Quantify Access Control Administrator Guide

Get started or find the details - everything you need to know.
Just select a topic or link below :-)

Users,
replay permissions,
and applications...

Create & Manage Users

Set Replay Permissions

Create & Manage Groups

Create & Manage Filters

Applications & Features

Active Directory
and licenses...

Manage Active Directory

Licenses

Find out more...

eLearning

Online Training

This Guide

Find a Topic

Your Red Box system may look different to the one used in this document.

Quantify Access Control - Admin Guide

About

You have full control over what recordings, applications, and features can be accessed by your users. Select a topic from the contents list to learn more.

This guide has been designed for Quantify System Administrators, and covers admin tasks associated with "Access Control". This guide is part of a set of Quantify Administrator Guides from Red Box.

If you'd like to view or distribute information separately, each main topic is available as a separate "Quick Question" document from the **help page** at redboxvoice.com

Note that for user information, please refer to the Quantify User Guide.

Users, Replay Permissions, and Applications

How Do I Create & Manage Users

How Do I Set Replay Permissions

How Do I Create & Manage Groups

How Do I Create & Manage Filters

How Do I Enable/Disable Apps & Features

Active Directory & Licenses

How Do I Manage Active Directory

How Do I Manage Licenses

How Do I Create & Manage Users

Contents

Create/Add a User

Each individual Quantify user should have a separate Quantify account. A user account is assigned permissions to restrict or allow access to Quantify features and functions, as well as access to recorded communications.

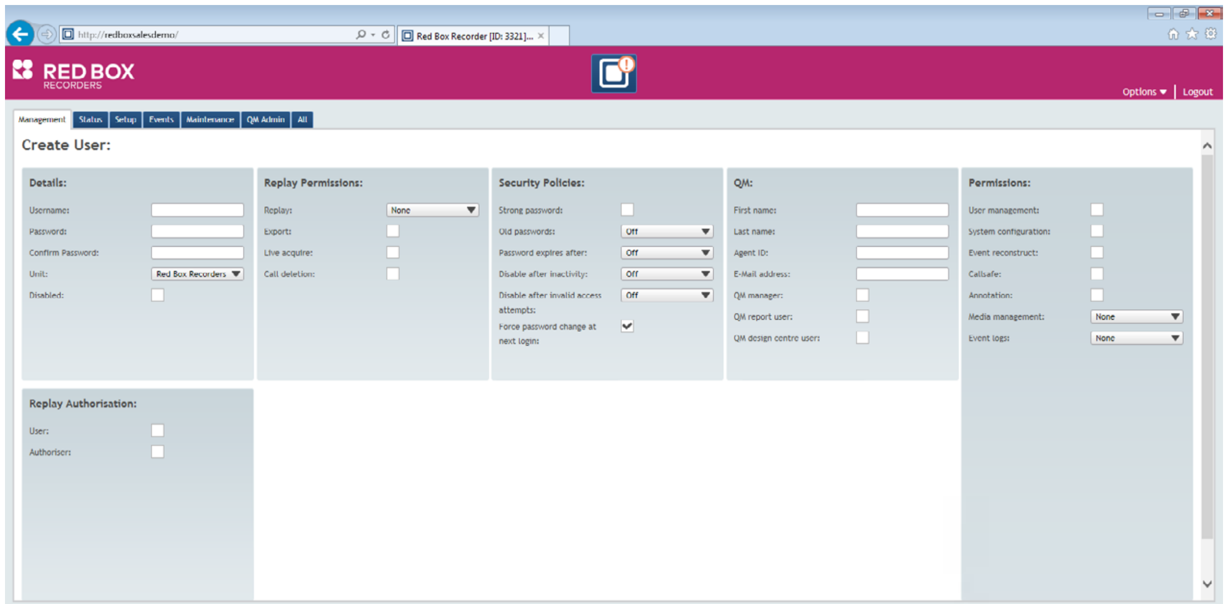
To create a user:

1. Login to Quantify with an administrator account (User Management permissions).
2. Go to **Configuration** > **Management** > **Users** and click the **Create** button.
3. Complete the **Create User** form (see below), and click the **OK** button when you're done.

Create User – Config Form

The six form panels are:

- **Details**: Main account details.
- **Replay Permissions**: Call replay permissions.
- **Security Policies**: Password and login security.
- **QM**: Quantify QM permissions. If you don't have Quantify QM, this panel won't be available.
- **Permissions**: General Quantify permissions.
- **Replay Authorisation**: Replay Authorisation role/permissions. If you don't have Quantify Replay Authorisation, this panel won't be available.

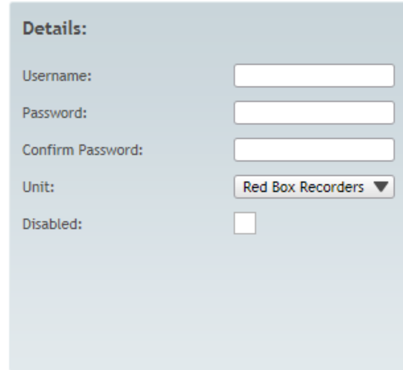


Contents

Create User – Form Panels

The tables below provide detailed information on each of the panels and fields in the **Create User** form.

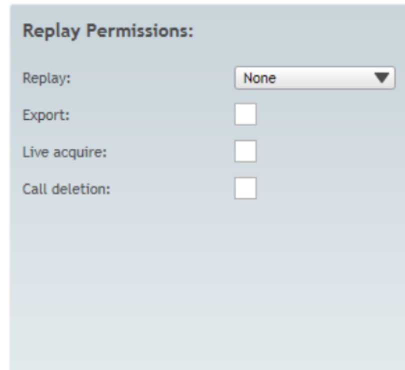
Details	
Username	Account username used for login.
Password & Confirm Password	Account password used for login.
Unit *	Assign the user to the selected "Unit". *
Disabled	Prevent the user from logging in. This can be useful where you want to disable an account (permanently or temporarily) but don't want to delete it - for example, if you use temporary agents on a regular basis you could enable and disable as needed.



* Units are only applicable to a licensed hosted recorder and may display using a different name.

Note: Active Directory users will also have some additional settings here. See "How Do I Manage Active Directory" for details.

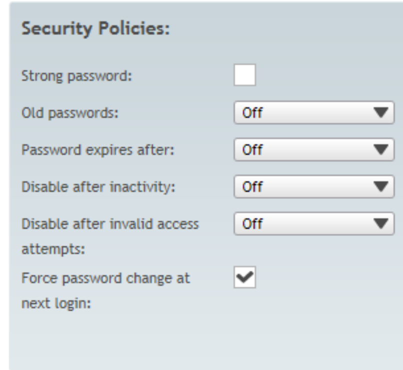
Replay Permissions	
Replay	Set the user's replay permissions: **None**: No calls can be replayed by this user. **Specific**: Allow user to replay specific calls only. You can specify database fields and/or security filters to define what calls can be replayed. **All**: Allow user to replay all calls. If this field is set to **Specific** or **All**, you can further restrict access to calls via **Replay Authorisation** (see below). See "How Do I Set Replay Permissions" for more information.
Export	Allow the user to export recorded calls to WAV files using Quantify Replay.
Live acquire	Allow the user to listen to live calls using Quantify Live Acquire.
Call deletion *	Allow the user to delete recorded calls. *



* The **Call Delete** function is very rarely available within Quantify. If you don't have **Call Delete**, this field won't be available.

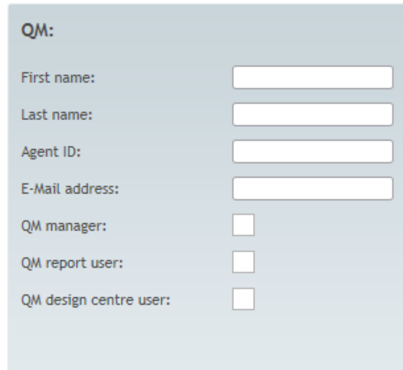
Contents

Security Policies	
Strong password	The password must contain at least one uppercase letter, one lowercase letter and one number.
Old passwords	Stops the user entering previously used passwords.
Password expires after	Password expires after specified period of time – user must then change their password.
Disable after inactivity	Account is disabled if the user does not log in within the specified period of time.
Disable after invalid access attempts	Account is disabled if more than the specified invalid logins attempts are made consecutively.
Force password change at next login	When the user next logs in they're forced to change their password.



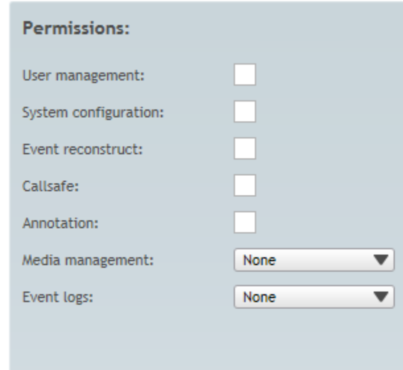
QM *	
First name	User's first name.
Last name	User's last name.
Agent ID	Unique ID used to identify an agent. This is often used to specify a staff ID number or extension number.
Email address	User's email address used by QM to send Coaching emails.
QM manager	Assign QM Manager permissions to the user. A QM Manager can perform evaluations, run reports, and view available evaluation form types.
QM report user	Allow the user to run QM reports.
QM design centre user	Allow the user to view and edit available evaluation form types.

* If you don't have Quantify QM, this panel won't be available.



Contents

Permissions	
User management	Admin permissions – allow the user to create, modify and delete users (except their own details).
System configuration	Admin permissions – allow the user to configure and control the Red Box Recorder. For example, set up recordable devices, turn the recorder on/off, etc.
Event reconstruct *	Allow the user to access Quantify Event Reconstruct (if available).
Callsafe *	Allow the user to access Quantify Callsafe (if available).
Annotation	Allow the user to annotate recorded calls.
Media management	Set the user's media management permissions: **None** – no permissions. **Remove/Replace Replay Media** – remove replace removable archive media. **Full Media Control** – full removable archive media and Network Attached Storage (NAS) control.
Event logs	Set the user's event log access permissions: **None**, **Own logs only**, or **Full** (all users' logs).



* Event Reconstruct and Callsafe are optional Quantify applications. If you don't have these applications, the fields won't be available.

Replay Authorisation *	
User	Allow the user to request to replay a call. Note that the user must also have their **Replay Permissions** set to **Specific** or **All** (see above) – although they will be able to see the calls in Quantify Replay and QM, they will have to request replay access.
Authoriser	Allow the user to receive, authorise and reject replay requests.

* If you don't have Quantify Replay Authorisation, this panel won't be available.

Edit, Delete, and Copy Users

Go to **Configuration** > **Management** > **Users** , highlight the user, and click the **Edit**, **Delete** or **Copy** button:

- **Edit**: Edit user account details, including password reset.
- **Delete**: Delete the user account. To delete multiple accounts, use the **Shift** and/or **Ctrl** keys to highlight multiple accounts, and click **Delete**.
  Note that although the user is deleted, all associated user data (annotations, event logs, QM evaluations, etc.) will not be deleted. Also, you can disable an account rather than delete it (**Edit** > **Details** > **Disabled**).
- **Copy**: Create a new user account, copying all non-personal data and settings from the highlighted user. This option is particularly useful when setting up users with very similar profiles.

Contents

User Options

There are a few additional options available for user settings – go to **Configuration** > **Setup** > **User Options**

User Options	
Enable Client Browser Cookies	Tick to enable system use of cookies with Quantify.
Login Expiry Time	Select the idle time after which a user will be automatically logged out of Quantify.
Event Log Limit	Select the number of event logs to display "per page" (in the **Configuration** > **Events** pages).
Device Configuration Text	**Always show device text**: Use the device text automatically assigned by the recorder to identify the device in recording alarms. You can view **Device Text** for all devices from **Configuration** > **Setup** > **Recording** **Show channel names**: Use channel names (if available) to identify devices. In general, this is the preferred setting as channel names are usually more "user friendly".
Default Language	Select the Quantify UI language for all users. Only installed language packs are available.
Enable Downloads	This feature is provided for legacy customers only and can be ignored.

Troubleshooting

The following are a few common issues you may encounter:

Issue:	User can't login
Problem/ Solution:	• Incorrect password. To reset a user password, go to *User* > **Details** > **Password** and change the password, then go to the **Security Policies** panel and tick **Force password change at next login**. • Account disabled. To re-enable an account, go to *User* > **Details** and untick the **Disabled** option. • Account deleted.

Issue:	User can't see Quantify Search & Replay
Problem/ Solution:	• No replay permissions assigned. To assign replay permissions, go to *User* > **Replay Permissions** and assign appropriate permissions.

www.redboxvoice.com
info@redboxvoice.com
+44 (0)115 937 7100

RBRQQA1004 V1.3

Red Box

How Do I Set Replay Permissions

1

Contents

In order for any user to find and replay recorded communications or listen to live calls, they must have replay permissions. This topic takes you through the main methods of assigning replay permissions.

