Red Box

Quantify Recording Control Administrator Guide

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

Select what to record, or not record...

- Manage Channels
- Manage Calls
- WorkStation Client
- Screen Recording

Monitor & maintain...

- Recording Alarms
- 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 Recording Control - Admin Guide

About

You have full control over what to record or not record across your Red Box System. You can enable/disable individual channels/devices, choose to record internal calls or not, Blacklist specific communications, and even put control in your agents' hands. To make sure you're recording when you should be, you can also configure and monitor alarms as needed. 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 "Recording 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.

Contents

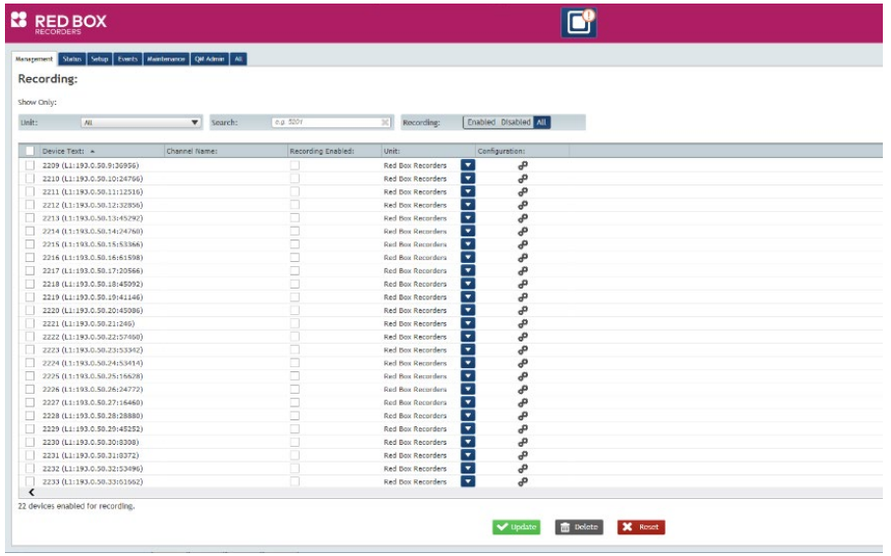
How Do I Manage Channels/Devices

Contents

A Channel can be regarded as a "recordable device" – that is, a fixed line phone, mobile phone, PC, radio, etc used as a communications device (for voice calls, video calls, Instant Messaging, etc.).

Manage Channels

To manage channels, go to **Configuration** > **Management** > **Recording**. Here you can see all "available" devices.



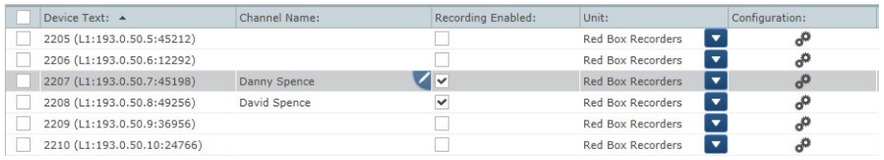
For most integration types (telephony, trader turret, radio, etc), devices are automatically detected when they are added to your network and will appear in the list. For some integration types, you will need to add a device "manually", as described in your Integration Guide — Red Box supports over 100 integration types, so there are too many to list here.

Similarly, some integration types will automatically populate the Channel Name field. If not, then you can edit the channel name "manually" as described below. In general, if the field is automatically populated, then don't change it in the recorder.

Edit a Channel Name

To edit a channel name:

1. From **Configuration** > **Management** > **Recording**, roll over the **Channel Name** field, click the ✎ **Edit** icon, and enter your **Channel Name**. The **Channel Name** is usually a number or person associated with the individual device.
2. Edit each **Channel Name** you want to change. When you're done, click the **Update** button to save your changes.



Contents

Enable/Disable a Channel/Device for Recording

If you want to record all communications for a channel/device, or ensure no communications are recorded, you must select the appropriate **Recording Enabled** setting for the channel.

To enable/disable a device:

1. Go to **Configuration** > **Management** > **Recording**.
2. To record all communications for a channel/device, tick the **Recording Enabled** box.
   To ensure the device is **not** recorded, untick the box.
3. Edit each channel you want to update. When you're done, click the **Update** button to save your changes.

Note that if a channel is enabled for recording, you also need to make sure all appropriate replay permissions are configured (including any defined groups and filters) to allow or restrict access to the recordings.

- To set general replay permissions (including applying filters and groups), go to **Configuration** > **Management** > **Users**, highlight a user and click **Edit**.
- To define filters, go to **Configuration** > **Management** > **Filter Management**.
- To define groups, go to **Configuration** > **Management** > **Groups**.

For finer control of what communications are recorded or not recorded (for example, calls between specific numbers, or outgoing calls from an individual extension), use the **Blacklist** settings – **Configuration** > **Management** > **Blacklisting**.

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

RBRQQA1006 V1.2

How Do I Select What Calls to Record

Contents

As well as selecting what channels/devices to enable/disable for recording, you also have control over what communications should be recorded or discarded. You can use Blacklisting, Internal Calls, and Agent Control, to refine your selections further.

Blacklisting

Blacklisting can be used to provide fine control of what communications are excluded from being recorded. Technically, once a device is enabled for recording, all communications are recorded, even blacklisted ones. However, the difference with blacklisted communications is that once the communication has ended, the data is discarded. Therefore, blacklisting applies to recorded communications only and does **not** affect Monitoring live calls (Live Acquire). Also note that blacklisting is not applied retrospectively.

Enable Blacklisting

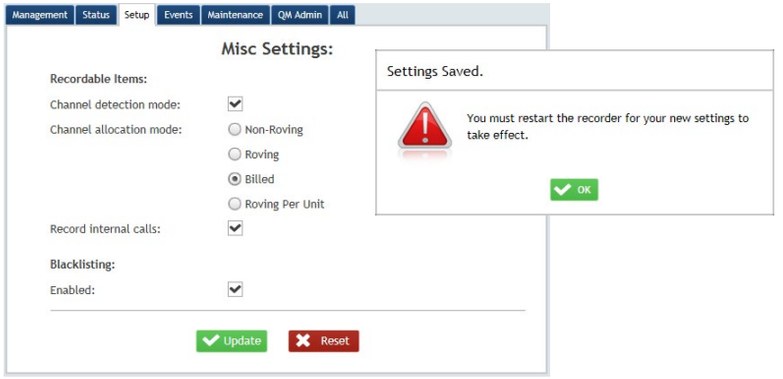
If blacklisting is not enabled (not visible in **Configuration** > **Management**) you can enable the feature in **Misc Settings**:

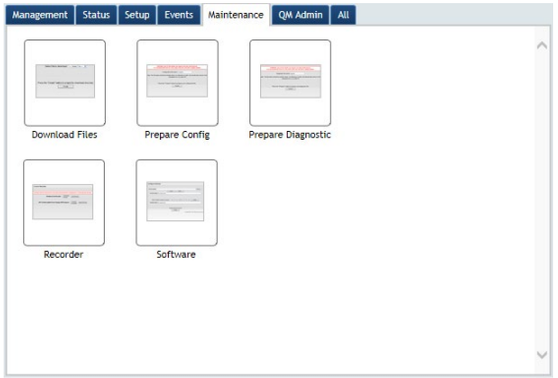
To enable blacklisting:

1. Login to Quantify with an administrator account (System Configuration permissions).
2. Go to **Configuration** > **Setup** > **Misc Settings**, tick the **Blacklisting Enabled** option, and click the **Update** button.
3. You'll need to restart the recorder for the change to be applied:
   - We recommend that a recorder restart is performed outside of normal usage hours.
   - Although not essential, we recommend that you prepare and download config (Configuration) & diag (Diagnostics) files before performing a restart:

     Prepare (Create): Go to **Maintenance** > **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.
   - To perform the restart, go to **Maintenance** > **Recorder**, select **Restart**, and then click the **Stop Recorder** button.





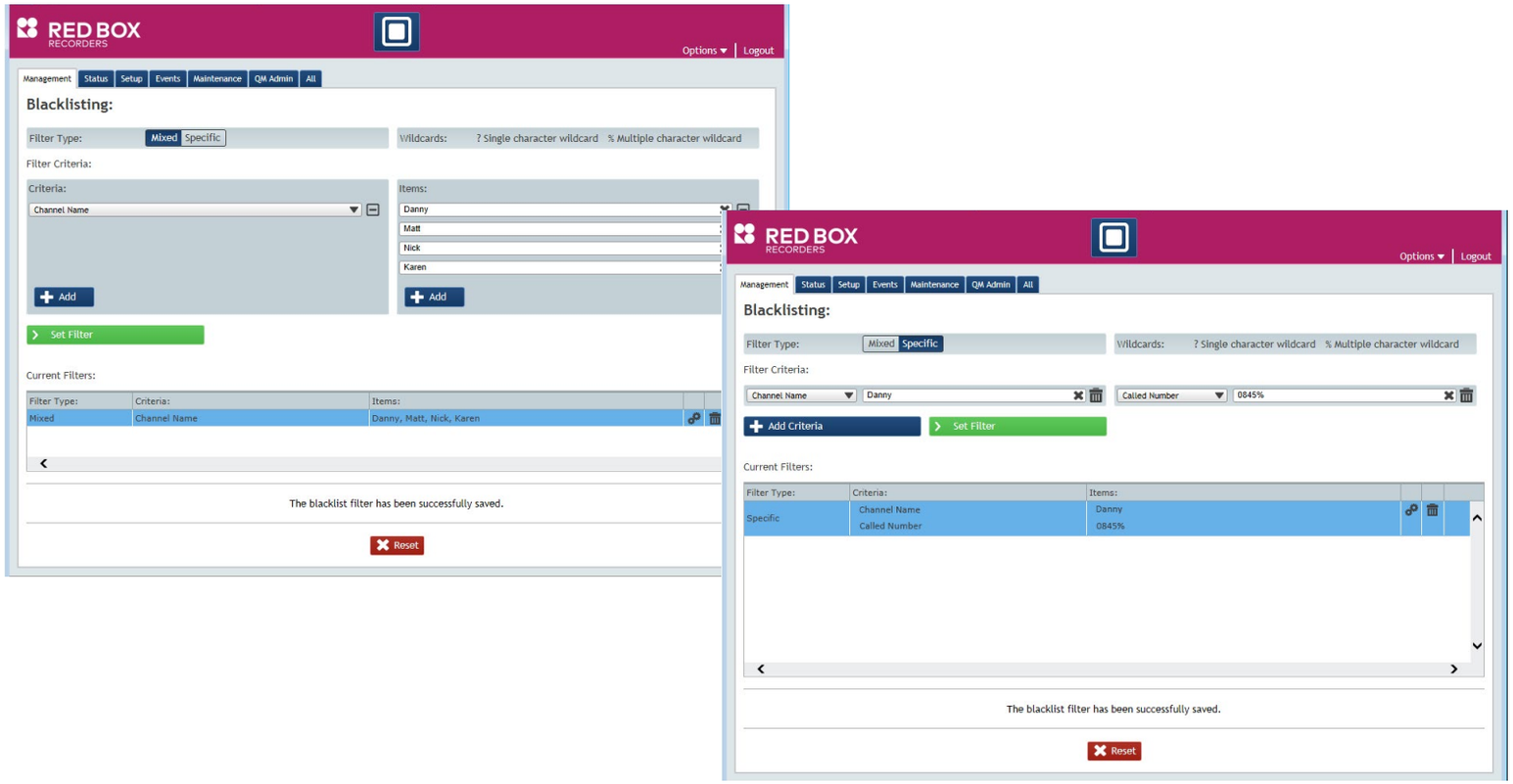
Contents

Create a Blacklist Filter

A blacklist filter is used to define what communications to discard. You can specify as many blacklist filters as you need.

