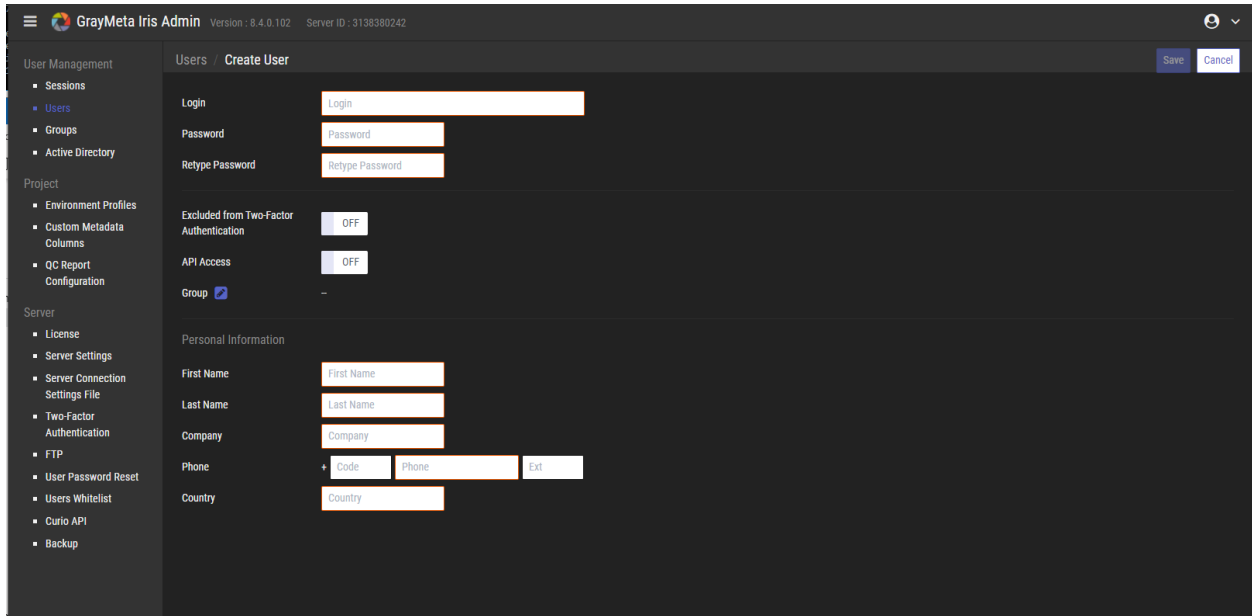
The screenshot displays the GrayMeta Iris Admin interface. The left sidebar contains navigation options under 'User Management', 'Project', and 'Server'. The main content area is titled 'User Sessions' and shows a table of active sessions. A red arrow points to a 'broken link' icon in the first column of the table, with a red text overlay that reads 'Click to forcibly terminate session'.

User	Group	App	Last Heartbeat Timestamp	Logged in computer name
test@test.com	Group A	Iris QC Anywhere Version 8	30 Mar 2022 16:39:25	MANPC

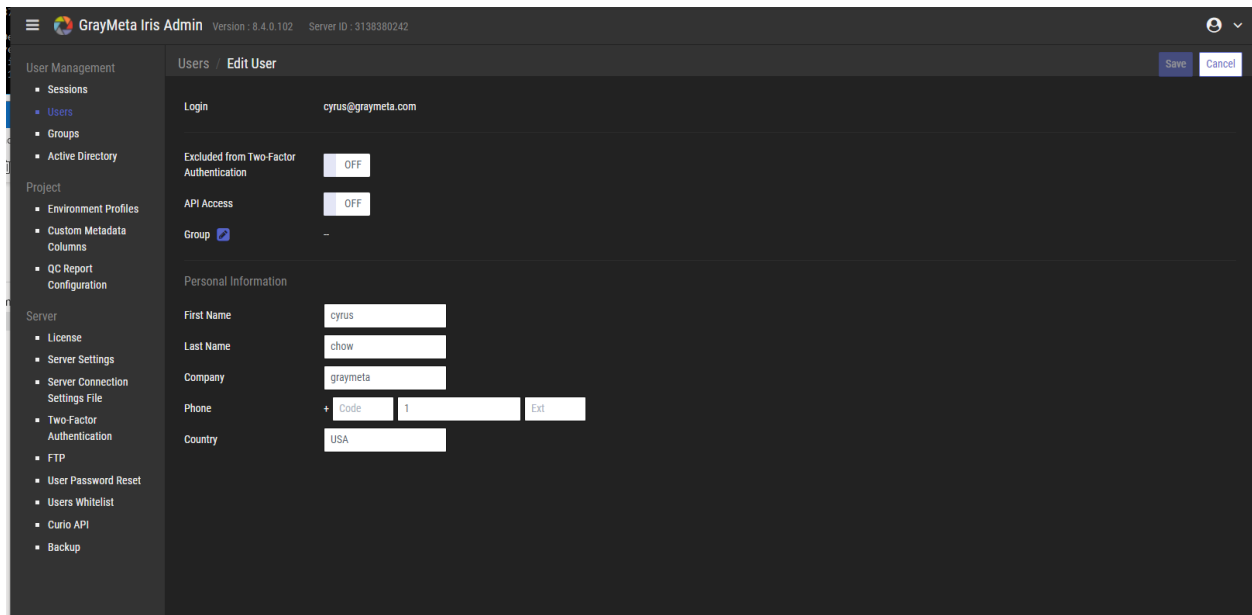
The list of Iris application client user sessions is shown here. Sessions can be closed by clicking the little icon button at the first column of the table. A session can be forcibly terminated by clicking on the “broken link” icon as shown above.

3.1.2 Users

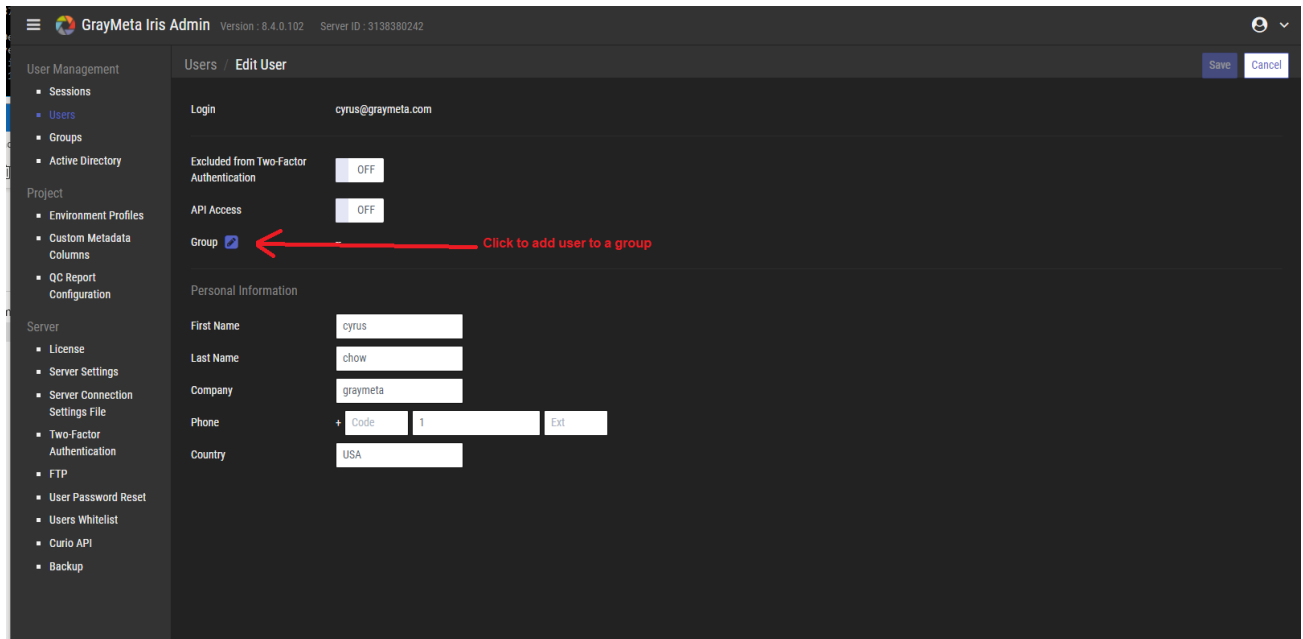
The list of Iris users is shown here. A new user can be created here (as well as from within the Iris application). To create a new user, click the “Create” button located at the top right.



