uniformance

PHD Security

Lesson Objective

Objective

Configure PHD security.

Topics

- System Administration Functions
- Public Vs. Private Security
- Role-Based Security
- Data Administration Main Menu
- Security Administration Forms
  - Users
  - Roles
  - Role Permissions
  - Integrated NT Security
  - Menu Access
  - Change Passwords
- Commit Permissions
- PHD Security Configuration Form
- Tag Configuration Rules
- Security Administration (R150 and later)
- PHDMAN Update Users and Update Tag Commands
- PHD Management Security
- Proxy Logins
- Documentation Summary
- Hands-on Exercises

References

- *PHD System Manual*
- *TPI Application User Guide*
- *Security Administration User Guide*

System Administration Functions

The PHD administrator performs system administration functions from menus and forms not normally available to application users.

Administration functions include:

A. Install Client Application

B. Database Attachment (Attach Tables)

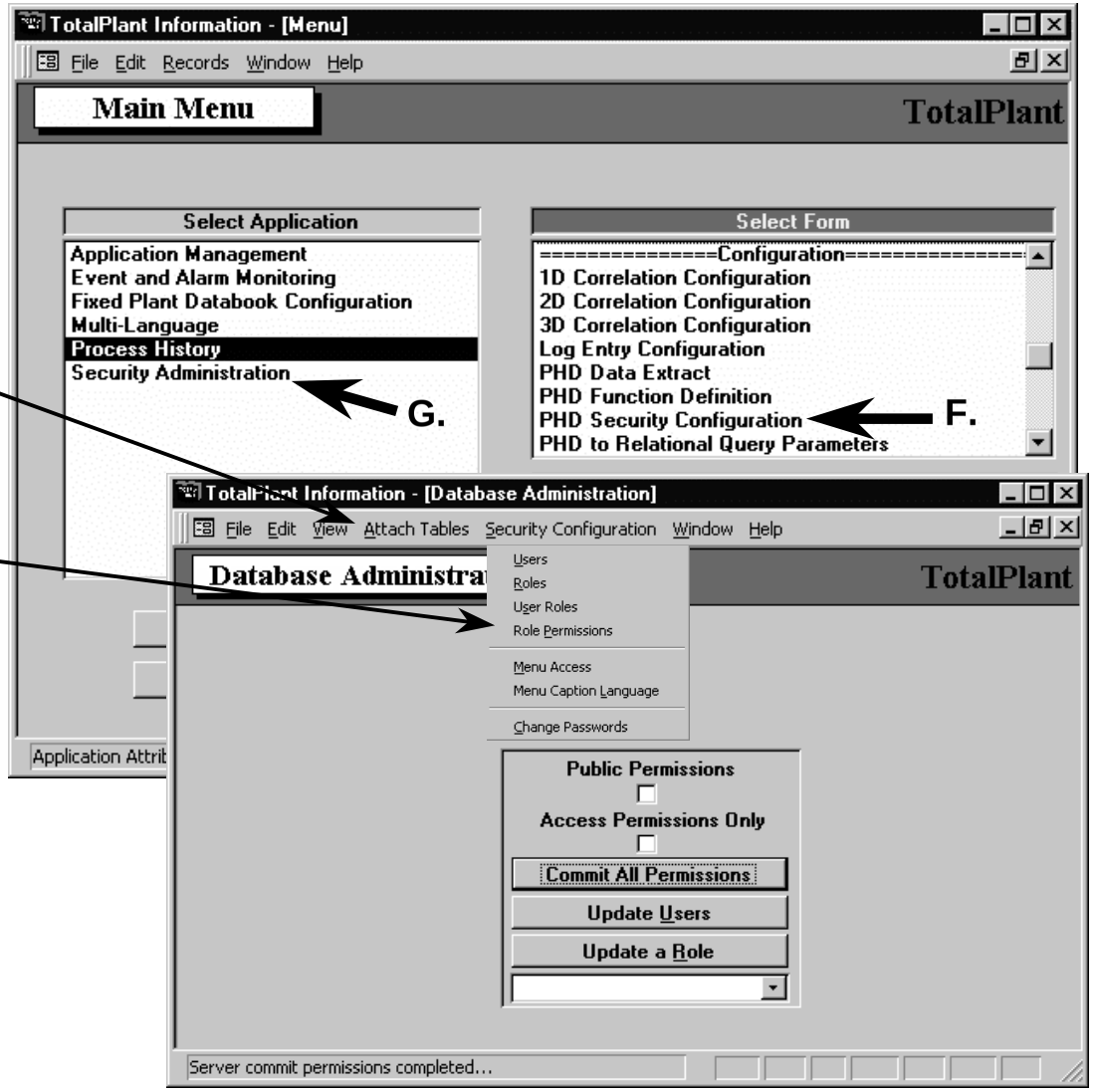
C. Role/Function Definition

D. User Enrollment

E. User Password Administration

F. Application Security (includes PHD Security Configuration form)

G. For R150 and later, you can give selected security administration rights to specific users. Those users would perform their administration through the Security Administration application.



Public Vs. Private Security

- When PHD is first installed, it has public security allowing all users full access to all tags, except those tags that have security roles assigned.
- If a site wants tag security, set up some general tag security, then disable *public* security.

  To enable private security, you must disable public security by setting the following system parameters to zero (0) through PHDMAN. Also, place the commands in the `phdparams.cmd` file for future startups.

```
PHDMAN SET TAG_PUBLICREAD 0
PHDMAN SET TAG_PUBLICWRITE 0
```

