Setting Up Security for OTBI Enterprise for HCM Cloud Service
Objectives

• After completing this lesson, you should be able to:
  – Identify and describe the security features of OTBI Enterprise for HCM Cloud Service.
  – Identify the process for managing users, enterprise roles, and authorization in OTBI Enterprise for HCM Cloud Service.

The goal of this training is to enable implementers to configure and deploy Oracle® Transactional Business Intelligence Enterprise for Human Capital Management Cloud Service. An implementer is responsible for performing the initial setup and configuration of Oracle® Transactional Business Intelligence Enterprise for Human Capital Management Cloud Service. This may be done by the customer or by an implementation partner.
Security Overview

• OTBI Enterprise for HCM Cloud Service security is tightly integrated with the Oracle Fusion Middleware security architecture, which provides:
  – An authentication provider that authenticates users.
  – A policy store provider that provides access to application roles and policies.
  – A credential store provider that provides access to credentials.

• OTBI Enterprise for HCM Cloud Service security is tightly integrated with the Oracle Fusion Middleware security architecture and delegates core security functionality to components of that architecture.

• Specifically, any OTBI Enterprise for HCM Cloud Service installation makes use of the following types of security providers:
  – An authentication provider that knows how to access information about the users and groups accessible to OTBI Enterprise for HCM Cloud Service and is responsible for authenticating users
  – A policy store provider that provides access to application roles and application policies, which form a core part of the security policy and determines what users can and cannot see and do in OTBI Enterprise for HCM Cloud Service
  – A credential store provider that is responsible for storing and providing access to credentials required by OTBI Enterprise for HCM Cloud Service
Security in OTBI Enterprise for HCM Cloud Service can be classified broadly into the following three levels:

- Object-level security: Object-level security controls the visibility to business logical objects based on a user’s role. Object-level security is set for metadata repository objects, such as business models and subject areas, and for web objects, such as dashboards and dashboard pages.
- Data-level security: Data-level security controls the visibility of data (content rendered in subject areas, dashboards, Oracle BI Answers, and so on) based on the user’s association to data in the transactional system.
- User-level security (authentication of users): User-level security refers to authentication and confirmation of the identity of a user based on the credentials provided.
About Authentication

- OTBI Enterprise for HCM Cloud Service installations use the embedded Oracle WebLogic LDAP server for user and group information.
- The default OTBI Enterprise for HCM Cloud Service policy store provider and credential store provider store default credentials, application roles, and application policies in files in the domain.
About Authorization

• After a user has been authenticated, the next critical aspect of security is ensuring that the user can do and see what he or she is authorized to do and see.

• Authorization for OTBI Enterprise for HCM Cloud Service is controlled by a security policy defined in terms of applications roles.
About Application Roles

• Application roles define a set of permissions granted to a user or group.
• Object-level and data-level security are implemented in OTBI Enterprise for HCM Cloud Service using application roles.

• Application roles define a set of permissions granted to a user or group. Object-level and data-level security are implemented in OTBI Enterprise for HCM Cloud Service using application roles. Application roles are also known as duty roles.

• Application roles are mapped to directory server groups and users. For example, the application roles BIAdministrator, BIConsumer, and BIAuthor are default application roles that are defined as part of an OTBI Enterprise for HCM Cloud Service installation. Application roles represent a functional role that a user or group has, which gives that user or group the privileges required to perform that role. For example, users or groups with the BIAdministrator application role have the administrative permissions necessary to configure and manage the OTBI Enterprise for HCM Cloud Service installation and create and edit content for others to consume. Any member of the BIAdministrators group is explicitly granted this role and implicitly granted the BIAuthor and BIConsumer application roles.
Advantage of Using Application Roles

- An application role can secure content in a way that is independent of any particular authentication provider and the users and groups within that provider.
- If the underlying authentication provider changes, the security rules persist.