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.



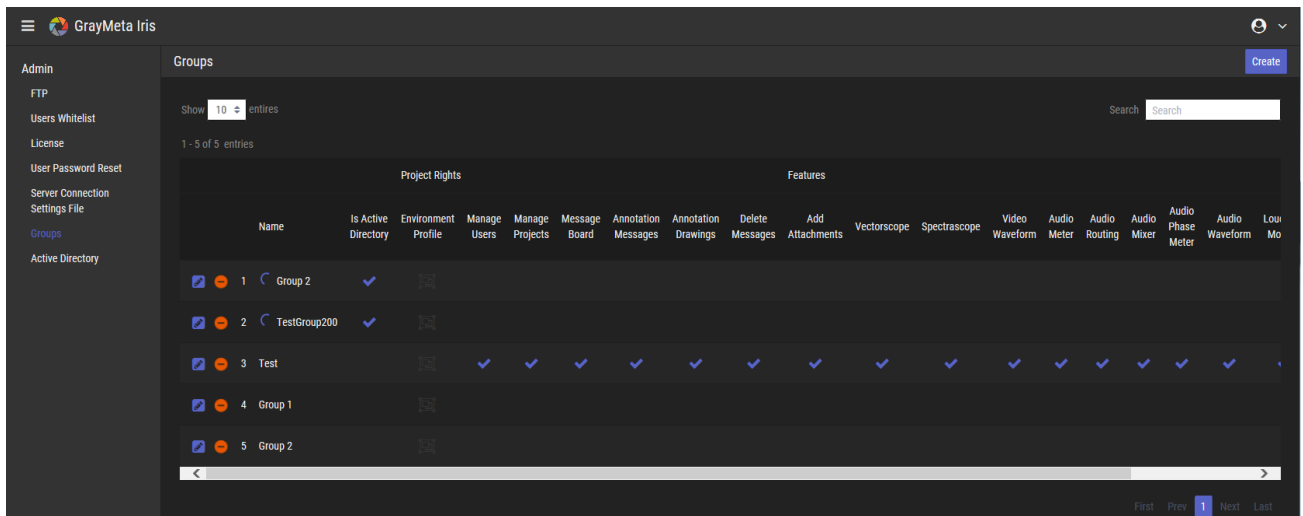
When editing user details, the user can be added to an Iris group.



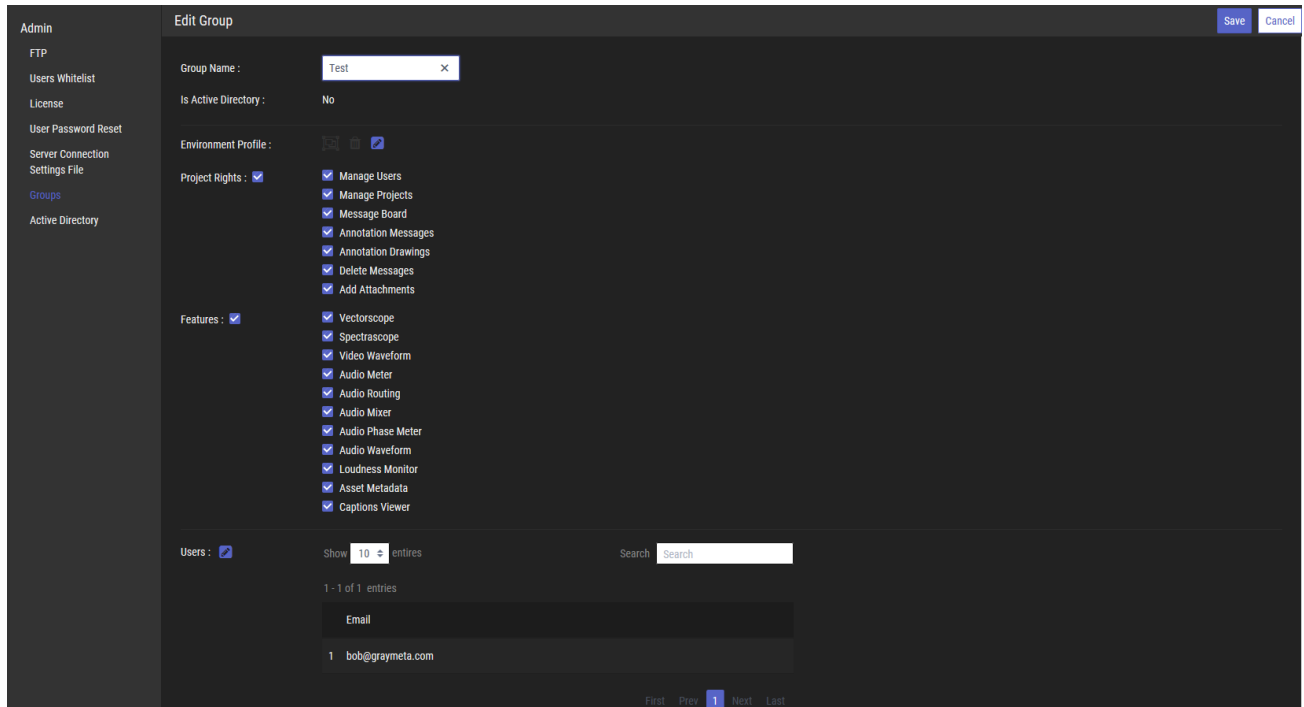
Each user has a setting to enable/disable access to the API and to be excluded from two-factor authentication. The default for both these settings are off.

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 Iris features.



