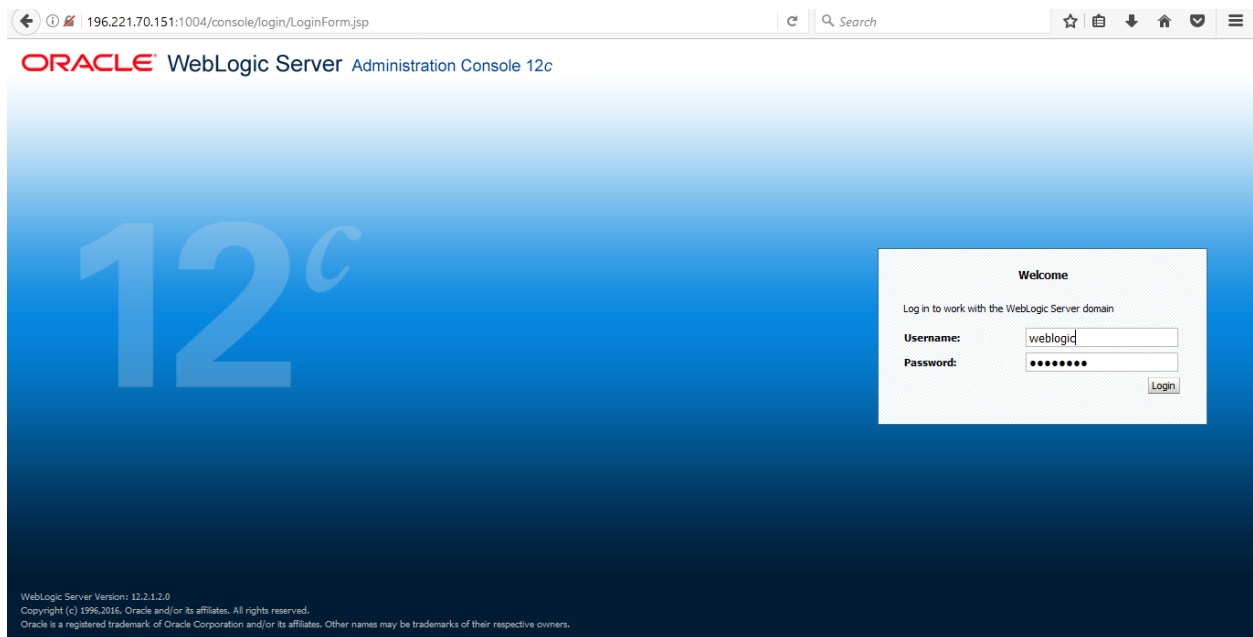


# LDAP Integration

---

To configure Weblogic server to allow user authentication through Active Directory

1. Login to **Weblogic Server Console** through <http://192.168.120.22:7001/console>



2. Click on **Security Realms** link on the life panel

196.221.70.151:1004/console/console.portal?\_nfpb=true&\_pageLabel=HomePage1

ORACLE WebLogic Server Administration Console 12c

Welcome, weblogic Connected to: efsa\_domain

Home Page

Information and Resources

Helpful Tools

- Configure applications
- Configure GridLink for RAC Data Source
- Configure a Dynamic Cluster
- Recent Task Status
- Set your console preferences
- Oracle Enterprise Manager

General Information

- Common Administration Task Descriptions
- Read the documentation
- Ask a question on My Oracle Support

Domain Configurations

Domain

- Domain

Resource Group Templates

- Resource Group Templates

Interoperability

- WTC Servers
- Jolt Connection Pools

Domain Partitions

- Domain Partitions
- Partition Work Managers

Resource Groups

- Resource Groups

Diagnosics

- Log Files
- Diagnostic Modules
- Built-in Diagnostic Modules
- Diagnostic Images
- Request Performance
- Archives
- Context
- SNMP
- Interceptors

Environment

- Servers
- Clusters
  - Server Templates
  - Migratable Targets
- Coherence Clusters
- Machines

Deployed Resources

- Deployments

Services

- Messaging
  - JMS Servers
  - Store-and-Forward Agents
  - JMS Modules
  - Path Services

Charts and Graphs

Change Center

View changes and restarts

Click the **Lock & Edit** button to modify, add or delete items in this domain.