Methods, Conflicts & Priorities

Replay permissions are used to control access to recorded communications and live calls. The three main replay permission methods/types are:

- **Direct**:

  Allow access to all communications, no communications, or a specific field (search criteria).

  Assigned via user account settings. Applies to Search & Replay **and** Monitoring (Live Acquire).

  See "Direct – All, None, Specific Field" for more details.

- **Specific Group**:

  Allow access to a specific group of channels (devices).

  Assigned via user account settings. Applies to Search & Replay **and** Monitoring (Live Acquire).

  See "Specific Group" for more details.

- **Filters**:

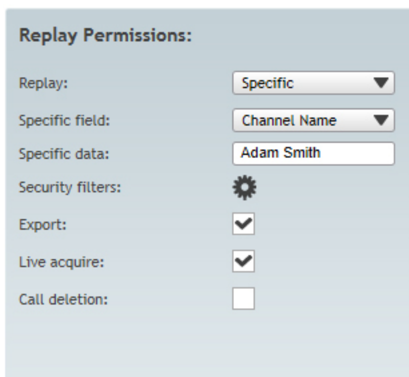
  Filter Direct or Group permissions — allow or deny access to communications that match one or more search criteria.

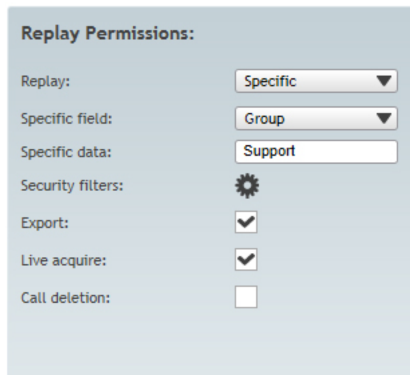
  Assigned via **Configuration** > **Management** > **Filters**. Applies to Search & Replay **only**.

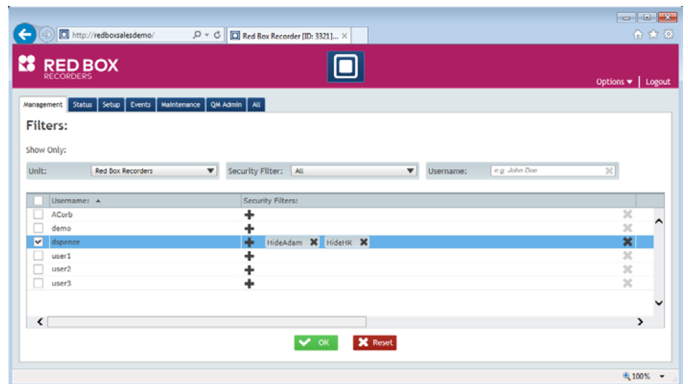
  See "Filters" for more details.

Choose your method(s) carefully, apply consistently, and try to avoid conflicts. When assigning replay permissions, remember the two main "rules":

- To **allow** replay, you must allow access on **all** applied permission types.
- To **deny** replay, you only need to deny access on **one** applied permission type.







Contents

Direct – All, None, Specific Field

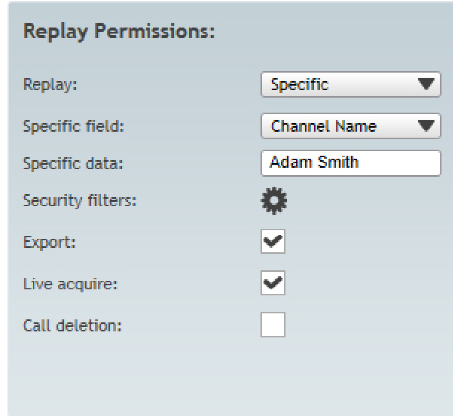
To assign “Direct” replay permissions:

1. Go to a user’s account settings (**Configuration** > **Management** > **Users**).
2. In the **Replay Permissions** panel, select one of the following options:

   None: No communications can be replayed by the user.

   Specific: Allow the user to only replay recorded communications that match the specified criteria — defined using the **Specific Field** and **Specific Data** options.

   All: Allow the user to replay all recorded communications.
3. Click **Ok** when you're done.

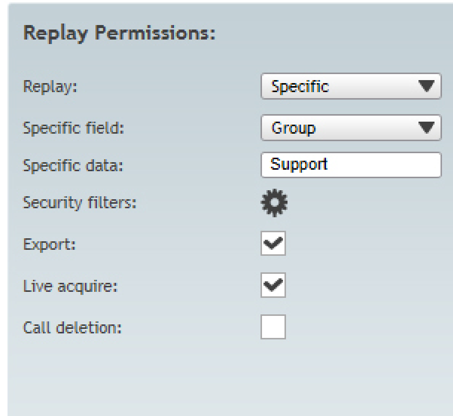


Specific Group

To assign replay permissions using Groups:

1. If you haven't done so already, create your Groups and add members:
   - To create a group: Go to **Configuration** > **Management** > **Groups** and click the **Configure Groups** button. Type your group name in the **Add group** field and click the **Add** button.
   - To add members: Click the **Configure Members** button and use the **+** and **✕** icons to add/remove a member to/from a group. Click the **Apply** button to save your changes

   Refer to "How Do I Create & Manage Groups" for more details.
2. To assign replay permissions using Groups, go to a user’s account settings (**Configuration** > **Management** > **Users**).
3. In the **Replay Permissions** panel, select:
   - **Replay** > **Specific**
   - **Specific Field** > **Group**
   - **Specific Data** > *“GroupName”*
4. Click **Ok** when you're done.



Note: Remember that over time as you add and remove group members, the changes are **not** applied retrospectively. That is, all communications accessible prior to the group change will remain accessible, or vice versa.

Contents

Filters

To assign Filters:

1. If you haven't done so already, create your filters:
   - Go to **Configuration** > **Management** > **Filter Management**.
   - Select your **Filter Type**:

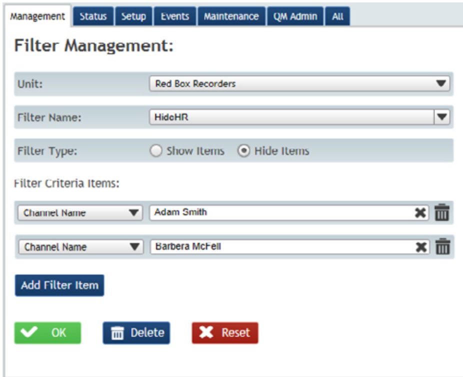
     Show Items – show items that match the specified criteria, hide everything else.

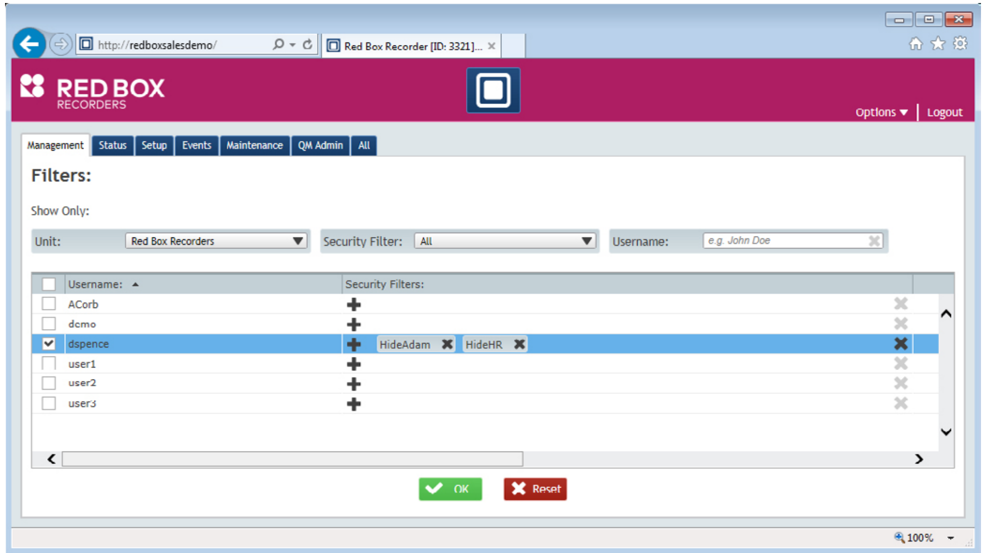
     Hide Items – hide items that match the specified criteria, show everything else.
   - Add your filter criteria as needed.

     Multiple criteria of the same type are applied as "OR" criteria – match one or more to apply.

     Multiple criteria of different types are applied as "AND" criteria – match all to apply.
   - Click **Ok** to create your filter.

   Refer to "How Do I Create & Manage Filters" for more details.
2. To apply/remove filters to/from Quantify users, go to **Configuration** > **Management** > **Filters** and click the **+** and **✕** icons as needed.
3. When you're done, click the **Ok** button to apply your changes.





www.redboxvoice.com
info@redboxvoice.com
+44 (0)115 937 7100

RBRQQA1009 V1.3

Contents

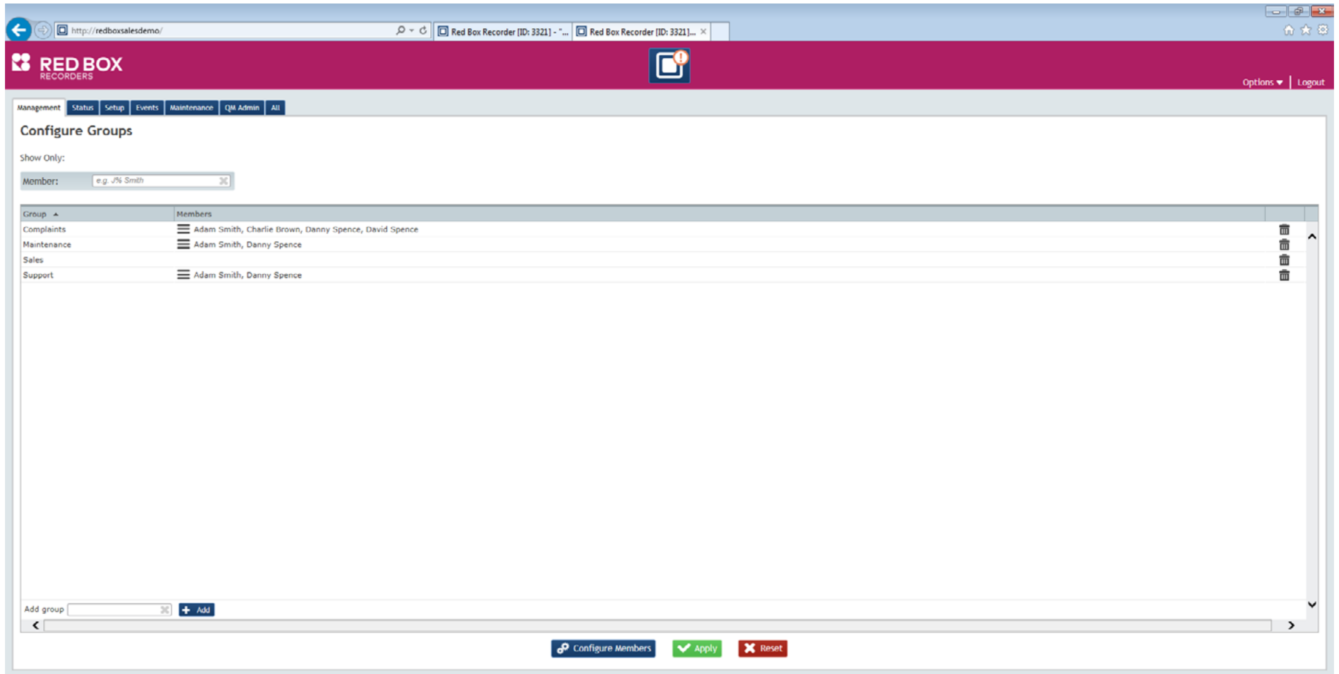
Previous Menu Next

A Group is used to group channel names together, which you can then use to assign flexible replay permissions – either within user replay permissions, or in combination with security filters. It's your choice which method you use to apply your access settings, but you should think carefully about which method provides you with the necessary functionality.

Create a Group

To create a group:

1. Login to Quantify with an administrator account (System Configuration permissions).
2. Go to **Configuration** > **Management** > **Groups** and click the **Configure Groups** button.
3. Type your group name in the **Add group** field and click the **Add** button.
4. Your new group will now be listed in the group list.



