

Oracle Forms - General

The Oracle Forms analyzer provides configuration settings to customize the monitoring of software services based on Oracle Application Server.

In the RUM Console, open the **AMD Configuration** window. Under **Configuration**, select **Global Front-End Monitoring Oracle Forms General** and tune the following Oracle Forms monitoring settings:

Generate ADS data for Oracle Forms traffic

Select this option to provide data to the report server that consists of low-level protocol information, such as raw HTTP traffic data, which enables you to view the full HTTP request-response dialog.

Unknown macro: 'scroll-ig'

Unknown macro: 'scroll-ig'

Oracle Forms Identification

Session identifier

This property defines a pattern used for identification of the session ID, which is required for Oracle Forms session recognition and stability.

You can find the session ID in the URL parameter of the POST request for a Forms servlet. Examples of a POST request for a Forms servlet include:

- POST/forms/lervlet;
- POST/forms/formsservlet;
- POST/forms/I90servlet;

Typically the identifier name (note that this is not the ID value) required by the AMD is `jsessionid` or `JServSessionIdforms`, as shown in the following graphic:

```
HTTP/1.1 200 OK (text/html)
Server: JBoss/1.4.0-GA-20051214
Expires: Wed, 11 Jan 1996 08:00:00 GMT
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/javascript
```

The default RUM Console setting is `jsessionid=`.

User Recognition

The following parameters listed under **User Recognition** enable you to use a login user name as the basis for reporting.

Login method

Specify the request method for the login URL using one of the following methods:

GET or POST

Used for user login detection in web traffic. This setting defines an HTTP method in a request that contains a client username. The available values are: `GET`, `POST`, or no entry.

OFLogin

Used for user login detection in an Oracle Forms binary stream. Select this option to configure user detection based on Oracle Forms internal login. Selecting `OFLogin` disables the **Login URL** parameter.

ICXLogin

Used for user detection in an Oracle Forms 6i mixed environment where the user login exists in web traffic and the Oracle Forms session ID exists in a pure binary stream. To produce the user name of the

Edit Rule

Software service: of-tcp-mytest; Analyzer: Oracle Forms over TCP

Services | User recognition | Oracle Form Monitoring | Availability | Options

Enabled

Rule description

IP Address	Ports	Group
10.170.20.35	9000	
10.170.20.35	8002	
10.170.20.36	9000	
10.170.20.36	8002	
10.170.10.242	8000	

Oracle Forms Servers (red bracket pointing to 10.170.20.35 and 10.170.20.36)

Web Server (blue bracket pointing to 10.170.10.242)

Oracle Forms operation, add web server and all Oracle Forms servers when defining services in the software service rule configuration, as shown in the following graphic. both the

The web traffic contains the user login and ICX Ticket data, and the Forms binary traffic contains a corresponding ICX ticket, which is used to associate the user login contained in the web traffic with the data in the Oracle Forms binary stream:



Note:

Another method for identifying user names for traffic data records that do not have an associated user name is to configure the CAS to map the monitored user's name between analyzers for a given client IP address.

Login URL

Defines the URL in an HTTP request containing a client username.

For an HTTP-based login, the login URL is the base URL where the username value is found in the trace file.

For an Oracle Applications/EBS login, the login URL is typically /OA_HTML/OA.jsp/.

This field is redundant when extracting the user name directly from Oracle Forms traffic, so it is disabled if the **OFLogin** method is selected.

Login name parameter

This property is used for searching for a user name in HTTP requests.

For an HTTP-based login, this is the POST parameter key for the username found in the login URL. It typically has a value containing a username string.

For an Oracle Applications/EBS login, the username key is typically `usernameField`.

For a Forms-based login, this is the label used for the username in the Forms login. Typically, this value is `username`.

Identification cookie pattern

This property helps to identify the cookie used for user assignment. Setting this properly helps AMD software match user names to TCP sessions.

For an HTTP-based login, this is the cookie key for a Forms session. Typically, it follows the `JSessionID` cookie for the login URL in the capture file, and the same cookie key is also found in the POST request for the Forms servlet.

For an Oracle Applications/EBS login, the key is usually customized.

For a Forms-based login, this is the cookie key for a Forms session. Typically, it is `JSessionID`.

