Oracle® Enterprise Single Sign-on Provisioning Gateway

Administrator's Guide

Release 11.1.1.5.0

E20983-01

March 2011

ORACLE®

Oracle Enterprise Single Sign-on Provisioning Gateway, Administrator's Guide, Release 11.1.1.5.0

E20983-01

Table of Contents

Abbreviations and Terminology

Following is a list of commonly-used abbreviations and terminology.

Abbreviation or Term	Full Name
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Agent
ESSO-Anywhere	Oracle Enterprise Single Sign-on Anywhere
ESSO-LM	Oracle Enterprise Single Sign-on Logon Manager
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset
ESSO-UAM	Oracle Enterprise Single Sign-on Universal Authentication Manager
FTU	First Time Use Wizard

Welcome

Oracle Enterprise Single Sign-on Provisioning Gateway (ESSO-PG) provides an administrator with the capability to automatically provision Oracle Enterprise Single Sign-on Logon Manager (ESSO-LM) with a user's ID and password by using a provisioning system. An administrator can add, modify, and delete IDs and passwords for particular applications within the provisioning system and have the changes reflected in ESSO-LM. From the provisioning system, an administrator can delete all usernames and passwords inside of ESSO-LM so that a user's access to all protected applications is eliminated.

This guide is intended for experienced administrators responsible for the planning, implementation, and deployment of ESSO-PG. Administrators are expected to understand single sign-on concepts and be familiar with Internet Information Services, Windows Registry settings, and the ESSO-LM Administrative Console. Persons completing the installation and configuration procedure should also be familiar with their company's system standards.

The ESSO-PG Administrative Console enables administrators to set up, manage, and gather information from the ESSO-PG Web service. The following modules can be accessed from the ESSO-PG Administrative Console:

- Settings
- Users
- Reports & Logs

Accessing the ESSO-PG Administrative Console

Open a Web browser and enter the following URL:

https://*yourserverhost*/v-go pm console/logon.aspx

where *yourserverhost* is the name of the server where ESSO-PG is installed.

The ESSO-PG Administrative Console Logon Page opens.

Logon Page

Enter your logon credentials to access the ESSO-PG Web Service and click **Log On**.

The **username** and **password** should be the same as the directory authentication credentials.

For example, for Active Directory or ADAM, the username would be in the format:

*domainname**username*.

For Sun or IBM, the username would be in the format: *uid=username*.

The ESSO-PG server only recognizes credentials that it has access to. On AD or ADAM, those recognized credentials are domain accounts. For Sun and IBM, the account must exist in the storage. If no storage has been defined, the account is authenticated against the local accounts on the server where the Web service account is running.

About

The About module provides information about which versions of ESSO-PG and Microsoft .NET Framework are installed.

Version Information:

Product Version. Indicates which version of ESSO-PG is installed.

.NET Framework. Indicates which version of Microsoft .NET Framework is installed.

Security Settings

ESSO-PG can be run without changing the default security settings. Security can be increased by changing several of the settings.

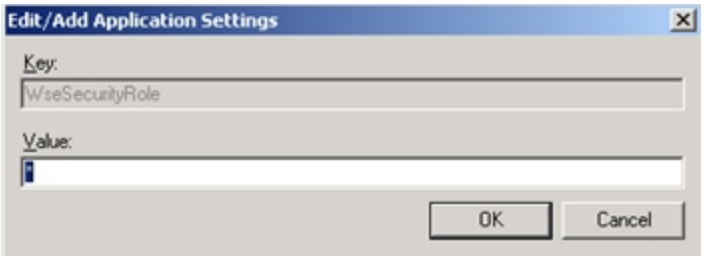
You can edit the ESSO-PG security settings through the Microsoft .Net Framework ASP.NET Configuration Settings. These settings are then changed in the ESSO-PG configuration files:

- <*local directory*>\ESSO-PG\Service\web.config
- <*local directory*>\ESSO-PG\Console\web.config

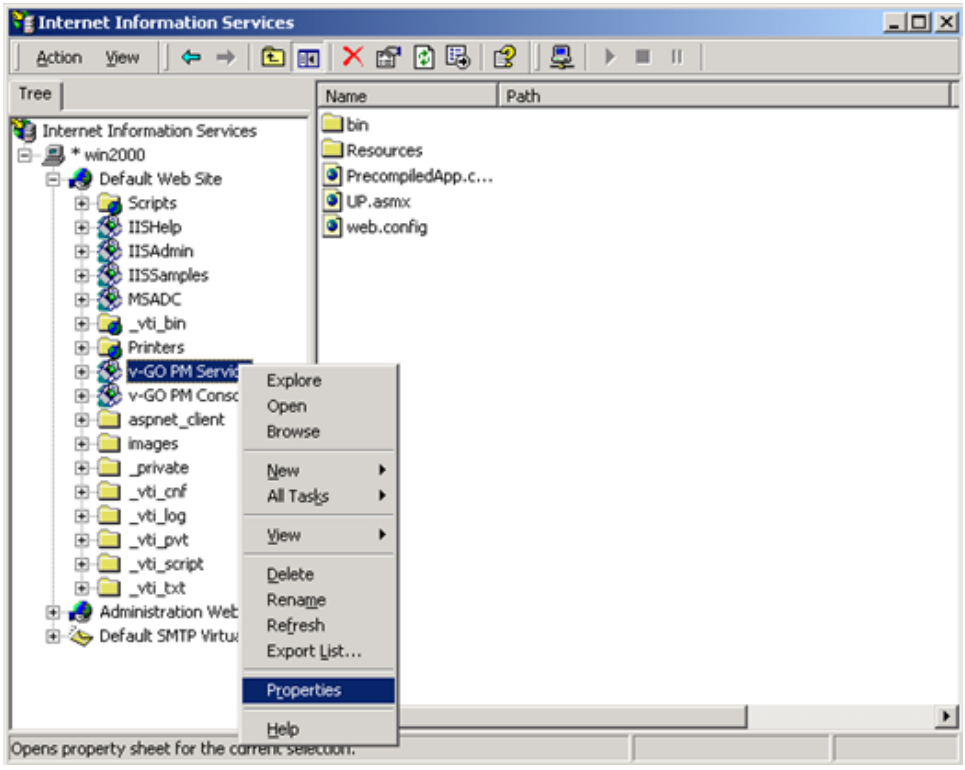
Restricting Access to the ESSO-PG Management Console by Roles

