Data Security

Data security for Oracle Web Customers, Oracle Web Employees, and Oracle Web Suppliers is controlled by:

- Secure Socket Layers (SSL) to secure communication between client and server
- HTTP cookies
- encryption of password, parameter function, and session identifier
- session expiration
- securing and excluding attribute control

Session Management

Session management features include:

- each session is assigned a unique identifier, which is stored in a table
- session identifier returned to client encrypted via cookie
- encryption includes IP address to validate physical machine as well as the user
- session expiration based on number of hours or number of hits

Attribute Control

By using securing and excluding attributes, you can control user's access to data based on their ID and their responsibility. Attributes are first defined using the Web Applications Dictionary. They become securing or excluding attributes when you define responsibilities and users using the system administration functions of Oracle Application Object Library. See: Defining Attributes: page 3 – 25.

Securing Attributes for Row–Level Security

Securing attributes allow rows (records) of data to be visible to specified users or responsibilities based on the specific data (attribute value) contained in the row.

For example, to allow a hypothetical user, Sue, in the ADMIN responsibility to see rows containing a CUSTOMER_ID value of 1000, assign the securing attribute of CUSTOMER_ID to the ADMIN

responsibility. Then give Sue a security attribute CUSTOMER_ID value of 1000.

When Sue logs into the Admin responsibility the only customer data she will have access to will have a CUSTOMER_ID value of 1000.

Note: Users can have multiple values made available to them.

See: Users Window, *Oracle Applications User's Guide, Release 11* and Responsibilities Window, *Oracle Applications User's Guide, Release 11*.

Excluding Attributes for Column–Level Security

Excluding attributes prevent certain columns of data from being visible to specified responsibilities.

For example, if for security reasons you did not want the hypothetical user Sue in the ADMIN responsibility to see data in the CONTACT_NAME column, you would assign her the excluding attribute CONTACT_NAME to the ADMIN responsibility. No users with the ADMIN responsibility can see CONTACT_NAME information.

See: Responsibilities Window, *Oracle Applications User's Guide, Release 11*.

Seeded Securing Attributes

Assign a securing attribute and value to define an attribute that must be matched by the user to see records. Attributes are defined using the Web Applications Dictionary. Assign securing attribute values for each user, and for each securing attribute assigned to all responsibilities for this user.

You may designate a user as an employee, supplier, and / or customer. This automatically assigns a contact ID value to this user for appropriate securing attributes as follows:

Contact	**ID**
Customer Contact	ICX_CUSTOMER_CONTACT_ID
Internal Contact	ICX_HR_PERSON_ID
Supplier Contact	ICX_SUPPLIER_CONTACT_ID

In addition, the following securing attributes are seeded:

Contact	ID
Customer	ICX_CUSTOMER_ORG_ID
Organization	ICX_HRG_ORG_ID
Supplier	ICX_SUPPLIER_ORG_ID
Customer Site	ICX_CUSTOMER_SITE_ID
Internal Site (location)	ICX_HR_SITE_ID
Supplier Site	ICX_SUPPLIER_SITE_ID

Predefined Security at Responsibility Level

The following list shows which responsibilities have predefined securing and excluding attributes:

Responsibility	Securing Attributes	Excluding Attributes
Credit Cards	ICX_HR_PERSON_ID	
Customer Registration		
Customer Services (Full Access)		
Customer Services (by Customer)		
Customer Services (by Customer Contact)		
EDI Transmissions (by Customer Site)	ICX_CUSTOMER_SITE_ID	
EDI Transmissions (Full Access)		
Events and Seminars		
Executive Overview		
Expense Reports		
Expense Reporting		
Global Assets Information		
Partner Information (by Customer)	ICX_CUSTOMER_ORG_ID	
Payments and Credits (by Customer)	ICX_CUSTOMER_ORG_ID	

Table 1 – 1 (Page 1 of 2)

Responsibility	Securing Attributes	Excluding Attributes
Payments and Credits (Full Access)		
Plan Inquiries		
Products and Orders (by Customer Contact)	ICX_CUSTOMER_CONTACT_ID	
Products and Orders (Full Access)		
Products and Orders (Guest Access)		
Project Control (by Employee)	ICX_HR_PERSON_ID	
Project Information (by Customer)	ICX_CUSTOMER_ORG_ID	
Purchasing		
Registration		
Requisitions		
Requisitions (by Preparer)	PREPARER_ID	
Requisitions (by Requester)	ICX_REQUESTOR_ID	
Requisitions (Full Access)		
Salesperson Services (by Employee)	ICX_CUSTOMER_ORG_ID	
Salesperson Services (Full Access)		
Service and Support (Full Access)		CS_PUBLIC_COMMENT
Service and Support (by Customer Contact)	ICX_CUSTOMER_CONTACT_ID	CS_COMMENT
Service and Support (by Customer)	ICX_CUSTOMER_ORG_ID	CS_COMMENT
Supplier Registration		
Supplier Services	ICX_LEVEL_ALTERED	ICX_DISTRIBUTION_ID, ICX_SUPPLIER, ICX_SUPSITE
Supplier Services (by Supplier Site)	ICX_LEVEL_ALTERED, ICX_SUPPLIER_SITE_ID	ICX_DISTRIBUTION_ID, ICX_SUPPLIER, ICX_SUPSITE
Supplier Services (by Supplier)	ICX_LEVEL_ALTERED, ICX_SUPPLIER_ORG_ID	ICX_DISTRIBUTION_ID, ICX_SUPPLIER, ICX_SUPSITE
Supplier Services (Full Access)		ICX_DISTRIBUTION_ID
Web Planning Inquiries		

Table 1 – 1 (Page 2 of 2)

Query Processing

When a user queries for data using Oracle Web Customers, Oracle Web Employees, and Oracle Web Suppliers, the Web Applications Dictionary determines if any securing attributes exist in a region, and, if so, determines whether the securing attributes match those assigned to the responsibility.

If there are securing attributes assigned at the responsibility level that exactly match those at the region level, securing attribute values are checked at the user level.

If there are no securing attributes assigned at the user level that match, no data is returned. If there are securing attributes assigned at the user level that match, data is returned to the user, but only if the *user's* securing attribute values exactly match the values of the returned data.

Excluded attributes assigned at the responsibility level prevent data being returned for these attributes.

For example, assume that Sue has the following attribute values:

Securing Attribute	Value
CUSTOMER_ID	1000
SITE_ID	123
SITE_ID	345
SITE_ID	567
CONTACT_ID	9876

Table 1 – 2

Assume that Sue requests data for CUSTOMER_ID, SITE_ID, or CONTACT_ID, and these attributes are defined in Web Applications Dictionary and for the Customer responsibility. For any rows of data with these attributes, Sue's securing attribute values are checked for exact matches.

In this case, any rows with a CUSTOMER_ID of 1000; SITE_ID of 123, 345, or 567; and CONTACT_ID of 9876 are returned.