

An Oracle White Paper
March 2011

Security Best Practices with Oracle Real User Experience Insight Release 11g

Introduction	3
Oracle RUEI	3
Non-intrusive Data Collection	3
Deployment Options	5
Operating System Requirements	5
Accounts	6
RUEI Configuration Settings	6
Linux OS Account	7
RUEI Super Administrator Account	7
Database Account	7
Web Server Access	7
Password Security Enforcement	8
LDAP Server User Authentication	8
SSO Server User Authentication	8
SSL Private Keys	9
Role-Based Security	9
Data Masking	11
Cookie Hashing	12
Enriched Data Exchange Facility	12
Export Report Data	13
Conclusion	13

Introduction

Customers, regulators, business partners and internal security officers can be confident that Oracle RUEI's offers the benefits of cutting-edge Real User Monitoring (RUM) technology, but without compromising security. It is based on a robust and proven security model that minimizes risk, and offers powerful controls to those responsible for security and compliance. This document highlights the recommended security practices to be followed when using Oracle Real User Experience Insight (RUEI) Release 11g to monitor network traffic.

Oracle RUEI

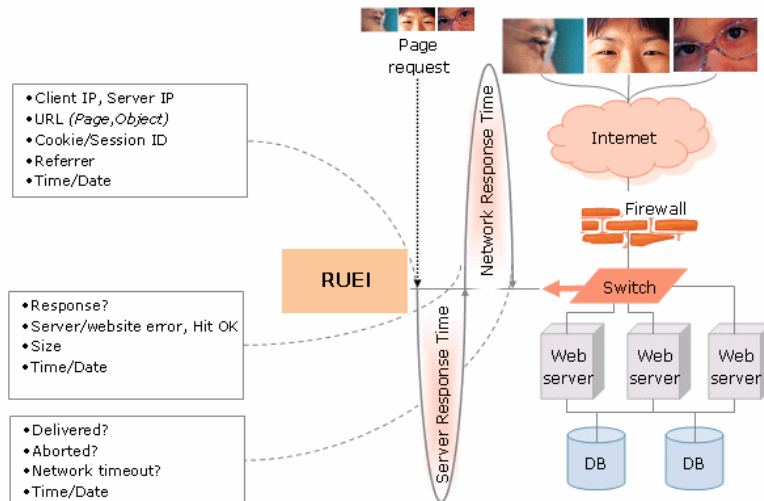
Oracle RUEI moves service delivery monitoring from the Data Center's perspective to the end-users' perspective. Its ability to see what the organization's end-users experience, together with its powerful reporting facilities, enables direct insight into every customer-facing component (such as webservers, load balancer, caching servers, reverse proxy servers, and so on) of even the most complex infrastructures, and delivers an information foundation that meets the needs of both IT and business users.

In most common deployment scenarios, Oracle RUEI is deployed completely "on premise" in the Data Center and, therefore, is easily integrated within the organization's security regulations and policies.

The rest of this document describes the security framework within which it operates. In particular, how Oracle RUEI delivers a leading-edge RUM solution that is 100% non-intrusive, and incorporates and facilitates security management best practices.

Non-intrusive Data Collection

Typically, Oracle RUEI is installed in front of the webservers, behind a firewall in the DMZ. The data collection method is based on Network Protocol Analysis (NPA) technology, and connection to the monitored environment is via a TAP or copy port. This method is 100% non-intrusive. Hence, it does not place any load on a webserver, or require installing software agents that will impact performance. In addition, it usually does not require any change to the current application or infrastructure. When a new application release is deployed, or when an additional webserver is added, there is no or very little change required to Oracle RUEI's monitoring environment.



When an object is requested by a visitor, Oracle RUEI sees the request and measures the time the underlying Web infrastructure requires to present the visitor with the requested object. At this point, Oracle RUEI knows who requested the page (the client IP), which object was requested (URL), and from which Web component the object was requested (server IP).

When the Web structure responds and sends the requested object to the visitor, Oracle RUEI sees that response. At this point, Oracle RUEI can see whether there is a response from the Web structure, whether this response is correct, how much time the underlying Web structure required to generate the requested object, and the size of the object. In addition, Oracle RUEI can also see whether the object was completely received by the visitor, or if the visitor aborted the download because something went wrong during transmission (that is, proof of delivery). Hence, Oracle RUEI can determine the time taken for the object to traverse the Internet to the visitor, and calculate the Internet throughput between the visitor and the Data Center (that is, the connection speed of the visitor).