To create a blacklist filter:

1. Login to Quantify with an administrator account (System Configuration permissions).
2. Go to **Configuration** > **Management** > **Blacklisting** and select your **Filter Type** and criteria:
   - **Mixed**: A **Mixed** filter is used to define multiple **Items** (data) to search across multiple **Criteria** (fields). Only one match is needed for a recorded communication to be discarded. For example, the **Mixed** filter shown below would blacklist all calls to/from channels **Danny**, **Matt**, **Nick**, or **Karen**.
   - **Specific**: A **Specific** filter is used to define one or more **Criteria** (fields) with specific **Items** (data). Here, all criteria/item pairs must match before a recorded communication is discarded. For example, the **Specific** filter shown below would blacklist calls from channel **Danny**, to any **0845** numbers.
   - Click the **+ Add** button to add criteria and items.
   - Click the **– Remove** button to remove criteria and items.
3. When you're done, click the **Set Filter** button to create your blacklist filter.



Contents

Review, Edit or Delete a Blacklist Filter

To review, edit or delete a blacklist filter:

1. Go to **Configuration** > **Management** > **Blacklisting**.
2. Highlight the filter to review/edit in the **Current Filters** list:
   - To edit the filter, click the **Edit Filter** icon. To delete the filter, click the **Delete Filter** icon next to the filter criteria.
   - To edit filter criteria, just edit the criteria fields and item data as needed. To add/remove criteria and items, use the **+ Add** and **– Remove** buttons.
3. When you're done, click the **Set Filter** button to save your changes.

Internal Calls

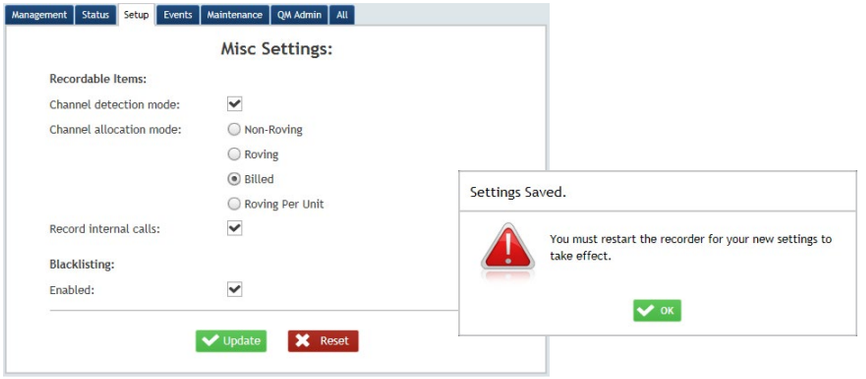
Use the **Internal Calls** setting to enable/disable recording of all communications between channels on the recorder. Note that recording internal calls may not be supported for your telephony system – if it isn't, the option won't be available.

To enable/disable recording of "internal calls":

1. Go to **Configuration** > **Setup** > **Misc Settings**, tick the **Internal Calls** option, and click the **Update** button.
2. You'll need to restart the recorder for the change to be applied:
   - We recommend that a recorder restart is performed outside of normal usage hours. Also, we recommend that you prepare and download config (Configuration) & diag (Diagnostics) files before performing a restart:

     Prepare (Create): Go to **Maintenance** > **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.
   - To perform the restart, go to **Maintenance** > **Recorder**, select **Restart**, and then click the **Stop Recorder** button.



Contents

Agent Control

The Record on Demand WorkStation Client feature allows agents to "Record" or "Discard" calls using buttons on their client PC. See "How Do I Manage WorkStation Client" in this Administrator Guide for more details.

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

RBRQQA1049 V1.1

How Do I Manage WorkStation Client

Contents

WorkStation Client (WSC) from Red Box provides four optional client-side features that link to your Red Box recording system:

- **PCI Suppression**: Mute (suppress) call audio during payment transactions. If Screen Data Capture is being used, this is also "muted" (blank screen).
- **Call Annotation**: Add notes (pre-defined and/or free text) to recorded communications.
- **Record on Demand**: Client initiated "Record" or "Discard" actions.
- **Channel Naming**: Auto-populate recorder channel names based on Windows login or Citrix User ID.

Your Installation Engineer will have done most of the installation and configuration for you, but you may need to review, add, or edit WSC clients and features.

WorkStation Client has three key components:

- **WSC Server**

  All WorkStation Client settings are configured globally on your recorder server, using the config app.

  - Identification rules define how to identify host PCs (clients) and how to map those PCs to phones. This can be a static mapping using the PCs hostname, or a more dynamic mapping using the Windows login name.
  - Client rules define the features that can be used on client PCs.
  - Feature rules define how each WSC feature operates across your WSC system.
  - Finally, client mapping links the discovered WSC clients with channels or extensions and defines what feature rules to use.

  See "WSC Server Settings".

- **WSC Client**

  Each client PC simply needs the WSC client app installed — see "WSC Client Application".

  All configuration of the applicable features available to the client is communicated by the WSC server — there's no additional client-side setup needed.

- **WSC Features**

  Each WSC feature has its own additional requirements, settings, and considerations — see "PCI Suppression", "Call Annotation", "Record on Demand", or "Channel Naming".

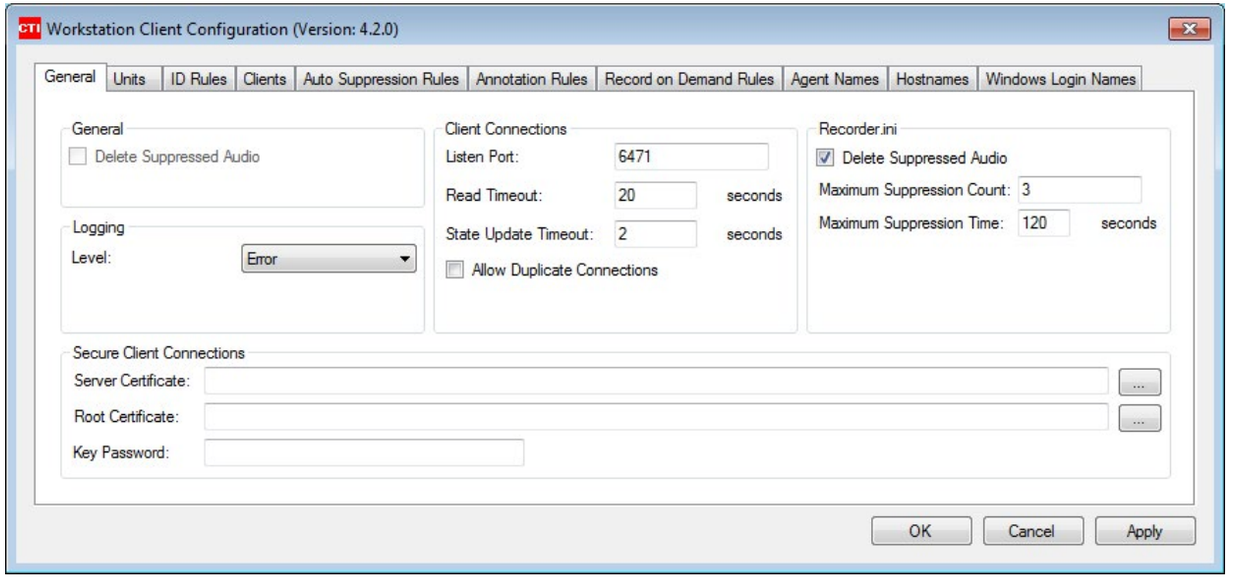
Note that WorkStation Client also has a number of different license requirements. If you need to review or update your licenses, see "WSC Licenses".

Contents

WSC Server Settings

Note that certain config settings are provided for Red Box Engineering use only and marked in this document using "*". Please do NOT change any of these settings without instruction from Red Box.

All WorkStation Client settings are configured globally on your recorder server, using the config app — **C:\LTR\utils\WSCConfigGUI\WSCConfigGUI.exe**



Tab	Description
General	• General recorder settings. • See "General Settings".
Units*	• Hosted server (if available) — list of units read from the recorder. • Provided for Red Box Engineering use only.
ID Rules	• Define how to identify your host PCs (clients) and how to map those PCs to actual phones. • See "ID Rules" and "Client PCs".
Clients	• Define the features that can be used on client PCs. • See "Client Features".
Auto Suppression Rules	• Define one or more rules to be used for automatic PCI suppression. • See "Feature Rules".
Annotation Rules	• Define one or more rules to be used for agent call annotation. • See "Feature Rules".
Record on Demand Rules	• Define one or more rules to be used for agent record on demand. • See "Feature Rules".

Contents

Tab	Description
Agent Names*	• Agent name mapping. Provided for legacy customers only. • Settings are provided for Red Box Engineering use only, and should **not** be changed.
Hostnames	• List of automatically discovered hostnames (for PCs with WSC Client installed). • This list is used to map computer **Hostnames** to **Extension**, **Channel Name** or **Logical Channel**. • See "Client PCs".
Windows Login Names	• List of automatically discovered Windows login names (for PCs with WSC Client installed). • This list is used to map **Windows Login Names** to **Extension** or **Channel Name**. • See "Client PCs".

General Settings

In general (no pun intended) these settings are configured during installation and won't need to be changed. If any changes are needed, you'll need to make the changes in the config app and then perform a recorder restart.

General	
Delete Suppressed Audio	Setting applies to audio suppressed using the WSC client. **Tick**: Delete suppressed audio. **Untick**: Mark suppressed audio. Replay of "marked" audio will show as silence for all Quantify users, except system administrators who will be able to replay the full audio.

Client Connections	
Listen Port*	• The server port to listen for client connections on. • * Setting is provided for Red Box Engineering use only, and should **not** be changed.
Read Timeout*	• Client connection timeout. • * Setting is provided for Red Box Engineering use only, and should **not** be changed.
State Update Timeout*	• Multi-recorder sync timeout. • * Setting is provided for Red Box Engineering use only, and should **not** be changed.
Allow Duplicate Connections	• Allow multiple client connections from the same host machine.