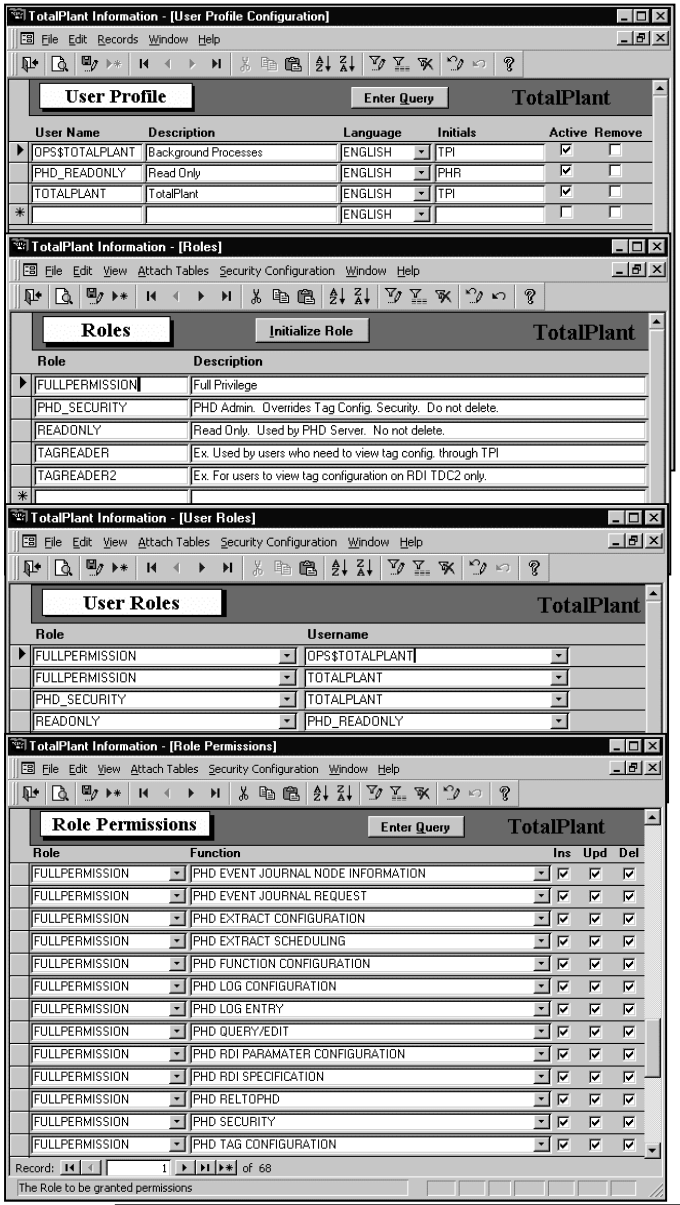
0 = public disabled, private enabled
1 = public enabled, private disabled
default values = 1 (public enabled)

With private security enabled, access to tags must be provided by entries in the PHD Security Configuration form for each User Role that is to have tag access.

With public security enabled, once an entry for a tag is made in the PHD Security Configuration form , then access to tags is no longer public, and each Role requiring access to tags must be configured to have the required access.

Refer to *PHD System Manual*, Tag Security and User Definition

Role-Based Security



Security Roles (Examples)

User Names (User Profile)

Doug
Mark
Tony

Role Names

FullPermission
PHD_Security
ReadOnly
Role A

User Roles

FullPermission: Doug
PHD_Security: Doug
ReadOnly: Mark, Tony
Role A: Tony

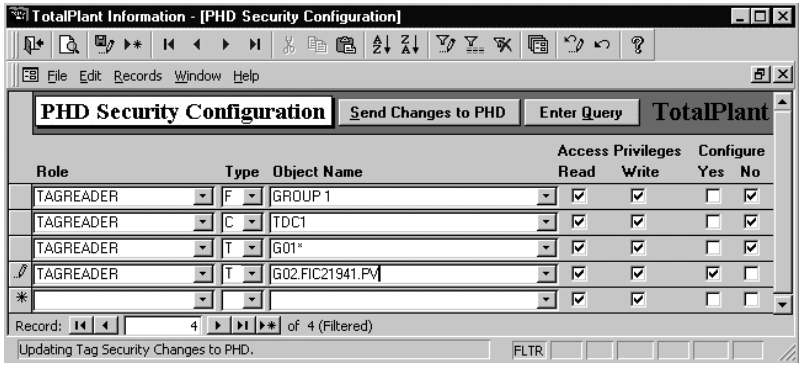
Role Permissions

FullPermission: All Functions, View, Insert, Update, Delete
PHD_Security: All Functions, View, Insert, Update, Delete
ReadOnly: All Functions, View Only
Role A: Virtual Tag Configuration, Insert, Update, Delete
PHD Function Definition, Insert, Update, Delete

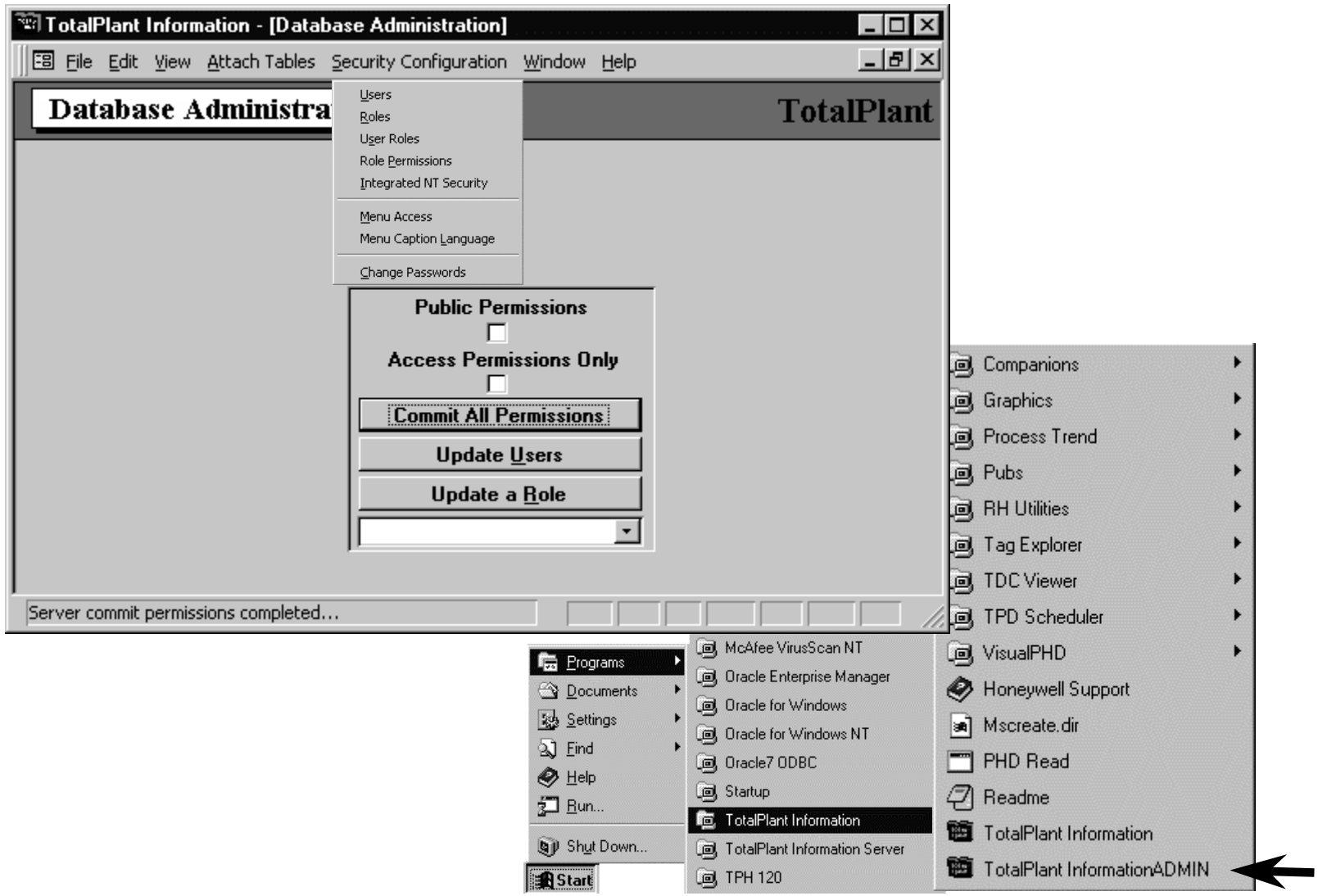
Tag Security

With private security, entries in the PHD Security Configuration form are required for roles/users to have access to any tags.