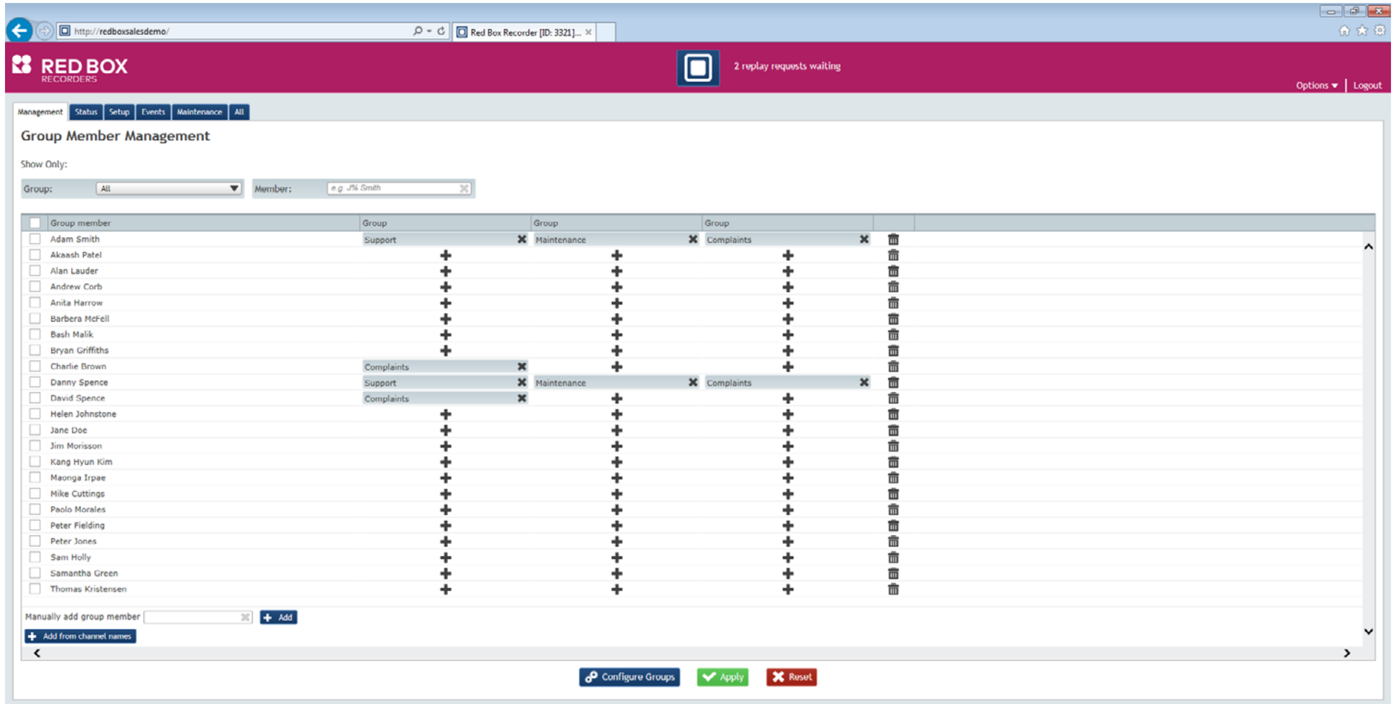
Contents

Add/Remove Members

The **Group Member** list displays all available channel names and the groups that they are a member of. You can use this screen to review group membership and add/remove members.

To add/remove members to/from a group:

1. Go to **Configuration** > **Management** > **Groups** – if you're already in **Configure Groups**, click the **Configure Members** button. This will display the **Group Member** list.



2. Use the list to configure your group members:
   - To add a member to a group, click a **+** icon and select the group.
   - To remove a member from a group, click the appropriate ✕ icon.
   - To remove a member from all groups and from the list, click the 🗑 **Delete** icon. Note that this just removes the member from the **Group Member** list, but doesn't delete the actual channel/channel name.

   Note: Added and removed group members are not applied retrospectively. That is, all communications accessible prior to the group change will remain accessible, or vice versa.

3. When you're done, click the **Apply** button to save your changes.

Contents

Update Member List

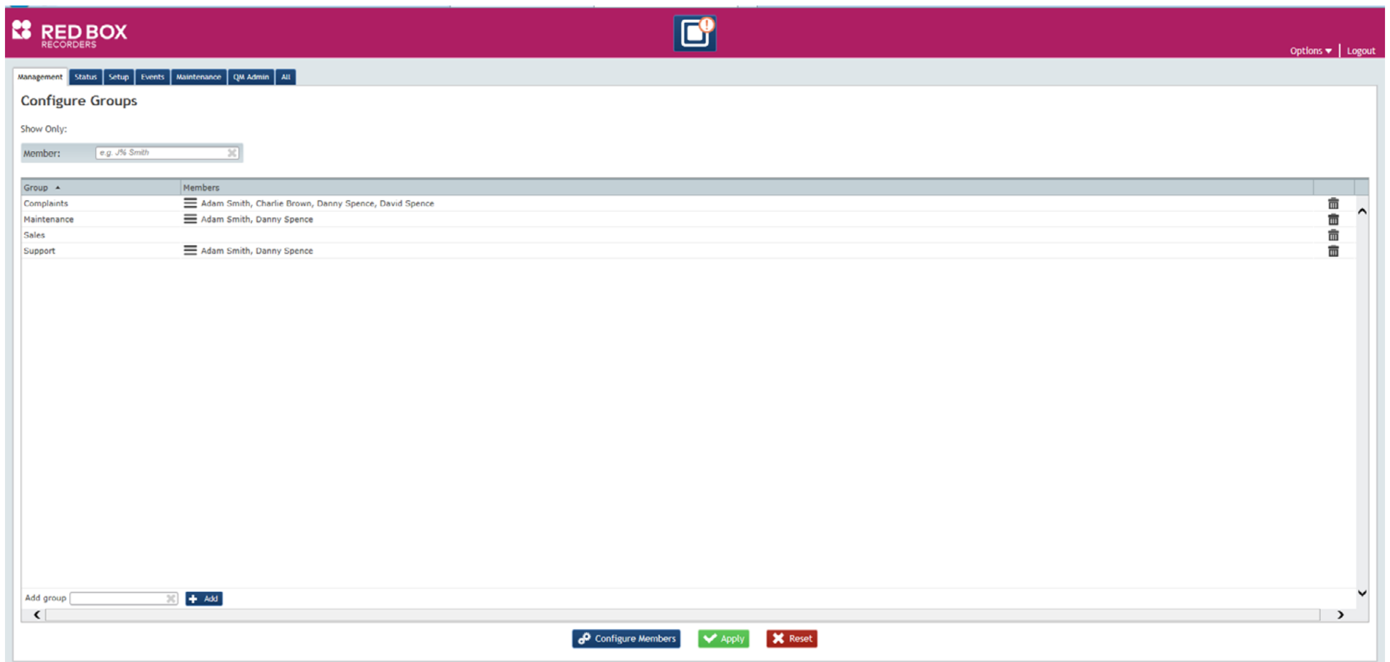
You can add and remove members to/from the **Group Member** list:

- To add channel names to the list, click the **Add from channel names** button to refresh the list with all available channel names.
- To add a member to the list manually, type the member name in the **Manually add group member** field and click the **Add** button. Note that the typed name must match a Channel Name or the added member will have no associated channel/device.

Review, Edit or Delete a Group

To review, edit or delete a group:

1. Go to **Configuration** > **Management** > **Groups** and click the **Configure Groups** button.
    - Group members are listed in the **Members** column. If you need to, roll over the ☰ **List** icon to view the full list.
    - To edit a group name, roll over the **Group Name** field, click the ✎ **Edit** icon, and enter your **Group Name**.
    - To delete a group, click the 🗑 **Delete** icon
2. When you're done, click the **Apply** button to save your changes.



Contents

Members of Multiple Groups

Channel names (devices) can be members of multiple groups, as you can see from the screenshots above — for example, **Danny Spence** and **Adam Smith** are members of the **Complaints**, **Maintenance** and **Support** groups. Multiple group membership can be very useful, but there are additional considerations:

- If a channel name is a member of multiple groups, you don't need to assign replay permissions for all groups in order to access those specific channels. For example, if you want to assign replay permissions for the **Support** group, you don't need to assign replay permissions to **Maintenance** and **Complaints** as well, just because **Danny Spence** and **Adam Smith** are members of all three groups.
- When assigning replay permissions, remember the two main rules. To allow replay, you must allow access on **all** applied permission types. To deny replay, you only need to deny access on **one** applied permission type. See "Assign Replay Permissions" below.
- Group information is stored along with a recorded communication in a specific order - the order in which groups are assigned in **Group Member Management**. To make sure a group name is found in the database, either always use the same order, or use the "**%**" wildcard when searching or filtering on a group name — for example, search for "**%Support%**" rather than just "**Support**".
- To avoid conflicts, multiple groups are **not** supported in Network Storage Filters. That is, if you've defined a channel as a member of multiple groups, the channel will **not** match the single group selection in the Network Storage Filter.

Assign Replay Permissions

Refer to "How Do I Set Replay Permissions" for more detailed information. The following description provides a brief overview.

Assigning replay permissions defines what recorded communications a user has access to. The three main replay permission methods/types are:

- **Direct** (**All**, **None**, **Specific Field**): Assign via user account settings. Applies to Search & Replay and Monitoring (Live Acquire).
- **Specific Group**: Assign via user account settings. Applies to Search & Replay and Monitoring (Live Acquire).
- **Filters**: Assign via **Configuration** > **Management** > **Filters**. Applies to Search & Replay only.

Choose your method(s) carefully, apply consistently, and try to avoid conflicts. When assigning replay permissions, remember the two main rules:

- To allow replay, you must allow access on **all** applied permission types.
- To deny replay, you only need to deny access on **one** applied permission type.

To provide access to recorded communications for a specific group (a group of channels/devices):

1. Create or edit a user account. In the **Replay Permissions** panel, select:
   - **Replay** > **Specific**
   - **Specific Field** > **Group**
   - **Specific Data** > "*GroupName*"

Contents

Naming Conventions

Consider your groups' names and how you want to apply replay permissions. For example:

- Let's say you have multiple sales teams with a team leader that can only access calls for their team, but a sales manager who can access all the teams.
- You could have groups named **SalesTeam1**, **SalesTeam2**, **SalesTeam3**, etc.
- Each team leader can be assigned access to their own sales team using their specific group name (e.g. Team Leader 1 – group **SalesTeam1**, Team Leader 2 – group **SalesTeam2**, etc).
- The sales manager could then be assigned access to all the sales teams using the "**%**" wildcard in the group name (**SalesTeam%**).

www.redboxvoice.com
info@redboxvoice.com
+44 (0)115 937 7100

RBRQQA1005 V1.3

Red Box

Contents

A Filter can be used to assign flexible replay permissions by filtering a user's search results. You can apply single or multiple filters as needed and a filter can allow or deny access to recorded communications that match one or more search criteria.

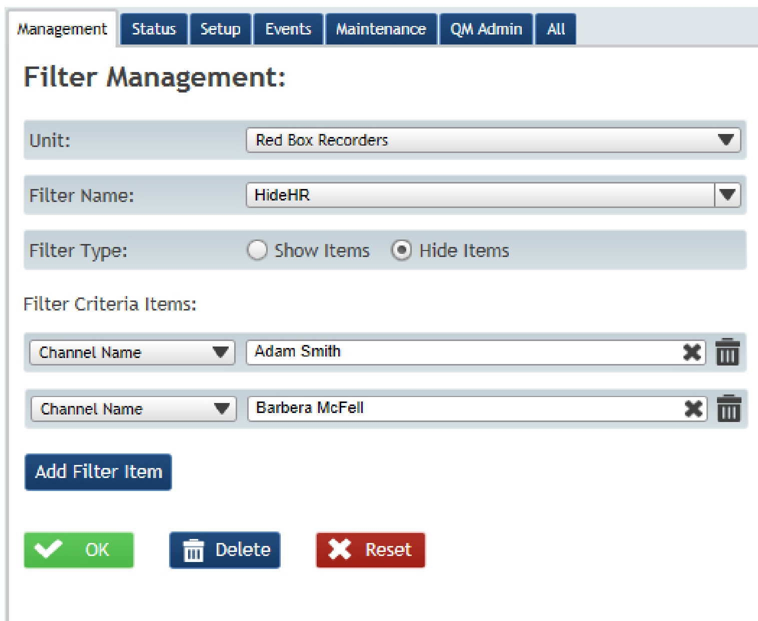
Note that filters do **not** apply to Quantify Live Acquire permissions.

Create a Filter

To create a filter:

1. Login to Quantify with an administrator account (System Configuration permissions).
2. Go to **Configuration** > **Management** > **Filter Management**.
3. Select your **Filter Type** — click **Show Items** or **Hide Items** (that is, show or hide items in search results).
4. Add your filter criteria — click **Add Filter Item**, select a database field and enter the data to match. You can also use the "**%**" wildcard character to broaden your criteria and ensure a match.
5. Click **Add Filter Item** to add further criteria — see "Multiple Criteria, Multiple Filters".
6. In the **Filter Name** field, type a name for your filter.
7. When you're done, click **Ok** to create your filter.

