Red Box
release 3

Red Box Web Interface

Installation and Administration

Red Box Web Interface Administration and Installation Guide.
M0087/1, Edition 1.5, May 2000. Red Box release 3.

Copyright notice

About this guide

This guide gives the installation and administration procedures for the Red Box web interface running on a Red Box release 3 system. The web interface includes on-line documentation which describes how to use its facilities for creating, viewing and amending selected Red Box records.

This guide contains the following chapters:

Chapter 1 introduces the Red Box web interface, and describes its requirements.

Chapter 2 gives step by step instructions on installing the Red Box web interface, including upgrading Red Box release 3 and installing the webserver.

Chapter 3 gives procedures for running the web interface, and for web interface administration.

Chapter 4 describes how to license Red Box for the web interface and set up Red Box web users.

Chapters 5 and **6** describe how to prepare for incident and RFC creation via the web interface.

Chapter 7 describes web interface administration.

Chapter 8 describes the web interface scripts.

Glossary

Terms used in this guide have the following meanings:

Glossary of terms

Term	Meaning
Cartridge process	A process created and run by the webserver. The web interface uses cartridge processes to connect to the Red Box database.
OWAS	Oracle Web Application Server. The Oracle product which the Red Box web interface uses as its webserver.
SQL*Net	Oracle's remote data access messaging software, based on TNS.
TNS	The Oracle Transparent Network Substrate technology for communications across networks.
TNS listener	A process that allows network access to the Red Box service.
Webserver	A system component that passes that handles requests from web browsers (see OWAS).
Web updater	A component of the Red Box web interface that implements updates to the Red Box database.

Conventions

This guide uses:

- Bold typeface for values such as command names to be entered on your keyboard. For example, **ucrbstart**.
- Italics for variables that you will replace with actual values. For example, ***service-name***.

Technical support

Make sure that you have as much information as possible to hand before contacting support.

Support contact information

General enquiries	**Ultracomp Support Centre**
Ultracomp Limited Ultracomp House Pinehill Road Crowthorne Berkshire RG45 7JD.	**Tel:** +44 (0) 118 973 3456 **Email:** support@ultracomp.co.uk **Internet:** http://www.ultracomp.co.uk

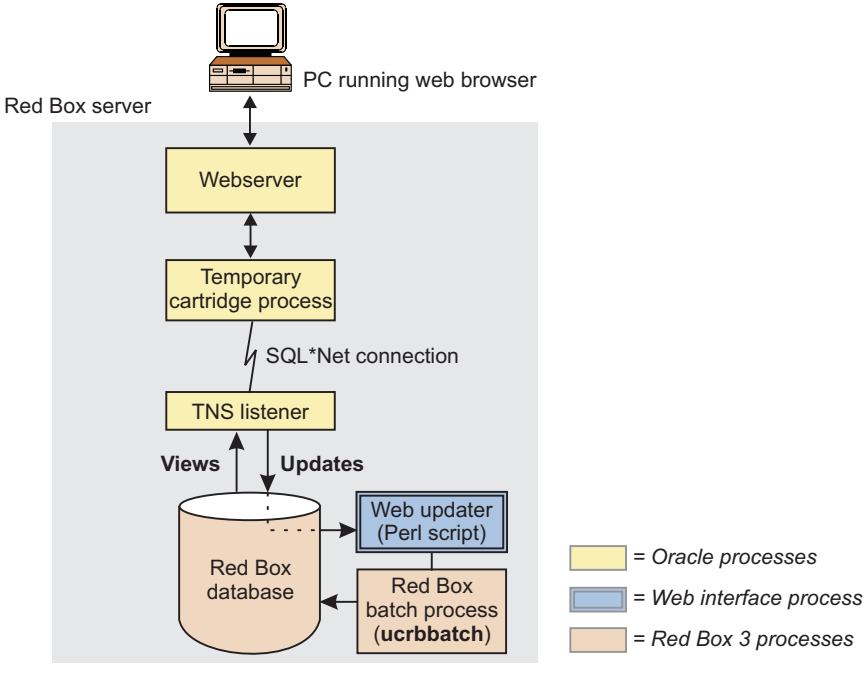
CONTENTS

INTRODUCTION

The Red Box web interface provides access to a subset of Red Box records via a PC web browser. You can use it to:

- Browse the Red Box database for existing incident reports and RFCs (Requests For Change).
- Create new incident reports and RFCs and carry out limited maintenance. For example, you can add symptoms to an incident, and resolve or withdraw it.
- Carry out web interface administration.

Figure 1.1 Main components of the web interface



1.1 Summary of web processing

When a user accesses Red Box via the web interface, their web browser passes requests to the Oracle **webserver**. The webserver analyses each request, and if it needs to access the Red Box database uses a **temporary cartridge process**. The cartridge process uses Oracle's messaging software, **SQL*Net**, to connect to the **TNS listener** of the Red Box service.

Within the **Red Box database**, each web request is analysed further as a procedure call. If the purpose of the call is only to view Red Box records, the procedure passes information back to the web browser for display.

If database updates are required, the procedure writes information to a communication area in the database, which is read by a **web updater** process. The web updater calls the Red Box batch process, **ucrbbatch**, which performs the required updates and reports the results back to the database procedure. The procedure passes information back to the web browser as for normal viewing.

The web interface can support any number of concurrent web sessions, although each web connection occupies one reserved Red Box application slot.

1.2 Web interface contents

The Red Box web interface package comprises:

- Two tapes, containing components for **rboxsw** and **owasuser**
- This *Red Box Web Interface Installation and Administration* guide.

1.3 Web interface requirements

The web interface requires the following PC and Red Box server components.

1.3.1 PC requirements

A PC can establish a Red Box web session using one of the following web browsers:

Table 1.1 Web browser requirements

Browser	Version
Microsoft Internet Explorer	Version 5 or later.
Netscape Navigator	Netscape Navigator is supplied as part of Netscape Communicator, which must be at version 4.6 or later.

PCs do *not* need to have the Red Box PC client installed.

1.3.2 Red Box server requirements

The Red Box web interface is supported on the following Red Box server systems:

- Sun Solaris version 2.5 or 2.6 on SPARC
- HP 9000 Series 700/800 systems running HP-UX version 10.20.

The Red Box server system must have the following software installed:

Table 1.2 Server software requirements

Software	Installation details
Red Box release 3 (Server software and Oracle7).	Installed as described in *Red Box Server Installation (UNIX systems)*.
Webserver (Oracle Web Application Server (OWAS) release 3.0 Standard Edition*).	You must obtain the webserver from Oracle and install it as described in Chapter 2 of this guide. Refer to your Oracle documentation for OWAS hardware and software requirements.
Red Box web interface	Installed as described in Chapter 2.

* The web interface does not use the extra facilities provided in the Advanced or Enterprise editions of OWAS.

Free file system space

The web interface software requires free space in UNIX users and Oracle tablespaces created during Red Box release 3 installation:

- 30 Mb in the UNIX user, **rboxuser**
- 10 Mb in the Oracle tablespace, **system**.

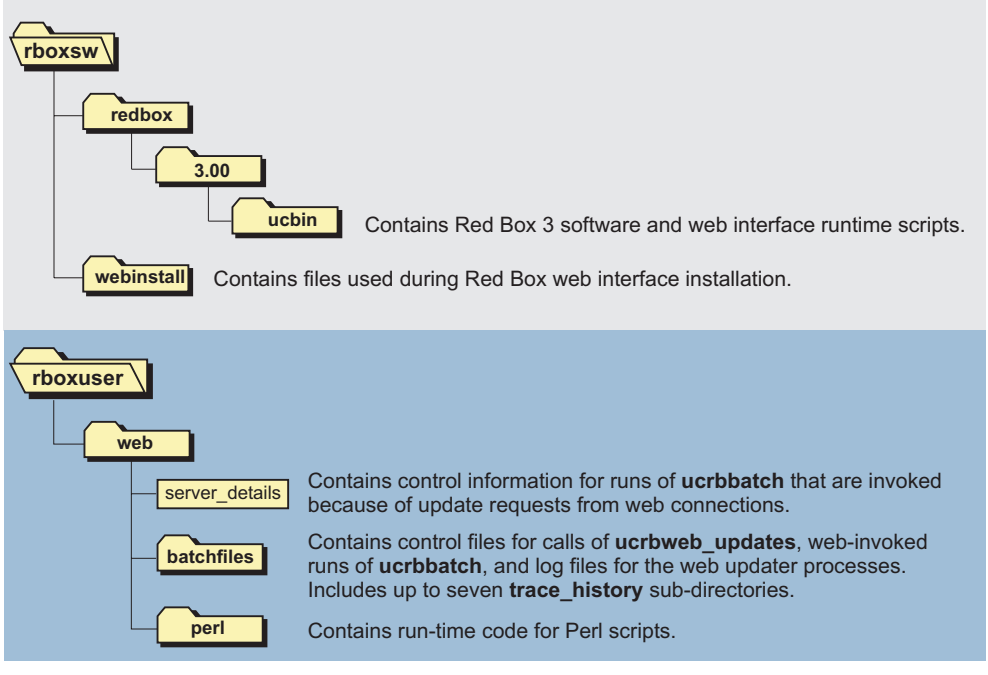
Use the following Red Box database maintenance commands to check the size and current usage of the Oracle7 tablespaces, and to extend them if necessary. For details, see *Red Box Server Administration (UNIX systems)*.

- Use **ucrbspace** to check the size and current usage of the **system** tablespace
- Use **ucrbextend** to add a new data file to the tablespace.

File placement

The web interface software is installed under the Red Box release 3 UNIX users **rboxsw** and **rboxuser**, as shown in the following diagrams.

