INTEGRIGY

WHITE PAPER

Guide to Auditing and Logging in the Oracle E-Business Suite

FEBRUARY 2014

GUIDE TO AUDITING AND LOGGING IN THE ORACLE E-BUSINESS SUITE

Version 1.0 – March 2003
Version 1.1 – February 2004
Version 1.2 – September 2005
Version 2.0 – February 2014

Authors: Stephen Kost and Mike Miller, CISSP-ISSMP

If you have any questions, comments, or suggestions regarding this document, please send them via e-mail to info@integrigy.com.

Table of Contents

OVERVIEW

Most Oracle E-Business Suite implementations do not fully take advantage of the auditing and logging features. These features are sophisticated and are able to satisfy most organization's compliance and security requirements.

The default Oracle E-Business Suite installation only provides a basic set of logging functionality. In Integrigy's experience, the implementation of database and application logging seldom exceeds meeting the needs of basic debugging. Most organizations do not know where to start or how to leverage the built-in auditing and logging features to satisfy their compliance and security requirements.

Even organizations already using centralized logging or Security Incident and Event Management (SIEM) solutions, while being more advanced in the Common Maturity Model (CMM), in Integrigy's experience are commonly challenged by the E-Business Suite's auditing and logging features and functionality.

This guide presents Integrigy's framework for auditing and logging in the Oracle E-Business Suite. This framework is a direct result of Integrigy's consulting experience and will be equally useful to both those wanting to improve their capabilities as well as those just starting to implement logging and auditing. Our goal is to provide a clear explanation of the native auditing and logging features available, present an approach and strategy for using these features and a straight-forward configuration steps to implement the approach.

Integrigy's framework is also specifically designed to help clients meet compliance and security standards such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), FISMA, and HIPAA. The foundation of the framework is PCI DSS requirement 10.2.

To make it easy for clients to implement, the framework has three maturity levels – which level a client starts at depends on the infrastructure and policies already in place.

The three levels are:

- **Level 1** – Enable baseline auditing and logging for application/database and implement security monitoring and auditing alerts
- **Level 2** – Send audit and log data to a centralized logging solution outside the Oracle Database and E-Business Suite
- **Level 3** – Extend logging to include functional logging and more complex alerting and monitoring

Audience and How to Read This Paper

The intended audience are Oracle E-Business Suite DBAs, application administrators, IT security staff, and internal audit staff. A working technical knowledge of the Oracle E-Business Suite and Oracle Databases is recommended.

The section discussing the logging functionality available in the Oracle E-Business Suite and the Oracle Database may be skipped if the material is already familiar. Internal audit and IT security staff may find it useful to proceed directly to the presentation of Integrigy's Security Monitoring and Audit Framework.

Oracle E-Business Suite Versions

The information in this guide is intended for and based on the Oracle E-Business Suite R12 (12.1). All the information and guidance should also be applicable to and be relevant for previous and future versions of the Oracle E-Business Suite, including but not limited to 11.5.x (11i) and 12.2.

For Oracle E-Business Suite 12.2, the most significant change is the inclusion of the Oracle WebLogic application server and additional auditing and logging should be enabled in WebLogic as it has an added layer of security and management.

INTEGRIGY'S FRAMEWORK FOR ORACLE E-BUSINESS SUITE SECURITY

The framework is a result of Integrigy's consulting experience and is based on compliance and security standards such as Payment Card Industry (PCI-DSS), Sarbanes-Oxley (SOX), IT Security (ISO 27001), FISMA (NIST 800-53), and HIPAA.

The foundation of the framework is the set of security events and actions that should be audited and logged in all Oracle E-Business Suite implementations. These security events and actions are derived from and mapped back to key compliance and security standards most organizations have to comply with. We view these security events and actions as the core set and most organizations will need to expand these events and actions to address specific compliance and security requirements, such as functional or change management requirements.

Table 1 presents the core set of audits that, if implemented, will serve as a foundation for more advanced security analytics. Implementing these audits will go a long way toward meeting logging and auditing requirements for most compliance and security standards like PCI requirement 10.2. The numbering scheme used in Table 1 will be referenced throughout the document.

Table 1 – Foundation Events for Logging and Security Framework

Security Events and Actions	PCI DSS 10.2	SOX (COBIT)	HIPAA (NIST 800-66)	IT Security (ISO 27001)	FISMA (NIST 800-53)
E1 - Login	10.2.5	A12.3 DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E2 - Logoff	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E3 - Unsuccessful login	10.2.4	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1 A.11.5.1	AC-7
E4 - Modify authentication mechanisms	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E5 - Create user account	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E6 - Modify user account	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E7 - Create role	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E8 - Modify role	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2

Table 1 – Foundation Events for Logging and Security Framework					
Security Events and Actions	**PCI DSS 10.2**	**SOX (COBIT)**	**HIPAA (NIST 800-66)**	**IT Security (ISO 27001)**	**FISMA (NIST 800-53)**
E9 - Grant/revoke user privileges	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E10 - Grant/revoke role privileges	10.2.5	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E11 - Privileged commands	10.2.2	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2
E12 - Modify audit and logging	10.2.6	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2 AU-9
E13 - Objects: Create object Modify object Delete object	10.2.7	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2 AU-14
E14 - Modify configuration settings	10.2.2	DS5.5 DS5.6 DS9.2	164.312(c)(2)	A 10.10.1	AU-2

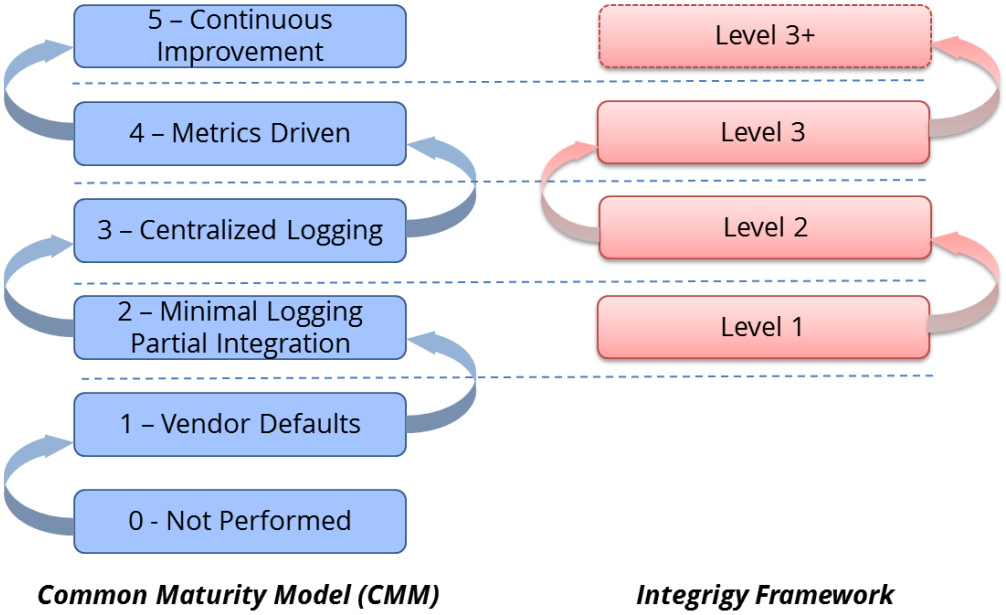
FRAMEWORK APPROACH

Integrigy's framework has three levels of maturity. Not all organizations will start at the same level. Which level a client starts at depends on the infrastructure and policies an organization already has in place. Integrigy's experience is that using this approach will give both specific guidance as well as vision.

The levels are:

- **Level 1** – Enable basic logging for Oracle E-Business Suite system administration and implement a best practices checklist for security monitoring and auditing. Implementation focus is on DBAs and application administrators.
- **Level 2** – Send basic log data to a centralized logging solution outside the Oracle Database and E-Business Suite. Implementation focus is on IT security and internal auditors and their meeting the basic requirements.
- **Level 3** – Send E-Business Suite functional and additional database logs to the centralized logging solution. Implementation focus is on IT security and internal auditors to meet advanced requirements for compliance and automation. This is commonly done to meet specific requirements for compliance PCI, SOX, HIPAA and ISO 27001.

Figure 1 - Integrigy Framework Compared to Common Maturity Model



Level 1

The first level focuses on logging and basic monitoring and auditing. Logging, monitoring, and auditing are separate but related disciplines. Logging provides the data for both monitoring and auditing. In the framework's first level optional logging functionality is enabled. This is functionality not enabled by the default Oracle E-Business Suite installation and is commonly not used. Once this functionality is in place, the framework then presents a best practice checklist for security monitoring and auditing for the Oracle E-Business Suite. For those customers considering a security monitoring and auditing program, this should be an ideal starting point.

Level 2

The second level of maturity focuses on integrating with a centralized logging solution. Given the complexity of the Oracle E-Business Suite and compliance requirements for protection and non-repudiation of log data, a centralized logging solution is required. Once the solution is in place, Level 2 of the framework presents where and how to start passing log and audit data from the Oracle E-Business Suite and Oracle Database.

Level 3

The third level of maturity is continuous. Once the basic log data is being passed to a centralized logging solution and/or Security Incident and Event Management (SIEM) system, the framework presents additional E-Business Suite configurations that can and should be considered for event correlation. As well, the framework identifies additional database and application server logs to be captured. Level 3 is continuous, as the possibilities of security incident and event correlation rules and filters are only limited by the data within the Oracle E-Business Suite.