- In the sample filter shown in the screenshot below, this filter will **hide all** recorded communications **to/from** "Adam Smith" **and**
  to/from "Barbera McFell".



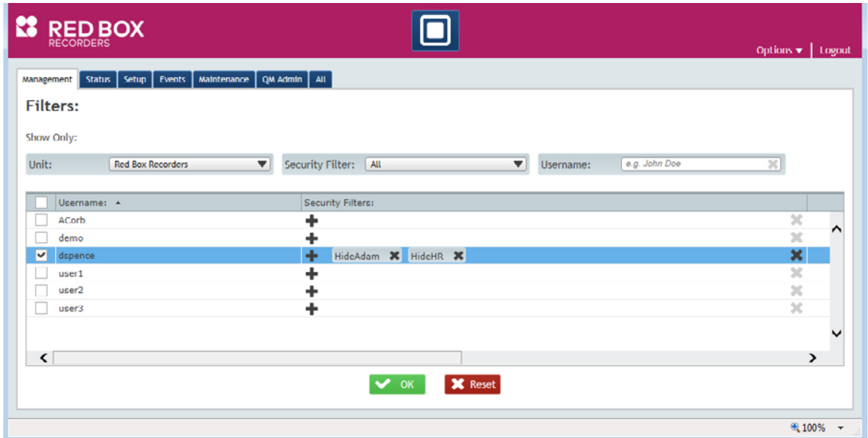
Contents

Apply/Remove Filters

Once you've created filters, you need to apply them to your Quantify users in order to assign the appropriate replay permissions, as described below. Also, see "Multiple Criteria, Multiple Filters" and "Assign Replay Permissions" for more detailed information.

To apply filters:

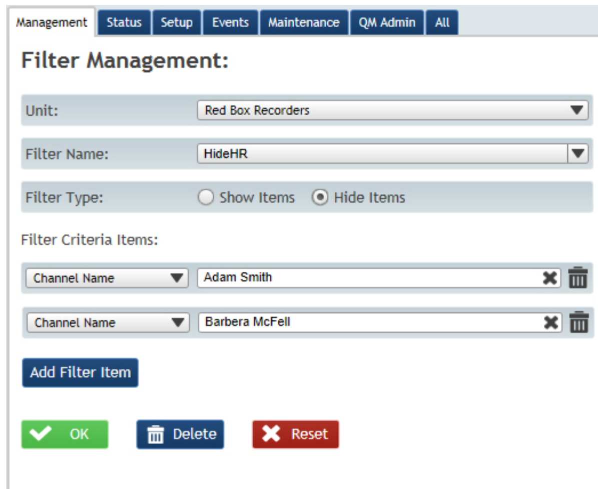
1. Go to **Configuration** > **Management** > **Filters**.
2. To apply/remove filters to/from Quantify users, click the **+** and **✕** icons. You can apply single or multiple filters to each user as needed.
3. When you're done, click the **Ok** button to apply your changes.



Review, Edit or Delete a Filter

To review, edit or delete a filter:

1. Go to **Configuration** > **Management** > **Filter Management**.
2. Select the filter to review/edit using the **Filter Name** drop-down menu:
   - To add criteria, click the **Add Filter Item** button.
   - To remove criteria, click the 🗑 **Remove** icon next to the filter criteria.
   - To edit criteria, just edit the filter criteria field and data as needed.
   - To delete the entire filter, click the main 🗑 **Delete** button.
3. When you're done, click the **Ok** button to save your changes.



Contents

Multiple Criteria, Multiple Filters

As stated previously, you can use multiple criteria within individual filters, and you can apply multiple filters to user accounts. When using multiple criteria and multiple filters, consider the following:

- **Multiple Criteria**
  - Multiple filter criteria of the same type are applied as a logical **OR**. That is, any recorded communication that matches **any** of the defined criteria is regarded as a match.
  - Multiple filter criteria of different types are applied as a logical **AND**. That is, any recorded communication that matches **all** of the defined criteria is regarded as a match.
- **Multiple Filters**
  - Multiple filters of the same type (show/hide) are applied as a logical **OR**. That is, any recorded communication that matches **any** of the applied filters is regarded as a match.
- **Allow (Show)/Deny(Hide) Replay**
  - To allow replay, you must allow access on **all** applied filters.
  - To deny replay, you only need to deny access on **one** applied filter.

Assign Replay Permissions

Refer to "How Do I Set Replay Permissions" for more detailed information. The following description provides a brief overview.

Assigning replay permissions defines what recorded communications a user has access to. The three main replay permission methods/types are:

- **Direct** (**All**, **None**, **Specific Field**): Assign via user account settings. Applies to Search & Replay and Monitoring (Live Acquire).
- **Specific Group**: Assign via user account settings. Applies to Search & Replay and Monitoring (Live Acquire).
- **Filters**: Assign via **Configuration** > **Management** > **Filters** (see "Apply/Remove Filters"). Applies to Search & Replay only.

Choose your method(s) carefully, apply consistently, and try to avoid conflicts. When assigning replay permissions, remember the two main rules:

- To allow replay, you must allow access on **all** applied permission types.
- To deny replay, you only need to deny access on **one** applied permission type.

www.redboxvoice.com
info@redboxvoice.com
+44 (0)115 937 7100

RBRQA1010 V1.3

Red Box

Contents

Red Box Recorders provides a powerful and flexible suite of applications and features to find, replay and manage your recorded communications. To provide and control access to these applications and features, you may need to configure licenses, general configuration settings, and user accounts – these are summarised below.

Summary

Quantify Applications

Application	Description	Enable, Disable, Configure
Assure, Daily System Check	Automatically tests that all devices are being recorded	• Licensed application – needs **Analytics** license on the recorder, and Daily System Check license in Quantify Insight. • All Quantify accounts with access to Quantify Insight (see below)can access the app. • For details, refer to the Quantify System Management Administrator Guide.
Event Reconstruct	Create and share timelines of recorded communications.	• Licensed application – needs licenses for **Replay Clients**, **Event Reconstruct Client** and **Event Reconstruct Concurrent Calls**. • To enable user access, tick **Event Reconstruct** option in User Account. Also requires appropriate replay permissions.
Insight	Dashboard for system status information.	• Licensed application – needs **Analytics** license. • Enable user access via Windows Active Directory. • For details, refer to the Quantify System Management Administrator Guide.
Live Acquire	Listen to live calls.	• Requires minimum of one Replay License. • To enable user access, tick **Live Acquire** option in User Account. Also requires appropriate replay permissions. • For information on Centralised Live Acquire, see "Centralised Live Acquire".
Quality Management	Call quality monitoring and performance assessment.	• Licensed application – needs **QM Clients** license. • To enable user access, set the appropriate **QM** options in the User Accounts. Also requires appropriate replay permissions. • For details, refer to the Quantify QM Guide.
Replay Authorisation	Fine control of who can replay recorded communications.	• Licensed application – needs **Replay Authorisation** license. • Set user roles via the **Replay Authorisation** options in User Accounts. • Define authorisation groups via **Configuration** > **Management** > **Replay Authorisation Groups**. • Also requires appropriate replay permissions for users. • For configuration details, see "Replay Authorisation - Setup".
Search & Replay	Search for and replay recorded communications.	• To enable user access, set appropriate replay permissions in User Account (no access if set to **None**). • Requires minimum of one Replay License for replay.

Contents

Quantify Features

Feature	Description	Enable, Disable, Configure
Audio Search	Search for spoken words.	• Licensed feature – needs **Audio Search** license. • Feature automatically available to all Search & Replay users – see above.
Blacklisting*	Control what communications are excluded from being recorded	• No separate license. • Enable/Disable via **Configuration** > **Setup** > **Misc Settings**. • Configure via **Configuration** > **Management** > **Blacklisting**. • For details, refer to the Quantify Recording Control Administrator Guide.
Call Delete	Delete calls from the recorder. License requires executive authority to purchase.	• Licensed feature – needs **Call Deletion** license. • To enable user access, tick **Call Deletion** option in User Account. • Feature available via Search & Replay – see above.
Call Export	Export call audio to WAV and call metadata to TXT, CSV, or XML.	• No separate license. • To enable user access, tick **Export** option in User Account. • Feature available via Search & Replay – see above. • For Bulk Export configuration, see "Install & Set Up Bulk Export".
CallSafe	Lock calls to prevent them being deleted.	• Licensed feature – needs **Callsafe** license. • To enable user access, tick **CallSafe** option in User Account. • Feature available via Search & Replay – see above.
Internal Calls*	Record internal calls, or not.	• No separate license. • Enable/Disable via **Configuration** > **Setup** > **Misc Settings**. • For details, refer to the Quantify Recording Control Administrator Guide.
Linked Calls*	Automatically identify linked calls (highlighted by the **+** Linked Calls icon).	• Licensed feature – needs **Linked Calls** license. • Feature automatically available to all Search & Replay users – see above. • Can be customised further by users, via their own **Replay Preferences** in Search & Replay.
Replay to Phone*	Replay audio to a phone rather than a PC.	• Licensed feature – needs **Replay to Phone** license. • Feature enabled/configured via user's **Options** menu in Search & Replay. • For configuration details, see "Replay to Phone - Client PC Setup".
Screen Data Capture:	Record PC screens.	• Licensed via Ekisa configuration app. • All record and replay PCs must have the appropriate Ekisa apps and services installed. • For configuration details, please contact Red Box Recorders.
Timeline View	Switch from the standard "grid" view to a Timeline view.	• Licensed feature – needs **Timeline View** license. • Feature automatically available to all Search & Replay users – **View Timeline** and **View Grid** buttons.
Workstation Client	PC client application with recording control features.	• Licensed feature – needs a **WSC** PP license with the appropriate feature options. Record on Demand also needs a separate **Record on Demand** license. • For details, refer to the Quantify Recording Control Administrator Guide.

* Feature not supported for all communication systems.

Contents

Replay Authorisation - Setup

Just like the feature, Replay Authorisation setup is very straight forward. First define your roles, and then set up groups to define which Authorisers can approve/reject replay requests from which Users.

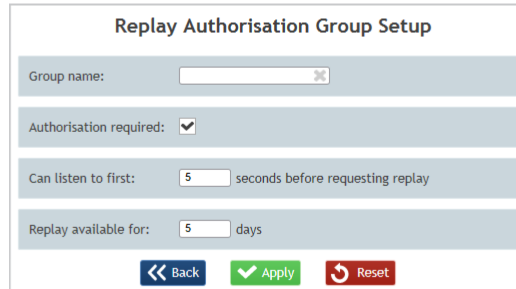
Define roles:

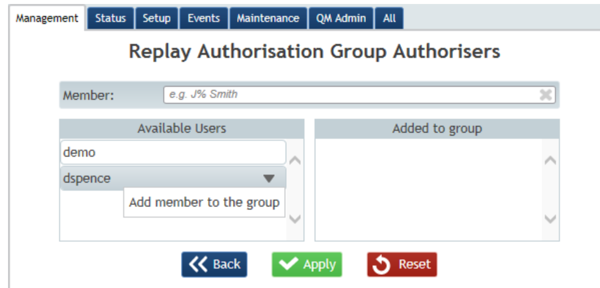
1. Login to Quantify with an administrator account (User Management permissions) and go to **Configuration** > **Management** > **Users**.
2. Highlight a user and click the **Edit** button.
3. In the **Replay Authorisation** panel select **Authoriser** or **User**.

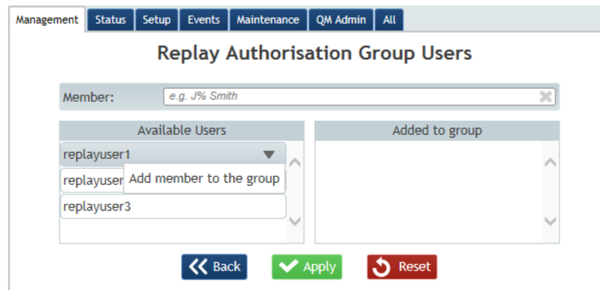
   If you don't select one of these replay authorisation roles, the Quantify user will be able to replay any recorded communication that they have replay permissions for, without requesting approval.

Set up groups:

1. Login to Quantify with an administrator account (User Management permissions) and go to **Configuration** > **Management** > **Replay Authorisation Groups**. Click the **Create** button, and enter your group details:
   - **Group name**: Descriptive group name.
   - **Authorisation required**: Tick — the Authoriser must specifically authorise, or reject, every replay request.
     Untick — all requests are automatically authorised. This can be useful where you want to allow full replay access, but you still want to have all replay requests logged and recorded for future reference (see **Configuration** > **Events** > **Replay Authorisation**).
   - **Can listen to first**: Set the preview length for all group Users.
   - **Replay available for**: Set the replay availability length for all group Users (for approved requests).
2. Once you've created a group, you can add members — highlight a group in the list and click the **Authorisers** or **Users** button. Now click an **Available** member on the left and select **Add member**. You can select as many Authorisers and Users as needed.