Figure 1.2 Web interface components



1.4 Planning for the web interface

Before updating your Red Box system for the web interface, consider the following:

Table 1.3 Planning considerations

Maximum number of concurrent web sessions (*max-web-sessions*)
Decide how many web log-ins you wish to allow at the same time. Each logged-in web session requires one reserved Red Box application slot, assigned via the **Web Slots** group created in section 4.2 on page 56.
Minimum and maximum number of cartridge processes (*min/max-cartridges*)
The webserver requires a cartridge process to pass a web request to Red Box. Cartridge processes are re-used by successive requests, regardless of which web session the requests relate to. Therefore, the maximum number of processes you will need is determined by the peak number of requests, not by the number of web sessions. Cartridge processes are created as required up to a maximum number, and idle processes eventually die down to a minimum number. The minimum and maximum numbers are set in the webserver configuration; for details, see Step D: "Set minimum and maximum cartridges value" on page 38. Consult Oracle for detailed recommendations, but a guide might be: • *Minimum value.* There is an overhead for each loaded process, so do not try to match high peak concurrency values. Configure a minimum value of at least one, and try to set it to 60-80% of your peak concurrency, provided this additional use of your system does not entail increasing your swap space usage to more than 75%. • *Maximum value.* Configure a high maximum number if possible. Higher values allow greater concurrency, but impose greater demands on your system.

Maximum number of web updaters (*max-updaters*)
Each database update is managed by the web updater as a single 'thread'. This means that the updater reads a request, runs **ucrbbatch** to perform the update, and waits for the result before reading the next update request. The standard startup procedures for a web-enabled Red Box system load one updater, but you can load additional ones to perform multiple updates concurrently. For details, see section 3.3 on page 54.

The considerations in Table 1.3 above will help you decide how to configure Red Box for the web interface. The following table describes the configuration values, and uses variables in ***italics*** to indicate values taken from Table 1.3. All configuration values are shown on the Red Box Slots screen (see section 4.3 on page 57).

Table 1.4 Configuring Red Box for the web interface

Number of Red Box slots
The **Licensed** field on the Slots screen shows the number of application slots for which your Red Box system is licensed. If the **Available** field contains the same number, all these slots are available to be allocated for Red Box use. In section 4.3 on page 57, you will assign the ***max-web-sessions*** number of reserved slots to the **Web Slots** group. To allocate these slots, either assign spare slots or re-allocate slots that are currently assigned to other groups. Alternatively, you can license additional application slots.
Number of database connections
The **Maximum Database** value on the Slots screen determines the maximum number of Oracle processes that the Red Box server will attempt to start. Each of the following requires an Oracle process to be started by the Red Box server: • Each logged-in PC client session • Each read-only views session

- Each operations control manager session
- Each run of **ucrbbatch**.

For the web interface, the **Maximum Database** value must include the ***max-updaters*** value. This will allow for the **ucrbbatch** processes invoked by web updaters.

Number of client connections

The **Maximum Client** value on the Slots screen determines the maximum number of Red Box client sessions that Red Box will accept. Each of the following requires a client session:

- Each PC client session, whether logging in, logged in or suspended
- Each operations control manager session
- Each run of **ucrbbatch**.

For the web interface, the **Maximum Client** value must include the ***max-updaters*** value. This will allow for the **ucrbbatch** processes invoked by web updaters.

Number of Oracle processes

The **Oracle Processes** value on the Slots screen is eight less than the maximum number of Oracle database processes that the Oracle system will allow (Red Box needs eight for its own processes). Each of the following requires an Oracle process:

- Each logged-in PC client session
- Each read-only views session
- Each operations control manager session
- Each web request
- Each web updater
- Each run of **ucrbbatch**.

For the web interface, the Oracle Processes value must allow:

1) 2 x ***max-web-sessions*** (one for each updater; one for **ucrbbatch** invoked by each updater).
2)The ***max-cartridges*** value. This will allow for web browser connections.

i You cannot increase the Oracle processes value directly on the Slots screen. Instead, you must edit the Oracle initialisation file, as described in the next section.

UNIX kernel parameters

You may need to tune the swap space and kernel parameters configured on your UNIX system to support any increases you have made to the above values.

For details of Red Box server requirements, see the *Red Box Server Installation Guide (UNIX Systems)*.

1.4.1 Editing the Oracle initialisation file

To change the **Oracle Processes** value on the Red Box Slots screen, you must edit the Oracle initialisation file.

1) Log in as **rboxsw**.
2) Amend the file:

   $RBOX_ADMIN/pfile/initucrb.ora
3) Edit the value of *nn* in the line:

   processes = *nn*

   where *nn* = 8 + the **Maximum Database** value required on the Slots screen.
4) Exit from **rboxsw**.

The new process count will be effective the next time the Red Box database is started.

i You should arrange to test the restart, because the additional semaphores and global memory may not be provided by your UNIX kernel settings, and you may, for example, need to edit your UNIX kernel parameters and swap space. Carry out the test when Red Box access is not required, but the machine is running its full load of other applications.

If you need advice on checking the current settings of your UNIX kernel or on modifying the values and rebuilding the kernel, contact the Ultracomp Support Centre.

INSTALLING THE WEB INTERFACE

The procedures to install the Red Box web interface are:

- Prepare for installation (section 2.1)
- Upgrade Red Box 3 (section 2.2)
- Install the webserver (section 2.3)
- Configure the webserver (section 2.4)
- Web-enable Red Box 3 (section 2.5)
- Set up automatic startup and shutdown (section 2.6)
- Configure hyperlinks (section 2.7)
- Configure PC web browsers (section 2.8)

2.1 Prepare for installation

Have ready the software and documentation that you will require during installation:

- Red Box web interface issue tapes (1 and 2)
- The Oracle Web Application Server (OWAS) release 3 CD-ROM and *Oracle Installation Guide*.

2.1.1 Passwords and other variable information

The installation instructions use variable names to refer to passwords and other information which you must supply. Table 2.1 lists these variable names in alphabetical order, and describes the information to be supplied. Use the blank right-hand column to write down the values that you will supply for each variable.

Table 2.1 Variables to be supplied during installation

Information required	Variable name	Your value
A password that the OWAS administrator will use for online configuration of the webserver.	***admin-password***	
A TCP (Transmission Control Protocol) port to be used by the webserver Administration Listener. To use the Oracle default, choose **8888**.	***admin-port***	
The directory under **rboxuser** which contains the files **dcmess.tab** and **text.tab**. To locate the directory: 1. Log in as **rboxuser**. 2. Enter **echo $HOME/tools**.	***batch-path***	
The domain name to be used for the IP address of the webserver machine. Normally this is the machine's hostname, for example, **foxweb** If you want to allow several domain names (for example, **foxweb** from local machines but **foxweb.ultracomp.co.uk** from outside), identify each name to be allowed.	***hostname1*** *Optional:* ***hostname2*** ***hostname3*** *... etc.*	

Information required	Variable name	Your value
Value of the environment variable ORACLE_HOME for **rboxsw**. To display the value: 1. Log in as **rboxsw**. 2. Enter **echo $ORACLE_HOME**.	***oracle-home***	
A password that the webserver UNIX username **owasuser** will use.	***owasuser-password***	
The IP address of the Red Box machine, or a name that the webserver machine will resolve to it. Because Red Box and the webserver are in the same machine, ***RB-machine-addr*** is likely to be the same as ***hostname1***.	***RB-machine-addr***	
The value of the environment variable RBOX_ADMIN for **rboxsw**. To display the value, enter **echo $RBOX_ADMIN**.	***rbox-admin***	
Password for the Oracle user **rboxadmin**. This user was created by the Red Box release 3 setup program, with the default password **rboxadmin.**	***rboxadmin-password***	
Value of the environment variable HOME for **rboxsw**. To display the value, enter **echo $HOME**.	***rboxsw-home***	
Port number for the Red Box server software. To find the value, see the **Port=** line in the Red Box configuration file, located in: **$RBOX_HOME/config/redbox.cfg**. The default for Red Box release 3 is **7300**.	***redbox-port***	

Information required	Variable name	Your value
Choose an Oracle service name to be used for SQL*Net access. To use the Ultracomp default, choose **rbox**.	***service-name***	
The value of the environment variable ORACLE_SID for **rboxsw**. To display the value, enter **echo $ORACLE_SID**.	***sid***	
Choose a TCP port to be used for SQL*Net access. To use the Oracle default, choose **1521**.	***sqlnet-port***	
The password for the Oracle user **sys**. This password was supplied to the Red Box release 3 setup program.	***sys-password***	
A UDP (User Datagram Protocol) port for inter-communication by webserver processes. To use the Oracle default, choose **2649**.	***UDP-port***	
A TCP port to be used by the webserver application listener. To use the Oracle default, choose **8889**.	***user-port***	
The absolute name of the home directory that you will give when creating **owasuser** in section 2.3.1 on page 27.	***web-home***	

2.2 Upgrade Red Box 3

This section upgrades Red Box 3 for the web interface.

2.2.1 Close the Red Box service

Before running the upgrade, Red Box (incuding Oracle) must be closed.

1) Stop the server software:

   Log in as **rboxuser**.
   Enter the command **ucrbshut**.
   Wait for the on-screen messages.
   Exit from **rboxuser**.

2) Stop the Red Box database:

   Log in as **rboxdba**.
   Enter the command **ucrbdbshut**.

   (If you are running a TNS listener, for example for domains or read-only views, shut that too).

   Wait for the on-screen messages.
   Exit from **rboxdba**.

2.2.2 Upgrade rboxsw

This section upgrades the Red Box UNIX user **rboxsw**. You will need the web interface issue tape 1.

Step A: Set up installation software under rboxsw

This step clears any files from earlier installations, reads the web interface components from issue tape 1, and creates the directory **$HOME/webinstall**.

1) Log in as **rboxsw**.

2) Insert the Red Box web interface issue tape 1.

3) Enter the commands:

cd $HOME
rm -rf webinstall
cpio -iBvduc < *tape-device-name*

where ***tape-device-name*** is the name of the tape device, for example, **/dev/rct0**.

Step B: Edit the installation scripts

Edit the scripts listed in the following table. Each line to be edited is identified by line number, using the format:

line number:*line contents*

The line contents contain variable names in italics. Replace each name with its value in Table 2.1 on page 20.