Figure 2 - Integrigy Framework Auditing and Logging Framework

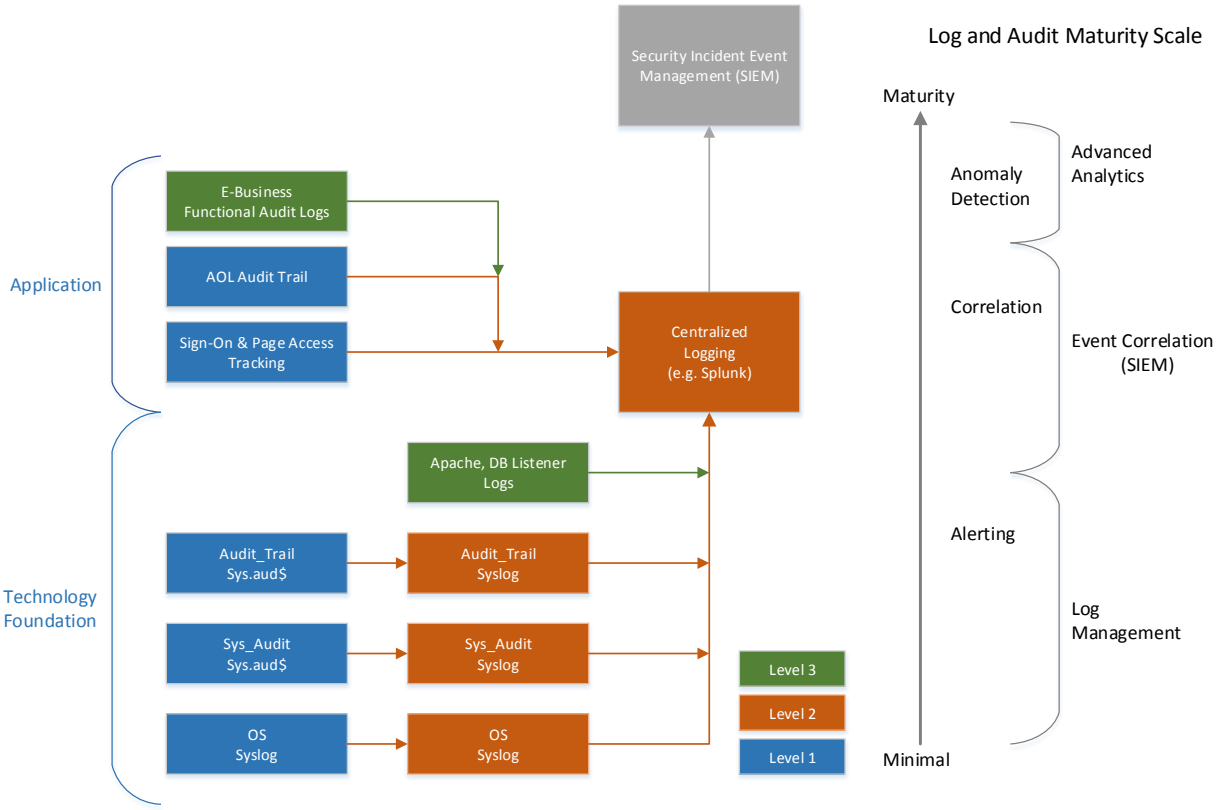
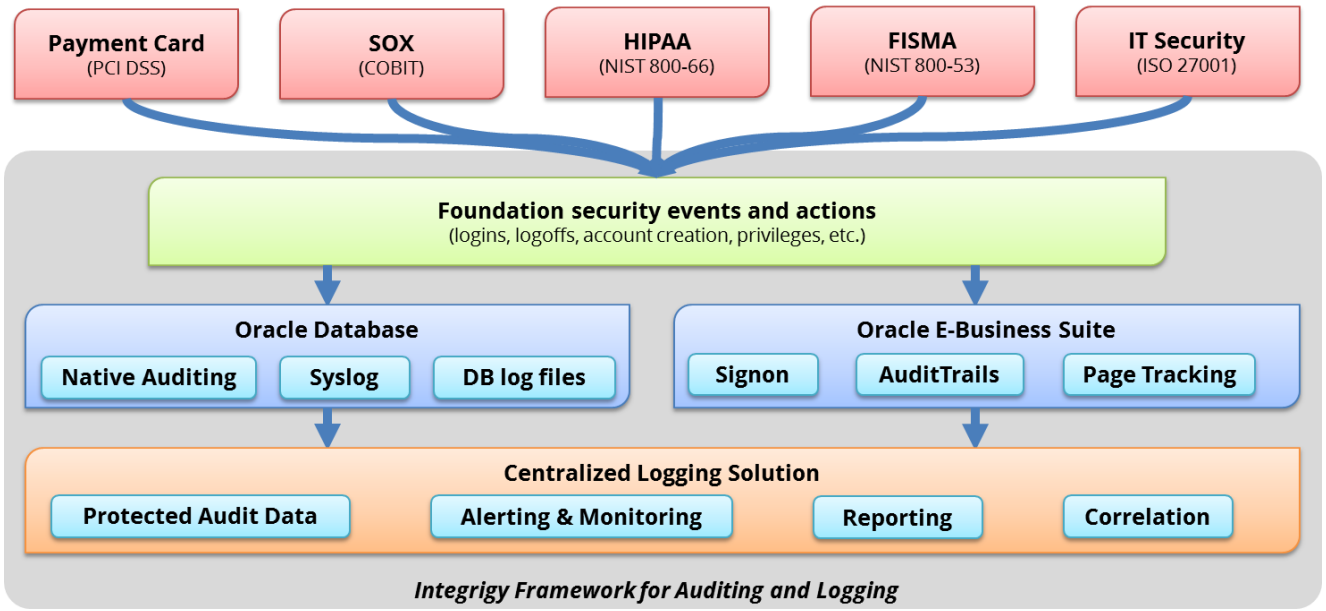


Figure 3 - Integrigy Framework for Auditing and Logging in Oracle E-Business Suite



LOG AND AUDIT FUNCTIONALITY

This section reviews the basic log and audit functionality available in the Oracle E-Business Suite and the Oracle Database. Some of this functionality is enabled by default – some of it is optional and needs to be configured. It should also be noted that more audit and monitoring functionality exists than what is discussed here. The scope of this discussion is limited to what is required to implement Integrigy's framework.

NOTE: This section may be optional if the reader is already familiar with the core auditing and logging functionality in the Oracle E-Business. The purpose is to provide an overview of the key auditing and logging features used to implement Integrigy's framework.

WHAT IS A LOG?

A "log" is a collection of messages that "paints a picture" of an event or occurrence. The following are general categories of log messages, all of which are important to Integrigy's framework:

- **Informational –** benign event occurrence, for example, a system reboot
- **Debug –** information to aid developers and administrators
- **Warning –** events affecting systems and applications
- **Error –** application or system fault
- **Alert –** something interesting has occurred

A log message has three parts:

1. **Timestamp** – when did the event occur
2. **Source** – server, application our person
3. **Data** – system message, SQL statement, debug code, etc.

OPERATING SYSTEM LOGGING

Most, if not all, Oracle E-Business Suite implementations running on UNIX or Linux will have Syslog enabled by the system administrators and/or hosting provider. Syslog is a standard for UNIX and Linux message logging and supports a wide variety of devices, from printers and network routers to database servers. Syslog messages generated by applications or services are sent to a message store on the system or can be delivered to a centralized server built for the specific purpose of log storage and analysis.

The following basic operating system events are assumed to be collected and available:

- System startup/shutdown
- Logons and attempted logons – IP address, port, time
- Process history and statics

ORACLE DATABASE

Oracle Databases offer a rich set of logging and auditing functionality. For Integrigy's Framework, standard Oracle Database auditing and the capability to send database audit logs to Syslog will be leveraged.

Standard Oracle Auditing

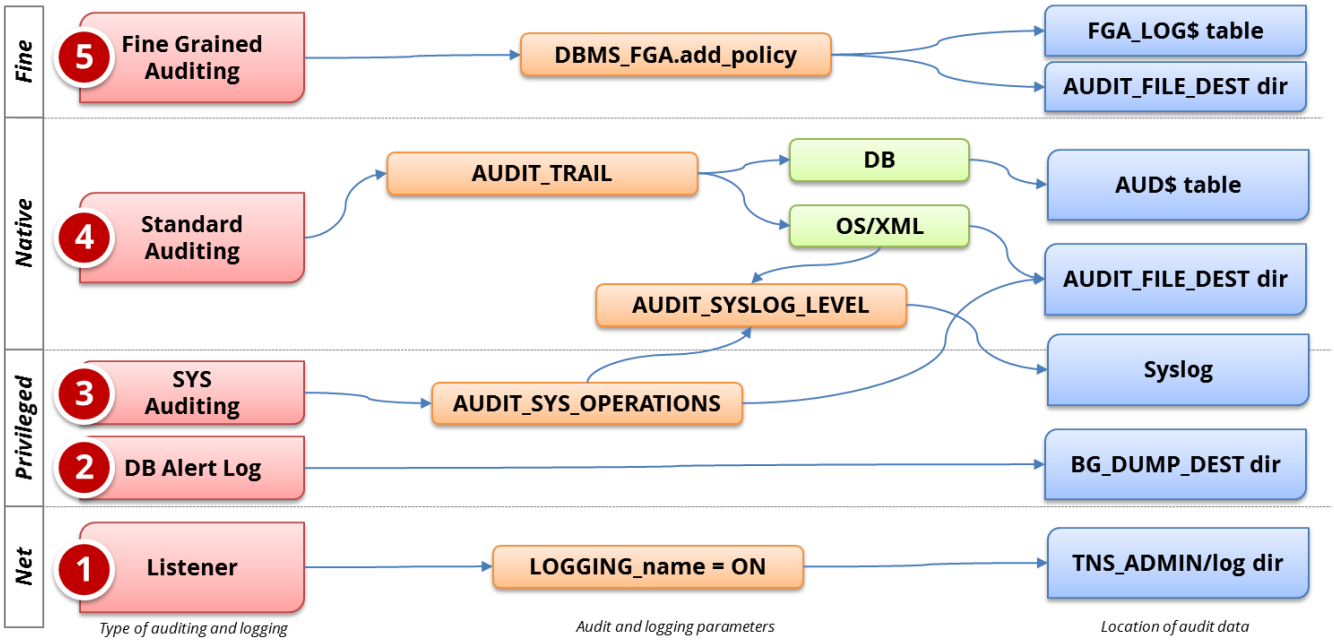
Standard auditing is available in all editions of the Oracle RDBMS. It can be used to audit SQL statements, privileges, schemas, objects and network and multitier activity. Standard auditing must be enabled, and once enabled, a regular program for purging data needs to be implemented.