PHD Security Configuration



Database Administration Main Menu

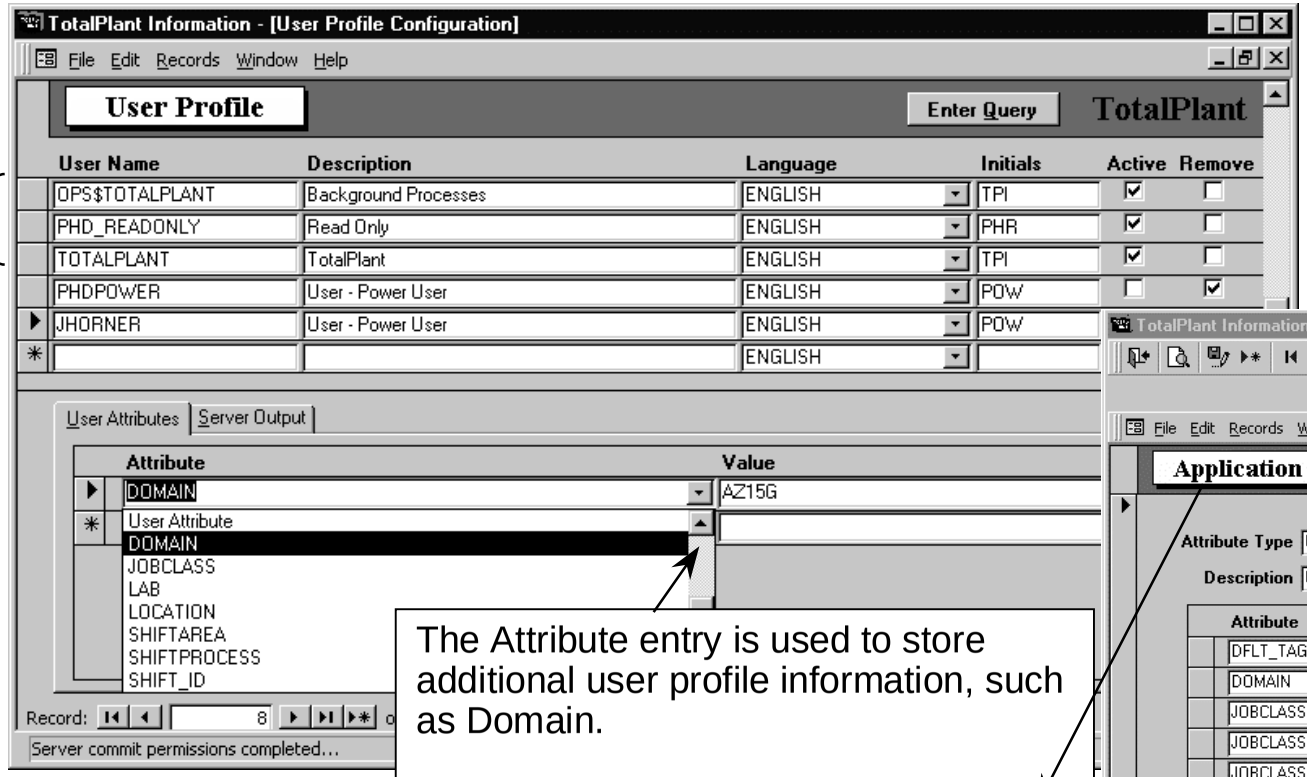


Reference: *TPI Application User Guide*

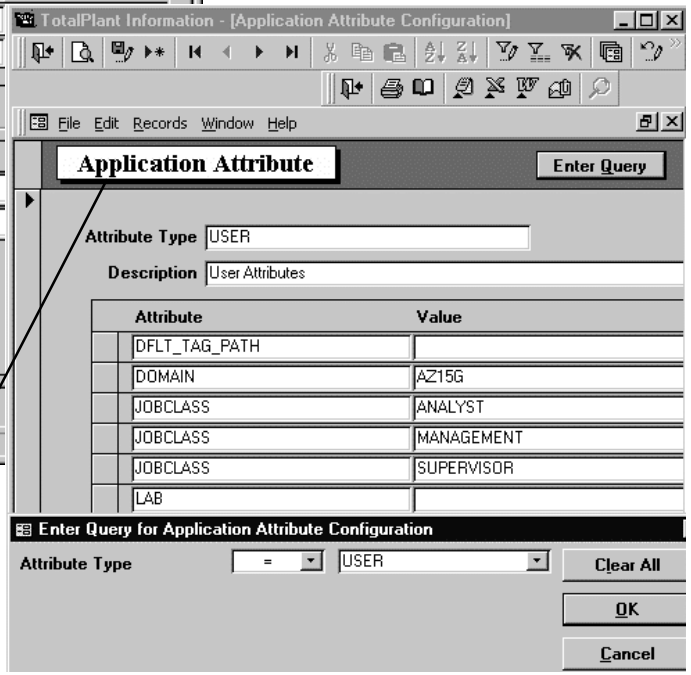
User Profile Form

Use this form to add users; then assign each user to one or more roles on the User Roles form.

Usernames included with PHD product.



Once a user is added through this form, the user name cannot be deleted.