By default, access to the ESSO-PG Management Console is not restricted; any user with a valid Windows or domain logon can access the site. In order to restrict access to a particular group, you must edit a setting in the ESSO-PG Service Properties:

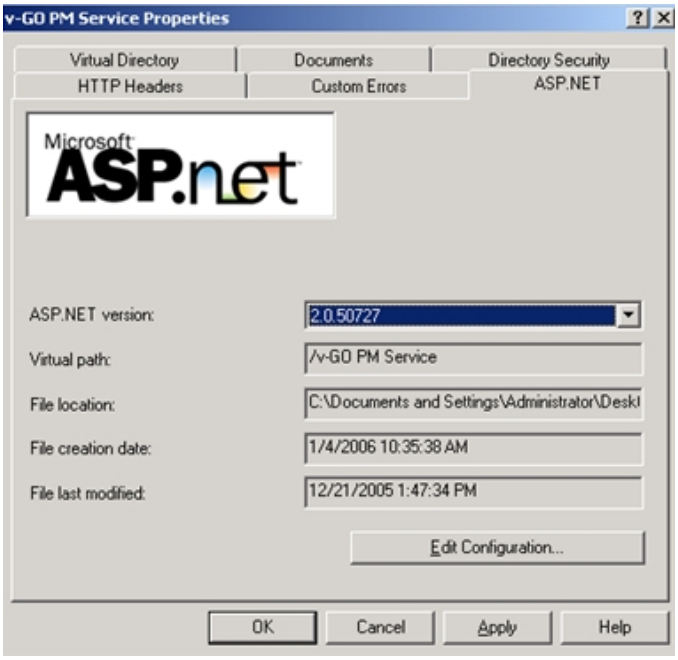
In the **Value** field, replace the asterisk (*) with the appropriate security role value to restrict access to the ESSO-PG Web service to users in the specified role.



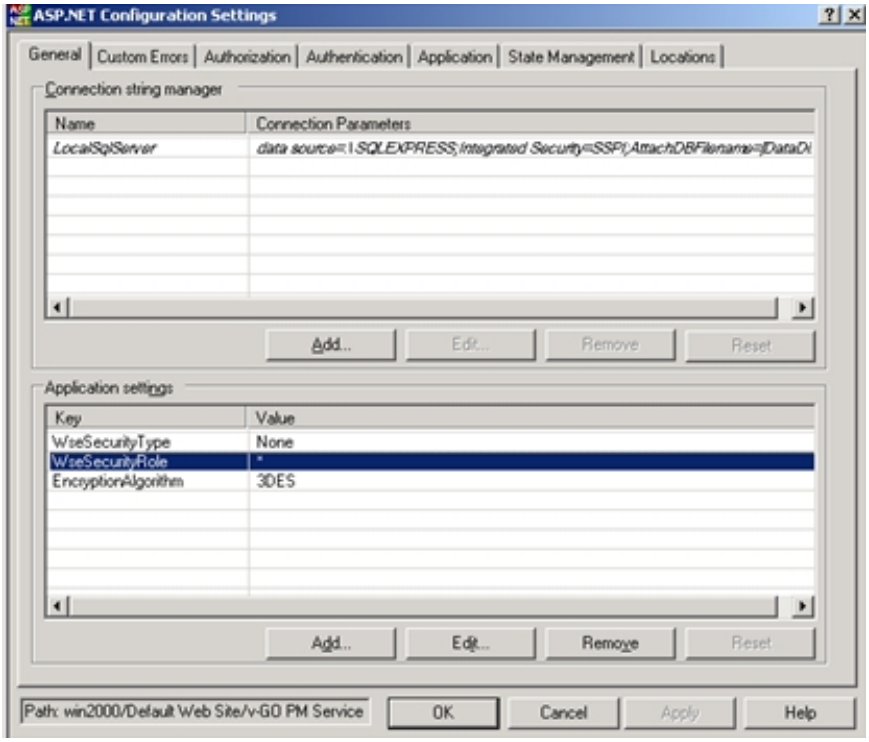
1. Go to **Control Panel > Internet Information Services**. Right-click the ESSO-PG Service Web site. Select **Properties**.



2. Click the **ASP.NET** tab. Verify that the ASP.NET version is set to 2.0.x. (Note that if it is not set to 2.0, you must change the setting and click Apply.) Click **Edit Configuration**.