To read HTTP(S) data streams, a software module (based on standard SSL specifications) reassembles TCP/IP packet streams. The capturing network interface does not have an assigned IP address and, therefore, does not have a functional IP stack. Hence, Oracle RUEI is not able to respond to incoming traffic received from the data collectors. Neither is Oracle RUEI capable of modifying any traffic in TCP streams. This makes Oracle RUEI “invisible” to the monitored networks, and a secure resource.

Oracle RUEI is able to identify users when they enter their names (such as in login fields) or email addresses anywhere on your Web application(s). This can be used to identify the amount of individual users and compare this to the amount of anonymous users. User identification also enables direct full session replay for poor performance issues.

Deployment Options

Typically, Oracle RUEI is deployed near the firewall or load balancer. Preferably just in front of any NAT translation device. This ensures maximum availability of real-user metrics, such as the client's IP address. To enable monitoring of the real-user traffic, a SPAN port or traffic regeneration TAP device can be used. Due to their technical nature, such devices or ports are completely non-intrusive. Typically, installation, configuration, and management of such devices and ports is performed by the party managing the network infrastructure.

Optionally, Oracle RUEI can be connected behind an SSL terminating device. This removes the need to import and update the SSL keys, but could remove performance and client location information. Therefore, such deployments are not preferred.

The use of multiple Collectors may be considered when there is a need to monitor very high levels of data traffic. In addition, this deployment also provides the possibility of enhanced security. For example, by placing the Collector(s) outside the office network, while placing the Reporter system within the network. This also allows for maximum flexibility in load-balanced or geographically split environments.

Operating System Requirements

Oracle RUEI is available for the Oracle Linux and RedHat Enterprise Linux operating systems. To protect the operating system, it is strongly recommended that you apply authorized patches on a regular basis. Both supported operating systems offer outstanding security update facilities.

An operating system account is created during installation, and does not have any password assigned. Therefore, this account cannot be used for external access (such as an SSH connection with password authentication) to the system. This account is used for internal application processing only. It is recommended that you leave this account untouched to avoid remote exploits.

Accounts

During installation of Oracle Real User Experience Insight (RUEI), a number of accounts need to be created:

- Linux OS accounts¹
- RUEI Super Administrator account
- Database account¹.

Each of these are considered in the rest of this section.

RUEI Configuration Settings

The main settings used by RUEI are specified in the `/etc/ruei.conf` file and are explained in Table 1.

TABLE 1: RUEI SETTINGS

SETTING	DESCRIPTION
RUEI_HOME	The home directory of the RUEI software.
RUEI_DATA	The directory for RUEI data files.
RUEI_USER	The RUEI operating system user.
RUEI_GROUP	The RUEI operating system user.
RUEI_DB_INST	The database instance name.
RUEI_DB_USER	The database user name.
RUEI_DB_TNSNSAME	The database connect string.

The use of these settings is fully explained in the *Oracle Real User Experience Insight Installation Guide*.

¹ The OS and database accounts are specified in the global RUEI configuration file `/etc/ruei.conf`.

Linux OS Account

The `RUEI_USER` and `oracle` OS accounts need to be created during installation. By default, the `RUEI_USER` account does not have an assigned password. Therefore, this account cannot be used for external access (such as an SSH connection with password authentication) to the system. Both of these accounts are used for internal application processing only. To avoid remote exploits, it is recommended that you leave the `RUEI_USER` account untouched.

RUEI Super Administrator Account

After installation has been completed, the initial RUEI application configuration can only be performed by the predefined user `admin`. The password for this user can only be set by changing to the `RUEI_USER` user, and running the `set-admin-password` utility. You are prompted to specify and confirm the password. It is recommended that you change this password on a regular basis (for example, every 90 days).

The Super Administrator (`admin`) can delegate tasks to other user by assigning them the Administrator role. Note that defining multiple Administrators avoids the risk of password sharing.

Database Account

RUEI uses one database account, `RUEI_DB_USER`. Password credentials for connecting to the database are stored in an Oracle wallet. The `ruei-prepare-db.sh` script prompts you for the RUEI database user password, and the password used to protect the wallet. Once the wallet password is stored in a secure location, the RUEI application can login to the database automatically. The wallet files are `cwallet.sso` and `ewallet.p12` and are located, by default, in the `RUEI_DATA` directory.

