

# Liberator 4.5

---

## Server-side RTTP Logging

April 2009

## Contents

<b>1</b>	<b>Preface .....</b>	<b>1</b>
1.1	What this document contains .....	1
	About Caplin document formats .....	1
1.2	Who should read this document .....	1
1.3	Related documents .....	1
1.4	Typographical conventions .....	2
1.5	Feedback .....	2
1.6	Acknowledgments .....	2
<b>2</b>	<b>Introduction to server-side RTTP logging .....</b>	<b>3</b>
<b>3</b>	<b>Defining the RTTP log file names .....</b>	<b>4</b>
<b>4</b>	<b>Configuring user RTTP logging using the EMC .....</b>	<b>5</b>
4.1	To enable single-session RTTP logging for a logged-in Liberator user .....	6
4.2	To disable single-session RTTP logging for a logged-in Liberator user .....	8
4.3	To enable permanent session logging for a logged-in Liberator user .....	9
4.4	To disable permanent session logging for a logged-in Liberator user .....	12
4.5	To enable permanent RTTP session logging for any Liberator user .....	13
4.6	To disable permanent RTTP session logging for any Liberator user .....	16
<b>5</b>	<b>Configuring User RTTP Logging from the Liberator .....</b>	<b>18</b>
<b>6</b>	<b>Interpreting server-side RTTP Logs .....</b>	<b>19</b>
6.1	Logging start and stop times .....	19
6.2	Separation of log traffic in log files .....	19
6.3	RTTP traffic log format .....	19
	Example 1 – RTTP type 5 connection .....	20
	Example 2 – RTTP type 2 connection .....	21

# 1 Preface

## 1.1 What this document contains

This document describes the server-side logging of RTTP messages between the Liberator and a client communicating over RTTP.

### About Caplin document formats

This document is supplied in Portable document format (*.PDF* file), which you can read on-line using a suitable PDF reader such as Adobe Reader®. The document is formatted as a printable manual; you can print it from the PDF reader.

## 1.2 Who should read this document

This document is intended for system administrators, testers, and developers.

## 1.3 Related documents

[1] **Liberator Administration Guide**

Contains instructions on how to install and configure Caplin Liberator.

## 1.4 Typographical conventions

The following typographical conventions are used to identify particular elements within the text.

<b>Type</b>	<b>Uses</b>
<i>/AFolder/Afile.txt</i>	File names, folders and directories
Some text in a dialog box	Dialog box output
Something typed in	User input – things you type at the computer keyboard
<b>rttp-log</b>	Configuration item name
<b>XYZ Product Overview</b>	Document name
◆	Information bullet point
■	Action bullet point – an action you should perform

**Note:** Important Notes are enclosed within a box like this.  
Please pay particular attention to these points to ensure proper configuration and operation of the solution.

**Tip:** Useful information is enclosed within a box like this.  
Use these points to find out where to get more help on a topic.

## 1.5 Feedback

Customer feedback can only improve the quality of our product documentation, and we would welcome any comments, criticisms or suggestions you may have regarding this document.

Please email your feedback to [documentation@caplin.com](mailto:documentation@caplin.com).

## 1.6 Acknowledgments

*Adobe Reader* is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries.

## 2 Introduction to server-side RTTP logging

The server-side RTTP logging feature allows you to record conversations between a Liberator and its users. The logging feature is enabled for individual users, and produces a continuously updated log file for every new session between the Liberator and the user.

**Note:** It is recommended that in a live system you only turn on RTTP traffic logging for troubleshooting purposes.

To set up RTTP logging, configure Liberator to log the RTTP protocol traffic between clients and the Liberator. To do this:

1. Define the naming convention for the log files.
  - See section 3 “Defining the RTTP log file names” on page 4.
2. Specify a list of user names (Liberator login names) whose RTTP traffic is to be logged.

You can do this in two ways:

- Through Liberator configuration, as detailed in section 5 (page 18).
- or
- If JMX monitoring is enabled for the Liberator, dynamically through the Users or Logs tab on the Enterprise Management Console (EMC), as explained in section 4 on page 5.

**Tip:** By default, the RTTP log files are generated in Liberator’s *var/rttp* directory.

**Note:** If you configure Liberator to write its log files to a directory other than the default *var* directory, make sure that you create within the new log directory a subdirectory to receive the server-side RTTP log files. The default name for this subdirectory is *rttp*, but you can change it through the definition of the RTTP log file names – see section 3 on page 4.

### 3 Defining the RTTP log file names

Define the names of the traffic log files by setting the **rttp-log** entry of the Liberator Configuration file *rttpd.conf*.

**Example:**

```
rttp-log rttp/RTTP_TRAFFIC_%l.%i
```

%l is the user name and %i is the RTTP session id. So in this case the name of the RTTP traffic log for user JSmith's session would typically be *rttp/RTTP\_TRAFFIC\_JSmith.0x-ab-9*

It is strongly recommended that the name of the RTTP traffic log file contains at least the user name and RTTP session id markers (%l and %i), so that a separate log file is generated for each session for each user who has RTTP logging enabled. If these markers are absent, the log entries for all RTTP sessions will be mixed together in the same file, making it difficult to determine which messages came from which sessions and users.

For reference information on the **rttp-log** Liberator configuration entry, see the **Liberator Administration Guide**.

## 4 Configuring user RTTP logging using the EMC

The Enterprise Management Console's Session tab allows you to switch RTTP traffic logging on and off for individual users.

### ◆ **Single-session logging**

You can immediately log the RTTP traffic for a user who is currently logged in to Liberator. This logs the traffic just for that session until the user logs out or you disable logging.

See "To enable single-session RTTP logging for a logged-in Liberator user" on page 6.

### ◆ **Permanent logging**

You can enable permanent logging for a user. This logs the user's RTTP traffic from the next time the user logs in to Liberator, and for all subsequent sessions until you disable logging. You can enable this type of logging either for a currently logged-in user, via the Users tab of the EMC, or by entering the user's login name on the EMC's Logs tab.

