User Guide

RadioAudit

Original Instructions: ENGLISH
Document Number: MOD-21-2511
Issue: 2.0

Copyright

Disclaimer

Although every reasonable effort has been made to ensure the accuracy of the information contained herein and any other referred document, this should not be construed as a commitment on the part of Sepura Limited and the liability of Sepura Limited for any errors and omissions shall be limited to the correction of such errors and omissions. Sepura Limited welcomes any comment and feedback as a way to improve any delivered documentation. The information contained herein has been prepared for the use of appropriately trained personnel, and it is intended for the purpose of the agreement under which the information is submitted. Any party using or relying upon this information assumes full responsibility for such use and in no event shall Sepura Limited be liable to anyone for especial, collateral, incidental, or consequential damages in connection with or arising out of the use of this information. The information or statements given in these documents regarding the suitability, capacity or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between Sepura Limited and the customer.

Application Disclaimer

The function(s) of the Application may be dependent upon, amongst other, the radio detecting a Bluetooth beacon, using GNSS data, connecting to a Bluetooth device or Wi-Fi network, or the radio receiving or sending TETRA messages which are reliant on independent infrastructure and / or the radio's Global Navigation Satellite System ("GNSS"), Bluetooth, Wi-Fi and TETRA services.

SEPURA does not warrant the accuracy and/or reliability of data derived by the radio's GNSS. The GNSS accuracy statistics set out in the specifications can only be achieved under certain conditions, e.g. open space, sufficient number of satellites visible, signal levels above acceptable magnitude, etc. and as such, inaccurate data may be output by the GNSS where all relevant conditions are not met. The Customer hereby agrees and acknowledges that data provided by the GNSS is for reference only.

SEPURA does not warrant the reliability of the radio's Bluetooth. The radio's detection of, or connection to other devices using Bluetooth may be compromised if the radios are not within signal range of the other devices or if signals are blocked by obstacles or other local conditions arise causing signal interference or device failure.

SEPURA does not warrant the reliability of the radio's Wi-Fi. The radio's detection of, or connection to other devices or infrastructure using Wi-Fi may be compromised if the radios are not within signal range of the other devices or infrastructure or if signals are blocked by obstacles or other local conditions arise causing signal interference or device / infrastructure failure.

SEPURA does not warrant the reliability of TETRA Data Communications. The radio's ability to send and receive data across a TETRA network may be compromised if the radios are not within TETRA network coverage or if coverage is blocked by obstacles or other local conditions arise causing network failure.

Whilst every effort is made to ensure the reliability of the Application(s), the nature of the technology and the circumstances of use are such that SEPURA cannot warrant that it will operate effectively in all circumstances and the Customer hereby agree that users should not entrust their safety to the Application(s). The Application(s) should in no way be regarded as a substitute for compliance with appropriate risk assessment and other safety procedures and practices.

Trademarks

The Sepura logo and some product branding logos and names are registered trademarks of Sepura Limited. All other trademarks appearing in this document are the property of their respective owners.

The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Sepura Limited is under licence. Other trademarks and trade names are those of their respective owners.

Contact Details

Sepura Limited
9000 Cambridge Research Park
Beach Drive, Waterbeach
Cambridge, CB25 9TL
United Kingdom
www.sepura.com

Contents

Contents (contd.)

1.0 About this Guide

This Guide describes the RadioAudit functions and how to install and configure RadioAudit to perform audits.

The information in this Guide relates to using RadioAudit on any of the following Sepura TETRA Radios:

- SC2/SCG
- SRH, STP and SRG

The following font styles are used throughout the Guide:

- **Bold**: Used to indicate a UI message, setting or a parameter.
- *Italic*: Used to indicate an application .exe file.
- `monospaced`: Used to indicate commands to be entered.

1.1 Pre-requisites

To configure the RadioAudit App, you will require a PC with a web browser and the AppSPACE Configuration Editor installed. The latest RadioAudit .appdef file must also be present on the PC.

1.2 References

The following documents are referenced in this guide:

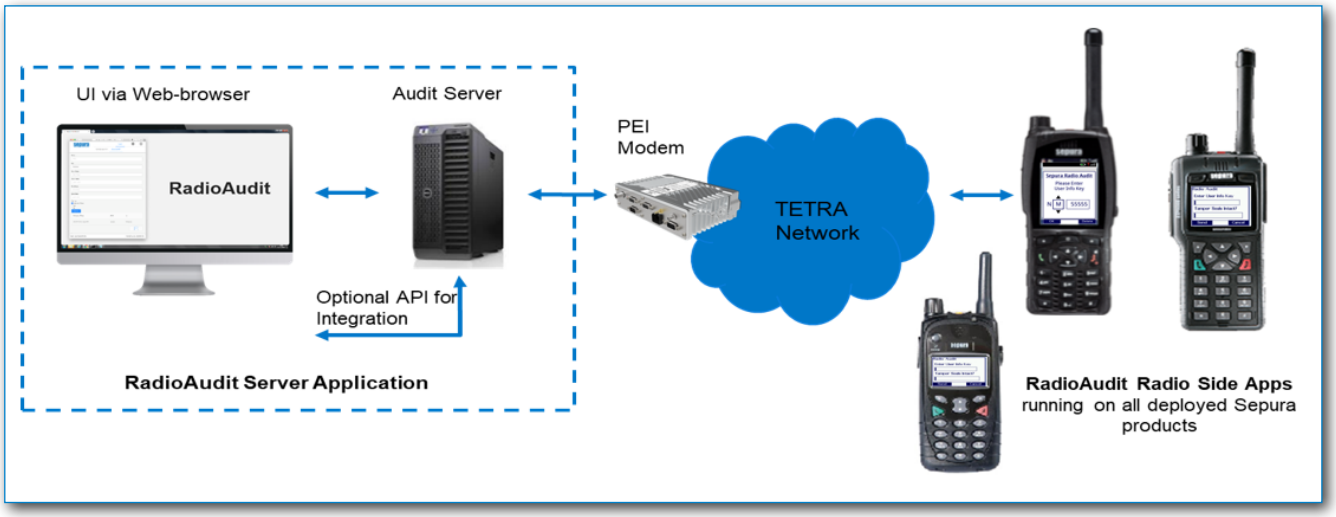
- Sepura Radio Manager User Guide
- AppSPACE Configuration Editor User Guide – MOD-21-2488

2.0 RadioAudit Overview

Sepura RadioAudit is a Radio and Control Room application that has been designed to simplify and automate the process of verifying and recording the identity of the radio user and the status of the radio's anti-tamper seal at the time of an audit.

Regular auditing of TETRA radios to verify both the device owner and the radio's security status is a necessary part of keeping communications secure.

The RadioAudit system consists of a web-based application and a radio AppSPACE application that communicate with each other over a TETRA network. The server application connects to the TETRA network via a PEI modem.



The RadioAudit Server Application is used to initiate the audit process. It communicates with the radio fleet over TETRA, manages the audit data received and provides a selection of data reports detailing the results of the audit. The data reports can be exported to Excel for further analysis. The RadioAudit Server Application includes:

- A user interface, accessible via a client web browser.
- An integrated database holding the radio, user, and audit data.
- An option for the use of a REST API, allowing all data to be shared with and available to a third party application for data storage, sharing, manipulation or presentation.

A radio AppSPACE application is used on the terminals to notify the radio user that an audit is in progress, and that the user should input and submit the requested details via the app.

Each radio remains fully operational during the audit process. The radio user can submit the audit information when convenient to do so.

Two types of radio-side application are provided to allow use of the product across all radio types. These are installed using Sepura Radio Manager:

SC and SCG radios	RadioAudit App (an AppSPACE application)
STP, SRH and SRG radios	RadioAudit SDA (Short Data Application)

The RadioAudit server application and radio AppSPACE application are controlled and activated by licences which are sold as part of the product.

3.0 RadioAudit Configuration

Audits are initiated by a Fleet Administrator to authenticate each radio holder within the fleet. The audit prompts radio users to enter a password to prove they are the legitimate holder of the radio and also if the tamper seal is intact or not.

3.1 RadioAudit App Configuration

The RadioAudit App, used on SC and SCG radios, can be configured using the AppSPACE Configuration Editor. The configuration file is then loaded using the Radio Manager. The following parameters can be configured:

Parameter	Description
Message Destination ISSI	The destination ISSI that the audit report will be sent to. If 'STATUSDEST' is entered, then the default destination, defined by radio customisation parameter [3133], is used
Message Source ISSI	The source ISSI from which the application triggers audits. If 'STATUSDEST' is entered, then the default source ISSI, defined by radio customisation parameter [3133], is used
Display Dialog Feedback	This specifies the display of a confirmation dialog box on the radio when the audit is successfully completed. This also shows a confirmation of the message delivery status.
Optional Fields	This specifies the additional fields reported by the radio when an audit is performed. The additional information is: location Area, latitude, longitude, firmware Version, BatteryInfo, SwitchOnText.
Minimum User Info Key length	This specifies the minimum length for the user info Key. When the minimum number of characters is entered, the radio shows the send option to the user. User can enter up to 15 characters.
Form Redrawing Timeout	This specifies the amount of time in seconds before the audit application redraws the form after being cleared by a user or radio action. For a portable, the audit application redraws on boot if the battery has been changed or removed and re-fitted.
Start Audit on Trigger Reception	This specifies if the audit information screen is shown as soon as the RadioAudit Server message is received by the radio or on next reboot. The RadioAudit info screen is shown as soon as the message is received when this is set to true.
Audit Form Title	This specifies the title text to display on the audit forms
Complete Audit Info Form	This specifies the audit info text to display on the initial form presented to the user on reception of a trigger message
Partial Audit Info Form	This specifies the text to display for the first question of the audit.
Second Question	This specifies the text to display for the second question of the audit.
Key Box Title	This specifies the text to display above the input text box
Yes String	This specifies the text to display on the Yes checkboxes.
No String	This specifies the text to display on the No checkboxes
Audit Feedback	This specifies the text to display on the feedback boxes showing once the audit is complete.

Parameter	Description
Message Failed Delivery Feedback	This specifies the text to display on the message delivery feedback boxes when an audit report fails to be delivered.
Version Screen Title	This specifies the text to display on the version pop up
Send Audit Report Key	This specifies the text to display on the context key used to send the audit report.
Key Selection Validation String	This specifies the text to display when selecting an entry for the User Info Key
Page Numbering String	This specifies the text to display on mobile radio for the paging

The RadioAudit Short Data Application (SDA) source and destination parameters, used on SRH, STP and SRG radios, can be configured using Radio Manager.

3.2 RadioAudit Server Configuration

The Apps Control Panel (ACP) is used for administration of the RadioAudit system global parameters that impact how RadioAudit will operate in various situations. The other ACP administrative parts define how RadioAudit connects to the external networks and other interfaces.

The ACP can be opened using your preferred browser:

1. Point your preferred browser to the http://localhost:8080 address.
2. Enter the following login credentials to log on:

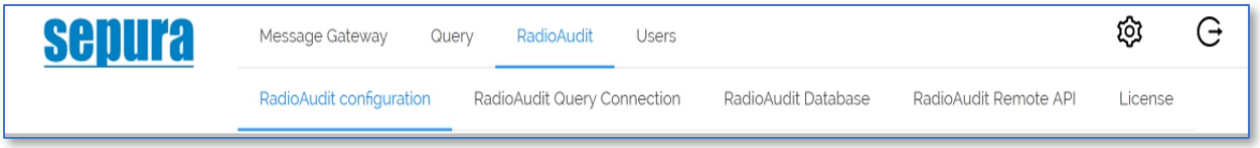
   Username: admin

   Password: password

> **Note:** It is recommended to change the password as soon as possible. This can be found under the Settings menu.

When logged on, the Apps Control Panel is displayed.

The RadioAudit configuration details can be found under the RadioAudit tab:



The configuration is divided into the following:

- **RadioAudit Configuration**: This is used to configure the RadioAudit system behavioural aspects.
- **RadioAudit Query Connection**: This is used to define the connection between RadioAudit Client and Query. These settings are defined during the installation and typically do not need any modifications.
- **RadioAudit Database**: This is used to define the RadioAudit system connection to the database where the RadioAudit data is stored. This setting is defined during the installation and typically does not need any modifications.

- **RadioAudit Remote API**: This is used to define the API for the remote API system. Usually, the configuration data for the RadioAudit Remote API can be left intact, but the RadioAudit Remote API definitions can be changed here.
- **Licence**: This is used for maintaining the RadioAudit licence.

