CHAPTER 3

Users

Overview

You can add, edit and delete TES users from the **Users** interface. TES validates login names against its own user database. Before a person can operate TES, they must have a TES user account. Once a user name is registered, the user must log into Windows with that user name. Other user information includes their assigned security policy, their contact information and the runtime users for whom the user can run jobs.

User Authentication

There are three distinct entries for adding users, “Interactive Users”, “Runtime Users” and “LDAP Groups”. TES 6.0 allows for the setup of a user that authenticates against Active Directory/LDAP. TES also supports
AD/LDAP only users.

At login, user credentials are validated against Active Directory/LDAP. Once authenticated, TES obtains the user’s AD/LDAP groups and other information such and phone number and email.

Once login has completed as described above, a record is established in TES to represent the Active Directory/LDAP only user if it is not already present and only if the user belongs to an Active Directory/LDAP group defined in TES. All user activity logging is then performed against this new user record allowing for correct auditing and reporting.

Active Directory/LDAP only users are allowed to create and own jobs and other objects if their security permissions permit.

User Account Concepts

Interactive User

During installation of the Windows master, you provide an existing user in the AD/LDAP User Account. TES creates the first TES user account for you with this information, and automatically assigns you **Super User** capability. Having the **Super User** option selected in a User Definition provides access to all TES functions, and supersedes all security policies because it encompasses all security permissions. From this point on, you can set up other users, and specify their user data.

Along with specifying other user data, you need to specify a security policy for each user. TES comes with default security policy templates to help specify the appropriate functions available for each user based on a default network scheduling model.

Note You cannot remove Super User capability from the initial TES user account until at least one more user has been defined and given Super User capability.

When a new user launches TES, TES checks to see if the user's login name is listed in the TES database. If the user is not listed, it displays an error message, and prevents the user from entering TES.

Runtime Users

If you are going to schedule jobs for other users, you can specify those users on the **Runtime Users** tab of the **User Definition** dialog. This is necessary to access commands and environments created by those users for whom you are scheduling.

LDAP Groups

LDAP users can be imported into TES for improving user audit trails. These imported users inherit security from multiple LDAP groups. Imported LDAP user information is stored into a user definition that includes email, telephone, etc. Imported LDAP users are allowed to be owners of scheduling constructs such as jobs if their security permits.

Users and Workgroups

Workgroups help organize users according to job function, security level, geographical area or any other category that may be helpful. TES workgroups can correspond to Windows workgroups, but they certainly do not have to. When you create a workgroup, you must always remember to add yourself to the workgroup. Creating a workgroup does not automatically make you a member of the workgroup. The extent of control you can wield over a workgroup is also dependent upon your individual TES security policy. For more information about security policies, see "Security Policies Pane" section on page 3-77.

Note When you install TES, you are automatically placed in the *Schedulers* workgroup. *Schedulers* is TES's default workgroup.

Impersonating a User

Impersonating a user is one of the higher-level security permissions. When you impersonate another user, you have access to their TES jobs, job actions, job events, system events, user variables, calendars and workgroups as if you had logged on as that user.

Contact Information

You can specify and update user contact information such as phone number and email address. TES or another user can use this contact information to inform you of the status of a job.

Users Interface

From the **Navigator** pane, choose **Administration>Runtime Users/Interactive Users** or **LDAP Groups** to display the **Users/LDAP Groups** interface.

To change how the list of users/groups is sorted, click the head of a column to use it as a sort key.

Buttons

The **Users** interface contains the following buttons:

- **Admd** – Displays the **User/LDAP Group Definition** dialog to add a new user/group.
- **Edit** – Displays the **User/LDAP Group Definition** dialog to edit a user/group.
- **Delete** – Removes the selected user/group definition from the TES database.
- **Copy** – Creates a copy of the selected user/group definition from the TES database. You can rename the user/group definition and save time when creating several user definitions with the same security profile.
- **Print** – Displays the **Reports** pane to view and print your user/group definitions. For more information, see <Jumps>“Monitoring Production” on page 361.
- **Refresh** – Updates the data in the current pane.

Search Field

Enter text that you want to search for within the columns displayed into this field.

Note This field at the top right of the grids will only search text columns that are not grayed out and are string-based. See Searchable Columns, page 2-35.

Columns

Note The **Users** interface contains the following columns:Depending on the selected user, some columns may not display.

- **Full Name** – The user’s full name.
- **Name** – The name of the user.
- **Domain** – The user’s domain.
- **Security** – The security policy assigned to the user.
- **Super User** – Indicates if the user has **Super User** capabilities.
- **Modified** – The last time this user definition was modified.

Users Preferences Dialog

If you choose **View > Preferences** from the main menu bar while viewing the **Users / LDAP Groups** interface, the **Users Preferences** dialog displays.

From the **Users / Group Preferences** dialog, you can select which columns are displayed in the **Users / LDAP Groups** interface and in what order the columns appear.

- A checkmark to the left of a column title indicates that it will be displayed in the pane. No checkmark indicates that it will not be displayed.
- To rearrange the order in which the columns are displayed, select the column and click the up or down arrow.

Navigator Context Menu

With a user/group selected, right-click in the **Interactive / Runtime Users** or **LDAP Groups** pane to display the context menu.

Depending on the user/group selected, the context menus contains the following elements:

- **Add User / Group** – Displays the **User / LDAP Group Definition** dialog to add a new user/group. Has the same function as the **Add** button.
- **Refresh** – Updates the data in the current pane.
- **Print** – Displays the **Reports** pane to view and print your user/group definitions. Has the same function as the **Print** button on the toolbar. For more information, see <Jumps>“Monitoring Production” on page 361.
- Note to the Writer: Unable to update the cross ref
- **Export** – Saves the data in the current pane as an HTML file.
- **Preferences** – Displays the **Preferences** dialog for the **User / LDAP Group** pane.
- **New Root Folder** – Allows you to create a new root folder for the **Navigator** pane.

Users Context Menu

With User/Group selected, when you right-click in the **Interactive / Runtime Users** or **LDAP Groups** pane, the context menu displays.

Depending on your selection, the context menus contain the following elements:

- **Add Interactive / Runtime Users / Group** – Displays the **User / LDAP Group Definition** dialog to add a new user/group.
- **Edit Interactive / Runtime Users / Group** – Displays the **User / LDAP Group Definition** dialog to edit the selected user/group. You can double-click a user/group name as an alternative to selecting this menu item.
- **Delete Interactive / Runtime Users / Group** – Deletes the selected user/group.
- **Copy Interactive / Runtime Users / Group** – Duplicates the selected user/group definition. You can use this option to efficiently create multiple users/groups with similar characteristics.
- **Refresh** – Updates the data in the current pane.
- **Print** – Displays a report with a list of selected users/groups with the option to print to a printer.

- **Print Selected** – Displays a report with a list of selected users/groups with the option to print selected users/groups only to a printer.
- **Add to all super users** – Adds a selected user/group record to all user records.
- **Impersonate User** – Impersonate another user, you have access to their Tes features as if you had logged on as that user.
- **End Impersonation** – Ends the impersonation of another user.

User Definition Dialog for Interactive Users

The **Users** interface for Interactive Users displays by choosing **Administration > Interactive Users**. To view the **User Definition** dialog, click the **Add** or **Edit** buttons from the **Interactive Users** interface or right-click in the **Navigator** pane and choose **Add Interactive Users** or **Edit Interactive Users** from the context menu. You can also double-click an Interactive user to display that user's definition.

Common To All Tabs

- **User Name** – Type a logon name for the user. This field is integrated with Windows to display existing users defined for the selected domain.

  You can use an active directory name in this field if you want but you must leave the **Domain** field blank for this to work. (An active directory name would be in this format, *username@domainname*, such as *jjohn@Tidalsoft*.)
- **Full Name** – The name of the user as displayed in TES panes consisting of up to 30 characters. This name must be unique.
- **Domain** – Specify a domain associated with this user account.

Security Tab

- **Super User** – Click this radio button to provide the user with access to all available TES functions.
- **Other** – Click this radio button to assign one of the other defined security policies from the drop-down menu.

Runtime Users Tab

Typically the runtime users option is used by users with the responsibility of running jobs for others such as Schedulers or Operators. When you select runtime users for a user definition, the user gains the rights and access to all of the runtime users' commands and environments, but only when scheduling and running jobs. This tab lists the defined users and user groups. The user being defined can only be a runtime user for a user if that user name is selected. User groups work the same way. You can either display the defined users or the defined user groups but not both at the same time.