Contents

Previous Menu Next

Install & Set Up Bulk Export

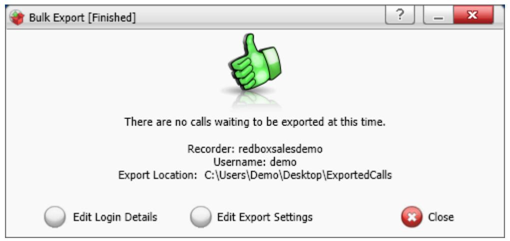
In general, a system administrator will install and set up Bulk Export, but it's pretty straightforward for anyone with a little PC knowledge.

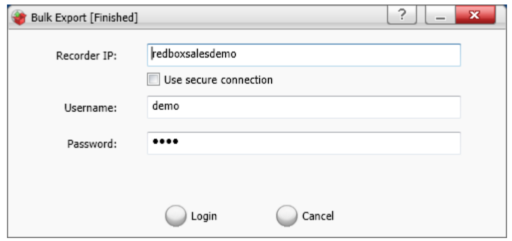
Install

To install the Bulk Export application on a client PC, simply download and run the Bulk Export Installer (**bulkexport.msi** file). If you don't have this file, you can download it from the recorder — login to Quantify and go to **Options** > **Support Centre** > **Downloads** > **Bulk Export Application**

Login

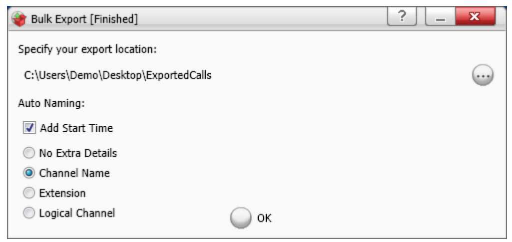
The Bulk Export application needs to be provided with the appropriate Quantify login details, for the user account used to export calls on the client PC. The easiest way to do this is to login to Quantify using that account and perform a bulk export which will automatically complete the login details. If you can't login to the account or you ever need to change login details (for example, changing Quantify users on the client PC), then simply run the Bulk Export application from the Windows Start menu and click **Edit Login Details**.





Bulk Export Settings

To set filename and location options for your exported calls, run the Bulk Export application from the Windows Start menu and click **Edit Export Settings**.



Contents

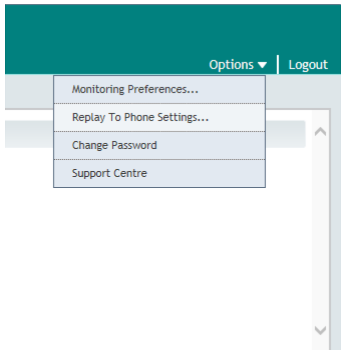
Replay to Phone - Client PC Setup

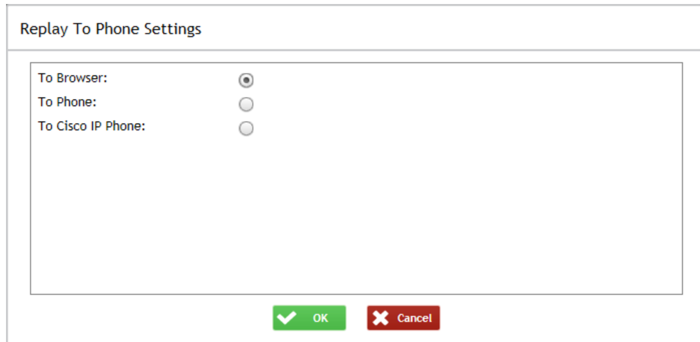
Follow the steps below to set up a Replay to Phone client. Note that you will need system information in order to set up Replay to Phone, so see your system administrator for help if you need to.

To set up a replay to phone client:

1. On the client PC, login using the user account.
2. From the Search & Replay application, click the **Options** menu and select **Replay to Phone Settings**.
3. Select the **To Phone** (including SIP phone) or **To Cisco IP Phone** option depending on your telephony integration type.
4. Edit the phone and email settings as needed — see "Phone & Email Settings".
5. When you're done, click **OK** to apply your changes.

Once phone & email settings have been applied, the settings are remembered. Therefore, the Quantify user can switch between the **To Browser** and the **To Phone** or **To Cisco IP Phone** options as required, without having to re-enter the information.

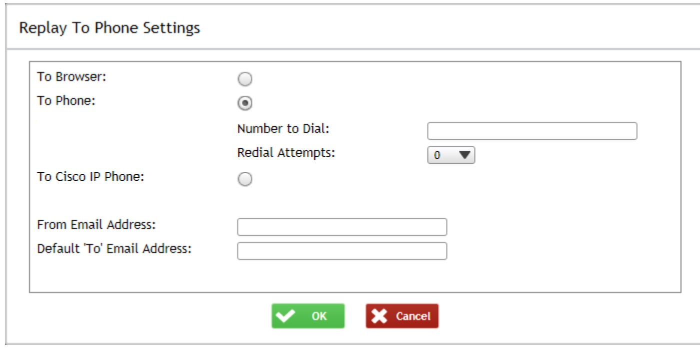


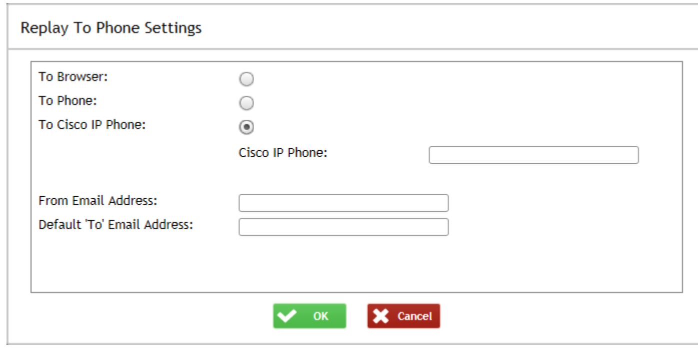


Contents

Phone & Email Settings

The tables below provide detailed information on each of the **Replay to Phone** settings — **Options** > **Replay to Phone Settings** > **To Phone** / **To Cisco IP Phone**





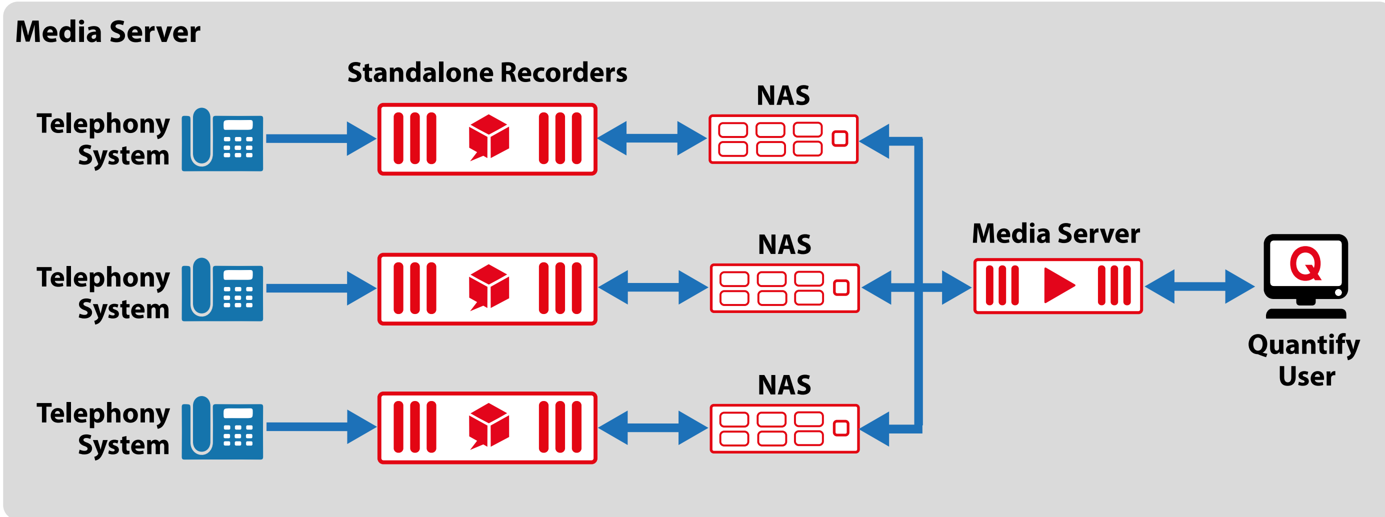
To Phone	
Number to Dial	Extension number used to replay the audio. Note that this extension needs to be part of the network "visible" to the Red Box recorder. When a call is replayed, the Red Box recorder will dial the stated extension number and replay the call.
Redial Attempts	Number of redial attempts to perform if there's no answer.
From Email Address	"From" Email address to use if a call is exported to a WAV file using the **Email** option during playback. Note that the user would need export permissions.
Default "To" Email Address	Email address to send call audio to, if exported using the **Email** option during playback. Note that the user would need export permissions.

To Cisco IP Phone	
Cisco IP Phone	Cisco IP phone number used to replay the audio. Note that this extension needs to be part of the network "visible" to the Red Box recorder.
From Email Address	"From" Email address to use if a call is exported to a WAV file using the **Email** option during playback. Note that the user would need export permissions.
Default "To" Email Address	Email address to send call audio to, if exported using the **Email** option during playback. Note that the user would need export permissions.

Contents

Centralised Live Acquire

Centralised Live Acquire makes use of a Media Server within a multi-recorder system, allowing users to login to Quantify, use Quantify Live Acquire as normal, **and** have "visibility" of **all** channels across **all** recorders.



Considerations

Once Centralised Live Acquire has been configured on your system, you may wish to consider the following:

- To use Centralised Live Acquire, your users will need to log in to the Media Server, if they weren't already.
- User accounts have an additional option in the **Permissions** panel **– Show Centralised Information**. If this option is ticked, a user can "filter" by recorder when using the Quantify Live Acquire application. This option is usually most useful for system administrators.
- Since users have "visibility" of all channels across all recorders, you may wish to look at replay permissions again.
- During setup, a Quantify Centralisation license is applied to each recorder and the Media Server. Also, the Media Server is configured as the "lead server". These setup steps allow Quantify system configuration settings on the "lead server" to be propagated across all recorders – therefore:
  - Any configuration related to individual recorders (such as enabling channels) should be performed on the recorder.
  - Any configuration related to the "system" (such as user accounts) should be performed on the Media Server. These are as follows: Active Directory Settings, Users, Enterprise Communications User, Groups, and Filters. Obviously, these system configuration settings are only accessible from the "lead server".
- When using Centralised Live Acquire, user account passwords don't support all the characters which are currently supported in Quantify. This is due to encryption restrictions which Centralisation depends on to share information between servers. The supported characters are: 0-9, a-z, A-Z, _ **–** @ . (dot). If a user has an account password which uses characters outside of the supported set, this can cause replay issues within Live Acquire. We therefore recommend that system administrators inform Live Acquire users of this password restriction.

Contents

Centralisation Setup

To set up a centralisation group (a Media Server and all associated recorders):

1. Apply licenses.
2. Configure the Media Server.
3. Check the system.

For details, refer to the step-by-step tables below. Note that this process requires server restarts and will automatically log users off the various servers. Therefore we recommend these steps are performed outside of normal operating hours.

Apply licenses:

1. Login to the Media Server and each of the recorders in turn using a system administrator account.
2. Go to **Configuration** > **Setup** > **Licensing** and check the current license status for **Centralisation** in the Quantify Licensing panel.
3. If needed, enter a license code and click the **Update** button to make your changes. If you've applied a new **Centralisation** license, you'll need to restart the server to apply the license. Although not essential, we recommend that you prepare and download config & diag files before performing a restart:
    - **Prepare (Create)**: Go to **Configuration** > **Maintenance** and click **Prepare Config** or **Prepare Diagnostic**. Enter a filename and click the **Prepare** button to create the file. Note that server performance can be affected.
    - **Download**: Go to **Configuration** > **Maintenance** > **Download Files** and select the file to download. Click the **Empty** button to clear the file folder on the server.