See "To enable permanent session logging for a logged-in Liberator user" on page 9, and "To enable permanent RTTP session logging for any Liberator user" on page 13.

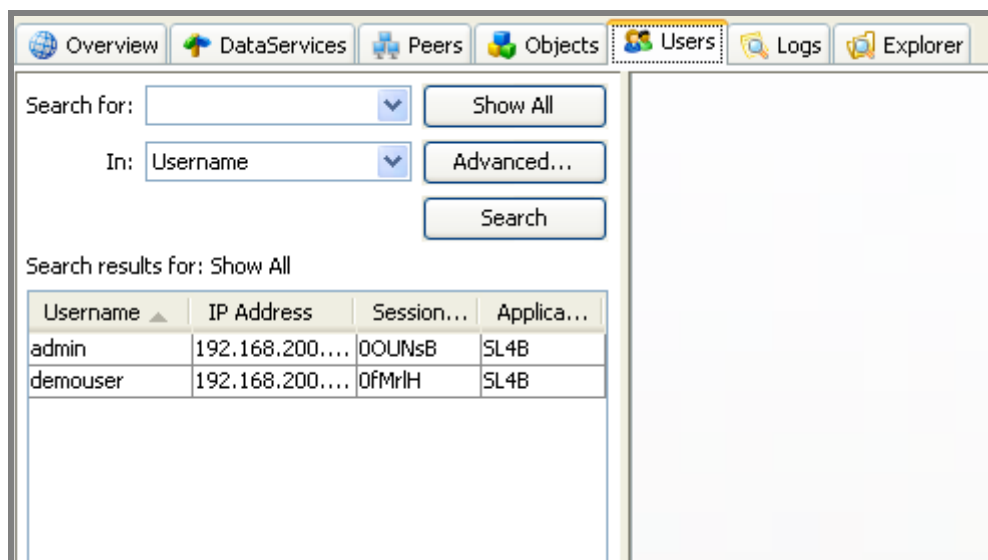
## 4.1 To enable single-session RTTP logging for a logged-in Liberator user

This feature allows you to immediately start logging RTTP traffic for a user who is logged in to Liberator. The traffic is logged until

- ◆ the user logs out,
- ◆ or you disable temporary logging for the user  
(see “To disable single-session RTTP logging for a logged-in Liberator user” on page 8),
- ◆ or the Liberator is restarted.

Once the user has logged out, session logging is *not* automatically enabled when they next log in again.

- Within the EMC, navigate to the Users tab. From here you can see a list of all of the users who are currently logged in to the Liberator (Figure 1).



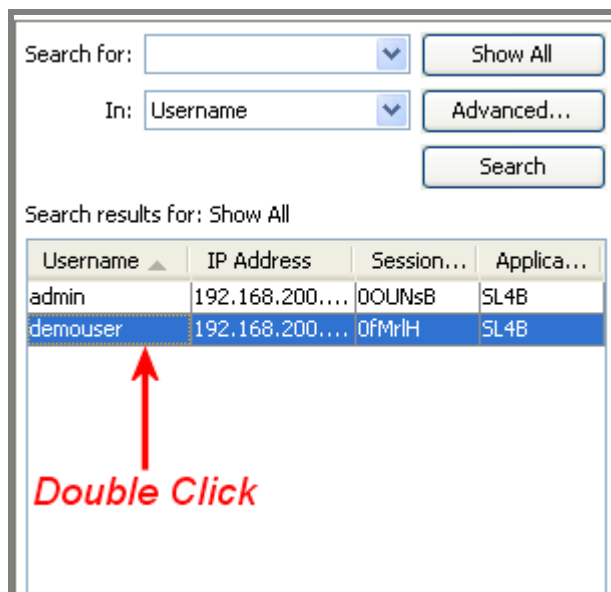
The screenshot shows the EMC interface with the 'Users' tab selected. The interface includes a search bar with a dropdown menu, a 'Show All' button, and an 'Advanced...' button. Below the search bar, there is a table titled 'Search results for: Show All' with columns for Username, IP Address, Session..., and Applica... The table lists two users: 'admin' and 'demouser'. The 'admin' user has an IP address of 192.168.200... and a session ID of 00UNsB. The 'demouser' user has an IP address of 192.168.200... and a session ID of 0fMrIH. Both users are using the SL4B application.

Username	IP Address	Session...	Applica...
admin	192.168.200...	00UNsB	SL4B
demouser	192.168.200...	0fMrIH	SL4B

Figure 1 – List of logged-in users on EMC Users tab

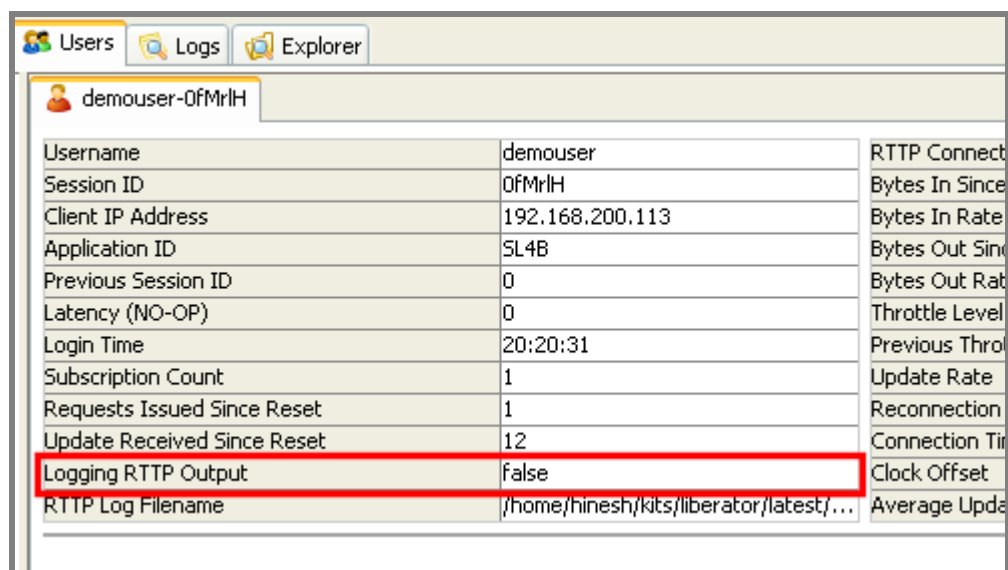


- *Double click* on the user for whom you wish to start server side RTTP logging (Figure 2).