Lock & Edit

Release Configuration

Domain Structure

efsa\_domain

- Domain Partitions
- Environment
- Deployments
- Services
- Security Realms**
- Interoperability
- Diagnostics

How do I...

- Search the configuration
- Use the Change Center
- Record WLST Scripts
- Change Console preferences
- Manage Console extensions
- Monitor servers

System Status

196.221.70.151:1004/console/console.portal?\_nfpb=true&\_pageLabel=SecurityRealmRealmTablePage

### 3. Click on **myrealm** link

196.221.70.151:1004/console/console.portal?\_nfpb=true&\_pageLabel=SecurityRealmRealmTablePage

ORACLE WebLogic Server Administration Console 12c

Welcome, weblogic Connected to: efsa\_domain

Home > Summary of Security Realms

Summary of Security Realms

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple active security realms in a WebLogic Server domain, but only one can be set as the default security realm, which is reserved for domain administrative purposes.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

Customize this table

Realms (Filtered - More Columns Exist)

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

Name	Default Realm
<a href="#">myrealm</a>	true

Showing 1 to 1 of 1 Previous | Next

Change Center

View changes and restarts

Click the **Lock & Edit** button to modify, add or delete items in this domain.

Lock & Edit

Release Configuration

Domain Structure

efsa\_domain

- Domain Partitions
- Environment
- Deployments
- Services
- Security Realms**
- Interoperability
- Diagnostics

How do I...

- Configure new security realms
- Enable automatic realm restart
- Delete security realms
- Change the default security realm

System Status

Health of Running Servers as of 9:38 PM

196.221.70.151:1004/console/console.portal?\_nfpb=true&\_pageLabel=SecurityRealmRealmTablePage

### 4. Open **Providers** tab then click on **Lock & Edit** to be able to add a new provider then click **New**

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled "Settings for myrealm" and has several tabs: Configuration, Users and Groups, Roles and Policies, Credential Mappings, **Providers**, and Migration. Under the "Providers" tab, there are sub-tabs for Authentication, Password Validation, Authorization, Adjudication, Role Mapping, Auditing, Credential Mapping, and Certification Path. The "Authentication" sub-tab is active, showing a table of Authentication Providers.

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS.

**Customize this table**

**Authentication Providers**

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	Trust Service Identity Asserter	Trust Service Identity Asserter Provider	1.0
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Asserter Provider	1.0

5. Enter provider Name **EFSAActiveDirectoryProvider** then from **Type** list select **ActiveDirectoryAuthenticator** then click **OK**

The screenshot shows the "Create a New Authentication Provider" dialog box in the Oracle WebLogic Server Administration Console. The dialog has "OK" and "Cancel" buttons at the top and bottom. The main content area is titled "Create a new Authentication Provider" and contains the following text:

The following properties will be used to identify your new Authentication Provider.  
\* Indicates required fields