This tab contains the following elements:

- **Show Users** – Displays all defined users for this installation. The runtime users (users for which this user can schedule and run jobs) are indicated by a checkmark to the left of the listed name.
- **Show Groups (Windows)** – Displays all defined user groups.

Agents Tab

This tab contains the following elements:

- **Untitled Text Field** – This field displays all defined TES agents for this installation. The agents which this user can use to run jobs are indicated by a checkmark to the left of the listed name.
- **All Agents** – Select the **All Agents** option when you want the user to have access to all available agents. When the **All Agents** option is selected, the check boxes to the left of each listed agent disappear.

Note If the **All Agents** option is not selected, and no individual agents are selected, the user will be unable to run any jobs.

Notification Tab

This dialog contains the following elements:

- **Phone Number** – The user's phone number.
- **Pager Number** – The user's pager number.
- **Email Address** – The user's email address. The email address entered here is used to receive notification during email actions and to log in for anonymous FTP.

Passwords Tab

This tab contains the following elements:

- **Windows/FTP Password** – This field is used for running jobs on Windows/FTP machines.
- **Confirm Password** – Retype the password you entered in the **Windows/FTP Password** field to verify its accuracy.
- **Adapter** – Contains the adapter name.
- **Password** – Contains the password for the associated adapter.
- **Add** – Click to add a new record via the **Change Password** dialog.
- **Edit** – Click to edit an existing record via the **Change Password** dialog.
- **Delete** – Click to delete a selected record.

Workgroups Tab

This tab contains the following elements:

- **Workgroup** – The names of the workgroups under which the user is a member. To be a member of a workgroup, you must be added into that workgroup by the workgroup's owner.
- **Owner** – The owners of the workgroups of which the user is a member.

Description Tab

A free text field for any comments regarding the user, up to 255 characters long.

User Definition Dialog for Runtime Users

The **Users** interface for Runtime Users displays by selecting **Administration>Runtime Users**. To view the **User Definition** dialog, click the **Add** or **Edit** buttons from the **Users** interface or right-click in the **Navigator** pane and select **Add Runtime Users** or **Edit Runtime Users** from the context menu. You can also double-click a Runtime user to display that user's definition.

LDAP Group Definition Dialog

The **LDAP Group** interface displays by selecting **Administration>LDAP Groups**. To view the **LDAP Group Definition** dialog, click the **Add** or **Edit** buttons from the **LDAP Group** interface or right-click in the **Navigator** pane and select **Add Group**. You can also select **Edit Group** from the context menu of the **LDAP Groups** pane or double-click an LDAP group to display that group's definition.

Note Features associated with LDAP Groups are common to other Users. See "Adding Interactive Users" section on page 3-70.

User Configuration Procedures

Adding Runtime Users

To add a Runtime user:

Step 1 From the **Navigator** pane, select **Administration>Runtime Users** to display the **Runtime Users** pane.

Step 2 Click the **Add** button or right-click in the **Navigator** pane and select **Add Runtime Users** from the context menu to display the **User Definition** dialog.

Step 3 If this is a new user definition, enter the new user name in the **User Name** field.

Step 4 For documentation, enter the **Full Name** or description associated with this user.

Step 5 In the **Domain** field, select a Windows domain associated with the user account required for authentication, if necessary.

Step 6 In the **Windows/FTP Password** field, enter the password for the user account provided by the Administrator.

Step 7 In the **Confirm Password** field, retype the password.

Step 8 If the passwords entered in the **Windows/FTP Password** and **Confirm Password** fields do not match, you must re-enter the password in both fields.

Step 9 Click **OK** to add or save the user record in the TES database.

Adding Interactive Users

To add an Interactive user:

Step 1 From the **Navigator** pane, select **Administration > Interactive Users** to display the **Interactive Users** pane listing all TES users.

If the TES users do not appear, you do not have the appropriate rights to view users.

Step 2 Double-click the name of an user account that you want to be able to run jobs to display the **User Definition** dialog.

Step 3 Click the **Runtime Users** tab in the **User Definition** dialog and select the check box(es) beside the name(s) of the Interactive user(s) you want to include in this TES users authorized user list.

Step 4 If you wish to restrict this user's access to specific servers, click the **Agents** tab and make the appropriate selections.

Step 5 Click **OK**.

Deleting a User

Note You cannot delete a user that presently owns a job, job event, system event, action, user defined variable or calendar. Open each item's dialog and reassign the ownership of the items before deleting the user

To delete a user:

Step 1 From the **Navigator** pane, select **Administration > Interactive Users** or **Runtime Users** to display the **Users** interface.

Step 2 Select the user to delete and click the **Delete** button on the TES toolbar or right-click the user record and select **Delete User** from the context menu.

Step 3 When a dialog asks you to confirm your choice, click **OK**.

Editing a User Definition

To edit a user definition:

Step 1 From the **Navigator** pane, select **Administration > Interactive Users** or **Runtime Users** to display the **Users** interface.

Step 2 Double-click the user record to edit or select the user name and click the **Edit** button or right-click the user record and select **Edit User** from the context menu to display the **User Definition** dialog.

Step 3 Edit the **User Name** if it does not match the Windows login name. Remember that the user name is case-sensitive.

Step 4 Edit the **Full Name** if necessary.

Step 5 To change the **Security Policy** for an Interactive user, select a new one from the drop-down menu on the **Security** tab. If you have the **Superuser** option set, the list is disabled. Click the **Superuser** option if you want the user to have access to all TES functions. To add or remove specific functions to a security policy, see "Security Policy Procedures" section on page 3-108.

Step 6 To add or remove runtime users for an Interactive user, click the **Runtime Users** tab.

Select the runtime users to add to the user's definition from the **Available Users** list.

- To include users, select the check box next to the user you want to include.
- To exclude users, clear the check box next to the user you want to exclude.

The user will have access to the commands and environments of the runtime users you assign.

Step 7 If you wish to change an Interactive user user's access to specific servers, click the **Agents** tab and make the appropriate selections.

Step 8 Click the **Notification** tab to edit contact information for the Interactive user.

Step 9 Edit the password information, if necessary.

Note You cannot edit Workgroups information from the **User Definition** dialog. For more information on TES workgroups, see "Workgroups Pane" section on page 3-72.

Step 10 Click the **Description** tab to edit the user's description (up to 255 characters).

Step 11 Click **OK**.

Step 12 Jobs in the production schedule that have not run yet will reflect the changes to the user data. Jobs that are running or that have completed retain the old user information.

Impersonating Another User

To impersonate a user:

Step 1 From the **Navigator** pane, select **Administration > Interactive Users** to display the **Interactive Users** pane.

Step 2 Right-click the user you want to impersonate and select **Impersonate User** from the context menu.

Step 3 When a dialog asks you to confirm your choice, click **OK**.

Ending User Impersonation

To end user impersonation:

Step 1 From the **Navigator** pane, select **Administration > Interactive Users** to display the **Interactive Users** pane.

Step 2 Right-click the user and select **End Impersonation** from the context menu

–or–

Select **Activities>End Impersonation** from the main menu bar.

Viewing Users

From the **Navigator** pane, select **Administration>Interactive/Runtime Users** or **LDAP Groups** to display the **Users/Groups** interface. If the users/groups do not display, you do not have the appropriate rights to view these items.

Workgroups Pane

A workgroup is a set of users categorized under a communal name for the purpose of sharing items (jobs, actions, events etc.) which are owned by the workgroup. Each user in the workgroup has access to these items based on their own individual security policy.

If you have appropriate rights in your security policy you can create your own workgroups from the **Workgroup** pane. This pane displays all existing workgroups (within the bounds of your security policy). When you create a workgroup, you become its owner, and can add users to it; however, you must be a **Super User**. To belong to a workgroup created by another user, you have to be added by that user.

Note If you own a workgroup and do not include yourself in it, the workgroup's associated items would not be accessible to you.

You can change the name and the members of any workgroup that you own. You cannot edit a workgroup that was created by another user unless you impersonate that user.

Workgroups help focus the information TES displays to each user. When you open the **Jobs**, **Actions**, **Job Events**, **System Events**, **Calendars**, or **Variables** panes, you will see only the items belonging to you and belonging to the workgroup(s) to which you belong.