**Figure 2 – Selecting a user on EMC Users tab**

When the specific user's tab opens up, you will see that their Logging RTTP Output field is set to false (Figure 3).



**Figure 3 – RTTP logging status for selected user**

- To begin logging the user's RTTP traffic, click on the 'Start RTTP logging' button.  
The Logging RTTP Output field changes to true, and logging starts (Figure 4).

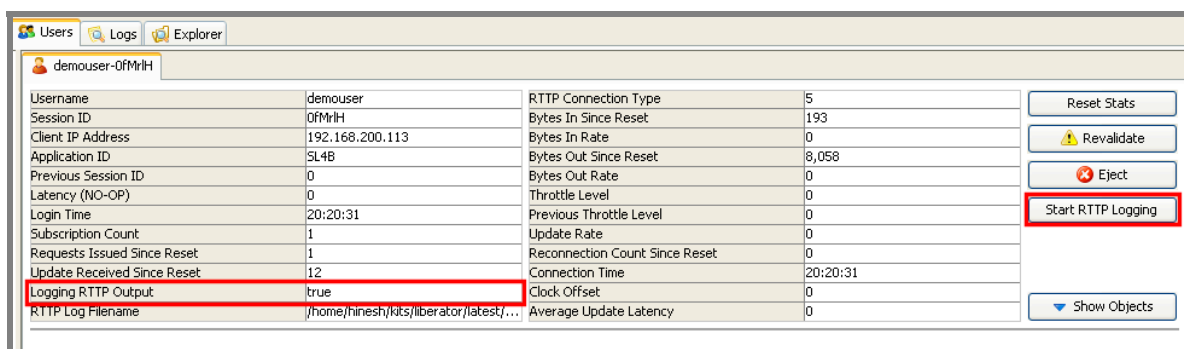


Figure 4 – Enabling single-session RTTP logging for a selected user

## 4.2 To disable single-session RTTP logging for a logged-in Liberator user

- Within the EMC, navigate to the Users tab and *double click* on the user for whom you wish to stop server side RTTP logging.  
(See “To enable single-session RTTP logging for a logged-in Liberator user” on page6.)
- When the specific user's tab opens up, click on the 'Stop RTTP logging' button.

The Logging RTTP Output field changes to false, and logging stops (Figure 5).

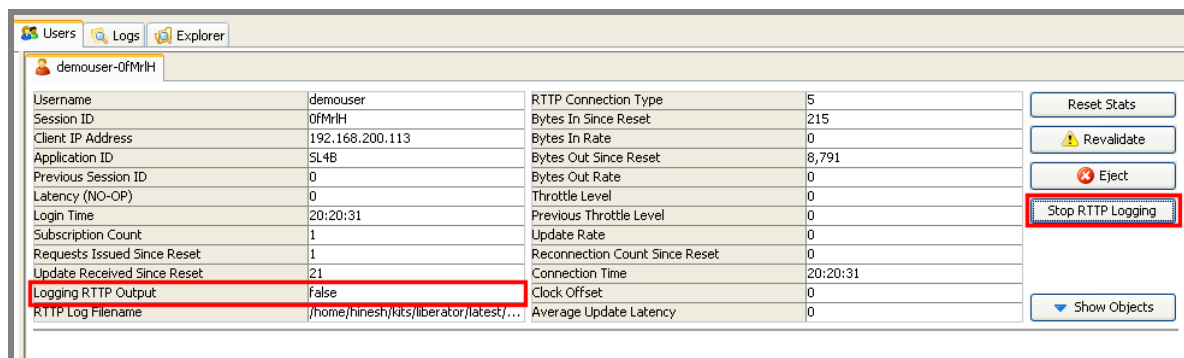


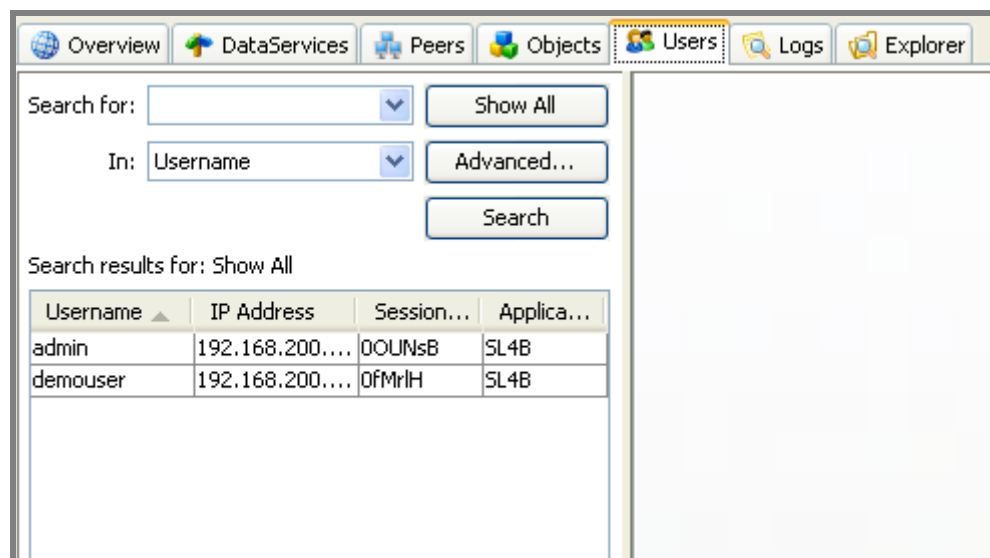
Figure 5– Disabling single-session RTTP logging for a selected user

### 4.3 To enable permanent session logging for a logged-in Liberator user

This feature allows you to permanently enable RTTP logging for a user who is currently logged in to Liberator. Logging of the user's RTTP traffic will start when the user next logs in to the Liberator – the user's current session is not logged. Subsequently, every time the user logs in to Liberator their RTTP traffic is logged. Logging remains enabled until either the Liberator is restarted, or you explicitly disable logging for that user (see "To disable permanent session logging for a logged-in Liberator" on page 12 and "To disable permanent RTTP session logging for any Liberator user" on page 16).

