

Red Box on the Net

Release 3.00c

Installation and Administration Guide

M0087a Edition 1



0. Contents

0.	Contents.....	2
0.1	Copyright notice	3
0.2	About this guide.....	3
0.3	Technical support.....	3
1.	Prepare your Red Box Service (Part 1)	4
1.1	License.....	4
1.2	Create Red Box Users for Web Servers	4
1.3	Custom Field Changes.....	4
	User/Department record changes for Web access control	4
	Problem Report record changes for Known Errors.....	5
	Implementing the changes	5
2.	Install Red Box on the Web software.....	6
3.	Add a Domain Name Server (DNS) entry	6
4.	Configure the Web Service	7
4.1	IIS 4.0	7
4.2	IIS 5.0	8
5.	Set Web Server Defaults	9
5.1	System Settings.....	9
5.2	User Settings	9
5.3	Incident Settings	9
5.4	RFC Settings.....	10
5.5	History Settings	11
6.	Prepare your Red Box Service (Part 2)	12
6.1	Users	12
6.2	Access Rights and Domains	12
6.2	Default Settings for Users.....	13
	Prefix Selection.....	13
	Prefix Defaults	13
	Domaining.....	14
7.	Server Administration	15
7.1.	Microsoft Management Console.....	15
	Red Box Server database connection.....	15
7.2	Amending Controlling Users and Max Logins.....	15
7.3	Initialisation File Settings	15
	[RedBoxNet] Section	16
	[Cache] Section.....	16
	Other Sections.....	16
7.4	Troubleshooting.....	17
	General.....	17
	Log Files	17

0.1 Copyright notice

This document is the copyright material of Fox IT Ltd. It may not be copied without prior consent, in writing, from Fox IT Ltd. All trademarks are acknowledged.

Fox IT Ltd endeavours to ensure that the information in this document is correct, but does not accept liability for any error or omission. However, Fox IT Ltd would be pleased to receive readers' views on the contents of this document.

The products described in this document are subject to licence agreements which govern their use. Statements in this document are not part of any licence or contract save insofar as they are incorporated into a licence or contract by express agreement. Issue of this document does not imply any entitlement to use of or access to any or all of the products or facilities it describes.

0.2 About this guide

This guide gives the installation and administration procedures for the Red Box on the Net 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.

0.3 Technical support

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

Support contact information

General enquiries	Fox IT Support Centre
Fox IT Limited Brook House 100 Chertsey Road WOKING Surrey GU21 5BJ.	Tel : +44 (0) 1483 221333 Email: support@fox-europe.com Internet: http://www.fox-europe.com

1. Prepare your Red Box Service (Part 1)

Before you can use Red Box on the Net, you must update the Red Box database to know about the new Web Servers you will be running.

1.1 License

You will need to obtain a licence for Red Box which includes the **WB** application.

Additionally, your licence must include one 'slots' option for each web server you wish to run. For example:

WB02,5

provides 5 slots for a Web Server (**WB02**) which has its Web Server ID entry in its .INI file:

ApplicationID=2.

1.2 Create Red Box Users for Web Servers

You will need to create one Red Box User record for each web server you wish to run. This user will be used by the web server to establish a connection to the Red Box database.

For server **WB02**, create a record for user **WB02** and set the password for the user to the user name twice, in this case **WB02WB02**. (Note that references to **02** are numeric).

Ensure that the owning group for the user has NO access rights, and do not assign any access rights to the User. This makes the user effectively unusable from a PC Client application for security.

1.3 Custom Field Changes

You may choose the fields to be used, for example **String 8** for a Character field, and the field labels (the tables below contains suggested values). You will use the **User Settings** Administrator options (see page 3) to define which fields you have selected, which will offer the field labels you have selected.

User/Department record changes for Web access control

Red Box on the Net uses custom fields in the User/Department record to identify users when they log in, and to implement access controls. You will need to create field changes to bring three custom fields into use. One of the fields needs a picture validator to be defined.

Picture Validator

Name	Picture	Message
Numeric	*{9}	Value must be numeric

Field Changes

Field Type	Suggested Field	Field Label	Picture	Encodes To	Lookup Values
Character	String 8	Max Logins	Numeric		
Lookup	Lookup 2	Controlling User		User/Department record	
Lookup	Lookup 4	NetID Type		Lookup Value	Personal Manager Red Box User

Problem Report record changes for Known Errors

You may not wish to make all existing Known Error data available to Customer users, so Red Box on the Net uses a custom field in the Problem Report record to indicate whether the record should be 'published'.