For example, if you belong to a Payroll workgroup, you can see all the jobs, actions, etc., that are owned by the Payroll workgroup and were created by you or other members of the workgroup.

The following figure shows a generic workgroup structure using five users and two workgroups. Note that, in this figure, **User 3** belongs to both workgroups, and therefore has access to all items (calendars, jobs, etc.) shown.

Workgroups Pane Interface

From the **Navigator** pane, select **Administration>Workgroups** to display the **Workgroups** pane.

Buttons

- **Add Workgroup** – Displays the **Workgroup Definition** dialog to add a new workgroup.
- **Edit Workgroup** – Displays the **Workgroup Definition** dialog to edit an existing workgroup.

Note You can change the name and the members of any workgroup that you own. You cannot edit a workgroup that was created by another user unless you impersonate that user.

- **Delete Workgroup** – Deletes the selected workgroup as long as the workgroup does not currently own any TES items.
- **Copy Workgroup**– Creates a copy of the selected workgroup definition from the TES database. You can rename the workgroup definition and save time when creating several workgroup definitions with the same security profile.
- **Print Workgroups** – Displays the **Reports** pane to view and print your selected workgroup definitions. For more information, see <Jumps>"Monitoring Production" on page 361.
- **Refresh** – Updates the data in the current pane.

Search Field

Enter text that you want to search for within the columns displayed into this field.

Note This field at the top right of the grids will only search text columns that are not grayed out and are string-based. See Searchable Columns, page 2-35.

Columns

- **Name** – The name of the workgroup.
- **Users** – The users that are included in the workgroup.
- **Owner** – The owner of the workgroup.
- **Modified** – The last time the workgroup definition was modified.

Workgroups Preferences Dialog

If you select **View>Preferences** from the main menu bar while viewing the **Workgroups** pane, the **Workgroups Preferences** dialog displays.

From the **Workgroups Preferences** dialog, you can select which columns are displayed in the **Workgroups** pane and in what order the columns appear.

- A checkmark to the left of a column title indicates that it will be displayed in the pane. No checkmark indicates that it will not be displayed.
- To rearrange the order in which the columns are displayed, select the column and click the up or down arrow.

Navigator Context Menu

When you right-click in the **Navigator** pane while viewing the **Workgroups** pane, the **Navigator** context menu displays.

The following describes the items in the Workgroups **Navigator** context menu:

- **Add Workgroup** – Displays the **Workgroup Definition** dialog to add a new connection.

- **Preferences** – Displays the **Preferences** dialog for the **Workgroups** pane.
- **Print** – Displays the **Reports** pane to view and print your workgroup definitions. Has the same function as the **Print** button on the toolbar. For more information, see <Jumps>“Monitoring Production” on page 361.
- **Export** – Saves the data in the current pane as an HTML file.
- **Refresh** – Updates the data in the current pane.
- Note to the Writer: Unable to update the cross ref

Workgroups Pane Context Menu

When you right-click in the **Workgroups** pane, the **Workgroups** context menu displays.

The following describes the items in the **Workgroups** context menu.

- **Add Workgroup** – Displays the **Workgroup Definition** dialog to add a new workgroup. If you add a workgroup, it displays in the **Jobs**, **Actions**, **Job Events**, **System Events**, **Workgroups**, **Calendars** and **Variables** panes.
- **Edit Workgroup** – Displays the **Workgroup Definition** dialog to edit the selected workgroup. You can double-click the workgroup as an alternative to selecting this menu item. Only a Super User or the selected workgroup’s owner can edit a workgroup.
- **Delete Workgroup** – Deletes the selected workgroup.
- **Print** – Displays the **Reports** pane to view and print your workgroup definitions. For more information, see <Jumps>“Monitoring Production” on page 361.
- Note to the Writer: Unable to update the cross ref

Workgroup Definition Dialog

The **Workgroup Definition** dialog displays when adding or editing a workgroup from the **Workgroups** pane.

Common To All Tabs

- **Workgroup Name** – The name of the workgroup, as displayed in the **Workgroup** pane (up to 30 characters). Each workgroup must have a unique name.
- **Owner** – The owner of the workgroup.

Users Tab

Displays a list of all defined TES users and allows you to assign security policies for each user within the workgroup, in addition to the user’s existing security policy.

Note Editing a user’s security policy while defining a workgroup does not remove permissions that the user already has. You can only assign additional security policies as part of the specific workgroup.

Groups Tab

Displays a list of all defined TES groups. A checkmark indicates groups that are assigned to the current workgroup.

Agents Tab

The **Agent** tab displays all the TES agents that the owner of the workgroup is authorized to use. The agents which the workgroup can use to run jobs are indicated by a checkmark to the left of the listed name.

This tab displays the following element:

- **All Agents for <workgroup owner>** – Select the **All Agents for <workgroup owner>** option when you want the workgroup to have access to all the agents available to the workgroup's owner. When this option is selected, the check boxes to the left of each listed agent disappear.

Note If the **All Agents for <workgroup owner>** option is not selected and no individual agents are selected, the workgroup cannot run any jobs.

Description Tab

The **Description** tab contains a free text field where you can enter comments about the workgroup (up to 255 characters).

Workgroups Procedures

Adding a Workgroup

To add a workgroup:

Step 1 From the **Navigator** pane, select **Administration>Workgroups** from the main menu bar TES to display the **Workgroups** pane.

Step 2 Click the **Add** button on the TES toolbar or right-click and select **Add Workgroup** from the context menu to display the **Workgroup Definition** dialog.

Step 3 Type a unique name for the workgroup in the **Workgroup Name** field (up to 30 characters).

Step 4 Click the **Members** tab.

Step 5 Select the users to add to the workgroup from the **Available Users** list.

- To include users in the workgroup, select the check box next to the user.
- To exclude users from the workgroup, clear the check box next to the user.

Note Always include yourself in the workgroups you define; otherwise, you cannot access its definition or owned items.

Step 6 Click the **Agents** tab.

Step 7 Select the agents to add to the workgroup.

Step 8 To enter a description for this workgroup, click the **Description** tab and type in the description. You can enter up to 255 characters.

Deleting a Workgroup

You can delete a workgroup from the **Workgroups** pane. Workgroups can be deleted *only* when they no longer own jobs, actions, job events, system events, calendars and/or variables. (Go to each item owned by the workgroup and change the ownership.)

To delete a workgroup:

Step 1 From the **Navigator** pane, select **Administration > Workgroups** from the main menu bar TES to display the **Workgroups** pane.

Step 2 Select the workgroup to delete and click the **Delete** button on the TES toolbar or right-click the workgroup and select **Delete Workgroup** from the context menu.

Step 3 Click **Yes** in the **Confirm** dialog.

Editing a Workgroup

You can change the name and the members of any workgroup that you own. You cannot edit a workgroup that was created by another user unless you impersonate that user.

When you change the members of a workgroup, updates for affected users will occur the next time they reopen the **Jobs**, **Actions**, **Job Events**, **System Events**, **Calendars** and/or **Variables** panes.

To edit a workgroup:

Step 1 From the **Navigator** pane, select **Administration > Workgroups** from the main menu bar TES to display the **Workgroups** pane.

Step 2 Select the workgroup you would like to edit and click the **Edit** button on the TES toolbar or double-click the workgroup you would like to edit or right-click the workgroup you would like to edit and select **Edit Workgroup** from the context menu.

Step 3 The **Workgroup Definition** dialog displays.

Step 4 To change the name of the workgroup, edit the **Workgroup Name** field.

Step 5 To include users in the workgroup, select the check box next to the name of the user you want to include. To exclude users from the workgroup, clear the check box next to the name of the user you want to exclude.

Note Always include yourself in the workgroups you define; otherwise, you will not have access to its definition or owned items.

Step 6 To edit the agents of the workgroup, click the **Agents** tab.

- To exclude agents from the workgroup, clear the check box next to the name of the agent you want to exclude.

- To include agents to the workgroup, select the check box next to the name of the agent you want to include.

Step 7 To edit the description of the workgroup, click the **Description** tab.

Step 8 Edit the description text for the workgroup. You can use up to 255 characters.

Viewing Workgroups

In the **Workgroups** pane, you can view all the workgroups that you own. When in the **Jobs**, **Actions**, **Job Events**, **System Events**, **Variables** and **Calendars** panes, all the workgroups that you own and belong to can be seen. Workgroup association can also be seen in the **User Definition** dialog.