**Note:** Use this EMC facility with caution in live systems, as it enables RTTP logging for all the user's subsequent sessions, until you turn the logging off or the Liberator is restarted. If RTTP logging is enabled for many users, it can adversely affect performance.

- Within the EMC, navigate to the Users tab. From here you can see a list of all of the users who are currently logged in to the Liberator (Figure 6).



The screenshot shows the EMC interface with the 'Users' tab selected. It features a search bar with a dropdown menu, a 'Show All' button, and an 'Advanced...' button. Below the search bar, there is a 'Search' button. The search results are displayed in a table with columns: Username, IP Address, Session..., and Applica... (Application). The table lists two users: 'admin' and 'demouser', both with IP addresses starting with '192.168.200...' and sessions labeled 'OOUNsB' and 'OfMrIH' respectively, both using 'SL4B' application.

Username	IP Address	Session...	Applica...
admin	192.168.200....	OOUNsB	SL4B
demouser	192.168.200....	OfMrIH	SL4B

Figure 6 – List of logged-in users on EMC Users tab

- *Right click* on the row detailing the selected user (Figure 7).

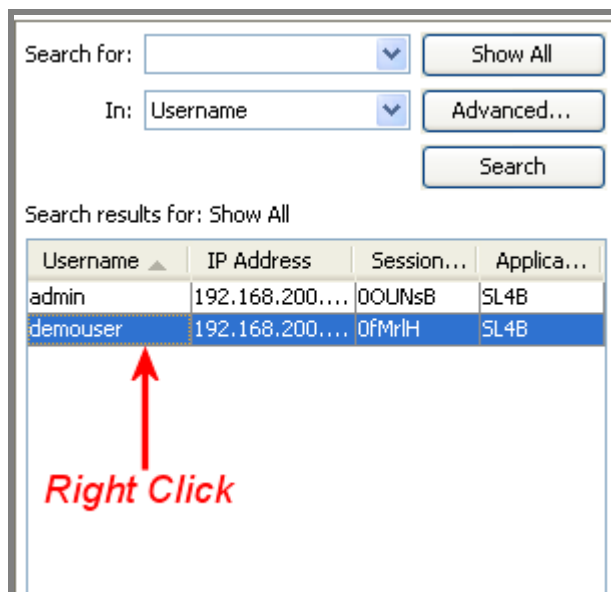
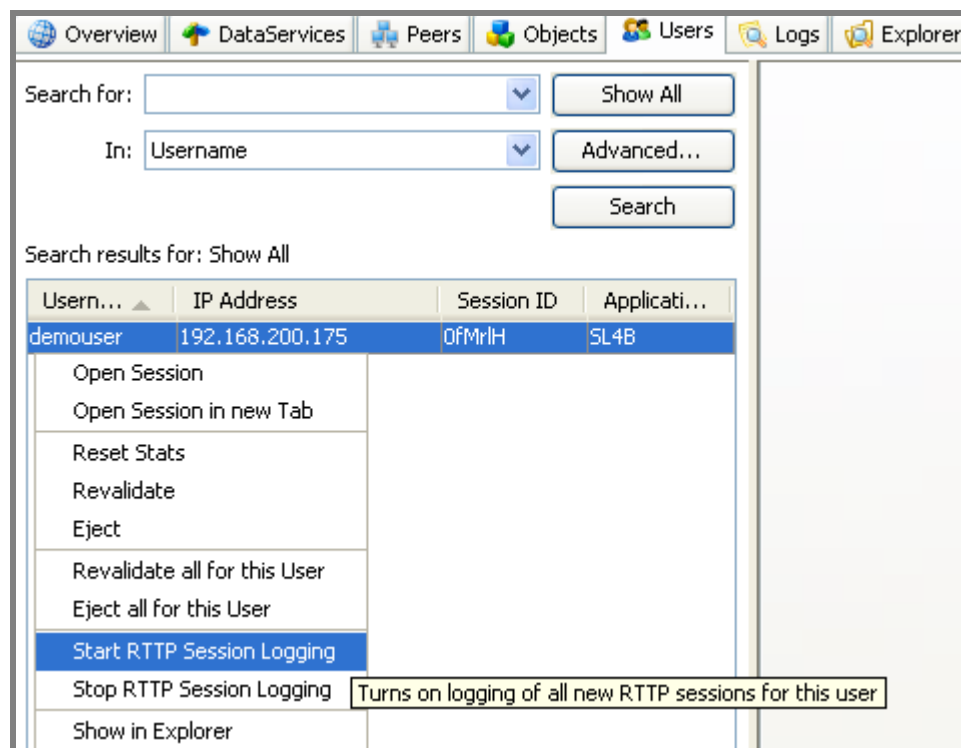


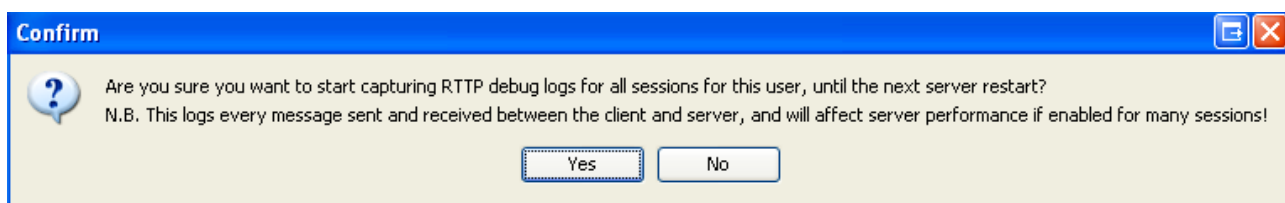
Figure 7 – Selecting a user on EMC Users tab

- From the pop-up menu that appears, select the option Start RTTP Session Logging (Figure 8).