The RadioAudit Configuration page contains the following settings:

Number of Retries:	This sets the number of times (up to a maximum of 50) the RadioAudit system will retry to send the audit request to the radios before triggering an alarm. This setting applies to all supported radios.
Timeout in hours before re-prompt:	This sets the time the system will wait for the audit response from radio users before resending the prompt.
Time in hours before re-prompt:	This sets the time after which the audit request is re-sent to radios where the user has opted to postpone the audit. This setting only applies to SRH, STP and SRG radios.
Messages per second:	This sets how many audit request messages are sent out per second. This setting depends on the network interface and the number of radios in the RadioAudit system.
Alarm from every incident:	This toggle defines whether an alarm is triggered for every issue detected in audit responses. This is a global toggle which when set overrides all alarm settings except Play alarm sound, Alarm message to Remote API, and Alarm highlighted.
Alarm when no reply within set time:	This toggle defines whether an alarm is triggered where the audit response has not been received within the set time.
Alarm when audit requests rejected by user times:	This setting determines how many audit requests the radio terminal user can postpone before an alarm is triggered. The possible values are 1, 2 or 3. This setting only applies to SRH, STP and SRG radios.
Alarm when incorrect user details entered:	This toggle defines whether an alarm is triggered for an issue where the user's details are not found in the RadioAudit database. These are the details entered by the radio terminal user.
Alarm when pool incorrectly reported:	This toggle defines whether an alarm is triggered when a pool radio is incorrectly reported as a personal radio by the radio terminal user, or a personal radio is reported as a pool radio.
Play alarm sound:	This toggle defines whether the RadioAudit Client plays a predefined alarm sound when detecting an issue in the received audit responses.
Alarm message to Remote API:	This toggle defines whether the detected alarms are reported to the remote API.
Alarm highlighted:	This toggle defines whether the RadioAudit Client highlights all issues in red in the different reports and audit data views.
Alarm message displayed in RadioAudit:	This toggle defines whether the RadioAudit client displays an alarm message when issues are detected in the audit responses.

Disable Tamper Seal Check:	This toggle defines whether the Tamper Seal Check is active by default when a new audit is created. This setting can be overridden when a new audit is created in the RadioAudit client.
Warning trigger for licence expiration in months:	This setting determines when the RadioAudit Client displays a pre-warning about an expiring licence. The possible options are 1, 2 or 3 months.

The RadioAudit Query configuration page contains the following settings:

Service Number:	This is the RadioAudit Query identification number. This is defined during installation and normally does not need to be changed.
Outbound Exchange:	This is the outbound exchange details that the Query uses for sending messages to the RadioAudit system. This is defined during installation and normally does not need to be changed.
Force creating outbound exchange:	This toggle determines whether the outbound exchange is created in a situation where no receiver has already created the receiving end of the exchange. This is defined during installation and normally does not need to be changed.
Outbound Exchange Type:	This is the outbound exchange type setting. This is defined during installation and normally does not need to be changed.
Delayed:	The default setting is ON and should not be changed.
Message Time To Live in Seconds:	This is the messages time-to-live (TTL) setting. This is adjusted during installation and should not be changed.
Inbound Exchange:	This is the inbound exchange details that the Query uses for receiving messages from the RadioAudit system. This is defined during installation and normally does not need to be changed.
Inbound Exchange Type:	This is the inbound exchange type setting. This is defined during installation and normally does not need to be changed.
Delayed:	The default setting is ON and should not be changed.
Inbound Exchange Routing Key:	This is the inbound exchange routing key used for routing the messages from the RadioAudit system to Query. This is defined during installation and normally does not need to be changed.

The RadioAudit Database page contains the following settings:

Database Name:	This is the name for the Mongo database that is used for storing the RadioAudit data. This setting is defined during installation and normally does not need to be changed.
MongoDB connection string:	This is the details of how RadioAudit connects to the Mongo database. This setting is defined during installation and normally does not need to be changed.

The RadioAudit Remote API configuration page contains the following settings:

Remote API URL:	This is the URL for the remote API. The format or the URL must be http://url/
Remote API Basic Authorisation token:	This is the token that is used for authentication towards the remote system.

Note: The RadioAudit API is subject to licence protection.

4.0 Using the RadioAudit Client

4.1 RadioAudit Main Interface

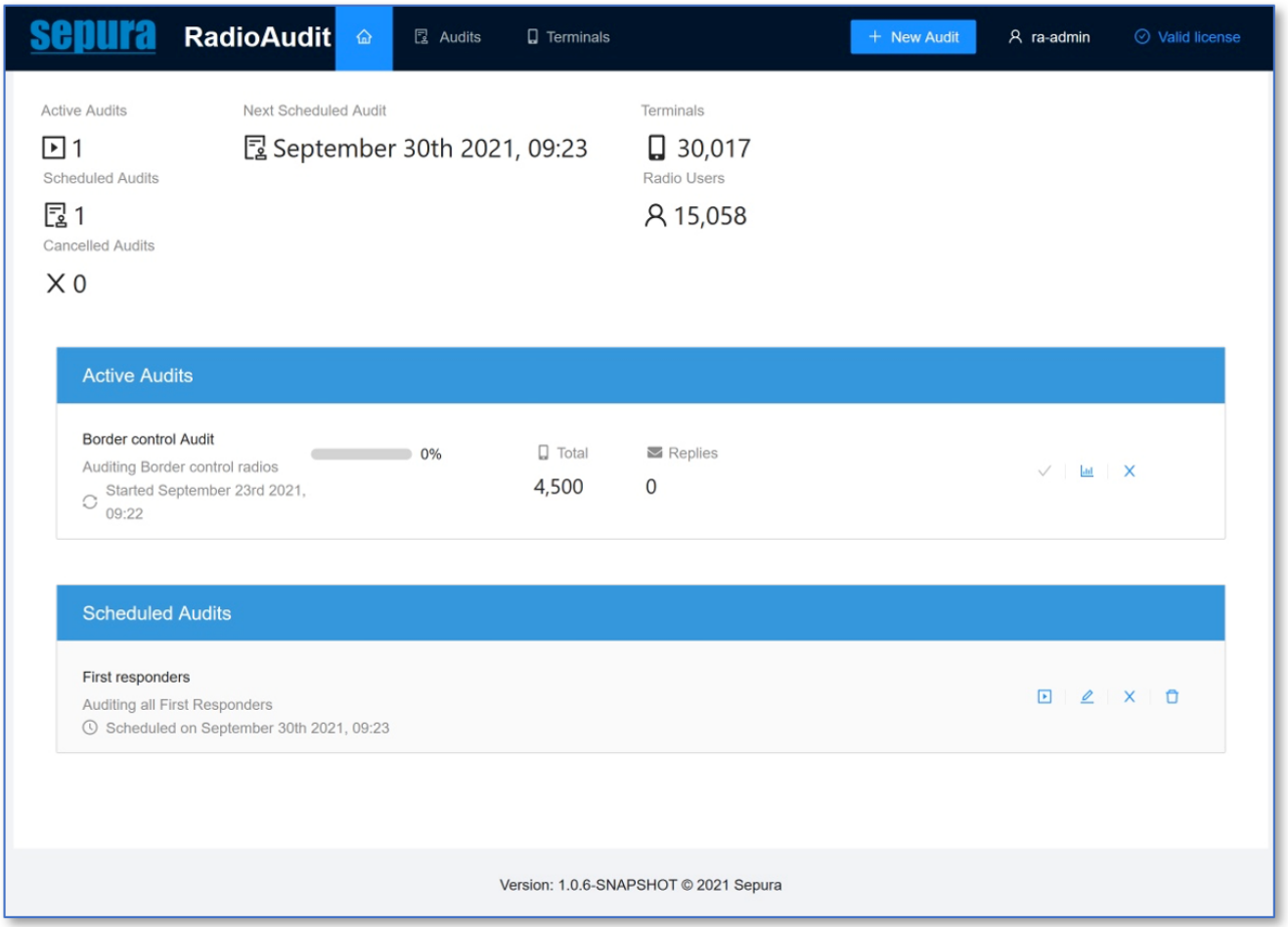
The Sepura RadioAudit client can be opened by pointing the browser to:
http://<name_or_ip_address_of_the_server>:18070

Enter the login credentials. The default credentials are as follows:

Username: ra-admin
Password: password

> **Note:** It is recommended to change the password as soon as possible.

The browser opens the main interface of the Sepura RadioAudit Client:



The Sepura RadioAudit Client Home screen consists of the following elements:

- The navigation toolbar at the top of the screen. See section 4.1.1
- An overview of the RadioAudit status and audit states, including the number of terminals and users in the database.

Below this are shown details of the Audits in the following order:

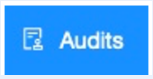
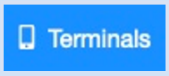
- Active Audits
- Scheduled Audits
- Cancelled Audits
- Completed Audit

The version of the Sepura RadioAudit Client is shown at the bottom of the screen

Each category lists the newest two audits from each category. The detailed view can be seen under the Audits menu.

4.1.1 RadioAudit Client Toolbar Elements

The Sepura RadioAudit Client toolbar consists of following buttons:

	Selects the Home page or Dashboard. This shows an overall view of the RadioAudit status.
	Selects the Audit details page. This page shows the detailed view of the audits.
	Selects the Terminals page. This page shows the detailed view of the radio terminals and the radio users.
	The New Audit button. This is used to create a new audit.
	The logged user details dialog
	The licence management dialog

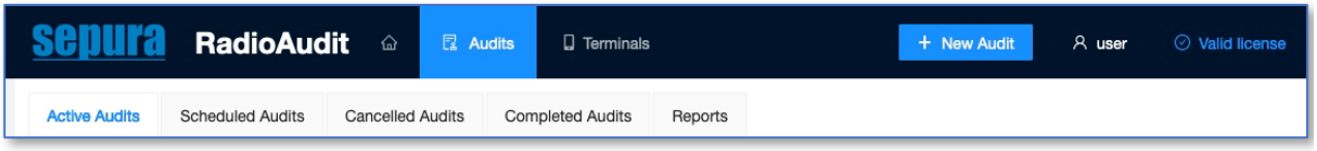
4.1.2 RadioAudit Client Management Icons

The following icons are used in the various pages of the RadioAudit client:

	This icon completes the audit. This icon is used to validate that an audit is complete. This is a manual operation done when the user has reviewed the data returned and validated the audit. The audit is moved under **Completed Audits**.
	This icon runs the audit immediately regardless of its scheduled state. The audit is moved to **Active Audits** if the scheduler is non-recurring. In case of a recurring audit, the **Active Audits** will have an instance of the scheduled audit and the **Scheduled Audit** view will be updated to show the next scheduled instance of the recurring audit. This icon is also used to re-run a cancelled audit. The audit is moved under **Active Audits**.
	This icon is used for editing the audit parameters.
	This icon displays the details of the active audit.
	This icon displays the terminal's audit history
	This icon opens the filtered Audit Exceptions Report.
	This icon is used for cancelling the audit. The audit is completed to the point where all received responses are included in the audit and the requests that have not yet been sent out to the terminals are cancelled. The audit is moved under **Cancelled Audits**.
	This button is used for deleting a scheduled audit, a cancelled audit, and a terminal.

4.1.3 Audit Pages

On the Audit pages are a number of sub-tabs that contain the details of the Audits.



- Active Audits. This view lists all audits that are either currently ongoing or audits that have not yet been completed by the user.
- Scheduled Audits. This view lists all scheduled audits.
- Cancelled Audits. This view lists all cancelled audits.
- Completed Audits. This view lists all completed audits.
- Reports. This view lists details of the audit exceptions.