Recorder.ini *	
Delete Suppressed Audio	Setting applies to **all** PCI suppressed audio. **Tick**: Delete suppressed audio. **Untick**: Mark suppressed audio. Replay of "marked" audio will show as silence for all Quantify users, except system administrators who will be able to replay the full audio.

Contents

Recorder.ini *	
Maximum Suppression Count	• The maximum number of suppressions allowed per call. Default is three. • Can be used to avoid agent error or system abuse. See "PCI Suppression".
Maximum Suppression Time	• The maximum period of time (in seconds) that audio can be suppressed. Once the timeout has been reached, recording will resume. • Set to zero ("0") to never timeout. • Can be used to avoid agent error or system abuse. See "PCI Suppression".

* Note that any changes to the **Recorder.ini** section will not be applied until the recorder is restarted.

Logging	
Level	• Message log level. **Info** covers the most information, **Error** covers the least. • Unless there's a particular issue, we recommend this is set to **Error** to only log error messages. • This setting does **not** require a recorder restart.

Secure Client Connections*	
Certificates*	• Hosted server certificates. • * All settings here are provided for Red Box Engineering use only, and should **not** be changed.

* Please see the **C:\SSL\WSC_readme.txt** file on the recorder server for instructions on creating certificates.

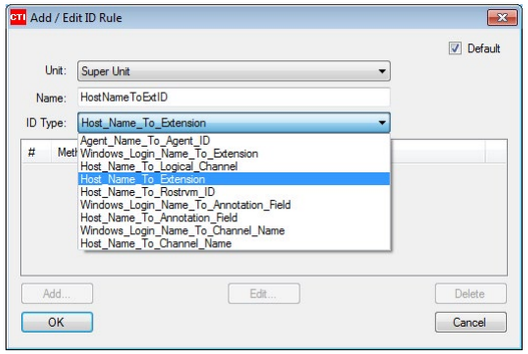
Contents

ID Rules

The **ID Rules** tab is used to define how the WSC server will identify your host PCs (clients) and how to map those PCs to actual phones. Options are:

Options	Description
Host_Name_To_Extension **Host_Name_To_Channel_Name** **Host_Name_To_Logical_Channel**	**Host Name**: Use the Hostname of client PCs to identify (discover) your WSC clients and then map each PC to a phone extension, channel name, or logical channel. Use the config app **Hostnames** tab to define individual mappings – see "Client PCs".
Windows_Login_Name_To_Extension **Windows_Login_Name_To_Channel_Name**	**Windows Login Name**: Use the Windows Login Name to identify (discover) your WSC clients and then map each PC to a phone extension or channel name. Use the config app **Windows Login Names** tab to define individual mappings – see "Client PCs".
Agent_Name_To_Agent_ID* **Host_Name_To_Rostrvm_ID*** **Windows_Login_Name_To_Annotation_Field*** **Host_Name_To_Annotation_Field***	These options are provided for Red Box Engineering use only, and should **not** be changed.

- To modify your default ID Rule, simply highlight the rule in the **ID Rules** tab and click the **Edit** button. Note that you must have a default rule defined.
- To add a rule, click the **Add** button. This allows you to define specific rules for individual client PCs (if needed).



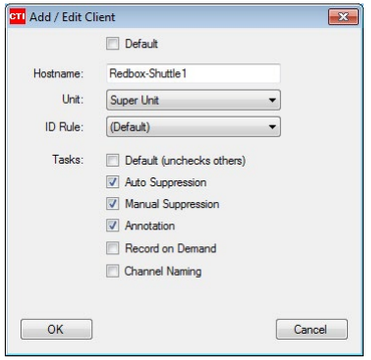
Contents

Client Features

The **Clients** tab is used to define the WSC features to be used on client PCs. Options are:

Options	Description
Auto Suppression	Enable PCI Suppression using an automatic trigger. You'll also need to define your triggers using the **Auto Suppression Rules** tab – see "Feature Rules" and "PCI Suppression".
Manual Suppression	Enable PCI Suppression using a manual trigger – see "PCI Suppression".
Annotation	Enable agent call annotation. You'll also need to define your rules using the **Annotation Rules** tab – see "Feature Rules" and "Call Annotation".
Record On Demand	Enable agent Record on Demand. You'll also need to define your rules using the **Record on Demand Rules** tab – see "Feature Rules" and "Record on Demand".
Channel Naming	Enable dynamic channel naming based on Windows login or Citrix User ID. See "Channel Naming".

- To modify your default **Client Features** entry, simply highlight the **<Default>** entry in the **Clients** tab and click the **Edit** button. Note that you must have a default entry defined.
- To add an entry, click the **Add** button. This allows you to define specific features for individual client PCs (if needed).



Contents

Feature Rules

Auto Suppression, Annotation, and Record on Demand all require rules to be defined in the WSC config app. These rules are used to specify how each feature operates across your WSC system. Once you've defined your rules, you can specify how to apply the rules to client PCs using the **Hostnames** or **Windows Login Names** tabs – see "Client PCs".

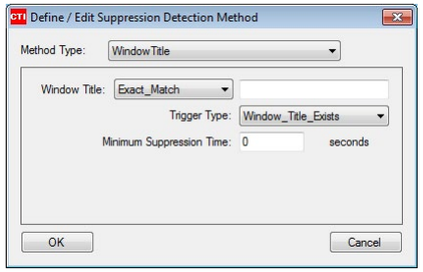
Auto Suppression Rules

To define an Auto Suppression rule:

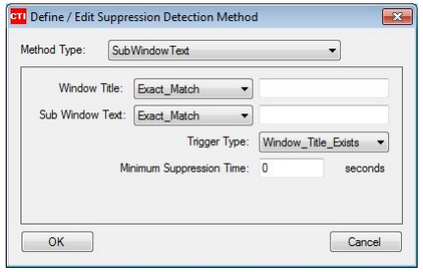
1. Click the **Auto Suppression Rules** tab. To edit a rule, highlight a rule and click **Edit**. To add a rule, just click **Add**. Note that if you're using Auto Suppression, you must have a default rule defined.
2. Now **Add** or **Edit** a trigger **Method**. A trigger **Method** defines what will trigger the start of suppression during a call - for example, when the agent opens a payment screen. Multiple methods can be defined and these are applied on an OR basis. To define a **Method**, select the **Method Type** (**WindowTitle** – trigger using a specific window, **SubWindowText** – trigger using text within a specific window, **BrowserHTML** – trigger using Internet Explorer) and associated options (see below).

   Note that for **Window** and **SubWindow** options, you may wish to use Microsoft® Spy++ or similar to view Window properties.

WindowTitle Options	
Window Title	Trigger using the specified window title and match pattern (**Exact_Match**, **Starts_With**, **Ends_With**, or **Contains**).
Trigger Type	Trigger when the window is open (**Window_Title_Exists**) or when it has focus (**Window_Title_Has_Focus**).
Minimum Suppression Time	Minimum time (in seconds) that the auto suppression will last for.

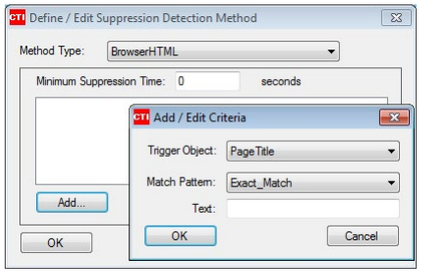


SubWindowText Options	
Window Title	Trigger using the specified window title and match pattern (**Exact_Match**, **Starts_With**, **Ends_With**, or **Contains**).
Sub Window Text	Trigger using the specified text found within the window, and the match pattern (**Exact_Match**, **Starts_With**, **Ends_With**, or **Contains**).
Trigger Type	Trigger when the window is open (**Window_Title_Exists**) or when it has focus (**Window_Title_Has_Focus**).
Minimum Suppression Time	Minimum time (in seconds) that the auto suppression will last for.



Contents

BrowserHTML Options (for use with Internet Explorer only)	
Triggers	**Add** or **Edit** a trigger and set the criteria (below).
Trigger Object	**Page Title**: Trigger when the specified web page is accessed. **URL**: Trigger when the specified URL is accessed. **HTML Body**: Trigger when a web page contains the specified content. **Domain**: Trigger when the specified domain name is accessed.
Match Pattern	Select the match pattern – **Exact_Match**, **Starts_With**, **Ends_With**, or **Contains**.
Text	Enter the text to match.
Minimum Suppression Time	Minimum time (in seconds) that the auto suppression will last for.

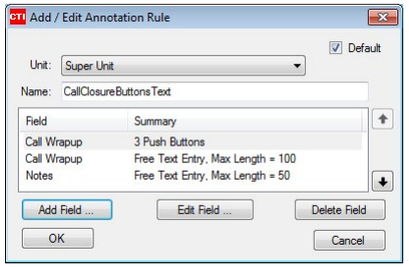


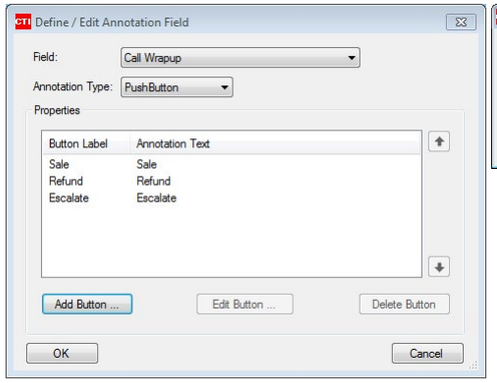
Annotation Rules

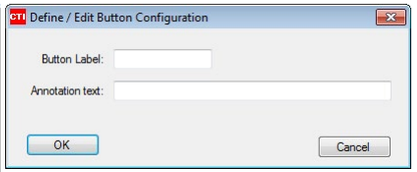
To define an Annotation rule:

1. Click the **Annotation Rules** tab. To edit a rule, highlight a rule and click **Edit**. To add a rule, just click **Add**. Note that if you're using Annotation, you must have a default rule defined.
2. Now **Add** or **Edit** a **Field** entry to define what annotation fields can be modified by WSC clients, and how the fields can be populated (**FreeTextEntry** or **PushButton**) – see below. Multiple fields can be defined.

Annotation Field Options	
Field	Select the annotation field to configure. The list of available fields is automatically populated from the annotation fields defined in the recorder (login to Quantify with an administrator account and go to **Configuration** > **Setup** > **Callstore**).
Annotation Type	Select how the fields can be populated by WSC clients (**FreeTextEntry** or **PushButton**).
Properties	If **PushButton** is selected as the **Annotation Type** you can add and edit buttons that will be shown in the agents' WSC client application. You can define a maximum of five buttons per field.