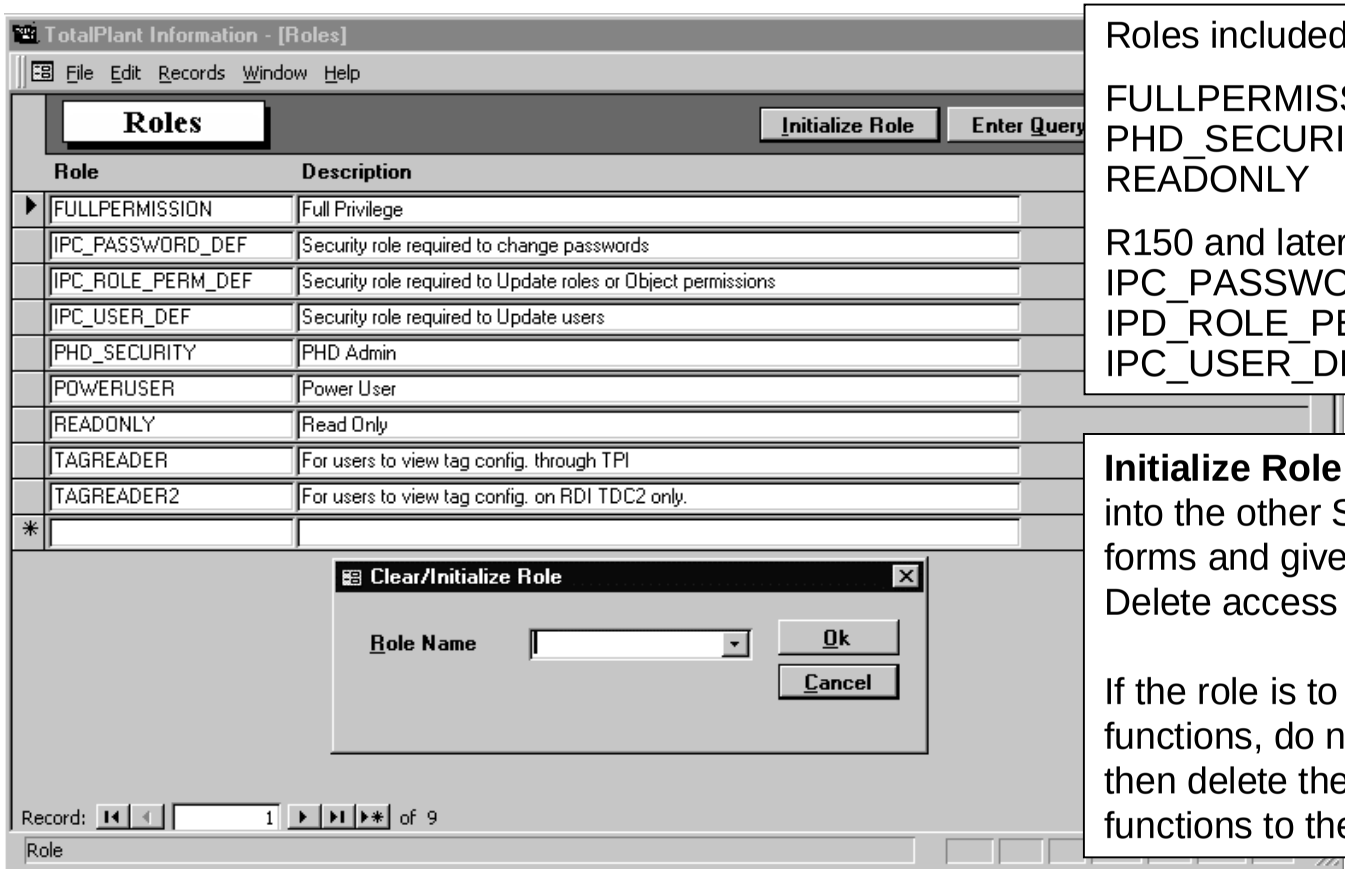
The Attribute entry is used to store additional user profile information, such as Domain.

The Attribute pull down list is built through the USER Attribute Type in the Application Attribute Configuration form (located in the Fixed Plant Databook).

Roles Form

The first step in configuring the security system is to define the role name

Example:
We want to define a role that can view Tag Configuration, but cannot change tag configuration. On the Roles form, we will add a role named “Tag Reader”. For this example, we will not initialize the role.



Roles included with PHD product:

FULLPERMISSION
PHD_SECURITY
READONLY

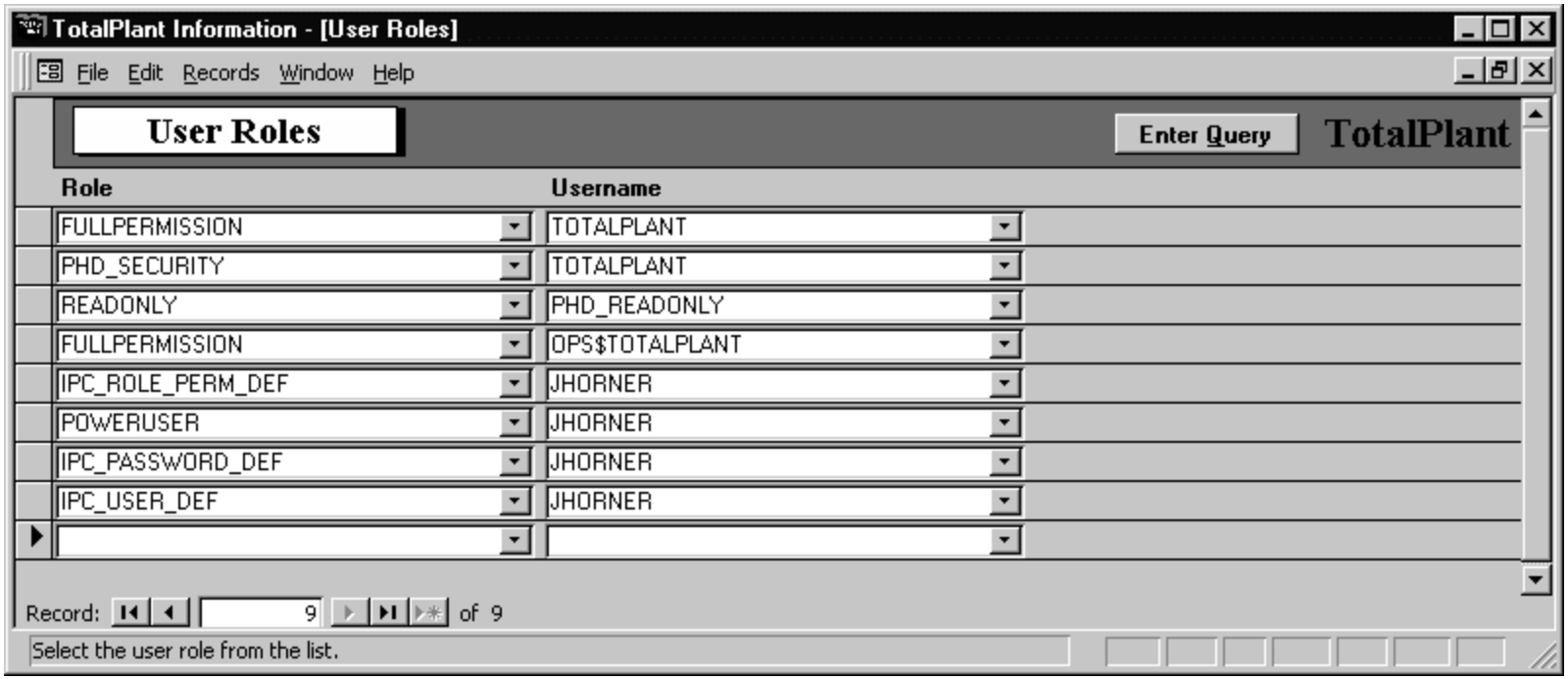
R150 and later:
IPC_PASSWORD_DEF
IPD_ROLE_PERM_DEF
IPC_USER_DEF

Initialize Role - Builds the new Role into the other Security Configuration forms and gives it Update, Insert, and Delete access to *all* the PHD functions.