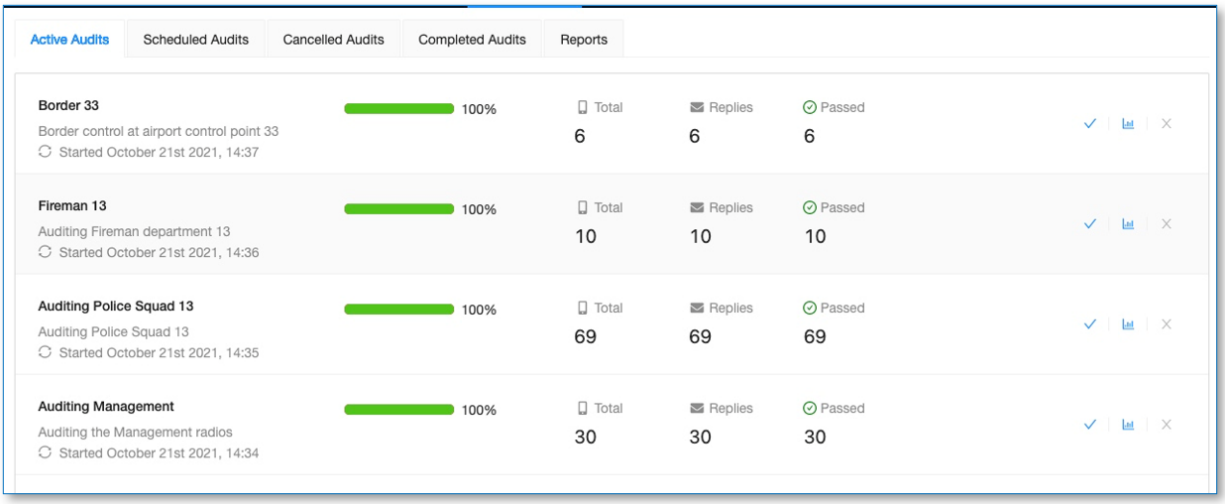
Switching between different views is done by selecting the corresponding tab from the toolbar. It opens the details pages of the selected audit category.

The information displayed on the Active, Cancelled and Completed Audit pages may include the following:

- The name for the audit with a detailed description of the audit
- A progress bar
- How many terminals were included in the audit
- How many terminal users responded to the audit requests
- How many terminals passed the audit
- How many terminals failed the audit

Active Audits Page

The Active Audits page lists all non-completed audits chronologically. Each audit can be checked in details.



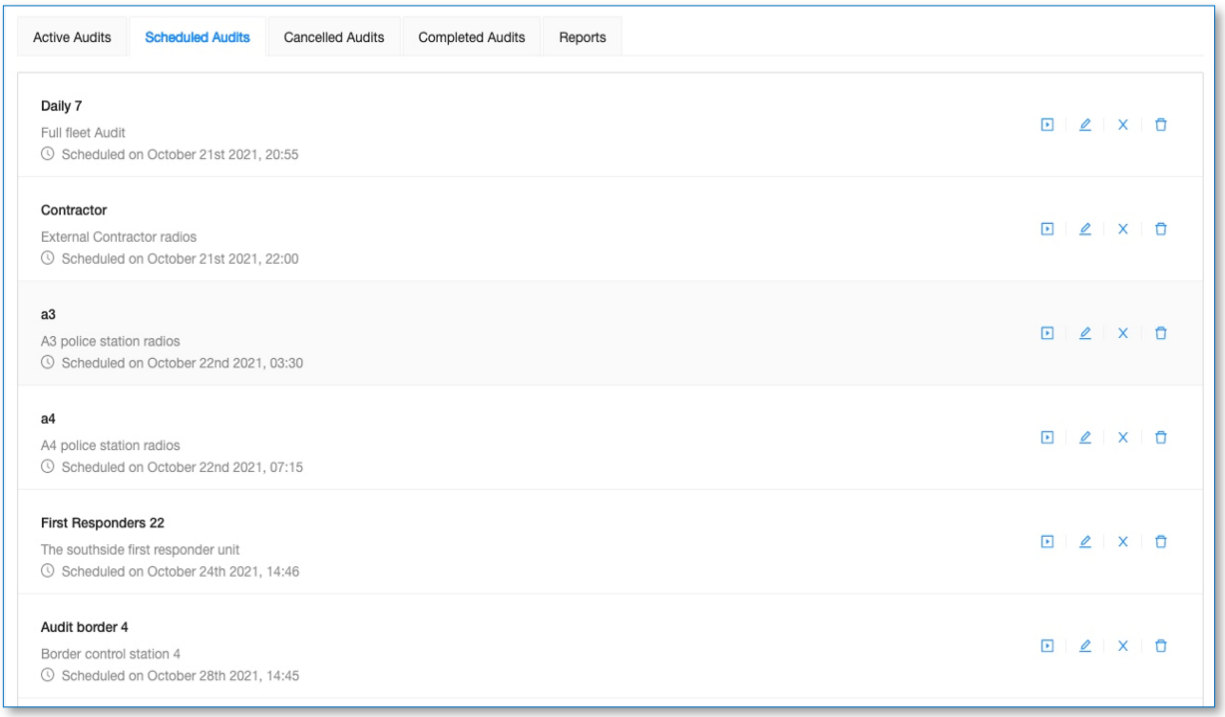
Each audit listed in the Active Audits page can be managed as follows:

- The audit can be Completed.

  This is a manual operation where the user accepts that the audit is complete and valid. The completed audit is moved from the Active Audits list to the Completed Audit list.
- Audit details can be examined by selecting the icon.

Scheduled Audits Page

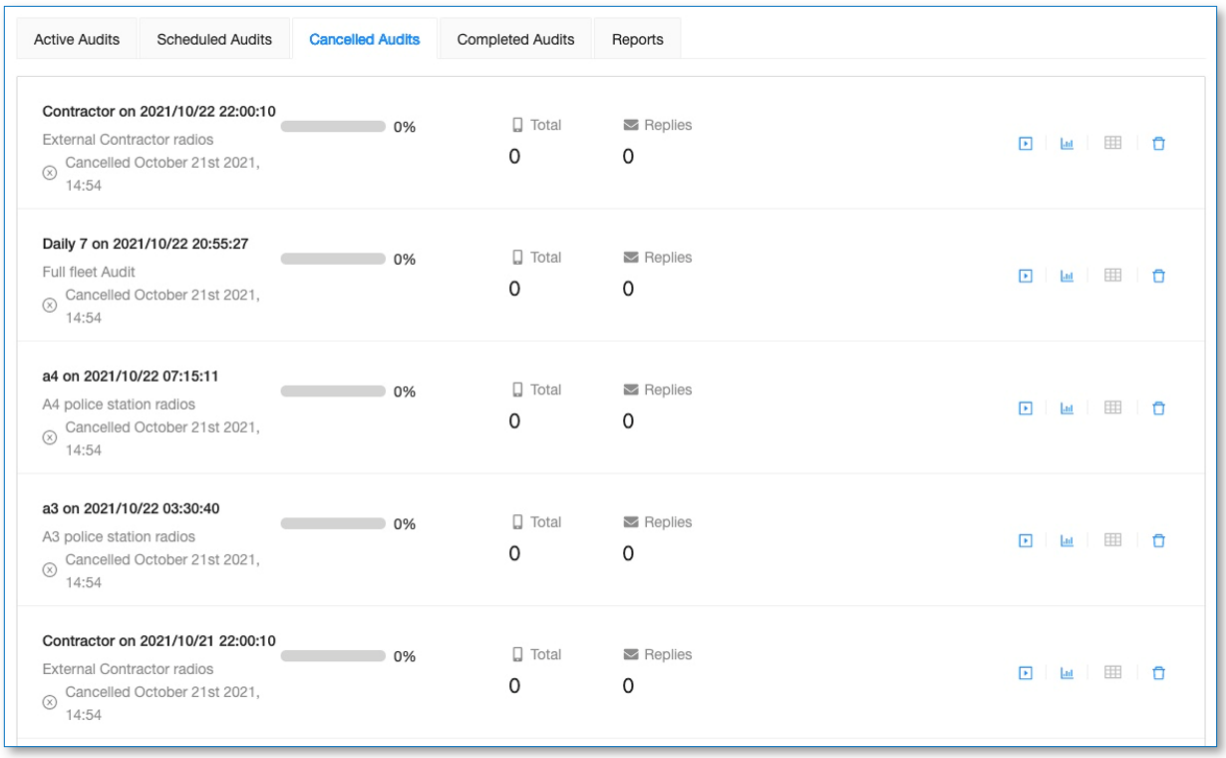
The Scheduled Audits page lists all audits that are scheduled to run.



Each audit listed under Scheduled Audits shows the name of the audit with a detailed description and when the audit is scheduled to run.

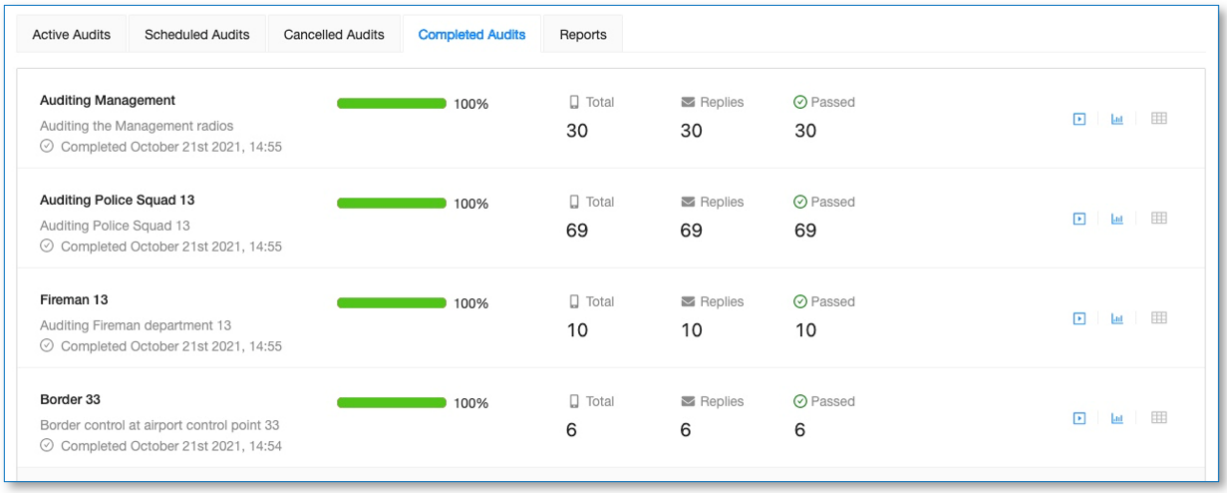
Cancelled Audits Page

The Cancelled Audits page lists the audits that have been cancelled by the user.



Completed Audits Page

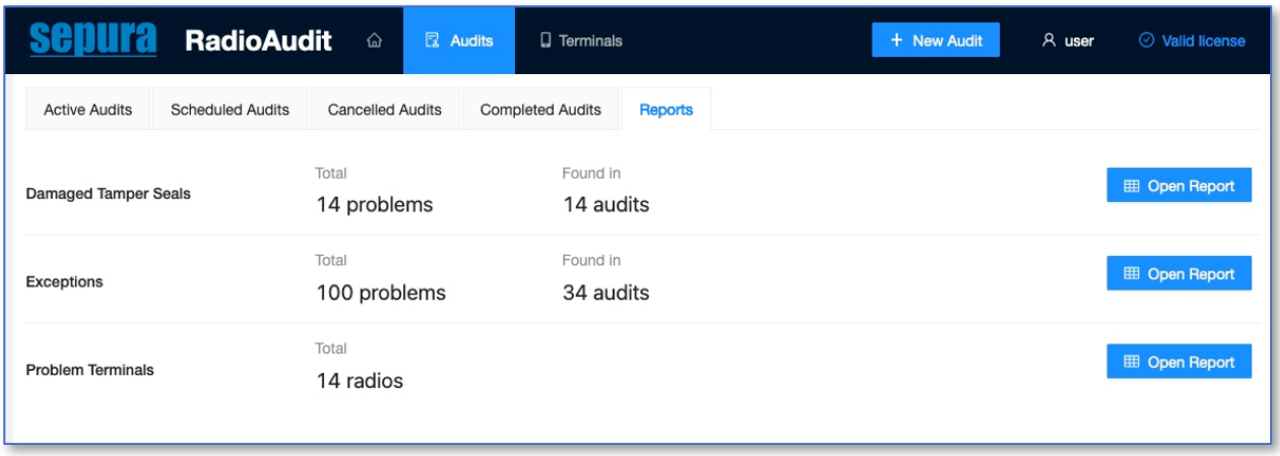
Under Completed Audits all audits that have been run and validated by the user are listed



Reports

Received audit data can be viewed using the RadioAudit application, with reports for:

- Damaged Tamper Seals
- Exceptions
- Problem Terminals
- Successful audits
- Invalid/incomplete audits