The variety and volume of data collected by standard auditing can be large and the output can be directed either to the database itself or to files in the operating system outside the database. Moving logs outside the reach of DBAs, either into the operating system or sent to a centralized log server, offers many security benefits. For more information on standard auditing refer to the reference section of this document.

Database Syslog

As noted earlier, Syslog is a standard for UNIX and Linux logging. Oracle Syslog option is a standard database feature that sends Oracle log data to the native operating system Syslog facility, which in turn can be forwarded directly to a centralized syslog server or collector. The native Oracle Syslog auditing has minimal performance overhead and provides immediate protection of the audit trail. However, it is possible for the DBA to disable auditing and mitigating controls must be established around possible deactivation of the auditing. For more information on Syslog refer to the reference section of this document.

Figure 4 - Database Auditing and Logging



ORACLE E-BUSINESS SUITE

By default upon installation, the Oracle E-Business Suite only audits and logs a limited set of information including:

- basic user logon information
- unsuccessful password attempts
- concurrent program execution
- creation and last update information for most records

Additional auditing and logging has to be enabled to capture key security events and actions such as responsibility selection, form usage, and security configuration history. Oracle E-Business Suite features AuditTrail and Page Access Tracking (PAT) will need to be enabled to audit and log key events.

Concurrent Requests

Concurrent request execution history is recorded in the APPLSYS.FND_CONCURRENT_REQUESTS table. There is no configuration required to setup or configure concurrent requests execution auditing other than to periodically purge it. However, most organizations only keep one month of less of history. Review the schedule and request settings for the ***Purge Concurrent Request and/or Manager Data Program*** (FNDCPPUR) program to determine how often the purge is run and how much history is maintained. This program is usually configured to purge all history older than x days (Mode = Age and Mode Value = days).

Unsuccessful Logins

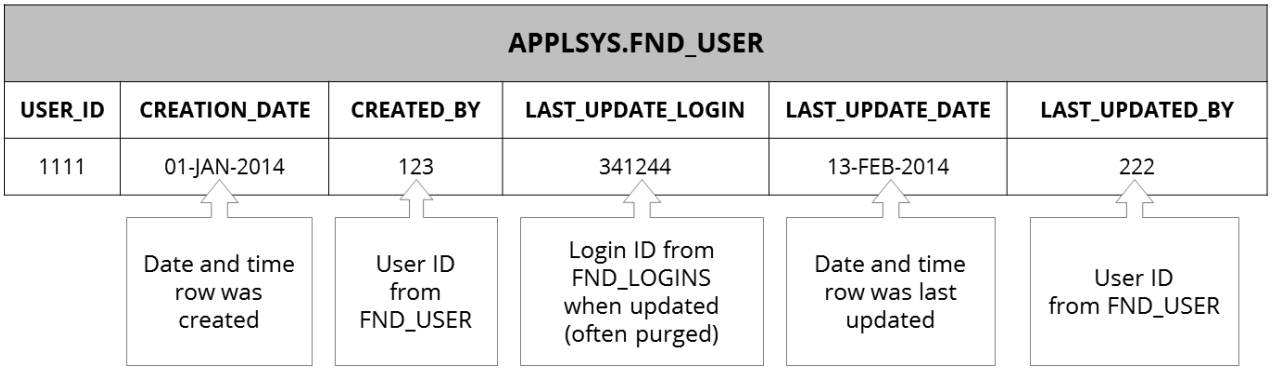
Unsuccessful password attempts are automatically recorded in the APPLSYS.FND_UNSUCCESSFUL_LOGINS and ICX.ICX_FAILURES tables. There is no way to disable this functionality. Review the schedule and settings for the concurrent program ***Purge Signon Audit Data*** to determine how often this information is purged.

Who Columns/About this Record

Almost all records and transactions in the Oracle E-Business Suite include the creation and last update information for the record. This data is stored as part of the database row and is referred to as the "Who Columns." No setup or configuration is required for Who Columns and no purge program is required.

It is important to note that any changes to the row between the creation and last update are not saved – only the creation information and last record update information will be saved. To save all update history for a row, Oracle E-Business Suite AuditTrail must be enabled for the table.

Figure 5 - Oracle E-Business Suite Who Columns Example



From Oracle E-Business Suite Forms user interface, any user can check a record's creation or last update information (Record History). If the form has header and detail information, either can be obtained. Be sure the cursor is in the correct block and from the menu select ***Help > Record History***.

As of Oracle E-Business Suite 12.1, Record History may be viewed for OA Framework pages. The system profile option "FND: Record History Enabled" (FND_RECORD_HISTORY_ENABLED) must be set to Yes. Record History must be enabled for each page using OA Framework personalizations. To enable Record History for a page, access Personalize page and set the "Record History Enabled" property to true on the header, table, or advanced table component of the page.

Sign-On Audit

Sign-On Audit is optional functionality to track end-user navigation activity in the professional forms (not Web or HTML forms). It has three levels: Login, What Responsibility was used, and What Forms were visited. For each option, the length of time is captured. Only Navigation activity is a captured – it is important to understand that what the end-user did in the form, be it viewed a record or updated a record, is not captured. If the requirement is to capture the end-user actions in the form, auditing must be enabled using Oracle E-Business Suite AuditTrail or third-party tools are required.

Sign-On Audit is turned off/on by the system profile option "Sign-On: Audit Level." If enabled, Sign-On Audit needs to regularly purge the data it collects. This can be done using the ***Purge Concurrent Request and/or Manager Data*** concurrent program.

Sign-On Audit data is collected in real-time and can be viewed through standard reports, a Form, or by using SQL.

The following are the standard reports for Sign-On audit data:

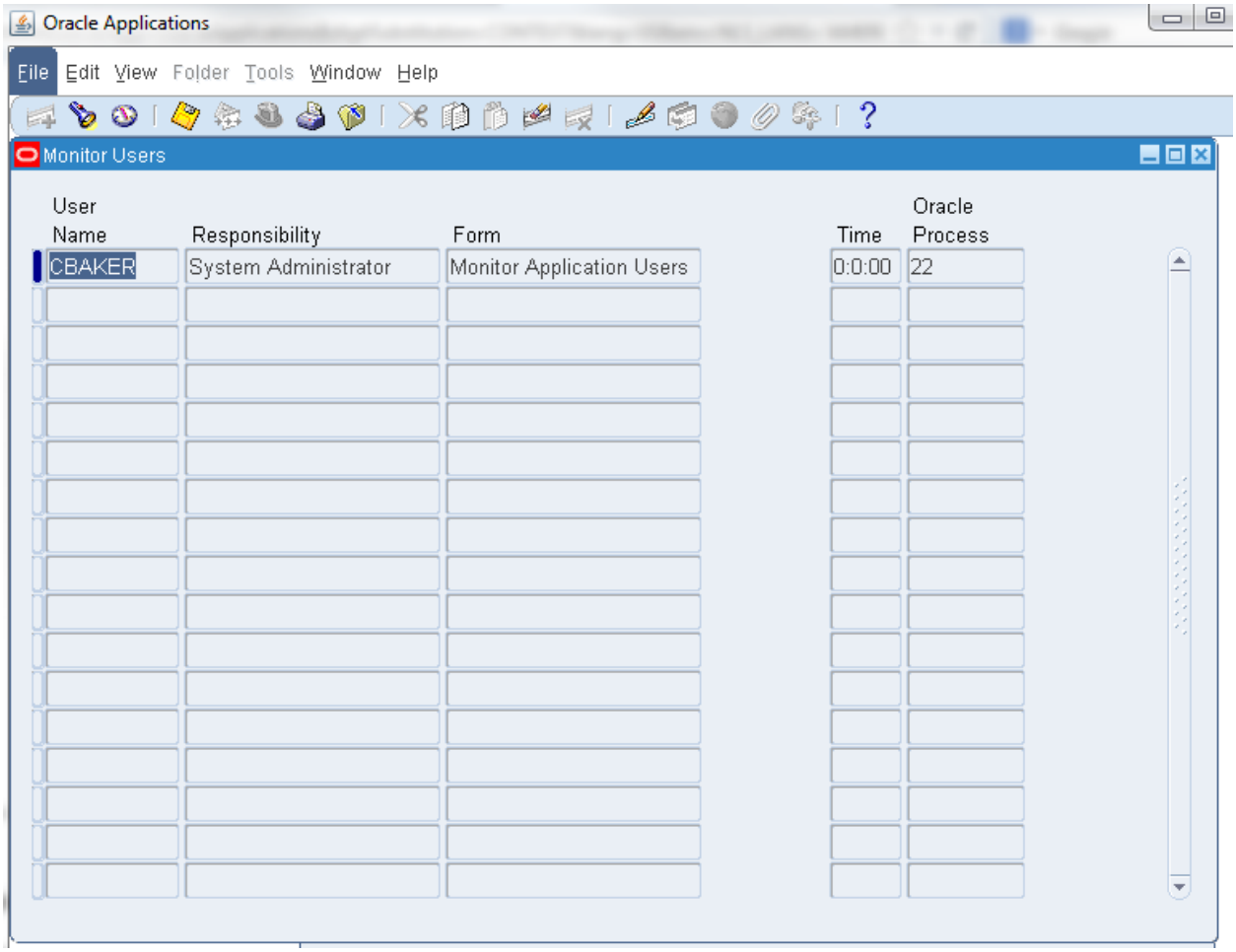
- Signon Audit Users
- Signon Audit Responsibilities
- Signon Audit Forms
- Signon Audit Concurrent Requests
- Signon Audit Unsuccessful Logins

The following tables store the Sign-On audit data:

- APPLSYS.FND_LOGINS
- APPLSYS.FND_LOGIN_RESPONSIBILITIES
- APPLSYS.FND_LOGIN_RESP_FORMS
- APPLSYS.FND_UNSUCCESSFUL_LOGINS

The menu function ***Monitor Users*** (FNDSCMON) can also be used to review Sign-On audit data. This form is accessed in the seeded responsibility "System Administrator" under ***Security -> User -> Monitor Users***.