3. In the ASP.NET Configuration Settings dialog box, highlight **WseSecurityRole** and click **Edit**.



- To restrict access for Sun or IBM directories, change the value to the group DN. For example, enter: `cn=testgroup,ou=users,dc=organization,dc=com`.
- To restrict access for AD or ADAM directories, change the value in the Domain\role format. For example, for the Domain Admins role under TESTDOMAIN, enter `TESTDOMAIN\Domain Admins`.

Changing the Encryption Algorithm

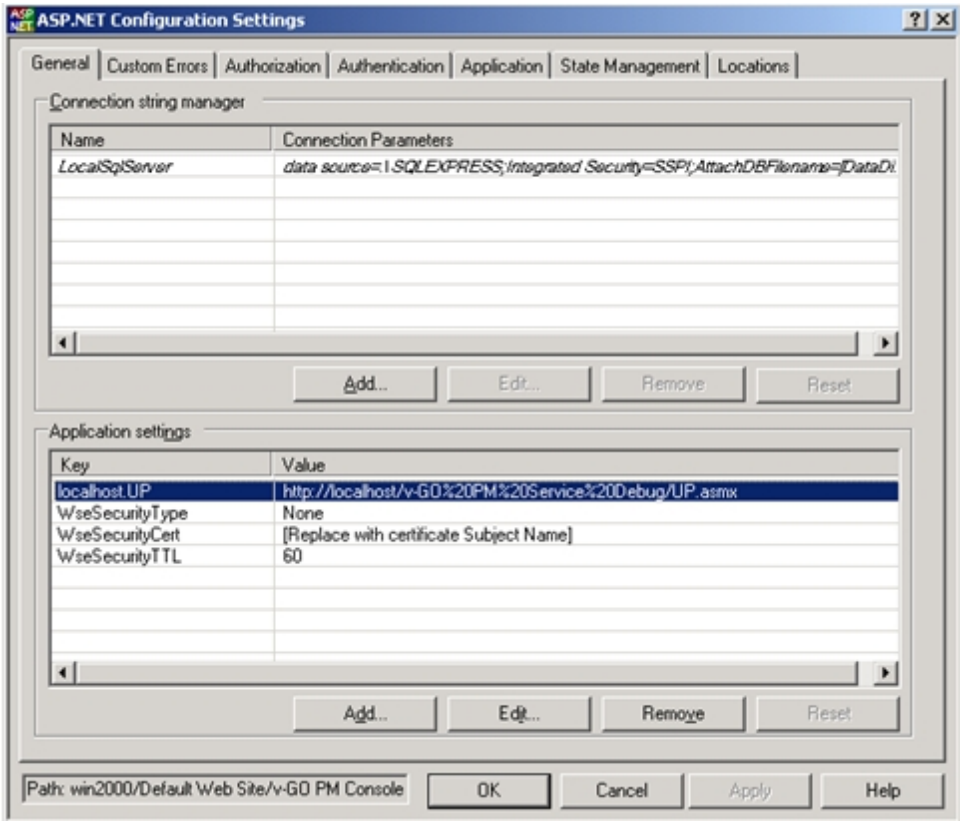
By default, the ESSO-PG Web service uses 3DES encryption. To increase security, you can change encryption to AES. In order to enable this feature, you must edit a setting in Oracle Service Properties:

1. Go to **Control Panel** > **Internet Information Services**.
2. Right-click the ESSO-PG Service Web site. Select **Properties**.
3. Click the **ASP.NET** tab. Verify that the ASP.NET version is set to 2.0.x. (If it is not set to 2.0, change the setting and click **Apply**.) Click **Edit Configuration**.
4. In the ASP.NET Configuration Settings dialog box, highlight **EncryptionAlgorithm** and click **Edit**.
5. In the Value field, replace 3DES with AES_256. This value causes the ESSO-PG Service to use the AES encryption method.

Enabling SSL

For testing purposes, you can enable SSL by changing the localhost.UP key in ESSO-PG Console Properties:

1. In the ASP.NET Configuration Settings dialog box, highlight localhost.UP and click **Edit**.



2. Go to **Control Panel** > **Internet Information Services**. Right-click the ESSO-PG Console Web site. Select **Properties**.
3. Click the **ASP.NET** tab. Verify that the ASP.NET version is set to 2.0.x. (If it is not set to 2.0, change the setting and click **Apply**.) Click **Edit Configuration**.
4. In the Value field, replace:
   http://localhost/ESSO-PG Service/UP.asmx
   by entering
   `https://localhost/ESSO-PG Service/UP.asmx`
5. You can now edit the properties for the ESSO-PG Service in IIS to turn off SSL.

Settings

Settings > Web Service Account

Use the Web Service Account page to set or change the Anonymous Logon for IIS Web Services. The ESSO-PG Web service runs as this domain account. The Web Service Account dialog box displays the current Anonymous Logon account and provides a logon form for changing this account.

You must be authenticated to the ESSO-PG Console as a member of the administrator group of the ESSO-PG Web server to change the account

The Web service account requires the following privileges:

- Read and write access to the Registry path `HKLM\Software\Passlogix`.
- Connect, read, and write access to the storage if AD or ADAM.

To change the Web service account, type in the account **User Name** (in the format Domain\Username) and **Password**, confirm the password, and click **Save**.

Settings > Storage

Use the Storage page to view or change connection settings for the directory service (Oracle Internet Directory, Microsoft Active Directory, Microsoft ADAM, IBM LDAP Directory, or Sun Directory Server) that is used as the repository for ESSO-PG data.