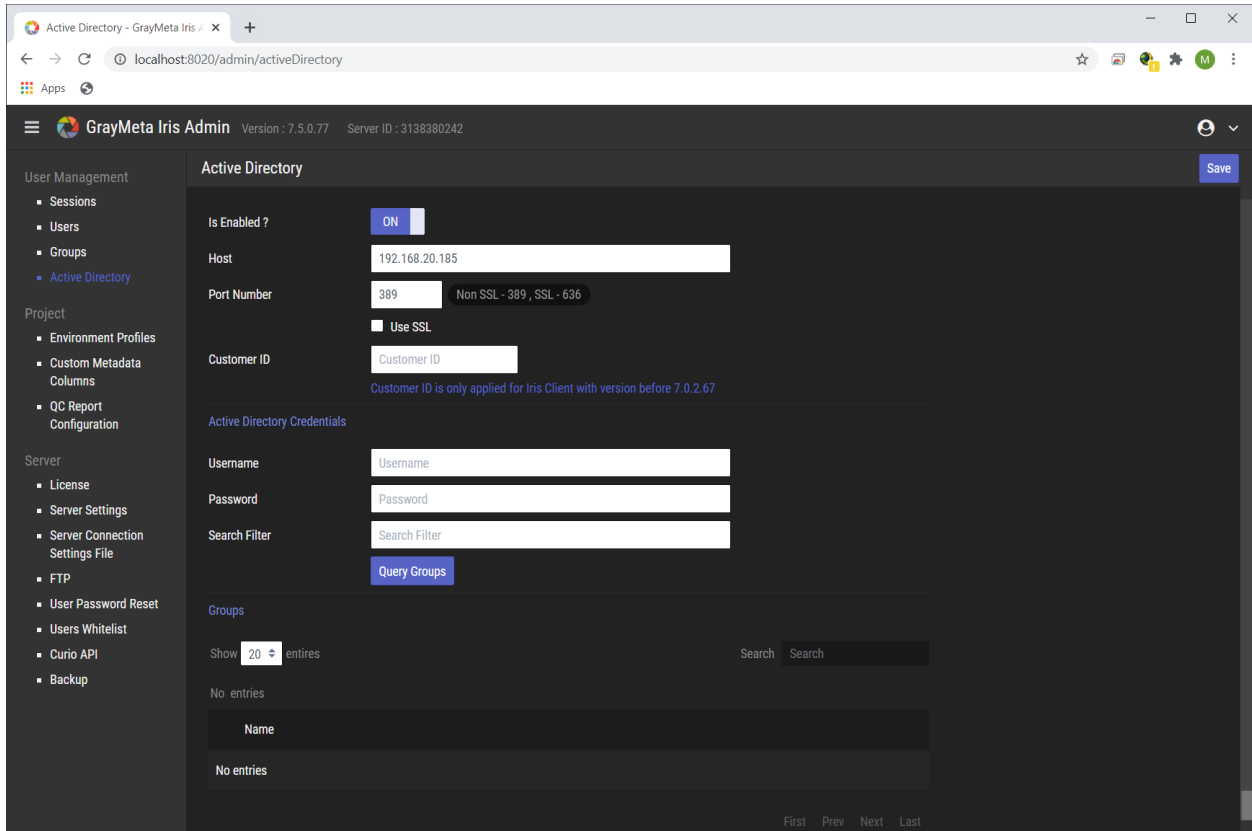
To specify group properties, click the edit button (blue pencil icon) and the following will be presented:



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 Iris accounts that were manually created by the user 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.

An Active Directory server is a centralized server that enables the management of user permissions and access to network resources. 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" that 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 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

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:

Active Directory Credentials

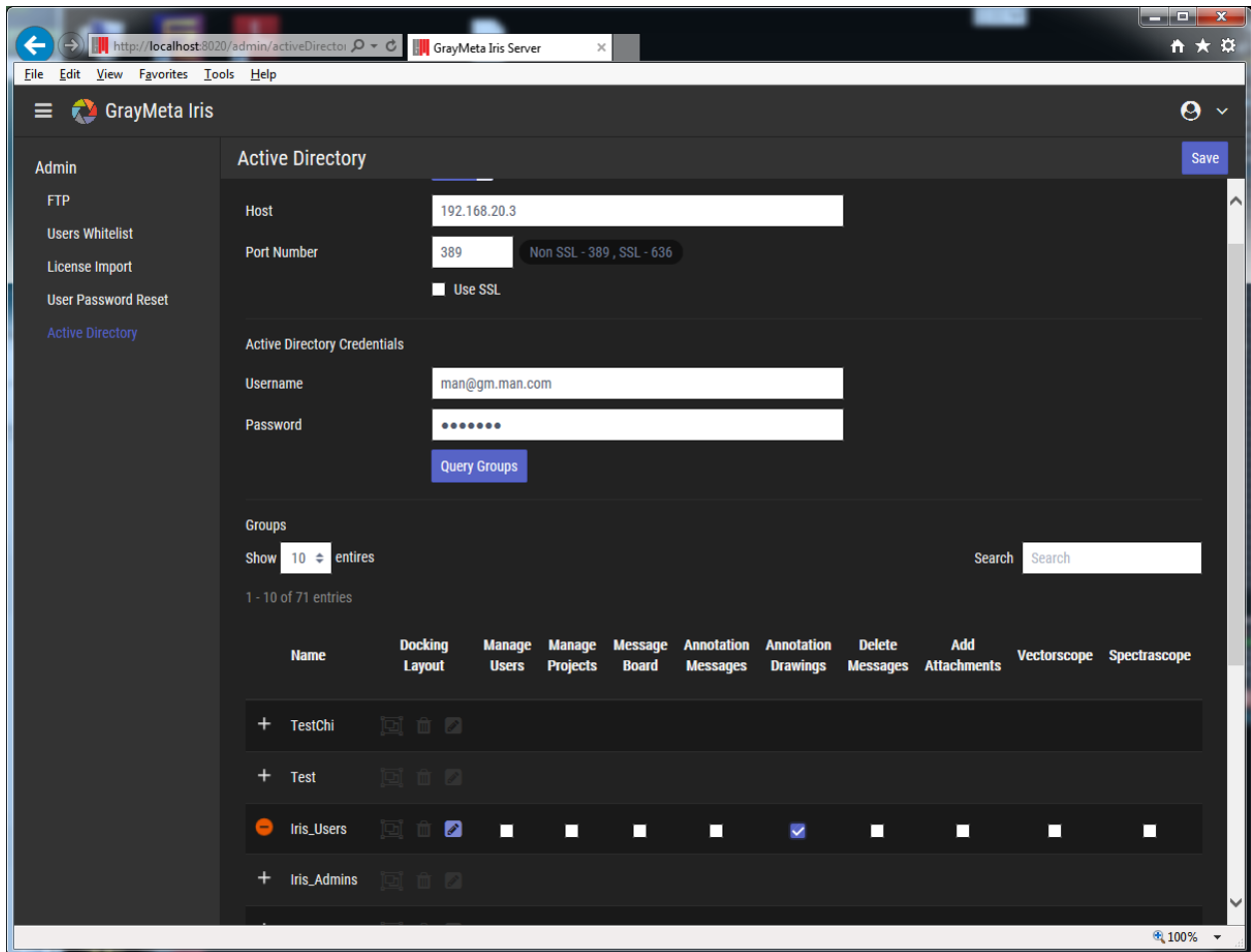
Username

Password

Search Filter

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 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:



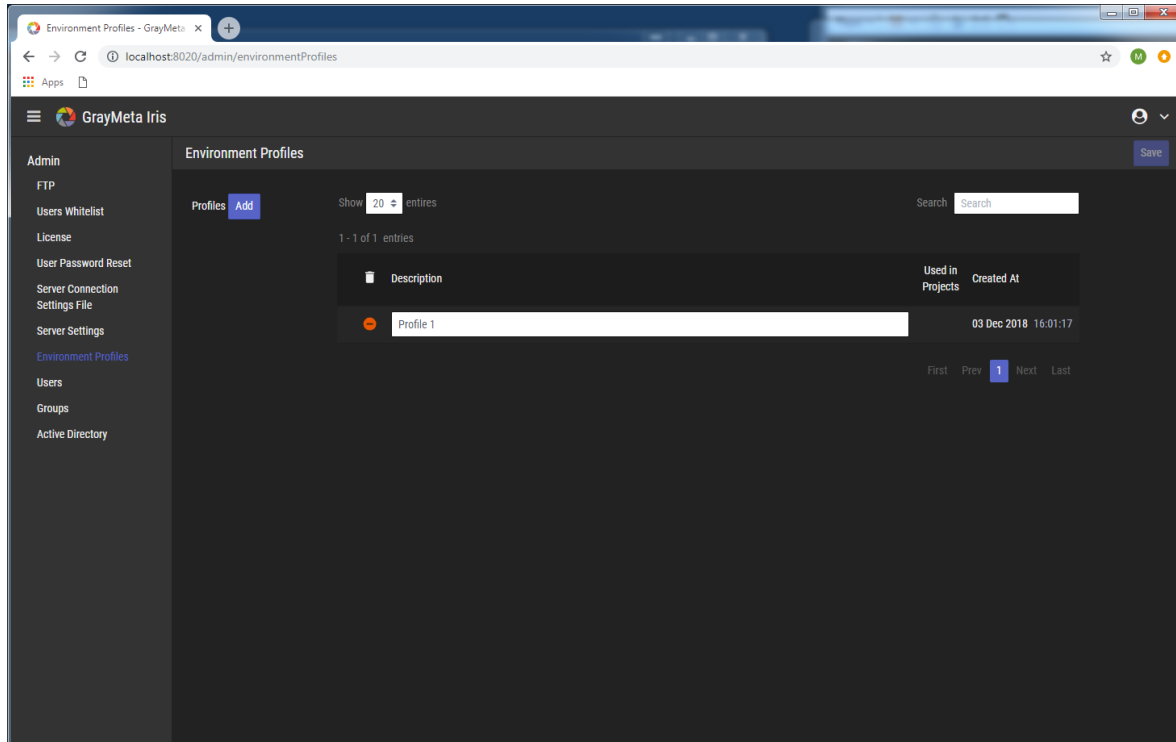
To enable a group, click the “+” button on the left and to disable it, click the same button. In the above screenshot, the group called “Iris_Users” is enabled. This means that somebody who is a member of this group will inherit the group’s permissions. When a group has been enabled, each group permission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

There is one more feature of groups that needs to be explained. As well as permissions, each group can also 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.

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 rubbish 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.

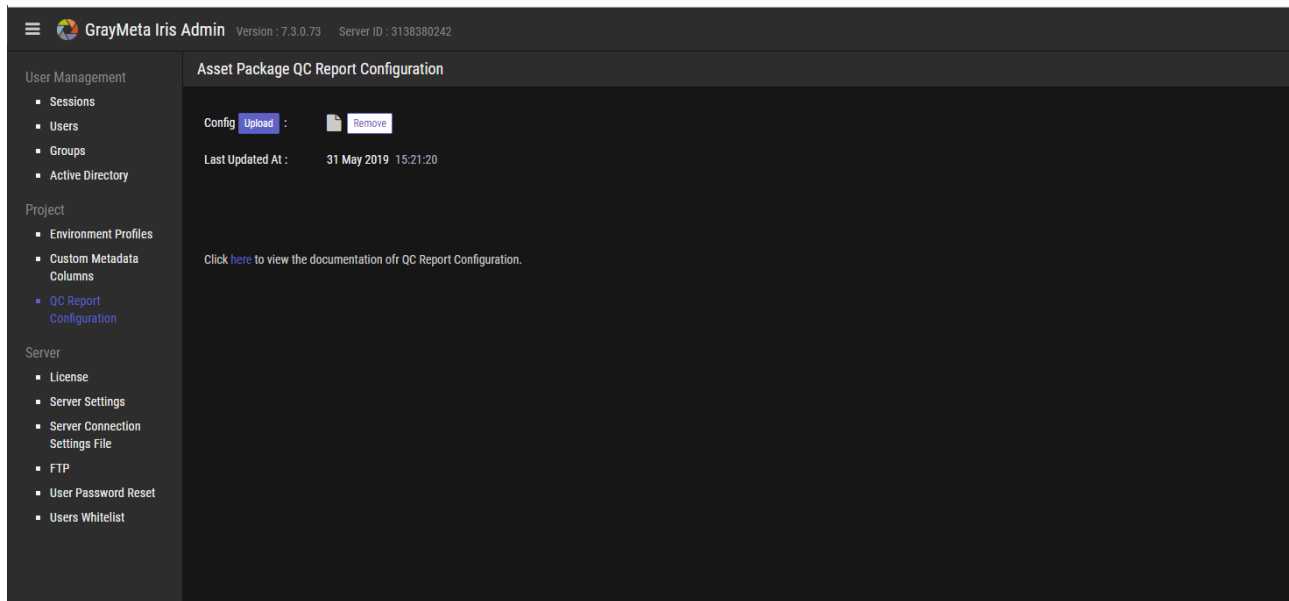
3.3.2 Custom Metadata Columns

The screenshot shows the GrayMeta Iris Server interface. The top navigation bar includes the logo, 'GrayMeta Iris Server', version '7.0.3.68', and server ID '348809218'. A left sidebar contains a menu with categories: 'User Management' (Sessions, Users, Groups, Active Directory), 'Project' (Environment Profiles, Custom Metadata Columns), and 'Server' (License, Server Settings, Server Connection Settings File, FTP, User Password Reset, Users Whitelist). The main content area is titled 'Custom Metadata Columns' and features a 'Save' button. Below the title, it indicates '1 - 5 of 5 entries'. A table lists the columns with their IDs and values:

	Column Header	Used in Projects
1	test column 1	
2	test column 2	
3	test column 3	
4	test column 4	
5	test column 5	

The list of custom metadata columns are shown here. Custom metadata can be set for each asset package through API and which is displayed in Iris application.

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, transforming 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:

Sample Files

[QCReporConfig.zip](#)
[QCReport_IrisReportData_Sample.xml](#)

Json Schema

ReportEntries array of object
 List of qc report entires.

Array [

XSLT_FilePath string
 Relative file path of XSLT file.

Extension string
 Optional File extension of the report. (e.g. .xml, .pdf)

IsPDF boolean
 Optional Default : **false**
 If it is set to true, the report after applying XSLT will export as a PDF file.
 Please make sure the report is in HTML format after the transform.

