DOWNLOAD PDF ORACLE E-BUSINESS SUITE SECURITY GUIDE

Chapter 1 : Frequently Asked Questions about EBS Security | Oracle E-Business Suite Technology Blog

Migrating Data Between Oracle E-Business Suite and Oracle Directory Services Enabling and Disabling Users Synchronizing Oracle HRMS with Oracle Directory Services.

Function Security Reports Overview of Data Security Data Security allows administrators to control user access to specific data, as well as what functions users can apply to that data. Function security can be considered "global" data security, in that access to a function is granted regardless of the data. Concepts and Definitions Objects Data Security uses the concept of an Object to define the data records that are secured. Object Data security permissions are managed on objects. Business entities such as Projects and Users are examples of objects. Only a securable business-level concept should be registered as an object. An object definition includes the business name of the object and identifies the main table and primary key columns used to access the object. An object instance generally corresponds to a row in the database. An instance is identified by a set of one or more primary key values as defined by the object. In addition, "All Rows" for an object indicates all data rows of the object. Object Instance Set An object instance set is a group of related object instances within an object. All instances that satisfy the predicate are considered members of the object instance set. The specific instances in the set can vary over time as object instance attributes change, or as new object instances are created. User and role information is stored in the Oracle Workflow directory service. For more information, see: Privileges given to users and groups determine their access to secured objects. The data security system allows you to assign privileges to groups of users instead of assigning privileges to each user individually. Users Users are individuals who have access to software applications at a particular enterprise. A user must have a unique name and should map one-to-one with an individual human or system. Groups Users can belong to Groups. The grouping can come from position or organization relationships modeled in applications such as Oracle Human Resources. Alternatively, ad-hoc groups can be created explicitly for security purposes. A group is sometimes referred to as a role. Functions and Permissions A function or a permission is the smallest unit of securable product functionality. You can register function definitions with the security system to represent actions that can be performed on an object or on the system in general. Granting a function to a set of users gives them permission to perform that function, and so a function may also be referred to as a permission. There are two broad categories of functions and permissions: An executable function definition must contain all information necessary to launch the function; often this includes the form name or URL plus parameters. The code that implements an abstract function calls the function security system to test whether the abstract function is granted. The system only allows the action if the abstract function is granted. Functions and permissions can either be at the system level or be sensitive to a data context. Navigation Menus and Permission Sets Functions and permissions are grouped into related sets so that administration of these functions can be performed in higher-level business terms. Functions and permissions are bundled into named sets, which can be defined for two purposes: Each set can also contain other sets. Menus are defined for navigation purposes and group UI pages into functional areas. Users access menus by selecting responsibilities. Permission sets are granted to users or roles through permission assignments grants. Grants A grant authorizes a particular role to perform a specified action or actions set of functions on a specified object instance or object instance set. Note that where you are creating a data security policy for an object by creating a grant, you need to include that object in your grant definition. Other than in this specific type of case, you do not need to specify an object in your definition. Security Context Security context refers to the context of the data in which the user is working. For example, data context could be the organization or responsibility with which the user is logged in. Implementation of Data Security Implement data security by granting access to a set of functions either a navigation menu or a permission set to a user or group of users. Data security policies can reflect access to: Each application user is assigned at least one responsibility. The information in this section can also be used to define a responsibility in the HTML-based Create Responsibility page. A responsibility determines whether the user accesses Oracle E-Business Suite or Oracle Mobile Applications; which applications functions a user can use; which reports and concurrent