Table 2.2 Edits to apply to scripts

Scripts	Edits to apply (replace variables in line numbers shown below)
Location: **$HOME/webinstall/upgrades** *Scripts:*	
listener.ora	Follow the instructions in the comments at the front of this script.
ucrbweb_import	220: UCRB_SYS_USER_PASSWD=***sys-password***
Location: **$HOME/webinstall/bin** *Scripts:*	
create_rboxweb	29: UCRBWEB_SYS_PASSWD=***sys-password***
web_upgrade_dba	38: TNS_ADMIN=***rboxsw-home***/sqlnet 100:RBOX_SVCNAME=***service-name***

Scripts	Edits to apply (replace variables in line numbers shown below)
web_upgrade_user	39:UCRB_REDBOX_PORT=***redbox-port*** 40:UCRB_DCMESS_TAB=***batch-path***/dcmess.tab 41:UCRB_TEXT_TAB=***batch-path***/text.tab

Step C: Set up the directory structure for rboxsw

This step copies the web interface scripts to the directory **$RBOX_HOME/ucbin**, including the scripts amended in the previous step. If the **ucbin** directory already contains web interface scripts from a previous installation, these scripts are preserved in the directory **$HOME/webinstall/save** before being replaced in **ucbin**.

Enter the commands:

1) **cd $HOME/webinstall/working**

2) **../bin/web_upgrade_sw | tee web_upgrade_sw.log**

   If this is the first installation of the web interface, the command will prompt for confimation to continue when it attempts to preserve scripts, because there are no files to preserve. Reply **Y** to each prompt.

   The command logs all its actions in the file:

   $HOME/webinstall/working/web_upgrade_sw.log.

2.2.3 Upgrade rboxdba

This section sets up the directory **$HOME/web** and updates the **.profile**.

1) Log in as **rboxdba**.

2) Enter the command:

   ~rboxsw/webinstall/bin/web_upgrade_dba

2.2.4 Start the Oracle software and its TNS listener

This section starts the Red Box database to add the code and data for the web interface. The **-l** switch starts the TNS listener so that the webserver may later connect to the service and install Oracle packages.

1) Log out and then back in to **rboxdba**. This ensures that the **.profile** is properly executed.

2) Enter the command:

   ucrbdbstart -l

   (‘**l**’ is a lower case L, for ‘listener’).

2.2.5 Upgrade rboxuser

This section sets up the directory **$HOME/web** and creates the **server_details** file, which contains information required by **ucrbbatch**.

1) Log in as **rboxuser**.

2) Enter the command:

   ~rboxsw/webinstall/bin/web_upgrade_user

2.2.6 Define the web interface Oracle username

This section creates the Oracle username RBOXWEB to hold code and data for the web interface.

1) Log in as **rboxsw**.

2) Enter the commands:

   cd $HOME/webinstall/working

   ../bin/create_rboxweb

3) Check for errors by entering:

   grep ORA create_rboxweb_*.lst | grep -v ORA-01434 | grep -v ORA-01918

The two **-v** switches filter out errors that can be ignored; that is, ones reporting 'synonym to be dropped does not exist' and 'user to be dropped does not exist'.

If any other errors are reported, contact the Ultracomp Support Centre.

2.3 Install the webserver

Use the Oracle Installer to install your OWAS (Oracle Web Application Server) release 3 product, but follow the sequence given in this section. You will need your OWAS product's installation CD-ROM and *Oracle Installation Guide*.

If you have a release of OWAS other than release 3, contact the Ultracomp Support Centre.

2.3.1 Create owasuser

This section creates the UNIX user **owasuser** in which to run the webserver.

1) Log in as **root**.

2) Create the webserver user with the following attributes.

Table 2.3 Webserver user attributes

Attribute	Value
Login name	**owasuser**
Comment	**'Webserver user'**
Login group	A low-privilege group such as **other**, which gives minimal access to other user's files.

Attribute	Value
Shell	Korn shell: **/bin/ksh** (mandatory).
Home directory	The full hierarchic path name for the **owasuser** home directory must end with a directory called **owasuser**, for example, **/home/owasuser**. The directory must be owned by the user. It will be used as the installation directory. For space requirements, see the Oracle documentation for your webserver version.

2.3.2 Initialise owasuser

This section reads the web interface components from issue tape 2, sets up the **owasuser** directory structure and creates startup scripts (**.profile** and **.kshrc**).

1) Log in as **owasuser**.

2) Insert the Red Box web interface issue tape 2.

3) Enter the command:

   cpio -iBvduc < ***tape-device-name***

   where ***tape-device-name*** is the name of the tape device, for example, **/dev/rct0**.

2.3.3 Set up SQL*Net access from webserver to Red Box

1) Log out and then back in to **owasuser**. This ensures that the **.profile** is properly executed.

2) Edit the file **$TNS_ADMIN/tnsnames.ora**, as shown below. Replace the variable names in italics with actual values from Table 2.1 on page 20. The file defines services that can be accessed by SQL*Net.

Contents of $TNS_ADMIN/tnsnames.ora

```
service-name =
(DESCRIPTION =
    (ADDRESS_LIST =
        (ADDRESS =
            (COMMUNITY = redbox.world)
            (PROTOCOL = TCP)
            (Host = RB-machine-addr)
            (Port = sqlnet-port)
        )
    )
    (CONNECT_DATA = (SID = sid)
    )
)
```

2.3.4 Install OWAS

1) Log in as **owasuser**.

2) Insert the OWAS product installation CD-ROM and start the Oracle Installer, as described in your *Oracle Installation Guide*.

3) The following table lists the Oracle Installer screens and prompts, and shows the responses you should make.

Table 2.4 Responses to Oracle Installer prompts

Screen/prompt	Response
Installation Options	**Add/Upgrade Software**.
Home Locator	Accept the proposed setting for **ORACLE_HOME**, which is taken from the issued **.profile**.
Installation Log Files	Accept the proposed settings.
National Language Support	Select **American/English**.
Software Asset Manager	Select **Oracle Web Application Server** and choose **Install**.
Node Installation Type	Select **Single Node Installation**.
Simple or Custom Intallation	Select **Custom Installation**.
Home Locator	Accept the proposed setting for **ORAWEB_HOME**, which is taken from the issued **.profile**.
Site Name	Accept the proposed setting for **ORAWEB_SITE**, which is taken from the issued **.profile**.
Official Hostname	Enter the value of ***hostname1*** from Table 2.1 on page 20. This may be offered as the default value.
UDP Service Port	Enter the value of ***UDP-port***.
TCP Service Port	Enter the value of ***admin-port***.
Password	Enter the value of ***admin-password***.
Shared Key	Select **NO**; this is a single node installation.
Choose JDBC Components	Uncheck all boxes.
Selective Product Install	None; no VRML, and no ODBC (if offered).
Update Menu	Uncheck box.
Information prompt to execute command	Choose **OK**.

Screen/prompt	Response
Prompt to follow steps to complete installation	Choose **OK**.
Software Asset Manager	Choose **Exit**.
Confirmation	Choose **YES**.

This completes the OWAS installation. Do not follow any other installation steps in the *Oracle Installation Guide*.

2.4 Configure the webserver

This section starts OWAS (Oracle Web Application Server) on your UNIX server, and configures it from a PC web browser.

2.4.1 Start the webserver

Start the WRB (Web Request Broker) and webserver Administration Listener:

1) Log in as **owasuser**
2) Enter the command:
   owsctl start wrb
3) Wait for the on-screen prompts to display the message:
   "Web Dispatcher is accepting requests now".
   If necessary, press Enter to return to the UNIX prompt.
4) Enter the command:
   owsctl start admin

2.4.2 Configure the webserver

Connect to the Oracle Administration Listener.

1) From a PC web browser, use the following URL:
   http://*hostname1*:*admin-port*
   Replace ***hostname1*** and ***admin-port*** with values from Table 2.1 on page 20.
   You are prompted for your administrator name and password.

2) Make entries as follows:

   Table 2.5 Name and password for Oracle administration

Network Password prompt	Entry
User Name	**admin**
Password	***admin-password*** from Table 2.1.

   The Oracle Web Application Server Welcome screen is displayed.

Step A: Configure the webserver listeners

This step deletes the **www** listener and creates a user-listener called **rblsnr**, which will provide access to **owasuser**'s data and to the Red Box service.

From the Welcome screen:

1) Click **Web Application Server Manager**.

2) Click **Oracle Web Listener**.

3) Delete listener **www** as follows:

   a) Scroll down to the list of Oracle web listeners. There should be two

listeners only: **admin** and **www**. For example:

Figure 2.1 List of Oracle web listeners

b) Choose the DELETE option for listener **www**.

c) When asked for confirmation, choose the **Confirm Delete** button.
A 'Success' screen is displayed.

4) Create the new listener, **rblsnr**, as follows:

a) On the 'Success' screen, click the **Create Listener...** button.
The Create New Oracle Web Listener screen is displayed.

b) Make the following changes *only*:

Table 2.6 Entries on Create New Oracle Web Listener screen

Field	Entry
Listener Name	**rblsnr**
Port Number	***user-port*** from Table 2.1 on page 20.
Host Name	***hostname1*** from Table 2.1. If you have alternative host names, you will enter them on the next screen. **!** The default entry in the **Host Name** field may be ***hostname1*** followed by a full stop. In this case, *you must delete the full stop*.

c) Leave other entries. Scroll down to the **Advanced Configuration...** button, and click on this button.

A 'Success' message and Advanced Configuration screen for **rblsnr** are displayed.

5) Configure **rblsnr** as follows:

On the Advanced Configuration screen, scroll to the headings below and make entries as described. Do not click on the buttons under individual headings.

a) Addresses and Ports heading

The table under this heading should contain one entry for ***hostname1***. To allow additional hostnames (***hostname2***, ***hostname3***, etc. in Table 2.1 on page 20), add each hostname as an independent line. Make each line identical to the one for ***hostname1***, except for the hostname.