Figure 6 - Oracle E-Business Suite Monitor Users Form



Page Access Tracking

Sign-On Audit only logs professional forms activity – it does not log Oracle Applications Framework (OAF) user activity. In addition to Sign-On Audit, Page Access Tracking is required to log OAF activity. Once enabled, the level of logging needs to be set as well as flagging those applications to be logged and has negligible overhead.

To configure Page Access Tracking, use the following navigation: ***System Administration -> Oracle Applications Manager -> Site Map > Monitoring > Applications Usage Reports > Page Access Tracking*** and Sign-on Audit Configuration.

Once enabled, Page Access Tracking requires two concurrent programs to be run. The program ***Page Access Tracking Data Migration*** must be run to move data from the staging tables into the reporting tables. This is usually done daily. To purge data on a regular basis, run the program ***Page Access Tracking Purge Data***.

The levels of logging are:

- Session info
- Session Info and Cookies
- Session Info, Cookies and URL Parameters
- Session Info, Cookies and All Parameters

Once configured, reports can be run for the following types of activity:

- Session
- Date
- Form
- User
- Application

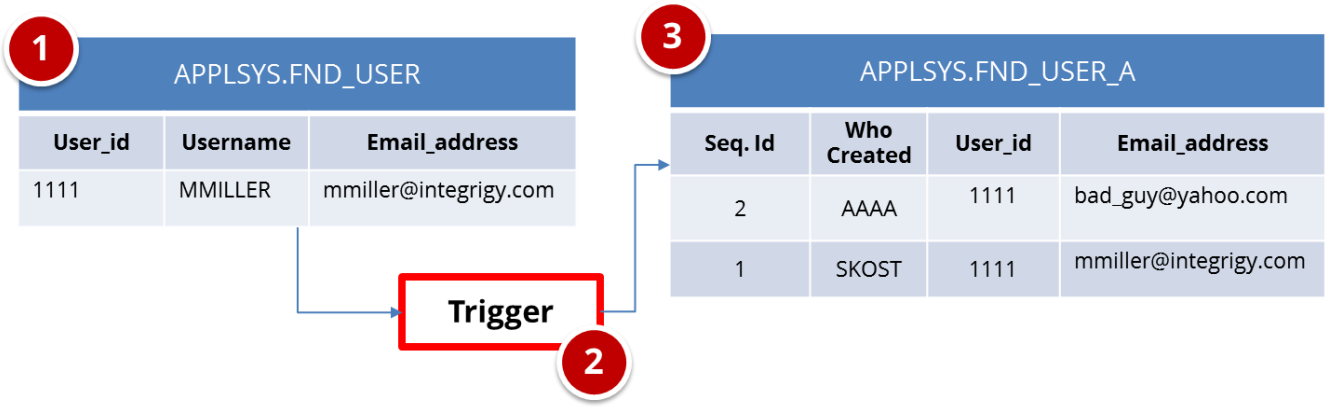
E-Business Suite AuditTrail

Any Oracle E-Business Suite table can be selectively chosen to have row changes audited – auditing can be done at the row or column level. By default, no tables are audited. Auditing frequently accessed tables (especially transactional tables) can cause severe database performance issues, thus auditing should be carefully designed.

AuditTrail information is stored in separate database tables detailing the user information and types of updates. The Oracle E-Business Suite AuditTrail functionality only tracks inserts, updates, or deletes, whereas the database's native auditing capability can also track selects on tables.

Oracle E-Business Suite AuditTrail maintains a full history of changes made at a table and column level. The AuditTrail is enabled by a shadow table (table name appended with _A) of the audited table and triggers on the audited columns. A concurrent program is used to create the shadow table and triggers.

Figure 7 – Oracle E-Business Suite Audit Trails Example



Auditing database row changes is very performance intensive and can cause significant database performance problems. Careful planning and reviews with a DBA should be performed before enabling any auditing. Only a minimal amount of auditing should be done and limited to non-transactional data. Auditing on transactional data may cause significant performance degradation of the entire application. Tables with more than a few changes an hour should not be considered for row level auditing.

For more information on setting up AuditTrail, see Appendix A – How to Configure E-Business Suite AuditTrail.

HR Audit Trails

If columns in HR DateTracking tables are audited using Oracle E-Business Suite AuditTrail, the standard audit history is supplemented. Dynamic SQL is generated from APPS.PY_AUDIT_REPORT_PKG and the results are stored in HR.HR_AUDITS and HR.HR_AUDIT_COLUMNS. Consult the *Oracle Human Resources Management Systems Configuring, Reporting, and System Administration Guide* for more information.

INTEGRIGY FRAMEWORK – LEVEL 1

Level 1 focuses on the basic logging that Integrigy recommends for all Oracle E-Business Suite implementations. This logging needs to be in place before proceeding to Levels 2 and 3 of the Framework, but assumes a centralized logging solution is not available yet. Level 1 auditing will be in addition to the standard default functionality such as "Who Columns."

The following summarizes the steps to implement Level 1:

1. Oracle Database logging
    a. Enable standard database auditing to the database (AUD$) per Integrigy's recommendations
    b. Enable AUDIT_SYS_OPERATIONS
2. Oracle E-Business Suite logging
    a. Set Sign-on Audit to log at the 'Form' level
    b. Enable Page Access Tracking
    c. Enable AuditTrail on key tables per Integrigy's recommendation
3. Set up policies and procedures for security monitoring and auditing

DATABASE AUDITING

Database auditing is vital to application logging and security monitoring as direct database access can be used to circumvent all application controls.

Level 1 assumes there is no centralized logging solution implemented and the database audit data should be written to the database (SYS.AUD$) for monitoring and reporting. Saving audit data to the database is not ideal as the DBA can manipulate the audit data, but provides for much simplified monitoring and reporting. If a centralized logging solution is implemented, then the database audit data should be written to Syslog per the instructions in Level 2.

Steps for Level 1 database auditing:

1. Enable native database auditing and store audit data to the database. In the init.ora file for the instance, set the database initialization parameter **AUDIT_TRAIL** to **DB**. This will write out all logs to the SYS.AUD$ table except for SYS Operations, which are always written to the operating system audit trail.
2. As the SYS user, configure database auditing per *Table 2 – Recommended Oracle E-Business Suite Database Auditing*.
3. The SYS.AUD$ table needs to be purged on a periodic basis per your organization's policy requirement. All rows should be backed up prior to being purged. Purging is configured through the use **DBMS_AUDIT_MGMT**.
4. In the init.ora file for the database instance, enable auditing of the SYS user by setting the database initialization parameter **AUDIT_SYS_OPERATIONS** to **TRUE**. Logs are written to the operating system's native audit trail.

Table 2 – Recommended Oracle E-Business Suite Database Auditing				
Framework Event	**Database Object**	**Oracle Audit Statement (audit {};)**	**Resulting Audited SQL Statements**	**Notes**
E1, E2, E3	Session	session	Database logons and failed logons	▪ All database logons and failed logons ▪ This is highly dependent on database usage and application. With application connection pooling, the number of database session is minimized. However, some frequent interface programs may result in large numbers of sessions.
E5, E6	Users	user	create user alter user drop user	▪ All changes to users ▪ Includes all password changes by users - actual password is not captured
E7, E8	Roles	role	create role alter role drop role	▪ All changes to roles ▪ SET ROLE is excluded which is frequently used and would be included if AUDIT ROLE was used
E13	Database Links Public Database Links	database link public database link	create database link drop database link create public database link drop public database link	▪ Creation and deletion of database links
E11, E14	System	alter system	alter system	▪ Changes to the database configuration ▪ Audits killing of sessions, open/closing wallet, and setting of initialization parameters
	Database	alter database	alter database	▪ Change to database and instance state
E9, E10	Grants (system privileges and roles)	system grant	grant revoke	▪ Captures only grants to system privileges and roles ▪ Grants/revokes on database objects will be captured as part of the object creation
E4	Profiles	profile	create profile alter profile drop profile	▪ All changes to password and resource profiles ▪ Assigning profiles to users will be captured as part of ALTER USER
E9, E10	Directories	grant directory	grant directory revoke directory	▪ Granting of directories

Table 2 – Recommended Oracle E-Business Suite Database Auditing				
Framework Event	**Database Object**	**Oracle Audit Statement (audit {};)**	**Resulting Audited SQL Statements**	**Notes**
E9, E10	Procedures Packages Functions Libraries Java Objects	grant procedure	grant <procedural type> revoke <procedural type>	▪ Granting and revoking of procedural objects
E9, E10	Object Grants	grant sequence grant table grant type	grant sequence grant table/view grant type revoke sequence revoke table/view revoke type	▪ Granting on sequence, tables, types, and views ▪ Grant table will also audit grant view
E12	Auditing	system audit	audit noaudit	▪ Changes to database auditing
E11, E14	SYSDBA and SYSOPER	sysdba sysoper	All SQL executed with sysdba and sysoper privileges	▪ Actions taken by DBAs – mostly occurs during weekly maintenance window