Field Changes

Field Type	Suggested Field	Field Label	Picture	Encodes To	Lookup Values
Lookup	Lookup 1	Publish KER		Lookup Value	Yes No

Implementing the changes

1. Create the **Numeric** picture validator
2. Create all the Field Changes and make them Ready.
3. Accept the changes
4. At a convenient point, reload the Red Box Server
5. Set up Field Mappings for the User/Department custom fields
6. Create Lookup Value records for the **Publish KER** and **NetID Type** fields

Note: For more information about creating field changes, refer to the Red Box Help system.

From the PC Client application, go to **Help | Contents**, and then navigate to the **Administration Application | Field Changes** section

2. Install Red Box on the Web software

Inserting the CD should 'auto-start' the installation program. Follow the on-screen instructions.

The Default directory for installing the software is:

```
C:\Inetpub\FoxIT\RedBox300c
```

Towards the end of the installation, you will be prompted for .INI file Server Settings. You will need to supply:

- the IP address and port number for you Red Box server
- the name of the server you are installing the software on
- the Web Server ID (used for licence checks and to construct the username to be used to establish a database connection):

For example:

```
Red Box Service Name      = 192.181.20.30
Port                      = 7300
Server Name               = RBWEB
Web Server ID             = 1
```

3. Add a Domain Name Server (DNS) entry

You must decide on the domain name to be used in the URL for Browsers to access Red Box on the Net, for example:

RedBox.MyCompany.com

You will then need to update your DNS with a mapping from this domain name to the IP address for the Web Server.

4. Configure the Web Service

You are now ready to create a new Web Site using the Microsoft Management Console for IIS. The exact details of how you do this vary slightly, depending on the version of IIS you are running.

4.1 IIS 4.0

1. Start MMC
2. Under Internet Information Server, select the host computer entry
Choose **Action | New | Web Site** to start creation Wizard.
3. Fill in the Web Site Description, e.g. Red Box 3.00c, choose Next
4. Accept the default IP address/port settings, choose Next
5. Browse to the directory where you installed Red Box on the Net, default:
C:\inetpub\FoxIT\RedBox300c.
Leave Allow anonymous access set and choose Next
6. Check access permissions for Read, Script and **Execute**; choose Finish
7. Select Properties (Tool bar or Right Mouse Button) for this new service (currently Stopped)
8. On the Web Site tab, choose the IP Addresses **Advanced...** button
Select the Multiple identities for this Web Site All Unassigned port 80 entry;
Choose Edit
Supply your chosen Host Header Name (the domain name you will supply in the Browser URL), for example Host Header **RedBox.MyCompany.com** if the URL is to be <http://RedBox.MyCompany.com>
choose OK, and choose OK on the **Advanced ...** tab to return to the property sheets screen.
9. On the Home Directory tab, Application Settings: check the **Run in separate memory space (isolated process)** box. Choose the Configuration button.
On the App Mappings tab, choose Add.
Use the Browse button to locate the WBIS300c.DLL (change file type in the dialog to .DLL); default location is C:\inetpub\FoxIT\RedBox300c. Supply .RBX as the Extension, and choose OK.
Choose OK on the App Mappings tab to return to the property sheets screen.
10. On the Documents tab, choose Add and type default document name **home.htm**.
Choose OK, and then use the up arrow to move this entry to the top of the list.
11. Choose OK to complete configuration of your Web Site.
12. **Start** the Web Site running (Tool bar or Right Mouse Button)