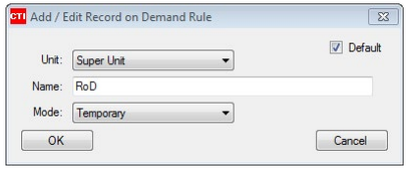
Contents

Record on Demand Rules

To define a Record on Demand rule:

1. Click the **Record on Demand Rules** tab. To edit a rule, highlight a rule and click **Edit**. To add a rule, just click **Add**. Note that if you're using Record on Demand, you must have a default rule defined.
2. The only setting available for a Record on Demand rule (apart from the name) is the **Mode** – select **Temporary** or **Permanent**.

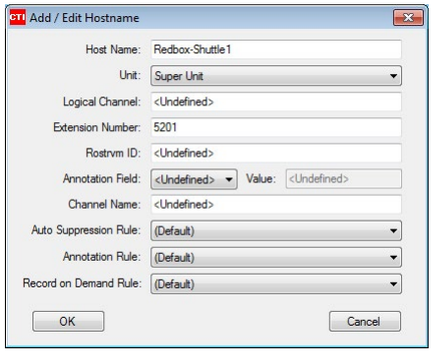
   Whenever a WSC client clicks the "**Record**" or "**Discard**" button on their PC, the call is either recorded or discarded in the recorder. If **Temporary** mode is used, the button click is only applied to the current call (or next call if currently not on a call). If **Permanent** mode is used, the button click is remembered and used for all calls going forward until a different button is clicked.



Client PCs

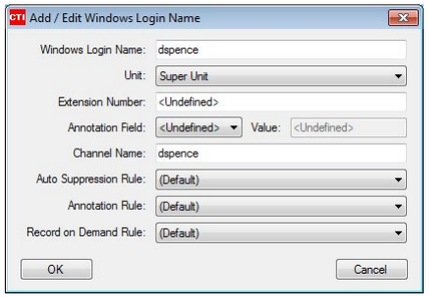
Once you've set your ID Rules, each WSC client PC discovered by the WSC server will be listed in the **Hostnames** and **Windows Login Names** tabs as appropriate (**Hostnames** for **Host_Name_To** ID Rules, and **Windows Login Names** for **Windows_Login_Names_To** ID Rules). For each entry in these tabs, you need to define what phone to map the PC/Login to, and what WSC feature rules to use. Your Installation Engineer will have done most of this during the install process, but new and updated clients will need to be added/modified here. Note that all client PCs need to have the WSC client installed - see "WSC Client Application".

Hostnames Options	
Host Name	Hostname of the client PC. In general you should not change this field unless you are pre-configuring a client.
Logical Channel	If you want to link this client PC to a logical channel in the recorder, enter a channel number here.
Extension Number	If you want to link this client PC to an extension number in the recorder, enter a number here.
Channel Name	If you want to link this client PC to a Channel Name in the recorder, enter a name here.
Auto Suppression Rule	Select the Auto Suppression rule to be used with this client PC. If you're using the **Default** rule there's no need to change the selection.
Annotation Rule	Select the Annotation rule to be used with this client PC. If you're using the **Default** rule there's no need to change the selection.
Record on Demand Rule	Select the Record on Demand rule to be used with this client PC. If you're using the **Default** rule there's no need to change the selection.
Unit* **Rostrvm ID*** **Annotation Field***	These options are provided for Red Box Engineering use only, and should **not** be changed.



Contents

Windows Login Name Options	
Windows Login Name	Windows Login Name for the client PC. In general you should not change this field unless you are pre-configuring a client.
Extension Number	If you want to link this client to an extension number in the recorder, enter a number here.
Channel Name	If you want to link this client to a Channel Name in the recorder, enter a name here.
Auto Suppression Rule	Select the Auto Suppression rule to be used with this client. If you're using the **Default** rule there's no need to change the selection.
Annotation Rule	Select the Annotation rule to be used with this client. If you're using the **Default** rule there's no need to change the selection.
Record on Demand Rule	Select the Record on Demand rule to be used with this client. If you're using the **Default** rule there's no need to change the selection.
Unit* **Rostrvm ID*** **Annotation Field***	These options are provided for Red Box Engineering use only, and should **not** be changed.



WSC Client Application

Each client PC simply needs the WSC client app installed as detailed below — for multiple PCs, you may want to install the client using a group policy.

To install/upgrade the WSC client app, run the **RBRWSC_Setup.msi** installer from the client PC using the following command line (replace `<IP address>` with the IP address of the recorder running the WSC Server):

```
msiexec /I <path to msi file>\RBRWSC_Setup.msi /QN RECORDERADDRESS="<IP address>"
```

Note that:

- If a primary/secondary recorder configuration is being used, then the IP addresses of both recorders should be specified so that the WSC operations are sent to both recorders to be actioned. Separate the IP Addresses with a "`;`" semicolon.
- If you require hostname mappings for Citrix or Terminal Services environments, see "Using Terminal Client Names as Hostnames".
- If you're using WSC with a Hosted recorder, see "Hosted".
- Once the WSC client app is installed, restart the client PC.
- All configuration of the WSC features available to the client is communicated by the WSC server — there's no additional client-side setup needed.

Contents

Once you've installed the WSC client, you may have a WSC window displayed on the client PC. This will depend on what features you are using and what feature rules have been implemented. A WSC window is displayed for the following:

- **PCI Suppression**: Manual suppression only – **Suppress** and **Resume** buttons.
- **Call Annotation**: Pre-defined annotation (buttons) or manual annotation (free text fields).
- **Record on Demand**: **Record** and **Discard** buttons.
- **Channel Naming**: No window.

Update Recorder IP Address

To change the recorder IP address that the WSC client application will connect to, reinstall the current version of the WSC client using the following command line:

```
msiexec /I <path to msi file>\RBRWSC_Setup.msi /QN RECORDERADDRESS="<new IP address>" REINSTALL=ALL
```

If the client PC does not automatically restart then it should be manually restarted to ensure all files are correctly updated and the application launched.

Using Terminal Client Names as Hostnames

In a Citrix or Terminal Services environment, the default behaviour will result in the server hostname being sent to the WSC server. This could be undesirable if a specific client is always associated with a specific phone, and you want to map the hostnames appropriately.

These environments "can" have certain identifiers for the client terminals. In order to try and use these identifying properties as the hostname, a "Terminal Naming" registry value must be added on the client PC:

- You can set this value as part of the WSC client installation by using the following command line:

  ```
  msiexec /I <path to msi file>\RBRWSC_Setup.msi /QN RECORDERADDRESS="<IP address>" TERMINALNAMING=1
  ```

  This will create and set the registry value needed in order to use the hostname of the terminal client.
- To enable Terminal Naming after installing the WSC client, create the following registry entry with a value of "**1**" (enabled):

  ```
  [HKLM]Software\Red Box Recorders Limited\RBRWSC\TerminalNaming
  ```

  To disable, delete the registry entry or set the value to "**0**".

Contents

Once Terminal Naming is enabled, the WSC client will look for one of three values to use as the hostname:

- The first is a registry value that's set by Citrix which contains the client name – both of the following are checked in order:

  `[HKCU]Software\Citrix\ICA Client\ClientName`

  `[HKLM]Software\Citrix\ICA Client\ClientName`

  If set, this contains the hostname of the connected client in session.
- The WSC client will then look for an **ini** file which, again, can be found in Citrix environments and contains the same client name. This file is named **WFCName.ini** and is found in the root directory of the system drive (e.g. **C:\WFCName.ini**).
- Finally, the WSC client will then look for the environment variable **CLIENTNAME** which is often set in both Citrix and Terminal Services environments.
- If none of these values are found, then the WSC client will fall back to the original hostname, which would be the hostname of the server in these environments.

When you're done, restart the client PC.

Hosted

If you're using WSC with a Hosted recorder:

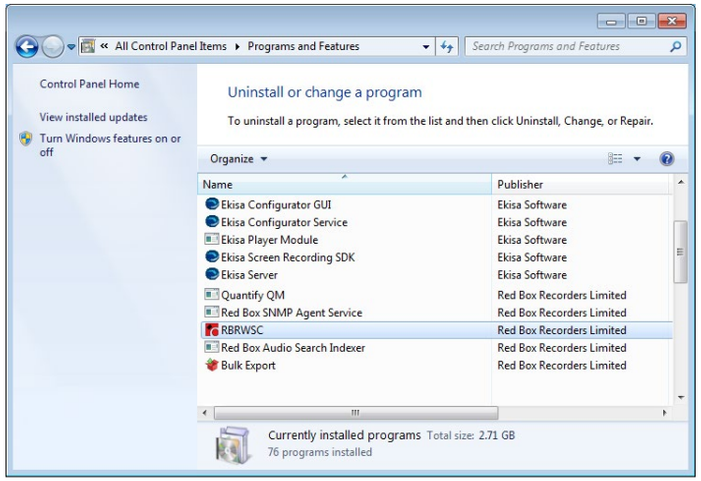
1. Deploy the client certificate on each WSC client PC.
2. Configure the registry on each client PC to identify the certificate:

   Registry Keys:

   ```
   64-bit machine: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Red Box Recorders Limited\RBRWSC
   32-bit machine: HKEY_LOCAL_MACHINE\SOFTWARE\Red Box Recorders Limited\RBRWSC
   ClientCertificatePassword = <PEM pass phrase>
   ClientCertificatePath = C:\SSL\WSC_Certs\<company name>_<organisational unit>.pem
   ```

Uninstall the WSC Client Application

The WSC Client can be uninstalled using the Windows Add/Remove Programs feature.



Contents

PCI Suppression

The PCI Suppression feature allows calls to be suppressed during payment transactions. All configuration of the PCI Suppression feature is performed on the WSC server. The main options are:

- **Total or User Suppression**

  Choose "total suppression" (delete audio) to ensure that no payment data is captured or "user suppression" (mark audio) to record payment details but restrict playback to system administrators for investigation purposes. See "General Settings" – **General** and **Recorder.ini** panels.

- **Automatic or Manual Suppression**

  Suppression of voice and screen recordings can be triggered two ways — automatically when opening or using a window, or manually by button. See "Client Features" and "Feature Rules" (Auto Suppression Rules).

- **Resume and Restrict**

  To avoid agent error or system abuse when suppression is triggered manually, PCI Suppression can be customised to automatically resume recording after a specified period of time. It's also possible to limit the number of times suppression can be initiated on one call. See "General Settings" (**Recorder.ini** panel) and "Feature Rules" (Auto Suppression Rules).

Note that manual control of PCI Suppression using DTMF tones or Cisco Phone Services is not covered in this guide.

Call Annotation

The Call Annotation WSC feature allows clients to add notes to recorded communications. To "use" Call Annotation:

- Define your Annotation Fields in the recorder Callstore – login to Quantify with an administrator account and go to **Configuration** > **Setup** > **Callstore** (this will require a recorder restart).
- Define your annotation rules (buttons or free text annotation) on the WSC server – see "Feature Rules" (Annotation Rules).
- You can also allow Quantify users to edit and update call annotation fields within Search & Replay:
  - Login to Quantify with an administrator account and go to **Configuration** > **Management** > **Users**.
  - Edit or create a user and tick the **Annotation** option in the **Permissions** panel.

