

Reference Guide

D301532X412

April 2012

OpenEnterprise Security Manager Reference Guide (V2.83)

Remote Automation Solutions

Website: www.EmersonProcess.com/Remote




Contents

1	Security Manager	1
1.1	Main Dialog	1
1.1.1	File Menu	2
1.1.2	Edit Menu.....	2
1.1.3	View Menu	2
1.1.4	Help Menu	3
1.1.5	Toolbar.....	3
1.1.6	Security Database	3
1.1.7	Fallback Databases	3
1.1.8	Connected	4
1.1.9	Active Database	4
1.1.10	Current User.....	4
1.1.11	Location.....	4
1.1.12	Administrative User	4
1.2	Property Page	4
1.2.1	Show System Tray Icon.....	4
1.2.2	Show Window	4
1.2.3	Minimized.....	5
1.2.4	Hide on Minimize	5
1.2.5	OK Button	5
1.2.6	Cancel Button	5
2	Index	6

1 Security Manager

The Security Manager component provides security on an OpenEnterprise Workstation. It is started automatically when any OpenEnterprise component is invoked. Once started, it remains running until the Workstation is closed down. The Login Client passes login requests to the Security Manager, which then negotiates the login request to the database. The Security Manager then informs all OpenEnterprise Workstation components (Desktop, Views and Toolbox) of the current user's security status.

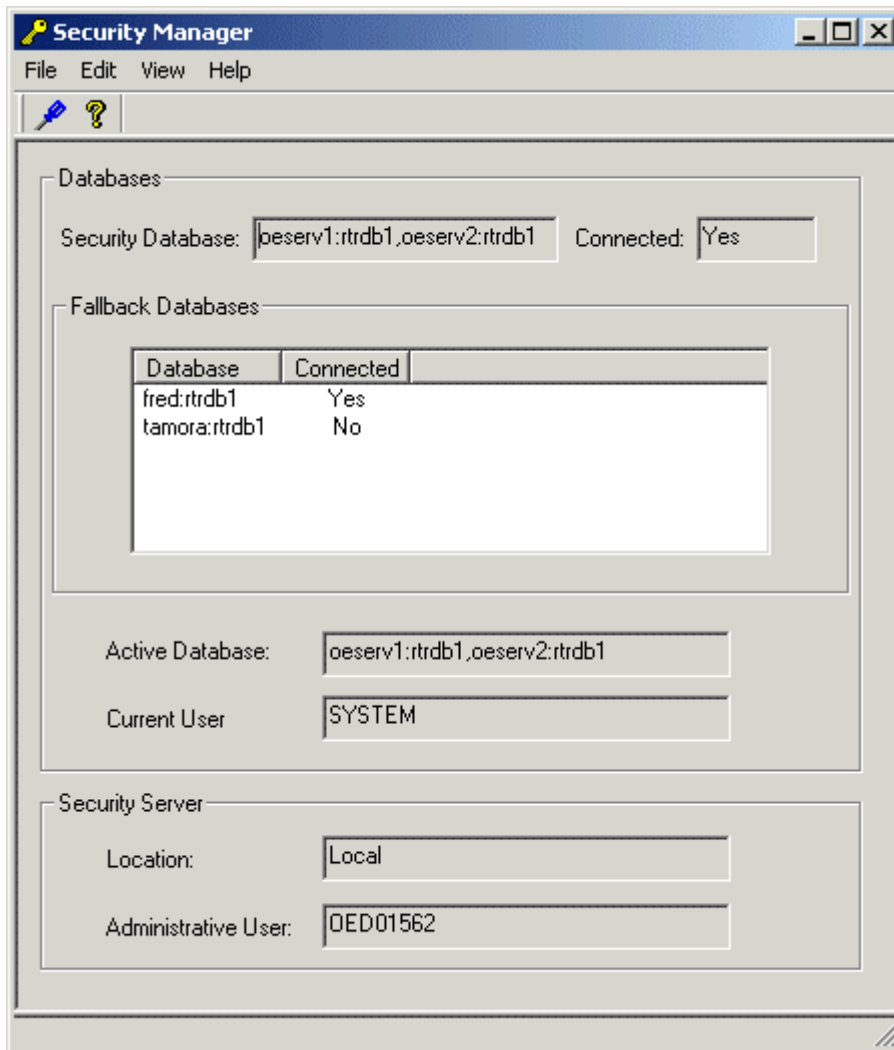
Whilst the Security Manager is running, it displays a System Tray icon -  that reflects its current database connectivity status by means of different border colors: -

- A Green border indicates that the security Manager is connected to the Security Configuration database.
- Cyan indicates that it is currently connected to one of the Fallback databases.
- Yellow indicates that it is using it's internal cache to satisfy any security requirements of the Workstation.
- Red indicates that it has never managed to connect to either the security configuration database or any fallback databases.