**Figure 8 – Enabling permanent RTTP Logging for a logged in user**

- Click Yes on the dialog box that pops up.



#### 4.4 To disable permanent session logging for a logged-in Liberator user

- Within the Users tab, *right click* on the row detailing the user and select the option Stop RTP Session Logging (Figure 9).

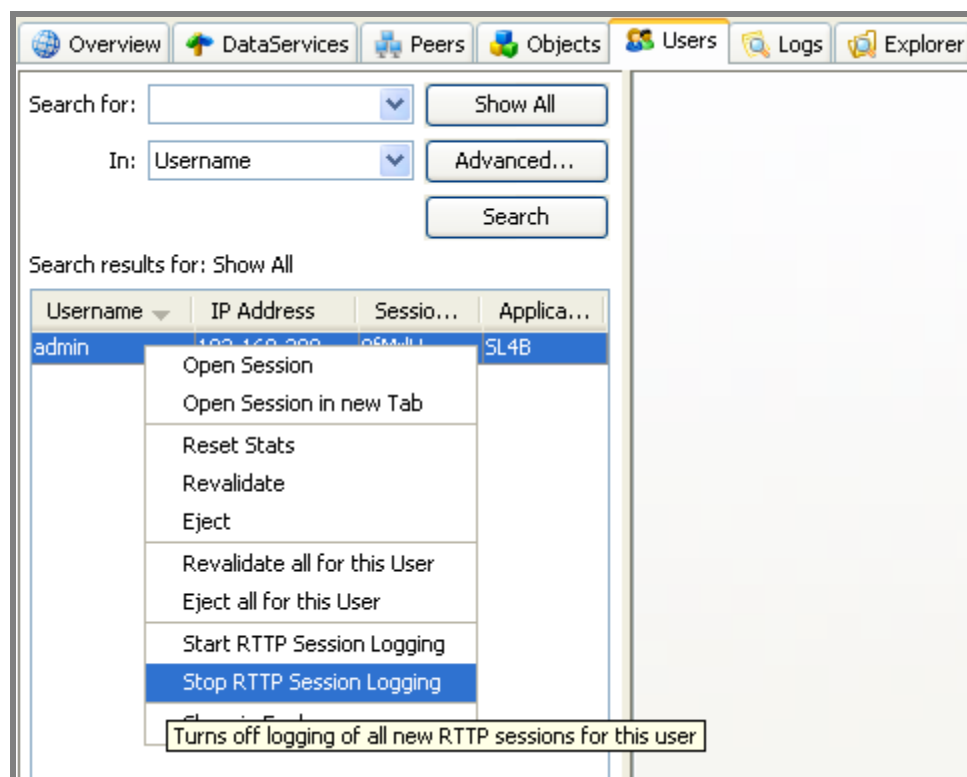
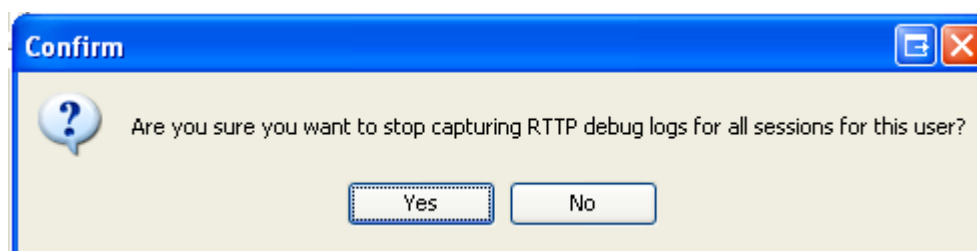


Figure 9 – Disabling permanent RTP Logging for a logged in user

- Click Yes on the dialog box that pops up.



## 4.5 To enable permanent RTTP session logging for any Liberator user

This feature allows you to permanently enable RTTP logging for a user, even if they are not currently logged in to the Liberator. Logging of the user's RTTP traffic will start when the user next logs in to the Liberator – the user's current session is not logged. Subsequently, every time the user logs in to Liberator, their RTTP traffic is logged. This continues until either the Liberator is restarted, or you explicitly disable logging for that user (see "To disable permanent session logging for a logged-in Liberator user" on page 12 and "To disable permanent RTTP session logging for any Liberator user" on page 16).

**Note:** Use this EMC facility with caution in live systems, as it enables RTTP logging for all the user's subsequent sessions, until you turn the logging off or the Liberator is restarted. If RTTP logging is enabled for many users, it can adversely affect performance.

- Go to the Logs tab and enter the name of the user in the box headed 'Log Sessions For Another User'.  
The user name must be a valid Liberator login name.
- Click the Add button (Figure 10 on page 14).