An application role is a logical role that can be used within the application to secure content in a way that is independent of any particular authentication provider and the users and groups within that provider. Security rules are built using application roles. If the underlying authentication provider changes, the security rules persist. In a different authentication provider, where group or usernames might be different, application roles could be remapped to different groups or users, and the BI security structure (built with application roles) would not be affected.
Default OTBI Enterprise for HCM Cloud Service Security Model

• During installation, three OTBI Enterprise for HCM Cloud Service security controls are preconfigured with initial values to form the default security model:
  – An embedded directory server functioning as an identity store designed to hold all user and group definitions that are required to control authentication
  – A file-based policy store designed to hold the application-role and permission grant mappings to users and groups that are required to control authorization
  – A file-based credential store designed to hold user and system credentials such as username and password combinations

• When operating in a development or test environment, you may find it convenient to use the default security model because it comes preconfigured. You then add user definitions and credentials that are specific to your business as well as customize the default application roles and permission grants that your business security policies require.

• After the identity, policy, and credential stores are fully configured and populated with data that is specific to your business, they provide all user, policy, and credential information needed by the OTBI Enterprise for HCM Cloud Service components during authentication and authorization.
OTBI Enterprise for HCM Cloud Service Security Process Overview

• OTBI Enterprise for HCM Cloud Service will be provisioned with fixed set of pre-populated enterprise roles, to which authorization is granted to various bits of functionality within OTBI Enterprise for HCM Cloud Service.
  – To create users, submit an SR and upload CSV files containing the list of users and their membership to the fixed set of enterprise roles.
  – To modify users, submit an SR and upload a CSV file which lists the changes to a user’s attributes.
  – To delete users, submit an SR and upload a CSV file which lists the users who need to be deleted.
  – Oracle Cloud Ops takes the provided CSV files from the SR and runs the OTBI Enterprise for HCM Cloud Service identity management script.

Each of these steps is covered in more detail on the slides that follow.
After you run the initial load plan, you need to provision the users who will be accessing OTBI Enterprise for HCM Cloud Service dashboards and reports.

OTBI Enterprise for HCM Cloud Service is provisioned with fixed set of pre-populated enterprise roles, to which authorization is granted to various bits of functionality within OTBI Enterprise for HCM Cloud Service.

To create users:
1. Log an SR and upload the add_user.csv and add_users_to_groups.csv files containing the list of users and their membership to the fixed set of enterprise roles. See the next slide for instructions to complete the add_user.csv and add_users_to_groups.csv files.
2. Once SR is complete, the user(s) will receive an email with their User ID and PW, and will be asked to change PW upon sign-on to OTBI Enterprise.
3. If the users are successfully added, the SR will be marked as Resolved.
4. If there are any errors the SR is reverted back to customer/implementer with the details and the failures files as attachment. Customer/implementer analyses the error log and provides new CSV files with fixed rows only.

Steps 1-4 are repeated until there are no errors, and the SR is closed and marked as “Resolved”.

Submitting an SR to Add New Users

- Select the following Service Type, Problem Type, and Sub Problem Type:
  - Service Type = Oracle Transactional Business Intelligence Enterprise for HCM Cloud Service
  - Problem Type = Hosting Services - Server Issue
  - Sub Problem Type = Add users in OTBI Enterprise

- Attach the add_user.csv and add_users_to_groups.csv files containing the list of users and their membership to the fixed set of enterprise roles (see instructions on the next slide).

- Once this SR is complete, the Implementer(s) and the Customer Admin(s) will receive an email with their User ID and PW. Users must change their PW upon sign-in.
Instructions for Filling Out the *add_users.csv* and *add_users_to_groups.csv* Files

- Attach the *add_user.csv* and *add_users_to_groups.csv* files containing the list of users and their membership to the fixed set of enterprise roles.
- If you do not know where to locate these .csv files, please contact the person in Oracle BI Product Management who has been assigned to assist you with your implementation.

- The *add-users.csv* file contains the list of users and their attributes such as mail address, first name, last name, display name, etc.
- In the 11.1.1.8.1 release, the mail attribute is automatically used as the unique login id (uid) for the user.
- The *add_users_to_groups.csv* file contains the assignment of the users to the predefined list of enterprise roles.
- In this example, Jan Smith is assigned to two predefined enterprise roles, PER_LINE_MANAGER_ABSTRACT and PAY_PAYROLL_MANAGER_JOB, and therefore appears in two rows in the csv file.
Predefined Enterprise Roles

- These are the predefined HCM enterprise roles and their mapped duty roles.