WorkingDirectory string

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

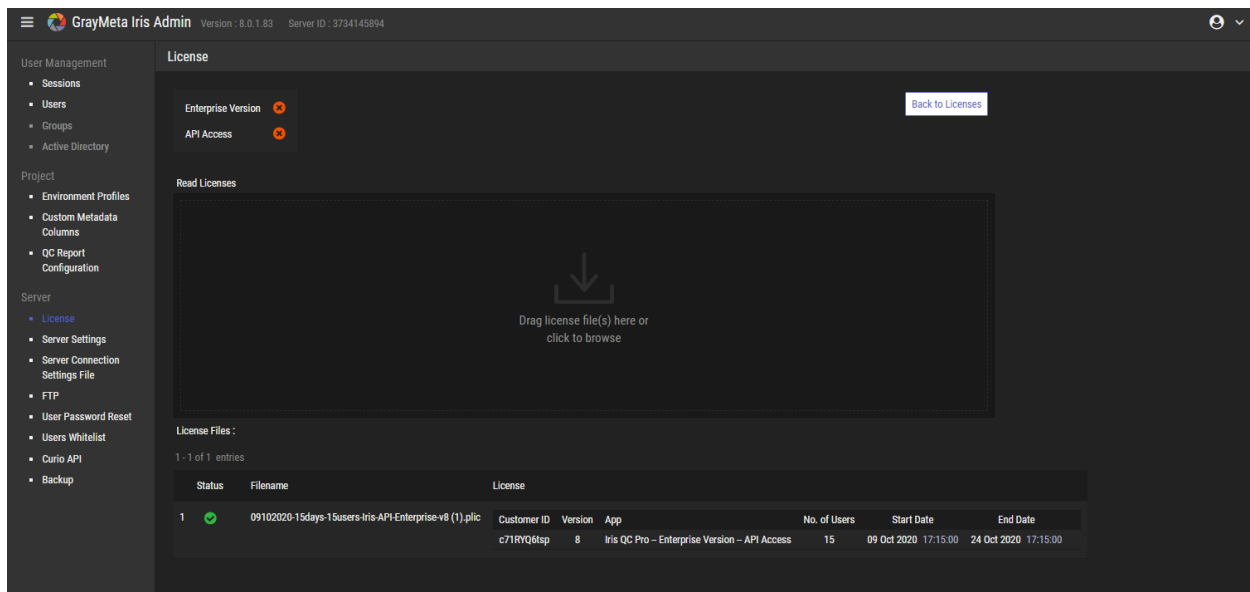
The screenshot shows the 'License' management page in GrayMeta Iris Admin. The interface includes a sidebar with navigation options like 'User Management', 'Project', and 'Server'. The main content area displays license details for 'Enterprise Version' and 'API Access', along with buttons for 'Delete All Licenses', 'Read Licenses', and 'Import Licenses'. A table lists the current licenses, showing one entry with a status of 'Valid' (green checkmark), Customer ID 'XLb3c4Q819', Version '7', App 'Iris QC Pro', 15 users, and a start date of '10 Sep 2020 18:31:00'. The table has columns for Status, Customer ID, Version, App, No. of Users, Start Date, and End Date. A search bar and pagination controls are also visible.

Status	Customer ID	Version	App	No. of Users	Start Date	End Date
Valid	XLb3c4Q819	7	Iris QC Pro	15	10 Sep 2020 18:31:00	-

This screen shows a current list of Iris Admin Licenses. 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:

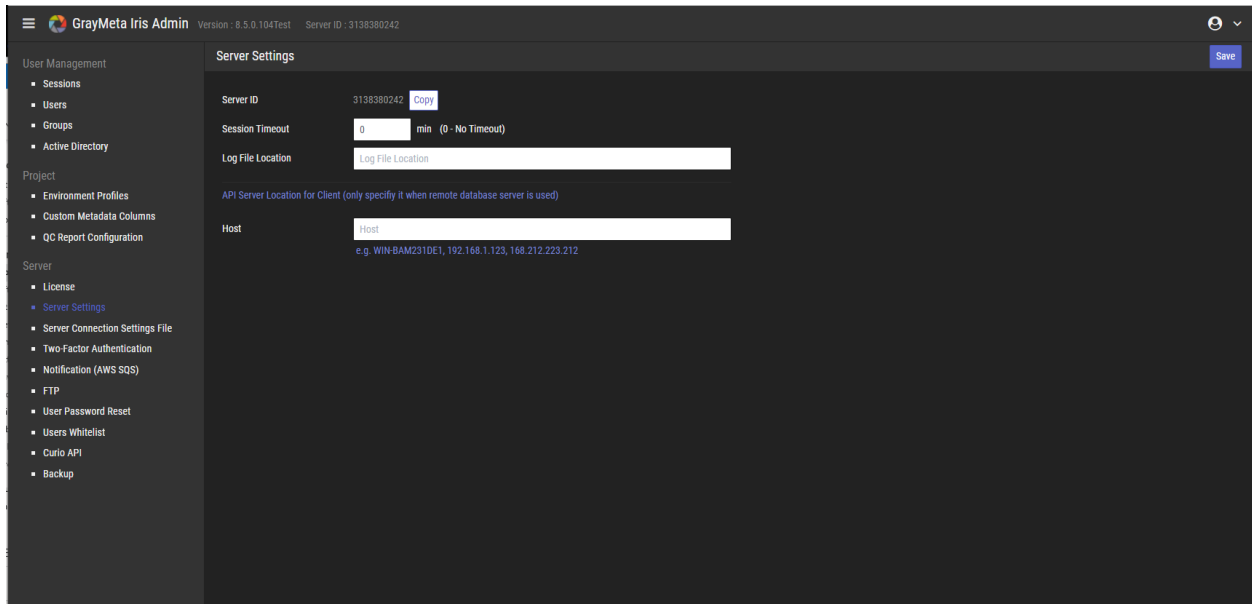


3.4.1.1 Auto Import Licenses

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.

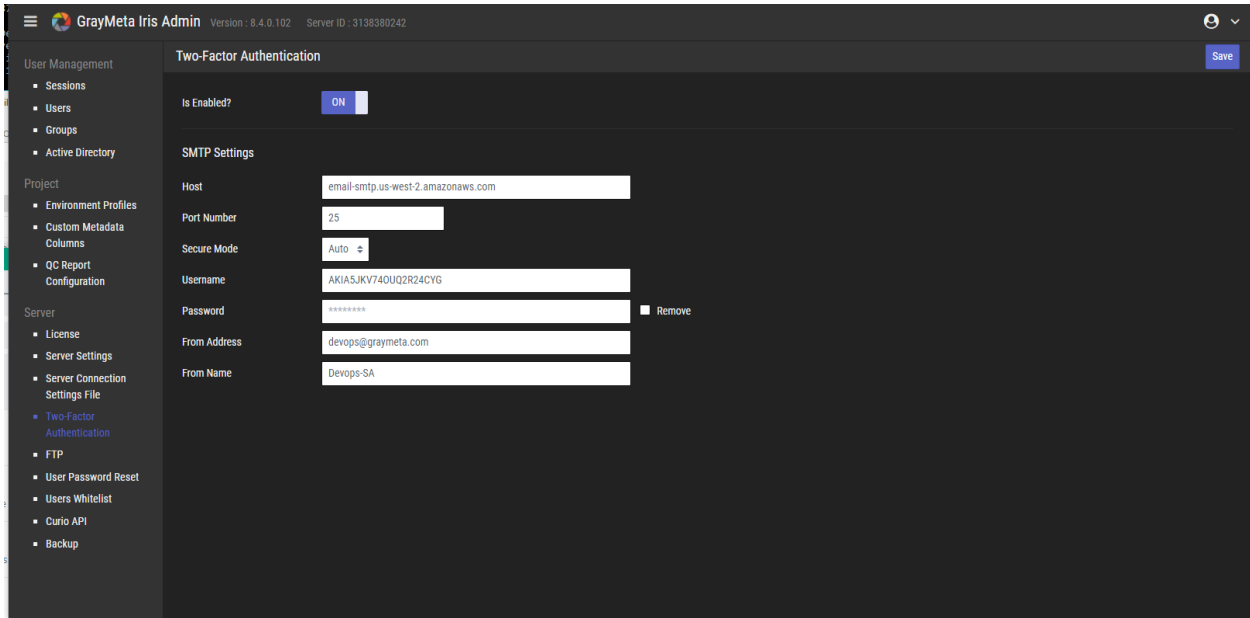
The setting for API location for client is used to specify the host name of the database in which the API needs to connect to. This is only required where the database is not located on the same machine as the Iris Admin server.