From the **Navigator** pane, select **Administration > Workgroups** from the main menu bar TES to display the **Workgroups** pane.

Viewing Members of a Workgroup

To view members:

Step 1 From the **Navigator** pane, select **Administration > Workgroups** from the main menu bar TES to display the **Workgroups** pane.

Step 2 Double-click the workgroup you would like to examine to display its definition.

Viewing the Workgroups to Which You Belong

To view a workgroup to which you belong:

Step 1 From the **Navigator** pane, select **Administration > Workgroups** from the main menu bar TES to display the **Workgroups** pane. If the TES users do not appear, you do not have the appropriate rights to view users.

Step 2 Double-click the user name to display its **User Definition** dialog with the user information.

Step 3 Click the **Workgroups** tab. All the workgroups that the user belongs to are listed.

Security Policies Pane

Security policies restrict access to certain TES functions. The defined access rights can be saved as a security policy, and then assigned to one user or multiple users.

For example, there might be different sets of users who:

- Administer TES
- Create and schedule jobs for themselves and others
- Operate the job schedule

You may have a set of users that creates jobs, a set of users that schedule jobs and another set that works with the job schedule. Using security policies, the users creating jobs can be restricted from inserting them into production and changing the schedule. The other users can be restricted from creating jobs.

TES includes default security policy templates that can be modified to create your own security policies. Each user within the supplied working model has a defined set of TES functions. When all the default security policies are in use, all aspects of scheduling are covered and available.

The following table lists the system features available for each of the default security templates:

Table 3-1 TES Security Policies

Default Security Policy	Available System Features
Scheduler_Administrator	The default for new installations. This includes all available functions.
Administrator	Configures users.
User	Creates, edits, and submits jobs. Creates workgroups and user-defined variables.
Scheduler	Edits and tests job schedules.
Operator	Runs and controls jobs. Responds to alerts that jobs may issue.
Inquiry	Views jobs and resources. Cannot perform modification.

Each security policy has its own name, description, and set of TES functions that it comprises it. Functions are chosen from a list of available functions and listed in the **Security Policy Definition** dialog. Once defined, security policies can be assigned to users from the **User Definition** dialog.

You can override security policy restrictions for a user by selecting the **Super User** option in the **User Definition** dialog. Users with Super User authority have access to all TES functions.

Note If you are the only defined TES user, you will not be allowed to remove the Super User option from your profile until you have defined at least one other TES user with Super User capability. This is a safety feature to prevent inadvertent exclusion from TES, which would require you to reinstall the product.

Security Policy Templates

TES includes a set of default security policy templates. Inherent in these templates is the default network scheduling model where each user has a defined set of scheduling tasks. When all the security policies are assigned to users, the result is a complete enterprise network scheduling solution. Each user makes their contribution to the entire scheduling process. Each user can be insulated from tasks that are not relevant to their scheduling role.

You can modify these templates to create your own scheduling model based on the needs of your organization. Use caution so that vital functions are not inadvertently left out of a particular profile.

Note Selecting the Super User option in a User Definition supersedes any security policy previously assigned. The Superuser option provides full and unrestricted access to *all* TES functions. Some functions, such as calendars supersede even SuperUser privileges and are controlled by the function's owner and available only to members of a workgroup. A SuperUser may access a function but can not modify the function if not a member of the workgroup.

Default Security Policies

The following table summarizes the functions that are available for each user account using the security policies provided with TES. If the function has been included in the security policy assigned to your user account then you have the capability described in that function.

Table 3-2 Functions available with the default security policies

Default Security Policy	Available Functions
TES Admin	All TES functions are available.
Administrator	Functions for configuring TES including configuring users, security, queues, agent lists, connections, and licenses.
	(Continued)
Scheduler	All functions except adding users.
Operator	Functions for end-user support such as schedule control and queue and agent list configuration. Ability to edit job information as necessary.
User	Functions for end-user activity excluding configuration and schedule control, but including the tools necessary for creating, editing and submitting jobs.
Inquiry	Functions for viewing jobs and other items, but not for creating, editing, or deleting.

TES Functions

Each security policy includes the TES functions that a user with that policy can perform. You can create new security policies from the **Security Policy Definition** dialog, or add and remove TES functions to an existing security policy. When you finish defining a security policy, you assign it to a user through the **User Definition** dialog.

Note To use a job as a job dependency, you must have the ability (security policy permission) to View the job. However, View permission alone does not enable you to perform job control functions on the job.

Function Descriptions

The following are descriptions of each TES function, grouped by category, that can be added to or removed from a security policy:

Agent Lists Category

Table 3-3 Agent Lists Functions

Function	Description
Add Agent List	Specify a group of agents for the purpose of agent fault tolerance (dynamic rerouting), workload balancing and job broadcasting. The list will be available to all users that schedule jobs.
Edit Agent List	Edit the properties of an agent list.
Delete Agent List	Delete any agent list that exists in theScheduler database.
View Agent List	View the properties of any agent list.

Alerts Category

Table 3-4 Alerts Functions

Function	Description
Acknowledge Alert	Acknowledge a console alert generated by a job event or system events.
Close Alert	Complete the response to a console alert.
View Alert	View alert details.

Calendar Category

Table 3-5 Calendar Functions

Function	Description
Add Calendar	Create a calendar of dates that determines when to run jobs. You can also create calendar groups and make calendars and calendar groups public if you have the **Add Public Data** function.
Edit Calendar	For calendars owned by you or your group you can change the dates within a calendar. You can also add and delete the calendars in calendar groups.
Delete Calendar	Delete your own calendars and calendar groups.
View Calendar	View the dates defined for a calendar.

Configuration and Licensing Category

Table 3-6 Configuration and Licensing Functions

Function	Description
Edit Configuration/License	Access to the **System Configuration** dialog. You can change master configuration data, update licenses, configure mail, job defaults, and other system-wide settings.
View Configuration/License	View alert details.

Connections Category

Table 3-7 Connections Functions

Function	Description
Add Connection	Add a new connection definition.
Edit Connection	Edit a connection definition.
Delete Connection	Delete a connection definition
View Connection	View the details of connection information.
Edit Agent Job Limit	Change the number of jobs that can run on an agent at the same time.
Edit Machine Name	Edit the agent machine designation.

General Category

Table 3-8 Connections Functions

Function	Description
Add Public Data	Add events, actions, calendars, and variables so that they can be used by anyone who schedules jobs. You must have the security rights to add and/or edit these items to make them public.
View Logs	View the audit trail of all scheduling activity, error messages, and diagnostics from the **Logs** pane. You can view all messages generated by the sources specified in the **System Configuration** dialog, **Logging** tab.
View Reports	View the results of TES reports.
View History	View the audit trail of TES activity.
View Master Status	Access to the **Master Status** pane, where you can view all the statistics related to the TES master.
Move Jobs to Production	Use Transporter to copy all jobs to other databases whether the user owns them or not.
Move Own Jobs to Production	Use Transporter to copy only the jobs that the user owns to other databases.

Job Actions Category

Table 3-9 Job Actions Functions

Function	Description
Add Job Actions	Create actions (messages, jobs, variable updates) to support specific job events and system events.
Edit Job Actions	Edit the properties of an action that is owned by you or your workgroup.
Delete Job Actions	Delete an action that you own.
View Job Actions	View the specifics of all actions available.

Job Classes Category

Table 3-10 Job Classes Functions

Function	Description
Add Job Class	Create a class to which jobs can be assigned. Job classes are available to all schedulers.
Edit Job Class	Edit a job class.
Delete Job Class	Delete a job class.
View Job Class	View the description of a job class.

Job Console (Activity) Category

Table 3-11 Job Console (Activity) Console Functions

Function	Description
View All Jobs	View the activity of all job occurrences as they are scheduled and run. You will also be able to view console alerts created by jobs. to add and/or edit these items to make them public.
View Own Jobs	View the activity of your own job occurrences or those owned by your workgroup(s) as they are scheduled and run. You will also be able to view console alerts created by those jobs.
Edit All Jobs	Edit the definition of any job or job group.
Edit Own Jobs	Edit job and job group definitions that are owned by you or your workgroup(s).
Control All Jobs	Apply job control to all jobs and job groups, within any limits set in the job control functions.
Control Own Job	Apply job control to jobs and job groups owned by you or the workgroup(s) you belong to, within any limits set in the job control functions.