If the role is to access only a few functions, do not 'Initialize Role' and then delete the exceptions; instead, add functions to the role one at a time.

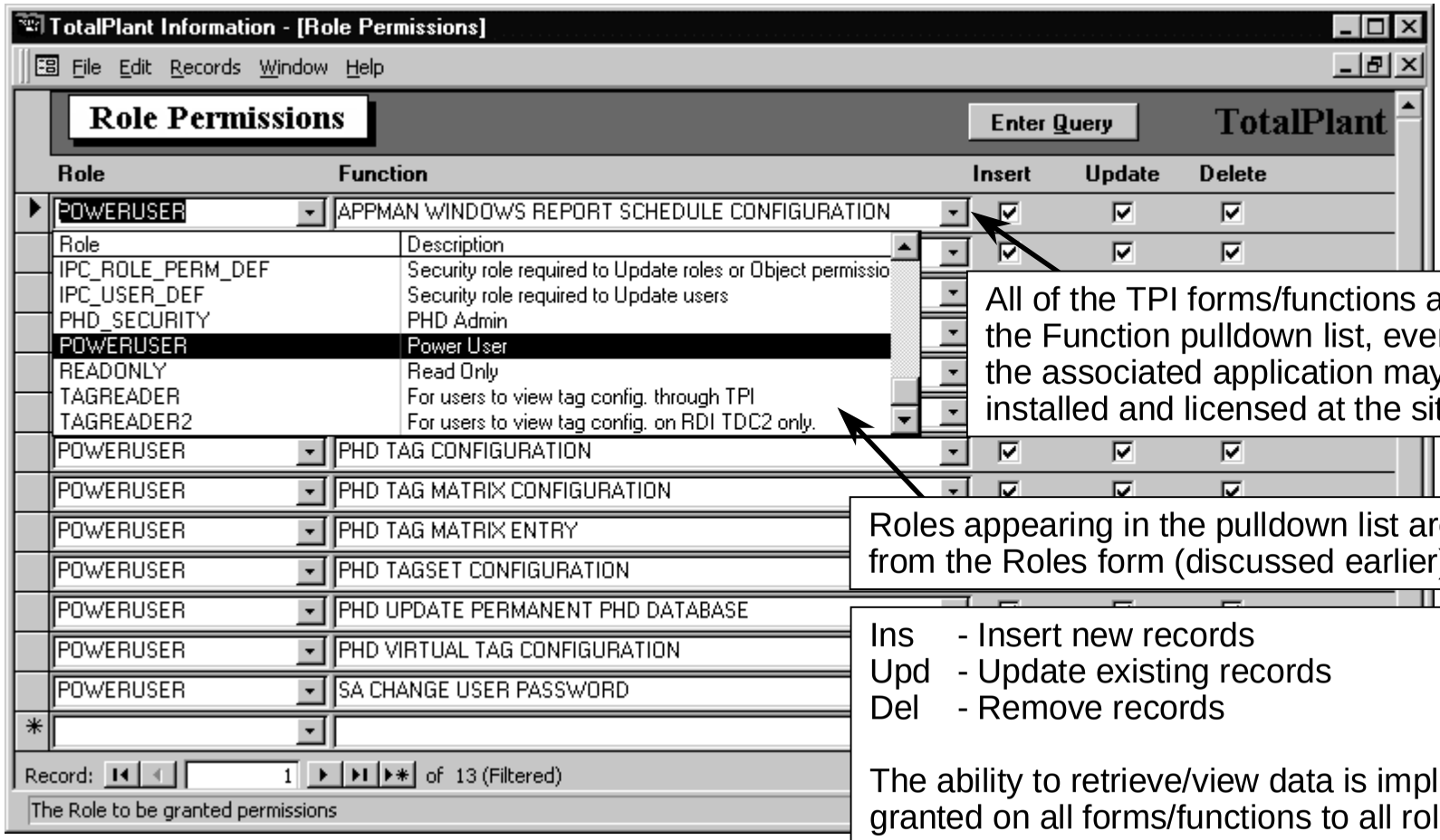
User Roles Form

This form is used to assign users to one or more roles.



Role Permissions Form

The Role Permissions form defines the data manipulation functions that each role can perform on each form in each application.



All of the TPI forms/functions appear in the Function pulldown list, even though the associated application may not be installed and licensed at the site.

Roles appearing in the pulldown list are defined from the Roles form (discussed earlier).

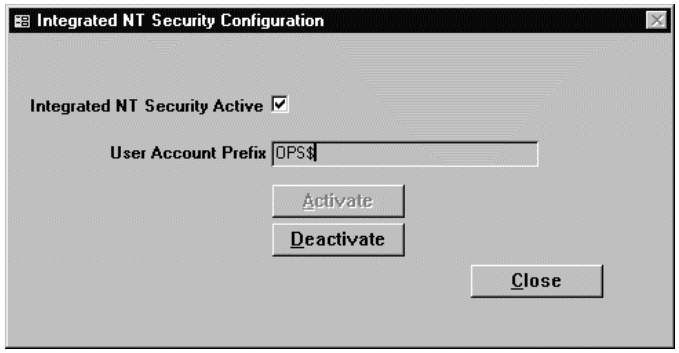
Ins - Insert new records
Upd - Update existing records
Del - Remove records

The ability to retrieve/view data is implicitly granted on all forms/functions to all roles.

You can prevent users from viewing data through the Menu Access configuration.

Integrated NT Security (R150 and later)