In the following example, *hostname1* is **foxweb**, and *hostname2* (**foxweb.ultracomp.co.uk**) has been added.

Figure 2.2 Addresses and Ports table showing entries for two hostnames

b) Log Time Style and Log Information File headings

You can choose your own preferences for the fields under these headings; see the Oracle help for possible values. Example entries are shown below.

Table 2.7 Example entries for log and user directory fields

Heading	Example entry (for details, see Oracle help)
Log Time Style	**LOCAL**
Log Information File	Name: **rblsnr.log** Format: **CLF** Format fields: **{clf c-ip sc-comment cs-method cs-uri}** For example: rblsnr.log CLF {clf c-ip sc-comment cs-method cs-uri}

c) Directory Mappings heading

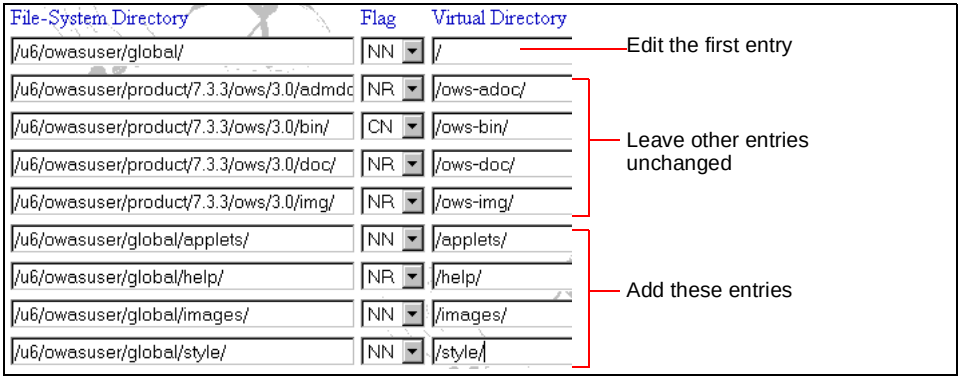
Edit the file system table in this section as shown in the following table. Note that the real and virtual directories in the two columns must start *and end* with '/'.

Table 2.8 Edits to directory mappings

File system directory	Flag	Virtual Directory
Overwrite the first entry with:		
***web-home*/global/**	**NN**	**/**
Leave other entries, then *add* the following:		
***web-home*/global/applets/** ***web-home*/global/help/** ***web-home*/global/images/** ***web-home*/global/style/**	**NN** **NR** **NN** **NN**	**/applets/** **/help/** **/images/** **/style/**

Replace ***web-home*** with its value in Table 2.1 on page 20.

Figure 2.3 Example directory mappings



6) This completes the configuration of **rblsnr**. Click the **Modify Listener** button. A 'Success' screen is displayed.

7) Click the **Admin** button to return to the Administration Home Page.

Step B: Create a Database Access Descriptor

This step creates a Database Access Descriptor (DAD) for the Red Box service.

From the Administration Home Page:

1) Click **Oracle Web Application Server**.

2) Click **DAD Administration**.

3) Click **Create New DAD**, and make the entries in Table 2.9 on page 36 *only*. Leave other fields and check boxes blank.

   Where an entry is qualified by '(for example)', you can choose a different value according to your preferences. Use Oracle help for descriptions of possible entries.

Table 2.9 Entries to Create new DAD screen

Field	Entry
DAD Name	**rbwdad**
Database User	**RBOXWEB**
Identified by	**Password**
Database User Password Confirm Password	**rboxweb**
ORACLE_HOME	Leave as set. *Note:* This ORACLE_HOME is for webserver code, and points within **owasuser**; Red Box's ORACLE_HOME is for database code, and points within **rboxsw**.
SQL*Net V2 Service	***service-name*** from Table 2.1 on page 20.
Database Role	Select **Default**
NLS Language	**AMERICAN_AMERICA.US7ASCII**

Field	Entry
NLS Currency	**£** (for example)
NLS ISO Currency	**United Kingdom** (for example - an Oracle territory name)
Store the user name and password in the DAD	Check this box.

4) Leave other fields and check boxes. Click the **Submit New DAD** button.
   A 'Success' message and the Database Access Descriptor screen is displayed.

5) Click the **Admin** button to return to the Administration Home Page.

Step C: Set up a PL/SQL agent for the Red Box service

From the Administration Home Page:

1) Click **Oracle Web Application Server**.

2) Click **Cartridge Administration**.

3) Click **PLSQL Cartridge**.

4) Click **Create New PL/SQL Agent**, and make the entries shown in Table 2.10 below.

Table 2.10 Entries to Create New PL/SQL Cartridge Agent screen

Field	Entry
Name of PL/SQL Agent	**rbwsqlagt**
Name of DAD to be used	DAD name from Table 2.9 on page 36; for example, **rbwdad**.
Protect PL/SQL Agent	**TRUE**
Authorized Ports	***user-port***
HTML Error Page	Leave blank.

Field	Entry
Error Level	**2**
DAD Username DAD Password	Leave these blank, because both username and password are stored in the DAD.
Install Web Application Server Developer's Toolkit PL/SQL packages	Check this box.
DBA Username	**sys**
Password	***sys-password***

5) Click the **Submit New Agent** button.

'Installing PL/SQL toolkit for user' messages are displayed, followed by a 'Success' screen.

6) Click the Cartridge button to display the Cartridge Administration screen.

Step D: Set minimum and maximum cartridges value

This step specifies the minimum and maximum number of cartridge processes that the webserver will run concurrently.

From the Cartridge Administration screen:

1) Click **Cartridge Summary (Web Request Broker)**.

2) In the Applications and Objects table, scroll to the row for the application **PLSQL**. Set the **Min** and **Max** values, following the recommendations given in Table 1.3 on page 14.

For example:

3) Scroll to the **Modify WRB Configuration** button, and click this button.

A 'Success' screen is displayed.

4) Click the **Home** button to return to the Oracle Web Application Server Welcome screen.

2.4.3 Start listener rblsnr

From the Welcome screen:

1) Click **Web Application Server Manager**.
2) Click **Oracle Web Listener**.
3) Start listener **rblsnr** as follows:
   a) Scroll down to the list of Oracle web listeners. There should two listeners only: **admin** and **rblsnr**.
   b) Choose the START option for listener **rblsnr**.

2.4.4 Close the webserver

This completes the configuration of the webserver, which can now be closed.

On the UNIX server:

1) (If necessary) log in as **owasuser**:
2) Enter the command:

   ucrbweb_service stop

   This closes all webserver processes including the two listeners **admin** and **rblsnr**.

It would be tidy to close your PC web browser at this point.

2.5 Web-enable Red Box 3

This section loads the Red Box software and data required to implement the web interface, and installs the Perl interpreter, which is required by the web updater.

2.5.1 Install the Red Box web-interface data and code

1) Log in as **rboxsw**.
2) Enter:

   cd $HOME/webinstall/working

   ../bin/initialise_rboxweb

   This command can take several minutes. It logs all its actions in the log and trace files within the directories:

   $HOME/webinstall/working
   $HOME/webinstall/textlog

2.5.2 Close the Red Box database

1) Log in as **rboxdba**.
2) Enter the command:

   ucrbdbshut -l

   (‘**l**’ is a lower case L, and closes the TNS listener)

2.5.3 Install a Perl interpreter

The Red Box web updater process is written in Perl. This section creates the file **perl.cpio**, which contains a copy of the entire Perl interpreter supplied with the webserver, and provides read permissions to all users and full permissions to **owasuser**.

1) Log in as **owasuser**.

2) Enter the commands:
cd $ORAWEB_HOME

For Sun Solaris systems, enter: **find perl -print | cpio -ovB -Hodc > $HOME/perl.cpio**
For HP-UX systems, enter: **find perl -print | cpio -ovBC > $HOME/perl.cpio**

3) Wait for the on-screen listing, then enter:
chmod 744 $HOME/perl.cpio

4) Create the directory containing the Perl runtime:
Log in as **rboxuser**.
Enter the commands:
cd $HOME/web.

For Sun Solaris systems, enter: **cpio -iBvdmuc < ~owasuser/perl.cpio**
For HP-UX systems, enter: **cpio -iBvdmu < ~owasuser/perl.cpio**

5) Delete the file **perl.cpio** which was used for the transfer:
Log in as **owasuser**.
Enter the command **rm $HOME/perl.cpio.**

This completes the installation of the web interface. If required, you can start the Red Box system to support PC client logins, by following the instructions in section 3.1 on page 51.

Before allowing access to the web interface, go through sections 2.6 to 2.8 below.

2.6 Set up automatic startup and shutdown

For manual startup and shutdown procedures, see Chapter 3.

You can automate the startup and shutdown of the web-enabled Red Box system by including issued scripts in your system startup and shutdown files. These scripts are supplied in **$HOME/webinstall/autostart** under **rboxsw** and should be executed in the order given below.

To start a web-enabled Red Box service:

S88dbstart to start the database
S89rbstart to start the Red Box software
S90wbstart to start the webserver

To close the service:

K48wbshut to stop the webserver
K49rbshut to stop the Red Box software
K50dbshut to stop the database

i Existing Red Box 3 users may have already copied the scripts **S88dbstart**, **S89rbstart**, **K49rbshut** and **K50dbshut** issued with Red Box 3. These users should still follow the procedures in this section, which will overwrite the existing scripts with new versions supplied for the web interface, and add the scripts **S90wbstart** and **K48wbshut**.

2.6.1 Copy the issued scripts

The contents of the issued scripts are shown in section 2.6.4 on page 45. To copy the scripts to your startup and shutdown files:

1) Log in as **root**.

   Use the example commands below.