Job Control Category

Table 3-12 Job Control Functions

Function	Description
Ad Hoc Job Control	Manually add an unscheduled job to production.
Cancel/Abort	Manually cancel or abort a job occurrence from the **Job Activity** pane. Canceled and aborted jobs cannot be resumed. They must be rerun.
Hold/Stop	Manually hold or stop a job occurrence from the **Job Activity** pane. The job can be restarted at a later time.
Override	Override a job's dependencies, allowing it to run even though its predefined dependencies have not been satisfied.
Release/Resume	Release a job requiring operator release, and resume a job that has been stopped or held.

Table 3-12 Job Control Functions

Function	Description
Rerun	Rerun a job.
Set Status	Set a job's completion status.

Job Events Category

Table 3-13 Job Classes Functions

Function	Description
Add Job Event	Set up conditions to trigger job alert messages and/or recovery procedures (job events).
Edit Job Event	Edit the properties of a job event owned by you or your workgroup(s).
Delete Job Event	Allows a user to delete job events that the user created or are owned by a workgroup to which they belong.
View Job Event	Allows a user to view the specifics of all job events (messaging service and recovery procedure constructs) available.
Allow All Jobs	Enables/disables the **Apply this event to all jobs** check box in the Job Event definition. If you do not have this enabled in your security policy, you cannot apply a job event to all jobs.

Jobs Category

Table 3-14 Job Functions

Function	Description
Add Jobs	Create new job and job group definitions. You have full control over what, where, and when the job or group runs. You can also specify dependencies for your definitions.
Assign Job Events	Assign predefined job events to a job or job group from the **Job** or **Job Group** definition dialogs.
Edit Jobs	Edit jobs for yourself or for your workgroup(s). You have full control over what, where, and when the job or group runs. You can also specify dependencies for your definition.
Delete Jobs	Delete jobs belonging to you and your workgroup(s).
View Jobs	View all the properties of the jobs and groups that you and your workgroup(s) own.
Enable Jobs	Enable (activate) jobs and job groups. A job cannot run unless it is enabled.

Queues Category

Table 3-15 Queue Functions

Function	Description
Add Queue	Create job queues to tune the throughput and allocation of system resources.
Edit Queue	Edit job queues to tune the throughput and allocation of system resources.
	(Continued)
Delete Queue	Delete a job queue.

Table 3-15 Queue Functions

Function	Description
View Queue	View all queues and their properties.
Edit System Queue	Edit the system queue, including setting the overall limit of the number of jobs run on the network concurrently. With the **Edit System Queue** function, users can also edit all other queues.
Edit Native Priority	Edit the CPU scheduling priority for jobs in a queue. This function applies to Nice values in Unix and to job classes in SAP.

Resources Category

Table 3-16 Resources Functions

Function	Description
Add Resources	Create new resources.
Edit Resources	Edit resource definitions.
Delete Resources	Delete existing resource definitions.
View Resources	View all the properties of the resources that you and your workgroup(s) own.

Schedule Category

Table 3-17 Schedule Functions

Function	Description
Shutdown Scheduler	Stops the master service.
Create Schedule	Manually generate job occurrences for the next production schedule period.
Pause/Resume Schedule	Prevent all jobs in the production schedule from launching. Also allows you to resume the schedule if it is paused.
Refresh Schedule	Updates the production data.

Security Category

Table 3-18 Security Functions

Function	Description
Add Security Policy	Allows a user to create a set of Scheduler functions that can be assigned to a user.
Edit Security Policy	Allows a user to add and remove functions to/from a Scheduler functions set.
Delete Security Policy	Allows a user to delete a Scheduler function set.
View Security Policy	Allows a user to view the function set associated with a security policy.

System Events Category

Table 3-19 System Events Functions

Function	Description
Add System Event	Set up conditions to trigger actions based on events generated by the system (system events).
Edit System Event	Edit the properties of a system event that belongs to you or your workgroup(s).

(Continued)

Table 3-19 System Events Functions

Function	Description
Delete System Event	Delete system events that belong to you or your workgroup(s).
View System Event	View the specifics of all system events (messages, jobs, variable updates) available.

Users Category

Table 3-20 Users Functions

Function	Description
Add Users	Add a new user definition to the Scheduler database.
Edit Users	Edit all properties of a user definition except for Assign Security Policy, Assign Runtime Users and Assign Agents.
Delete Users	Delete any user from the Scheduler database.
View Users	View all user information.
Edit Personal Data	Update the personal data properties (**User Definition** dialog, **Other** tab) of your user definition.
Assign Security Policy	Specify the functions that will be available to another user.
Assign Runtime Users	Assign access to other user accounts for the purpose of running jobs.
Impersonate User	Operate Scheduler as another user. You assume all characteristics of that user, including their security policy.
Assign Agents	Designate the agent(s) on which a user is allowed to run jobs.

Workgroups Category

Table 3-21 Workgroups Functions

Function	Description
Add Workgroup	Can create a group of users to share data.
Edit Workgroup	Can redefine the users who belong to a workgroup.
Delete Workgroup	Can delete a workgroup, disabling the sharing of data between users.
View Workgroup	Can view workgroup definitions.

Variables Category

Table 3-22 Variables Functions

Function	Description
Add Variable	Create variable definitions.
Edit Variable	Edit variable definitions that belong to you and your workgroup(s).
Delete Variable	Delete user-defined variables that belong to you and your workgroup(s).
View Variable	View variables that belong to you and your workgroup(s).

Fault Monitor Category

Table 3-23 Fault Monitor Functions

Function	Description
Control Fault Monitor	Enables a user to use the control options in the context menu in the **Fault Monitor** pane.
View Fault Monitor	Enables a user to view the **Fault Monitor** pane

OracleApps Jobs Category

Table 3-24 OracleApps Jobs Functions

Function	Description
Add OracleApps Job	Create and add OracleApps jobs to the TES production schedule.
Edit OracleApps Job	Edit OracleApps job definitions.

Variable Events Category

Table 3-25 Variable Events Functions

Function	Description
Add Variable Events	Create and add variable events to the TES production schedule.
Edit Variable Events	Edit variable events that belong to you and your workgroup(s).
Delete Variable Events	Delete variable events that belong to you and your workgroup(s).
View Variable Events	View all the properties of the variable events that you and your workgroup(s) own.
Suspend Variable Events	Suspends the variable events that you and your workgroup(s) own.
Resume Variable Events	Resumes suspended variable events that you and your workgroup(s) own.

File Events Category

Table 3-26 File Events Functions

Function	Description
Add File Events	Create and add file events to the TES production schedule
Edit File Events	Edit file events.
Delete File Events	Delete file events that belong to you and your workgroup(s)
View File Events	View all the properties of the file events that you and your workgroup(s) own.
Suspend File Events	Suspends the file events that you and your workgroup(s) own.
Resume File Events	Resumes suspended file events that you and your workgroup(s) own.

Email Events Category

Table 3-27 Email Events Functions

Function	Description
Add Email Events	Create and add Email events to the TES production schedule
Edit Email Events	Edit Email events.
Delete Email Events	Delete Email events that belong to you and your workgroup(s)
View Email Events	View all the properties of the Email events that you and your workgroup(s) own.
Suspend Email Events	Suspends the Email events that you and your workgroup(s) own.
Resume Email Events	Resumes suspended Email events that you and your workgroup(s) own.

Oracle DB Events Category

Table 3-28 Oracle DB Events Functions

Function	Description
Add Oracle DB Events	Create and add Oracle DB events.
Edit Oracle DB Events	Edit Oracle DB events.
Delete Oracle DB Events	Can delete Oracle DB event definitions.
View Oracle DB Events	Can view Oracle DB event definitions.
Suspend Monitoring	Can suspend the operation of the Oracle DB monitor.
Resume Monitoring	Can resume the operation of the Oracle DB monitor.

Oracle DB Jobs Category

Table 3-29 Oracle DB Jobs Functions

Function	Description
Add Oracle DB Jobs	Create and add Oracle DB jobs to the TES production schedule.
Edit Oracle DB Jobs	Edit Oracle DB job definitions.

SAP Jobs Category

Table 3-30 SAP Jobs Functions

Function	Description
Add SAP Job	Create and add SAP jobs to the TES production schedule.
Edit SAP Job	Edit SAP job definitions.
Delete SAP Job	Delete SAP job definitions.
View SAP Job	View SAP job definitions.
View Job Log	View job's job log.
View Job Spool	View job's job spool.