4.2 IIS 5.0

1. Start MMC
2. Under Internet Information Server, select the host computer entry
Choose **Action | New | Web Site** to start creation Wizard.
Choose Next.
3. Fill in the Web Site Description, e.g. Red Box 3.00c, choose Next
4. Accept the default IP address/port settings.
In the Host Header for this site: enter the domain name you will supply in the Browser URL, for example Host Header **RedBox.MyCompany.com** if the URL is to be <http://RedBox.MyCompany.com>
Choose Next
5. On the Web Site Home Directory screen, browse to the directory where you installed Red Box on the Net, default: C:\inetpub\FoxIT\RedBox300c.
Leave Allow anonymous access set and choose Next
6. On the Web Site Access Permissions screen. check access permissions for Read, Run Script and **Execute**; choose Next and then Finish
7. Select Properties (Tool bar or Right Mouse Button) for this new service (currently Stopped)
8. On the Home Directory tab, Application Settings: set Application Protection to **High (Isolated)**
Choose the Configuration button.
On the App Mappings tab, choose Add.
Use the Browse button to locate the WBIS300c.DLL (change file type in the dialog to .DLL); default location is C:\inetpub\FoxIT\RedBox300c.
Supply .RBX as the Extension, and choose OK.
Choose OK on the App Mappings tab to return to the property sheets screen.
9. On the Documents tab, choose Add and type default document name **home.htm**.
Choose OK, and then use the up arrow to move this entry to the top of the list.
10. Choose OK to complete configuration of your Web Site.
11. **Start** the Web Site running (Tool bar or Right Mouse Button)

5. Set Web Server Defaults

Start a Red Box on the Net session from your browser using the Host Header you supplied when configuring the Web Service, for example <http://RedBox.MyCompany.com>.

Login to a user with FULL (Administrator) access rights, and choose each of the Administration menu option in turn:

- System Settings
- User Settings
- Incident Settings
- RFC Settings
- History Mask

*N.B. You may refer to the Red Box on the Net context sensitive Help information available for each screen (**Help** button at top right of each page) for an explanation of the option settings.*

Choose the **Submit** button to save the changes on each page visited. The new settings are effective immediately; you do NOT need to reload the Web Server or the Red Box server.

5.1 System Settings

Consider carefully the values you choose for:

TIMEOUT_MINS	this is the period after which an inactive session may be re-used by another user.
RETRIEVAL_LIMIT	This limits the number of records a user may retrieve, thus limiting his impact on other users on the same Web Server, as well as limiting the total Red Box server loading.
EMAIL_ADMINISTRATOR	This is the Email address used for the Contact Administrator link provided at the bottom of every page

For more information about the format strings to be entered for the Display Control section, go to the Red Box Help system, **Help | Search** and search for keyword **formats**; in the list of topics you will find **Date formats** and **Number formats**, which include specifications and examples.

5.2 User Settings

This is where you define which custom fields (see page 3) are to be used to control users' access to Red Box on the Net. Select the relevant field names from the lists provided.

5.3 Incident Settings

Before Customer users can submit incident reports, you must supply Incident Report-creation field values for the fields they do not supply. These values are set on the Incident Settings screen.

Each setting must reference an existing Help Desk record, created using the PC client; use the '?' buttons to select from lists of valid records.

These values will be used to complete any mandatory fields not implicitly supplied by the selected Prefix defaults (Customer and Operator users), or not explicitly set (Operator users).

Incident field	IR-creation settings
Method General Category Team	<p>In these fields, enter the names of the method, general category and Help Desk team to be assigned to all incidents created by Customer users.</p> <p>For Customer users, the fields are not displayed on the New Incident Report screen.</p>
IR prefix	<p>Specify the prefix to be displayed as the default on the New Incident Report form, if no other value is set by the Prefix Selection option (below). All prefixes available for selection must have Auto Sequence = Yes.</p>
Prefix Selection	<p>Select None, or select one of the following options to make alternative IR prefixes available to incident submitters.</p> <ul style="list-style-type: none"> • 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. • 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)	<p>The New Incident screen offers these Impacts for selection if no Impacts can be derived from the selected IR Prefix defaults.</p> <p>Impacts must have Enable Use on IR Create set</p>

5.4 RFC Settings

Before web users can submit RFCs, you must supply RFC-creation field values for the fields they do not supply. These values are set on the RFC Settings screen.

Each setting must reference an existing Change Management record, created using the PC client; use the '?' buttons to select from lists of valid records.

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 screen. The prefixes must have Auto Sequence = Yes
Initial status	The RFC has this status code before its processing starts (that is, while its status type is Not Started). The New RFC screen does not show the status code, but the one specified here will be passed to all web-created RFCs. You must choose a status code that is associated with the Not Started RFC status type.
Impact <i>(supply up to 3)</i> Priority <i>(supply up to 3)</i>	The New RFC screen offers these Impacts and Priorities for selection In order for web users to submit new RFCs, the RFC Settings must supply at least one Impact and one Priority.