Table 2.11 Example commands to copy automatic startup and shutdown scripts

For HP-UX systems, enter:
cp *rboxswHomeDirectory*/**webinstall/autostart/S88dbstart /sbin/rc2.d/S900dbstart** **cp** *rboxswHomeDirectory*/**webinstall/autostart/S89rbstart /sbin/rc2.d/S901rbstart** **cp** *rboxswHomeDirectory*/**webinstall/autostart/S90wbstart /sbin/rc2.d/S902wbstart** **cp** *rboxswHomeDirectory*/**webinstall/autostart/K48wbshut /sbin/rc0.d** **cp** *rboxswHomeDirectory*/**webinstall/autostart/K49rbshut /sbin/rc0.d** **cp** *rboxswHomeDirectory*/**webinstall/autostart/K50dbshut /sbin/rc0.d**
For Sun Solaris systems, enter:
cp *rboxswHomeDirectory*/**webinstall/autostart/S88dbstart /etc/rc2.d** **cp** *rboxswHomeDirectory*/**webinstall/autostart/S89rbstart /etc/rc2.d** **cp** *rboxswHomeDirectory*/**webinstall/autostart/S90wbstart /etc/rc2.d** **cp** *rboxswHomeDirectory*/**webinstall/autostart/K48wbshut /etc/rc0.d** **cp** *rboxswHomeDirectory*/**webinstall/autostart/K49rbshut /etc/rc0.d** **cp** *rboxswHomeDirectory*/**webinstall/autostart/K50dbshut /etc/rc0.d**

2.6.2 Edit rboxdba and rboxuser .profiles

This section is for Red Box users who have upgraded to release 3.
Skip this section if you are a new Red Box 3 user.

The automatic startup and shutdown scripts use '**su -**' to ensure that a suitable execution environment is available for the underlying script such as **ucrbdbshut**. This means that the username's **.profile** is executed, but in a no-terminal context.

To avoid terminal interaction in a no-terminal context, edit the **.profile** for your existing **rboxdba** and **rboxuser** users, as described below. You do not need to edit the **.profile** for **owasuser**, which is already suitable.

1) Edit **~rboxdba/.profile** and **~rboxdba/.profile**

2) In each **.profile**, find the extract below and add the text shown in bold. In the extract, colons indicate where part of the script has been skipped.

Extract from .profile — add the text shown in bold typeface

```
:
:
# Set certain terminal I/O options
if tty -s
then
        eval `/usr/ucb/tset -m ansi:ansi -m :\?${TERM:-ansi} -r -s -Q`
        stty intr '^C' erase '^H' echoe tab3
:
:
        EDITOR=vi
        export EDITOR
fi
:
:
```

2.6.3 Contents of startup and shutdown scripts

The contents of the issued scripts are shown below.

i The three startup scripts name log files with similar names to the startup scripts (**S88dbstart.log**, **S89rbstart.log** and **S90wbstart.log**). For HP-UX systems, you may want to amend the log file names to match the HP-UX script names given in Table 2.11 on page 43 (**S900dbstart**, **S901rbstart** and **S902wbstart**).

Table 2.12 Contents of startup and shutdown scripts

Issued scripts
Script: **S88dbstart**

```
# ------------------------------------------------------------------------
# Red Box Oracle7 database automatic start-up script.
# ------------------------------------------------------------------------

if [ -f /etc/profile ]
then
    . /etc/profile 1>/dev/null 2>&1
fi

if [ "$1" = "start_msg" ]
then
    echo "Starting Red Box Database"
else
    if [ -f /etc/rboxtab ]
    then
        su - rboxdba -c "ucrbdbstart -lw 1>S88dbstart.log 2>&1"
    fi
fi
```

Issued scripts

Script: **S89rbstart**

```
# ------------------------------------------------------------------
# Red Box automatic start-up script.
# ------------------------------------------------------------------

if [ -f /etc/profile ]
then
    . /etc/profile 1>/dev/null 2>&1
fi

if [ "$1" = "start_msg" ]
then
    echo "Starting Red Box Server"
else
    if [ -f /etc/rboxtab ]
    then
        su - rboxuser -c "ucrbstart -u 1>S89rbstart.log 2>&1"
    fi
fi
```

Script: **S90wbstart**

```
# ------------------------------------------------------------------
# Web service automatic start-up script.
# ------------------------------------------------------------------

if [ -f /etc/profile ]
then
    . /etc/profile 1>/dev/null 2>&1
fi

if [ "$1" = "start_msg" ]
then
    echo "Starting web service"
else
    su - owasuser -c "ucrbweb_service start 1>S90wbstart.log 2>&1"
fi
```

Issued scripts

Script: **K48wbshut**

```
# ------------------------------------------------------------------
# Web service automatic shutdown script.
# ------------------------------------------------------------------

if [ -f /etc/profile ]
then
     . /etc/profile 1>/dev/null 2>&1
fi

if [ "$1" = "stop_msg" ]
then
     echo "Stopping web service"
else
     su - owasuser -c "ucrbweb_service stop 1>K48wbshut.log 2>&1"
fi
```

Script: **K49rbshut**

```
# ------------------------------------------------------------------
# Red Box automatic shutdown script.
# ------------------------------------------------------------------

if [ -f /etc/profile ]
then
     . /etc/profile 1>/dev/null 2>&1
fi

if [ "$1" = "stop_msg" ]
then
     echo "Stopping Red Box Server"
else
     su - rboxuser -c 'ucrbshut -u 1>K49rbshut.log 2>&1'

     sleep 60
fi
```

Issued scripts

Script: **K50dbshut**

```
# ------------------------------------------------------------------------
# Red Box Oracle7 database automatic shutdown script.
# ------------------------------------------------------------------------

if [ -f /etc/profile ]
then
     . /etc/profile 1>/dev/null 2>&1
fi

if [ "$1" = "stop_msg" ]
then
     echo "Stopping Red Box Database"
else
     su - rboxdba -c "ucrbdbshut -l 1>K50dbshut.log 2>&1"

     sleep 60
fi
```

2.7 Configure hyperlinks

2.7.1 Edit web interface help

Edit the front page of the web interface help to provide a link to your organisation's home page, where the help text offers:

Your intranet YOUR ORGANISATION'S HOME PAGE

1) Log in as **owasuser**.
2) Enter:
   cd $HOME/global/help
3) Ensure that you have write access to **home.htm**, by entering:
   chmod 600 home.htm
4) Edit **home.htm**. Either insert a link to your organisation's home page or edit out the offer to jump to your home page.

2.7.2 Edit your organisation's intranet

You may need to edit pages within your intranet to provide links to either or both of:

- The web interface help front page:
  http://*hostname*:*user-port*/help/home.htm
- The web interface login screen:
  http://*hostname*:*user-port*/rbwsqlagt/plsql/uc_wakeup

2.8 Configure PC web browsers

Each web browser to be used to connect to Red Box must be configured as follows:

- **To accept cookies**
  A cookie called UCWEBINIT is used by the web interface.
- **To execute Java**
  The password-check screen is implemented as a Java applet.
- **Preferably, to execute Javascript**
  Various components of the help system use Javascript.

Some of these options may be the browser defaults, but you should check and adjust them as necessary. The instructions for doing this will be specific to the browser and browser version.

RUNNING THE WEB INTERFACE

If you followed the procedures in section 2.6 on page 42 to set up automatic startup and shutdown, your Red Box system will start up and shut down automatically with the UNIX server, and will be web-enabled.

This chapter gives the procedures for:

- Manual startup (section 3.1)
- Manual shutdown (section 3.2)
- Starting and stopping additional web updaters (section 3.3)

3.1 Manual startup

To start the server software manually:

1) Start the Red Box database and the TNS listener, and initialise the database for the web service:

   Log in as **rboxdba**.
   Enter the command **ucrbdbstart -lw**
   Wait for the on-screen messages.
   Exit from **rboxdba**.

2) Start the Red Box server software and one web updater:

   Log in as **rboxuser**.
   Enter the command **ucrbstart -ru.**
   Wait for the 'ucrbstart ends OK' message.
   Exit from **rboxuser**.

3) Start the webserver:

   Log in as **owasuser**.
   Enter the command **ucrbweb_service start**.
   Wait for the on-screen 'started OK' messages.
   Exit from **owasuser**.

3.2 Manual shutdown

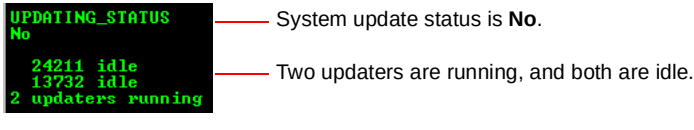
To close the system manually:

1) Prevent web users submitting more update requests:

   Log in as **rboxuser**.
   Enter the command:

   ucrbweb_updates hold

   The command stops further updates, and reports the status of web updaters (idle or processing). For example:



2) If any updaters have the status 'processing', wait for them to become idle. At periodic intervals, enter the command:

   ucrbweb_updates status

   Wait for the command to report the status 'idle' for all updaters.

3) Stop the webserver:

   Log in as **owasuser**.
   Enter the command **ucrbweb_service stop**
   Wait for the on-screen 'closing' messages.
   Exit from **owasuser**.

4) Stop the Red Box server software and web updaters:

   Log in as **rboxuser**.
   Enter the command **ucrbshut -u**
   The command stops one updater and displays the number still running.
   For each updater still running, enter the command **ucrbweb_updates stop**
   Exit from **rboxuser**.

5) Shut the Red Box database and the TNS listener:

   Log in as **rboxdba**.
   Enter the command **ucrbdbshut -l**.
   Wait for the on-screen messages.
   Exit from **rboxdba**.

3.3 Additional web updaters

The instructions for manual startup, and the automatic startup script (see **S89rbstart** in section 2.6.3 on page 45), load only one updater. You may wish to load additional updaters, as discussed in Table 1.3 on page 14.

3.3.1 To load an updater

You can load a web updater when the Oracle software is running.

Log in as **rboxuser**.
Enter the command **ucrbweb_updates start**
The command confirms how many updaters are now running.
Exit from **rboxuser**.