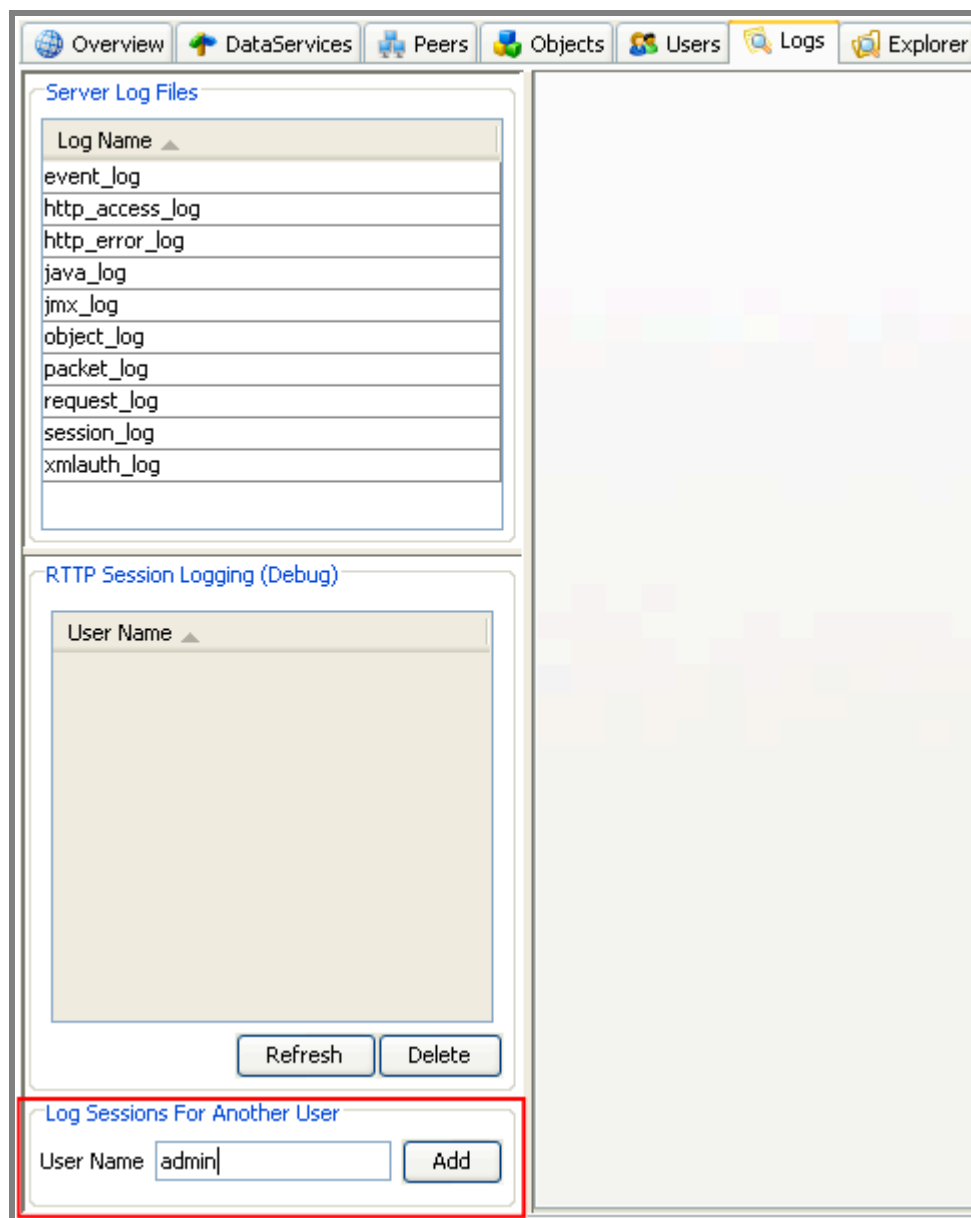
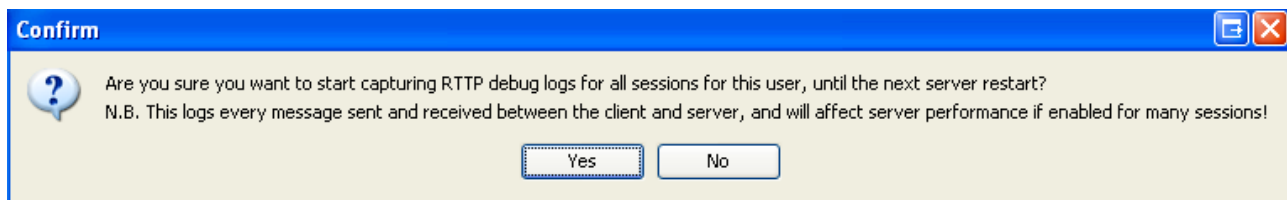


Figure 10 – Enabling RTTP session logging for a named user



- Click Yes on the dialog box that pops up.



## 4.6 To disable permanent RTTP session logging for any Liberator user

- Go to the Logs tab and select the required user from the list headed 'RTTP Session Logging (Debug)'.
- Click the Delete button (Figure 11).