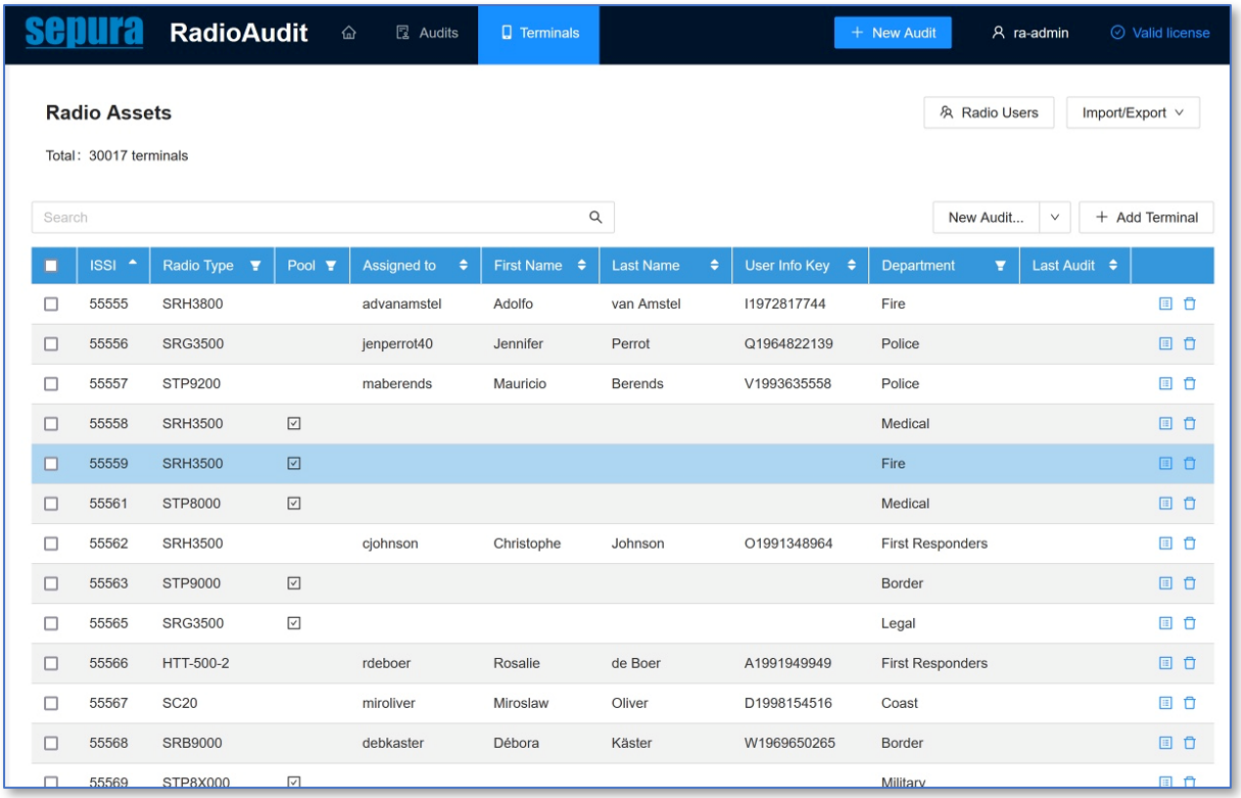
4.1.4 Terminals Page

The terminals page is where:

- All audits are planned and set up. See "4.3 Running an Audit" on page 19.
- The terminals and users are maintained.

The terminals page is divided into two sections. The upper section contains an overview, and tools to maintain the terminals and users, and start the audits.

The lower section lists the terminals that are available in the system.



4.2 User and Data Management

When the RadioAudit Client is run for the first time, the database is empty. The database needs to be populated with terminal and user details. This is done by creating a CSV file.

4.2.1 Creating a CSV File

This section explains how to modify an exported Radio Manager radio fleet CSV Excel file to support the CSV import of RadioAudit. This section does not explain how to export the radio fleet data from Radio Manager into a CSV Excel file. Refer to the Sepura Radio Manager User Guide for further information.

When the Radio Manager radio fleet data has been exported into CSV, you need to modify the CSV file to support the CSV import into RadioAudit.

RadioAudit expects to find the following information in the CSV file:

- Radios with their ISSI numbers and other details
- Users with their details
- Pool radios with their assigned users

The Radio Manager export used in the following example may differ from some Radio Manager CSV exports, but the essential details explained apply.

A typical Radio Manager CSV radio pool export CSV file contains the following headers (not all are shown in the example):

//HardwareCode	TEI	ISSI	Additional In	User Informa	ISSI Range	PUK	PIN	Serial Numb

Do the following:

1. Remove all columns but:
   - **//HardwareCode**
   - **ISSI**

     This will result in a CSV file that has two columns:

//HardwareCode	ISSI
2. Add the following new columns after the ISSI column:

pool	firstName	surname	username	userInfoKey	department

   The header information is not case sensitive, but the syntax of the headers must be correct or the import to RadioAudit will fail.

The contents of the added columns are as follows:

- **pool**: This is either **FALSE** or **TRUE**.

  If this is set to **TRUE**, then the radio is part of a free issue pool that can be used by any of the users registered within the RadioAudit database. User related information to this ISSI does not need to be provided.

  If this is set to **FALSE**, then the radio is a personal radio. All the following user related information must be added. This is mandatory information.
- **firstName**: This is the user's first name.

  When importing plain user information, this is mandatory.
- **Surname**: This is the user's surname.

  When importing plain user information, this is mandatory.
- **Username**: This is the user's username.

  When importing plain user information, this is mandatory.
- **userInfoKey**: This is the user's personal key, used to identify the user on the radio app.

  This is free text. When importing plain user information, this is mandatory.
- **department**: This is the identifier of the department to which the radio and/or user is assigned to.

  This is free text and is mandatory information.

The following types of information are allowed:

- A row of the CSV may contain a radio definition.
- A row of the CSV may contain a user definition.
- A row of the CSV may contain a personal radio definition.

  See the following example:

//HardwareC	issi	pool	firstName	surname	username	userInfoKey	department
PSYTW001T3	12917006	FALSE	Jan-Peter	van der Leek	jvanderleek8	L777292650	DJO6
TG01STUSW	12917029	TRUE					FYL1
			Terje	Nogueira	tenogueira7	Z894469897	TWO7

- The second row is an example of a personal radio entry. This is where the row contains both the radio and user details.
- The third row is an example of a pool radio entry. This is where there is no user information necessary, and **pool** is set to **TRUE**.
- The fourth row is an example of a user entry. This is where there is no radio information necessary. The users are potential pool radio users who may respond to the audit.

When all the details have been entered into the CSV file, **Save** the CSV file. Select an appropriate file name.

When the CSV file has been saved, it can be imported to the system by selecting **Import Terminals from CSV** . This opens the File Explorer where you can select the CSV file to be imported.

Note: If the installed RadioAudit system is not licensed, the import will fail with an error message if the CSV file has more than three rows in it. The unlicensed RadioAudit system allows a maximum of three rows to be added into the database.

4.2.2 Terminal Management

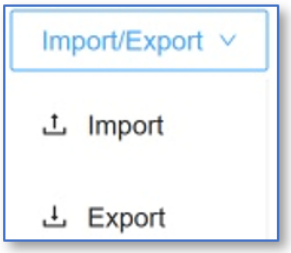
When the CSV file meets the licence conditions the data is successfully imported into the system and after refreshing the browser, it is displayed in the Terminals list.

The list can be updated by:

- Adding new terminals to the list.
- Editing existing terminal properties.
- Deleting existing terminals from the list.

Adding New Terminals Using a CSV

When the CSV is created it can be imported into RadioAudit.



1. Select **Import** from the **Import**/**Export** pull-down menu.

   The following warning is displayed:

   The existing records may be overwritten or deleted when importing this CSV file. Is this OK?

Note: It is important to create a CSV that does not list radio terminals that already exist in the database. The CSV import will fail as the system does not allow existing radio terminals to be overwritten by CSV import.

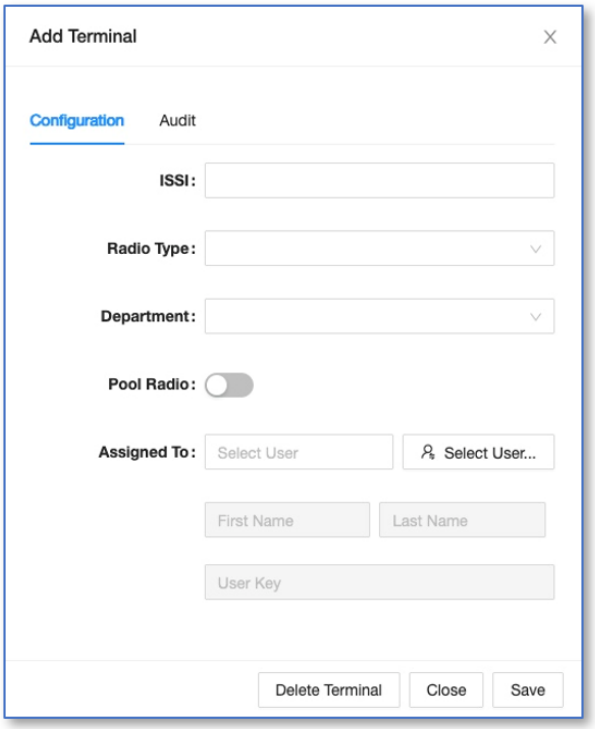
2. Select **OK** to import the CSV file. The new radio terminals are added to the database.

Adding New Terminals Manually

Select Add Terminal on the Terminals page. The Add Terminal dialog is displayed

Adding a new terminal requires the following data:

- **ISSI**: This is the TETRA terminal ISSI number
- **Radio Type**: The available Radio Types can be selected from a pull-down list. If the Radio Type is not listed, it can be added via the same pull-down list.
- **Department**: Select from the pull-down list of existing departments or add a new department.
- **Pool Radio**: The terminal can be a pool radio, or a radio assigned as a personal radio. Set this accordingly.
- **Assigned To**: This is the user ID. Select the user from the list of defined users using **Select User**.



Note: If you try to add a personal radio without Assigned To details the system will indicate an error and will not save the new radio until the error is fixed.

When the terminal details have been entered select Save and the new terminal is added to the list of terminals.

When a radio terminal is a personal radio, it must be assigned to a user. This is so the RadioAudit system can determine user exceptions in the received audit reports.

Note: Only one radio terminal can be assigned to a user.

Assigning a User to a Terminal

To assign a user to an existing terminal:

1. Select the Edit icon at the end of the required terminal row. The **Edit Terminal** dialog is displayed.
2. Toggle the **Pool Radio** switch off. This will expand the dialog to contain user details.
3. Select **Select User** to open the user list dialog. Select the user from the list and then select **Assign**. The users details are loaded into the terminal dialog.
4. Select **Save**. The terminal is assigned to the user.

Unassigning a Terminal

Unassigning a terminal from a user means that the radio terminal will be set as a pool radio:

1. Select the Edit icon at the end of the required terminal row. The **Edit Terminal** dialog is displayed.
2. Toggle the **Pool Radio** switch on.
3. Select **Save**. The radio terminal is unassigned.

Deleting a Terminal

Terminals can be deleted individually or in bulk.

Individual terminals are deleted by selecting the Delete icon at the icon toolbar. The radio terminal is deleted, and any user assignments are automatically removed. The user record remains intact.

Deleting terminals in bulk can be done by selecting each radio terminal checkbox one by one or using search and filter capabilities to select the required terminals.

When the list of radio terminals to be deleted is created select **Delete Selected**. The radio terminals and any radio terminal user assignments will be removed. The user record remains intact.

Exporting Selected Radio Terminals

In addition to performing a full export, selected terminals can be exported into a CSV file.

Exporting terminals can be done by selecting each radio terminal checkbox one by one or using search and filter capabilities to select the required terminals.

When the list of radio terminals is ready, select **Export Selected**. This opens the **File Save** dialog where you can save the CSV into the relevant directory.

4.2.3 User Management

The users that have been defined in the RadioAudit system can be maintained from the Terminals page by selecting **Radio Users**. This opens a dialog where all the users defined in the system are listed.

From the opened dialog you can:

- Add new users
- Maintain existing users' details
- Delete users, either individually or in bulk.

Adding a New User

A new user is added by selecting **Add User.** The **Add New User** dialog is opened.

The following details for the user can be added:

- **User ID**: This is the user ID for the created user.
- **First Name**: This is the users first name.
- **Last Name**: This is the user's last name.
- **User Info Key**: This is users information key that the user will enter the RadioAudit App for identifying the exact user who has been responding to the radio audit request.

When all the details have been entered select **Add User**.

> **Note:** If the new user does not appear automatically, refresh the browser.

Modify User Details

The user details can be modified by selecting the **Edit** icon from the tool icons.