programs the user can run; and which data those reports and concurrent programs can access. Responsibilities cannot be deleted. Overview of Function Security Before defining your responsibility, do the following: Use the Request Groups window to define the Request Group you wish to make available with this responsibility. Use the Menus window to view the predefined Menu you can assign to this responsibility. Responsibilities Block An application name and a responsibility name uniquely identify a responsibility. Responsibility Name If you have multiple responsibilities, a pop-up window includes this name after you sign on. Application The owning application for the responsibility. Responsibility Key This is the internal key for the responsibility that is used by loader programs, concurrent programs that load messages, user profiles, user profile values, and other information into Oracle E-Business Suite tables. The responsibility key is unique per application. Avoid using the following characters in the responsibility keys: The default value for the start date is the current date. If you do not enter an end date, the responsibility is valid indefinitely. You cannot delete a responsibility, because its information helps to provide an audit trail. You can deactivate a responsibility at any time by setting the end date to the current date. If you wish to reactivate the responsibility later, either change the end date to a date after the current date, or clear the end date. Available From This is the navigator from which the responsibility will be available Oracle E-Business Suite forms navigator, mobile navigator. A responsibility may be associated with only one Oracle E-Business Suite system. Data groups are used for backward compatibility only. Oracle Application Framework does not support the data groups feature. You should not define any custom data groups. Transaction managers can only process requests from responsibilities assigned the same data group as the transaction manager. Note that such users can also access requests from a Submit Requests window you customize with a request group code through menu parameters Note: The Request Security Groups feature is provided for backward compatibility. New responsibilities should be created in accordance with Role-Based Access Control and should not have a default request security group. Menu exclusions should be used for backward compatibility only. Define function and menu exclusion rules to restrict the application functionality accessible to a responsibility. Type Select either Function or Menu as the type of exclusion rule to apply against this responsibility. When you exclude a menu, all of its menu entries, that is, all the functions and menus of functions that it selects, are excluded. Name Select the name of the function or menu you wish to exclude from this responsibility. The function or menu you specify must already be defined in Oracle E-Business Suite. Table columns represent attributes that can be assigned to a responsibility as Securing Attributes or Excluded Attributes. These attributes are defined in the Web Application Dictionary. Excluded Items Use the List of Values to select valid attributes. You can assign any number of Excluded Attributes to a responsibility. Securing Attributes Use the List of Values to select valid attributes. You can assign any number of securing attributes to the responsibility. For more information on setting up system administration for the HRMS products, see: This user is an authorized user of Oracle E-Business Suite, and is uniquely identified by a username. If you have upgraded from a previous release of Oracle E-Business Suite, ensure that you have run the Party Merge concurrent program to update your user data. If you have not run this program, you may receive errors in querying your user data. For more information, see the Oracle Trading Community Architecture documentation. Users Block Enter these fields for the user. The username should only contain characters allowed by Oracle Single Sign-On. Or, for a group account, you can define the application username so as to indicate the purpose or nature of the group account. Password Enter the initial password of an application user. An application user enters this password along with his username to sign on to Oracle E-Business Suite. A password must be at least five 5 characters and can be up to thirty 30 characters. All characters are allowed except control characters, which are non-printable. Oracle encourages the use of non-alphanumeric characters because they add complexity, making passwords harder to guess. This window does not display the password you enter. After you enter a password, you must re-enter it to ensure you did not make a typing error. If the application user already exists and the two entries do not match, the original password is not changed and an error message is displayed.

Chapter 2 : Troubleshooting Guide for BI Publisher Enterprise E-Business Security Model

Single Sign-On Integration Overview of Single Sign-On Integration. This chapter is intended to provide guidance for those planning to deploy or integrate Oracle E-Business Suite Release in an enterprise single sign-on environment.

Forms A series of pop-up windows will appear, leading the user to the Oracle Access Manager login page for re-authentication. When an application session is terminated because the maximum valid period has been reached, or because of a period of user inactivity, Oracle E-Business Suite redirects the user to Oracle Access Manager for re-authentication. Oracle Access Manager checks the single sign-on cookie; if it is still valid, the user is redirected back to Oracle E-Business Suite Release If the single sign-on cookie has expired as well, Oracle Access Manager requires the user to authenticate again before redirecting him back to Oracle E-Business Suite Release The application session timeout value takes precedence over the Oracle Access Manager timeout settings. For example, until an application session times out or the user explicitly logs out , a user may continue to access the partner application even if his Oracle Access Manager security cookie has expired. User Management Options This section describes the various options for management of users in a single sign-on environment. Local Access to Oracle E-Business Suite Selected users can be permitted to log in to the application directly, that is, without going through the single sign-on process. This allows users such as the system administrator to troubleshoot a configuration when Oracle Access Manager is not functioning correctly, or is unavailable. Such local users can now log into the application directly by using the applications login page, AppsLocalLogin. This shared information has the following characteristics: A GUID uniquely identifies a user across multiple systems. A number of processes are used to establish this link. The most commonly used ones are explained below, and the rest in the more advanced deployment scenarios later in this section. The provisioning system consists of components of both Oracle Directory Services and Oracle E-Business Suite that queue user events on each system, plus an Oracle Directory Services process that periodically pushes or pulls these events to or from Oracle E-Business Suite. The provisioning process establishes the GUID link for provisioned accounts. During this process, single sign-on accounts are automatically linked to Oracle E-Business Suite application accounts. Provisioning has the following characteristics: Once linked, user changes from either system can be provisioned into the other. The provisioning process between Oracle Directory Services and each Oracle E-Business Suite instance is determined by a provisioning profile. The provisioning profile controls which user events are provisioned, the direction of provisioning, and the user attributes included in each event. Oracle E-Business Suite is said to be a provisioning integrated application with Oracle Directory Services when a provisioning profile is created for it. Refer to the Supported Attributes section for information on which attributes can be provisioned between the systems, and Configuring Directory Integration Platform Provisioning Templates for more details on the provisioning process. Creating New Users After the initial migration, you may choose to allow new users to be created either from Oracle Directory Services or from Oracle E-Business Suite, and then provision them into the other system. Bidirectional Provisioning Alternatively, you may choose to create new users from either Oracle Directory Services or Oracle E-Business Suite, and then provision them into the other system. Bidirectional provisioning requires careful planning, and the following restrictions must be considered: Whether new users are created in either Oracle Directory Services or Oracle E-Business Suite, they must be granted the appropriate roles or responsibilities using Oracle E-Business Suite User Management in order to access application functionality. As there is no mechanism to roll back the original change on the system that triggered the event, the failure can put the entire system into an unstable state. It is therefore essential to coordinate the account policy on all the systems involved, and place appropriate safeguards on the user creation process. For example, user names created directly on one system need to be chosen in the context of names used across the single sign-on environment. Updating User Information User information stored in Oracle Directory Services single sign-on accounts is generally managed independently of user information stored in Oracle E-Business Suite Release System administrators must decide: This determines the provisioning direction for that attribute. Note the following current restrictions: However, if changes are made