Fields marked with an asterisk [*] are required

When you have completed your changes, click **Save Changes** to apply the new settings to ESSO-PG. After the storage settings are saved, you will be prompted to re-authenticate to ESSO-PG.

The information on this page is encrypted and saved to the registry under `HKLM\Software\Passlogix\PM\Server\Storage`.

Setting	Value
***Storage Type**	Choose one of the following storage locations: • Oracle Internet Directory • Oracle Directory Server Enterprise Edition • Oracle Virtual Directory • Sun Directory Server • Microsoft Active Directory • Microsoft ADAM • IBM LDAP Directory • Novell eDirectory
***Server**	Enter either the name of the server or the IP address of the server.
***Root DN**	The root directory. For example, DC=mydir,DC=com.
Provide this setting for Oracle Directories, Active Directory, IBM LDAP Directory, Novell eDirectory, and Sun Directory Server storage only:	
***User Path(s)**	The fully qualified path indicating the location of user accounts. There can be unlimited paths to search. The paths are searched in the order they are entered and are separated by a semicolon (;). For example, CN=users,DC=mydir,DC=com

Setting	Value
Provide these settings for Active Directory and or ADAM storage only:	
Prepend Domain	Select this option to add the user's domain to the username when naming the user's container. For example, for the domain *passlogix* and user *jamesk*, the container is named *jamesk* with this flag disabled and *passlogix.jamesk* with this flag enabled.
Provide this setting for Active Directory storage only:	
Locate in User	Select to enable searching for ESSO-PG user data under the Active Directory user objects.
Provide this setting for Sun LDAP storage only.	
User Prepend	Specifies the user naming attribute for user objects in the directory.This setting is used to form the relative distinguished name (RDN) of a user object. Typical values include "CN" or "UID."
Provide these settings for Oracle Directories, IBM LDAP Directory, Novell eDirectory, or Sun Directory Server storage only:	
***Connect as User**	The user name of the directory administrator.
***Password**	The password of the directory administrator.
Provide this setting for Oracle Directories, Active Directory, IBM LDAP Directory, Novell eDirectory, or Sun Directory Server storage only:	
Use secure connection (SSL)	Select to enable secure socket layer.
If using Configuration Objects or Role/Group support, provide these settings for all directory storage types:	
Use configuration objects instead of application list	Select to enable the use of configuration objects (COs) instead of application configuration lists, also known as the entlists. The ESSO-PG Server obtains the access control rights of its provisioning clients by searching the directory for provisioning objects. It finds only the objects it has access to.
Role/Group support	Select to enable Role/Group-based access control of administrative users. Enabling Role/Group support activates configuration object support. If Role/Group support is enabled, permissions should be specified. If no permissions are specified, by default, all users and groups are denied access for all actions. See Setting up Role and Group Support for information on setting up permissions.
Configuration and role/group objects root DN	Specifies where to begin the search for configuration and provisioning objects. The search moves from the specified locations downward. For example, *ou=vgoconfig,dc=test2003,dc=com* or *dc=passlogix,dc=com.* The path to this container must exist and contain at least one template prior to the input of these storage settings. The template can be in a sub-container rather than in the path itself. If this container does not exist, you will get an error message. See Setting up Role and Group Support for information on setting up permissions.

Settings > Event Log

Use the Event Log page to configure the server where events will be logged. When you have completed your changes, click **Save Changes** to apply the new settings to ESSO-PG.

Setting	Value
Database Type	Select the database you are using: • Oracle database • Microsoft SQL Server • Syslog Daemon The Syslog Daemon is not a database; however, you select it on the Event Log Settings page from the Database Type drop-down list in order to send events to the daemon. There are no parameters to set for the Syslog daemon. Configuration is done manually following installation. See the *ESSO-PG Installation and Setup Guide* for more information.
Provide this setting for Oracle Database only:	

Connection String	Enter the database connection string.
	For example, this string should be in the following form when using: Oracle using external authentication:
	`Provider=[OLE DB Provider] ;Data Source=[SID]; User Id=/;`
	Microsoft's Oracle OLE Provider:
	`Provider=MSDAORA ;Data Source=ORCL; User Id=/;`

Provide this setting for Microsoft SQL Server database only:	
Server	Enter the name of the server where events will be logged. SQL Server must be running on this machine, although the ESSO-PG database does not have to exist. If this is the first time this server is used by ESSO-PG, the Initialize Event Log box must also be checked so the ESSO-PG database is created. You cannot use the IP address of the server to specify the current machine. You must use the actual machine name (for example, pdevrx2). The name localhost cannot be used to refer to the local machine. You must use the name of the machine.
Provide this setting for the Oracle and SQL databases:	
Initialize Event Log	When enabled, this setting creates the ESSO-PG database on the specified server. If the database already exists, all existing data in the database is erased. Typically, this setting is used on the initial install and when you want to clear the log entries in the database. This setting is not saved.

Users

Users > Manage SSO Users

This page allows you to search for users and to add, modify, or delete their credentials. Users can be searched for by name or by the logons they have.

Find Users

Show user(s) with User Name. Enter the user name to search for. Leave this field blank to perform a search on all users. In the drop-down list, select either **substring match** or **exact match**.

Only show users who have logons for. This list includes all the possible applications available to users in your organization. Select one or more application to filter the result to show only users who have logons for these applications.