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.

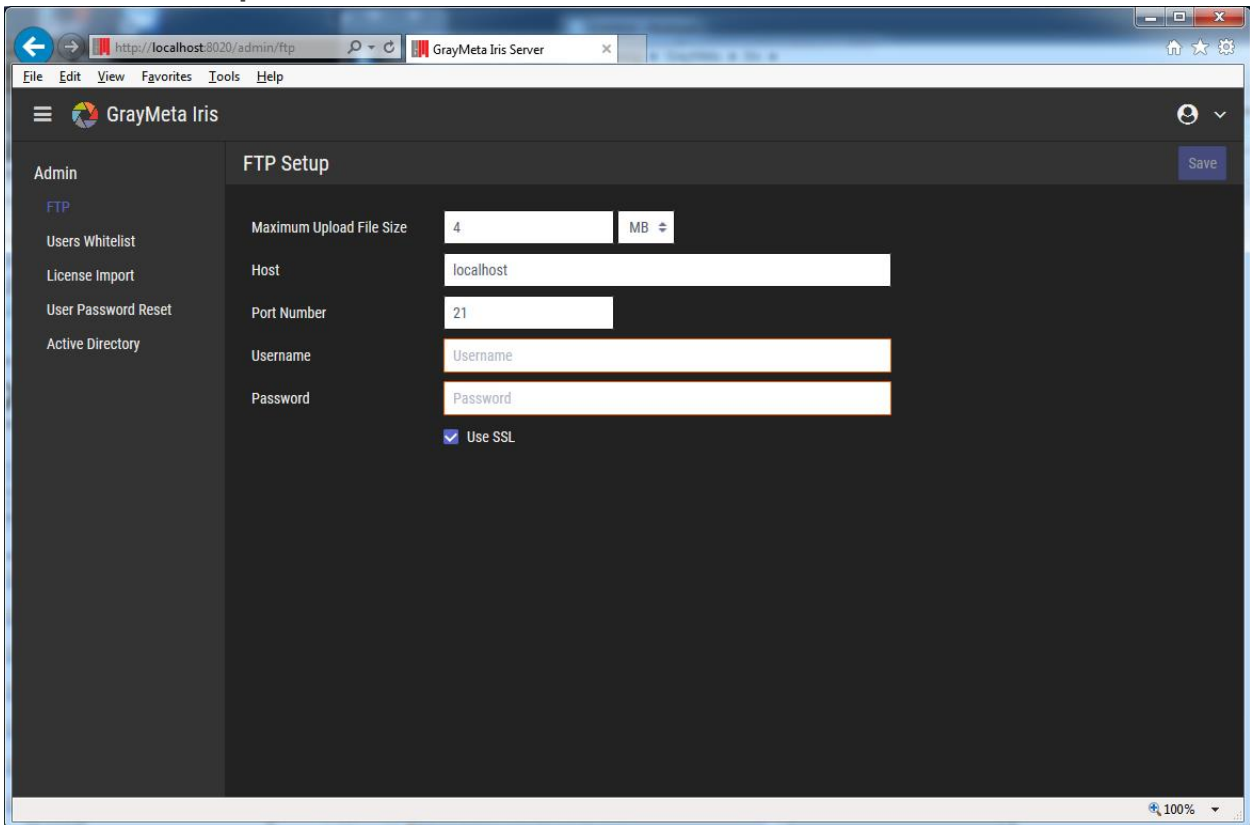
3.4.4 Two-Factor Authentication

Version 8.9.0.122



This page allows two-factor authentication to be switched on/off. The email SMTP settings must be set up here to enable two-factor code to be sent.

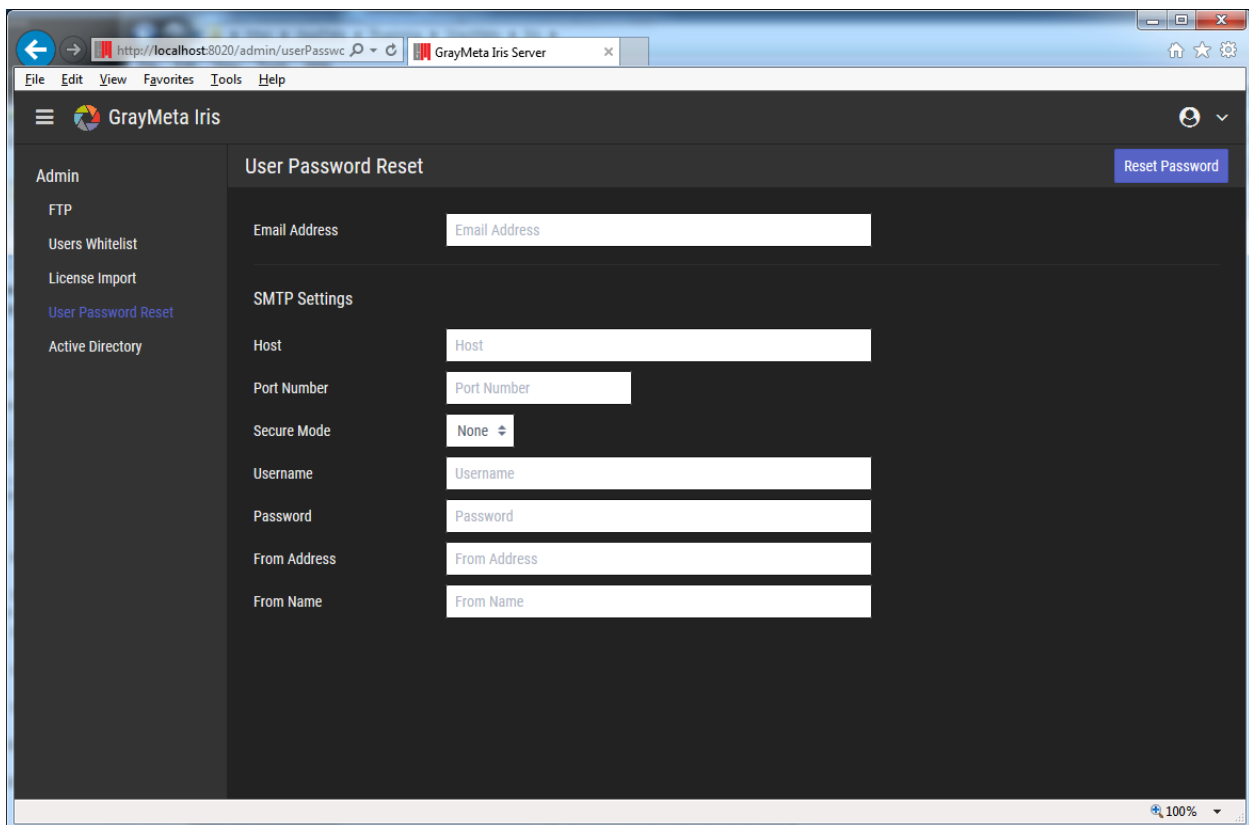
3.4.5 FTP Setup



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.