The user details **Properties** dialog is displayed.

All the details can be edited freely. When the editing is complete select **Enter**. The changes are saved into the RadioAudit database, and the user details are updated automatically.

Delete Individual Users

An individual user can be deleted by selecting the Delete icon at the end of the user row. A warning dialog is presented to the user.

Select **OK** to confirm deletion of the user. Select **Cancel** to terminate the delete operation.

> **Note:** If the user has an assigned terminal, this must be unassigned before the deletion is attempted.

4.2.3.4 Delete Users in Bulk

The users can be deleted in bulk by either individually selecting each user checkbox, or by page of users by checking the **Select All** checkbox on the displayed page .

> **Note:** The search and filter capabilities can be used to narrow down the set of users to be deleted in bulk.

When the selection is done select **Delete Selected** at the top of the user list.

This will prompt a confirmation dialog

Select **OK** to delete selected users. Select **Cancel** to terminate the delete operation.

Any terminal assignments will be removed, and the users are deleted from the system. The terminals will be left intact.

4.3 Running an Audit

4.3.1 Log on RadioAudit Client

The Sepura RadioAudit client can be opened by pointing the browser to:

http://<name_or_ip_address_of_the_server>:18070

The login screen is displayed:

Enter the login credentials and select **Log in**. The browser opens the main interface of the Sepura RadioAudit Client.

The default credentials are as follows:

Username: ra-admin

Password: password

> **Note:** It is recommended to change the password as soon as possible.

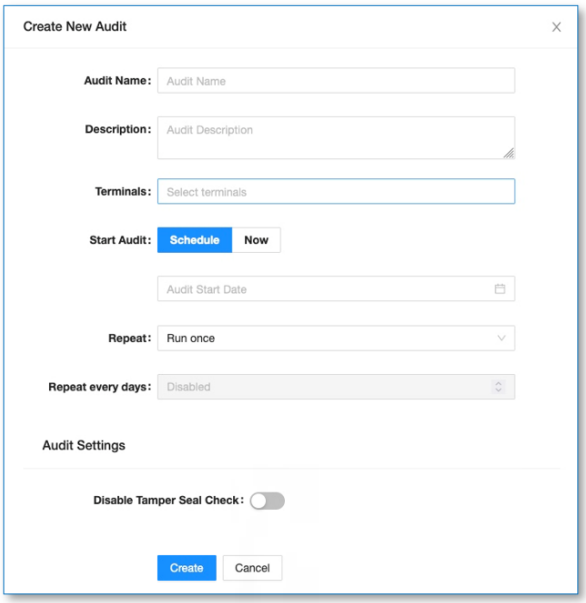
4.3.2 Creating an Audit

The audit process begins by identifying the terminals that will be audited. There are number of ways to do this:

- By selecting New Audit.
- By selecting predefined New Audit pull down menu options
- By selecting Terminals from the list of terminals
- By filtering the Terminals in the list

Creating an Audit Using New Audit

On selecting New Audit, the Create New Audit dialog is displayed:



The following details should be entered into the dialog:

Audit Name: The descriptive name for the audit.

Description: The is the description of the audit.

Terminals: Select Terminals from the pull-down list. The following options are available:

- **All Terminals**: This selects all terminals in the database.

  There may be large number of terminals in the database so this option should be used with care as it will create a very lengthy audit.
- **Departments**: The Terminals are selected on a department basis.

  Multiple departments can be picked from the list by selecting the department names.
- **Radio Use**: This allows the selection of either Pool Radios or Assigned Radios.
- **Radio Generation**: This allows the selection of the required radio generation.
- **Start Audit**: The selection options are:

  > **Scheduled**: This is for recurring audits

  > **Now**: This is for audits that are started immediately
- **Repeat**: This is a recurrence setting. The options are:

  > **Run Once**: When set the audit will run just once

  > **Every Year**: The audit will run yearly until cancelled

  > **Every 6 months**: The audit will run every six months until cancelled

  > **Every 3 months**: The audit will run every 3 months until cancelled

  > **Every X days**: The audit will run every set number of days until cancelled
- **Repeat days**: This is a recurrence setting for **Every X** days selection.

  For any other option it will be greyed out.
- **Disable Tamper Seal Check**: This toggle determines whether the **Terminal Tamper Seal** check option will be displayed to the radio user or not.

  This setting is determined by the global setting in the Apps Control Panel. Toggling the setting per audit will override the global setting.

When all the details have been entered select Create. This will create the audit and depending on the settings it will either start immediately or as per the schedule set.

> **Note:** If the number of terminals in the audit exceeds the number of terminals licensed, the creation of the audit will fail with an error displayed to the user. Reduce the number of terminals in the audit to match the licence limit.

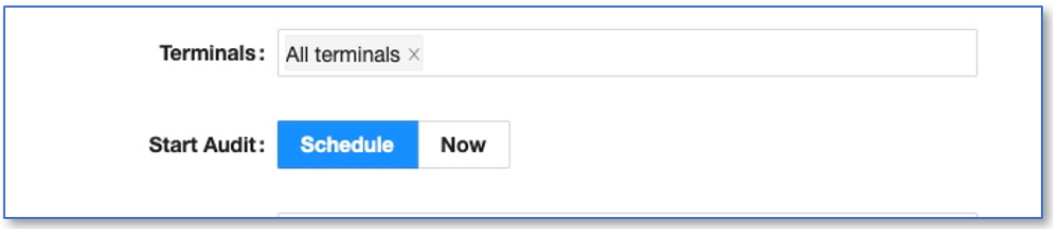
Creating an Audit Using Predefined Menu Options

To create an audit using the predefined **New Audit** menu options select one of the following options:

- All Terminals
- From This Page Only

All Terminals

Selecting the **All Terminals** option opens the **Create New Audit** dialog with the **Terminals** field pre-filled.



Complete the rest of the **Create New Audit** dialog as required.

When all the details have been entered select **Create**. This will create the audit and depending on the settings it will either start immediately or as per the schedule set.

> **Note:** There may be large number of terminals in the database so this option should be used with care as it will create a very lengthy audit.

From This Page Only

Selecting the **From This Page Only** option opens the **Create New Audit** dialog with the Terminals field pre-filled based on the selection.

> **Note:** The number of terminals selected depends on the pagination setting. Filters can be used to collect the required list of terminals on the visible page.

Complete the rest of the **Create New Audit** dialog as required.

When all the details have been entered select **Create**. This will create the audit and depending on the settings it will either start immediately or as per the schedule set.

Creating an Audit by Selecting Terminals from the List

Creating an audit by selecting terminals from the list can be done as follows:

- By selecting individual terminals
- By grouping selected terminals

> **Note:** The filters and search capability can be used to narrow down the list of terminals to choose from.

Selecting individual terminals

Individual terminals can be selected by checking the checkbox at the left of each terminal row. This introduces a new entry called **Selected Terminals** under the **New Audit** menu list:

When all the required terminal checkboxes have been checked, select the **Selected Terminals** option under the **New Audit** menu list. This opens the **Create New Audit** dialog with the **Terminals** field pre-filled based on the selection.

Complete the rest of the **Create New Audit** dialog as required.

When all the details have been entered select **Create**. This will create the audit and depending on the settings it will either start immediately or as per the schedule set.

Grouping selected terminals

Grouping selected terminals is done by checking the **Select All** checkbox at the top of the terminal rows. This will select all the terminals on the current page. Multiple pages can be selected by moving to the next page and checking the select all checkbox again.

> **Note:** The filters and search capability can be used to narrow down the list of terminals to choose from.

When all the required terminal checkboxes have been checked, select the **Selected Terminals** option under the **New Audit** menu list. This opens the **Create New Audit** dialog with the **Terminals** field pre-filled based on the selection.

Complete the rest of the **Create New Audit** dialog as required.

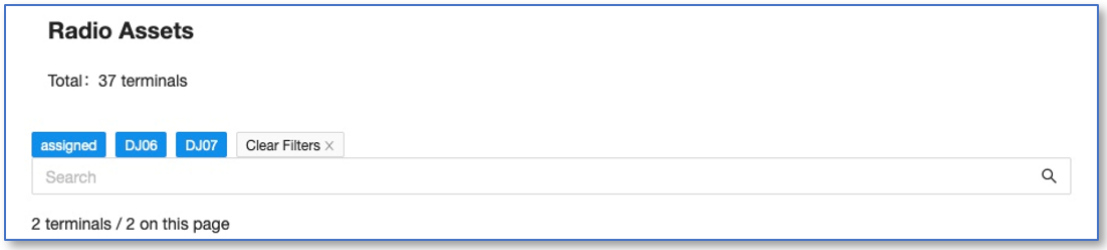
When all the details have been entered select **Create**. This will create the audit and depending on the settings it will either start immediately or as per the schedule set.

Creating an Audit by Filtering the Terminals List

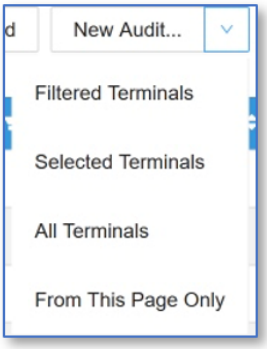
Creating an audit by filtering the terminals list can be done as follows. The filters can be accessed by selecting the icon in the Terminals list header.

This opens a filter specific pop-up window from which the filter action can be selected. Multiple filters can be set as required

The Terminals list will be filtered accordingly, and the filters will be displayed at the top of the Terminals list



The set filters can be cleared by selecting **Clear Filters**. This will clear all set filters and the Terminals view will be restored to its previous state. When all the required terminal checkboxes have been checked, select the **Filtered Terminals** option under the **New Audit** menu list.



This opens the **Create New Audit** dialog with the **Terminals** field pre-filled based on the selection. Complete the rest of the **Create New Audit** dialog as required.

When all the details have been entered select **Create**. This will create the audit and depending on the settings it will either start immediately or as per the schedule set.

4.3.3 Creating an Audit Using Search Capabilities

Audit contents can also be created using the RadioAudit search capabilities.

Typing in the search box will immediately display all the radio terminals that match the entered search string. The search string is case insensitive.

Note: Some data is not searchable but is displayed as text in the radio terminals list.

The following radio terminal fields are used in the search:

- ISSI
- Assigned To
- First Name
- Last Name
- User Info Key
- Department

When all the required terminal checkboxes have been checked, select the **Filtered Terminals** option under the **New Audit** menu list.

This opens the **Create New Audit** dialog with the **Terminals** field pre-filled based on the selection.

Complete the rest of the **Create New Audit** dialog as required.

When all the details have been entered select **Create**. This will create the audit and depending on the settings it will either start immediately or as per the schedule set.

4.3.4 Completing an Audit

An audit that has been run must be completed. This is done manually. The initial selection is done in the **Create Audit** dialog.

Scheduled completion of the audit does not require any manual interaction when set. It can still be manually completed.

Manual completion of the audit is done from the Active Audit page by selecting the Complete Audit icon .

This will complete the audit and move the audit from the **Active Audits** to the **Completed Audits** page.

4.3.5 Cancelling an Audit

The following audits can be cancelled:

- An Active Audit that has not completed the run
- A Scheduled Audit that is listed in the Scheduled Audits list.

Cancelling an Active Audit

An active audit can be cancelled up until the radio response rate has reached 100%. Select the Cancel Audit icon in the tool icon section. A confirmation dialog is presented to the user:

When cancelled the audit is moved to **Cancelled Audits** and any remaining audit requests are deleted. The audit data is updated with the final response details from the radios.

Cancelling a Scheduled Audit

A Scheduled Audit can be cancelled if it is listed in the **Scheduled Audits** list. Cancellation is always against the latest instance of the scheduled audit.

Cancelling a Single Instance

Cancelling an audit that has only a single instance is done by selecting the Cancel Audit icon in the tool icon section. A confirmation dialog is presented to the user:

When cancelled the scheduled audit is moved to **Cancelled Audits**. The audit data is updated with the final response details from the radios.

Cancelling an Instance from a Recurring Audit

Cancelling an instance from a scheduled recurring audit is done by selecting the Cancel Audit icon in the tool icon section. A confirmation dialog is presented to the user:

When cancelled the scheduled audit is moved to **Cancelled Audits**. The audit data is updated with the final response details from the radios.

4.3.6 Deleting an Audit

Only scheduled audits or cancelled audits can be deleted. These are audits that have not run yet or are not completed.

The deletion is done by selecting the Delete Audit icon in the tool icon section. A confirmation dialog is presented to the user.