Contents

Record on Demand

The Record on Demand WSC feature allows clients to "Record" or "Discard" calls. To "use" Record on Demand:

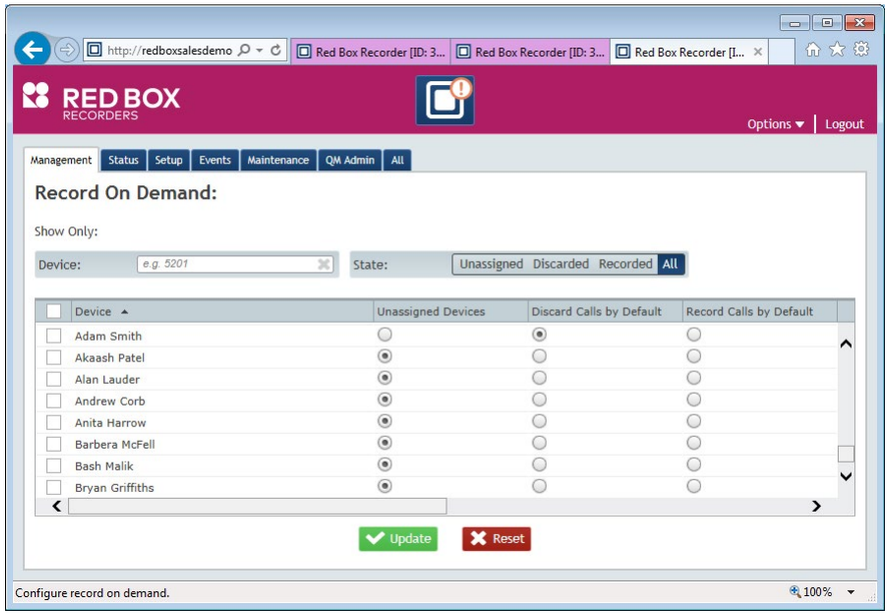
- Define your feature rules (**Permanent** or **Temporary**) on the WSC server – see "Feature Rules" (Record on Demand Rules).

  Whenever a WSC client clicks the "**Record**" or "**Discard**" button on their PC, the call is either recorded or discarded in the recorder. If **Temporary** mode is used, the button click is only applied to the current call (or next call, if not on a call). If **Permanent** mode is used, the button click is remembered and used for all calls going forward until a different button is clicked.

- Set the Record on Demand defaults on your recorder as appropriate:
  - Login to Quantify with an administrator account and go to **Configuration** > **Management** > **Record on Demand**.
  - Select the appropriate option for each device (channel) that you wish to use Record on Demand with:

    If your WSC feature rules are set to **Temporary**, select **Unassigned** (don't use Record on Demand), **Discard Calls by Default** (discard unless **Record** button is clicked), **Record Calls by Default** (record unless **Discard** button is clicked).

    If your WSC feature rules are set to **Permanent**, you can ignore the settings in the recorder as they will be altered when clients click their **Record** or **Discard** buttons. The recorder list is useful to review the current state for each channel though.



Contents

Channel Naming

The Channel Naming WSC feature will auto-populate the channel names on your recorder based on the Windows login or Citrix User ID associated with the client PC. To "use" Channel Naming:

- Set your ID Rules to map hostnames to extensions (**Host_Name_To_Extension** option) – see "ID Rules".
- This features doesn't require any feature rules.
- Set your extension number mapping in the **Hostnames** tab – see "Client PCs" (Hostnames Options).

When a user logs into a PC associated with an extension, the Channel Naming feature will populate the Channel Name field for the extension in the recorder with the user's Windows login name or Citrix User ID.

This feature is most useful during system implementation or in situations where a desktop PC and phone extension are fixed but is used as a "hotdesk" so different users will log into the PC.

WSC Licenses

WorkStation Client has a number of different license requirements. The steps below show how to check WSC licenses on your recorder, and how to apply new license codes if needed.

To check and apply licenses:

1. Login to Quantify with an administrator account (System Configuration permissions) and go to **Configuration** > **Setup** > **Licensing**.
2. WSC requires a PP License (Protocol Processor):
   - **PP Name**: Check that you have a **WSC CTI Server** PP license with the correct options.
   - **Max Number of Clients**: Maximum number of concurrent WSC client connections.
   - **Options**: Licensed WSC features – **PCI Screen** (Automatic PCI Suppression), **PCI Agent** (Manual PCI Suppression), **Annotation**, **Record on Demand**, **Channel Naming**.

   Note that Record on Demand also requires a separate **Record on Demand** recorder license.

   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.
3. If you have a new license code, enter the code in the **New License Code** field and click **Update** to apply the license. Note that a new/updated PP license will require a recorder restart.

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

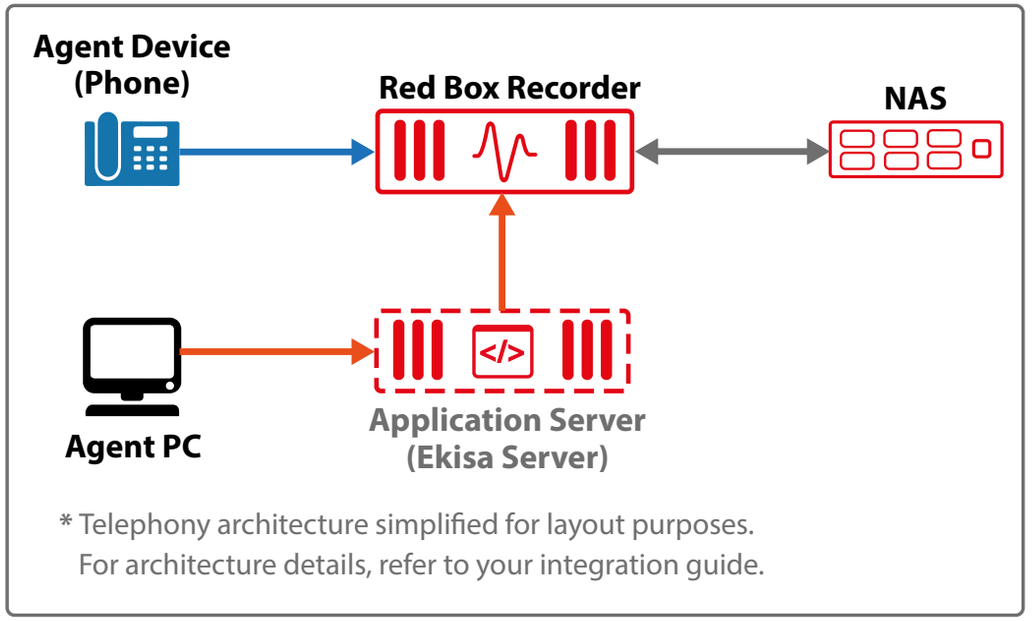
RBRQQA1032 V1.2

How Do I Manage Screen Recording

Contents

The Red Box screen recording capability is provided by the Ekisa ScreenLogger software. Agent PCs are linked with Agent Devices (phones) so that during an active call the Agent's PC screen is recorded along with the call audio – generally known as a screen recorded call. Screen recorded calls can then be processed, searched, replayed, exported, and transcribed using the Red Box Quantify software and export services in the same way as any other call.

Your Red Box Installation Engineer will have already installed and configured your screen recording system for you. This topic is designed for customer System Administrators and provides details on how to add (new) and update (existing) agents for screen recording, and how to modify Call Wrap Up settings.



Contents

Prerequisites

Before you add an Agent PC to the screen recording system, you need to run the following installers on their PC:

- **EkisaWorkstationInst:** Simply follow on-screen instructions to install the service. You'll need to enter the Ekisa Server name or FQDN during installation – the server should be on the same domain as the Agent's PC in order to record the screen.
- **XVIDInst:** Run the **msi** file to install the XVid video codec – this is a specific codec optimised for use with screen recording (not required for ScreenLogger V3.x).

If you don't have the **EkisaWorkstationInst** or **XVIDInst** installers, please contact Red Box for help, or you can search for the files on an existing PC that's already being recorded.

When you add a new agent for screen recording, you'll link an Agent's PC with their phone. The phone being recorded needs to be in the Recorder's device list and set to record. To check this, login to Quantify using a system administrator account and go to **Configuration** > **Management** > **Recording** – see "How Do I Manage Channels/Devices" for more information, if needed. Note that if the Agent's device is **not** in the recording list, you may need to refer to the specific Integration Guide from Red Box to add the device to your recording system. Again, please contact Red Box for help, if needed.

Add an Agent

Adding an agent to your screen recording system is a two part process. First you'll need to edit the **ekisa.ini** file on the Recorder server to link an Agent's PC with their phone, and then you need to configure the ScreenLogger software on the Ekisa server to enable the agent for screen recording.

Note: The Recorder **ini** files contain a range of configuration settings that directly impact recording functionality. Do **not** change any other setting without consulting Red Box. If you're unfamiliar with editing **ini** files, please contact Red Box for help.

Contents

Recorder Configuration

To configure the Recorder:

1. On the Recorder server, open the **C:\LTR\Config\ekisa.ini** file. This file is used to link an agent's workstation and device. Now open your **C:\LTR\PP*<PP_abc.ini>*** file. This **ini** file is used to set general configuration options for recording your telephony system, and also contains device details which you'll need to copy to the **ekisa.ini** file. The actual name of the ***PP_abc.ini*** file will depend on your telephony system. Your Installation Engineer will have provided this file name during install and we've listed some of the common ones below, but if you don't know yours, just contact Red Box for help.

   Note that sample **ini** files are shown in "Sample Recorder ini Files".

2. In the **PP_abc.ini** file, scroll down to the **[Extensions]** section and find the device for your agent – each device is listed in the following format, depending on your telephony system:

   <DeviceNumber>=<DeviceID or ChannelName>~<AgentID>~<LineID>~<DeviceIP>~<Port>~<DeviceSettings>

   For example: **00000002=102~6201~1~193.0.2.1~16538~N~**

   You're only interested in the **<AgentID>** and **<DeviceID or ChannelName>**. Find the agent you want to add to your screen recording system and copy their **DeviceID** or **ChannelName** (this depends on your specific telephony system – only one of these will be used).

3. In the **ekisa.ini** file, scroll down to the **[Mapping]** section and add a line for the new agent:

   <DeviceID>or<ChannelName>=<WorkstationName>or<AgentName>

   For example: **102=dspence**

   Use the **DeviceID** or **ChannelName** that you copied from the **PP_abc.ini** file, and also enter either the name of the Agent's Workstation (Computer Name) or their Agent Name (Windows login name). Simply follow the same format used to define your other agents.