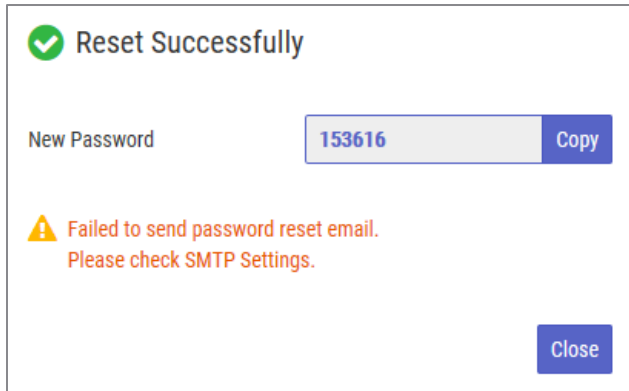
3.4.6 User Password Reset



The screenshot shows a web browser window with the URL `http://localhost:8020/admin/userPasswrc`. The page title is "GrayMeta Iris Server". The interface is dark-themed and features a sidebar menu on the left with the following items: Admin, FTP, Users Whitelist, License Import, User Password Reset (highlighted), and Active Directory. The main content area is titled "User Password Reset" and contains a "Reset Password" button in the top right corner. The form includes the following fields:

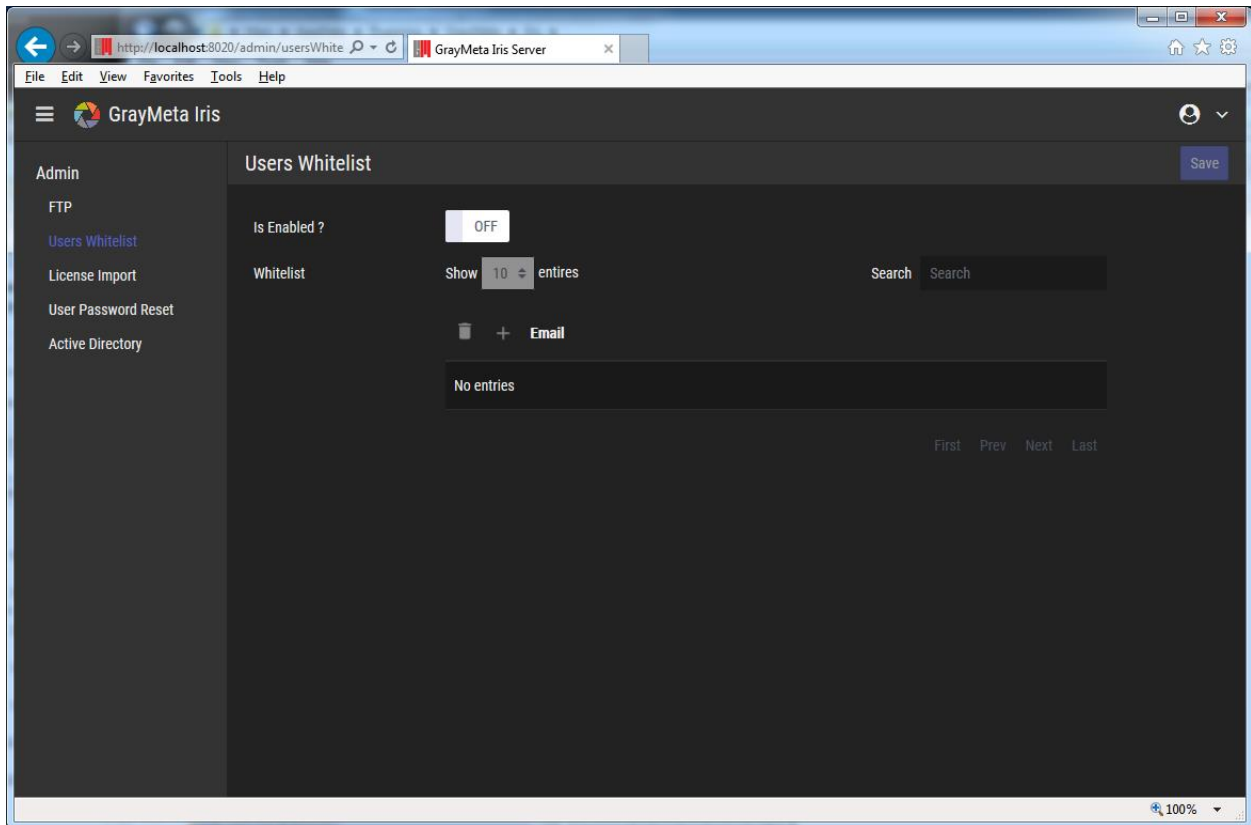
- Email Address:
- SMTP Settings section:
 - Host:
 - Port Number:
 - Secure Mode:
 - Username:
 - Password:
 - From Address:
 - From Name:

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.