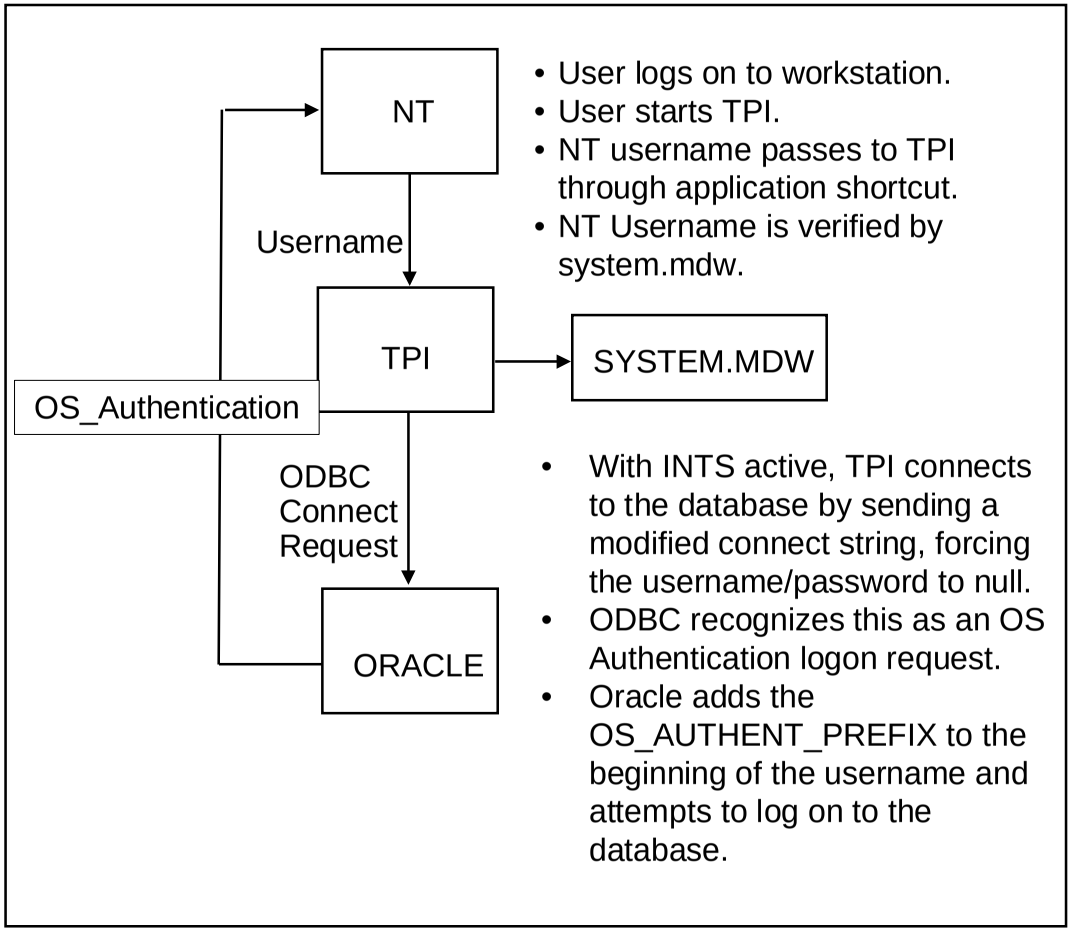
Integrated NT Security (INTS) enables logging into the Oracle database without a username and password. The NT username (used to log on to NT) with the account prefix is passed to Oracle.



The following areas are directly affected by INTS:

- ODBC
- TPI
- TPI Admin
- PHD
- Background Processes

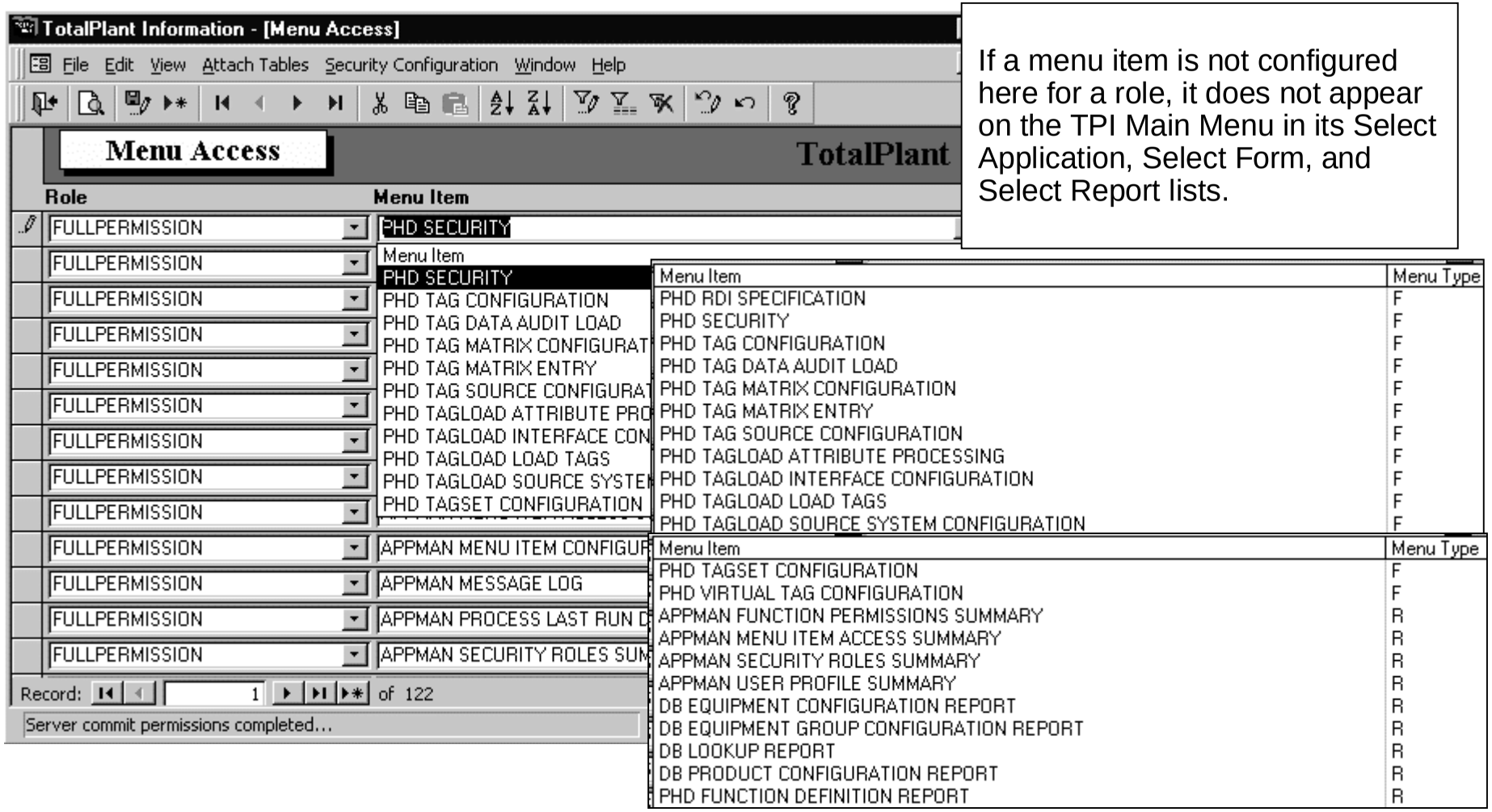
The impact of INTS is widespread and must be fully understood to minimize implementation problems.



The INTS lab exercise following of this training module fully describes how to implement INTS. The Uniformance R150 Software Change Notice provides this information also.

Menu Access

Menu Access controls what forms and reports are available for selection from the TPI Main Menu by a particular role.