Show additional information. The search results list the usernames. The search results can also show **Logons** or **Pending Provisioning Instructions**. Select either of these options if desired.

Click **Find Users** when all information has been entered.

Search Results

The results list the **User Name** and, depending on whether additional information was selected, **Logons** and, if applicable, any **Pending Provisioning Instructions**. Use the buttons (which highlight on mouse-over) to add, delete, and modify users. Click on a user's name to view or edit that user's profile.

Applications that are not predefined (for example, on-the-fly Web applications) cannot be provisioned.

Add New Logon

Delete SSO User or

Delete Logon or

Cancel Provisioning Request

Modify Logon

user 1 Click on User Name

Users

Users > Manage SSO Users > Add New Logon

This page allows you to create a provisioning instruction to add a new application logon for a specific user. This page is accessed by searching for a user on the Manage SSO Users page and clicking the button next to the **User Name**.

Add Logons

SSO User. The ESSO-LM user name selected from the user search results.

Application. Lists all of the available applications. There is also an option to **not list applications that user already has a logon for**. After an application is selected, the Logon Information section refreshes and text boxes appear for each field required by the selected application.

Description. Allows you to modify a logon's description field as seen in the ESSO-LM Logon Manager. This field is optional.

Logon Information

User ID. User's username or ID for the application.

Password/Confirm Password. User's password for the application.

> After the **User ID** field is created, it cannot be modified. If a User ID must be changed, you must delete the existing logon and add a new logon with a new User ID. Depending on the requirements of the application being added, you might be prompted for additional fields, such as a Third or Fourth Field. Similarly, some applications might not require all of the fields. In such cases, the unnecessary fields do not appear.
>
> When you have entered all the required information, click **Add Logon** to submit your add request.

Users > Manage SSO Users > Delete SSO User

This dialog asks if you are sure that you want to delete the selected SSO user. Click **OK** to delete or **Cancel** if do not want to delete this user. When you click **OK**, a message will confirm that this user has been deleted.

Access this dialog box by searching for a user on the Manage SSO Users page and clicking the button next to **User Name**.

Users > Manage SSO Users > Delete Logon

This dialog box asks if you are sure that you want to delete the selected logon. Click **OK** to delete or **Cancel** if do not want to delete this logon. When you click **OK**, a message will confirm that this logon has been deleted. Access this dialog box by searching for a user on the Manage SSO Users page and clicking the button next to **Logon**.

Users > Manage SSO Users > Cancel Request

This dialog asks if you are sure that you want to cancel the pending provisioning instruction. Click **OK** to cancel or **Cancel** if do not want to cancel this request. When you click **OK**, the page will refresh and the pending provisioning instruction will no longer be displayed. Access this dialog box by searching for a user on the Manage SSO Users page and clicking the button next to **Pending Provisioning Request**.

Users > Manage SSO Users > Modify Logon

This page allows you to modify an application logon. Any fields that you leave blank on this page will not be changed. Access this page by searching for a user on the Manage SSO Users page and clicking the button next to **User Name**.

Logon to Modify

SSO User. The ESSO-LM user name selected from the user search results.

Application. The application to be modified.

User ID. Username or ID for the application.

> After the User ID field is created, it cannot be modified. If a User ID must be changed, you must delete the existing logon and add a new logon with a new User ID.
>
> If a logon does not have User ID associated with it, the password field cannot be modified. A User ID must exist in order to modify the password. Logons that do not have a User ID associated with them should be deleted and recreated with a User ID, if a new one is required.

New Logon Information

Password/Confirm Password. User's password for the application.

Description. Allows you to modify a logon's description field as seen in the ESSO-PG Logon Manager.

Third Field. The third field for this logon.

Fourth Field. The fourth field for this logon.

> Third and Fourth Fields are required only if the identified application is configured with a Third or Fourth Field. Depending on the requirements of the application being added, you might be prompted for additional fields. Some applications might not require all of the fields. In such cases, the unnecessary fields do not appear.
>
> When you have entered all the necessary information, click **Modify Logon** to submit your modify request.

Users > Manage SSO Users > Edit User

This page displays the selected user's logons and any pending provisioning instructions. Access this page by searching for a user on the Manage SSO Users page and clicking on the user's name in the search results list.

Edit User

User Name	Displays the selected user's name.
	Click to add a new logon for this user
	Click to delete this user.
Logons	Lists the logons assigned to the user.

Use the links and buttons (which highlight on mouse-over) to add, delete, and modify user logons.

Delete All Logons	Removes all logon credentials from the user's directory.
Advanced Delete	Allows you to generate a custom delete request.
	Deletes the specific logon associated with this user.
	Changes a user's logon credentials for a specific logon.

If a logon does not have user ID associated with it, the password field cannot be modified. Any credentials that do not have a user ID associated with them should be deleted and replaced.

Pending Provisioning Items	Displays any provisioning instructions pending for the selected user. Displays the provisioning instruction (such as add or delete), the application, and the creation and execution date for the provisioning instruction. Click **Cancel Instruction** to delete this instruction from the repository.

Advanced Delete

SSO User. Displays the ESSO-LM user name selected from the user search results.

Application. Lists the applications that can be deleted from this user. Select the application to delete from the drop-down list. The credential fields associated with the selected application are displayed. You must fill in all the credential fields exactly as they are stored in the directory:

- **User ID.** Enter the User ID.
- **Password/Confirm Password.** User's password for the application. These fields only appear if the application is configured to only have a password field.
- **Description.** Logon's description field as seen in the ESSO-LM Logon Manager.
- **Third Field.** The third field for this application logon.
- **Fourth Field.** The fourth field for this application logon.