   Note that an entry for the **DeviceID** or **ChannelName** may already exist in the **ekisa.ini** file, with the **WorkstationName** or **AgentName** set to **<undefined>**. In this case, simply replace **<undefined>** with the agent's **WorkstationName** or **AgentName**. Do **not** use duplicate entries.

4. Save and close the **ekisa.ini** file, and close the **PP_abc.ini** file. Now restart the **CTIServer_Ekisa** Windows service to apply the changes you made to the **ekisa.ini** file, and update the list of Agent Workstations. We recommend that you restart the service outside of normal operating hours.

   To finish adding an agent, see "ScreenLogger Configuration".

Telephony System	*PP_abc.ini* File
Avaya Aura AES/DMCC	PP_ActiveRecording.ini
BT ITS	PP_mtd.ini
Cisco Active	PP_ActiveRecording.ini
IP Trade	PP_ActiveRecording.ini
IPC Unigy (& Unigy 360)	PP_ActiveRecording.ini

Telephony System	*PP_abc.ini* File
Mitel MiVoice Business	PP_Mitel_CTI.ini
SIP Active	PP_ActiveRecording.ini
SIPREC	PP_ActiveRecording.ini
Unify OSB	PP_ActiveRecording.ini
Unify OSV	PP_ActiveRecording.ini

Contents

Sample Recorder ini Files

As stated, the specific layout of your **ekisa.ini** and **PP_abc.ini** file will depend on your telephony system and screen recording implementation. Here's a quick sample of each file just to illustrate the general data, but follow the specific formats already used in your own existing **ini** files.

ekisa.ini - Notepad

```
[Mapping]
101=jsmith
102=dspence
103=ajones
104=asmith
105=sspence
106=acarter
107=spatel
108=jjones
109=thauer
110=<undefined>
```

PP_ActiveRecording.ini - Notepad

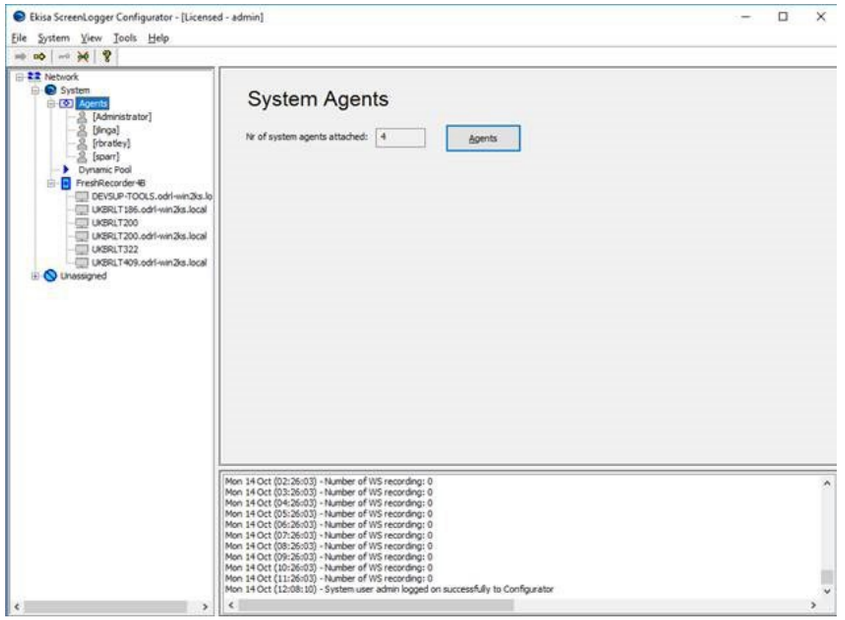
```
[Extensions]
Total=00000200
00000001=101~5201~1~193.0.1.1~16536~Y~
00000002=102~6201~1~193.0.2.1~16538~N~
00000003=103~5202~1~193.0.1.2~49230~N~
00000004=104~6202~1~193.0.2.2~49232~N~
00000005=105~5203~1~193.0.1.3~57520~N~
00000006=106~6203~1~193.0.2.3~57522~N~
00000007=107~5204~1~193.0.1.4~4250~Y~
00000008=108~6204~1~193.0.2.4~4252~N~
00000009=109~5205~1~193.0.1.5~45212~N~
00000010=110~6205~1~193.0.2.5~45214~Y~
00000011=111~5206~1~193.0.1.6~12292~N~
```

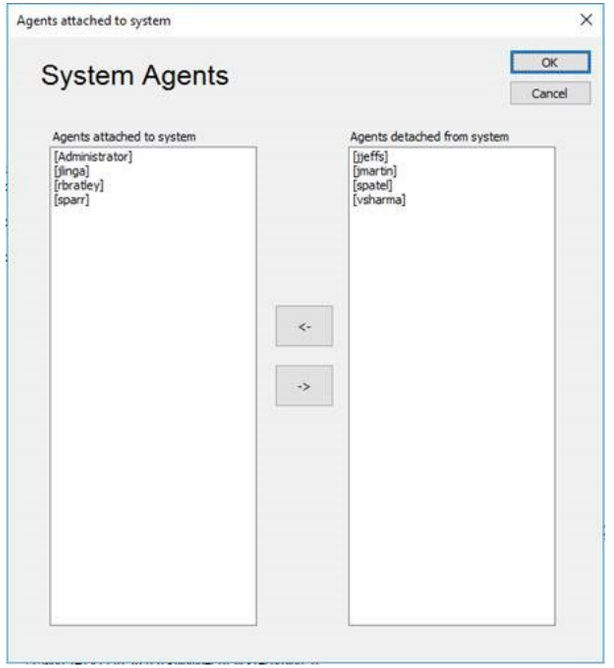
Contents

ScreenLogger Configuration

To configure the ScreenLogger:

1. Open the Ekisa ScreenLogger Configuration app on the Ekisa server – you can find this in **Start** > **Ekisa**. Login using your Ekisa administrator account details – your Installation Engineer will have provided this information during install, but if you don't know yours, just contact Red Box for help.
2. Open **Network** > **System** > **Agents** in the "Architecture" panel on the left and click on **Agents**. Now click the **Agents** button in the "Action" panel on the right. You should now see your **System Agents** list.
3. To record an Agent's PC, simply highlight the agent in the "**detached**" list and move them to the "**attached**" list. If you need to remove an agent from the attached list (stop recording an Agent's PC), just do the reverse.
4. Click **OK** when you're done. Your agent should now be showing in the **Agents** list in the Architecture panel. Your Agent's PC and call audio will now be recorded when they make or receive a call. You may want to test that everything is ok – see "Test an Agent".





Contents

Test an Agent

Once you've added an agent, you should check that screen data is being captured by the Ekisa ScreenLogger and then check that call audio is being recorded (along with the screen recording) and is available within Quantify.

To test ScreenLogger:

1. Open the Ekisa ScreenLogger Configuration app on the Ekisa server, and open **Network** > **System** > **Workstations** in the "Architecture" panel on the left. Right click the **Workstation** and select **Start Test Recording**. Obviously you need to make sure that the agent's PC is logged in and being "used". After about 10 seconds, right click the workstation again and select **Stop Test Recording**.

   Note that this is just a test recording within the ScreenLogger system and will not be available in Quantify.
2. Open the Ekisa Player Module app on the Ekisa server – you can find this in **Start** > **Ekisa** > **Player**. Note that your Installation Engineer will have provided login details for this app.
3. Search for the test recording and replay the recording.

   If you can't find or replay the test recording, check your Recorder and ScreenLogger configuration.

To test Quantify:

1. Make a test call to/from the Agent's phone. Also, make sure that the Agent's PC is logged in and being "used" during the call.
2. Login to Quantify, go to Search and Replay, find the call, and replay the recording. Call audio will replay in the Media Player and the screen recording will replay in a pop-up.

   Tip: All screen recorded calls populate the **Screen Event ID** metadata field with "**EVT...**" and also populate the **Extra Recording** metadata field with "**screen**". You can use these metadata fields as a handy way to find screen recorded calls (search **Screen Event ID** > **EVT%** or **Extra Recording** > **screen**).

   If you can't find or replay the test recording in Quantify, check your Recorder and ScreenLogger configuration. Also note that to replay a screen recorded call within Quantify, you need to have the Player Module and XVid video codec installed on the PC being used to replay the call – see "Player Module for Quantify".

Status Information

You can also use the Ekisa ScreenLogger Configuration app to check Agent and Workstation status information. Open the app on the Ekisa server (**Start** > **Ekisa**):

- The **Agent** and **Workstation** icons in the "Architecture" panel on the left show basic status information – Grey: Offline, Blue: Online, Red: Recording.
- Click on an Agent or Workstation in the Architecture panel to view detailed status information, such as which Agent is logged onto an individual Workstation.

Contents

Edit an Agent

Editing an agent depends on what you need to do – disable recording or change name.

To disable recording:

1. To completely disable recording for an agent (no call audio or screen data will be captured):
   - Login to Quantify using a system administrator account, go to **Configuration** > **Management** > **Recording** and disable the required channel.
   - Open the Ekisa ScreenLogger Configuration app on the Ekisa server, open **Network** > **System** > **Agents** in the "Architecture" panel on the left. Right click the agent and select **Detach Agent**.
2. To only disable screen recording for an agent (no screen data will be captured, but call audio will continue to be recorded and available in Quantify):
   - Open the Ekisa ScreenLogger Configuration app on the Ekisa server, open **Network** > **System** > **Agents** in the "Architecture" panel on the left. Right click the **Agent** and select **Detach Agent**.

To change an agent's name:

1. To change an agent's name, first disable the channel for recording while you make the change – login to Quantify using a system administrator account, go to **Configuration** > **Management** > **Recording** and disable the required channel.
2. Update the name change in your telephony system and the Agent's PC login as needed.
3. On the Recorder server, open the **C:\LTR\Config\ekisa.ini** file and update the **[Mapping]** information for your agent as needed.
4. On the Recorder server, restart the **CTIServer_Ekisa** Windows service. This will apply the changes you made to the Recorder server **ini** files and update the list of Agent Workstations that can be recorded. We recommend that you restart the service outside of normal operating hours.
5. Now open the Ekisa ScreenLogger Configuration app on the Ekisa server, open **Network** > **System** > **Agents** in the "Architecture" panel on the left and check the agent is **attached** to the system.
6. Finally, re-enable recording on the Recorder – login to Quantify, go to **Configuration** > **Management** > **Recording** and enable the required channel.

Contents

Player Module for Quantify

To replay screen recorded calls within Quantify, you need to run the following installers on each PC you want to use to replay those calls:

- **EkisaPlayerModuleInst:** Simply follow on-screen instructions to install the player. You may need to enter the Ekisa Server name or FQDN during install.
- **XVIDInst:** Run the **msi** file to install the XVid video codec – this is a specific codec optimised for use with screen recording (not required for ScreenLogger V3.x).

If you don't have the **EkisaPlayerModuleInst** or **XVIDInst** installers, please contact Red Box for help, or you can search for the files on an existing PC that's already being used to replay screen recorded calls.