3.3.2 To close an updater

To close a web updater:

Log in as **rboxuser**.
Enter the command **ucrbweb_updates stop**
The command confirms how many updaters are now running.
Exit from **rboxuser**.

CONFIGURING RED BOX FOR WEB ACCESS

Having started the Red Box server, load the PC client at a Red Box PC and use the Administration application to create and amend database records required by the web interface. You may need to:

- License the web interface (section 4.1)
- Create a **Web Slots** group (section 4.2)
- Allocate slots for web use (section 4.3)
- Set up access rights for web users (section 4.4)
- Set up Red Box user records for web users (section 4.5).

When configuring Red Box, you will need the information in the tables given in section 1.4 on page 14.

4.1 License the web interface

Your site has a single product licence for Red Box, which covers all the applications for which your site is licensed including the web interface. The licence details are given on the installation record form supplied with your version of Red Box, and include the option code **WB** if you are licensed for the web interface.

i If you licensed the web interface during Red Box installation, your licence details will include the **WB** option code, and you do not need to change them.

If you purchased the web interface separately, you will have received a second installation record form, which has a new checksum and adds the **WB** option code. In this case, you must update your Red Box licence as follows:

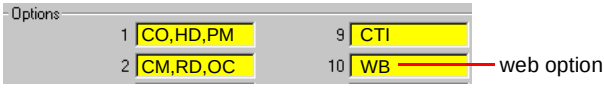
1) In the Administration application, choose **System | Licence**.

   The Licence - View screen is displayed.

2) Choose the **Amend** button, and amend fields as necessary with details from the installation record form provided with the Red Box web interface. You will need to change the checksum and add the web option code **WB.**

3) Choose the **OK** button.

Figure 4.1 Example licence options



4.2 Create a Web Slots group

The web interface requires a group named **Web Slots**, whose sole function is to allocate reserved slots for web sessions. Web sessions cannot use unreserved slots.

i The Web Slots group must *not* have members assigned; if it does, no web access is allowed.

Do not add slots to any other user group to allow web access.

To create the Web Slots group record

In the Administration application:

1) Choose **Users | Group | Create**.
   The User Group - Create screen is displayed.

2) Make the following entries:

Table 4.1 Entries on User Group - Create screen

Field	Entry
Group	**Web Slots** (include initial capitals and space).
Access Rights	You can reference any access rights record. It will not be used, because a web user's access to Red Box records is restricted by the access rights specified in their Red Box user record.
Description	Enter any description.
Slot Usage	These read-only fields will contain values when you assign slots in the next section.

3) Choose the **OK** button to create the group record and display its view screen.

4.3 Allocate slots for web use

This section uses the Red Box Slots screen to allocate slots required for the web interface.

In the Administration application:

1) Choose **Users | Slots**.
   The Slots screen is displayed.

2) Check the following values on the Slot Usage tab, and amend them if necessary using configuration values calculated in Table 1.4 on page 15.

   a) **Oracle Processes**. This read-only value will reflect any changes made to the **processes=** value in the Oracle initialisation file prior to the last database reload.

   b) **Maximum Database**.

   c) **Maximum Client**.

   d) **Reserved**. This read-only value will increase when you assign reserved slots to the Web Slots group in step 3, unless you re-allocate reserved slots from other groups.

3) Assign slots to the **Web Slots** group:

   a) Choose the Group Settings tab.

   b) Scroll to the **Web Slots** group and highlight this line.

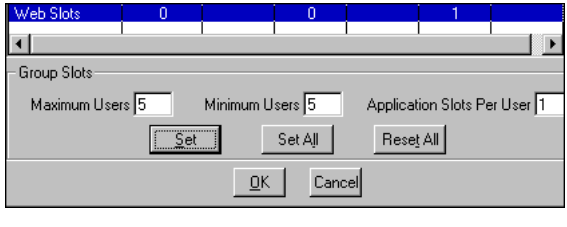
   c) Under the Group Slots heading, make the following entries:

Table 4.2 Slot settings for Web Slots group

Field	Entry
Maximum Users Minimum Users	The max-web-sessions value in Table 1.3 on page 14. Set both fields to the same value.
Application Slots Per User	**1**

Choose the **Set** button to apply your settings to the Web Slots group.

Figure 4.2 Example slot settings



4) Choose the **OK** button to update all values and exit the Slots screen.

4.4 Set up access rights for web users

This section describes how to set up up access rights for:

- Users who will access the web interface only (web-only users)
- Users who will use the web interface and PC client.

You can create new access rights records especially for web users, or amend existing access rights records.

For each access rights record:

1) Display the Access Rights - View screen:

2) Allow access to the Web Interface application:
   a) Choose the **Applications** button.
   b) In the list of applications, highlight the line for the Web Interface.
   c) Select check boxes for the access you wish to allow:

Access	Permissions
Read	Allows web users to view database records.
Insert and Amend	Allows web users to update the database.
Delete and Supervisor	The web interface does not use these access rights.

   d) Choose the **Set** button. This applies your access settings to the Web Interface.

e) If required, set access to other applications as follows:

Red Box user	Access to other applications
Web-only users	Do not allow access to other applications. Web-only users will access all Red Box records via the web interface application.
Users of web interface and PC client	Set the required access to other Red Box applications.

f) Choose the **OK** button to return to the Access Rights - View screen.

3) Set access rights to records:

a) Choose the **Records** button.

b) For each record type that will be accessed via the web interface, set **Read**, **Insert** and **Amend** access as required. Note that when creating records, you need insert access to the record type you are creating *and* read access to any record types referenced by the new record.

i Make sure that the access allowed to the web interface in step 2 covers the access to record types. For a user to be allowed access to a record type, the record type access rights and the application access rights must *both* allow the access required. For example, to create RFCs a user must have 'Insert' access rights both to the web interface application and to the RFC Details record type.

c) Having set the required access to record types, choose the **OK** button to return to the Access Rights - View screen.

4.5 Set up Red Box user records for web users

Anyone who accesses Red Box via the web interface requires a Red Box user record and password in the same way as any other Red Box user. Their access rights must allow access to the web application, but their user group does not need slots assigned for web sessions; this is because the **Web Slots** group allocates reserved slots for all web users.

This section describes how to set up up Red Box user records for:

- Web-only users
- Users who will use both web interface and PC client.

4.5.1 Encrypt passwords

For a user to be able to log in via the web interface, they must have an encrypted Red Box user password. If the password is not encrypted, login attempts will be rejected with the message 'Invalid username and/or password'.

To encrypt passwords:

1) Select the Red Box password encryption option.

   In the Administration application:

   a) Choose **System | System Options**, then the Password Control tab.
   b) If the **Encrypt Passwords** field is set to **No**, choose the **Amend** button.
   c) Change the setting to **Yes**, and choose the **OK** button.

2) Supply encrypted passwords.

   With the encryption option set to **Yes**:

   a) For new users, create Red Box records and supply passwords in the normal way. The passwords will be encrypted.

b) For existing users who had passwords supplied without encryption:

View their Red Box user record.
Choose the **Change Password** button.
Supply a new password. The passwords will be encrypted.

4.5.2 Set up web-only users

Create or amend a Red Box user record for each web-only user, as follows:

1) Assign an access rights record that allows access to the web interface application only, and all required record types. Do not allow access to other Red Box applications.

2) Assign a user group that has all slots set to zero:

Maximum Users = 0

Minimum Users = 0

Application Slots Per User = 0

Because the group has **Maximum Users** set to zero, it will not allow PC client logins.

4.5.3 Set up users who require both web interface and PC client

Create or amend Red Box user records for these users as follows:

1) Assign an access rights record that allows:

a) Access to the web interface.
b) Access to the required PC client applications.
c) Access to the relevant record types.

2) Assign a user group that allocates slots for the number of concurrent PC client applications required. Do not reserve additional slots for web use.

When users log in under this group:

a) If they log in to the PC client, they use their group's application slots.
b) If they log in to the web interface, they do not use slots from their user group. Instead, they use a reserved slot from the **Web Slots** group.

PREPARING FOR INCIDENT CREATION VIA THE WEB

This chapter describes the details that are logged for an incident report created via the web interface.

To prepare for incident creation via the web, you must:

- Set up IR prefixes (section 5.2)
- Supply IR-creation values in the web interface System Settings (Table 5.2).

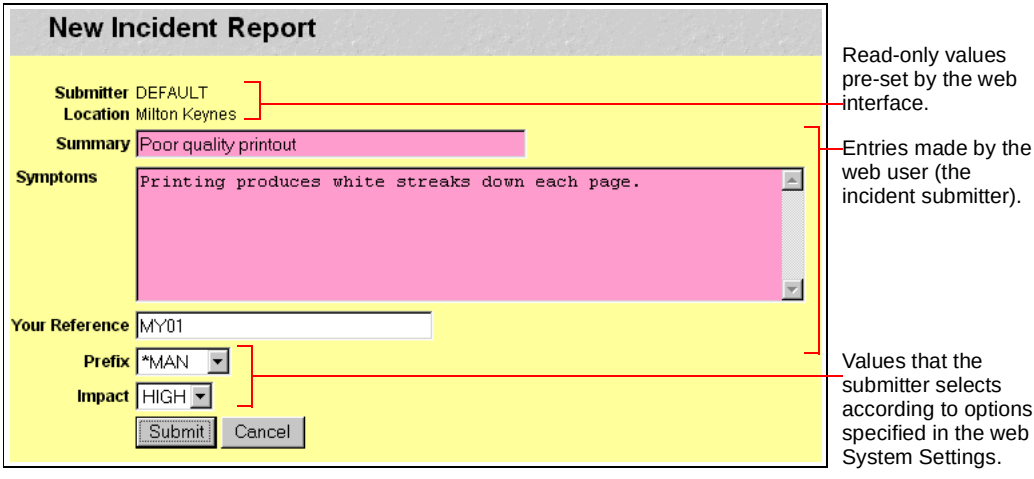
With the exception of IR prefixes, the Red Box records (submitter, team, etc.) referenced by web-created incident reports do not require special values. Incidents can reference existing Help Desk records, or they can reference records created especially for web users (incident submitters).