All instances of the selected audit are deleted.

4.3.7 Modifying an Existing Audit

Existing audit can be modified. This applies only to scheduled audits. Modifying an audit can be done by selecting the Edit icon in the tool icon section.

This will open the **Create New Audit** dialog showing the audit parameters. The audit parameters can be edited as required.

When the changes are complete, select **Update** to accept the changes. Selecting **Cancel** will cancel the modifications.

4.3.8 Re-running an Audit

A completed or cancelled audit can be re-run. Rerunning an audit is done by selecting the Run the Audit Again icon in the tool icon section. This will open the **Create New Audit** dialog showing the audit parameters. The audit parameters can be edited as required.

When the changes are complete, select **Update** to accept the changes. Selecting **Cancel** will cancel the re-run attempt.

The re-run audit is listed in the **Active Audits** page.

4.3.9 Start Scheduled Audit Now

A Scheduled Audit can be started immediately. Select the Run the Audit Again icon in the tool icon section.

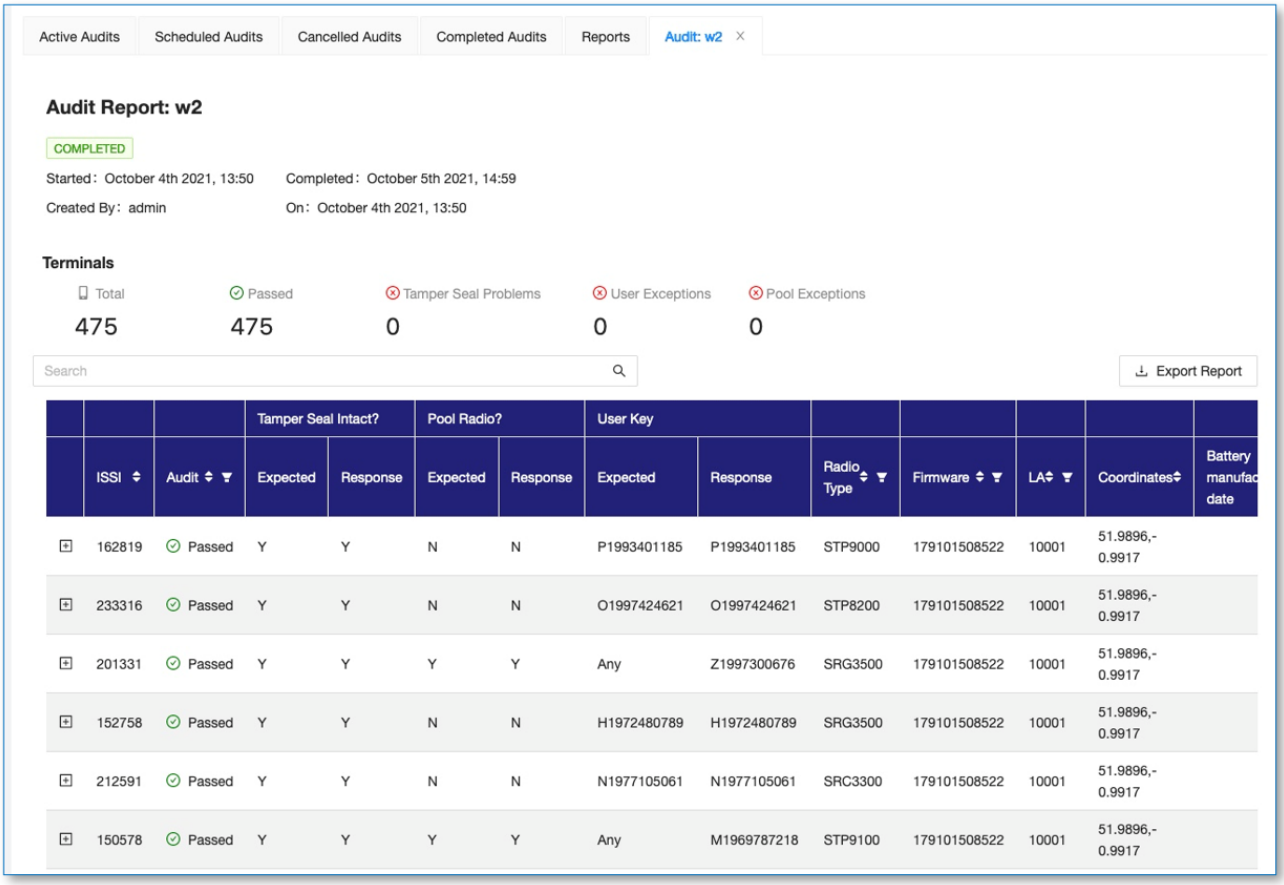
This will open the **Create New Audit** dialog showing the audit parameters. The audit parameters can be edited as required.

When the changes are complete, select **Update** to accept the changes. Selecting **Cancel** will cancel the run now attempt.

The manually started scheduled audit is listed in the **Active Audits** page.

4.3.10 Viewing Audit Data

When selecting the **Open the Audit** data icon it opens a new view where the audit details are displayed.



The page is divided into two sections:

- An overview of the audit and terminals
- The detailed view of terminals included in the audit

The overview has the following details of the selected audit:

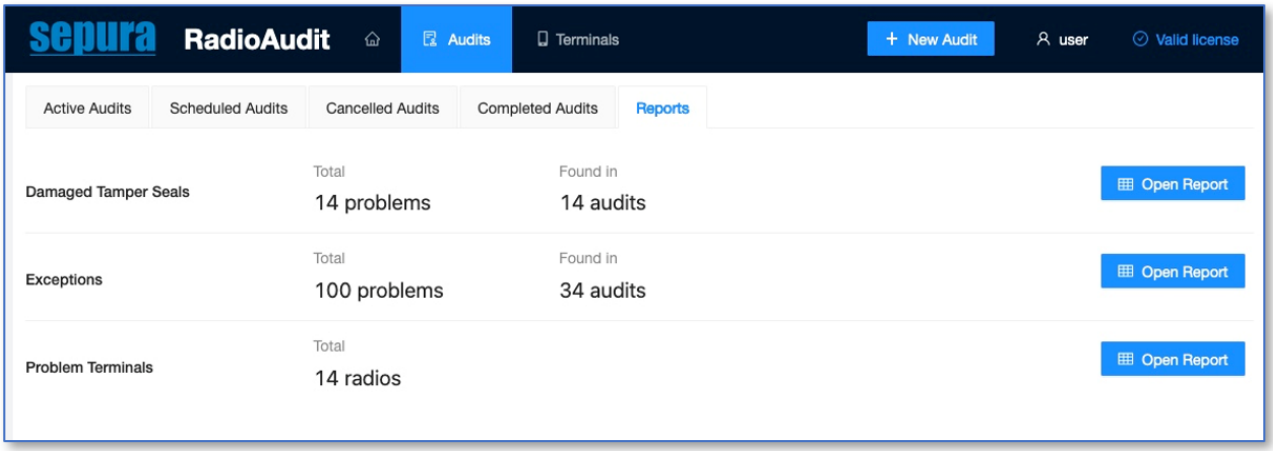
- The name of the audit.
- The status of the audit. The status icon can be as follows:
  > **Started**: This is an active audit.
  > **Cancelled**: This is a cancelled audit.
  > **Completed**: This is a completed audit.
- **Started**: When the audit was started.
- **Completed**: When the audit was completed. This will be visible only when looking at completed audit details.
- **Cancelled**: When the audit was cancelled. This will be visible only when looking at cancelled audit details.
- **Created By**: This is the details of the user who created the audit.
- **On**: This is the date when the user created the audit.

The simple statistics section also contains the following details of the terminals in the selected audit:

- **Total**: This is the number of terminals that were selected for this audit.
- **Passed**: This is the number of terminals that had no issues reported.
- **Tamper Seal Problems**: This is the number of terminals that were reported to have issues with the terminal tamper seal.
- **User Exceptions**: This is the number or terminals that were reported by a user that does not exist in the RadioAudit database.
- **Pool Exceptions**: This is the number of terminals that were incorrectly reported either as pool radios or personal radios.
- **No Response**: This is the number of terminals that did not send any response to the audit requests. This is only visible in the Cancelled Audits data.

4.3.11 Exception Reports

The audit exception reports can be viewed from the Reports page under Audits.



- **Damaged Tamper Seals**: This report lists the audits that had damaged tamper seals reported.
- **Exceptions**: This report lists the user and pool radio exceptions. These are recorded when users incorrectly report pool radios or when users, that are not defined in the database, are detected responding to the audit requests.
- **Problem terminals**: This special report lists the terminals that repeatedly report the same issue or are repeatedly ignoring the audit requests.

5.0 Using the RadioAudit App

This chapter outlines the most typical RadioAudit use case, indicating how and when various parts of the product will be used throughout the workflow. This example assumes that the product has already been commissioned with the relevant radio fleet and that user data has already been imported into the server application.

When the Sepura RadioAudit App has been installed on the radio terminal, by the radio fleet manager, and the radio has been switched on, there is no additional user interaction needed to operate this function on the radio. When the RadioAudit request is received by the radio it will prompt the user with appropriate user dialogs.

5.1 Radio Functions

To maintain the critical safety capability of the radio, all radio functions are available for use while the audit is in progress. However, the audit request will continuously re-appear when using the radio to remind the user to complete the audit.

To avoid such interruptions during normal operations, it is strongly recommended that the user complete the audit as soon as it appears after the radio is powered on.

5.2 Audit Operation

The RadioAudit system initiates an audit and communicates with each radio being audited by sending out a dedicated SDS message over the TETRA network

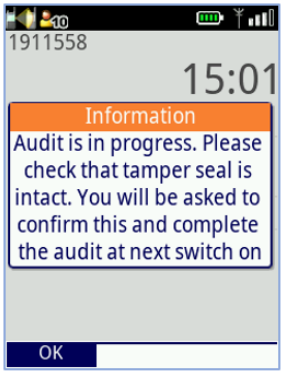
Each radio receives an SDS message, notifying the radio user that an Audit is in progress. The radio remains fully operational during the audit process.

5.2.1 SC and SCG Radios

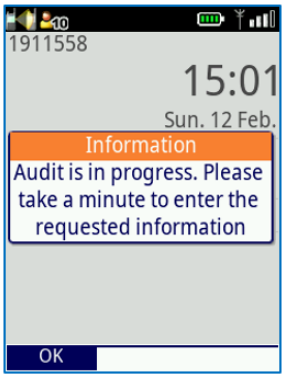
To complete the audit, users of SC and SCG radios should do the following:

1. On receipt of the audit notification, select **OK**.

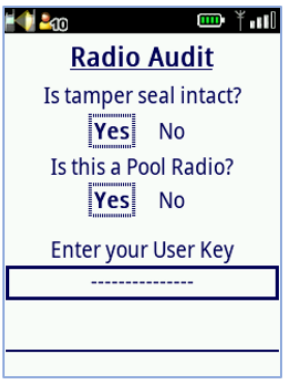
   A full audit requests that the tamper seal be checked. Continue with step 2.



   If a partial audit is requested, the tamper seal does not need to be checked. Continue with step 6.



2. Switch off the radio, remove the battery and check that the tamper seal is intact.
3. Replace the battery and switch the radio on.
4. When switch on is complete the request for audit information is displayed.
5. Select **Yes** if the tamper seal is intact, select **No** if the seal is damaged.
6. Select **Yes** if the radio is a pool radio, select **No** if the radio is assigned to you.
7. Using the alphanumeric keys enter your User Key.
8. Select **Send**. The audit information is complete and is sent to the RadioAudit server.



This completes the audit request.

5.2.2 SRH, STP and SRG Radios

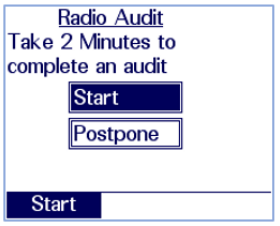
To complete the audit, users of SRH, STP and SRG radios should do the following:

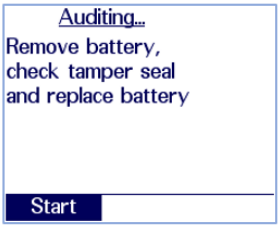
1. On receipt of the audit notification, select **Start** to start the audit.

   Select **Postpone** to postpone the audit. The audit notification will reappear at set intervals as a reminder.

