Oracle® Argus Analytics

Security Configuration Guide

Release 1.1.1.1

E41345-01

June 2013

This guide describes essential security management options for the following applications:

- Oracle Argus Analytics
- Oracle Business Intelligence Enterprise Edition

1 Introduction

This guide presents the following security guidelines and recommendations:

2 Configuring Strong Password on the Database and WLS

Although the importance of passwords is well-known, the following basic rule of security management is worth repeating:

Ensure all your passwords are strong passwords.

You can strengthen passwords by creating and using password policies for your organization.

For guidelines on securing passwords and for additional ways to protect passwords, refer to the Oracle Database Security Guide specific to the database release you are using.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the Weblogic Server default accounts, such as weblogic.

- Password for the database listener. If you do not configure the database listener to require an authorization password, you unnecessarily expose the underlying database service names to unauthorized individuals.

3 Closing All Open Ports not in Use

Keep only a minimum number of ports open. You should close all ports that are not in use.

4 Disabling the Telnet Service

The Argus Analytics application does not use the Telnet service. Telnet listens on port 23 by default.

If the Telnet service is available on the Argus Analytics host machine, Oracle recommends that you disable Telnet in favor of Secure Shell (ssh).

Telnet, which sends clear-text passwords and user names through a login, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

5 Disabling Other Unused Services

In addition to not using Telnet, the Argus Analytics application does not use the following services or information for any functionality:

- **Simple Mail Transfer Protocol (SMTP):** This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.
- **Identification Protocol (identd):** This protocol is generally used to identify the owner of a TCP connection on UNIX.
- **Simple Network Management Protocol (SNMP):** This protocol is one method for managing and reporting information about different systems.

Therefore, restricting these services or information will not affect the Argus Analytics application. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure.

If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

6 Checking External Links That May Expose Account Data

In Argus Analytics, you can add customized links to the Home page, Dashboards, Report pages, and the Help icons. Any information that can be made available through a URL can be made accessible to Argus Analytics Onsite users.

In addition, your customized links support passing session parameters, such as login user ID and user role, to a URL. By passing these session parameters, you can create target Web pages that switch the content according to the user login ID, user role, study, and site. You can create links that access websites relevant to your business.

However, be aware that in some situations, such as links that access external websites, passing account data and session information may pose a security risk. In these cases, you can define the link to pass no session parameters to the URL.

7 Enabling SSL for OBIEE

This section comprises the following sub-sections:

7.1 Enabling SSL

Refer to the **Configuring SSL for Oracle Argus Analytics in OBIEE** section in the **Oracle® Argus Analytics Installation Guide** to enable SSL.

7.2 Setting up a Secure Cookie on WebLogic Server

Refer to the MOS Note **How to set up Secure Cookies on WebLogic Server** section (Doc ID 1267117.1) to set up the secure SSL cookie.

8 Setting up Session Timeout in OBIEE

To configure the setup session timeout between OBI presentation service and the browser, execute the following steps:

1. Edit the instanceconfig.xml file (config\OracleBIPresentationServicesComponent\coreapplication_obips1).
2. Update the following line in the Security block: <ClientSessionExpireMinutes> 210</ClientSessionExpireMinutes>.
3. Restart OBI Presentation Services.

> **Note:** The internal default value is 210 minutes. After this duration, the presentation service removes the browser session information from its memory.

9 Logging Security Restrictions

Query logging level defines the exposure of database queries to OBIEE users. By default, each user account's Logging Level is set to 0 (zero), which is no logging. Implement the following steps to set the levels for a user:

1. Open BI Administration tool and click Manage > Identity.
2. Double-click the name of the user to select and update the logging level in the pop-up menu.
3. Enter the following information in the Logging Level:
   a. Level 0: No Logging
   b. Level 1: Logged details are SQL statements, query response durations, user id, session id , request id.
   c. Level 2: Everything Logged in level 1 with additional information such as repository name, business model name, subject area name, no of rows returned, etc.
   d. Level 3: Everything Logged in level 2 with additional information such as logical query plan, purged cache, etc.
   e. Level 4: Everything Logged in level 3 with additional information of query execution plan.

f. Level 5: Everything Logged in level 4 with detailed query execution plan

10 Creating a New Security Realm

A security realm can optionally include Identity Assertion, Auditing, and Certificate Registry providers. If your new security realm includes two or more providers of the same type (for example, more than one Authentication provider or more than one Authorization provider), you need to determine how these providers should interact with each other.

Custom Authorization and Role Mapping providers may or may not support parallel security policy and role modification, respectively, in the security provider database.

If your custom Authorization and Role Mapping security providers do not support parallel modification, the WebLogic Security framework can enforce a synchronization mechanism that results in each application and module being placed in a queue and deployed sequentially. To do this, set the Deployable Provider Synchronization Enabled and Deployable Provider Synchronization Timeout controls for the realm.

11 Deleting the MAPVIEWER Component in OBIEE 11g

OBIEE 11g Mapviewer component comes with some demo code which can pose some security vulnerabilities.

Hence, it is recommended that you delete the Mapviewer component by using the following steps:

1. Login to the OBIEE 11g Administrator Console.
2. Navigate to **Deployments** > **Control** tab and click the **Next** hyperlink till the Mapviewer application is displayed.
3. Select the checkbox against the deployed Mapviewer application [Mapviewer (11.1.1)].
4. Click the **Stop** > **When Work Completes** button to shutdown the Mapviewer application.
5. Once the operation completes, reselect the checkbox against the Mapviewer application [Mapviewer (11.1.1)] and click **Delete** to remove the application from the Domain Configuration.
6. Activate the pending changes by clicking **Activate Changes** to completely delete the Mapviewer application.

12 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=accid=info or visit http://www.oracle.com/pls/topic/lookup?ctx=accid=trs if you are hearing impaired.

Oracle Argus Analytics Security Configuration Guide, Release 1.1.1.1
E41345-01