User Administration Overview

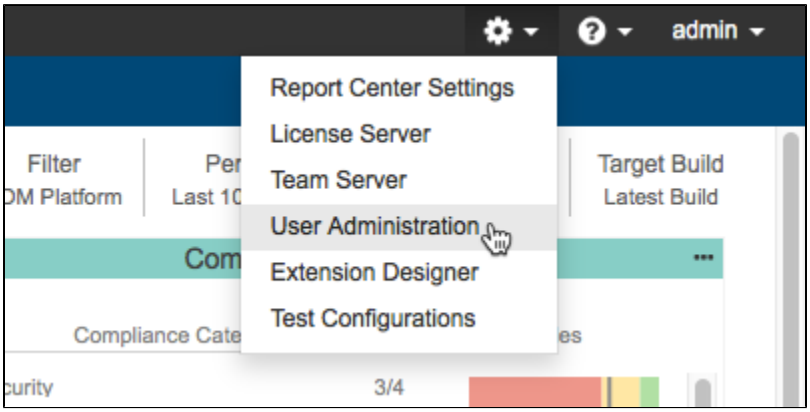
In this section:

About User Administration

Users with administrator privileges can access the user administration page, which is an interface for performing the following tasks:

- Adding or removing users from the database
- Defining user groups
- Granting and managing user and user group permissions
- Connecting DTP to your organization's user directories (see Configuring LDAP)

Choose **User Administration** from the settings drop-down menu to open the User Administration page:



There are two basic steps for managing users in DTP:

1. **Adding users to the database**. You can add users manually or sync DTP with your LDAP system, which imports users from your company directory into the database.
2. **Configuring permission and groups**. You can specify custom permissions for each user or add them to groups, which enables you to define a set of permissions once and add users accordingly.

Default Admin User

The user appointed to manage DTP should have administrative permissions assigned at the beginning of the security configuration. Those permissions include the following:

- Basic permissions (`pstsec_basicAccess:true`): If defined and set, it provides authorized access to the security module. This permission setting allows the administrator to edit defined users and permission groups.
- Administration permissions (`pstsec_administration:true`): If defined and set, it enables the administrator editing privileges to modify Users section.

The administrative (admin) user already exists in the database. For security reasons, we recommend assigning administrative permissions to the selected user with a unique password.

Terminology

The following table defines user-related terminology:

Permission	Permissions refer to the type of access a user has to a specific functionality. The permission format includes the applicable tool, name of the permission type, and permission value (`tool:name:value`).
	
	For example, the following permission grants access to Report Center data for a project called 'Core':
	
	`grs:project:Core`
	
	You can also user regular expressions to grant access based on project name patterns. For example, you could granting access to previous or future project versions:
	
	`grs:project:Core \d\.\d`
	
	The permission in the example above grants access to projects 'Core 1.0', 'Core 1.1', and so on.
	
	Permission applies to both Permission group and User.

Native Permissions	Permissions granted to a permission group.
Inherited Permissions	Permissions inherited from a parent permission group.
Permission Group	Set of permissions. Permission groups can have multiple native permissions. Additionally, each permission group can have multiple parent permission groups. It is possible to enable/disable both Native and Inherited Permission in permission groups, which is useful when you build an extended hierarchy but only need specific permissions from inherited ones.
User	DTP user. Each user can have multiple of permissions (Native Permissions) and can be a member of multiple permission groups. The Inherited Permissions for a user are grouped and reflect the permission groups hierarchies. Any permission can be disabled /enabled based on specific needs. Permissions inherited by a user from different permission groups are separated but linked with the individual ones.
Perspective	Set of Report Center reports and functionalities that are available to users

Permissions

The following tables describe permissions available in DTP.

PST Permissions

PST permissions (Parasoft permissions) provide basic access to the core DTP system.

Permission Name	Value	Description
basicAccess	true false	Required to login, but additional permissions are necessary to specify what DTP features the user can access.
administration	true false	Grants access to the DTP Control Center so that the user can deploy and manage DTP applications.

PSTSEC Permissions

PSTSEC permissions (Parasoft security) provide access to user and user group management functionality.

Permission Name	Possible Values	Description
basicAccess	true false	Required to login to the DTP Security application (User Administration component). Provides ability to modify one's own personal data, but no one else's.
administration	true false	Grants right to edit and modify user and permission groups data.

GRS Permissions

GRS permissions (group reporting system) provide access to Report Center data, dashboards, source code, etc.

Permission Name	Possible Values	Description
basicAccess	true false	Required to login to Report Center, but additional permissions are necessary to specify which features the user can access.
administration	true false	Grants access to Report Center administration pages
project	[project name] regex pattern	Grants access to the data associated with a specific project. You can use a regular expression to grant access to related projects. For example, if `grs:project:Core` provides access to a project called Core, you can use the regular expression `grs:project:Core \d\.\d` to provide access to Core 1.0, Core 1.1, etc. projects.
prioritizeAll	[project name] regex pattern	Enables the user to set the priority of violations associated with the project. Team default permission: Leader (leader inherits permissions from member)
prioritizeOwner	[project name] regex pattern	Enables the user to set the priority of violations assigned to the user.
viewSourceCode	[project name] regex pattern	Enables the ability to view source code associated with the project.Team default permission: Member.
testSessionStatusChange	[status value to status value] regex pattern	Deprecated since 5.4 (related to Project Center).
reqStatusChange	[status value to status value] regex pattern	Deprecated since 5.4 (related to Project Center).
defectStatusChange	[status value to status value] regex pattern	Deprecated since 5.4 (related to Project Center).
testStatusChange	[status value to status value] regex pattern	Deprecated since 5.4 (related to Project Center).
scenarioDeleteRestore	[status value to status value] regex pattern	Deprecated since 5.4 (related to Project Center).

scenarioStatusChange	[status value to status value] regex pattern	Deprecated since 5.4 (related to Project Center).