SAP Variants Category

Table 3-31 SAP Variants Functions

Function	Description
Add/Edit Variants	Create and edit SAP variants.
Delete Variants	Can delete SAP variants.

SAP Process Chains

Table 3-32 SAP Process Chains Functions

Function	Description
Enable Planning View	Can enable planning view.

MSSql Events

Table 3-33 MSSql Events Functions

Function	Description
Add MSSql Events	Create and add MSSql events.
Edit MSSql Events	Can edit MSSql events.
	(Continued)
Delete MSSql Events	Can delete MSSql event definitions.
View MSSql Events	Can view MSSql event definitions.
Suspend Monitoring	Can suspend the operation of the MSSql monitor.
Resume Monitoring	Can resume the operation of the MSSql monitor.

MSSql Jobs

Table 3-34 MSSql Jobs Functions

Function	Description
Add MSSql Jobs	Create and add MSSql jobs to the TES production schedule.
Edit MSSql Jobs	Can edit MSSql job definitions.
Delete MSSql Jobs	Can delete MSSql job definitions.
View MSSql Jobs	Can view MSSql job definitions.

PeopleSoft Jobs Category

Table 3-35 PeopleSoft Functions

Function	Description
Add PeopleSoft Job	Create and add PeopleSoft jobs to the TES production schedule.
Edit PeopleSoft Job	Edit PeopleSoft job definitions.

Table 3-35 PeopleSoft Functions

Function	Description
Delete Workgroup	Delete a workgroup, disabling the sharing of data between users.
View Workgroup	View workgroup definitions.

PeopleTools Category

Table 3-36 PeopleTools Functions

Function	Description
Enable PeopleTools Access	Can access PeopleTools.

WebService Jobs Category

Table 3-37 WebService Jobs Functions

Function	Description
Add WebService Jobs	Create and add WebService jobs to the TES production schedule.
Edit WebService Jobs	Can edit WebService job definitions.
Delete WebService Jobs	Can delete WebService job definitions.
View WebService Jobs	Can view WebService job definitions.

Horizon Jobs Category

Table 3-38 Horizon Jobs Functions

Function	Description
Add Horizon Jobs	Create and add Horizon jobs to the TES production schedule.
Edit Horizon Jobs	Can edit Horizon job definitions.
Delete Horizon Jobs	Can delete Horizon job definitions.
View Horizon Jobs	Can view Horizon job definitions.

Default Security Policies and Their Associated Functions

The following shows which TES functions are associated with each default security policy, grouped by function category

:

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
Agent Lists category						
Add agent list	✓	✓	✓	—	—	—
Edit agent list	✓	✓	✓	—	—	—
Delete agent list	✓	✓	✓	—	—	—
View agent list	✓	✓	✓	✓	✓	✓
Alerts category						
View alert	✓	—	✓	✓	✓	✓
Acknowledge alert	✓	—		✓	—	—
						(Continued)
Close alert	✓	—	—	✓	—	—
Calendars category						
Add calendar	✓	—	✓	—	—	—
Edit calendar	✓	—	✓	—	—	—
Delete calendar	✓	—	✓	—	—	—
View calendar	✓	—	✓	✓	✓	✓
Configuration/Licensing category						
Edit configuration/license	✓	✓	—	—	—	—
View configuration/licensing	✓	✓	—	—	—	—
Connections category						
Add connection	✓	✓	—	—	—	—
Edit connection	✓	✓	✓	—	—	—
Delete connection	✓	✓	—	—	—	—
View connection	✓	✓	✓	✓	—	—
Edit machine name	✓	✓	✓	—	—	—
Edit agent job limit	✓	✓	✓	—	—	—
General category						
Add public data	✓	✓	✓	—	—	—
View logs	✓	✓	✓	✓		✓
View reports	✓	—	✓	✓	✓	✓
View history	✓	—	✓	✓	✓	—

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
View master status	✓	✓		✓	—	—
Move jobs to production	✓	—	—	—	—	—
Move own jobs to production	✓	—	—	—	—	—
Job Actions category						
Add job actions	✓	—	✓	—	—	—
Edit job actions	✓	—	✓	—	—	—
Delete job actions	✓	—	✓	—	—	—
						(Continued)
View event actions	✓	—	✓	✓	✓	—
Job Classes category						
Add job class	✓	—	✓	—	—	—
Edit job class	✓	—	✓	—	—	—
Delete job class	✓	—	✓	—	—	—
View job class	✓	—	✓	✓	✓	✓
Job Console (Activity) category						
View all	✓	—	✓	✓		✓
View own	✓	—	✓	✓	✓	✓
Edit all	✓	—	—	—	—	—
Edit own	✓	—	—	—	—	—
Control all	✓	—	✓	✓	—	—
Control own	✓	—	—	—	✓	—
Job Control category						
Ad hoc job control	✓	—	✓	✓	✓	—
Cancel/abort	—	—	✓	✓	✓	—
Hold/stop	✓	—	✓	✓	✓	—
Override	✓	—	✓	✓	—	—
Release/resume	✓	—	✓	✓	—	—
Rerun	✓	—	✓	✓	✓	—
Set status	✓	—	✓	✓	—	—
Job Events category						
Add job events	✓	—	✓	—	—	—

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
Edit job events	✓	—	✓	✓	—	—
Delete job events	✓	—	✓	—	—	—
View job events	✓	—	✓	✓	✓	✓
Allow all jobs	✓	—	✓	✓	—	—

(Continued)

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
Jobs category						
Add jobs	✓	—	✓	—	✓	—
Edit jobs	✓	—	✓	—	P	—
Delete jobs	✓	—	✓	—	—	—
View jobs	✓	—	✓	✓	✓	✓
Assign job events	✓	—	✓	✓	✓	—
Enable jobs	✓	—	—	—	—	—
Queues category						
Add queue	✓	✓	✓	—	—	—
Edit queue	✓	✓	✓	✓	—	—
Delete queue	✓	✓	✓	—	—	—
View queue	✓	✓	✓	✓	✓	✓
Edit system queue	✓	✓	✓	—	—	—
Edit native priority	✓	✓	✓	—	—	—
Resources category						
Add resources	✓	✓	✓	—	—	—
Edit resource	✓	✓	✓	✓	—	—
Delete resource	✓	✓	✓	—	—	—
View resource	✓	✓	✓	✓	✓	✓
Schedule category						
Create schedule	✓	—	✓	—	—	—
Pause/resume schedule	✓	—	✓	✓	—	—
Shutdown Scheduler	—	—	—	—	—	—
Security category						
Add security	✓	✓	—	—	—	—
Edit security	✓	✓	—	—	—	—
Delete security	✓	✓	—	—	—	—
View security	✓	✓	—	—	—	—

(Continued)

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
System Events category						
Add system event	✓	—	✓	—	—	—
Edit system event	✓	—	✓	✓	—	—
Delete system event	✓	—	✓	—	—	—
View system event	✓	—	✓	✓	✓	✓
Timezone category						
Add Timezone	—	—	—	—	—	—
Edit Timezone	—	—	—	—	—	—
Delete Timezone	—	—	—	—	—	—
View Timezone	—	—	—	—	—	—
User Administration category						
Add users	✓	✓	—	—	—	—
Edit users	✓	✓	—	—	—	—
Delete users	✓	✓	—	—	—	—
View users	✓	P	✓	✓	—	—
Edit personal data	✓	✓	✓	✓	✓	—
Assign security policy	✓	✓	—	—	—	—
Assign runtime users	✓	✓	✓	✓	—	—
Impersonate user	✓	✓	✓	—	—	—
Assign agents	✓	✓	—	—	—	—
Variables category						
Add variables	✓	✓	✓	—	—	—
Edit variables	✓	✓	✓	✓	—	—
Delete variables	✓	✓	✓	—	—	—
View variables	✓	✓	✓	✓	✓	—
Workgroups category						
Add workgroup	✓	✓	✓	—	✓	—
Edit workgroup	✓	✓	✓	—	✓	—

(Continued)