When you have entered all the information has been entered, click **Submit** to submit your delete request.

Users > Add New SSO User

This page allows you to create new ESSO-LM users. This creates a storage object in the repository for the user. After the user is created, the Add New Logon page appears so that you can add applications for the new user.

Add New SSO User

User Name. Enter the user name to add. Click **Next**. The Add New Logon screen opens.

The user name must exist in the directory. If it does not, an error will occur.

Reports

Reports & Logs > Event Log

Use the Event log page to view the ESSO-PG event log. Events can be viewed by date periods and can be filtered by event type.

1. To select a date, click **Choose**.
2. Enter appropriate search parameters and click **View Log**. The log entries appear at the bottom of the screen:
   - Date/Time
   - Event Type
   - Provisioned User
   - Application
   - Execute Date
3. Click the  button for details on the status of the instruction.

The log is exportable to a CSV file, which can be loaded into many optional tools (Microsoft Excel, for example) for analysis.

1. To export the log file, click **Export Log**.
2. Select the export destination for the log file and click **OK**. These are the list of fields exported to this file:
   - Time Stamp
   - Event Type
   - User Name
   - Application
   - Execute Date
   - Provisioning Agent

Reports & Logs > Status Request

The Status page provides a summary of the status of the selected provisioning instruction.

State. The state of the instruction:

- Pending
- Retrieved
- Processed

Result. The result of the instruction:

- Success
- Failure
- Retrieved

Description. A detailed textual description of the instruction processing result.

Modified Date. The last time the instruction was modified. If the state of the instruction is "Pending," all the other fields are left blank.

Click **Back to Event Log** to return to the Event Log page.

Reports & Logs > Generate Report

Use the Generate Report page to download a CSV-formatted file containing all the data stored in the repository.

Select the type of report to generate:

Logons. This option generates an application report (user's credentials). This report contains the following fields:

- User DN (for example, cn=user1,ou=people,ou=vgo,dc=passlogix,dc=com)
- User name (for example, user1)
- Application Name
- Last Used Date
- Modified Date

Provisioning Instructions. This option generates a provisioning item report (user's provisioning instructions). This report contains the following fields:

- Instruction Type
- Instruction GUID
- Current Status
- Provisioned User
- Application
- Create Date/Time
- Execute Date/Time
- Provisioning Agent

Select the type of report to generate and click **Download Report**.

Setting Up Role or Group Support

ESSO-PG Role/Group support provides the capability to manage provisioning rights for specific applications and users. These provisioning rights are configured and managed in the ESSO-LM Administrative Console. To set up Role/Group support, open the ESSO-LM Administrative Console by clicking **Start** > **Programs** > **Oracle**> **ESSO-LM Console**.

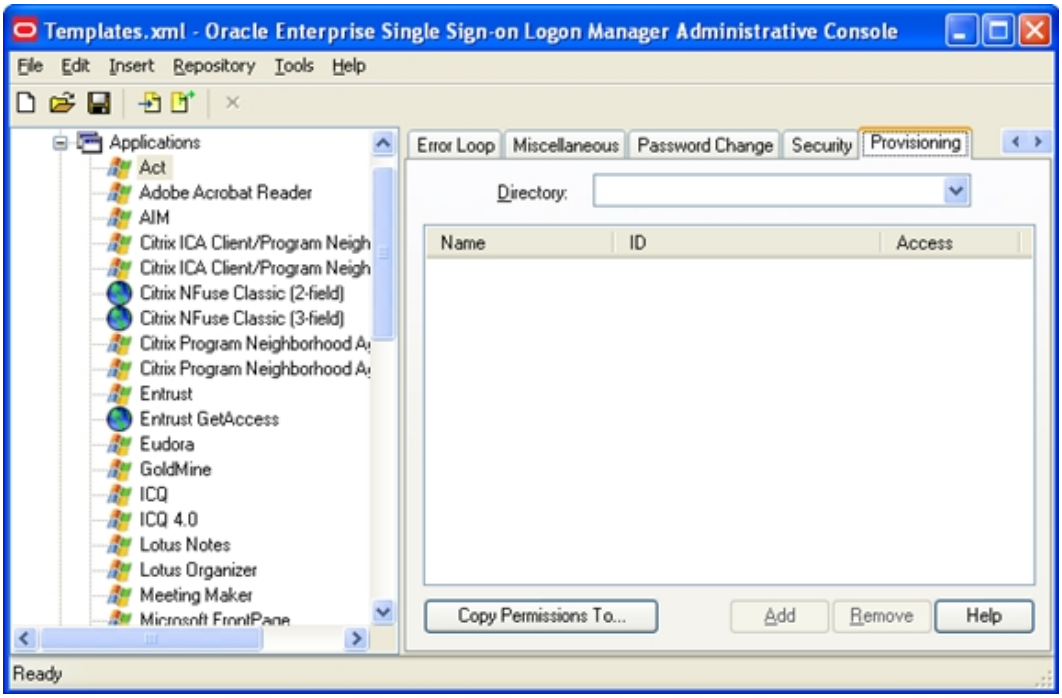
Two panels are available to manage provisioning rights:

- A Provisioning tab, which is located on the individual application panel. This tab enables you to manage provisioning rights for specific applications.
- A Provisioning Manager node, which is located in the ESSO-LM Administrative Console tree (left pane). This node enables you to manage provisioning rights for users.