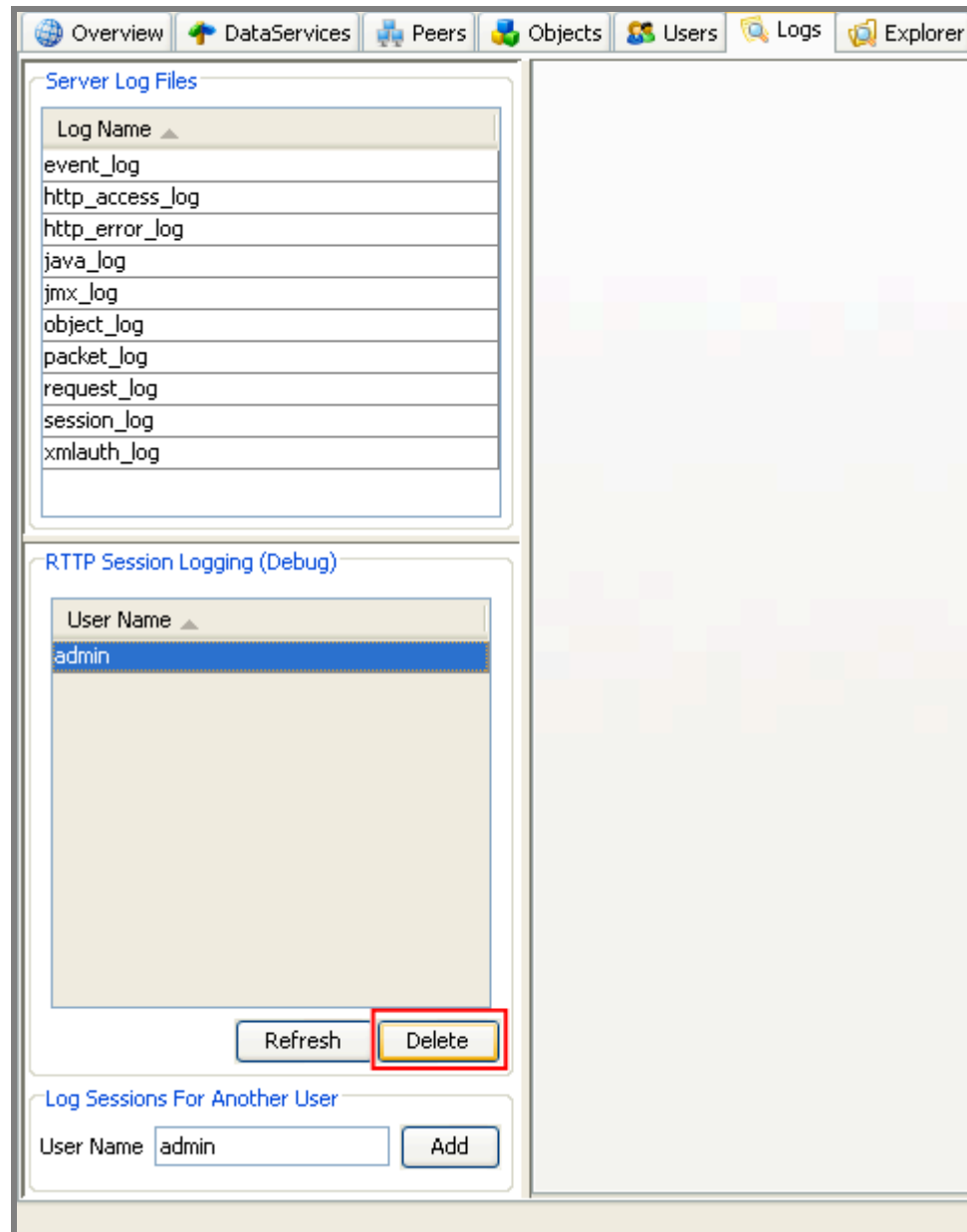
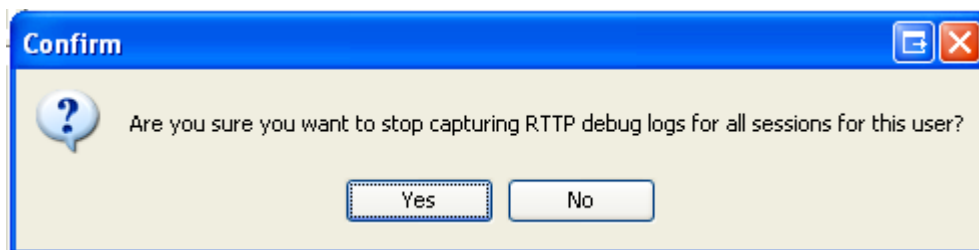


Figure 11 – Disabling RTTP session logging for a named user

- Click Yes on the dialog box that pops up.



## 5 Configuring User RTTP Logging from the Liberator

You can turn on traffic logging for individual users by setting the Liberator configuration entry **rttp-log-users** in the Liberator configuration file (*rttpd.conf*).

**Note:** This option should only be used for debugging test installations. It permanently enables traffic logging for the specified users; the users' traffic will be logged even after Liberator is restarted. Logging can only be turned off by stopping the Liberator and changing the **rttp-log-users** configuration option. In a live system you should normally turn RTTP logging on and off using the Enterprise Management Console (see section 4 on page 5).

If the **rttp-log-users** configuration entry is absent or empty, only RTTP traffic logs that have been specified using the Enterprise Management Console will be generated

The user names can be defined as a space separated list, or as individual entries, or a combination of the two.

**Examples:**

```
rttp-log-users Alf Bill Carl
```

or

```
rttp-log-users Alf
```

```
rttp-log-users Bill
```

```
rttp-log-users Carl
```

**Note:** To ensure the RTTP session logs are created, check that the Liberator's log directory contains a directory called *rttp* – see the note in section 2 on page 3.

For reference information on **rttp-log-users**, see the **Liberator Administration Guide**.

## 6 Interpreting server-side RTTP Logs

### 6.1 Logging start and stop times

You can see exactly when you started or stopped logging RTTP traffic for a particular user from the following log lines within the RTTP log:

```
### 04 Mar 20:42:33.89 STARTING  
...  
### 04 Mar 20:42:39.63 STOPPING
```

### 6.2 Separation of log traffic in log files

The default log file naming convention causes an RTTP traffic log file to be generated for each combination of user and RTTP session, so if a user has more than one session established concurrently, you can easily analyze the traffic for the individual sessions.

### 6.3 RTTP traffic log format

RTTP traffic log entries have the format:

```
>>>TIMESTAMP  
<RTTP message as text>  
or  
<<<TIMESTAMP  
<RTTP message as text>
```

where:

- ◆ >>> indicates that the RTTP message has been sent from the Liberator to the client
- ◆ <<< indicates that the RTTP message has been sent to the Liberator from the client
- ◆ **TIMESTAMP** has the format **dd\_mon hh:mm:ss.ss** (for example 23\_Aug 15:22:14.07)

## Example 1 – RTTP type 5 connection

The following log is for an RTTP type 5 (Streaming JavaScript) connection, established using StreamLink for Browsers on the client. It shows a "NOOP+OK" being sent by a Liberator. During periods of inactivity, clients regularly send "NOOP" messages to the server. The server responds by sending "NOOP+OK" messages back to clients (if the server is available). This is reminiscent of 'pinging' a server, and receiving "reply" messages back indicating that the server is up and running.