The web interface assigns all incidents the same method, general category and team, so you may find it useful to create special web versions of these records. These can filter the incidents and make them easy to identify. For example, you could create a method called **WEB**.

5.1 Supplying incident details

When a web user chooses the option to create a new incident, the web interface displays a New Incident Report form for completion. Figure 5.1 shows an example.

Figure 5.1 New Incident Report form



The details logged for each incident comprise:

- **Values pre-set by the web interface**.

  The following values are displayed read-only on the New Incident Report form, and are passed to the incident, provided they are not overridden by **Default Only** values in the IR prefix.

  Table 5.1 Incident values pre-set by the web interface

Incident field	Pre-set value
Submitter	Submitter's user/department name.
Location	The location named in the submitter's user/ department.

- **IR-creation settings.**

  Before web users can submit incident reports, you must supply IR-creation settings in the web interface System Settings (for details, see section 7.2 on page 80). Each setting must reference an existing Help Desk record, created using the PC client.

  Table 5.2 Incident values supplied via the web interface System Settings

Incident field	IR-creation settings
Method	Specify the method, general category and Help Desk team to be assigned to all incidents. The web interface passes these fields to all new incidents, although the fields are not displayed on the New Incident Report form.
General Category	
Team	
IR prefix	Specify the prefix to be displayed as the default on the New Incident Report form. All prefixes available for selection must have the values described in section 5.2 on page 69.
Prefix Selection	Select **None**, or select one of the following options to make alternative IR prefixes available to incident submitters. • **Prefixes with user as default submitter** This option offers prefixes whose **Default Submitter** field names the submitter's owning user/department. • **Prefixes with user's location as default** This option offers prefixes whose **Default Location** field names the location in the submitter's owning user/department record. • **Prefixes linked to submitter** This option offers prefixes that are linked to the submitter's owning user/department.

Incident field	IR-creation settings
	• **Prefixes linked to submitter's location** This option offers prefixes that are linked to the location named in the submitter's owning user/ department.
Impact (*supply up to 3*)	The New Incident Report form offers impacts for selection, in the order given in the web interface System Settings. The first impact is the default. In order for web users to submit new incidents, the system settings must name at least one impact.

- **Entries made by the submitter on the New Incident Report form**.

  The submitter selects an IR prefix and impact from those allowed in the IR-creation settings, and supplies values in the following fields:

  Table 5.3 Entries made by the incident submitter

Field	Value
Summary	The submitter must complete these fields.
Symptoms	
Reference	This field is optional.

- **Prefix defaults.**

  Red Box uses defaults in the IR prefix for empty incident fields. **Default Only** values in the IR prefix will override incident fields that contain values. For details, see section 5.2.2 on page 69.

- **Department and phone number**.

  Red Box assigns the default department specified in the IR prefix, or if none, the department named in the submitter's user/department record. If neither record specifies a department, Red Box leaves the incident's **Department** field blank.

  The phone number (if any) is the one specified in the department record.

5.2 Prefix values

IR prefixes that are available to web users should have their sequence number and defaults options set as follows.

5.2.1 Sequence number options

Each IR prefix must specify:

Auto Sequence = Yes

The other sequence number options are unimportant.

i Once the web interface has allocated a sequence number, the number will not be re-used even if the incident creation fails. This can lead to gaps in sequence numbers.

5.2.2 Prefix defaults

If possible, do not specify '**xxx Only**' defaults options in IR prefixes that can be selected by web users. These options (**Default Only**, **Department Only**, **Links Only**, **Location Only** and **Submitter Only**) have the following effects on web-created incidents:

- **Default Only** values override values passed by the web interface.

- If **Department Only**, **Links Only**, **Location Only** or **Submitter Only** options are restrictive, they may clash with values passed by the web interface and cause the incident creation to fail.

! If a **Default Only** value in the IR prefix overrides the submitter name, the web user will find that they cannot view the incident later using the web interface viewing options. These options only allow users to view incidents submitted for their own user/department.

PREPARING FOR RFC CREATION VIA THE WEB

This chapter describes the details that are logged for an RFC created via the web interface.

To prepare for RFC creation via the web, you must:

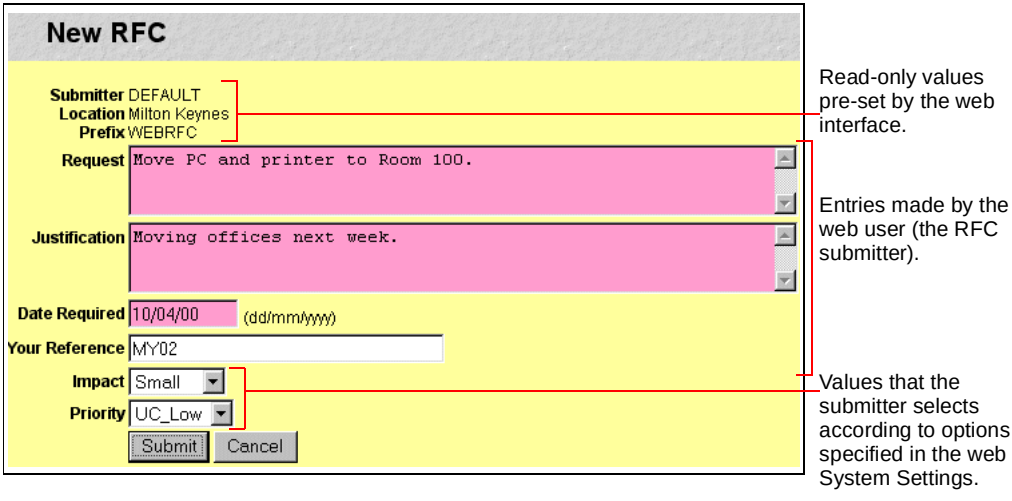
- Set up RFC prefixes (section 6.2)
- Supply RFC-creation values in the web interface System Settings (Table 6.2).

With the exception of RFC prefixes, the Red Box records referenced by web-created RFCs do not require special values. RFCs can reference existing Change Management records, or they can reference records created especially for web users (RFC submitters).

6.1 Supplying RFC details

When a web user chooses the option to create a new RFC, the web interface displays a New RFC form for completion. Figure 6.1 shows an example.

Figure 6.1 New RFC form



The details logged for each RFC include:

- **Prefix defaults**.

  Red Box applies any defaults from the RFC prefix named in the CM application defaults, then it applies defaults from the RFC's own prefix. For details, see the section 6.2.3 on page 76.

- **Values pre-set by the web interface**.

  The following values are displayed read-only on the New RFC form, and are passed to the RFC, provided they are not overridden by **Default Only** prefix values.

  Table 6.1 RFC values pre-set by the web interface

RFC field	Pre-set value
Submitter	Submitter's user/department name.
Location	The location named in the submitter's user/ department.

- **RFC-creation settings.**

  Before web users can submit RFCs, you must supply RFC-creation settings in the web interface System Settings (for details, see section 7.2 on page 80). Each setting must reference an existing Change Management record, created using the PC client.

  Table 6.2 RFC values supplied via the web interface System Settings

Field	RFC-creation setting
RFC prefix	All web-created RFCs will have this RFC prefix. Its name is displayed read-only on the New RFC form. The prefix should have the options described in section 6.2 on page 74.
Initial status	This is the status code to be displayed for the **Not Started** status type. The New RFC form does not display this value, but it is passed to all new RFCs.
Impact (*supply up to 3*)	The New RFC form offers impacts and priorities for selection, in the order given in the web interface System Settings. The first impact is the default impact, and the first priority is the default priority. In order for web users to submit new RFCs, the System Settings must name at least one impact and one priority.
Priority (*supply up to 3*)	

- **Entries made by the submitter on the New RFC form**.

  The submitter selects an impact and priority from those allowed in the RFC-creation settings, and supplies values in the following fields:

Table 6.3 RFC entries made by the RFC submitter

Field	Submitter's entry
Request	The submitter must complete these fields.
Justification	
Date Required	
Reference	This field is optional.

6.2 Setting up RFC prefixes

You should check any RFC prefixes whose options can affect web-created RFCs. These prefixes are:

- The RFC prefix (if any) named in the Change Management application defaults. Initially, a new RFC contains defaults specified in this prefix. For details, see section 6.2.3 on page 76.
- The RFC prefix specified in the web interface System Settings. The web interface assigns this prefix to all new RFCs. The RFC's prefix determines the RFC's options for:

  a) Sequence numbering.
  b) Automatic model assignment.

  Set these options as described in the following sections. If the RFC's prefix has **Default Only** default values, these will override existing RFC values taken from the application default prefix.

6.2.1 Sequence number options

The RFC prefix specified in the web interface System Settings must specify:

Auto Sequence = Yes

The other sequence number options are unimportant.

i Once the web interface has allocated a sequence number, the number will not be re-used even if the RFC creation fails. This can lead to gaps in sequence numbers.

6.2.2 Model assignment

The RFC prefix specified in the web interface System Settings specifies its automatic model assignment options.

- To create each RFC with a model attached:

  a) Set:

  Supply Model On Create = Mandatory

  b) Supply a default model. This must be a **Default Only** model if it is to override any default model given in the prefix named in the CM application defaults.

  If Red Box cannot find a default model in either prefix, the RFC creation fails.

- To create each RFC without a model attached, set:

  Supply Model On Create = Not Allowed

  With this setting, Red Box creates each RFC without a model assigned, and ignores any default models.

If the RFC's prefix specifies:

Supply Model On Create = Optional

Red Box assigns an RFC model provided it can find a default, either in the application default prefix or in the RFC's own prefix. If it does not find a default, it leaves the model unassigned.