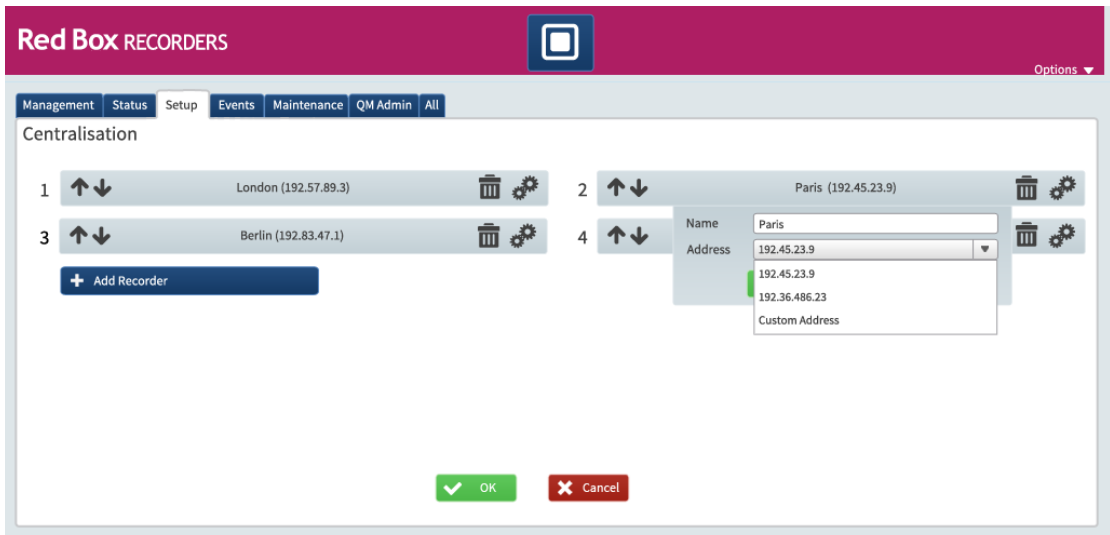
   To perform the restart, go to **Maintenance** > **Recorder**, select the **Restart** radio button and then click the **Stop Recorder** button.

Contents

Set up the Media Server:

1. Login to the Media Server using a system administrator account.
2. Before doing any configuration, first check that the Media Server has all user accounts that need to be shared across the system **–** go to **Configuration** > **Management** > **Users** and check the list.
3. Now go to **Configuration** > **Setup** > **Centralisation**, click the **Add Recorder** button, and enter details for the Media Server – a "user friendly" name plus IP address. This will define the Media Server as the lead server. Click the **Update** button to apply the changes.
4. Click the **Add Recorder** button again and enter details for a recorder that you want to include in this centralisation group – a "user friendly" name plus IP address. Repeat this for each recorder you want to add. Note that:
   - You can't add a recorder that's part of another centralisation group.
   - As stated above the server listed as number **1** (the Media Server) is regarded as the lead server. If the Media Server fails at any point, then the next server in the list (number **2**, obviously) will temporarily takeover as the lead server for centralisation, until server **1** is "back online". This continues, in order, for each server in the list.
   - If you want to change the hierarchy of recorder servers at any point, just use the **Move Up**/**Move Down** buttons or drag & drop the servers in the list.
   - If you need to change any of the server details, or remove one, click the **Configure** (cogs) or **Remove** (trash) icon.

   Once you've added all the required recorder servers, click the **Update** button to apply the setup changes. Note that any users currently logged into the individual recorders will be temporarily logged out.
5. Lastly, set an Enterprise Communications Account for the Media Server **–** this account is used by the Media Server to access all recorders in the system for centralised configuration settings. This account needs to have full replay permissions, admin permissions, and **not** an Active Directory account. To select an account, go to **Configuration** > **Setup** > **Misc Settings**, select an account, and click **Update**.



Contents

Check the system:

1. Login to the Media Server using an administrator account with Replay, Live Acquire, and Centralised Information permissions.
2. Go to **Live Acquire**, select the **Channel Overview** tab and check that all expected channels are visible. If needed, live acquire a call and/or perform a previous call search.
3. Go to **Configuration** > **Management** > **Users** and create a new (temporary) user account. Now login to one of your recorders using the temporary account, to check that user accounts are being synchronised across your system.

Centralised Live Acquire is now successfully configured across your Red Box multi-recorder system.

Contact Centre Aware Live Acquire

This optional Live Acquire feature can be used in a standalone or centralised Live Acquire environment, and allows system administrators to define Live Acquire groups and provide access to those groups for Quantify users.

Considerations

As a system administrator, if you plan to implement Contact Centre Aware Live Acquire you need to consider the following:

- Once Contact Centre Aware Live Acquire is enabled, your users will no longer be able to create their own groups in Live Acquire. You will define their groups for them.
- Live Acquire groups are defined using channel groups and security filters. If you've used security filters previously to define replay permissions, these security filters will now also apply to Live Acquire (which they didn't previously) – you may wish to review the impact of these new settings.

Setup

To set up Contact Centre Aware Live Acquire:

1. Apply the **Contact Centre Aware Monitoring** license.
2. Create Live Acquire Groups.
3. Apply your Live Acquire Groups to your Quantify users, as needed.

For details, refer to the step-by-step tables below.

Apply license:

1. Login to the recorder using a system administrator account.
2. Go to **Configuration** > **Setup** > **Licensing** and check the current license status for **Contact Centre Aware Monitoring** in the Quantify Licensing panel. If needed, enter a license code and click the **Update** button to make your changes. There's no need to restart the recorder.

Contents

Create Live Acquire groups:

Creating Live Acquire groups is a two stage process – first create channel groups, then create security filters to match your groups.

Create Channel Groups:

1. Login to the recorder using a system administrator account. Note that for a centralised system, login to the Media Server to create groups.
2. Go to **Configuration** > **Management** > **Groups** and click the **Configure Groups** button.
3. Type your group name in the **Add group** field and click the **Add** button. Your new group will now be listed in the group list.
4. Click the **Configure Members** button. This will display the **Group Member** list.
5. Use the list to configure your group members (channels):
   - To add a member to a group, click a **+** icon and select the group.
   - To remove a member from a group, click the appropriate ✕ icon.
   - To remove a member from all groups and from the list, click the **Delete** icon. Note that this just removes the member from the **Group Member** list, but doesn't delete the actual channel/channel name.
6. When you're done, click the **Apply** button to save your changes.

Create Security Filters:

1. Login to the recorder with a system administrator account and go to **Configuration** > **Management** > **Filter Management**. Note that for a centralised system, login to the Media Server to create filters.
2. Select your **Filter Type** – for filters used with Live Acquire, select **Show Items**.
3. Add your filter criteria – click **Add Filter Item**, select the **Group** database field, and enter the group name.
4. In the **Filter Name** field, type a name for your filter – you'll probably want this to match the **Group** name.
5. When you're done, click **Ok** to create your filter.

When you're finished, you'll have a set of security filters that match your channel groups. These now define your Live Acquire groups and can be applied to individual user accounts as needed – see "Apply Live Acquire Groups to Quantify users:" on page 4.

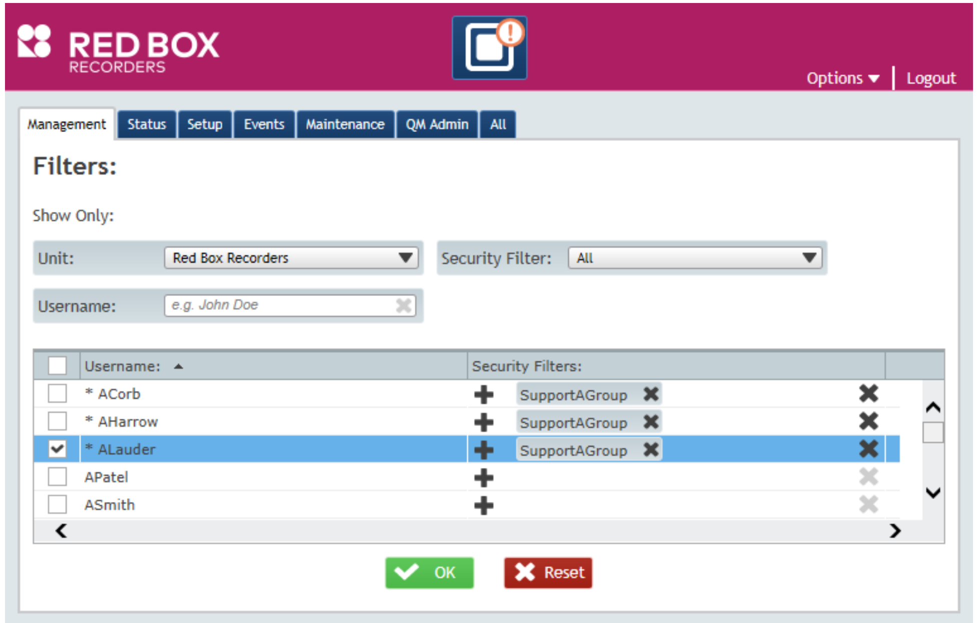
Contents

Previous
Menu
Next

Apply Live Acquire Groups to Quantify users:

1. Login to the recorder with a system administrator account and go to **Configuration** > **Management** > **Filters**. Note that for a centralised system, login to the Media Server to create filters.
2. To apply/remove filters (Live Acquire Groups) to/from Quantify users, click the **+** and **✕** icons. You can apply single or multiple filters to each user as needed.

   Note that, as a reminder, by applying a filter (Live Acquire Group) to a user, you are giving them Replay and Live Acquire permissions for all channels within that group.
3. When you're done, click the **Ok** button to apply your changes.



www.redboxvoice.com
info@redboxvoice.com
+44 (0)115 937 7100

RBRQQA1029 V1.3

How Do I Manage Active Directory

Contents

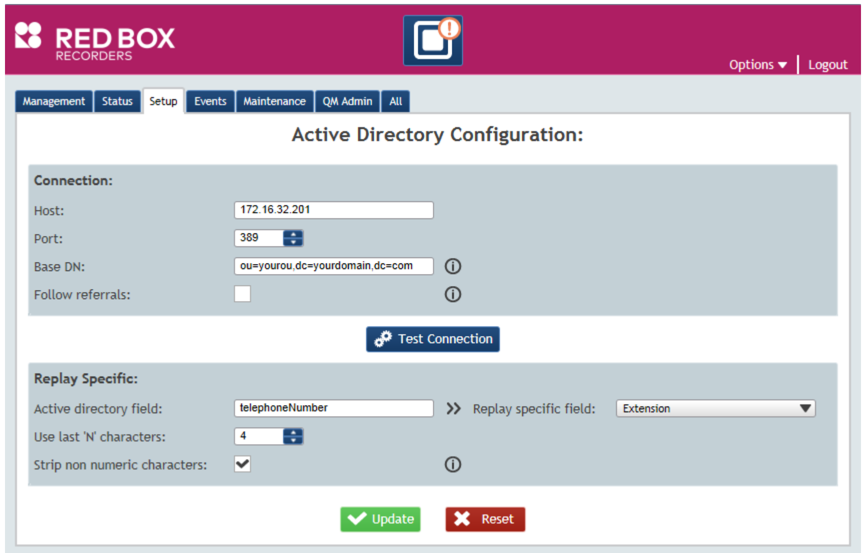
Your Red Box Recorder supports Windows Active Directory integration and Single Sign-On. This topic covers the setup and management of Active Directory and Single Sign-On as it relates to the recorder — general Windows configuration is **not** covered.

Windows Active Directory Setup

Windows Active Directory support allows you to synchronise accounts between your recorder and Active Directory server.

To configure Windows Active Directory on the recorder:

1. Login to the recorder using a Quantify system administrator account with system configuration permissions, and go to **Configuration** > **Setup** > **Active Directory**
2. Enter the **Connection** and **Replay** details (see below). You can click the **Test Connection** button to test the connection to your Active Directory server.
3. When your done, click the **Update** button to save your changes. See "Login & Accounts" for details of the Quantify login and account creation process.

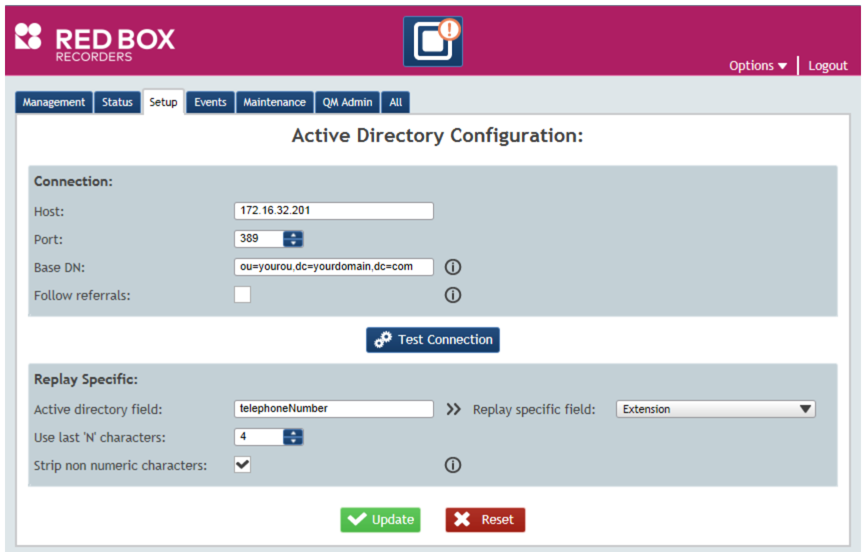


Contents

Connection & Replay Settings

Connection Options	
Host	IP address of the Active Directory server to use.
Port	Active Directory server port to use.
Base DN	Base domain names to start searching for users.
Follow Referrals	Allows Quantify to follow LDAP referrals (search continuations). You may need to enable this option if you have Active Directory accounts stored on multiple domains or domain controllers.