Note the database password never expires. That is, it is set to unlimited. If you need to change it, you will need to run the `ruei-prepare-db.sh` script.

More information about Oracle recommended security policies is available at <http://www.oracle.com/technology/deploy/security/database-security/index.html>.

Web Server Access

By default, Apache Web server installation is secured through the use of SSL, and it is recommended that you configure it with a server certificate signed by a trusted CA. In addition, it is possible to enhance the level of the Web server security through the use of client certificates. For further information, please consult the relevant Apache documentation.

Password Security Enforcement

Note that newly created users must (by default) change their initial passwords within seven days. Otherwise, their accounts will be locked. This setting is configurable between 1 – 30 days. Note that it is also possible to specify the number of failed login attempts after which a user account is locked. This must be between 1 – 10 times. The default is five times.

While a password's expiration period can be set to 0, (that is, never expires), it is *strongly* recommended that users are required to change their passwords at regular intervals (for example, every 90 days).

LDAP Server User Authentication

In order to provide enhanced security, RUEI can be configured to enable user authentication via an LDAP server, rather than through the settings held locally on your RUEI installation. If an LDAP server connection is available, it is recommended this is used for user authentication. Note because the Administrator user is predefined, and their password is set during initial configuration (see the *Oracle Real User Experience Insight Installation Guide*), only local authentication is available for this user.

If you plan to use LDAP authentication, it is recommended that you define your LDAP connection *before* the creation of user accounts. This is in order to prevent having to modify previously specified user settings.

SSO Server User Authentication

In order to provide enhanced security, RUEI can be configured to enable user authentication via an Oracle Single Sign-On (SSO) server, rather than through the use of an LDAP server or the settings held locally on your RUEI installation.

When enabled, RUEI users (other than the Super Administrator user) are automatically re-directed to the Oracle SSO logon page. They then logon to RUEI through this page, rather than the RUEI login dialog. Note because the Super Administrator user is predefined, only local authentication is available for this user. However, other users with Administrator privileges still need to logon via the Oracle SSO server.

When enabled:

- Requires the Oracle HTTP server.
- LDAP authentication is automatically disabled.
- All currently defined RUEI users are disabled.

- The currently defined password policy settings only apply to the Super Administrator user. The Oracle SSO server enforces its own defined password policies.

SSL Private Keys

As mentioned earlier, Oracle RUEI can be configured to monitor encrypted data (such as HTTPS and SSL). In order to do this, a copy of the webserver's private SSL keys needs to be imported into the system. If the key is encrypted, you must specify the passphrase. The supplied file can be in PEM, DER, or PKCS12 format, and must include the key and matching certificate. The key must be an RSA key. Note that ephemeral keys (such as DES_40, RS2_4-0, and RC4_40) are not supported.

Each time the system on which a Collector is running is re-started, all keys must be re-activated. In the case of keys that have activation passwords defined for them, their passwords must be re-entered. The activation passwords are stored on disk encrypted in the 3DES format.

The keys are held on the Collector system(s), and all private key decryption takes place on the Collector system. In addition, the use of a dedicated system is strongly recommended, further ensuring that sensitive data is not compromised.

Optionally, you can configure notifications about pending SSL key expirations. This allows you to plan the importation of new keys, and ensures that there are no gaps in the monitored data while new keys are obtained and activated.

It is *strongly* recommended that you regularly inspect Collector and Reporter log files to verify that all sensitive data is masked correctly. Applications often change over time, and so do their use of POST variables or user identification in URL arguments.