Using the Provisioning Tab

To access the **Provisioning** tab, expand **Applications** on the left side of the ESSO-LM Administrative Console and double-click any application. Click the **Provisioning** tab.

From this tab, you can add or remove permissions. You can also select the level of access rights (add, modify, or delete applications) for those permissions.



Control	Value
Directory	Enables you to select the target directory server.
Name	Lists the groups or users who currently have access to this item.
ID	Lists the user's account name.
Access	Indicates the permissions that have been granted to the user or group (Add, Modify or Delete Logon). To change a user or group's access rights, right-click the user or group and select **Add Logon**, **Modify Logon**, or **Delete Logon** from the shortcut menu.

Control	Value
Copy Permissions To	Enables you to apply the provisioning rights for the current application to multiple applications. Click this button to display a dialog box listing all the applications. Select the applications that you want these provisioning rights to be copied to. Use **Ctrl**+click or **Shift**+click to select multiple entries. Click **OK**.
Remove	Removes selected users or groups from the list. Select a user or group to remove; use **Ctrl**+click or **Shift**+click to select multiple entries.

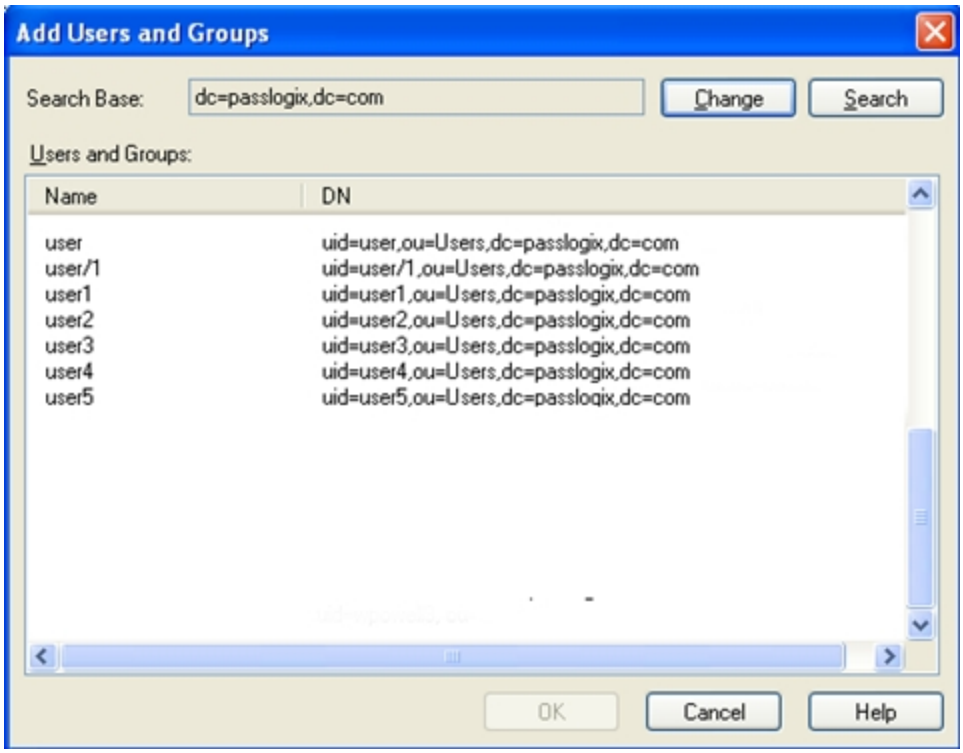
Adding Users or Groups

The dialog box that you use to add users or groups depends upon which directory server is being used:

- LDAP
- Active Directory or ADAM

LDAP

Use the Add Users and Groups dialog box to select the individual users or user groups that are to be added to the access list for the current configuration item (Add Logon, Modify Logon, or Delete Logon).