Double click on the Security Manager's icon to open it's User Interface (UI). This provides information and the ability to configure the behaviour of the UI.

1.1 Main Dialog

The Security Manager provides information concerning its connectivity to the designated Security database and any Fallback database that may have been configured. It also displays the name of any Currently logged in user, the location of the Security Manager, and the Administrative user being used by the Security Manager to obtain security information.



1.1.1 File Menu

The File Menu provides an option to Exit the application. This will cause the application to close as a Windows process if the Security Manager is not currently supplying data to a client, but if it has a subscribing client, it will hide itself, but remain running as a process. The UI can be invoked again by double clicking on its icon in the System Tray.

1.1.2 Edit Menu

The Edit Menu provides an option to open the Properties dialog, which enables the user to configure pre-connect databases and the way that the UI behaves.

1.1.3 View Menu

There are two options available from this menu: -



1. **Toolbar** - when checked, the toolbar is visible under the Menu bar.
2. **Status Bar** - when checked, the Status Bar is visible at the bottom of the Main Dialog window. It displays information on the current status of the Security Manager.

1.1.4 Help Menu

This provides an option to open the About dialog, which provides information on the version and build of OpenEnterprise being used and contact information.

1.1.5 Toolbar

This contains two icons: -

- Properties icon  - selection opens the Security Manager Properties dialog.
- About icon  - selection opens the About dialog, which provides information on the version and build of OpenEnterprise being used and contact information.

1.1.6 Security Database

This is the default Security Database. It is stored in the data for the *Database* value, found on the *OpenEnterprise\Tasks\OESecurityManager* key in the OpenEnterprise settings file. This value is defined when OpenEnterprise is installed. This key and its value can be viewed with the OpenEnterprise Settings Editor, although it should normally never be changed.

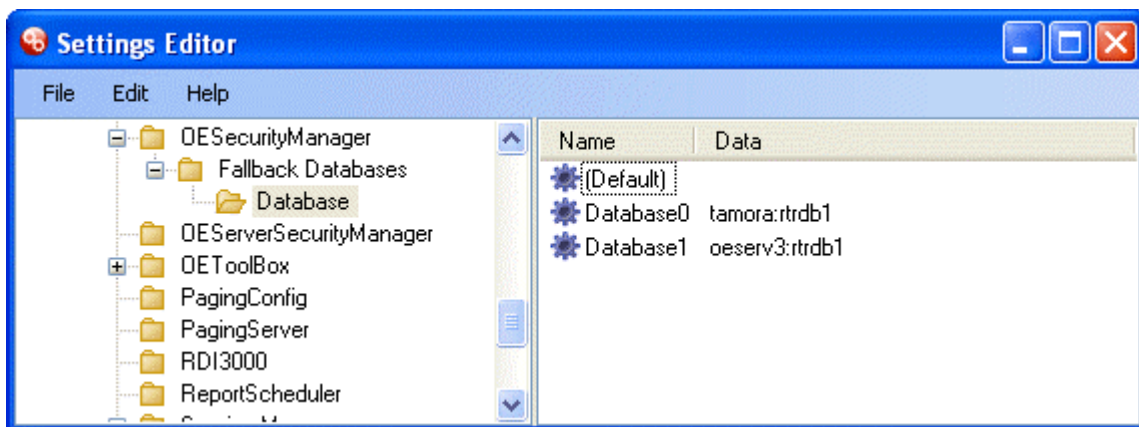
The Security Manager always attempts to connect to this database first to retrieve security information. If the database is unavailable, it will then attempt to connect to any configured fallback databases. If none of these is available, and it has been running before, the Security Manager will use its internal cache to provide security information.

Back

1.1.7 Fallback Databases

All configured fallback databases will be listed here, together with their connection status. Fallback databases have to be configured manually by creating a new key under the *OpenEnterprise\Tasks\OESecurityManager* settings key. This key can be viewed and modified with the OpenEnterprise Settings Editor.

The new key must be called *Fallback Databases*. Then another key is created under this, called *Database*. Then, on this key, string values named *Database0*, *Database1* etc should be created and the Value data should contain the data source string for each fallback database (i.e *oeserv3:rtrdb1*). Here is an example:-



Back

1.1.8 Connected

Gives the connection status of the Security Manager to the defined Security Database.

1.1.9 Active Database

Displays the currently active database. This is the database that is being used by the Security Manager for security information.

1.1.10 Current User

Displays the user currently logged into OpenEnterprise on the Workstation.