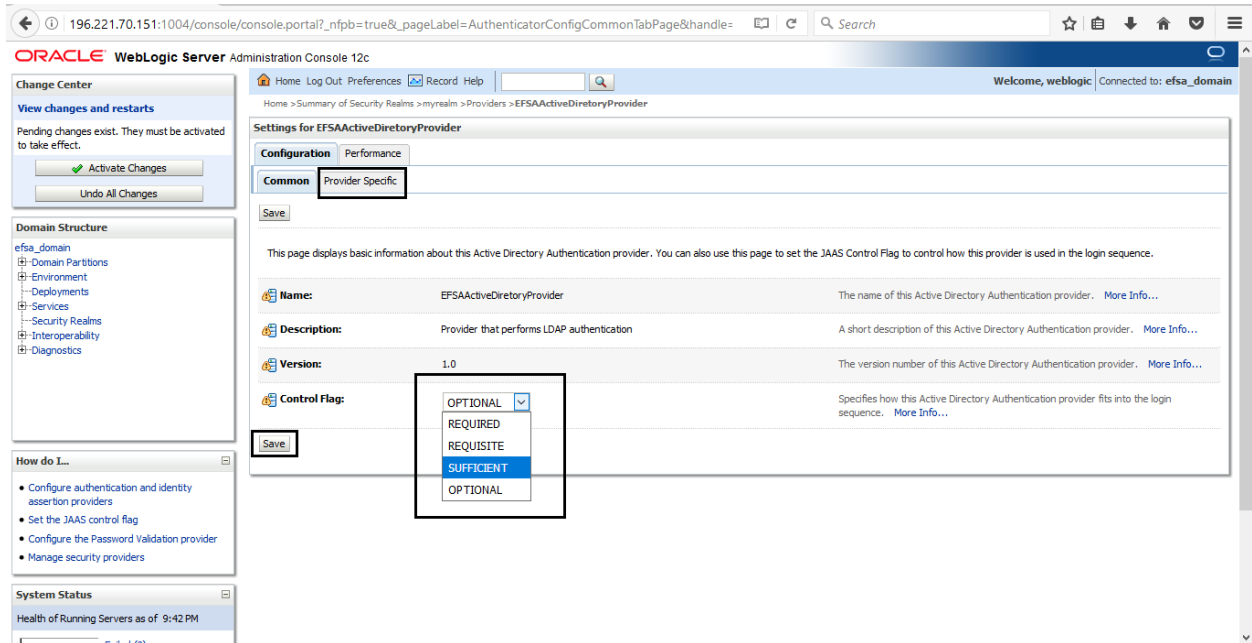
The name of the authentication provider.

\* **Name:**

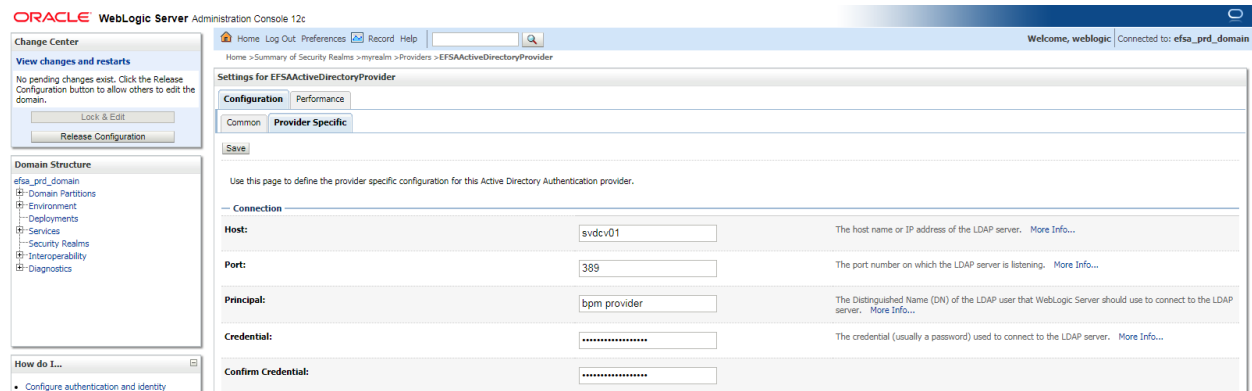
This is the type of authentication provider you wish to create.

**Type:**

6. Open **DefaultAuthenticator** and in **Common** tab change **Control Flag** to **SUFFICIENT** then click **Ok**
7. Open **EFSAActiveDirectoryProvider** and change **Control Flag** to **SUFFICIENT** then open **Provider Specific** tab



## 8. Enter Active Directory Host, Port, Principal and Credential (Password)



## 9. In Users section

- a. Edit **User Base DN** to **DC=GOV, DC=FSA**
- b. Change **cn=** to **sAMAccountName=** in **User From Name Filter** field
- c. Change **cn** to **sAMAccountName** in **User Name Attribute** field
- d. Select **Use Retrieved User Name as Principal**