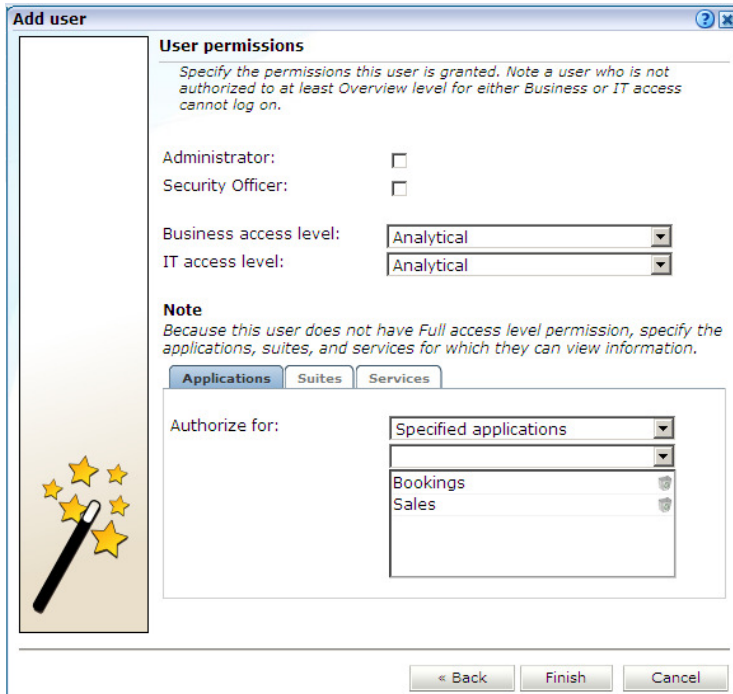
As explained above, a separate Security Officer access role is available to manage the importation and activation of SSL keys. This allows for the strict management and distribution of SSL keys.

Note that SSL keys are never included in a RUEI configuration backup. Therefore, the original private keys will need to be uploaded to the Reporter in the event of a restore of the RUEI configuration.

Role-Based Security

Oracle RUEI supports five levels of authorization that precisely regulate what users are able to do. The Administrator maintains the basic network-related configuration (such as mail settings and Collector attachments) used by the system. In addition, they act as first point of contact for system issues, and are responsible for such things as performing backups of the current configuration, and the administration of the other users authorized to work with the system.

Figure 1: User Permissions Dialog.



Business users are concerned with evaluating visitor behavior according to business goals. As such, they may be concerned with improving customer satisfaction, retention, and loyalty, increasing conversion rates, or monitoring the effectiveness of website-based marketing activities.

IT users are concerned with supporting the IT and other technical information the system needs to monitor the Web environment. Typically, they are responsible for deeper analysis of failed SLAs or KPIs.

For both Business and IT users, their assigned authorization level determines the level of access they have to the system's functionality. This includes the use of dashboard functionality, as well as on-demand and mailed reports, and drill-down into the information captured during monitoring.

Users with Full access level permission have access to all information within the Data Browser, reports, the KPI overview facility, and dashboards. For all other users, the information available to them is managed as part of their user profile.

KPIs, user flows, and dashboards can be defined as generic or bound to a specific application, suite, or service. Access to the information within an item is automatically managed through each user's assigned permissions.

If an item is defined as generic, only users that are authorized to access all applications would be able to view the item. This is because a generic item can contain information about multiple applications, suites, or services. Similarly, if a user is only authorized to view information about two applications, they would only be able to view KPIs, dashboards, Data Browser information, and reports directly concerning those two applications.

Security Officers and Administrators

Within RUEI, the Security Officer and Administrators are responsible for managing all system settings that are affected by the organization's network security policy. In particular, they:

- Import the security certificates and private keys used to decrypt HTTPS transactions, and keeps them up-to-date.
- Decide the scope of what is monitored within the organization's network. They can set up network filters to prevent the capturing of specific networks or hosts, or Virtual Local Area Networks (VLANs), or to reduce overall network traffic.
- Implement and maintain security-related measures for private data passed in Web traffic.

Data Masking

The Collector(s) can be configured to omit logging of sensitive information in POST URL arguments, HTTP headers, cookies and their values, Oracle Forms elements, and the contents of URLs. This is called *masking*, and it allows you to prevent passwords, credit card details, and other sensitive information from being recorded on disk. It is strongly recommended that you verify that all sensitive data is blinded correctly on a regular basis. This is because applications change over time, and so can the POST variables that they use. The Collector and Reporter log files can be found in the `/processor/data/wg_x_/app-id` directories within `RUEI_DATA`.

Several directories on the Reporter system may hold sensitive data which was captured during monitoring. This is especially true if the Replay Viewer has been enabled. It is *strongly* recommended that you encrypt this data. It is *strongly* recommended you select full disk encryption during the disk partitioning phase of the operating installation procedure. In this case, a passphrase is required when booting. This is fully explained in the *Oracle Real User Experience Insight Installation Guide*.