6.2.3 Prefix defaults

An RFC prefix can supply defaults for the following fields: **Submitter**, **Location**, **Department**, **General Category**, **Team** and **Model**. When an RFC is created via the web, the values in these fields are derived as follows:

1) Initally, the RFC contains any defaults specified in the application default prefix.
2) Defaults in the RFC's own prefix (the one specified in the web interface System Settings) are used where they specify **Default Only** values, and for fields where the application default prefix did not supply a value.
3) The web interface overrides the RFC's **Submitter**, **Location** and **Department** with the:

   a) The submitter's user/department name

   b) The user/department's location

   c) The user/department's department, if any (the department is an optional field).

Submitter, location and department defaults

The RFC prefix specified in the System Settings *must not*:

- Specify a **Default Only** submitter, location or department. If it does, the web interface cannot override these values with details about the RFC's submitter.
- Specify **Linked Only** values for submitter, location or department. If the list of links does not include the RFC submitter's user/department, location or department, the RFC creation will fail.

General category defaults

To assign a general category to all RFCs, specify a default either in the prefix specified in the CM application defaults or the RFC's own prefix. If there is no default, Red Box leaves the RFC's **General Category** field blank.

Team defaults

You must specify a default team either in the prefix specified in the CM application defaults or the RFC's own prefix. If Red Box cannot assign a team, the RFC creation fails.

Model defaults

If the RFC's own prefix specifies:

Supply Model On Create = Mandatory

then there must be a default model specified either in the prefix specified in the CM application defaults, or in the RFC's own prefix. If model assignment is mandatory and Red Box cannot find a default model, the RFC creation fails.

SETTING WEB ADMINISTRATION OPTIONS

Your first use of the web interface must include supplying system settings. You may also wish to change the level of history displayed for incidents, and check slot usage. These web interface administration options can be accessed by the Red Box **Administrator** user only.

7.1 Logging in as Administrator

Log in to the web interface by using links described in section 2.7.2. The URL for the web interface login screen is:

http://*hostname*:*user-port*/rbwsqlagt/plsql/uc_wakeup

On the web interface login screens, supply the Red Box Administrator name and password.

Table 7.1 Administrator name and password

Username	Administrator
Password	Administrator's password.

When you are logged in, the web interface displays the user details for the Administrator user. The web interface menu on the left of the screen includes administration options only.

7.2 Supplying system settings

To supply system settings, choose the **Settings** option from the Administrator's web interface menu, and supply values as follows. Choose the **Submit** button to update the web interface.

Table 7.2 Web interface system settings

Field	Entry
Session control TIMEOUT_MINS	Interval in minutes for which a logged in user's session is protected from being timed out. The interval is reset to this value each time the user accesses the Red Box database. *i* Accessing help or any other web pages does not cause a reset, so users who are connected to Red Box and navigate to other pages may be timed out, and have to log in again.
Updating control UPDATING_ALLOWED	• **Yes** allows users to to send update requests to Red Box (equivalent to **ucrbweb_updates release**). • **No** prevents future update requests (equivalent to **ucrbweb_updates hold**). Users will receive a message if they attempt an update.
BATCH_WAIT_SECS	Maximum time in seconds that a web session will wait for an update to be completed. This covers incident report or RFC creation, and incident report maintenance. If the update is not complete within this time, the user will be told whether the update has been abandoned or is being processed. In the latter case, they are also told how to check for its completion.
IR-creation settings	See Table 5.2 on page 67.

Field	Entry
RFC-creation settings	See Table 6.2 on page 73.
Display control MAX_LIST_LENGTH	The length of lists displayed by the web interface when a user chooses the **Search** button for incident reports or RFCs. This limit operates differently from the retrieval limit in the PC client; the list length applies to all users, and sets an upper limit to the number of records listed, even if the query returns more records. There is no equivalent to a **More** button in the web interface.
NUMBER_PATTERN CURRENCY_PATTERN DATE_PATTERN DATE_TIME_PATTERN	These are formatting patterns for the web interface display in fields of these types. The patterns differ from those in the PC client. Follow the format model guidelines in the *Oracle Server SQL Reference: Operators, Functions, Expressions, Conditions*. If you leave the fields empty, Oracle will apply the database defaults. Note that the case of a pattern affects text output, such as month names.
System parameters TRACE_LEVEL	The default is **Minimum**. Only change this value if you are asked to do so by Ultracomp support.

7.3 Masking incident history types

When they view incident reports, web users with read access rights to history records will see a related history list. You can control the types of event for which history is shown, by selecting predefined groups or individual event types.

While logged in as Administrator:

1) Choose the **History Mask** option.

   The web interface shows the current settings.

2) Select history types and actions as follows.

Table 7.3 Options on the IR History Mask screen

Button	Meaning
Show All	Users will see history for all event types.
Show None	Users will see no history.
Group	Users will see the history types selected under the Groups heading. To use this option: 1)Under the Groups heading, select check boxes for the groups of history to be displayed. Users will see history for all event types within those groups. 2)Choose the **Group** button.
Custom	Users will see history types selected under the Events heading. To use this option: 1)Under the Events heading, select check boxes for individual event types. 2)Choose the **Custom** button.

Button	Meaning
Reset	Resets changes you have made to the form since it was output.
Cancel	Cancels the form, and returns to the user details display, without making any changes to the history mask.

7.4 Viewing slots usage

You can display the number of slots currently used by web interface sessions. The figures do not include any PC client sessions.

While logged in as Administrator:

1) Choose the **View Slots** option.

   The web interface shows the current values.

   Table 7.4 Slot usage values

Field	Meaning
Protected	These slots are occupied by logged in users who are within the session timeout period you have defined in the system settings.
Reclaimable	These slots are occupied by logged in users outside the timeout period.
Free	Free slots are not occupied by any users.
Total	This is the total number of reserved application slots assigned to the **Web Slots** user group.

2) Choose the **Refresh** button to update the values while they are displayed.

WEB SCRIPTS

The following table describes the web interface scripts available to UNIX users.

Table 8.1 Web interface scripts

Script	Parameter	Function
Under **owasuser:**		
ucrbweb_service	start	Starts the webserver.
	stop	Stops the webserver.
Under **rboxdba:**		
ucrbdbshut	-l	Closes the TNS listener as well as the Red Box database.
ucrbdbstart	-l	Starts the TNS listener as well as the Red Box database.
	-w	Resets the Red Box database for a new Web service.
Under **rboxuser:**		
ucrbshut	-u	Stops the web updater as well as the Red Box server software. The updater's log should report a STOP command and then its own closure.
ucrbstart	-h	Stops requests to the updater being written to the communication area (see section 1.1 on page 10), as well as starting the Red Box server software. The **-h** switch is equivalent to **ucrbweb_updates hold**.

Script	Parameter	Function
	-r	Releases the updater's command pipe as well as starting the Red Box server software. The **-r** switch is equivalent to **ucrbweb_updates release**.
	-u	Starts the web updater as well as the Red Box server software.
ucrbweb_updates	flush	Only use under direction from Ultracomp.
	hold	Prevents the web interface from taking new update requests from users (sets the UPDATING_ALLOWED system setting to **No**). This option is called if the **-h** switch is supplied to **ucrbstart**.
	init	Only use under direction from Ultracomp.
	release	Allows the web interface to take new update requests from users (sets the UPDATING_ALLOWED system setting to **Yes**). This option is called if the **-r** switch is supplied to **ucrbstart**.
	start	Starts an updater as an autonomous background process, logging to files **updater.log** and **updater**_*process-id*.**log** in the directory **$HOME/web/batchfiles**. This option is called if the **-u** switch is supplied to **ucrbstart**.
	status	Shows the UPDATING_ALLOWED system setting and the current state of the web updaters (idle or processing). It does *not* show the state of the command pipe.
	stop	Places a STOP command in the command pipe, causing an updater to close once all the commands before the STOP have been read from the pipe. This option is called if the **-u** switch is supplied to **ucrbshut**.

Script	Parameter	Function
Under **rboxuser** (or any user with SQL*Plus access to Red Box:)		
ucrbweb_kill	*RedBox-username*	Kills all sessions for the user identified by *RedBox-username*, as if they had been timed out. ***i*** If the username contains spaces, enclose the name in quotes; for example, **ucrbweb_kill "Joe Soap"**
ucrbweb_showtrace		Displays the trace information collected while the TRACE_LEVEL system setting is at **Maximum**. Only use under direction from Ultracomp..
ucrbweb_import		Imports the web interface components exported by an upgraded **ucrbexport**, as described below.

8.1 Reorganising and moving a web-enabled database

In both cases below, before starting:

- Oracle should be running, and
- Red Box should be shut.

Both cases should be performed under UNIX user **rboxsw**.

8.1.1 Reorganising a web-enabled database

In this case, the new database is set up under the same UNIX users as the old one, and the scripts, directory structures, etc of those users are left unchanged. After setting up the new database by using **ucrbsetup**, it is necessary to remove any existing web information and then recreate it from the two web export files.

1) Set up the main Red Box via **ucrbsetup**
2) Ensure Oracle is running but Red Box is closed.
3) Remove existing web information and create a new empty RBOXWEB:

   cd ~/webinstall/working
   ../bin/create_rboxweb | tee create_rboxweb.log
4) Load its data from the previous database:

   cd
   ucrbweb_import

8.1.2 Moving a web-enabled database

In this case, the new database is set up under a new set of UNIX users, possibly on a different machine. After setting up the new database by using **ucrbsetup**, it is necessary to create the web environment in the same way as for a full installation (except for **initialise_rboxweb** and installing the PL/SQL development kit from the webserver), and then recreating the web information as for a reorganisation.

1) Set up the main Red Box via **ucrbsetup**.
2) Ensure Oracle is running but Red Box is closed.
3) Install the web interface as described in Chapter 2, except for **initialise_rboxweb** and installing the PL/SQL development kit from the webserver.
4) Remove existing web information and create a new empty RBOXWEB. If **initialise_rboxweb** was called earlier:

   cd ~/webinstall/working
   ../bin/create_rboxweb | tee create_rboxweb.log
5) Load its data from the previous database:

   cd
   ucrbweb_import

INDEX