<ul style="list-style-type: none"> <li>Configure authentication and identity assertion providers</li> <li>Manage security providers</li> </ul>	<b>Confirm Credentials:</b> <input type="password" value="....."/>					
	<input type="checkbox"/> <b>SSLEnabled</b> <span style="float: right;">Specifies whether the SSL protocol should be used when connecting to the LDAP server. <a href="#">More Info...</a></span>					
<b>System Status</b> Health of Running Servers as of 12:43 PM	<b>Users</b>					
<table border="1"> <tr><td>Failed (0)</td></tr> <tr><td>Critical (0)</td></tr> <tr><td>Overloaded (0)</td></tr> <tr><td>Warning (0)</td></tr> <tr><td>OK (5)</td></tr> </table>	Failed (0)	Critical (0)	Overloaded (0)	Warning (0)	OK (5)	<b>User Base DN:</b> <input type="text" value="DC=GOV,DC=FSA"/> <span style="float: right;">The base distinguished name (DN) of the tree in the LDAP directory that contains users. <a href="#">More Info...</a></span>
Failed (0)						
Critical (0)						
Overloaded (0)						
Warning (0)						
OK (5)						
	<input type="checkbox"/> <b>All Users Filter:</b> <input type="text"/> <span style="float: right;">If the attribute (user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. <a href="#">More Info...</a></span>					
	<input type="checkbox"/> <b>User From Name Filter:</b> <input type="text" value="(&amp;(sAMAccountName=%u)()c"/> <span style="float: right;">If the attribute (user name attribute and user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. <a href="#">More Info...</a></span>					
	<b>User Search Scope:</b> <input type="text" value="subtree"/> <span style="float: right;">Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. <a href="#">More Info...</a></span>					
	<input type="checkbox"/> <b>User Name Attribute:</b> <input type="text" value="sAMAccountName"/> <span style="float: right;">The attribute of an LDAP user object that specifies the name of the user. <a href="#">More Info...</a></span>					
	<input type="checkbox"/> <b>User Object Class:</b> <input type="text" value="user"/> <span style="float: right;">The LDAP object class that stores users. <a href="#">More Info...</a></span>					
	<input checked="" type="checkbox"/> <b>Use Retrieved User Name as Principal</b> <span style="float: right;">Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal in the Subject. <a href="#">More Info...</a></span>					

## 10. In Groups section

### a. Edit Group Base DN to DC=GOV, DC=FSA

<b>Groups</b>	
<b>Group Base DN:</b> <input type="text" value="DC=GOV,DC=FSA"/>	<span style="float: right;">The base distinguished name (DN) of the tree in the LDAP directory that contains groups. <a href="#">More Info...</a></span>
<input type="checkbox"/> <b>All Groups Filter:</b> <input type="text"/>	<span style="float: right;">An LDAP search filter for finding all groups beneath the base group distinguished name (DN). If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the Group schema. <a href="#">More Info...</a></span>
<input type="checkbox"/> <b>Group From Name Filter:</b> <input type="text" value="(&amp;(cn=%g)(objectclass=grou"/>	<span style="float: right;">An LDAP search filter for finding a group given the name of the group. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. <a href="#">More Info...</a></span>
<b>Group Search Scope:</b> <input type="text" value="subtree"/>	<span style="float: right;">Specifies how deep in the LDAP directory tree to search for groups. Valid values are subtree and onelevel. <a href="#">More Info...</a></span>
<b>Group Membership Searching:</b> <input type="text" value="unlimited"/>	<span style="float: right;">Specifies whether group searches into nested groups are unlimited, limited or off. Valid values are unlimited, limited and off. <a href="#">More Info...</a></span>
<b>Max Group Membership Search Level:</b> <input type="text" value="0"/>	<span style="float: right;">Specifies how many levels of group membership can be searched. This setting is valid only if GroupMembershipSearching is set to limited. Valid values are 0 and positive integers. For example, 0 indicates only direct group memberships will be found, and a positive number indicates the number of levels to search. <a href="#">More Info...</a></span>
<input type="checkbox"/> <b>Ignore Duplicate Membership</b>	<span style="float: right;">Determines whether duplicate members are ignored when adding groups. The attribute cycles in the Group membership. <a href="#">More Info...</a></span>
<input type="checkbox"/> <b>Use Token Groups For Group Membership Lookup</b>	<span style="float: right;">Indicates whether to use the Active Directory TokenGroups attribute lookup algorithm instead of the standard recursive group membership lookup algorithm. <a href="#">More Info...</a></span>