Default: `JServSessionIdroot`

The sample login URL show the configuration parameters for the login URL, request method, user name parameter, and the key for the HTTP cookie for the Forms session.

After configuring the **Error Messages** table, you must enable the availability of an error category on the **A** **availability** tab to view error message data in DMI reports. For more information, see [Oracle Forms - Availability](#).

Thresholds

When you configure Oracle Forms monitoring, you are able to define operation time thresholds on several levels starting from general settings of the analyzer, through per software service, to a per individual operation level. Note that global setting **Page load time/operation threshold** is ignored for Oracle Forms monitoring.

Operation timeout

The maximum time that a single operation should last. An operation with a longer execution time is regarded as unsuccessful or broken. Increase the value of this option if your Forms application response time is slow.

Default value: 1 second.

From what we saw in the real traffic, the default value should be suitable for most scenarios. We do not recommend decreasing it. Increasing it to two seconds could prove useful in some very rare cases. Oracle Forms protocol carries only basic UI updates and to assemble real user actions from this, AMD analysis needs to rely on heuristics, which makes the timeout value an important aspect in the process.

Session state timeout

How long (in seconds) a session ID is regarded as valid and recognized by the analyzer.

Default value: 28800 seconds (8 hours).

Max. length of property

The maximum length of a text string that is send in a binary Oracle Forms message.

Default value: 20000 bytes.

Operation Pattern Matching and Processing

Operation pattern matching may be the key to understanding and debugging your Web applications. Setting all the parameters related to this issue will enable better presentation of the data by the report server. With them, you can see the actual relations between particular components of your Web application.

Operation name pattern

Use this field to influence how the content of a transaction name is formed. This string must contain keywords that will be replaced with real values. They can be used in any order and separated by any characters. Note that these keywords are case sensitive.

The following keywords are supported:

- `%parentTitle%` - window title of the previously active window
- `%resultTitle%` - window title of the new window
- `%controlTitle%` - the name of the control (for example, button's caption)
- `%className%` - the type of the control (for example, `ButtonItem`)
- `%propName%` - action (for example, `pressed`)
- `%moduleName%` - the name of the module in use

Default: `%parentTitle%\t%resultTitle%\t%className%:%controlTitle%`

Figure 1. Sample Oracle Forms operation name pattern recorded on the AMD

```
PT:Work Request Submission RT:Work Request Submission CT:Save CN:
ButtonItem PN:pressed
```

`%moduleName%` Processing

Use this setting to include a module's path or extension in reports. Note that this property is not part of the default configuration.

`%parentTitle%` Processing

These settings make it possible to transform a parent title. An extended POSIX regular expression (entered in the **Regex Pattern** column) matches the parent title and allows the selection of only a part or parts of the title for further processing (using grouping subexpressions). **Output Pattern** describes how to assemble the pieces matched by **Regex Pattern**. This is a string that may contain back references (backslash character “\” followed by a non-zero decimal digit) to subexpressions matched and grouped in **Regex Pattern**.

The following setting removes everything from the `%parentTitle%` from the “(” character to the end:

Regex Pattern: `(.+)\(`

Output Pattern: `\1`

If the parent title were `PT:Fiscal Report Submission (RNO-975310)`, after this transformation you would have `PT:Fiscal Report Submission`.

Several instances of this property are allowed. Default: no action.

%resultTitle% Processing

Similarly to **%parentTitle% Processing**, this property makes it possible to transform the new window's title. An extended POSIX regular expression (entered in the **Regex Pattern** column) matches the parent title and allows the selection of only a part or parts of the title for further processing (using grouping subexpressions). **Output Pattern** describes how to assemble the pieces matched by **Regex Pattern**. This is a string that may contain back references (backslash character “\” followed by a non-zero decimal digit) to subexpressions matched and grouped in **Regex Pattern**.

The following setting regroupes `%resultTitle%` components so that the requested strings appear first, although they are detected in a different order:

Regex Pattern: `([^\]*) ([^\]*) ([^\]*)(.*)`

Output Pattern: `\3 \1 \2 \4`

If the result title were `RT:Work Request Submission Illegal x00AF`, after the transformation you would have `RT:Illegal Work Request Submission x00AF`.

Several instances of this property are allowed. Default: no action.

See [Regular Expression Fundamentals](#) to learn more on using regular expressions in Data Center Real User Monitoring configuration tasks.