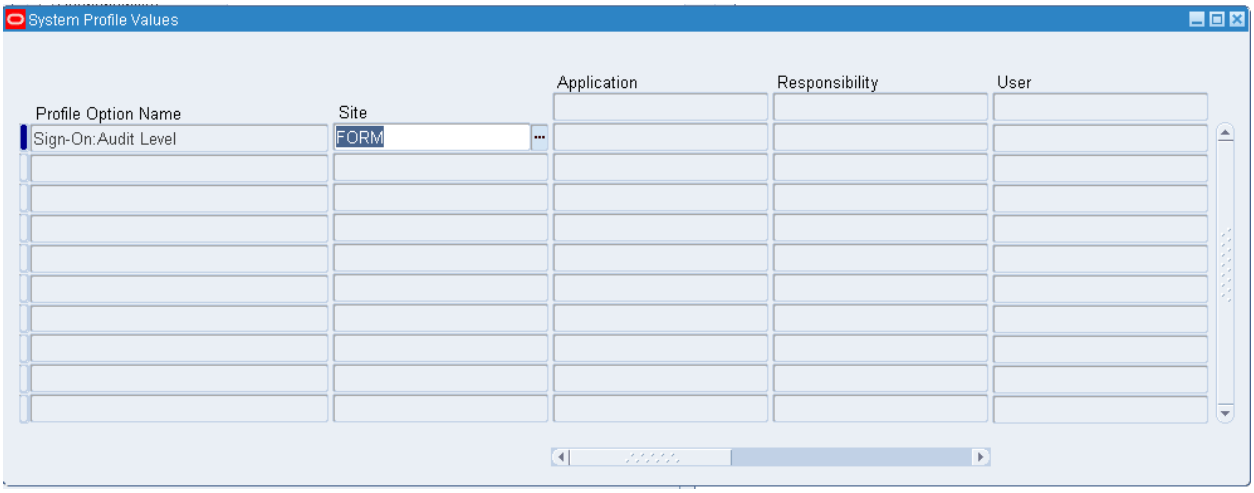
As part of the Framework Level 1, we do not recommend enabling extensive auditing of database object (e.g., tables, indexes, procedures, etc.) creation, modification, or deletion since in an Oracle E-Business Suite environment this will generate a significant amount of audit data. The application itself is creating temporary objects and there are frequent changes due to patching. The APPS user is the account used during these activities and mostly originates from the application or database servers, thus the audit trail becomes fairly meaningless.

E-Business Suite Logging

Sign-On Audit Level

Set Sign-On: Audit Level to **FORM** – by default it is set to **OFF**. This will gather the maximum information about end-user navigation activity within the professional forms. Once set, it is required to schedule a recurring concurrent program to purge the Sign-On data. To do this, schedule ***Purge Signon Audit Data*** to run monthly and set the Audit Date parameter per the organization's policy requirement for audit data retention. If the policy is 12 months, then this parameter should be set to 12 months in the past.

Figure 8 - Oracle E-Business Suite Sign-On Audit Level



Enable Page Access Tracking

Sign-On Audit only tracks navigation activity within the professional forms. Page Access Tracking logs Oracle Applications Framework (OAF) navigation activity. It also has the option of consolidating all navigation activity, Sign-On, and OAF logs into a single source.

To enable Page Access Tracking: **System Administrator -> Oracle Application Manager -> Applications Usage -> Configure**.

The following are the recommended Page Access Tracking configurations for the Integrigy Framework:

1) Monitor application
   (1) Web access = **Yes**
   (2) Form access = **Yes**

   The system profile option JTF_PF_MASTER_ENABLED stores the Web Access value (true or false).

2) Information capture level
   (1) Web = **Session Info, Cookies and All Parameters**
   (2) Form = **Login / Logout and Responsibility Changes and Form Access**

   Please note that system profile option 'JTF_PF_LEVEL' stores the Web information capture level.

JTF_PF_LEVEL	Description
22	Session info
118	Session Info and Cookies
254	Session Info, Cookies and URL Parameters
126	Session Info, Cookies and All Parameters – **Recommended by Integrigy**

3) Track applications – For Level 1 the following applications are recommended:

   - System Administration
   - Oracle Application Manager
   - Application Object Library
   - Application Shared Technology
   - Common Modules-AK

   The system profile option 'JTF_PF_ENABLED' stores a true/false value for each application in the E-Business Suite as to whether or not page access tracking is specifically enabled.

4) Optionally, configure logging for specific user(s) or responsibility(s). To do so, use Oracle Forms to set up the profile JTF_PF_ENABLED. This will be a requirement later in Level 3.
5) Schedule daily imports with the concurrent program ***Page Access Tracking Data Migration***. This Java current program calls the PL/SQL package JTF_PF_CONV_PKG.MIRGRATE_DATA to move the Page Access Tracking data from its staging tables into the JTF_PF_% tables. It also consolidates the FND_SIGNON audit logs into the JTF_PF_% tables.
6) Schedule purging with the concurrent program ***Page Access Tracking Purge Data*** – retain per company policy. If no policy exists, Integrigy recommends six to twelve months of rolling data.
7) Review the following system options based on the size of the implementation and compliance requirements:
   a) JTF_PF_FLUSH_INTERVAL for the collection time interval. The default value is 120 seconds.
   b) JTF_PF_BUFFER_SIZE for the maximum number of page log accesses in the buffer. The default value is 20 accesses.

Figure 9 - Page Access Tracking Configuration Page

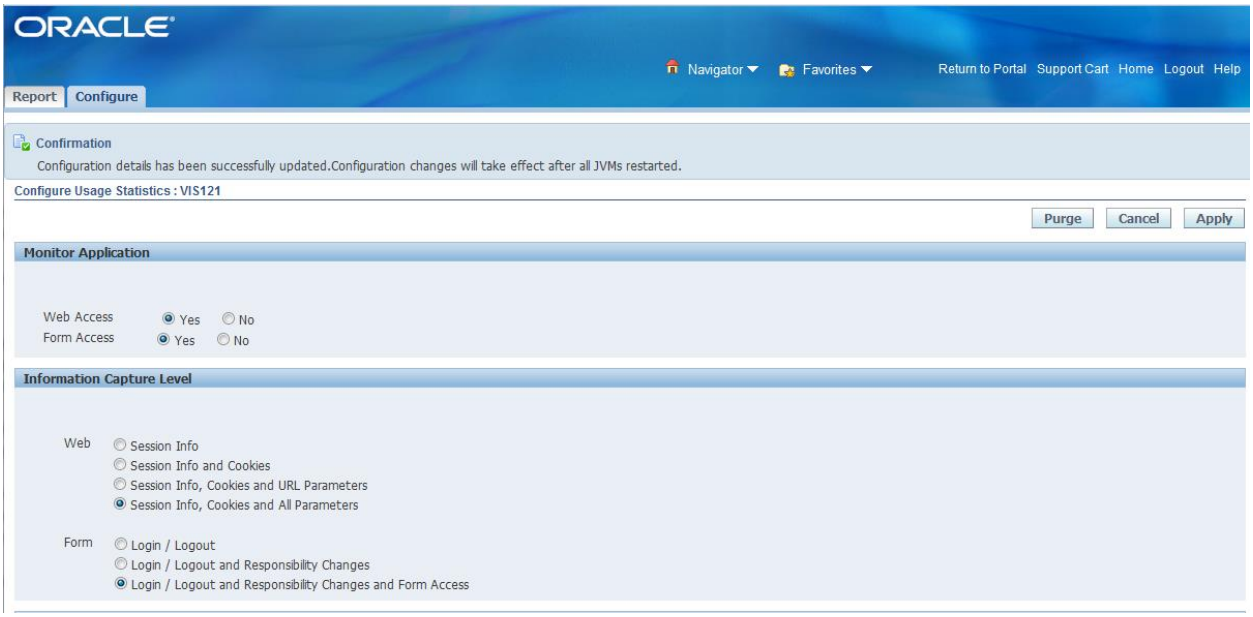
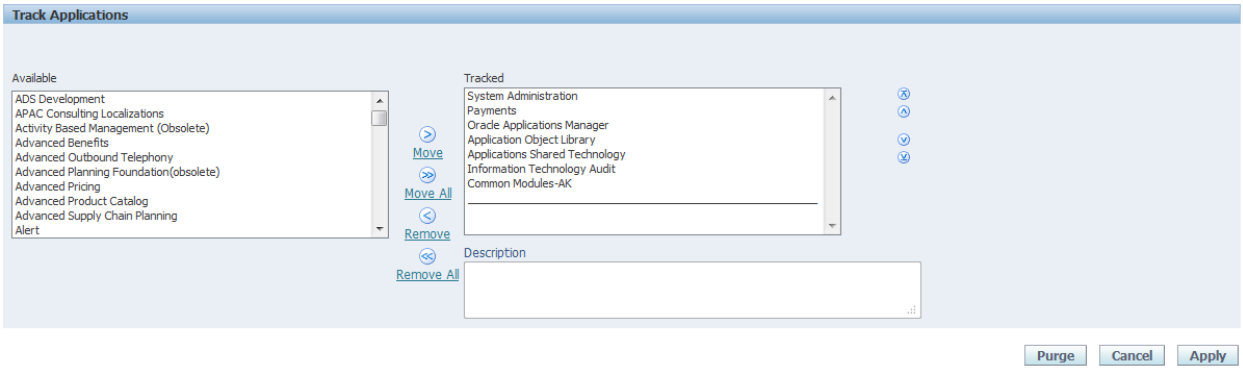


Figure 10 - Page Access Tracking Configuration Screen



Use Audit Trail on Key AOL tables

The following Application Object Library (AOL) tables (also known as "Foundation" tables) are recommended for auditing. Refer to Appendix A – How to Configure E-Business Suite AuditTrail for instructions on how to enable AuditTrail. We have identified the tables that should be audited, however, columns for each table will be site specific and need to be selected as part of the AuditTrail definition.