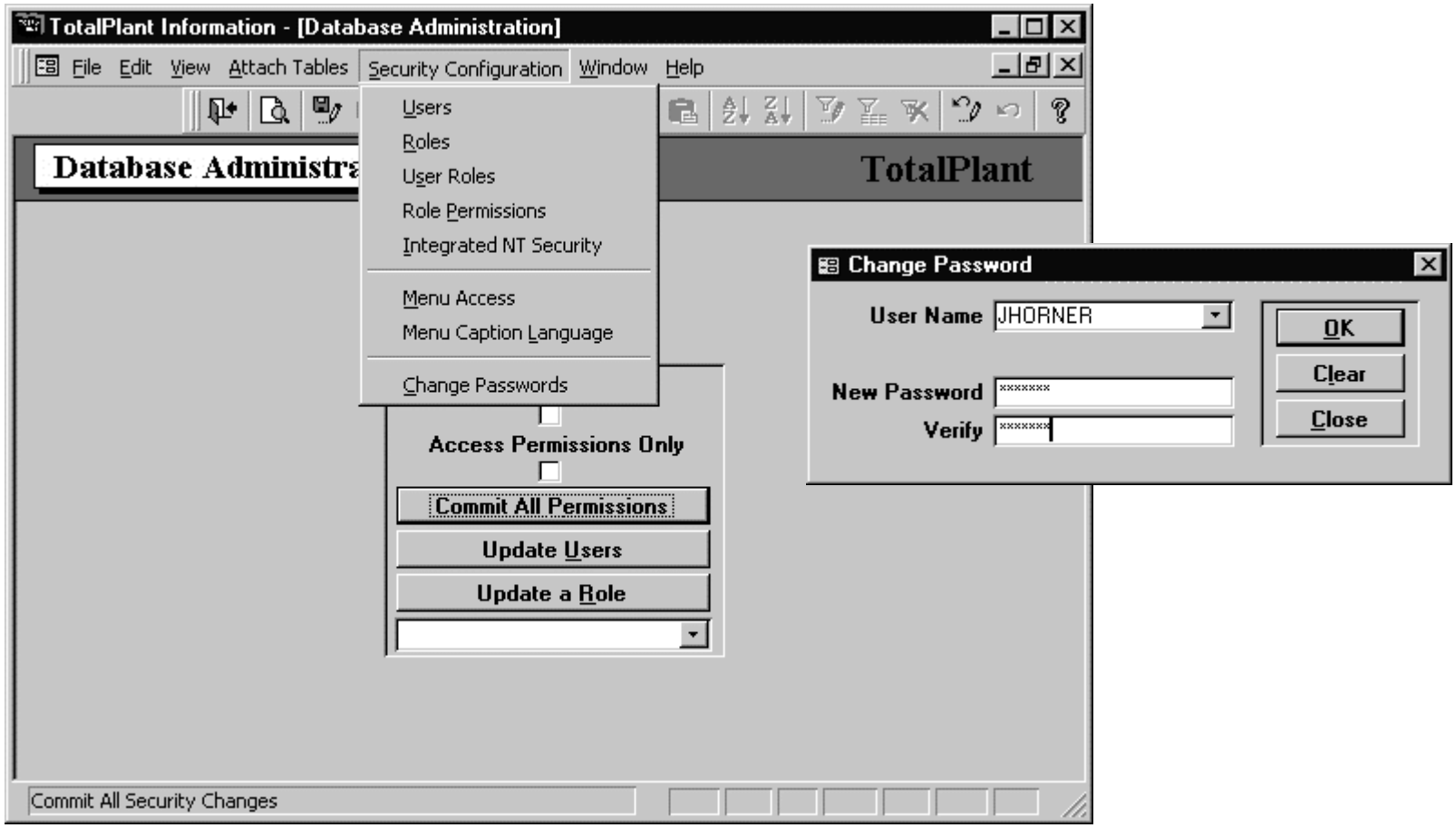


If a menu item is not configured here for a role, it does not appear on the TPI Main Menu in its Select Application, Select Form, and Select Report lists.

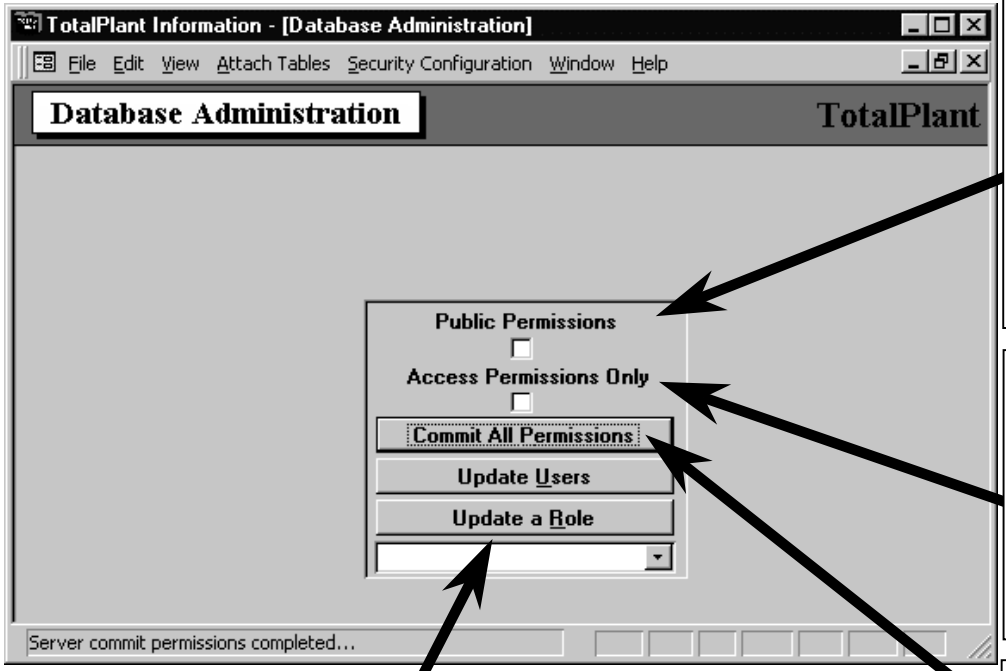
Change Passwords

Use the Change Password dialog to alter passwords for user accounts.
Until the Commit All Permissions button is selected, users are not available to have their passwords altered.

Do not use the TPI Change Password dialog to change passwords if Integrated NT Security (INTS) is active.



Commit Permissions



Public Permissions
Grants all users public permissions (insert, update, delete) on the TPI tables and views in Oracle. It does not affect or grant full access to TPI forms and reports as defined in the Menu Access form.

Select this option only after consulting Honeywell.

Access Permissions Only
Applies security to the access components (all forms, queries, and table attachments contained within the IPAPP.MDE file). Select this only if you are preparing a new ipapp.mde and you do not wish to change the permissions in Oracle.

Commit All Permissions
Updates all roles, users, and permissions.

Update Users
Users are added (or removed) and assigned to roles. *Role permissions are not updated*.
New roles are created and assigned to users. You can add new users and assign them to existing roles while other users are using the system.