Delete workgroups	✓	✓	—	—	—	—
View workgroups	✓	✓	✓	✓	✓	—

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
Fault Monitor category						
Control FaultMon	—	—	—	—	—	—
View FaultMon	—	—	—	—	—	—
PeopleSoft Jobs category						
Add PeopleSoft Jobs	✓	✓	✓	—	—	—
Edit PeopleSoft Jobs	✓	✓	✓	✓	—	—
Delete PeopleSoft Jobs	✓	✓	—	—	—	—
View PeopleSoft Jobs	✓	✓	✓	✓	✓	✓
OracleApps Jobs category						
Add OracleApps Jobs	✓	✓	✓	—	—	—
Edit OracleApps Jobs	✓	✓	✓	✓	—	—
Delete OracleApps Jobs	✓	✓	✓	—	—	—
View OracleApps Jobs	✓	✓	✓	✓	✓	✓
Remote Jobs Jobs category						
Add Remote Jobs Jobs	✓	✓	✓	—	—	—
Edit Remote Jobs Jobs	✓	✓	✓	✓	—	—
Delete Remote Jobs Jobs	✓	✓	✓	—	—	—
View Remote Jobs Jobs	✓	✓	✓	✓	✓	✓
SSH Jobs category						
Add SSH Jobs	✓	✓	✓	—	—	—
Edit SSH Jobs	✓	✓	✓	✓	—	—
Delete SSH Jobs	✓	✓	✓	—	—	—

(Continued)

View SSH Jobs	✓	✓	✓	✓	✓	✓
JMS Jobs category						
Add JMS Jobs	✓	✓	✓	—	—	—
Edit JMS Jobs	✓	✓	✓	✓	—	—
Delete JMS Jobs	✓	✓	✓	—	—	—
View JMS Jobs	✓	✓	✓	✓	✓	✓
JMS Events category						
Add JMS events	✓	—	✓	—	—	—

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
Edit JMS events	✓	—	✓	✓	—	—
Delete JMS events	✓	—	✓	—	—	—
View JMS events	✓	—	✓	✓	✓	✓
Suspend Monitorings	✓	✓	—	—	—	—
Resume Monitorings	✓	✓	—	—	—	—
Variable Events category						
Add Variable Events	✓	✓	✓	—	—	—
Edit Variable Events	✓	✓	✓	✓	—	—
Delete Variable Events	✓	✓	✓	—	—	—
View Variable Events	✓	✓	✓	✓	✓	✓
Suspend Variable Events	✓	✓	—	—	—	—
Resume Variable Events	✓	✓	—	—	—	—
File Events category						
Add File Events	✓	✓	✓	—	—	—
Edit File Events	✓	✓	✓	✓	—	—
Delete File Events	✓	✓	✓	—	—	—
View File Events	✓	✓	✓	✓	✓	✓
Suspend Monitorings	✓	✓	—	—	—	—
Resume Monitorings	✓	✓	—	—	—	—

(Continued)

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
Email Events category						
Add Email Events	✓	✓	✓	✓	—	—
Edit Email Events	✓	✓	✓	✓	—	—
Delete Email Events	✓	✓	✓	✓	—	—
View Email Events	✓	✓	✓	✓	✓	✓
Suspend Email Events	✓	✓	—	—	—	—
Resume Email Events	✓	✓	—	—	—	—
Horizon Jobs category						
Add Horizon Jobs	✓	✓	✓	✓	—	—
Edit Horizon Jobs	✓	✓	✓	✓	—	—
Delete Horizon Jobs	✓	✓	✓	✓	—	—
View Horizon Jobs	✓	✓	✓	✓	✓	✓
MSSQL Events						
Add MSSql Events	✓	✓	✓	—	—	—
Edit MSSql Events	✓	✓	✓	✓	—	—
Delete MSSql Events	✓	✓	✓	—	—	—
View MSSql Events	✓	✓	✓	✓	✓	✓
Suspend Monitorings	✓	✓	—	—	—	—
Resume Monitorings	✓	✓	—	—	—	—
MSSql Jobs category						
Add MSSql Jobs	✓	✓	✓	✓	—	—
Edit MSSql Jobs	✓	✓	✓	✓	—	—
Delete MSSql Jobs	✓	✓	✓	✓	—	—
View MSSql Jobs	✓	✓	✓	✓	✓	✓
Oracle DB Events						
Add Oracle DB Events	✓	✓	✓	—	—	—
Edit Oracle DB Events	✓	✓	✓	✓	—	—
Delete Oracle DB Events	✓	✓	✓	—	—	—

(Continued)

View Oracle DB Events	✓	✓	✓	✓	✓	✓
Suspend Monitorings	✓	✓	—	—	—	—

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
Resume Monitorings	✓	✓				
Oracle DB Jobs						
Add Oracle DB Jobs	✓	✓	✓	✓		
Edit Oracle DB Jobs	✓	✓	✓	✓		
Delete Oracle DB Jobs	✓	✓	✓	✓		
View Oracle DB Jobs	✓	✓	✓	✓	✓	✓
PeopleSoft Jobs						
Add PeopleSoft Jobs	✓	✓	✓	✓		
Edit PeopleSoft Jobs	✓	✓	✓	✓		
Delete PeopleSoft Jobs	✓	✓	✓	✓		
View PeopleSoft Jobs	✓	✓	✓	✓	✓	✓
People Tools						
Enable People Tools Access	✓	✓	✓			
SAP Events						
Add SAP Events	✓	✓	✓			
Edit SAP Events	✓	✓	✓	✓		
Delete SAP Events	✓	✓	✓			
View SAP Events	✓	✓	✓	✓	✓	✓
Suspend Monitorings	✓	✓				
Resume Monitorings	✓	✓				
SAP Jobs						
Add SAP Jobs	✓	✓	✓			
Edit SAP Jobs	✓	✓	✓	✓		
Delete SAP Jobs	✓	✓	✓			
View SAP Jobs	✓	✓	✓	✓	✓	✓
View Job Log						

(Continued)

View Job Spool						
SAP Variants						
Add/Edit Variants	✓	✓	✓			
Delete Variants	✓	✓	✓			

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
SAP Process Chains						
Enable Planning View	✓	✓	✓			
WebService Jobs						
Add WebService Jobs	✓	✓	✓			
Edit WebService Jobs	✓	✓	✓	✓		
Delete WebService Jobs	✓	✓	✓			
View WebService Jobs	✓	✓	✓	✓	✓	✓
Agent Lists category						
Add agent list	✓	✓	✓			
Edit agent list	✓	✓	✓			
Delete agent list	✓	✓	✓			
View agent list	✓	✓	✓	✓	v	✓
Alerts category						
Acknowledge alert	✓			✓		
Close alert	✓			✓		
View alert	✓		✓	✓	✓	✓
Calendars category						
Add calendar	✓		✓			
Edit calendar	✓		✓			
Delete calendar	✓		✓			
View calendar	✓		✓	✓	✓	✓
Configuration/Licensing category						
Edit configuration/license	✓	✓				
View configuration/licensing	✓	✓				

(Continued)

Table 3-39 Default Security Policies and Associated Functions

Function	Scheduler-Admin	Administrator	Scheduler	Operator	User	Inquiry
Connections category						
Add connection	✓	✓				
Edit connection	✓	✓	✓			
Delete connection	✓	✓				
View connection	✓	✓	✓	✓		
Edit machine name	✓	✓	✓			
Edit agent job limit	✓	✓	✓			
General category						
Add public data	✓	✓	✓			
View logs	✓	✓	✓	✓		✓
View reports	✓		✓	✓	✓	✓
View history	✓		✓	✓	✓	
View master status	✓	✓		✓		
Move jobs to production						
Job Actions category						
Add job actions	✓		✓			
Edit job actions	✓		✓			
Delete job actions	✓		✓			
View event actions	✓		✓	✓	✓	
Job Classes category						
Add job class	✓		✓			
Edit job class	✓		✓			
Delete job class	✓		✓			
View job class	✓		✓	✓	✓	✓
Job Console (Activity) category						
View all	✓		✓	✓		✓
View own	✓		✓	✓	✓	✓
Edit all	✓					

Security Policies Pane Interface

From the **Navigator** pane, select **Administration>Security Policies** to view the **Security Policies** pane.

All existing security policy names are displayed. If security policies do not appear, you do not have the appropriate rights to view security policies.