Table 3 – Foundation Events for Logging and Security Framework	
Framework Events	**Oracle EBS AuditTrail Tables**
E1 - Login	[1]
E2 - Logoff	[1]
E3 - Unsuccessful login	[2]
E4 - Modify authentication mechanisms	FND_PROFILE_OPTIONS (also E12, E14) FND_PROFILE_OPTION_VALUES (also E12, E14)
E5 - Create user account E6 - Modify user account	FND_USER
E7 - Create role E8 - Modify role	FND_RESPONSIBILITY
E9 - Grant/revoke user privileges	WF_LOCAL_USER_ROLES WF_USER_ROLE_ASSIGNMENTS
E10 - Grant/revoke role privileges	FND_MENUS FND_MENU_ENTRIES FND_REQUEST_GROUPS FND_REQUEST_GROUP_UNITS FND_RESP_FUNCTIONS FND_GRANTS FND_DATA_GROUPS FND_DATA_GROUP_UNITS FND_FLEX_VALIDATION
E11 - Privileged commands	FND_ORACLE_USERID
E12 - Modify audit and logging	ALR_ALERTS FND_AUDIT_GROUPS FND_AUDIT_SCHEMAS FND_AUDIT_TABLES FND_AUDIT_COLUMNS

Table 3 – Foundation Events for Logging and Security Framework	
Framework Events	**Oracle EBS AuditTrail Tables**
E13 - Objects: Create object Modify object Delete object	FND_CONCURRENT_PROGRAMS FND_EXECUTABLES FND_FORM FND_FORM_FUNCTIONS
E14 - Modify configuration settings	FND_ENABLED_PLSQL ([3] 11i only)

[1] Login/Logoff audit trail is captured with Signon Audit and stored in APPLSYS.FND_LOGINS.
[2] Unsuccessful logins are captured by default and stored in APPLSYS.FND_UNSUCCESSFUL_LOGINS.
[3] FND_ENABLED_PLSQL is generally not used in R12 as the mod_plsql functionality is disabled by default.

Security Monitoring and Auditing

For Level 1, the assumption is that centralized logging and analysis tools and/or a SIEM is not available. Standard Oracle E-Business Suite functionality will be discussed instead. Recommendations are made for what to monitor. Whom to notify in case of a monitoring alert is not possible to recommend because it will be unique to each client site and implementation.

Oracle Alerts are able to send immediate emails based on SQL statements. For most all the security alerts recommended, custom Oracle Alerts and/or custom reports can be created. Whether or not the alerts are sent immediately or in the form of a daily summary should be determined by each customer's unique risk profile.

Our recommended security monitoring and auditing alerts (Table 4) are by no means conclusive. Simple things can trigger serious high risk security events and can differ between Oracle E-Business Suite implementations. As such, the table below should be seen as much as a starting point as it is an educational tool. What to monitor for and whom to notify will largely be determined by each client's unique risk profile.

Table 4 – Level 1 Security Monitoring and Auditing Alerts			
Frame work	**What to Monitor For**	**Description**	**Source**
E1	Direct database logins (successful or unsuccessful) to EBS schema database accounts	Direct database attempts, attempts to connect other than through the E-Business Suite, should all be investigated - especially for the SYS, APPS and APPLSYSPUB.	SYS.AUD$ login activity for any of the database accounts listed in APPLSYS.FND_ORACLE_USERID (except APPS and APPLSYSPUB)
E1, E11	User SYSADMIN successful logins	Each login of the user SYSADMIN should be logged and reviewed. Daily support should not be done through this account.	APPLSYS.ICX_SESSIONS APPLSYS.FND_LOGINS

Table 4 – Level 1 Security Monitoring and Auditing Alerts			
Frame work	**What to Monitor For**	**Description**	**Source**
E1, E11	Generic seeded application account logins	Except for the GUEST accounts, immediate action should be taken if there is attempted login to one of the accounts listed Table 5 "Default Oracle E-Business Suite Users."	APPLSYS.ICX_SESSIONS APPLSYS.FND_LOGINS
E1, E11	Unlocking of generic seeded application accounts	The accounts listed in Table 5 "Default Oracle E-Business Suite Users" should always be end-dated. If the end-date for one of these accounts changes, immediate action is required.	APPLSYS.FND_USER
E1 E2	Login/Logoff	Basic login/logoff of user from Oracle E-Business Suite	APPLSYS.ICX_SESSIONS APPLSYS.FND_LOGINS (Note Proxy User sessions will appear as new logins)
E3	User SYSADMIN - unsuccessful login attempts	Multiple unsuccessful login attempts for SYSADMIN should be considered as a security event. These attempts can also lock the SYSADMIN user. Locking this user can cause applications issues.	APPLSYS.ICX_FAILURES APPLSYS.FND_UNSUCCESSFUL_LOGINS
E4	Modify authentication configurations to database	Database profiles enforce password practices. Changes to how passwords are created, used and validated need to be audited.	Database Profile statements in SYS.AUD$
E4	Modify authentication configurations to Oracle E-Business Suite	How Oracle E-Business Suite authentication occurs (local or SSO) and, if local, how passwords are controlled all need to be logged and audited.	APPLSYS.FND_PROFILE_OPTION_VALUES For profile_option_name like 'APPS_SSO%' or like 'APPS_AUTH_%' And for profile_option_name like 'SIGNON_PASSWORD%'
E6	New database accounts created	Any changes to the standard Oracle E-Business Suite database accounts or creation of new accounts should be audited. Such changes are rare and can indicate inappropriate activity.	SYS.AUD$

Table 4 – Level 1 Security Monitoring and Auditing Alerts			
Frame work	**What to Monitor For**	**Description**	**Source**
E9, E10, E12, E13, E14	Updates to AOL tables under AuditTrail	The tables recommended to be configured for Audit Trail should not change on a regular basis. Any change to these tables should be alerted or reported per client's risk polices.	Shadow "_A" tables configured for AOL Audit Trail
E12	Turning Sign-On Audit off	If enabled, disabling Sign-On audit off is a security event.	APPLSYS.FND_PROFILE_OPTION_VALUES For "SIGNONAUDIT:LEVEL"
E12	Turning off AuditTrail	If enabled, disabling Audit Trail is a security event.	APPLSYS.FND_PROFILE_OPTION_VALUES For "AUDITTRAIL:ACTIVATE" Column State in APPLSYS.FND_AUDIT_GROUPS APPLSYS.FND_AUDIT_TABLES
E12	Turning Page Access Tracking off	If enabled, disabling Page Access Tracking audit off is a security event.	APPLSYS.FND_PROFILE_OPTION_VALUES For "JTF_PF_MASTER_ENABLED"
E12	Turning Audit Trail off	If enabled, disabling audit trail is a security event.	V$PARAMETER
E12	Turning audit sys operations off	If enabled, disabling audit sys operations is a security event.	V$PARAMETER for "audit_sys_operations"
E12	Turning database audit off	If enabled, disabling database auditing off is a security event.	V$PARAMETER for "audit_trail"

Table 5 – Default Oracle E-Business Suite Users		
User Name	**Module**	**Disable/End Date (If module not being used)**
AME_INVALID_APPROVER	AME	yes
APPSMGR	AOL/FND	yes
ASADMIN	AOL/FND	yes
ASGADM	ASG	See module
ASGUEST	AS	See module
AUTOINSTALL	AOL/FND	yes
CONCURRENT MANAGER	AOL/FND	yes
FEEDER SYSTEM	AOL/FND	yes
GUEST	AOL/FND	NO

Table 5 – Default Oracle E-Business Suite Users		
User Name	**Module**	**Disable/End Date (If module not being used)**
IBE_ADMIN	IBE, ONT	See module
IBE_GUEST	IBE	See module
IBEGUEST	IBE, IBU	See module
IEXADMIN	IEX	See module
INDUSTRY DATA	AOL/FND	yes
INITIAL SETUP	AOL/FND	yes
IRC_EMP_GUEST	IRC	See module
IRC_EXT_GUEST	IRC	See module
MOBADM	ASG	yes
MOBDEV	ASG	yes
MOBILEADM	ASG	see
OP_CUST_CARE_ADMIN	XDP	see
OP_SYSADMIN	XDP	see
ORACLE12.0.0	AOL/FND	NO
ORACLE12.1.0	AOL/FND	NO
ORACLE12.2.0	AOL/FND	NO
ORACLE12.3.0	AOL/FND	NO
ORACLE12.4.0	AOL/FND	NO
ORACLE12.5.0	AOL/FND	NO
ORACLE12.6.0	AOL/FND	NO
ORACLE12.7.0	AOL/FND	NO
ORACLE12.8.0	AOL/FND	NO
ORACLE12.9.0	AOL/FND	NO
PORTAL30	AOL/FND	yes
PORTAL30_SSO	AOL/FND	yes
STANDALONE BATCH PROCESS	AOL/FND	yes
SYSADMIN	AOL/FND	NO
WIZARD	AOL/FND	yes
XML_USER	AOL/FND	yes

INTEGRIGY FRAMEWORK – LEVEL 2

The second level of the framework focuses on integrating with and/or building a centralized logging solution if such a solution does not exist. Such solutions are commonly built using enterprise logging solutions such as Splunk, HP ArcSight, RSA enVision, or Q1 Radar. There are a number of commercial and open-source solutions that can support all the logging and auditing in the Integrigy Framework. For Integrigy's framework, the specific tool is used is not important. What is important is the solution provides (1) ability to accept logs from Syslog, database connections, and reading files, (2) security and archiving of log data, and (3) unified alerting and reporting capabilities.

Centralized logging solutions protect the log data. Non-repudiation and division of duties is achieved by removing log data from each source and storing it in a secure, central location. Consolidating an organization's log data also offers significantly more options for creating security alerts that cross application, team, and geographic boundaries. Centralized logging is also a key requirement for security standards including PCI and HIPAA.

Once the foundation of centralized logging is created with Level 2, an organization can proceed to Level 3. Contact Integrigy with questions and/or assistance with specific centralized logging tools and/or vendors.

Level 2 Tasks

1. Implement centralized logging solution if does not exist
2. Redirect database logs to centralized logging
3. Configure database connector and send Oracle E-Business Suite Sign-on and navigation activity
4. Transition Level 1 alerts and build additional Level 2 alerts

IMPLEMENT CENTRALIZED LOGGING SOLUTION

The installation and configuration of tools such as Splunk (Free or Enterprise) or HP ArcSight is beyond the scope of this paper. The first requirement for Level 2 is for such a solution to be in place.