5.5 History Settings

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 on the History Settings 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) Click on 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) Click on the Custom button.

6. Prepare your Red Box Service (Part 2)

6.1 Users

Red Box on the Net users are identified at login as being one of two User Types:

User Type	Allowed Usage
Operator	This refers to users logging in using their own Red Box User name, which would also allow them access via the full PC Client application. Subject to normal access rights and domain checks, they will be allowed to view and amend Incident Reports via their HD Team membership, and to create Incidents for submitters other than themselves
Customer	There are two types of Customer Net user: <ul style="list-style-type: none"> • Personal Personal users are restricted to viewing or amending Incidents for which they are the Submitter, or which were submitted from their Location. Their amendment options are strictly limited (Add Symptoms, Withdraw or Resolve) • Manager Managers may view a wider range of Incidents that their domain allows. They have some extra amendment options for Incidents (Add History, Change Impact).

The Username supplied at login is, at first, assumed to be a User/Department record name.

If a matching record is found with a non-blank Controlling User custom field, this controlling Red Box User is used for completion of the login, and the User Type field determines whether this is a Personal, Manager or Red Box User (Operator).

If no matching User/Department record is found, the Username is then assumed to be a Red Box User name. If a matching Red Box User is found, this is used to complete the login procedure. In this case the User Type is set to Operator.

6.2 Access Rights and Domains

Red Box on the Net uses the standard Red Box Access Rights and Domains, if implemented, to restrict data available to users. It does this in two ways:

Menu Options If a user does not have the requisite access rights for an action, that option is not offered on the menu. For example, a user who does not have **Insert** access rights to **RFC Details** records is not offered the **New RFC** menu option.

Selected Data When selecting records to view, the user's selection criteria are supplemented by any Domain constraints.

When viewing a record, clicking on a field value link may result in a 'No data found' or 'Access Denied' error message.

You may wish to set up new Access Rights records, specifically for Web access, to be used by the Controlling Red Box Users for **Personal** and **Manager** customer users.

6.2 Default Settings for Users

The Administrator settings have Web Server-wide scope. They are really provided as a 'catch-all' to supply suitable values for the creation of an incident report or RFC, where the user does not supply all the values necessary for the mandatory fields.

You may wish to have different default values for individual users, or groups of users. This may be achieved by using prefix defaults and/or domaining.

Prefix Selection

The Administrator settings for IR and RFC **Prefix Selection** options allow you to control which Prefixes are offered to users for Incident and RFC creation.

For example, if you have a group of users at location **BRISTOL**, and you would like all their incidents to be created with a Prefix **BRS1**, you could:

- ❑ set the Prefix Selection administrator option in Incident Settings to:
Prefixes with user's location as default
- ❑ create a Prefix record **BRS1** with the default location set to **BRISTOL**
- ❑ ensure that the User/Department records for all users in the group have location **BRISTOL**

If you created further Prefixes with default location **BRISTOL**, these would also be offered on the New Incident screen.

Note that, in the example above, if there are no Prefix records with default location **BRISTOL**, then the default IR Prefix from the Incident Settings administrator option will be the only Prefix offered on the New Incident screen.

Prefix Defaults

Much of the processing associated with the **New Incident** facility is governed by the selected Prefix, and the default values it conveys for General Category, Team, Impact and so on.

Customer users	Changing the selected Prefix may cause the list of Impacts to be changed, depending on the Prefix defaults.
Operator users	Initial values offered on the New Incident screen are taken from the Prefix defaults; changing the selected Prefix will cause other fields to be updated with Prefix default values. The lists of values offered for '?' buttons will be governed by the Prefix defaults.

When setting the **Incident Settings** administrator options, you should bear in mind the restrictions that may be imposed by the defaults settings for the IR Prefix record selected in **IR_PREFIX**.

For example, if **Links Only** has been specified in its General Category defaults, make sure that the default General Category specified on the Incident Settings (**IR_GEN_CAT**) is one of the links visible under **General Category Links**.

Similarly, you should ensure that the default Team (**IR_HD_TEAM**) and Impacts (**IR_IMPACT_1**, **IR_IMPACT_2**, and **IR_IMPACT_3**) in the Incident Settings are visible under the **xxx Links** button for the corresponding default setting **IR_PREFIX** record.

Domaining

If you have the Red Box Domains module, you may want to place controlling Red Box Users in a domain which restricts their access to certain database records.