1.1.11 Location

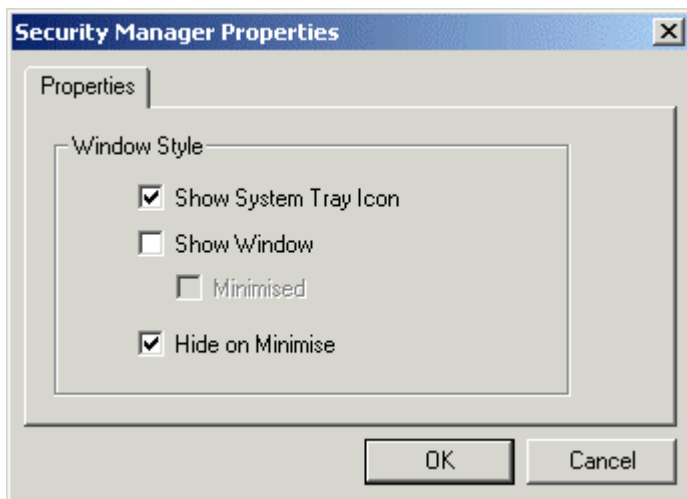
This will normally say 'Local'. It refers to the Iconics Security Server, which usually runs on the local machine. The Workstation Security Manager updates the Iconics Security Server with security information on the logged in user. This is then used by the Iconics Security Server to control access to functions and objects within OpenEnterprise Graphics.

1.1.12 Administrative User


The Administrative user being used by the Security Manager to login to the Iconics Security Server to provide security information for OpenEnterprise Graphics.

1.2 Property Page

This tab on the Property dialog enables the user to configure the way that the Security Manager User Interface behaves. Changes are implemented when the user selects the **[OK]** button at the bottom of the Properties dialog.



1.2.1 Show System Tray Icon

When checked, the Security Manager's icon -  will be displayed in the System Tray when it is running. Double clicking on this icon in the System Tray will open the User Interface.

1.2.2 Show Window

When checked, the Security Manager's User Interface will be displayed on startup.

1.2.3 Minimized

When the *Show Window* box is checked, this option becomes enabled. If checked, on startup the Security Manager's User Interface will be displayed as a minimized icon on the Windows Task Bar.

1.2.4 Hide on Minimize

If checked, when the Security Manager's User Interface is minimized, it will also be hidden. If the *Show System Tray Icon* box and *ShowWindow* boxes are unchecked at the same time that this box is checked, then at startup the Security Manager's User Interface will not be available.

The interface may be restored by using the Settings Editor to manually change the *ShowtrayIcon* value on the *OpenEnterprise\TasksNotes Client Server* key to 1. A restart will be necessary before the change takes effect.

1.2.5 OK Button

When this button is selected, changes made to any tab are saved, and the Property dialog is closed. Changes will be applied immediately.

1.2.6 Cancel Button

When this button is selected, the Property dialog is closed without saving any changes made on either tab.

2 Index

A

Active Database 5
Administrative User 6

C

Cancel Button 7
Connected 5
Current User 6

E

Edit Menu 4

F

Fallback Database 5

G

General Tab 6

H

Help Menu 4
Hide on Minimize 6

L

Location 6

M

Main Dialog 3
Minimized 6

O

OK Button 7

S

Security Database 5
Security Manager Overview 3
Show System Tray Icon 6
Show Window 6

V

View Menu 4

Reference Guide

D301532X412

APRIL 2012

DISCLAIMER

Bristol, Inc., Bristol Babcock Ltd, Bristol Canada, BBI SA de CV and the Flow Computer Division, are wholly owned subsidiaries of Emerson Electric Co. doing business as Remote Automation Solutions ("RAS"), a division of Emerson Process Management. ROC, FloBoss, ROCLINK, Bristol, Bristol Babcock, ControlWave, TeleFlow and Helicoid are trademarks of RAS. AMS, PlantWeb and the PlantWeb logo are marks of Emerson Electric Co. The Emerson logo is a trademark and service mark of the Emerson Electric Co. All other marks are property of their respective owners.

The contents of this publication are presented for informational purposes only. While every effort has been made to ensure informational accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. RAS reserves the right to modify or improve the designs or specifications of such products at any time without notice. All sales are governed by RAS' terms and conditions which are available upon request. RAS does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any RAS product remains solely with the purchaser and end-user.

Engineered and supported by:

Remote Automation Solutions,

Blackpole Road, Worcester, WR3 8YB, UK

Registered office: Meridian East, Leicester, LE19 1UX

Registered in England and Wales, Registration No. 00671801

VAT Reg No. GB 705 353 652

Emerson Process Management
Remote Automation Solutions
1100 Buckingham St
Watertown, CT 06795
T 1 (860) 945 2200
F 1 (860) 945 2278
www.EmersonProcess.com/Remote
binfo@EmersonProcess.com

Emerson Process Management
Remote Automation Solutions
Blackpole Road
Worcester, WR3 8YB
T 44 (0) 1905 856848
F 44 (0) 1905 856930
www.EmersonProcess.com/Remote
oedsupport@EmersonProcess.com