Hot Desking

If your screen recording system is being used in a hotdesk environment (individual workstations can be used by a number of different agents), you need to make sure that the **EkisaWorkstationInst** and **XVIDInst** installers are installed on all PCs that you want to record – see "Prerequisites".

Licensing

Your ScreenLogger software will be licensed for the total number of concurrent workstations that can be recorded. To review your licenses, open the Ekisa ScreenLogger Configuration app on the Ekisa server (you can find this in **Start** > **Ekisa**) and select **Network** > **System**. The **Licenses Issued** panel shows the number of licenses for your system, and the **Licenses Assigned** panel shows the number of licenses currently in use. If you need to purchase additional licenses, please contact Red Box for details.

Contents

Call Wrap Up

The "Call Wrap Up" feature provided in Quantify 5C and above allows you to extend the screen recording past the end of the audio call, allowing you to record "call wrap up" activities after the audio call has ended. To configure this feature on the recorder server, edit the **C:\LTR\Config\ekisa.ini** file and add or modify the following section:

```
[Wrapup]
CallWrapupTime=<TimeInMilliseconds>
```

Set the `<TimeInMilliseconds>` to define how long you want the screen recording to continue past the end of an audio call (1000 milliseconds = 1 second). Now restart the **CTIServer_Ekisa** Windows service to apply the changes – we recommend that you restart the service outside of normal operating hours.

Note the following:

- The ScreenLogger software provides "keyframes" once per second, so the actual wrap up time will be approximately +/– one second.
- Setting a large call wrap up time may have a significant impact on your storage requirements.
- Playback within Quantify works in the same way as any other screen recorded call.
- If a new audio call is received by an agent during the scheduled wrap up time, the wrap up period will be cancelled for that agent and a new screen recording session will start immediately.

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

RBRQQA1066 V1.0

How Do I Set Up Recording Alarms

Contents

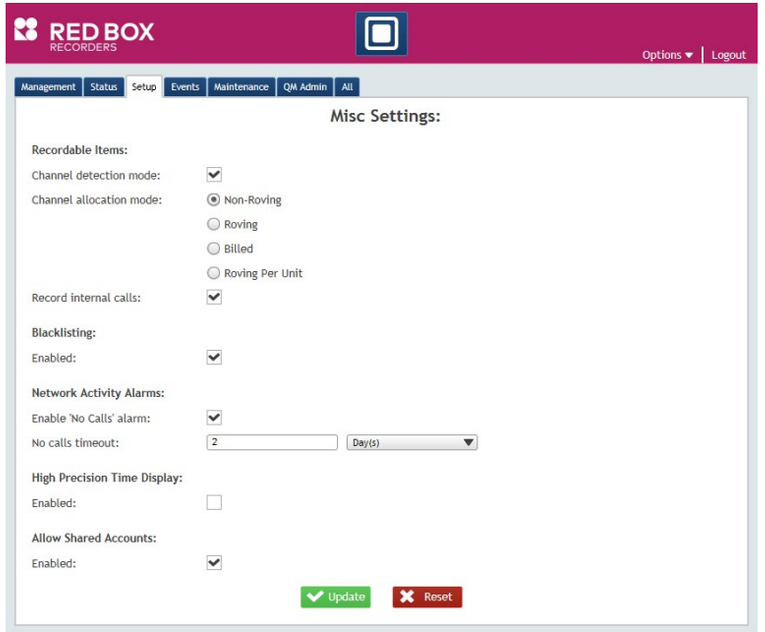
Using Quantify, you can monitor and manage a number of recording alarms designed to alert you when "no calls" or "silent calls" are recorded. This topic takes you through those alarms.

General Alarm

You can set up a general "No Calls" alarm to notify you when no calls have been recorded for a set number of days. If you need more granularity, see "Device Specific Alarms".

To set up a general alarm:

1. Login to Quantify with an administrator account (System Configuration permissions) and go to **Configuration** > **Setup** > **Misc Settings**.
2. Tick the **Enable No Calls Alarm** option and enter your timeout period (in Days, Hours, or Minutes).
3. When you're done, click **Update** to save your settings.



Alarms are reported via the Quantify main menu and can also be viewed at any time from **Configuration** > **Status** > **Recorder Status**. Similarly, Quantify Insight will also report this alarm type via the **Recording Status** indicator. See "Monitor & Manage Alarms" for more details.

Contents

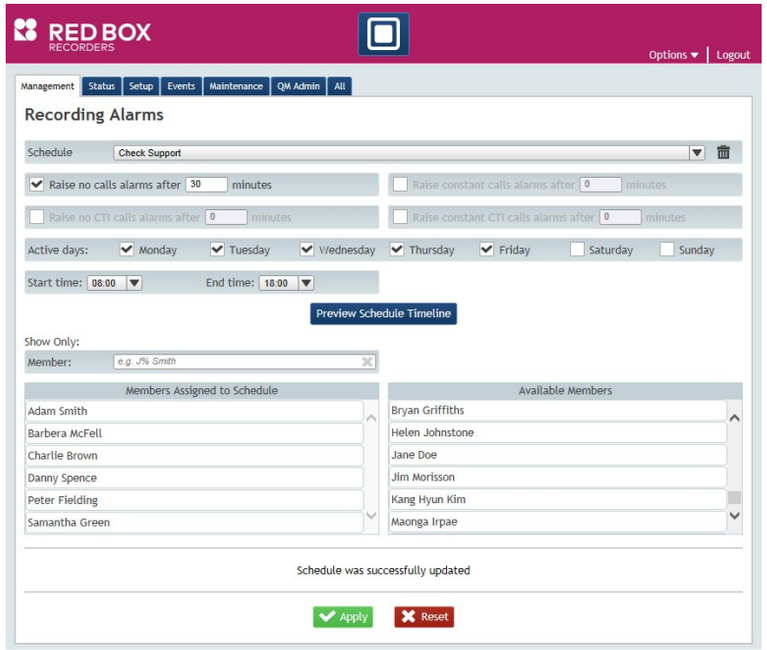
Device Specific Alarms

You can set up specific "Recording Alarms" to notify you when no calls (or constant calls) have been recorded for one or more devices during specific days and times.

To set up a recording alarm:

1. Login to Quantify with an administrator account (System Configuration permissions) and go to **Configuration** > **Management** > **Recording Alarms**.
2. In the **Schedule** drop-down menu, type a name for your alarm. In general, we recommend you use a descriptive name to help identify the alarm type in any notifications.
3. Now select what type of recording event will trigger the alarm:
   - **No Calls** - activate the alarm if **no calls** are recorded for the set number of minutes.
   - **Constant Calls** - activate the alarm if there are **constant calls** being recorded for the set number of minutes. This could indicate a "stuck" call or simply excessive call length.
   - You can select between "standard" and "CTI" call types.
4. Select the active days and active time-frame for the alarm. You can preview the schedule using the **Preview Schedule Timeline** button.
5. Select what devices to monitor — drag and drop channels (devices) from the **Available** list to the **Assigned** list.
6. When you're done, click **Apply** to apply your new alarm.

Alarms are reported via the Quantify main menu and can also be viewed at any time from **Configuration** > **Status** > **Recorder Status**. Similarly, Quantify Insight will also report this alarm type via the **Recording Status** indicator. See "Monitor & Manage Alarms" for more details.



Contents

Trend Analysis Alarms

Please note that the following trend analysis alarms apply to Quantify Version 4A SP3 and later releases.

Your Red Box Recorder will automatically perform trend analysis to compare recorded data in the last hour with recorded data from the same time period in the previous week. The following general alarms can help to highlight potential issues:

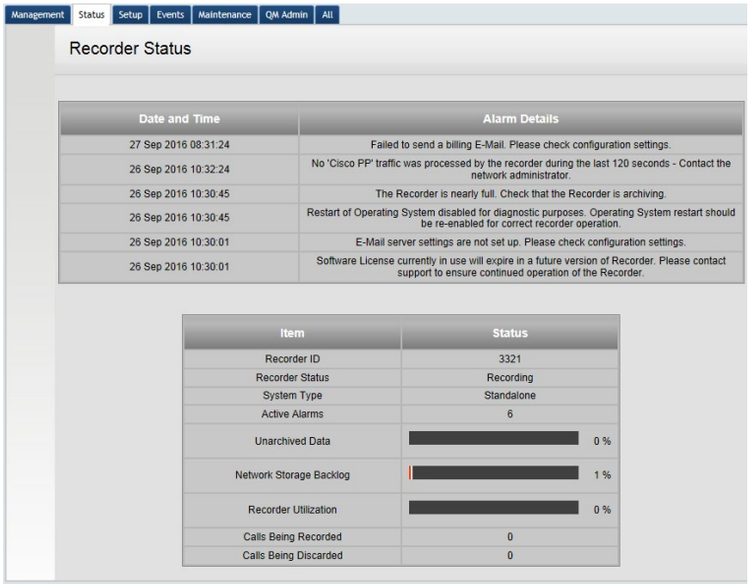
- **Recording Trend Alarm**: Compares the number of recordings (calls) with the previous week. This alarm could indicate that one or more devices are no longer being recorded.
- **Packet Trend Alarm**: Compares the number of packets with the previous week. This alarm could indicate that although calls are being recorded, there's no audio (silent calls).

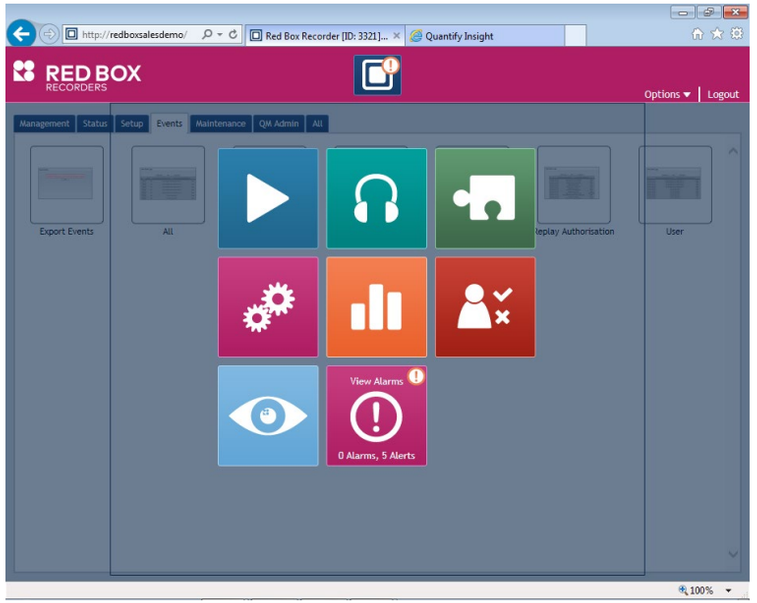
As with the other recording alarms, the trend analysis alarms are reported via the Quantify main menu and can also be viewed at any time from **Configuration** > **Status** > **Recorder Status**. Similarly, Quantify Insight will also report these alarms via the **Health** indicator. See "Monitor & Manage Alarms" below.