Key fields for domaining are as follows:

- Prefix
- Location
- General Category

7. Server Administration

7.1. Microsoft Management Console

The Red Box on the Net Web Server is started and stopped using the Microsoft Management Console (MMC) of the Internet Information Server (IIS).

The MMC provides controls to **Stop** and **Start** the Web Service. These are provided as VCR-style toolbar controls, and on the Right Mouse Button (RMB) menu options. When the service is stopped, it refuses page requests from browsers; when started again, requests are processed as normal. The first page request received after the service is loaded causes it to establish the database connection to the Red Box Server; this causes a short delay in processing this first request.

Additionally (for IIS 4.0 only) you may need to use the **Unload** option. This button is found in the service Properties (toolbar or RMB), on the Home Directory tab. When you unload the service, all current sessions are terminated and the connection to the Red Box Server is closed. The **Unload** action is implicit when you **Stop** the service on IIS 5.0.

Red Box Server database connection

You may wish to stop (and unload if necessary) the Web Service when you want to shut down the Red Box Server, for example when performing a backup. However, this is not essential, as the Web Service is resilient to loss of connection to the Red Box Server.

This first page request received after loss of connection will receive an error message indicating that the connection to the Red Box Server has failed, and offering a link to retry.

The first page request received after the Red Box Server has been restarted will cause the database connection to be re-established (again, this causes a short delay in processing this request).

7.2 Amending Controlling Users and Max Logins

Information about Controlling users, User Types and concurrency limits (Max. Logins) for users is cached in the Web Server for efficiency. Any changes you make to these settings in the Red Box database will not be implemented by the Web Server until it is next reloaded (Stop/Unload and Start using MMC, or use the **Reload Server** button on the **View Slots** administrator menu option).

7.3 Initialisation File Settings

Red Box on the Net Web Server installation creates an initialisation file, **RedBoxNet.ini**, containing the values you supplied during installation and skeleton entries for other options.

You will have set values most of the other options when you followed the instructions in the Set Web Server Defaults section (see page 3).

[RedBoxNet] Section

The values for `ApplicationID`, `ServiceName`, `Port`, and `PCId` were set initially during Installation.

If your Red Box server address details change you will need to amend the `ServiceName` and `Port` settings.

You may need to change the `ApplicationID` setting if your Red Box licence details change for the relevant **WB0n,<slots>** option (The `ApplicationID` value must correspond with 'n' in **WB0n**)

The `Heartbeat` setting (seconds) controls the frequency of 'keep alive' messages sent to the Red Box server to prevent the connection being timed-out.

The `LogFileGens` setting controls how many log files are created. For example, a value of 3 will generate log files with the filenames **RedBoxNet.000**, **RedBoxNet.001** and **RedBoxNet.002**. The next log file generated would overwrite **RedBoxNet.000**.

```
[RedBoxNet]
ApplicationID=0
Heartbeat=120

LogFileGens=5
NextLogFileGen=1
LogFile=RedBoxNet.LOG

;rbmhFile=dcmess.tab
;TextFile=text.tab

ServiceName=RedBoxServer
Port=RedBoxPort
PCId=ServerName
```

[Cache] Section

The Red Box on the Net Web Server caches system information, in the same way as a PC Client application can. You should not change these settings, as you will adversely affect the performance of the server.

```
[Cache]
Cacheall=1
Path=Cache
Update=Yes
```

Other Sections

Settings in the following sections should only be amended using Red Box on the Net Administrator menu options. The values were set initially during the Set Web Server Defaults section (see page 3). **Do not attempt to make changes directly to these sections of the initialisation file.**

```
[System]
[User]
[Help Desk]
[Change Management]
[History]
```

7.4 Troubleshooting

General

The Red Box System Administrator's Guide gives general troubleshooting guidance. In this context, the Red Box on the Net Web Server appears to the main Red Box server as just another client connection (like a PC Client), so diagnosing problems is very similar from the server point of view.

Log Files

Red Box on the Net maintains a sequence of log files (**RedBoxNet.nnn**) in the 'Home Directory' configured for the Web Service. By default, the tracing level for the Web Server is set to **Minimum**. You can increase this to **Maximum** using the System Settings administration menu option. Any change you make to this setting is reflected immediately in the trace file - you do not need to reload the Web Server.

Note: Timestamps on messages in the trace file are Red Box database server times.