License Server Permissions

License Server permissions provide access to License Server functionality (see Configuring License Server). License Server is available as an integrated feature in DTP or as a standalone application.

Permission Name	Possible Values	Description
basicAccess	true false	Grants access to view License Server configuration pages.
administration	true false	Grants access to License Server administration pages to manage licenses (add, remove, reserved, and so on).

TCM Permissions

TCM permissions (team center manager) provides access to Team Server functionality (see Configuring Team Server).

Permission Name	Possible Values	Description
basicAccess	true false	Grants access to view Team Server configurations.
administration	true false	Grants access to Team Server administration pages to manage stored data, such as grant/limit access to Team Server data, created sandboxes, and load test configuration.

EM Permissions

EM permissions (Environment Manager) provides access to Continuous Testing Platform and/or Environment Manager (legacy).

Permission Name	Possible Values	Description
role	administration	Grants access to all Environment Manager activities: testing privileges, provisioning environments, defining systems and environments, controlling access permissions, and test data management. See the Environment Manager User Guide for additional information.
role	system	Grants the ability to provision environments and to create and execute test jobs in Environment Manager. Appropriate permissions to the resources is required for both actions. This role also grants the ability to execute all repository actions on test data. See the Environment Manager User Guide for additional information.
role	provision	Grants the ability to provision environments for sources the user has access to in Environment Manager. This role also grants read-only access to test data. See the Environment Manager User Guide for additional information.

Built-in User Groups

To ease user and group configuration, the DTP provides a set of built-in groups that contain common permissions. We recommend using them as parents when you create your own groups.

Built-in groups cannot be edited

You can create and manage custom groups (see Creating and Managing Groups), but the built-in groups cannot be changed.

PST Basic Access

This group defines basic permissions. Each newly-created user is automatically assigned as a member of this group. The membership of this group allows users to login to Report Center, but it does not allow access to the administration controls within these modules. Additional permissions are required to perform any actions.

PST Basic Access group preview

General

Name PST Basic Access

Description Group defines basic permissions for PST

Type Built in group

Permissions

Native

Tool	Name	Value
grs	basicAccess	true
ls	basicAccess	true
pst	basicAccess	true
pstsec	basicAccess	true
tcm	basicAccess	true

PST Administration

This group defines administration permissions. Members of this group are granted administration permissions for applications within DTP (Report Center, Team Server, License Server, and User Administration) and can manage data available through administration pages.

PST Administration group preview

General

Name PST Administration

Description Group defines admin permissions for PST

Type Built in group

Permissions

Native

Tool	Name	Value
grs	administration	true
ls	administration	true
pst	administration	true
pstsec	administration	true
tcm	administration	true

Inherited

	Tool	Name	Value
☑	grs	basicAccess	true
☑	ls	basicAccess	true
☑	pst	basicAccess	true
☑	pstsec	basicAccess	true
☑	tcm	basicAccess	true

GRS Basic Permissions

This group defines basic permissions for Report Center. Members of this group can view specific legacy Report Center reports associated with the projects he or she is assigned to.

GRS Basic Permissions group preview

General

Name GRS Basic Permissions

Description Group defines basic permissions for GRS

Type Built in group

Permissions

Native

Tool	Name	Value
grs	perspective	Basic
grs	perspective	QA

GRS Extended Permissions

This group defines extended permissions for Report Center. Members of this group can view specific legacy Report Center reports associated with the projects he or she is assigned to.

GRS Extended Permissions group preview

General

Name GRS Extended Permissions

Description Group defines extended permissions for GRS

Type Built in group

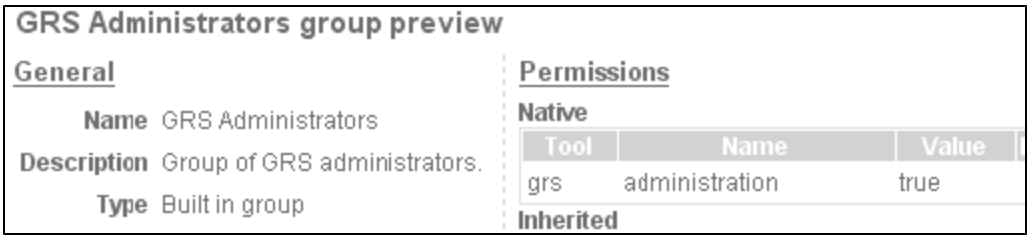
Permissions

Native

Tool	Name	Value
grs	perspective	Efficiency
grs	perspective	Management

GRS Administrators

This group defines administration permission for Report Center. Members of this group can access administration pages for edits, modifications, and management.



GRS Administrators group preview

General

Name GRS Administrators

Description Group of GRS administrators.

Type Built in group

Permissions

Native

Tool	Name	Value
grs	administration	true

Inherited