to user data in Oracle Directory Services, the HR connector does not synchronize these changes back to HR. A bidirectional connector is planned for a future build. However, the provisioning process may be set up so that when a single sign-on account in Oracle Directory Services is deleted, the associated Oracle E-Business Suite application accounts is end-dated. Subject to organizational security and audit policies, it may be preferable to disable single sign-on accounts in Oracle Directory Services rather than delete them, since this allows an applications account to be re-enabled at a later date as required. This can be particularly useful in the case of contractors who may leave and rejoin. Password Management One of the major objectives of single sign-on integration is centralized user password management using Oracle Directory Services, which provides the following features: End-User Password Changes The majority of end users will be able to change their single sign-on passwords using the standard methods provided by Oracle Directory Services. For example, users may employ Oracle Identity Manager. Password Policies Oracle Directory Services is designated as the master user directory for passwords. For example, Oracle Directory Services system administrators may establish policies for password expiration, minimum length, and alphanumeric mixes. If the provisioning profile specifies that passwords in application accounts are to be provisioned from Oracle E-Business Suite Release Passwords stored in Oracle Directory Services are case sensitive. Mixed case passwords in Oracle E-Business Suite are migrated with the case preserved. This is true even if Oracle Directory Services or the third-party LDAP directory has been designated as the master user directory for passwords. All existing password-related features in the Oracle E-Business Suite remain the same for local accounts. For users who have both single sign-on and local access to Oracle E-Business Suite, local password change in Oracle E-Business Suite can be synchronized to Oracle Directory Services, if the provisioning profiles are set up accordingly. The reverse direction is not possible, because Oracle Directory Services only stores the hash of the passwords, not encrypted passwords as Oracle E-Business Suite does. Critical Implementation Decisions Oracle Directory Services has a powerful and flexible set of configuration options. Most Oracle E-Business Suite system and security administrators will be able to use the default Oracle Directory Services configuration. Security administrators with advanced security requirements may choose to use alternative Oracle Directory Services configurations. Items of particular importance to Oracle E-Business Suite integration include: Identity management realm What attribute is chosen as the nickname attribute Whether new users are to be created: If so, what user attributes are to be provisioned, and the direction of provisioning. Oracle Access Manager settings: Single Sign-On Profile Options. Set Oracle E-Business Suite profile options see: Override at the user level for users who have special needs. The solutions given should be interpreted as guidelines or building blocks rather than definitive instructions, as all real world deployments will be unique. In the cases presented, the solutions are built upon the basic scenario discussed above, and only highlight those actions that are different from or additional to, the basic one. Other than the default seeded administrative accounts, no user accounts have been registered yet. No single sign-on infrastructure in place. Oracle Access Manager authenticates user credentials against user entries in Oracle Directory Services. If Oracle Directory Services is the source, details of user accounts can be propagated to each Oracle E-Business Suite instance by using the provisioning process. If an Oracle E-Business Suite instance is the source, the provisioning process will propagate user accounts from that instance to Oracle Directory Services, and then to the other Oracle E-Business Suite instances. Solution Details User Management Options In this solution, the system administrator must decide which component will be the point of user enrollment and the source of truth for user information. Oracle Directory Services is the point of user enrollment and source of truth. After a user is created in Oracle Directory Services, the user identity can be propagated to each Oracle E-Business Suite instance using the provisioning process. The provisioning profile can also be configured such that user profile information change in Oracle Directory Services can be propagated to each Oracle E-Business Suite Release Other than the default seeded Release A third-party authentication mechanism is in use as a corporate single sign-on solution. A third-party LDAP directory is in use as a corporate user directory. Oracle E-Business Suite and Oracle Access Manager need to be set up to enable Oracle E-Business Suite delegation of authentication to Oracle Access Manager, which in turn delegates the functionality to the third-party single sign-on authentication mechanism. Oracle Directory Services needs to be set up to synchronize a minimal set of user