REDIRECT DATABASE LOGS TO CENTRALIZED LOGGING

Writing logs to the operating system is more secure for many reasons, including providing a separation of duties between DBAs and system administrators. There are two steps:

1. To route Oracle database audit logs to the operating system instead of the database set **AUDIT_TRAIL** parameter to **OS** and set **AUDIT_FILE_DEST** to provide a location to write the log files**.**
2. Write logs using the Syslog format. In the init.ora file for the instance, set the **AUDIT_TRAIL** parameter to **OS** and **AUDIT_SYSLOG_LEVEL** to 'LOCAL1.WARNING' or another valid Syslog setting. This setting may be used by the logging server to classify the event.

CONFIGURE DATABASE CONNECTOR FOR AUDIT DATA IN DATABASE TABLES

With the centralized logging solution in place, configure a database connector per the vendor's instructions. Once the connector is in place, pass the Oracle E-Business Suite navigation tables to the centralized logging

solution. Custom queries are required for many of the tables as these tables have referential IDs rather than usable values in many columns (e.g., USER_ID vs. USER_NAME).

Table 6 – Oracle E-Business Suite Navigation Tables (Framework: E1, E2, E3)	
Table	**Description**
APPLSYS.FND_USERS	This is the base table defining all users and their associated email addresses and links to HR records
APPLSYS.FND_LOGINS	Sign-On Audit table
APPLSYS.FND_LOGIN_RESPONSIBILITIES	Sign-On Audit table
APPLSYS.FND_LOGIN_RESP_FORMS	Sign-On Audit table
APPLSYS.FND_UNSUCCESSFUL_LOGINS	Unsuccessful logins via the Personal Home Page (Self Service/Web Interface) are stored in both the FND_UNSUCCESSFUL_LOGINS and ICX_FAILURES tables.
ICX.ICX_FAILURES	The ICX_FAILURES table contains more information than the FND_UNSUCCESSFUL_LOGINS. Failed logins to the Professional Interface (Forms) are only logged to the FND_UNSUCCESSFUL_LOGINS tables.
JTF.JTF_PF_SES_ACTIVITY	Page Access Tracking Table
JTF.JTF_PF_ANON_ACTIVITY	Page Access Tracking Table
JTF.JTF_PF_APP_SUMM	Page Access Tracking Table
JTF.JTF_PF_HOST_SUMM	Page Access Tracking Table
JTF.JTF_PF_PAGE_SUMM	Page Access Tracking Table
JTF.JTF_PF_USER_SUMM	Page Access Tracking Table
APPLSYS.WF_USER_ROLE_ASSIGNMENTS	Need for E-Business end-user entitlements and role assignments
APPLSYS.FND_USER_RESP_GROUPS	Need for E-Business end-user entitlements and role assignments

How to Find The IP Address of an End-User

For those looking to pass the actual IP address of the Oracle E-Business Suite end-user to the centralized logging solution, this might or might not be possible. To find the IP address of an end-user, Oracle Support Note 879092.1, "How To Find The IP Address Of The Client Machine From Where A Particular Forms User Is Connected?" provides a two-step process. Sign-on Audit must be enabled and the shell scripts provided in the Support Note need to be run. If a load balancer is in use, it should be configured to relay the IP address of the end-user otherwise the shell scripts will note work.

TRANSITION LEVEL 1 ALERTS AND BUILD ADDITIONAL LEVEL 2 ALERTS

As much as possible transition all alerting built for Level 1 to the centralized logging solution. Alerting out of the logging solution (or SIEM) will be more efficient and can provide event correlation capabilities. Moreover, as more alerts will be built, it will consolidate alerting into a single tool.

As with Level 1, the table below is by no means conclusive. Simple things can trigger serious high risk security events. As such, the table below should be seen as much as a starting point as it is an educational tool. What to monitor for and whom to notify will largely be determined by each client's unique risk profile.

Table 7 – Level 2 Security Monitoring and Auditing Alerts			
Event	**What to Monitor For**	**Description**	**Source**
E1	Successful or unsuccessful login attempts to E-Business without network or system login	Logins or attempts to login into the Oracle E-Business Suite without first logging onto the network or gaining access to the building should be flagged and investigated.	ICX_FAILURES FND_UNSUCCESSFUL_LOGINS
E1	Successful or unsuccessful logins of named database user without network or system login	Named database accounts, those associated with staff and employees for the purposes of support should be monitored for if the user has first logged on to the network and/or gained access to the building.	Database log
E3	Horizontal unsuccessful application attempts – more than 5 users more than 5 times within the hour	Attempts to brute force groups of users should be alerted and investigated. This alert may be based per IP address or other system identifier. The specific alert threshold will be unique to each client.	ICX_FAILURES FND_UNSUCCESSFUL_LOGINS
E3	Horizontal unsuccessful direct database attempts – more than 5 users more than 5 times within the hour	Attempts to brute force groups of users should be alerted and investigated. This alert may be based per IP address or other system identifier. The specific alert threshold will be unique to each client.	Database log
E9	End-users granted System Administration Responsibility	End-users gaining access to the highly privileged system administration rights should be carefully reviewed.	APPLSYS.WF_USER_ROLE_ASSIGNMENTS
E9	Addition or removal of privileges granted to user SYSADMIN	SYSADMIN, and its associated responsibility and menu, should not be used for day-to-day support. Additions of functional menus and roles should be investigated.	APPLSYS.WF_USER_ROLE_ASSIGNMENTS
N/A	Monitor for database attacks	The following standard Oracle error messages may indicate a potential database attack: ORA-29532, ORA-28000, ORA-24247, ORA-29257, ORA-01031	Database log

INTEGRIGY FRAMEWORK – LEVEL 3

Level 3 builds on the connectivity and basic centralized logging established in Level 2. This level identifies additional database and application server logs to be interfaced and also calls for the inclusion of Oracle E-Business Suite functional configuration tables to be monitored and for additional administration navigation activity to be logged. These additions to the centralized logs allow Oracle E-Business Suite clients to meet compliance requirements such as PCI, SOX, and HIPPA and provide vital automation of the compliance tasks.

People and business processes commonly use multiple applications and technologies. The objective of centralized logging is to consolidate logs from all applications and technologies. While the E-Business Suite is but one application, as the Enterprise Resource Planning (ERP) application, it is the cornerstone of most business processes. This is why the objective of Level 3 is the integration of E-Business Suite functional logs with the centralized logging solution.

Level 3 is continuous. Once a baseline is established from which alerts and reports are used to report anomalies, as business processes change, tolerances and alerts need to be adjusted to the new baseline. As well, the possibilities of new security alerts and audits is limited by the data consolidated into the centralized logging solution from the Oracle E-Business Suite, ticket systems, password vaults, network, badging systems, or any other sources capable of producing logs.

Level 3 Tasks

1. Pass additional database logs and application server logs
2. Begin passing logs for E-Business Suite functional setups and configurations
3. Automate compliance tasks
4. Create additional alerts

ADDITIONAL DATABASE AND APPLICATION SERVER LOGS

Each log management or SIEM vendor will have their own set of log parsers and capabilities. The recommendation for Level 3 is to send additional database and web server logs to assist with additional logging for who is coming into the Oracle E-Business Suite, from where and when.

Apache Logs

Apache server logging is defined in the Apache configuration file (HTTPD.CONF) which is located at $ORA_CONFIG_HOME/10.1.3/Apache/Apache/conf/httpd.conf. For the Oracle E-Business Suite, the Apache logging level is set by the Autoconfig using the parameter 's_apache_log_level'. Integrigy recommends the default log setting of 'warn'.

Apache Log Levels	Description
emerg	Emergencies, system is not useable
alert	Action must be taken
crit	Critical conditions
error	Error conditions
warn	**Warning conditions - Default**
notice	Normal but significant condition
info	Information
debug	Debug level messages

Apache Logs	Location within E-Business Suite Instance Home
HTTP and PLS access logs	$LOG_HOME/ora/10.1.3/Apache/access_log*
HTTP listener error log for both http & pls	$LOG_HOME/ora/10.1.3/Apache/error_log*
Security Logs	$LOG_HOME/ora/10.1.3/Apache/mod_rewrite.log $LOG_HOME/ora/10.1.3/Apache/sec_audit.log $LOG_HOME/ora/10.1.3/Apache/sec_debug.log

Listener Log

The database listener log provides information regarding database connections, for example IP addresses of clients, and it should be sent to the centralized logging solution. Within the listener's control file ($TNS_ADMIN/listener.ora), confirm that logging is enabled (LOG_STATUS = On) and the location of the listener log (parameter = LOG_DIRECTORY_listener_name).

E-Business Suite Functional Setup and Configurations

Level 2 focused on system administration. Level 3 focuses on functional setups and key controls to support sophisticated security and audit alerts. Level 3 should be complementary to any Government Risk and Compliance (GRC) implementations. GRC and centralized logging (or SIEM) solutions have similarities but serve separate purposes. Integrigy recommends a GRC solution be implemented to satisfy segregation of duties and functional risk and compliance. However, if no GRC implementation exists, then the centralized logging solution can be expanded to meet many risk mitigation needs.

A first effort could be alert on key roles and responsibilities within the E-Business Suite. Responsibilities that are infrequently used to configure and setup approval rules, cash controls, or credit card encryption need to be closely monitored. Only appropriate individuals and/or teams should be using these responsibilities and menus.

For example, an alert or a report could be set to flag a logon to Payments Setup (IBY) if it is used outside first shift Eastern time US.

Examples of Responsibilities / Role Activity	
Application/Responsibility	**What to audit**
Payments Setup Administrator (IBY)	All accesses
Trading Community Architecture	All accesses
Approvals Management Administrator (AME)	All accesses
Workflow Administrator	All accesses
Cash Management Setup	All accesses
Order Entry Administrator	All accesses

In the example above, expanding which applications are tracked through Page Access Tracking should be considered.