Buttons

The **Security Policies** pane interface contains the following buttons:

- **Add Security Policy** – Displays the **Security Policy Definition** dialog to add a new security policy.
- **Edit Security Policy** – Displays the **Security Policy Definition** dialog to edit an existing security policy.
- **Delete Security Policy** – Removes the selected security policy definition from the TES database.
- **Refresh** – Updates the data in the current pane.
- **Print** – Displays the **Reports** pane to view and print your security policy definitions. For more information, see <Jumps>“Monitoring Production” on page 361.
- Note to the Writer: Unable to update these cross ref

Search Field

Enter text that you want to search for within the columns displayed into this field.

Note This field at the top right of the grids will only search text columns that are not grayed out and are string-based. See <Jumps>“Searchable Columns” on page 35.

Columns

The **Security Policies** pane interface contains the following columns:

- **Name** – The name of the security policy.
- **Description** – A description of the security policy. The **Description** field in the **Security Policy Definition** is optional, so there may not be any data in this column.
- **Modified** – The last time the security policy was modified.

Security Policies Preferences

Select **View>Preferences** from the main menu bar while viewing the **Security Policies** pane to display the **Security Policies Preferences** dialog.

From this dialog, you can select which columns are displayed in the **Security Policies** pane and in what order they appear.

- A checkmark to the left of a column title indicates that it will be displayed in the pane. No checkmark indicates that it will not be displayed.

- To rearrange the order in which the columns are displayed, select the column and click the up or down arrow.

Navigator Context Menu

When you right-click in the **Navigator** pane while viewing the **Security Policies** pane, the **Navigator** context menu displays.

This context menu contains the following options:

- **Add Security Policy** – Displays the **Security Policy Definition** to add a new security policy. Has the same function as the **Add Security Policy** button.
- **Preferences** – Displays the preferences for the **Security Policies** pane.
- **Print** – Displays the **Reports** pane to view and print your security policy definitions. Has the same function as the **Print** button on the toolbar. For more information, see <Jumps>“Monitoring Production” on page 361.
- **Export** – Saves the data in the current pane as an HTML file.
- **Refresh** – Updates the data in the current pane.
- Note to the Writer: Unable to update these cross ref

Security Policies Context Menu

When you right-click in the **Security Policies** pane, the **Security Policies** context menu displays.

This context menu contains the following options:

- **Add Security Policy** – Add a new security policy definition by displaying the **Security Policy Definition**.
- **Edit Security Policy** – Edit the selected security policy by displaying the **Security Policy Definition**.
- **Delete Security Policy** – Deletes the selected security policy.
- **Print Security Policies** – Displays the **Reports** pane to view and print your security policy definitions. For more information, see <Jumps>“Monitoring Production” on page 361.

Security Policy Definition Dialog

The **Security Policy Definition** displays when you edit or add a security policy from the **Security Policies** pane.

Common To All Tabs

Security Policy Name – The name of the security policy (up to 30 characters). Each security policy name must be unique.

Functions Tab This tab contains the following elements:

- **Category** – Functions are grouped into categories, as shown in the tables in “TES Functions” section on page 3-79.
  - No checkmark to the left of the category means that none of the functions in that category are assigned.

  - A gray checkmark to the left of the category means that some of the functions in that category are assigned.
  - A black checkmark to the left of the category means that all of the functions in that category are assigned.
- **Functions Assigned** – The list of functions assigned to the security policy.

  For more information about TES functions, see "TES Functions" section on page 3-79.

Checklist Context Menu

Double-clicking a function category displays a small checklist context menu in the **Functions Assigned** column. The checklist context menu displays all the functions that belong to that category. Clicking the **Browse** button to the far right of the category, next to the **Functions Assigned** column, will also display the checklist for that category. Click **Close** in the checklist to return to the **Functions** tab. A black checkmark to the left of a function signifies that the function has been selected. No checkmark to the left of a function signifies that the function has not been selected.

Functions Tab Context Menu

Right-clicking the **Functions** tab of the **Security Policy** definition displays the following context menu of options for granting and revoking basic functions in all categories simultaneously in the security policy:

Note The options in the Functions context menu to grant or revoke all of a type of function only apply to the basic functions. More advanced functions must be granted/revoked individually. For example, the **Grant All Edit** option grants the **Edit Queue** function but not the more advanced functions of **Edit System Queue** or **Edit Nice Queue Value**.

- **Grant All Functions** – Enables all functions in all categories, in effect, giving the user Superuser privileges.
- **Grant All Functions for Category** – Enables all functions in a selected category.
- **Grant All Add** – Enables each of the basic **Add** functions in each category.
- **Grant All Edit** – Enables each of the basic **Edit** functions in each category.
- **Grant All Delete** – Enables each of the basic **Delete** functions in each category.
- **Grant All View** – Enables each of the basic **View** functions in each category.
- **Revoke All Functions** – Cancels all functions in all categories.
- **Revoke All Functions for Category** – Cancels all functions in a selected category.
- **Revoke All Add** – Cancels each of the basic **Add** functions in each category.
- **Revoke All Edit** – Cancels each of the basic **Edit** functions in each category.
- **Revoke All Delete** – Cancels each of the basic **Delete** functions in each category.
- **Revoke All View** – Cancels each of the basic **View** functions in each category.

Description Tab

Description – Any user comments regarding the security policy, up to 255 characters.

Security Policy Procedures

Adding a Security Policy

Though each user must have a security policy, not all security policies need to be assigned to users. It is recommended that the administrator assign functions to a security policy on a need-to-use basis. New user definitions are assigned the **Operator** security policy by default.

To add a security policy:

Step 1 From the **Navigator** pane, select **Administration>Security Policies** to display the **Security Policies** pane.

All existing security policy names display. If security policies do not appear, you do not have the appropriate rights to view security policies.

Step 2 Click the **Add** button or right-click and select **Add Security Policy** from the context menu to display the **Security Policy Definition** dialog.

Step 3 In the **Security Policy Name** field, type the name of the security policy.

Step 4 The name must be unique and the length must not exceed 30 characters.

Step 5 Click the **Functions** tab and select the functions to assign to the security policy.

Step 6 For more information about TES functions, see "TES Functions" section on page 3-79.

Step 7 Click the **Description** tab and type a description for the security policy, up to 255 characters. (optional)

Step 8 Click **OK** to close the security policy.

Step 9 The security policy is added to the TES database. The security policy can now be assigned to users.

Assigning Functions to a Security Policy

To assign a function:

Step 1 From the **Navigator** pane, select **Administration>Security Policies** to display the **Security Policies** pane.

All existing security policy names display. If security policies do not appear, you do not have the appropriate rights to view security policies.

Step 2 Double-click the security policy, or select the security policy record and click the **Edit** button or right-click the security policy and select **Edit Security Policy** from the context menu to display the **Security Policy Definition** dialog.

Step 3 All function categories appear in the **Category** column on the **Functions** tab.

Step 4 Double-click a category to display a drop-down list of available functions.

Step 5 Click the individual check box for each function to add or remove the function or right-click a category and select the **Grant All Functions** option from the context menu to select all functions of a category. (Conversely, select the **Revoke All Functions** option to remove the functions for a category.)

Step 6 Click **Close** in the checklist context to return to the **Functions** tab.

Deleting a Security Policy

Note You cannot delete a security policy that is being used by any user. You must assign a different security policy to each user using that security policy before you can delete it.

To delete a security policy:

Step 1 From the **Navigator** pane, select **Administration>Security Policies** to display the **Security Policies** pane.

All existing security policy names display. If security policies do not appear, you do not have the appropriate rights to view security policies.

Step 2 Select the security policy you want to delete.

Step 3 Click the **Delete** button on the TES toolbar.

Step 4 Click **OK** in the **Delete Confirmation** dialog.

Editing a Security Policy

With appropriate security rights, you can change functions available to a user by editing the user's security policy.

To edit a security policy:

Step 1 From the **Navigator** pane, select **Administration>Security Policies** to display the **Security Policies** pane.

All existing security policy names display. If security policies do not appear, you do not have the appropriate rights to view security policies.

Step 2 Double-click the security policy to edit or select the security policy and click the **Edit** button or right-click the security policy and select **Edit Security Policy** from the context menu.

Step 3 The **Security Policy Definition** dialog displays.

Step 4 You can change the name, description, and set of functions available to the user who has the security policy.

Step 5 To change the functions assigned, click the **Functions** tab and add or remove functions.

Step 6 For information about how to assign functions, see "Assigning Functions to a Security Policy" section on page 3-108.