<table>
<thead>
<tr>
<th>Enterprise Role ID in OTBI-E</th>
<th>Description</th>
<th>Mapped Duty Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>PER_LINE_MANAGER_ABSTRACT</td>
<td>Line Manager</td>
<td>OBIA_ABSENCE_AND_LEAVE_ACCRUAL_ANALYSIS_DUTY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_COMPENSATION_ANALYSIS_DUTY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_WORKFORCE_DEPLOYMENT_ANALYSIS_DUTY</td>
</tr>
<tr>
<td>PAY_PAYROLL_MANAGER_JOB</td>
<td>Payroll Manager</td>
<td>OBIA_PAYROLL_ANALYSIS_DUTY</td>
</tr>
<tr>
<td>OBIA_HCM_HRVPVIEWALL</td>
<td>Human Resources VP – View All</td>
<td>OBIA_HCM_HRVPVIEWALL (which contain the following)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_AU_HCM_ABSC_ACRD_DUTY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_AU_HCM_COMP_DUTY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_AU_HCM_PYRL_DUTY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_AU_HCM_WRKFC_DPYMT_DUTY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_AU_HCM_RORNT_DUTY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_AU_HCM_WRKFC_FKNSV_DUTY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_AU_HCM_WRKFC_GENH01_GAINLOSS_DUTY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OBIA_AU_HCM_WRKFC_GAINLOSS_DUTY</td>
</tr>
</tbody>
</table>
Submitting an SR to Assign Existing Users to Additional Roles

• Select the following Service Type, Problem Type, and Sub Problem Type:
  – Service Type = Oracle Transactional Business Intelligence Enterprise for HCM Cloud Service
  – Problem Type = Hosting Services - Server Issue
  – Sub Problem Type = Add users to groups in OTBI Enterprise

• Attach the add_users_to_groups.csv files containing the list of existing users and their additional membership to one or more of the fixed set of enterprise roles (see instructions on the next slide).

• Once this SR is complete, the specified user(s) will have been granted the additional enterprise role(s).

• If the additional roles are successfully granted to the user, the SR will be marked as Resolved.

• If there are any errors the SR is reverted back to customer/implementer with the details and the failures files as attachment. Customer/implementer analyses the error log and provides new CSV files with fixed rows only. Steps are repeated until there are no errors, and the SR is closed and marked as “Resolved”.
Instructions for Filling Out the add_users_to_groups.csv Files

- Ensure the user(s) have already been granted access to OTBI Enterprise for HCM Cloud Service. This SR is only if the user(s) needs to be granted additional enterprise roles.

- Attach the add_users_to_groups.csv file containing the list of existing user(s) and their additional membership to the fixed set of enterprise roles.

- If you do not know where to locate this .csv file, please contact the person in Oracle BI Product Management who has been assigned to assist you with your implementation.

<table>
<thead>
<tr>
<th>mail</th>
<th>groupname</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jdoe@acme.com">jdoe@acme.com</a></td>
<td>PAY_PAYROLL_MANAGER_JOB</td>
</tr>
<tr>
<td><a href="mailto:pmiller@acme.com">pmiller@acme.com</a></td>
<td>PER_LINE_MANAGER_ABSTRACT</td>
</tr>
<tr>
<td><a href="mailto:jmitch@acme.com">jmitch@acme.com</a></td>
<td>PAY_PAYROLL_MANAGER_JOB</td>
</tr>
<tr>
<td><a href="mailto:biphoton@acme.com">biphoton@acme.com</a></td>
<td>OBIA_HCM_HRVP_VIEWALL</td>
</tr>
</tbody>
</table>

In the 11.1.1.8.1 release only the following three enterprise roles are supported:

- PAY_PAYROLL_MANAGER_JOB
- PER_LINE_MANAGER_ABSTRACT
- OBIA_HCM_HRVP_VIEWALL
Submitting an SR to Modify Users

• Select the following Service Type, Problem Type, and Sub Problem Type:
  – Service Type = Oracle Transactional Business Intelligence Enterprise for HCM Cloud Service
  – Problem Type = Hosting Services - Server Issue
  – Sub Problem Type = Modify existing users in OTBI Enterprise

• Attach the modify_users.csv file containing the list of users to be modified (see instructions on the next slide).