attributes when integrating with a third-party LDAP directory. The user is also logged out of the third-party single sign-on solution, if the administrator has set this up in the samplecleanup script. Oracle recommends retaining the third-party LDAP directory as the master source of truth for user information. Creation of a new single sign-on account in the third-party LDAP directory automatically triggering the creation of a new single sign-on account in Oracle Directory Services. Ability to specify users to be synchronized, and which attributes of the users are to be created in Oracle Directory Services. System administrators also create provisioning profiles to integrate Oracle E-Business Suite Release 12 with Oracle Directory Services, which results in: Creation of a new account in Oracle Directory Services automatically triggering the creation of a new application account in Oracle E-Business Suite Release Ability to specify user attributes created in Oracle E-Business Suite. Updating User Information optional System administrators can configure synchronization profiles to synchronize some or all of the user attributes from the single sign-on account in the third-party LDAP directory into the single sign-on account in Oracle Directory Services when those attributes are modified. System administrators can configure provisioning profiles to provision some or all of the user attributes from Oracle Directory Services into Oracle E-Business Suite when those attributes are modified. Terminating and End-Dating Users Synchronization and provisioning profiles can also be used to configure the system such that terminating a user in the third-party LDAP directory also end-dates the user in Oracle E-Business Suite. Password Management Password management can, if desired, remain as it was before the integration. Most end users should use the methods provided by the third-party LDAP directory for password maintenance functions. To reset single sign-on passwords, an administrator should follow the methods provided by the third-party LDAP directory. Security administrators with advanced security requirements may choose to use alternate Oracle Directory Services configurations. Oracle E-Business Suite integration:

Chapter 3 : Oracle E-Business Suite Security Guide

Oracle E-Business Suite, the Oracle E-Business Suite technology stack, and optional Oracle Technology integrations provide various auditing and logging capabilities. Deciding which one to use and how to use it will depend on what you're trying to achieve.

Chapter 4 : Security Best Practices for Release 12 | Oracle E-Business Suite Technology Blog

Oracle Application Object Library Security Overview of Oracle E-Business Suite Security. As System Administrator, you define Oracle E-Business Suite users, and assign one or more responsibilities to each user.

Chapter 5 : Oracle E-Business Suite | Integrigy

Keep up-to-date on the latest Oracle E-Business Suite Release Update Packs (RUPs) and Updates for Oracle E-Business Suite Release and Often times the latest releases and RUPs include security fixes and new security features.

Chapter 6 : Integrigy Guide to Auditing and Logging in Oracle E-Business Suite | Integrigy

Oracle E-Business Suite (EBS) version 12 is an internet-enabled product that can be managed from a single site. Version 12 is current as of A company can operate a single data center with a single database, similar to other ERP products.

Chapter 7 : Oracle E-Business Suite Financials R A Functionality Guide | PACKT Books

A quick reference guide for securing the Oracle E-Business Suite (EBS). The guide includes information on (1) default EBS application users, (2) database accounts, (3) EBS password change utilities (FNDCPASS, AFPASSWD), (4)

security related.

Chapter 8 : Integrigy | Oracle Database Security Oracle E-Business Suite Security

Dear Schan, Could you please help me on the server sizing for Oracle e-business suite Release I dont have much expertise on Oracle EBS and we need to decide on it fast.

Chapter 9 : Oracle E-Business Suite Security Quick Reference | Integrigy

Client redirects are a potential attack vector. The Oracle E-Business Suite + Allowed Redirects feature allows you to define a whitelist of allowed redirects for your Oracle E-Business Suite environment. Allowed Redirects is enabled by default with Oracle E-Business Suite