Replay Options	
Active Directory Field >> Replay Specific Field	Allow Active Directory field data to be used to apply direct replay permissions on automatically created user accounts. Data from the specified **Active Directory Field** is used for the selected Quantify database field (**Replay Specific Field**), and is applied to the user account's Replay Permissions — **Replay** set to **Specific**, **Field** set to the selected **Replay Specific Field** and **Data** set to the data from the **Active Directory Field**. See "Login & Accounts" below for an example (item 3).
Use Last "N" Characters	Only use the last "N" characters from the **Active Directory Field**.
Strip Non-Numeric Characters	Remove any non-numeric characters from the **Replay Specific Field**.



Contents

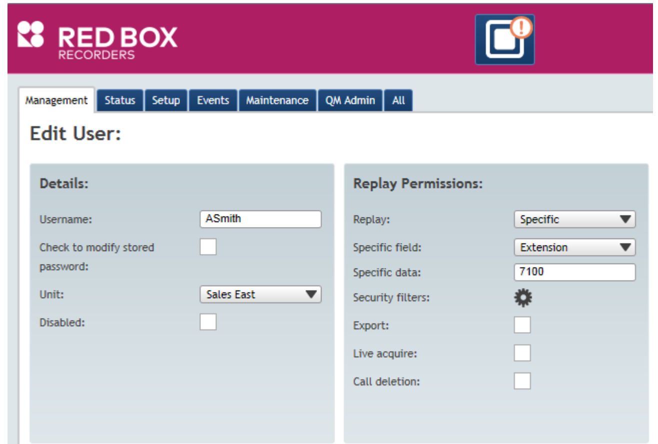
Login & Accounts

Once Active Directory settings have been configured, the following occurs when a user logs in to Quantify:

1. If the user already exists in Quantify but **not** in Active Directory, then the user logs in as usual and the password is validated against the recorder.
2. If the user doesn't already exist in Quantify or in Active Directory, then the login fails.
3. If the user doesn't already exist in Quantify but **is** in Active Directory, then the password is validated against Active Directory and if OK a user account is automatically created in Quantify with direct Replay Permissions defined by the **Replay Options** listed above.

   For example, using the sample settings shown in "Windows Active Directory Setup", let's say Adam Smith logs into Quantify for the first time. His direct office phone number is +441159377100. His password is checked against the Active Directory entry and a new Quantify user account is created with direct replay permissions — **Replay** set to **Specific**, **Field** set to **Extension**, and **Data** set to **7100**. This means Adam would be able to search and replay his own calls only.

   Once a user account has been automatically created, a system administrator can then assign further replay, application, and feature permissions as needed.



4. Once a user has a Quantify account **and** is in Active Directory, the password is validated against Active Directory and the user's Replay Permissions are loaded from the Quantify user settings.

   Note that if Active Directory is set up once Quantify users have already been created on the recorder, we recommend that a system administrator pro-actively resolves any account conflicts **before** applying Active Directory support.

Contents

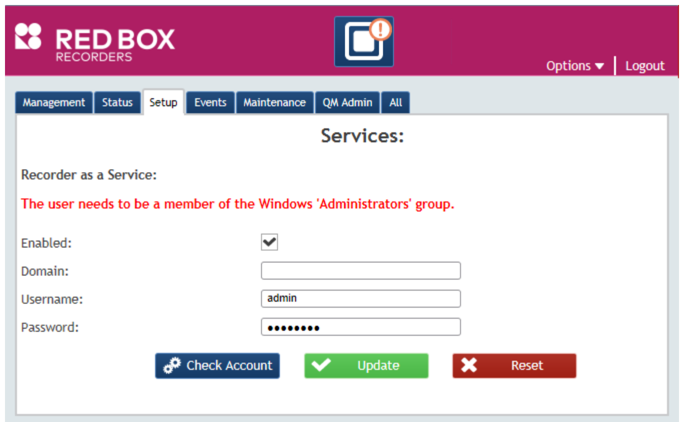
Single Sign-On

For complete account synchronisation, you can also enable single sign-on so that once a user has signed into a PC there's no need to sign into Quantify. To set up single sign-on, first configure and restart the recorder, then configure the browser on client PCs.

Configure Recorder

To enable Single Sign On:

1. Login to the recorder using a Quantify system administrator account with system configuration permissions, and go to **Configuration** > **Setup** > **User Options**.
2. In the **Logins** section, tick the **Enable Single Sign-On** option. If this option is not available, Windows Active Directory has not been configured correctly — see "Windows Active Directory Setup".
3. Go to **Configuration** > **Setup** > **Services** and tick **Enabled** to allow the recorder to be used as a service. Enter the username, password and domain for the Active Directory account you want to use to run the service. This account needs to be a local Windows Administrator and have permissions to browse your Active Directory to validate user logins. Note that if you already run the recorder as a service, this step may not be needed.
4. Restart the recorder to apply the changes — see "Restart Recorder" below.



Contents

Restart Recorder

Restart your recorder to apply single sign-on. Note that a restart can take a number of minutes and no recording will take place during the restart, therefore we recommend this is done outside of normal usage hours.

To restart your recorder:

1. Although not essential, we recommend that you prepare and download config (Configuration) & diag (Diagnostics) files before performing a restart:
    - **Prepare (Create)**: Go to **Configuration** > **Maintenance** and click **Prepare Config** or **Prepare Diagnostic**. Enter a filename and click the **Prepare** button to create the file. Note that recorder performance can be affected.
    - **Download**: Go to **Configuration** > **Maintenance** > **Download Files** and select the file to download. Click the **Empty** button to clear the file folder on the recorder.
2. To perform the restart, go to **Maintenance** > **Recorder**, select the **Restart** radio button and then click the **Stop Recorder** button.

Contents

Set Up Internet Explorer and/or Chrome

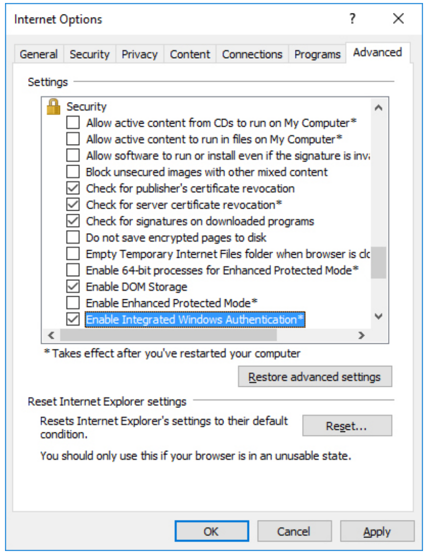
The following settings are in addition to the "standard" Internet Explorer and Chrome setup for Quantify.

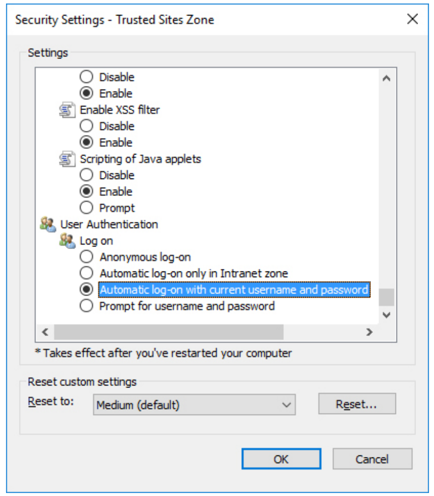
To set up Internet Explorer and/or Chrome on a client PC:

The following steps use Internet Explorer to configure settings. If you're using Google Chrome, these settings will be inherited/imported when you next open Chrome.

1. Enable Integrated Windows Authentication — go to **Internet Explorer** > **Tools** > **Internet Options** > **Advanced**, scroll to the **Security** section and tick the **Enable Integrated Windows Authentication** option.
   Click **Apply** and then **Ok**.
2. Set User Authentication options — in the **Security** tab click the **Custom level** button, scroll to the **User Authentication** section and select **Automatic logon with current user name and password**.
3. Restart the PC for the changes to take affect.

Note that Chrome support for call replay is only provided in Quantify Release 4B and later.





Contents

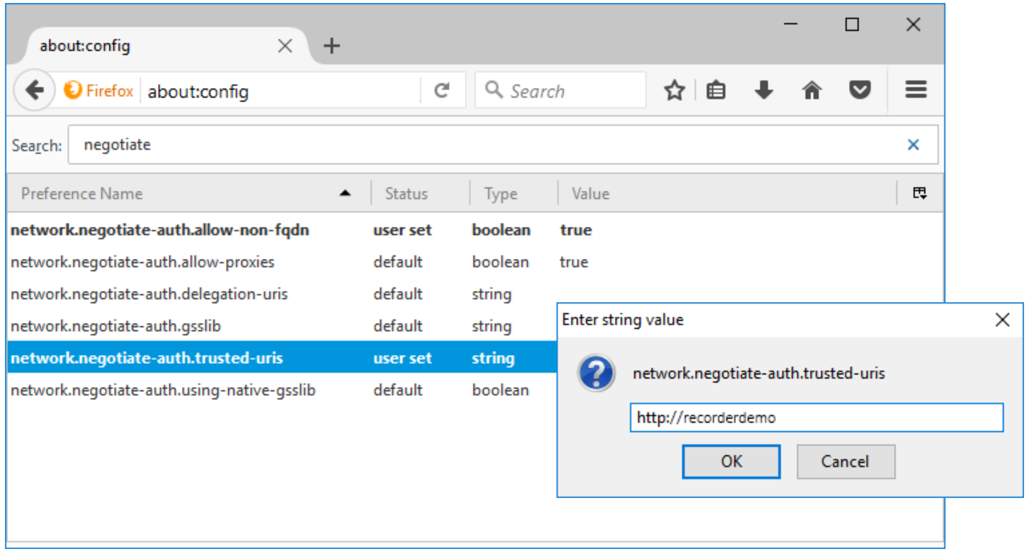
Set Up Firefox

The following settings are in addition to the "standard" Firefox setup for Quantify.

To set up Firefox on a client PC:

1. Enable Integrated Windows Authentication:
   - In Firefox enter **about:config** in the address bar. Click the "confirm" button to skip the warning, if displayed.
   - Type "**negotiate**" in the **Search** box and double-click the **network.negotiate-auth.trusted-uris** preference.
   - In the **value** dialogue box, add the recorder address using http or https as required. When you're done, click **OK**.
   - Double-click the **network.negotiate-auth.allow-non-fqdn** preference to set its value to **true**.
2. Restart the PC for the changes to take affect.

Note that Firefox support for call replay is only provided in Quantify Release 4B and later.



www.redboxvoice.com
info@redboxvoice.com
+44 (0)115 937 7100

RBRQQA1042 V1.1

Red Box

How Do I Manage Licenses

1

Contents

The Red Box software is designed to provide flexible licensing options for individual applications and features. This topic covers all licensing options.

Check & Apply Licenses

To check and apply licenses:

1. Login to Quantify with an administrator account (System Configuration permissions) and go to **Configuration** > **Setup** > **Licensing**. From here you can check your current licenses.

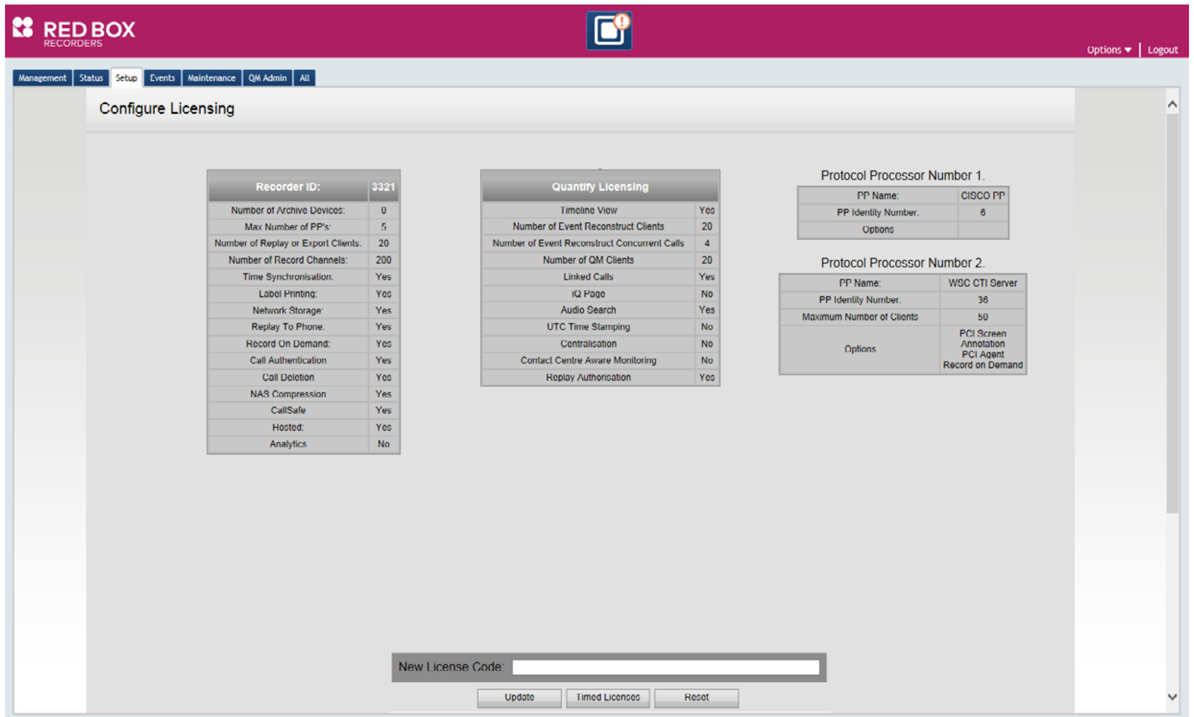
   To view "Time Limited" licenses, click the **Timed Licenses** button.