11. As for the remaining settings keep all the default values then click Ok

Static Groups		
Static Group Name Attribute:	<input type="text" value="cn"/>	The attribute of a static LDAP group object that specifies the name of the group. <a href="#">More Info...</a>
Static Group Object Class:	<input type="text" value="group"/>	The name of the LDAP object class that stores static groups. <a href="#">More Info...</a>
Static Member DN Attribute:	<input type="text" value="member"/>	The attribute of a static LDAP group object that specifies the distinguished names (DNs) of the members of the group. <a href="#">More Info...</a>
Static Group DN's from Member DN Filter:	<input type="text" value="(&amp;(member=%M))objectclass"/>	An LDAP search filter that, given the distinguished name (DN) of a member of a group, returns the DN's of the static LDAP groups that contain that member. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. <a href="#">More Info...</a>
Dynamic Groups		
Dynamic Group Name Attribute:	<input type="text"/>	The attribute of a dynamic LDAP group object that specifies the name of the group. <a href="#">More Info...</a>
Dynamic Group Object Class:	<input type="text"/>	The LDAP object class that stores dynamic groups. <a href="#">More Info...</a>
Dynamic Member URL Attribute:	<input type="text"/>	The attribute of the dynamic LDAP group object that specifies the URLs of the members of the dynamic group. <a href="#">More Info...</a>
User Dynamic Group DN Attribute:	<input type="text"/>	The attribute of an LDAP user object that specifies the distinguished names (DNs) of dynamic groups to which this user belongs. <a href="#">More Info...</a>
General		
Connection Pool Size:	<input type="text" value="6"/>	The LDAP connection pool size. Default is 6. <a href="#">More Info...</a>
Connect Timeout:	<input type="text" value="0"/>	The maximum time in seconds to wait for the connection to the LDAP server to be established. If this attribute is set to 0, there is no maximum time limit. <a href="#">More Info...</a>
Connection Retry Limit:	<input type="text" value="1"/>	Specifies the number of times to attempt to connect to the LDAP server if the initial connection failed. <a href="#">More Info...</a>
Parallel Connect Delay:	<input type="text" value="0"/>	The delay in seconds when making concurrent attempts to connect to multiple LDAP servers. <a href="#">More Info...</a>
Results Time Limit:	<input type="text" value="0"/>	The maximum number of milliseconds for the LDAP server to wait for results before timing out. If this attribute is set to 0, there is no maximum time limit. <a href="#">More Info...</a>
<input type="checkbox"/> Keep Alive Enabled		Specifies whether to prevent LDAP connections from timing out. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> Follow Referrals		Specifies that a search for a user or group within the LDAP Authentication provider will follow referrals to other LDAP servers or branches within the LDAP directory. By default, this attribute is enabled. <a href="#">More Info...</a>
<input type="checkbox"/> Bind Anonymously On Referrals		By default, the LDAP Authentication provider uses the same DN and password used to connect to the LDAP server when following referrals during a search. If you want to connect as an anonymous user, enable this attribute. <a href="#">More Info...</a>
<input type="checkbox"/> Propagate Cause For Login Exception		Specifies whether the providers should propagate the cause of the LoginException. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> Cache Enabled		Specifies whether a cache is used with the LDAP server. <a href="#">More Info...</a>
Cache Size:	<input type="text" value="32"/>	The size of the cache (in kilobytes) that is used with the LDAP server. <a href="#">More Info...</a>
Cache TTL:	<input type="text" value="60"/>	The time-to-live of the cache (in seconds) that is used with the LDAP server. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> Cache Statistics Enabled		Specifies whether to enable statistics of the cache. <a href="#">More Info...</a>
GUID Attribute:	<input type="text" value="objectguid"/>	Specifies the name of the GUID attribute defined in the Active Directory LDAP server. The default value is objectguid. <a href="#">More Info...</a>
Identity Domain:	<input type="text"/>	The name of the identity domain. <a href="#">More Info...</a>
<input type="button" value="Save"/>		