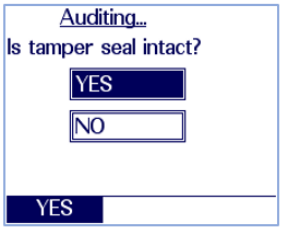
   A full audit requests that the tamper seal be checked. The audit continues with step 2.

   If a partial audit is requested, the tamper seal does not need to be checked and the audit continues with step 6.
2. Switch off the radio, remove the battery and check that the tamper seal is intact.
3. Replace the battery and switch the radio on.

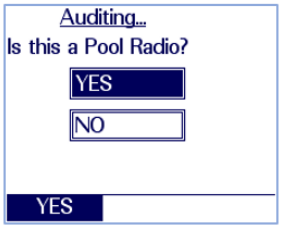




4. When switch on is complete the request for audit information is displayed.
5. Select **Yes** if the tamper seal is intact, select **No** if the seal is damaged.

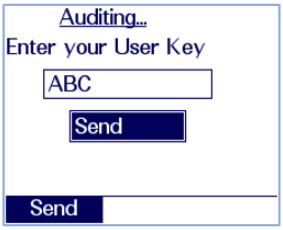


6. Select **Yes** if the radio is a pool radio, select **No** if the radio is assigned to you.



7. Using the alphanumeric keys enter your **User Key**.
8. Select **Send**. The audit information is complete and is sent to the RadioAudit server.

This completes the audit request.



6.0 RadioAudit App Installation

The RadioAudit App for Sepura SC2 and SCG TETRA radios is installed using Radio Manager. Refer to the Sepura Radio Manager User Guide for details.

6.1 Radio Requirements

The RadioAudit App is compatible with the following radios:

Handheld:

- Sepura SC Series using V2.0 Firmware or later

Mobile:

- Sepura SCG using V3.1 Firmware or later

The Sepura SC2 and SCG TETRA radio's configuration file is generated using the AppSPACE Configuration Editor. Refer to the AppSPACE Configuration Editor User Guide for further information.

The parameters that can be configured are listed in "3.1 RadioAudit App Configuration" on page 3.

The configuration file is then loaded onto the TETRA radio using Radio Manager. Refer to the Radio Manager User Guide for further information.

7.0 RadioAudit Server Installation

The following sections should be read carefully when installing Sepura RadioAudit. The sections contain important prerequisite checks that should be done prior to the installation.

You must have Administrator privileges on the machine to install Sepura RadioAudit.

7.1 PC Requirements

Important: RadioAudit must be installed on a clean and dedicated server. Multiple Sepura applications cannot be installed and run on the same server.

Minimum Hardware requirements:

- 64-bit PC Server, 3GHz+ CPU, 8GB memory, 256GB disk space (SSD or RAID recommended)

Operating System

- Windows Server 2016 or later or Windows 10 Pro

Requires Sepura SCG22 or SRG3900 for PEI connection to the TETRA network

7.1.1 Firewall Settings

All service to service connections normally take place in “localhost” and therefore do not require any specific firewall ports to be opened. The following external ports are used:

Service	Port
Apps Control Panel	TCP/8080
RadioAudit Client	TCP/ 18070 -> HTTPS/8498
RabbitMQ Management	TCP/15672

7.1.2 User Homedrive Settings

If the user’s homedrive is not the C: drive, then execute the steps in section 7.3.2 after the RadioAudit installation has been done. This is needed because the Erlang cookie is stored, by default, on the user’s homedrive.

Note: If the homedrive is not the C: drive, then the RabbitMQ service cannot run as expected and other services dependent on RabbitMQ cannot start or do not function correctly.

7.1.3 Connection to TETRA PEI Radio Modem

To support USB connection of your PC or Server with the Radio Modem, first install the Virtual COM Port FTDI driver on your PC from www.ftdichip.com/Drivers/VCP.htm

Configuration can be done automatically during the Sepura RadioAudit installation if the TETRA-PEI modem is connected, and driver is installed. The Sepura RadioAudit installer requires the SSI number in TETRA-PEI modem to be defined:

1. Using the appropriate cable, connect the TETRA-PEI Radio Modem to the PC/Server USB port.
2. Check that the connection has been established by ensuring that the TETRA-PEI Modem appears in the PC Device Manager.
3. Under the ‘General’ Tab of the PEI modem connection check that the Manufacturer field reads ‘FTDI’.

7.2 Server Application Installation

To install the RadioAudit software on a Windows Server 2016 or Windows 10 machine, do the following:

1. Start the RadioAudit Windows installation by running the Sepura RadioAudit installer:

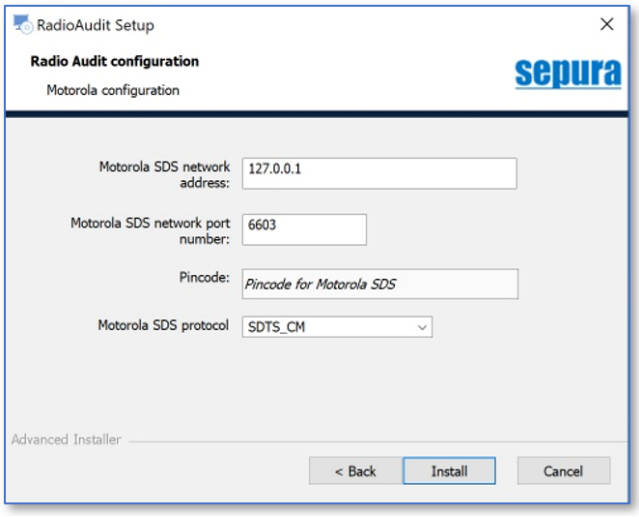
   RadioAudit.exe
2. Select **Yes** in the User Account Control dialog.
3. In **RadioAudit Setup**, select **Next** to continue.
4. Accept the Licence Agreement terms and select **Next** to continue.
5. It is recommended to use the default selection in Prerequisites. Select **Next** to continue.
6. Accept the default installation folder location by selecting **Next**.
7. In Network configuration enter the following details:
   - **Application ISSI**: This is the ISSI number that will be used by RadioAudit as sender identifier. Enter an appropriate ISSI number here.
   - **Select network type**: This is a pull-down list where you can select how the RadioAudit will connect to the network. The possible options are as follows:
     > **Motorola**: This is for Motorola SDR TETRA network. Select **Next** and go to section 7.2.1.
     > **Nebula**: This is for Teltronic Nebula TETRA network. Select **Next** and go to section 7.2.2.
     > **TCS Gateway**: This is for Airbus TETRA network. Select **Next** and go to section 7.2.3.
     > **TETRA PEI**: This is for TETRA PEI connection. Select **Next** and go to section 7.2.4.

The installer will create the suitable configuration based on your selection.

7.2.1 Motorola SDR Configuration

When selecting Motorola from the pull-down list, the installer will prompt for additional data:

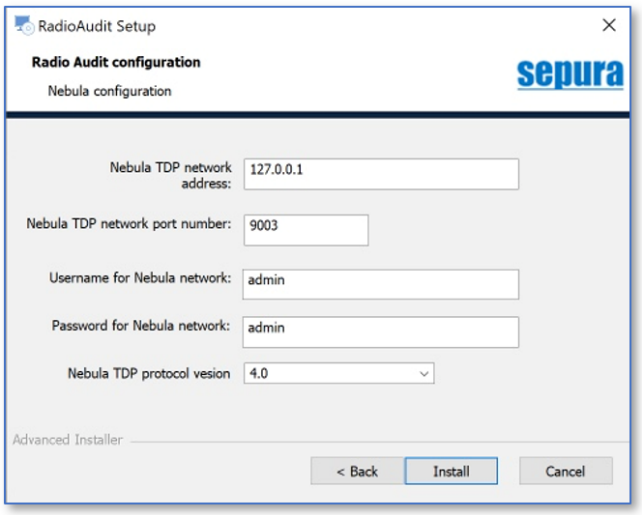
1. Enter the following details:
   - **Motorola SDR network address**: This is the IP address for the Motorola SDR.
   - **Motorola SDR network port number**: This is the IP port for the Motorola SDR. The default is 6603.
   - **Pincode**: This is the PIN code for the Motorola SDR access.
   - **Motorola SDS protocol**: This is the SDS protocol variant selection. Typically, this is left as default.
2. Select **Install** and continue to "Installation Completion" on page 34.



7.2.2 Nebula Configuration

When selecting the Nebula from the pull-down list, the installer will prompt for additional data:

1. Enter the following details:
   - **Nebula TDP network address**: This is the IP address for the Nebula network.
   - **Nebula TDP network port number**: This is the IP port for the Nebula network. The default is 9003.
   - **Username for Nebula network**: This is the login username for accessing the Nebula network.
   - **Password for Nebula network**: This is the login password for accessing the Nebula network.
   - **Nebula TDP protocol version**: With this pull-down list you can select the protocol version that is supported by the Nebula network.

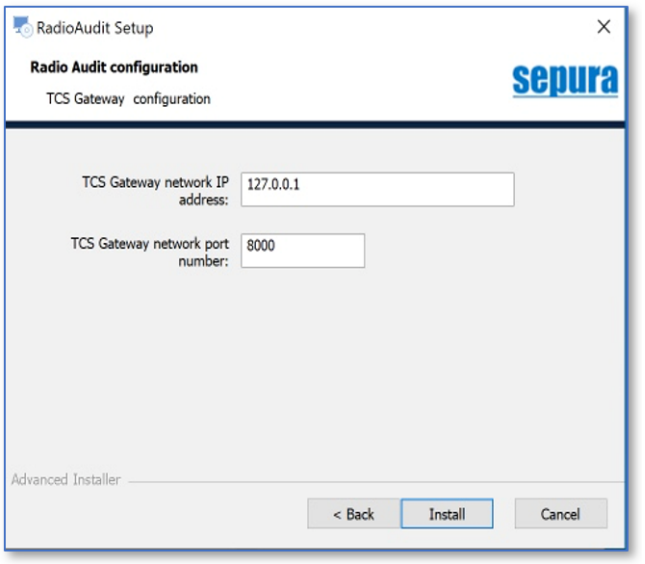


2. Select **Install** and continue to "Installation Completion" on page 34.

7.2.3 TCS Gateway Configuration

When selecting the TCS Gateway from the pull-down list, the installer will prompt for additional data:

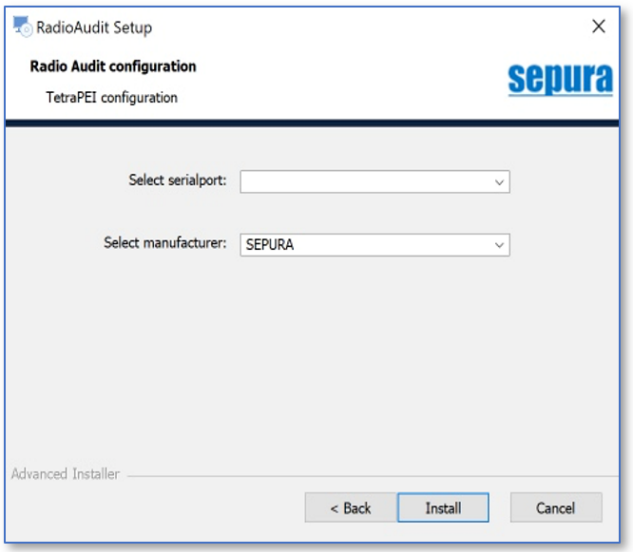
1. Enter the following details:
   - **TCS Gateway network IP address**: This is the IP address for the TCS Gateway.
   - **TCS Gateway network port number**: This is the IP port for the TCS Gateway. The default is 8000.
2. Select **Install** and continue to "Installation Completion" on page 34.



7.2.4 TETRA PEI Configuration

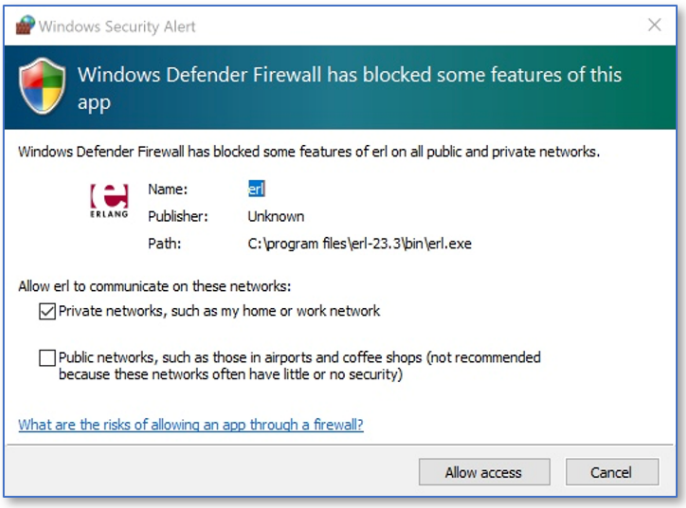
When selecting the TETRA PEI from the pull-down list, the installer will prompt for additional data:

1. Enter the following details:
   - **Select serialport**: This is the pull-down list for the serial port where the TETRA PEI radio is attached to. See section 7.1.3.
   - **Select manufacturer**: Select the TETRA PEI radio manufacturer form pull-down list. The default is Sepura. Another supported PEI radio is Airbus.
2. Select **Install** to continue.