   See "License Types" for more details on the licenses available.

2. If you have a new license code, enter the code in the **New License Code** field and click **Update** to apply the license.

   For some license types you will need to restart the recorder to apply the license (see "License Types" and "Recorder Restart").

   If you need to purchase a new license, or need to be advised of an existing license code, please contact your dealer or Red Box.



* Screen layout modified for display purposes.

Contents

License Types

Use the following tables to review the license types available from Red Box. If a recorder restart is required to fully apply the license, see "Recorder Restart".

Recorder Licenses

General licenses that apply directly to the recorder.

License	Description	Restart Required?
Number of Archive Devices	Maximum number of removable archives (DVD and Tape). Note that a dual drive system counts as two archive devices.	Y
Max Number of PP's	Maximum number of Protocol Processor (PP) licenses. This refers to the total number of integration types licensed on the recorder and can refer to a telephony type (e.g. Cisco, Avaya, Mitel), trader turret type (e.g. BT Unified Trading, Etrali Open Trade), radio type (e.g. Motorola Astro), mobile telephony type (e.g. Vodafone, Teleware), PC comms (e.g. Cisco IM, Skype), or PC support (WorkStation Client **–** PCI suppression, agent call annotation, agent record on demand, channel naming). See "Protocol Processor (PP) Licenses" for more details.	N
Number of Replay or Export Clients	Maximum number of users that can concurrently replay or export recorded communications. See "Replay Licenses" for more details.	N
Number of Record Channels	Maximum number of channels (devices) that can be recorded simultaneously — this includes any valid "temporary" time limited licenses. See "Record Licenses" and "Time Limited Licenses".	N
Time Synchronisation	Enable time synchronisation (SNTP).	Y
Label Printing	Enable label printing. This feature is used to create labels for removable archive media — go to **Configuration** > **Status** > **Media**.	Y
Network Storage	Allow use of Network Storage (NAS) — Callstore Extension or Network Archive.	Y
Replay to Phone*	Allow calls to be replayed to a phone (selected via the **Options** menu in Search & Replay).	Y
Record on Demand	Enable use of agent Record on Demand with WorkStation Client.	N
Call Authentication	Enable Call Authentication. This enables both the digital signature within the recorder and the Call Authentication tab in the Quantify Media Player.	Y
Call Deletion	Enable use of the Call Delete feature. Call Delete is usually a restricted feature — access is assigned within user account settings.	Y
NAS Compression*	Allow use of a NAS Compression server.	N
Callsafe	Enable use of the Callsafe feature. Callsafe is usually a restricted feature — access is assigned within user account settings.	Y
Hosted	Display features and options for Quantify Hosted. Note that once Hosted has been licensed on a recorder, it cannot be "unlicensed"/disabled.	Y
Analytics	Enable use of Quantify Insight.	Y

* Feature not supported for all communication systems.

Contents

Quantify Licenses

General licenses that apply to the Quantify software suite.

License	Description	Restart Required?
Timeline View	Allow use of the Timeline View in Quantify Search & Replay.	N
Number of Event Reconstruct Clients	Maximum number of concurrent Quantify Event Reconstruct users.	N
Number of Event Reconstruct Concurrent Calls	Maximum number of concurrent communications (voice call, video call, IM, text messages, screen recording) that can be used with Event Reconstruct.	N
Number of QM Clients	Maximum number of Agents that can be used with Quantify Quality Management (QM).	Y
Linked Calls*	Enable automatic identification of linked calls (highlighted by the **+** Linked Calls icon). This feature can be customised further by users, via their own **Replay Preferences**.	N
iQ Page	Historic feature. No longer enabled.	—
Audio Search	Enable Quantify Audio Search — search for spoken words and phrases.	Y
UTC Time Stamping	Enable UTC Time Stamping (Coordinated Universal Time) of recorded communications. If UTC is **not** enabled, the recorder's local time is used. Note that once UTC has been licensed on a recorder, it cannot be "unlicensed"/disabled.	Y
Centralisation	Enable Centralised Live Acquire — allow the use of Centralised Live Acquire on a Media Server giving "visibility" of all channels across a multi-recorder systems.	Y
Contact Centre Aware Monitoring	Enable Contact Centre Aware Monitoring — for multi-recorder systems, allow Monitoring (Quantify Live Acquire) to show the status of channels (devices) from all recorders.	N
Replay Authorisation	Enable use of the Replay Authorisation feature — request and allow/deny replay.	Y

* Feature not supported for all communication systems.

Contents

Protocol Processor (PP) Licenses

Protocol Processor (PP) licenses refer to the integration types licensed on the recorder.

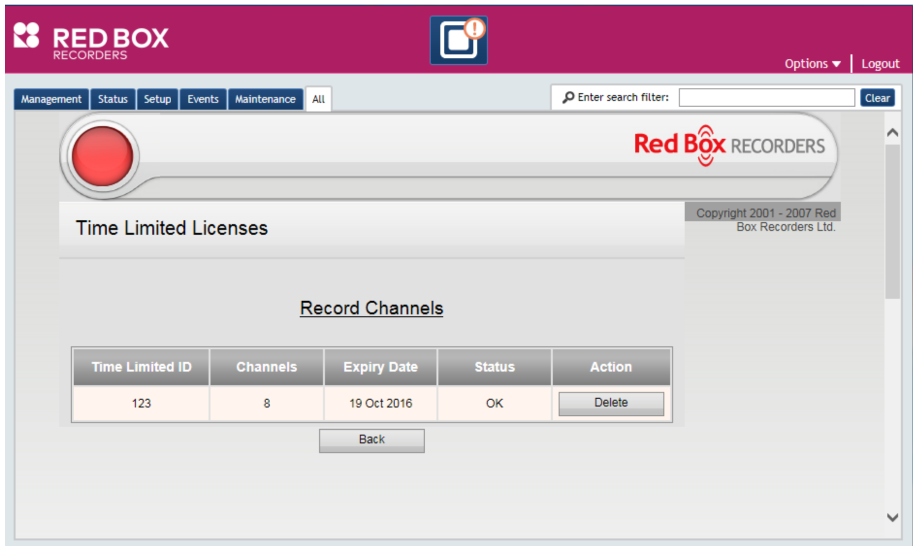
PP Type	Description	Restart Required?
Telephony **Trader Turret** **Radio** **Mobile Telephony** **PC Comms**	Integration type(s) licensed on the recorder — license will refer to a telephony type (e.g. Cisco, Avaya, Mitel), trader turret type (e.g. BT Unified Trading, Etrali Open Trade), radio type (e.g. Motorola Astro), mobile telephony type (e.g. Vodafone, Teleware), or PC comms type (e.g. Cisco IM, Skype). Red Box actively supports over 50 integration types — too many to list here.	Y
PC Support	WorkStation Client — This is a slightly unique integration type and refers to PC support, covering PCI suppression, agent call annotation, agent record on demand, and channel naming.	Y

Time Limited Licenses

Time Limited Licenses can be used to temporarily enable additional channels on your recorder. This can be useful, for example, when trying to satisfy seasonal variations or for evaluation purposes. To view time limited licenses, click **Timed Licenses**.

License	Description	Restart Required?
Number of Record Channels - Time Limited	Defines the number of additional channels (devices) that can be recorded simultaneously, which are applied on a "temporary basis" until the defined **Expiry Date**.	N

As a time limited license approaches and exceeds the expiry date, this is shown in the **Status** field. You will also receive notifications via events and alarms.



Contents

Monitor & Manage Licenses

In general, licenses require very little attention — simply use **Licensing** within the **Configuration** app to monitor and manage your licenses, and you will also receive notifications via events and alarms if there are any issues.

The two most "dynamic" license types are the record licenses (maximum number of channels that can be recorded simultaneously) and replay licenses (maximum number of users that can concurrently replay or export recorded communications). Issues with these licenses can result in calls not being recorded or users being unable to replay calls, so they may need to be monitored a little more closely.

Replay Licenses

A replay license is used whenever a user attempts to replay or export a call using any Quantify application. The license is not released until that user performs a logout — that is, they click **Logout** in Quantify, not just close their browser or the Quantify tab. Once the user performs a logout, the replay license is released and becomes available for another user.

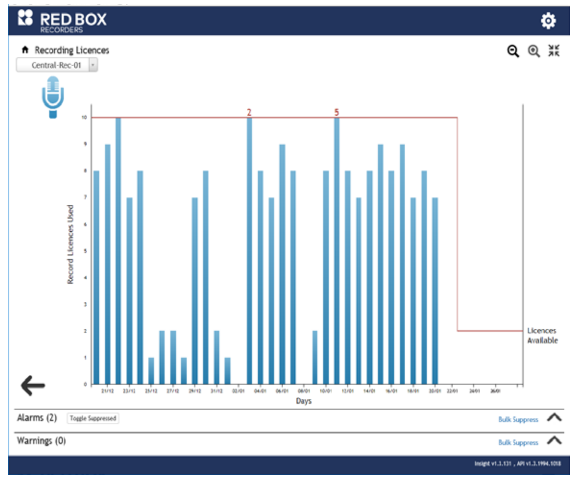
With this in mind, it's advisable to promote a simple login/logout etiquette so that licenses are used and released efficiently. To monitor and manage this, go to **Configuration** > **Status** > **Logged in Users** — here you can see the number of logged in users and the number of allocated replay licenses. To force a logout, simply click the user's name — you'll be asked to confirm the logout.

If you have Quantify Insight installed, you can use the **Users** status indicator to keep an eye on your replay licenses. You can even have alerts sent to you via email so there's no need to constantly monitor the status for issues.

Record Licenses

Similar to a replay license, a record license is used whenever recording is started for a channel (device). To see how many devices are being recorded, go to **Configuration** > **Status** > **Recorder Status**.

As with replay licenses, if you have Quantify Insight installed, you can use the **Recording Status** indicator to keep an eye on your record licenses. You can even have alerts sent to you via email so there's no need to constantly monitor the status for issues.



Contents

Recorder Restart

As indicated in "License Types", some licenses require a recorder restart before the license is fully applied. Follow the steps below to restart your recorder — note that a restart can take a number of minutes and no recording will take place during the restart, therefore we recommend this is done outside of normal usage hours.

To restart your recorder:

1. Although not essential, we recommend that you prepare and download config (Configuration) & diag (Diagnostics) files before performing a restart:
   - **Prepare (Create)**: Go to **Configuration** > **Maintenance** and click **Prepare Config** or **Prepare Diagnostic**. Enter a filename and click the **Prepare** button to create the file. Note that recorder performance can be affected.
   - **Download**: Go to **Configuration** > **Maintenance** > **Download Files** and select the file to download. Click the **Empty** button to clear the file folder on the recorder.
2. To perform the restart, go to **Maintenance** > **Recorder**, select the **Restart** radio button and then click the **Stop Recorder** button.

Troubleshooting

Troubleshooting licenses is pretty straightforward. If an attempt is made to exceed license restrictions (try to exceed number of replay or record licenses, attempt to use an unlicensed feature, etc.) then an appropriate error message will be displayed and/or an event/alarm will be raised.

If you enter a new license code within **Licensing** and you get an error message stating "The license code entered was invalid":

- Firstly, check the license code you've been provided with and re-enter the code. Make sure you enter the hyphen characters and check for the obvious similarities between letter "O" and number "0", letter "I" number "1", letter "S" number "5", etc.
- License codes are associated with an individual Recorder ID — make sure you're using the correct recorder and license "combination".

www.redboxvoice.com
info@redboxvoice.com
+44 (0)115 937 7100

RBRQQA1007 V1.3

Red Box