12. Click on **Activate Changes** to commit all the changes to the server then **restart** all managed servers

# Users Information and Integration with HITS

---

User main information that is needed in the application is saved in the database distributed on multiple tables. This information should be updated frequently by Database Jobs and Triggers provided by EFSA to migrate latest info from HITS. Next is a description for all the tables to help in the migration process.

The tables are:

1. ADMIN\_USERS
2. ADMIN\_LK\_USER\_GRADES
3. ADMIN\_LK\_USER\_TITLE
4. ADMIN\_DEPARTMENTS
5. ADMIN\_LK\_DEPARTMENT\_TYPES

## ADMIN\_USERS

This table contains all user data

Column	Description
<b>USER_ID</b>	User Id
<b>USER_LOGIN_NAME</b>	User system login name
<b>FIRST_NAME</b>	User First Name
<b>SECOND_NAME</b>	User Second Name
<b>THIRD_NAME</b>	User Third Name
<b>FAMILY_NAME</b>	User Family Name
<b>FULL_NAME</b>	User Full name
<b>DEPARTMENT_ID</b>	User Department Id
<b>USER_TITLE</b>	User Title
<b>IS_USER_ACTIVE</b>	Flag to determine if user account is active or not – by default active
<b>USER_DEGREE</b>	User Degree
<b>MOBILE_NO</b>	User Mobile Number
<b>USER_EMAIL</b>	User Email
<b>MANAGER_ID</b>	User Manager Id
<b>HIRING_DATE</b>	User Hiring date
<b>USER_GRADE</b>	User Grade

<b>LEVEL_NO</b>	User Level
<b>SEND_MAIL</b>	Flag to determine whether to send Email by BPM engine to user or not - by default true
<b>INTERNAL_NUMBER</b>	User Internal office phone number

## ADMIN\_LK\_USER\_GRADES

This table contains user grades lookup values

Column	Description
<b>GRADE_ID</b>	Grade Id
<b>GRADE_AR_NAME</b>	Grade Arabic Name
<b>GRADE_EN_NAME</b>	Grade English Name

## ADMIN\_LK\_USER\_TITLE

This table contains user titles lookup values

Column	Description
<b>TITLE_ID</b>	Title Id
<b>TITLE_AR_NAME</b>	Title Arabic Name
<b>TITLE_EN_NAME</b>	Title English Name

## ADMIN\_DEPARTMENTS

This table contains all the departments' data

Column	Description
<b>DEPARTMENT_ID</b>	Department Id
<b>DEPARTMENT_CODE</b>	Department Id – same as Department Id
<b>DEPARTMENT_EN_NAME</b>	Department English Name
<b>DEPARTMENT_AR_NAME</b>	Department Arabic Name
<b>PARENT_DEPARTMENT_ID</b>	Parent Department Id
<b>DEPARTMENT_TYPE</b>	Department Type
<b>DEPARTMENT_LEVEL</b>	Department Level
<b>MANAGER_ID</b>	Department Manager Id
<b>UPDATE_DATE</b>	Department Updated information date
<b>UPDATE_USER</b>	Department Updated information by

	User
<b>CREATED_DATE</b>	Department Created date
<b>CREATED_USER</b>	Department Created by User

## **ADMIN\_LK\_DEPARTMENT\_TYPES**

This table contains department type lookup values

<b>Column</b>	<b>Description</b>
<b>DEPT_TYPE_ID</b>	Department Type Id
<b>DEPT_TYPE_AR_NAME</b>	Department Type Arabic Name
<b>DEPT_TYPE_EN_NAME</b>	Department Type English Name