Once key roles and responsibilities are being monitored, the focus should turn to those tables that control the functional setups of the Oracle E-Business Suite. Which tables need to be monitored depends on the modules the client is using. The alerts do not need to incorporate the entire records of these tables. The primary key and the four Who Columns (About this) record will suffice for most monitoring.

Additional examples of alerts based on functional setups and configurations:

- Changes to Credit card encryption settings (IBY.IBY_SYS_SECURITY_OPTIONS)
- Changes to supplier bank accounts (IBY.IBY_EXT_BANK_ACCOUNTS)

Automate Compliance Tasks

Throughout this document, the recommended logging alerts are all able to be mapped back to PCI, HIPAA, NIST 800-53, IS0 27000, and SOX (COBIT). By building these alerts, staff members do not need to manually monitor and need only to review and confirm. This should largely automate compliance tasks, however, each client will have their own unique compliance requirements.

Additional Alerts

As with Levels 1 and 2, the table below is by no means conclusive. Simple things can trigger serious high risk security events. As such, the table below should be seen as much as a starting point as it is an educational tool. What to monitor for and whom to notify will largely be determined by each client's unique risk profile.

Table 8 – Level 3 Security Monitoring and Auditing Alerts

Event	What to Monitor for	Description	Source
E1	Key functional setup and configuration activity	Add additional responsibilities (and possibly Users) to Page Access Tracking for those modules critical for the client's functional setups and configurations.	JTF.JTF_PF_SES_ACTIVITY JTF.JTF_PF_SESSION_SUMM JTF.JTF_PF_APP_SUMM JTF.JTF_PF_HOST_SUMM JTF.JTF_PF_PAGE_SUMM JTF.JTF_PF_USER_SUMM JTF.JTF_PF_ANON_ACTIVITY
E1	SYSADMIN usage pattern	The user SYSADMIN should not be used for day-to-day support. From where on the network, when and how often should be monitored and regularly reviewed.	ICX_SESSIONS FND_LOGINS Standard report

Table 8 – Level 3 Security Monitoring and Auditing Alerts			
Event	**What to Monitor for**	**Description**	**Source**
E6, E11	E-Business Suite Proxy user grants	Proxies allow one user to act on behalf of others. Creating a proxy should be reported if not also raise an alert. Proxies also need to be regularly reviewed for appropriateness.	WF_USER_ROLE_ASSIGNMENTS WHERE ROLE = 'UMX|UMX_MANAGE_PROXIES'
E5, E11	Database account creation and privilege changes	Whenever a database account is created it should be reported. Changes to privileges should also be reported. E-Business Suite database accounts should only be rarely created or changed. Monitoring and periodic reviews are required.	SYS.DBA_USERS
E6	FND User email account changes	Changes to end-user email addresses need to be carefully watched. The risks include accounts being taken over through password resets to financial approvals controls and information leakage.	FND_USER
E14	Tables listed in APPLSYS.FND_AUDIT_TABLES	For any table being audited, changes should be reported, especially if not included in the above (Level 3 alert #5).	These tables will all have a corresponding *_A shadow audit table
E13, E14	Reconcile creation and updates to Forms, Menus, Responsibilities, System Profiles and Concurrent Programs	Changes to the records that define E-Business application security and key functionality should be monitored for appropriateness. The time of day, location on the network should be weighted in the alerts.	FND Tables

APPENDIX A – HOW TO CONFIGURE E-BUSINESS SUITE AUDITTRAIL

Step 1 – Set AuditTrail Profile Option

The System Profile Option ***AuditTrail:Activate*** must be set to ***Yes.*** The default value for ***AuditTrail:Activate*** is ***null*** (which equals No).

Be sure to log out of the applications to activate the profile option in your session.

Step 2 – Select the Audit Installations

- As System Administrator, select ***Security -> AuditTrail -> Install***.
- Query all schemas. For R12, some schemas are selected by default and should be unchecked to remove any unnecessary auditing.
- Check all the schemas for which auditing should be enabled. For example, if you want to audit FND_USERS, you would check APPLSYS since the FND_USERS table is in the APPLSYS schema.
- Save your selections.

Step 3 – Create a New Audit Group

- As System Administrator, select ***Security -> AuditTrail -> Groups***.
- Query all existing Audit Groups and remove all unnecessary groups.
- Create a new audit group by setting the ***Application Name*** to the application that owns the table (e.g., Application Object Library for APPLSYS), the ***Audit Group*** to a new name (e.g., My Audits), and ***Group State*** should be set to ***Enable Requested***.
- Add the tables to be audited. Columns will be defined in the next step.
- Save the new audit group.

Step 4 – Define Table Columns to be Audited

For each table defined in the above step, define the columns to be audited using these steps –

- As System Administrator, select ***Security -> AuditTrail -> Tables***.
- Query the table name.
- The primary key columns will always be saved. Add the columns that need to be audited. Do not ever add the following columns as user information is automatically added:

  Creation Date
  Created By
  Last Update Login
  Last Update Date
  Last Updated By

- Save the columns.

Step 5 – Run AuditTrail Update Program

Run the ***AuditTrail Update Tables*** program to activate the auditing. This program will create a shadow table for each audited table and create triggers on each audited column in the original table. The shadow table will have the same name as the audited table appended with "_A". Two views will be created for each column with the names "_AC#" and "_AV#" where # is a sequential number.

Step 6 – Setup Purge

The AuditTrail data should be purged on a periodic basis. There is no standard purge program and the AuditTrail must be manually disabled to permit purging.

Use the following procedure to purge audit date –

1. As System Administrator, select ***Security -> AuditTrail -> Groups*** *and* select the "Security Audit" group and then set the state of the group to be purged to a value of "Disable – Purge Table"
2. Run the "Audit Trail Update Tables" Report
3. Purge the data from the shadow table
4. Select ***Security -> AuditTrail -> Groups***
5. Select the "Security Audit" group and set the group state to "Enable"
6. Run the "Audit Trail Update Tables" Report

Troubleshooting

See the *Oracle E-Business Suite System Administration's Guide - Security* Chapter 5 for more information on configuring and accessing the AuditTrail information. Oracle Support Note 105624.1 contains information on troubleshooting AuditTrail issues.

REFERENCES

GENERAL

- "Building an Audit Trail in an Oracle Applications Environment", Jeff Hare and Stephen Kost, http://www.integrigy.com/files/Building_an_Audit_Trail_in_an_Oracle_Applications_Environment.pdf
- "Real World Database Auditing", Stephen Kost, Collaborate 2009, Session #602, http://www.integrigy.com/files/IOUG%202009%20-%20Real%20World%20Database%20Auditing.pdf
- Oracle E-Business Suite System Administrator's Guide – Security Release 12.1, Oracle Corporation, Part No. E12843-05, June 2013, http://docs.oracle.com/cd/E18727_01/doc.121/e12843.pdf
- "Oracle E-Business Suite Development & Extensibility Handbook", Anil Passi and Vladimir Ajvaz, McGraw Hill – Oracle Press, 2010
- "Oracle E-Business Suite Security", John Able, McGraw Hill – Oracle Press, 2007
- "Oracle Database Security Guide 11g Release 1 (11.1) B28531-20", Oracle Corporation, July 2013, http://docs.oracle.com/cd/B28359_01/network.111/b28531.pdf
- "Using Audit Vault With Oracle E-Business Suite", Oracle Corporation, Steve Chan, 14 July 2011, https://blogs.oracle.com/stevenChan/entry/using_audit_vault_with_oracle
- "Logging and Log Management", Chuvakin, Schmidt and Phillips, Elsevier, Inc. 2013

ORACLE SUPPORT

- "Secure Configuration Guide for Oracle E-Business Suite Release 12", Oracle Support Note ID 403537.1, Oracle Corporation, 9 October 2013, https://support.oracle.com/rs?type=doc&id=403537.1
- "Troubleshooting (Audit Trail)", Oracle Support Note ID 105624.1, Oracle Corporation, 10 December 2013, https://support.oracle.com/rs?type=doc&id=105624.1
- "Overview of Oracle E-Business Suite AuditTrails", Oracle Support Note ID 60828.1, Oracle Corporation, 27 August 2013, https://support.oracle.com/rs?type=doc&id=60828.1
- "Page Access Tracking in Oracle Applications Release 12", Oracle Support Note ID 402116.1, Oracle Corporation, 21 April 2013, https://support.oracle.com/rs?type=doc&id=402116.1
- "Understanding Data Auditing in Oracle Application Tables", Oracle Support Note ID 69660.1, Oracle Corporation, 10 December 2013, https://support.oracle.com/rs?type=doc&id=69660.1
- "Auditing How To, Troubleshooting, and Error Message Document", Oracle Support Note ID 1579731.1, Oracle Corporation, 3 September 2013, https://support.oracle.com/rs?type=doc&id=1579731.1
- "Integrating Oracle E-Business Suite Release 12 with Oracle Database Vault 10.2.0.3", Oracle Support Note ID 744363.1, Oracle Corporation, 5 December 2013, https://support.oracle.com/rs?type=doc&id=744363.1
- "Master Note For Oracle Database Auditing", Oracle Support Note ID 1299033.1, Oracle Corporation, 7 January 2014, https://support.oracle.com/rs?type=doc&id=1299033.1
- "Master Note for Oracle Database Fine-Grained Auditing", Oracle Support Note ID 1533543.1, Oracle Corporation, 25 April 2013, https://support.oracle.com/rs?type=doc&id=1533543.1
- "Master Note For Oracle Audit Vault", Oracle Support Note ID 1199033.1, Oracle Corporation, 23 October 2013, https://support.oracle.com/rs?type=doc&id=1199033.1

About Integrigy

Integrigy Corporation (www.integrigy.com)

Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. AppDefend, our enterprise web application firewall is specifically designed for the Oracle E-Business Suite. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

INTEGRIGY
Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681 USA
888/542-4802
www.integrigy.com