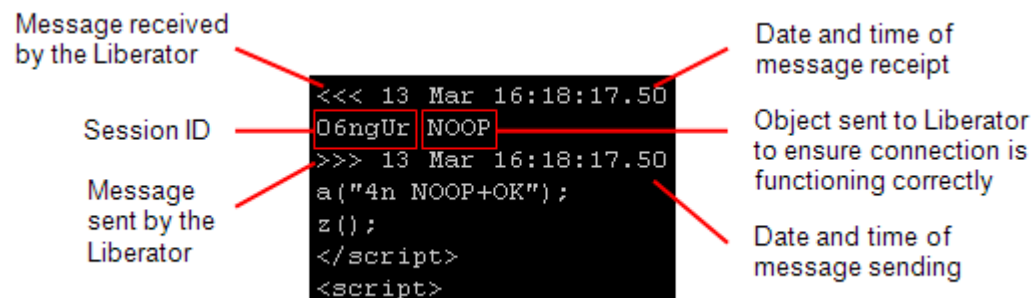


Figure 12 – Sample Log for an RTTP type 5 connection

## Example 2 – RTTP type 2 connection

The following log is for an RTTP type 2 (HTTP Tunneled) connection, established using StreamLink for Java on the client. The client has requested one object from the Liberator – “/DEMO/MSFT”

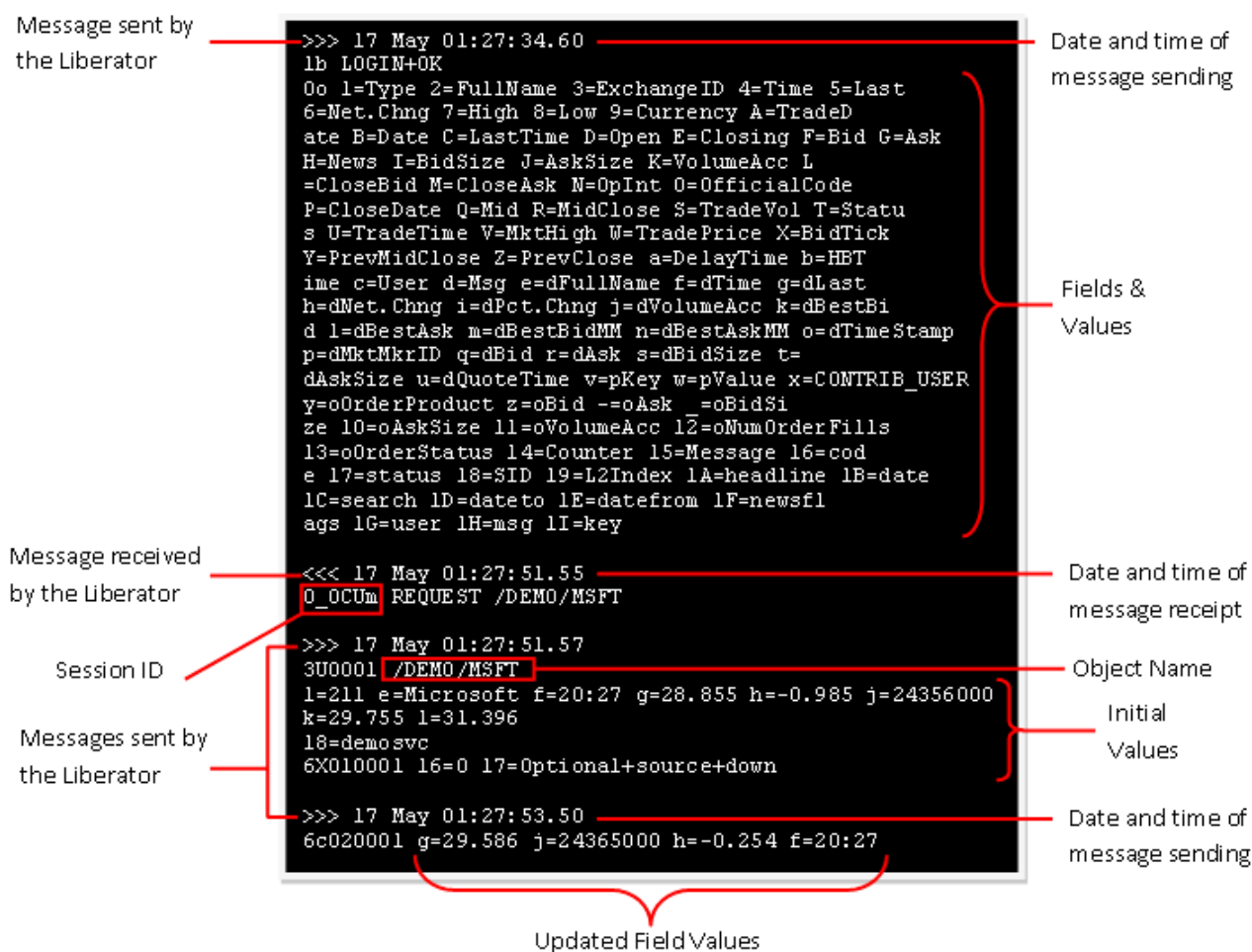


Figure 13 – Sample Log for an RTTP type 2 connection

## Contact Us

Caplin Systems Ltd

Triton Court

14 Finsbury Square

London EC2A 1BR

Telephone: +44 20 7826 9600

Fax: +44 20 7826 9610

[www.caplin.com](http://www.caplin.com)

The information contained in this publication is subject to UK, US and international copyright laws and treaties and all rights are reserved. No part of this publication may be reproduced or transmitted in any form or by any means without the written authorization of an Officer of Caplin Systems Limited.

Various Caplin technologies described in this document are the subject of patent applications. All trademarks, company names, logos and service marks/names ("Marks") displayed in this publication are the property of Caplin or other third parties and may be registered trademarks. You are not permitted to use any Mark without the prior written consent of Caplin or the owner of that Mark.

This publication is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, warranties of merchantability, fitness for a particular purpose, or non-infringement.

This publication could include technical inaccuracies or typographical errors and is subject to change without notice. Changes are periodically added to the information herein; these changes will be incorporated in new editions of this publication. Caplin Systems Limited may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

This publication may contain links to third-party web sites; Caplin Systems Limited is not responsible for the content of such sites.