By default, the Replay Viewer is disabled. However, if enabled, it shows "raw" collected data. Masking is not applied to content and, therefore, any sensitive information contained within the content becomes visible in the Replay viewer. You can specify that URLs should be treaded using any of the masking methods described below by selecting **Configuration > Security > Masking > URL prefix masking**:

- **Complete logging** preserves all parts in both the Replay viewer and Collector log files.

- **No request body** preserves all parts in Collector log files, but request bodies are not preserved in the Replay viewer.
- **Headers only** preserves all parts in the Collector log files, but only request and response headers are preserved in the Replay viewer.
- **No replay** preserves all parts in the Collector log files, but nothing is preserved in the Replay viewer.
- **No logging** specifies that nothing is preserved in either the Replay viewer or Collector log files.

It is *strongly* recommended that you carefully review your information security requirements before (partially) enabling Replay view functionality.

To purge all collected from a RUEI installation, you should disable the recording of replay viewer data (**Configuration > Security > Masking > URL prefix masking**), and logon to each required Collector system as `root`, and issue the following command:

```
rm -rf RUEI_DATA/collector/wg/REPLAY/
```

Cookie Hashing

By default, all cookie values within RUEI are hashed. This mechanism provides a unique identifier (a hash). However, while this provides a unique value for comparison purposes, it is not in a human-readable format. For example, five different user IDs would receive five different hashes when logged, while multiple sessions by the same visitor would receive the same hash. This manufactured (hashed) value provides uniqueness, but not the real value itself.

Besides hashing of the cookie values, you can specify truncation, blinding, or plain as masking method for cookies. These options are fully explained in the *Oracle Real User Experience User's Guide*.

You should be aware that modifying the cookie masking settings, may make any sensitive information placed in the cookie visible, not only in the Reporter interface, but also in any exported data that contains cookie information. Therefore, it is *strongly* recommended that you carefully review your information security requirements before changing the (default) cookie masking setting.

Enriched Data Exchange Facility

The Enriched data exchange facility enables you to combine the data gathered by RUEI with other data sources. These could include, for instance, Customer Relationship Management (CRM) or Business Intelligence (BI) systems. Using this functionality, you can produce customized analysis of your Web environment using your own BI tooling, as well as integrate

RUEI's rich set of collected data with offline data to obtain greater insight into what drives your sales and revenue.

The facility works by exporting the data collected by every 5-minute period to a database. By default, the data is exported to the same database instance as used by the Reporter. However, it is *strongly* recommended that you configure an alternative database instance for enriched data export. Access to data in the export database is available via SQL. The procedure to do this is fully described in the *Oracle Real User Experience Insight Installation Guide*.

Export Report Data

The report data within RUEI is available for export to host or client systems. For example, to a Business Intelligence (BI) system. The exported data is in Unicode (UTF-8) format. By default, access to the export file (`export.php`) is denied to any HTTP request by the following entry in the `/etc/httpd/conf.d/uxinsight.conf` file:

```
<Files export.php>
    Deny from all
</Files>
```

To grant access to the export facility, the `Deny from all` entry must be overridden. For full authentication configuration, see the *Oracle Real User Experience Insight User's Guide*.

Conclusion

RUM has a number of critical differences with other application performance monitoring strategies, such as device monitoring and synthetic testing checks. RUM technologies make it possible to monitor all user traffic, all the time, at the application level. This has created a security dilemma. By peering into real user traffic, these technologies are looking at sensitive information, such as credit cards and passwords.

Hence, while implementations of RUM technologies is proceeding at a rapid pace, organizations need to realize that improperly secured RUM approaches can expose personally identifiable information to disgruntled employees, hackers, or identity thieves.

Oracle RUEI is uniquely positioned to deliver the benefits of RUM. It is based on a robust and proven security model that minimizes risk, and offers powerful controls to those responsible for security and compliance.

Whether your organization uses the Internet as a marketing channel, or Extranet-based supply chain and back-office integration, or Intranet deployment of internal applications, Oracle RUEI delivers a leading-edge solution without compromising on security.



Security Best Practices for Oracle Real User
Experience Release 11g
March 2011
Author: Paul Coghlan
Contributing Authors: Eddy Vervest

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2011, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.