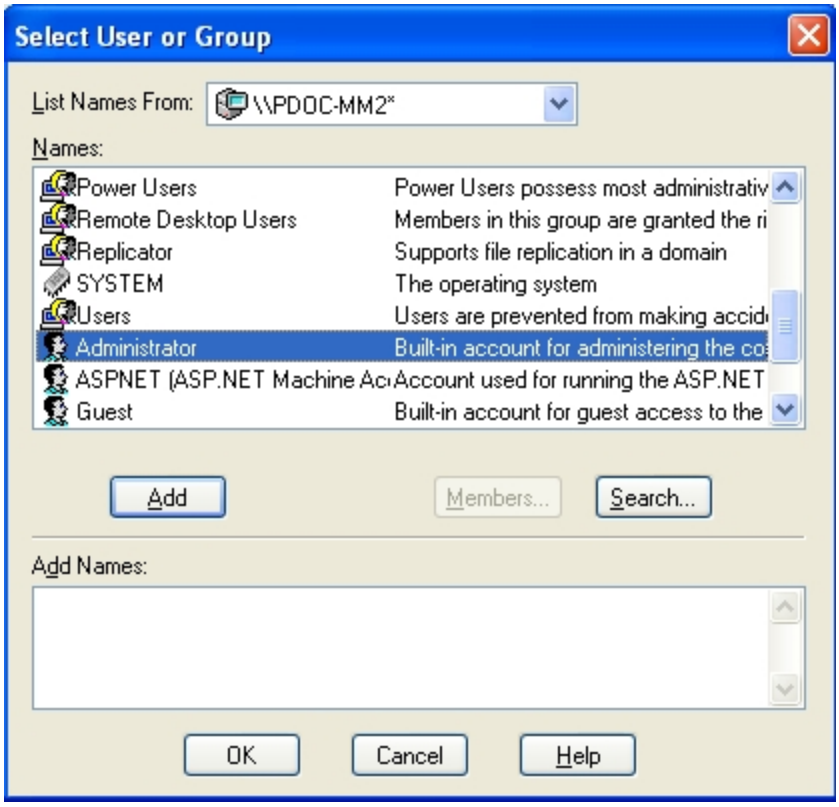


Control	Value
Search Base	The base (highest-level) directory to begin searching for user or group accounts. All subdirectories of the base directory are searched. Enter a location or click **Change** to browse the directory tree.

Control	Value
Change	Displays the Select Search Base dialog box to browse for a base directory for the search. Use this dialog box to browse to and select the base (highest-level) directory to search for user and group names. Click **OK** when finished.
Search	Begin searching the base directory for users and groups.
Users or Groups	Lists the search results. Select the names to be added to the access list for the current configuration item. Use **Ctrl**+click or **Shift**+click to select multiple entries. Click **OK** when finished to copy your selections to the access list.

Active Directory and ADAM

Use the Select User or Group dialog box to select the individual users or user groups that are to be added to the access list for the current configuration item (Add Logon, Modify Logon, or Delete Logon).



Controls	Value
List Names From	Select an Active Directory domain or server.
Names	Lists the names of users and groups for the selected domain or server. Select one or more names to add to the access list.
Add	Copies users and groups selected in the Names list to the Add Names list. Use **Ctrl**+click or **Shift**+click to select multiple entries.

Controls	Value
Members	When a group is selected the Names list, displays the Global Group Membership dialog box, which lists the members of the selected group.
Search	When a group is selected the Names list, displays the Global Group Membership dialog box, which lists the members of the selected group.
Add Names	Displays the names of the users or groups that you have you have added so far. Click **OK** to add these names to the access list for the current configuration item. You can type or edit user names in this list. However, entries are checked for invalid account names, and duplicate account selections are automatically removed when you click OK.

Using the Provisioning Manager Node

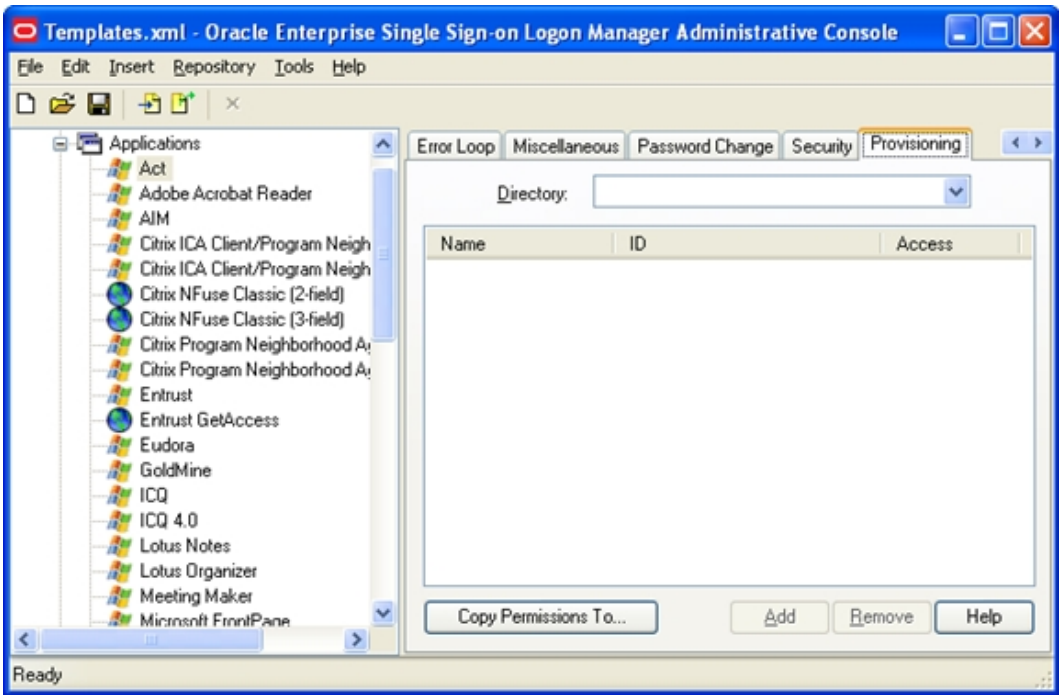
Use the **Provisioning Manager** node to manage provisioning rights for users. To access, click the **Provisioning Manager** node from the tree in the left pane. When you select the node, a pane (the right pane) is displayed with two tabs:

- Default Rights
- Delete SSO User Right

Default Rights

Use the **Defaults Rights** tab to define the provisioning rights for each new application created. This feature sets standard rights for each application created. After each application is created, change the rights as needed.

The controls on this tab function the same as the controls on the **Provisioning** tab.



Delete SSO User Right

Use the **Delete SSO User Right** tab to define the users to grant the Delete SSO User functionality to in the ESSO-PG Management Console.

The controls on this tab function in the same manner as those on the **Provisioning** tab.