7.2.5 Installation Completion

The firewall that is active on the target machine may prompt for access to Erlang or other services.



It is advisable to allow access to the prompted services:

1. Select **Allow Access**.
2. Wait until the RadioAudit services are installed and the complete install dialog is displayed. This may take some time.
3. Select **Finish** to complete the RadioAudit installation.

7.3 Post-install Checks

After installation of the RadioAudit, it is recommended that the following basic checks are done to verify that the RadioAudit services have been installed correctly, and the system is ready for use.

7.3.1 Checking Windows Services

Check the windows services using, for example, Task Manager for the following services:

- Check that the Apache Zookeeper service is up and running. If it is not running, try to start the service.
- Check that the MongoDB service is running. If the MongoDB service is not running, try to start the service.
- The following services must all be running. If not try to start the service.
  - > Apps Control Panel
  - > Message Gateway,
  - > Query
  - > RadioAudit
  - > ZK-Cache
- Check the RabbitMQ service is running. If it is not running, try to start the service.

7.3.2 Environment Variable Checks

If the Message Gateway or Query services refuse to start or give an Access denied error when trying to restart the service, check the following environment variables:

1. Open the RabbitMQ Command Prompt from Windows Start > RabbitMQ Server.
2. Type in: `>set`.
3. Check where the HOMEDRIVE environment variable is pointing to. If it is not a local disk, such as C: enter the following commands:

```
>SET HOMEDRIVE=C:
>rabbitmq-plugins.bat enable rabbitmq_management
>rabbitmq-service.bat stop
>rabbitmq-service.bat install
>rabbitmq-service.bat start
```

4. Start the failing services. Check the rest of the services as per section 7.3.1.

7.3.3 Checking the Apps Control Panel

When the processes are running, check that the Apps Control Panel can be opened using your preferred browser.

1. Point your preferred browser to the http://localhost:8080 address
2. Enter the following login credentials to log on.

   Username: admin

   Password: password

When logged in the Apps Control Panel is displayed.

Note: It is recommended to change the password from the default.

The Apps Control Panel tabs are:

- **Message Gateway** – This opens the network connectivity settings page.
- **Query**: This opens the Query configuration page.
- RadioAudit: This opens the RadioAudit specific configuration page.
- **Users**: This page is for managing the users that have access to the system.

7.3.4 Testing Connectivity

When the RadioAudit has been installed and all services are OK it is good to check that the messages from the RadioAudit AppSPACE App terminal are going to the RadioAudit backend.

This can be checked by sending a simple “echo” SDS message to the TETRA PEI radio’s ISSI.

The message is in the format:

```
echo <here's your text>.
```

You should receive an SDS message back having the text you originally sent.

Example: If you sent the message “echo hello”, you should receive an SDS message containing the text “hello”.

7.3.5 Logging On to the RadioAudit Client

The Sepura RadioAudit client can be opened by pointing the browser to:

http://<name_or_ip_address_of_the_server>:18070

The login screen is displayed:

Enter the login credentials and select Log in. The browser opens the main interface of the Sepura RadioAudit Client.

Username: ra-admin

Password: password

Note: It is recommended to change the password from the default.

Note: If the RadioAudit client does not open using the URL http://<server>:18070, try https://<server>:8488 instead. The browser may state this is an unsafe site. Accept the exception and continue.

7.4 Licensing

Sepura RadioAudit features are activated and protected by licence. If RadioAudit is installed without any licence the software will run in Demo mode.

The licence enables the feature set for the product variant installed and is obtained by sending the installation ID (unique machine code) that is generated during the installation of the software to Sepura Customer Support. The licence file supplied by Sepura is imported into RadioAudit to authenticate the installation and activate the features. The licence locks the RadioAudit installation to a specific computer, preventing duplication of the software and prohibits the software from being run from other computers.

The licence can be added during the installation, if the licence key is available, or after the RadioAudit has been installed using either Apps Control Panel or RadioAudit Client.

7.4.1 ACP Licence Management

The RadioAudit licence can be managed with the ACP by going to the Licence tab under RadioAudit.

The ACP licence page displays the following information:

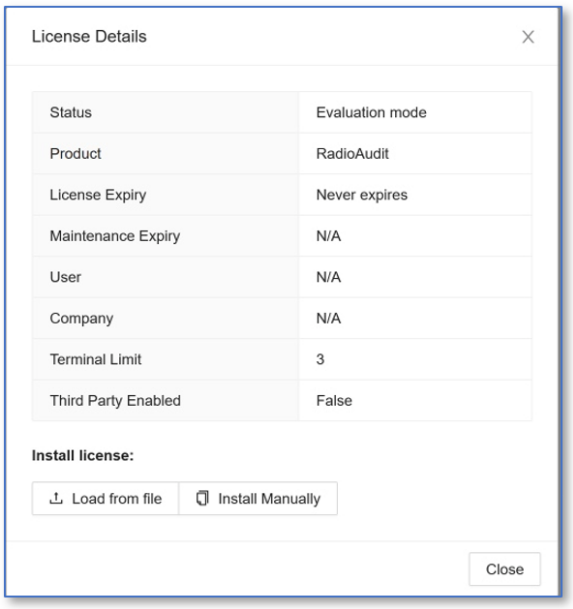
- **Valid**: This displays the details of the validity of the licence. The possible options are:
  - > **Evaluation Mode**: This is the default displayed when the RadioAudit system does not have any licence. In this mode the maximum terminals that can be added into the RadioAudit system is restricted to three.
  - > **Licence Expired** (Evaluation mode): This is displayed when the valid licence has expired. RadioAudit reverts to Evaluation Mode.
  - > **Licence Valid**: This is displayed when the licence is valid.
  - > **Licence Invalid** (Evaluation mode): This is displayed when the licence details entered are not a valid licence. RadioAudit reverts to Evaluation Mode.
  - > **Mismatch Hardware ID**: This is displayed when a licence that has the incorrect Hardware ID is entered into the system. RadioAudit reverts to Evaluation Mode.
- **User**: This is the licence holder’s name.
- **Company**: This is the licence holder company name.
- **Expiration date**: This displays the date when the licence will expire or in the case of a perpetual licence it will display “Never Expires”.
- **Maintenance expiration date**: This displays the date when the maintenance period expires. Typically, this is 356 days from the creation of the licence.
- **Max terminals**: This displays how many terminals can be configured in the RadioAudit system with the installed licence.
- **RadioAudit Remote API**: This displays whether the licence has remote API enabled or not.
- **Hardware ID**: This displays the Hardware ID of the target computer. This ID is required when requesting a licence from Sepura.

Finally, the dialog has the **Update licence** drop box. This is where the provided licence key is pasted.

When a valid Licence key has been pasted into the drop box, select **Install licence**. The ACP will refresh the page to automatically display the updated licence status.

7.4.2 RadioAudit Client Licence Management

The licensing status can also be checked from the RadioAudit client toolbar. The RadioAudit licence is checked by selecting **Valid licence** from the toolbar. The following dialog is opened:



The licence can be added in two ways.

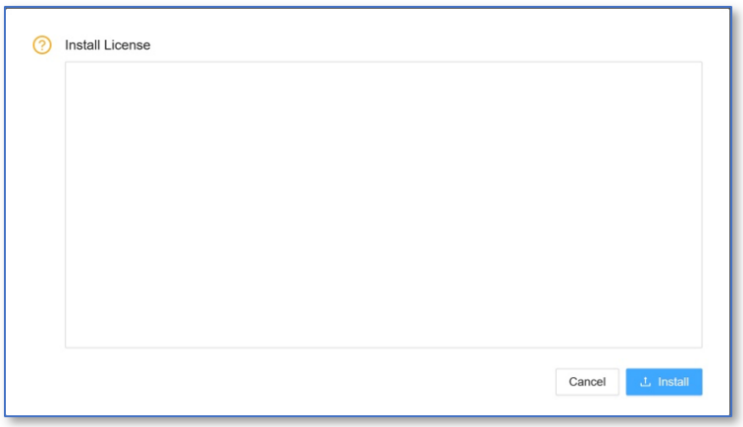
- Importing a licence key file
- Pasting in the licence key details

Importing Licence File

The licence file can be imported by selecting **Load from file**. Select the licence file from the File Explorer and select Open. The imported licence will refresh the RadioAudit Client to automatically display the updated licence status.

Install Licence Manually

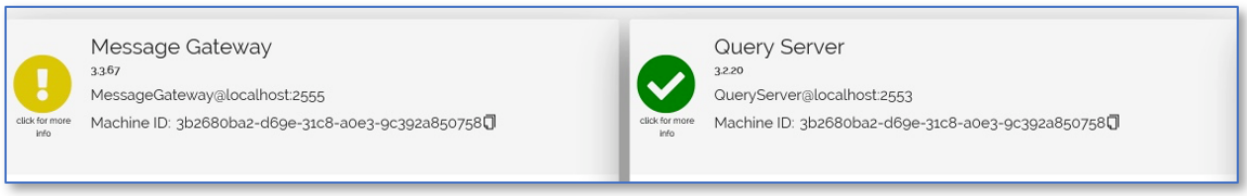
Install the licence manually by selecting **Install Manually**. The following dialog is opened:



Paste the licence key into the dialog and select Install. The entered licence will refresh the RadioAudit Client to automatically display the updated licence status.

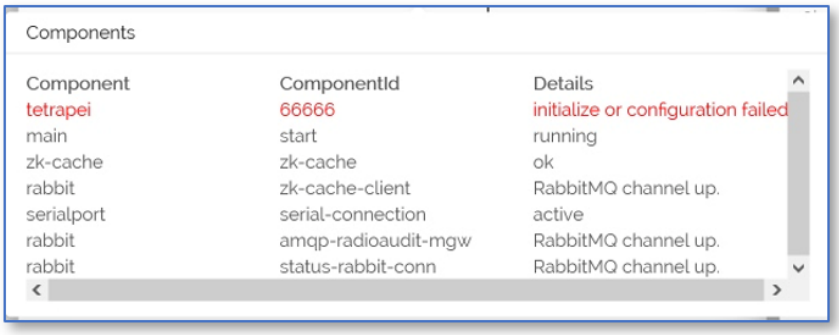
8.0 Troubleshooting

The following section explains the most common faults and the actions needed to fix the fault. The ACP status view shows the most imminent issues.



The Icon colour and contents give immediate feedback of the system service status.

In the above example the Query is working correctly, but the Message Gateway has some issues that needs closer investigation. This is done by selecting the exclamation mark icon. A pop-up window opens which shows details of the fault:



In the above example the TETRA PEI connection has some issues which need closer investigation. The issue could be any of the following:

Issue	Solution
USB cable detached from either the PC or the terminal.	Reconnect the USB cable
The terminal is powered off	Power the terminal on
The power cable is disconnected from the terminal	Reconnect the power cable

8.1 RadioAudit Faults

The following table contains the most common RadioAudit faults:

Fault	Remedy
ACP login window does not appear	Check that Apps Control Panel service is running. Restart ACP service if its status is not running.
ACP user cannot log on	Check that the username and password are correct. Check that Sepura RadioAudit system services are running . Restart any service if its status is not running. See section 7.3.1
RadioAudit server reboot required	It is imperative to check after the server is up and running that the Sepura RadioAudit services are running. Restart any service if its status is not running. See section 7.3.1
RadioAudit not working correctly	Check the RadioAudit installation as detailed in section 7.3. If necessary, repair the installation.

For further assistance with RadioAudit faults, contact Sepura Customer Support.

www.linkedin.com/sepura

www.facebook.com/sepuraplc

@sepuraplc

www.instagram.com/sepuraplc

www.youtube.com/sepuraplc

Contact Details

Sepura Limited.
9000 Cambridge Research Park
Beach Drive, Waterbeach
CAMBRIDGE
CB25 9TL. UK

www.sepura.com