• Once this SR is complete, the specified user(s) will have been modified.

• If the user is successfully modified, the SR will be marked as Resolved.

• If there are any errors the SR is reverted back to customer/implemeniter with the details and the failures files as attachment. Customer/implementer analyses the error log and provides new CSV files with fixed rows only. Steps 1-4 are repeated until there are no errors, and the SR is closed and marked as “Resolved”.
Instructions for Filling Out the modify_users.csv File

• Ensure the user(s) have already been granted access to OTBI Enterprise for HCM Cloud Service. This SR is only if the user(s) name needs to be modified. Their Mail (i.e. User ID) cannot be modified.

• If an attribute is unchanged, keep it as-is in the .csv file

• Attach the modify_users.csv file containing the list of existing user(s) and the modifications that need to be made.

• If you do not know where to locate this .csv file, please contact the person in Oracle BI Product Management who has been assigned to assist you with your implementation.

<table>
<thead>
<tr>
<th>mail</th>
<th>givenName</th>
<th>sn</th>
<th>middleName</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jsmith@acme.com">jsmith@acme.com</a></td>
<td>Jan</td>
<td>Smith</td>
<td></td>
</tr>
<tr>
<td><a href="mailto:bjohanson@acme.com">bjohanson@acme.com</a></td>
<td>Boris</td>
<td>Johnson</td>
<td>Adam</td>
</tr>
</tbody>
</table>

Cells in yellow are the updated attributes.
Submitting an SR to Delete Users

• Select the following Service Type, Problem Type, and Sub Problem Type:
  – Service Type = Oracle Transactional Business Intelligence Enterprise for HCM Cloud Service
  – Problem Type = Hosting Services - Server Issue
  – Sub Problem Type = Delete users from OTBI Enterprise

• Attach the delete_users.csv file containing the list of users to be deleted (see instructions on the next slide).

• Once this SR is complete, the specified user(s) will have been deleted.
Instructions for Filling Out the delete_users.csv File

- Ensure the user(s) have already been granted access to OTBI Enterprise for HCM Cloud Service.
- Attach the delete_users.csv file containing the list of existing user(s) that need to be deleted.
- If you do not know where to locate this .csv file, please contact the person in Oracle BI Product Management who has been assigned to assist you with your implementation.

<table>
<thead>
<tr>
<th>email</th>
<th>delete_users.csv</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jo@mycompany.com">jo@mycompany.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:bob@mycompany.com">bob@mycompany.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:jbloggs@mycompany.com">jbloggs@mycompany.com</a></td>
<td></td>
</tr>
</tbody>
</table>

- If the user is successfully deleted, the SR will be marked as Resolved.
- If there are any errors the SR is reverted back to customer/implementer with the details and the failures files as attachment. Customer/implementer analyses the error log and provides new CSV files with fixed rows only. Steps 1-4 are repeated until there are no errors, and the SR is closed and marked as “Resolved”.

Submitting an SR to Reset a User’s Password

• If a user forgets or loses their password, submit an SR to request that the user's password be reset.

• Select the following Service Type, Problem Type, and Sub Problem Type:
  – Service Type = Oracle Transactional Business Intelligence Enterprise for HCM Cloud Service
  – Problem Type = Hosting Services - Server Issue
  – Sub Problem Type = Password Reset

• Provide the user’s user id (uid), which is also the email address of the user.

• Once this SR is complete, the specified user’s password will have been reset and the user will be notified via email with their new password. User must change their PW upon sign-in.
Summary

• In this lesson, you should have learned how to:
  – Identify and describe the security features of OTBI Enterprise for HCM Cloud Service.
  – Identify the process for managing users, enterprise roles, and authorization in OTBI Enterprise for HCM Cloud Service.