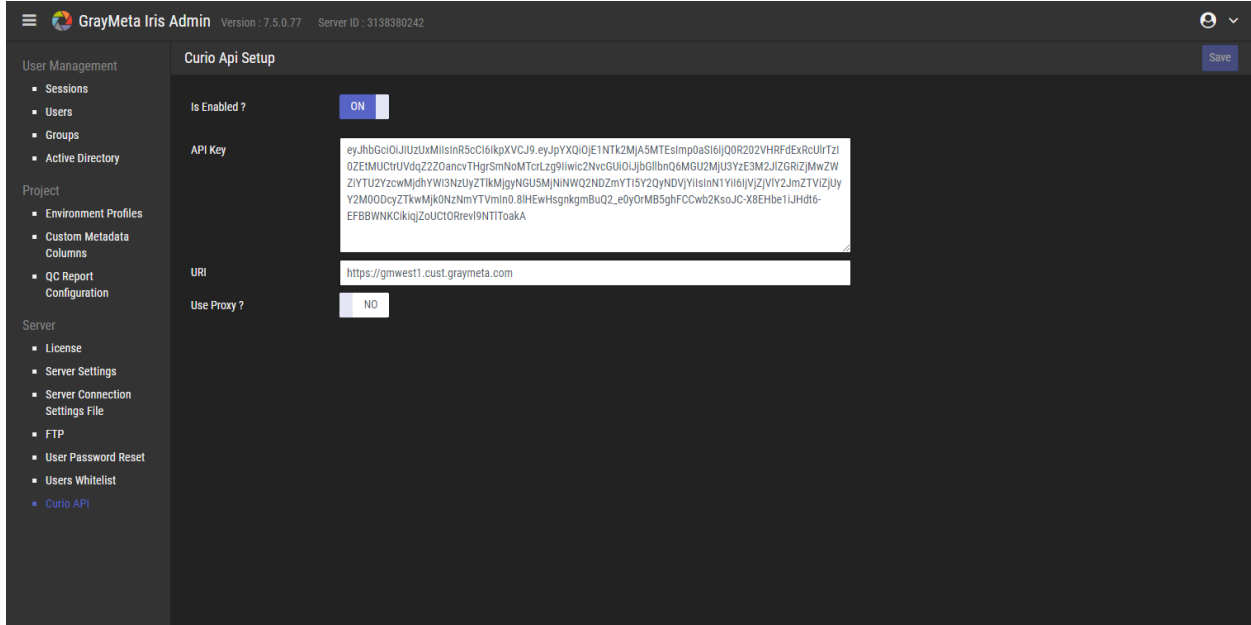
3.4.7 Users Whitelist



When the whitelist is enabled, only users specified in the whitelist can only use the collaboration features of Iris. 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.

3.4.8 Curio API

The Iris Client is able to integrate with Curio by way of making API calls to Curio. This integration provides a means of accessing data from Curio that can be represented in Iris Client.

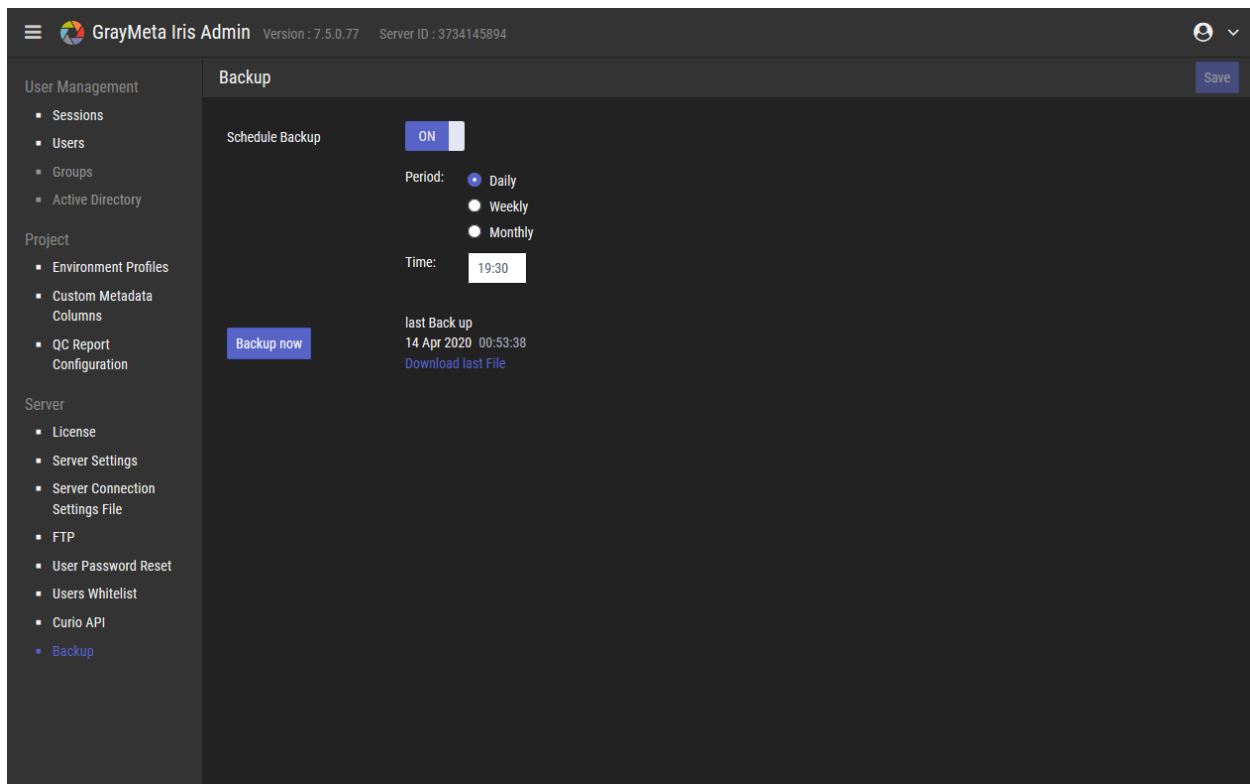


Accessing Curio requires use of API keys and a uri to the Curio location. These details must be entered here to grant Iris Admin access to Curio. Access to Curio is enable or disabled by clicking the “Is Enabled?” button.

For Iris Clients that have no direct internet access, it is possible to access Curio via a proxy located on the same machine as Iris Admin. This means that Iris Client can still access Curio indirectly through the proxy. If proxy access is required, enable the “Use Proxy?” button.

3.4.9 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.

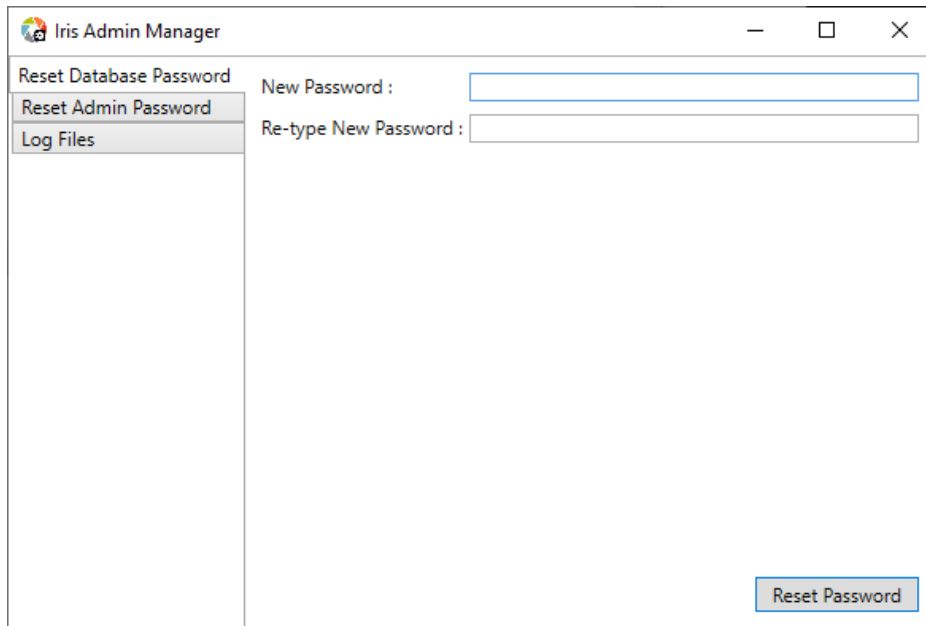
The last backup can be downloaded by clicking “Download Last File”. It is also possible to access all previous backups by going to the folder location **%public%\Documents\GrayMeta\Iris Server\Backup**

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

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.