Monitor & Manage Alarms

Monitor and manage your recording and trend analysis alarms to help prevent data loss:

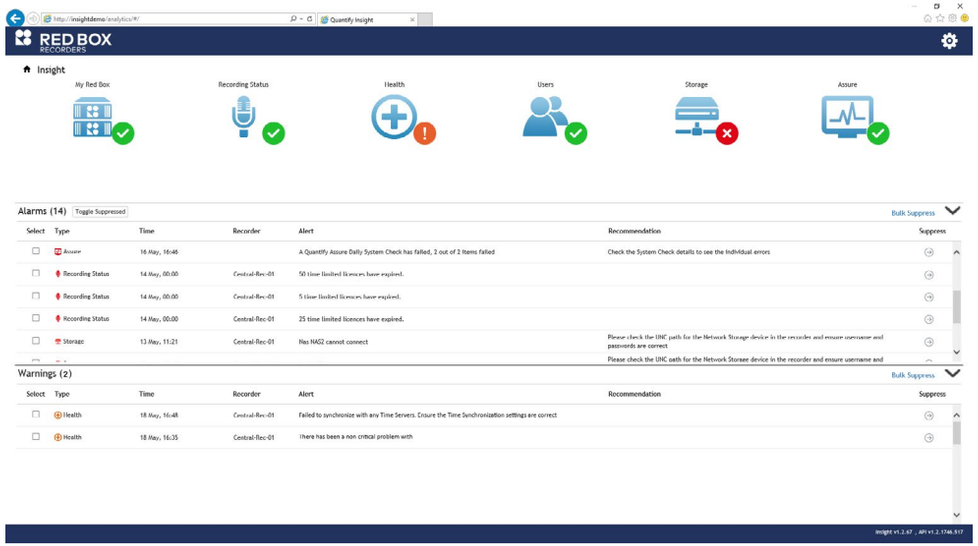
- **Quantify Alarms**: All alarms are reported via the Quantify main menu and can also be viewed at any time from **Configuration** > **Status** > **Recorder Status**.



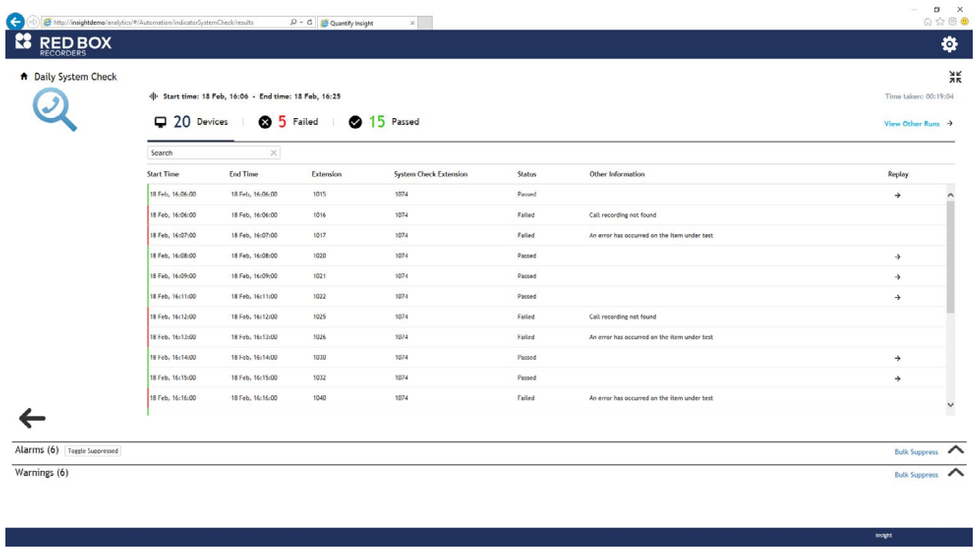


Contents

- **Quantify Insight**: By far the easiest way to monitor and manage all of your alarms is to use Quantify Insight (provided as part of Quantify Version 4A SP2 and later). Quantify Insight monitors a comprehensive set of critical system information, including recording status, and provides clear and concise status indicators, alarms, warnings, and recommendations — you can even get alarms, summary reports, and other information emailed to you.



- **Quantify Assure - Daily System Check**: Quantify Assure - Daily System Check (DSC) can also be used to automatically check that every phone in your telephony system is recording correctly, using a test call. As with general alarms and status information, you can also get DSC test results emailed to you. If you don't have Quantify Assure - Daily System Check, contact your dealer or Red Box for details.



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

RBRQQA1013 V1.2

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, but for "recording control" you can focus on **PP Licenses** and the **Number of Record Channels**, as well as the more optional **Workstation Client**, **Record on Demand** and **Time Limited Licenses**.

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.

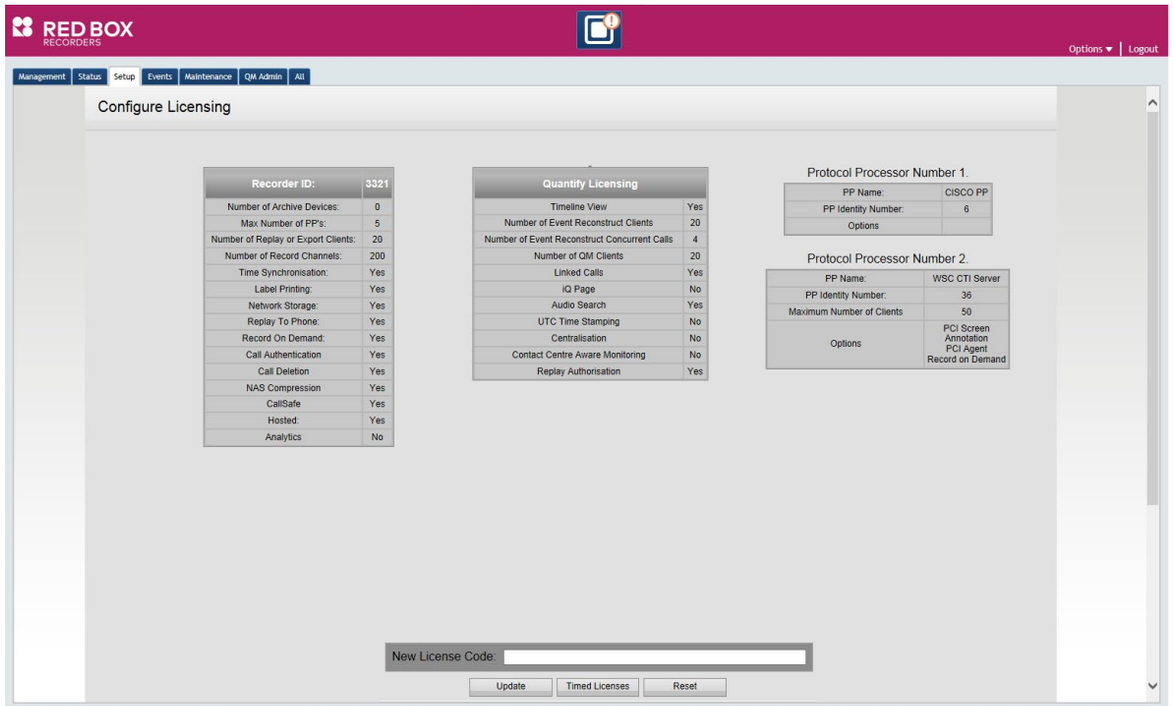
   To view "Time Limited" licenses, click the **Timed Licenses** button.

   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 "Recorder Licenses" for more details.	N
Number of Replay or Export Clients	Maximum number of users that can concurrently replay or export recorded communications. See "Recorder 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 "Recorder 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.

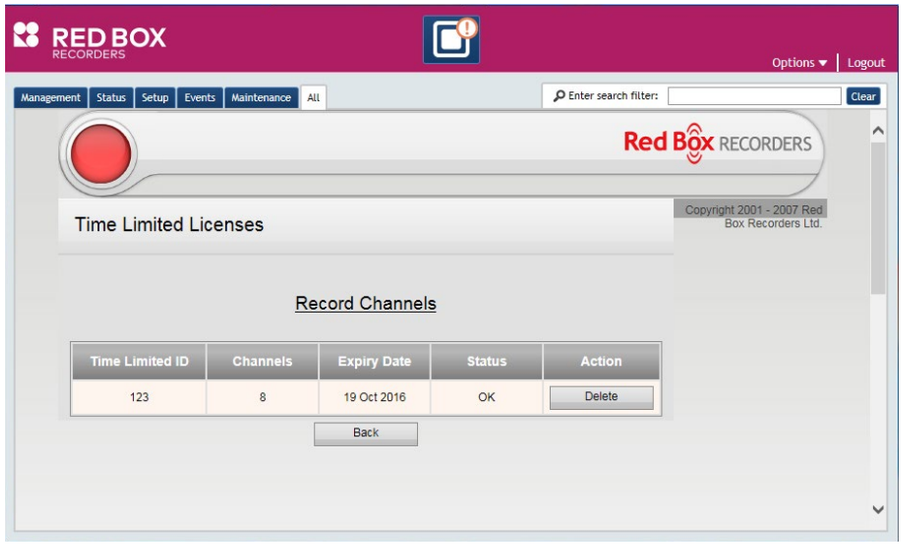
PP Type	Description	Restart Required?
Telephony **Trader Turret** **Radio** **Mobile Telephony** **PC Comms**	Integration type(s) licensed on the recorder — license will refer to a telephony type (e.g. Cisco, Avaya, Mitel), trader turret type (e.g. BT Unified Trading, Etrali Open Trade), radio type (e.g. 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 the **Timed Licenses** button.

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.

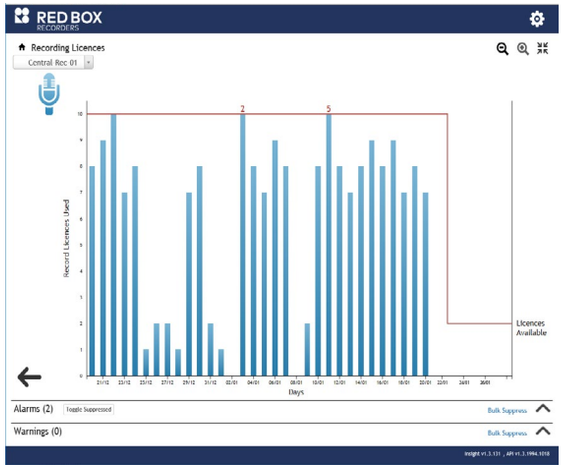
With this in mind, it's advisable to promote a simple login/logout etiquette so that licenses are used and released efficiently. To monitor and manage this, go to **Configuration** > **Status** > **Logged in Users** — here you can see the number of logged in users and the number of allocated replay licenses. 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 V1.4