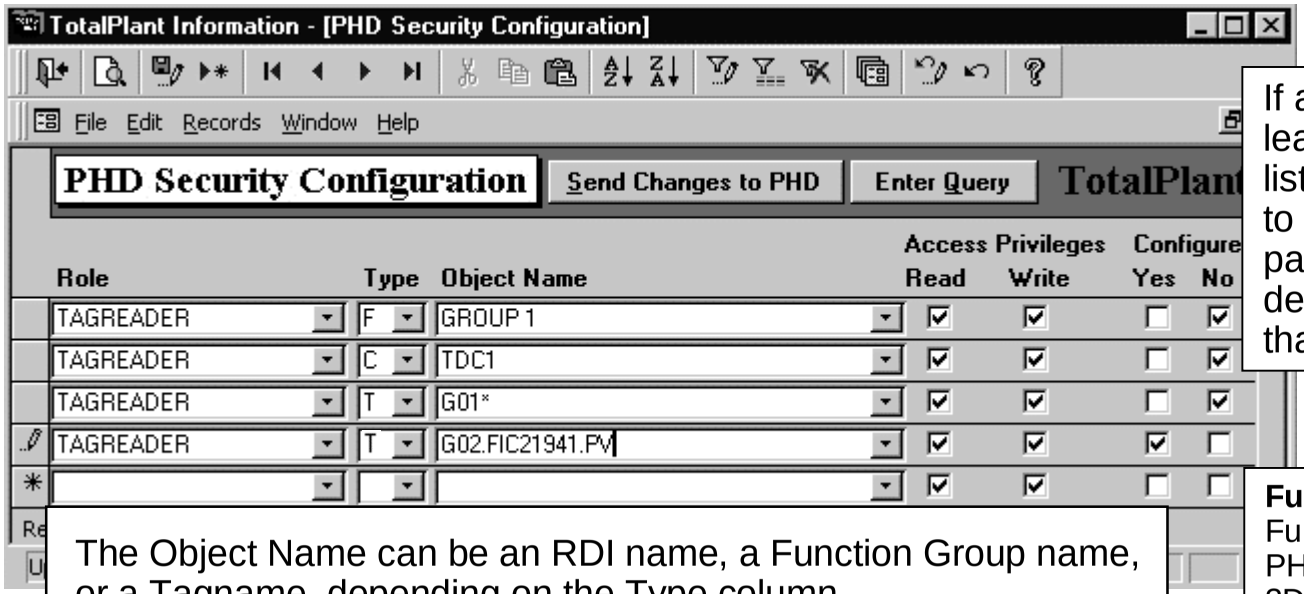
Update a Role
Updates all permissions for a selected role. Only users with the selected role are affected. Update a Role takes considerably more system time than Update Users.

PHD Security Configuration Form

If a site wants private security, the next step is to determine *how* the site wants to manage tags.

Assignment of tag security roles can be done on a tagname basis, by RDI, and on a PHD function group basis.

- **Function Security** - Username A in role A has access to function group A
- **Collector (RDI) Security** - Username A in role A has access to tags on collector A
- **Individual Tag Security** - Username A in role A has access to specified tag(s)



If a user is not a member of at least one role matching the list of required roles assigned to read, write, or configure a particular tag's data, PHD will deny the attempted access to that tag.

The Object Name can be an RDI name, a Function Group name, or a Tagname, depending on the Type column.

Tag Names can be wildcarded:
- underscore (_) for single character wildcard
- asterisk (*) for multiple character wildcard

Function Groups
Function Groups are groupings of PHD Function Definitions and 1, 2, 3D Correlation Table Functions. The functions are grouped together through the Function Group entry on their configuration forms. The user must first define the Function Group names in the Fixed Plant Databook.

Refer to *PHD User Guide*, PHD Security

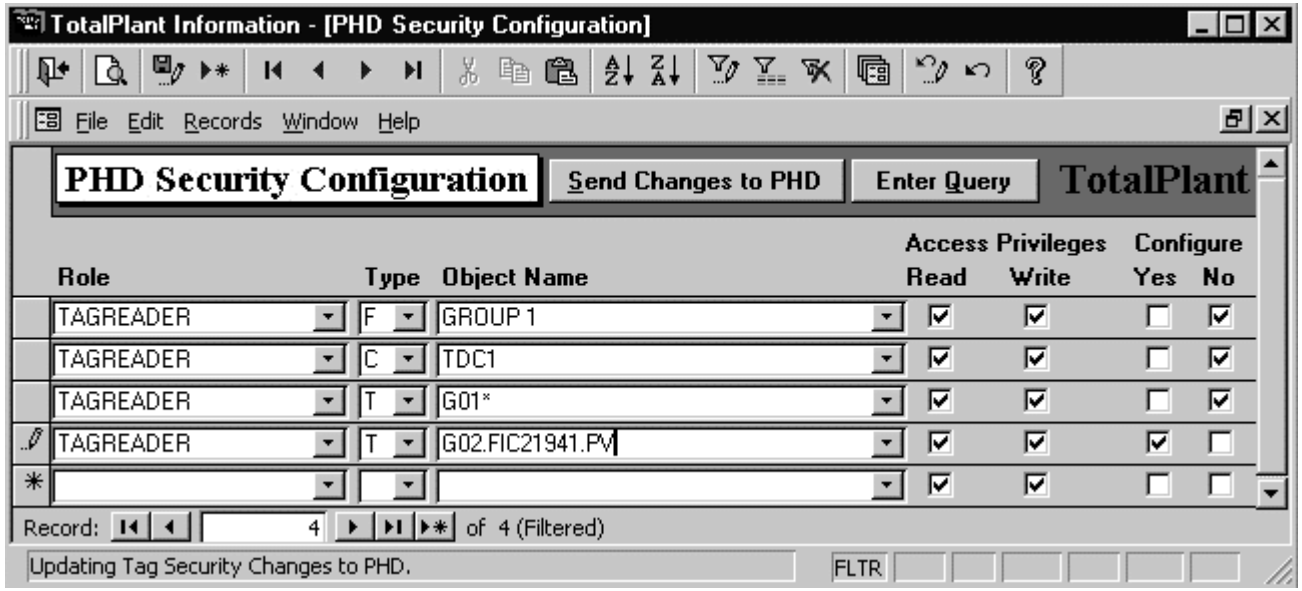
PHD Security Configuration Form, *continued*

Access Privileges

Read - Read data for all tags matching the object name.

Write - Write (Put) data to all tags matching the object name. (Tags must have Put Download enabled and RDI must be configured to do control.)

Configure - Allows the role to configure the object name.
T - modify or delete tags
C - modify, delete, or create tags on the collector
F - modify, delete, or create functions in the function groups



Send Changes to PHD - Informs PHD to update its internal security for the tags affected. The application does this automatically when you close the form.

Helpful Hint

For users who will not be doing tag configuration:

Provide access to all tags or provide access to a pattern of tags.
Ex: For role A, give read/write access to Area A (such as tags with names `A.*`),but read-only access to Area B.

For users who will be configuring tags:

Use collector-based security. It is easier to do. People who are configuring tags tend to need access to multiple collectors. Assign a collector to a role.

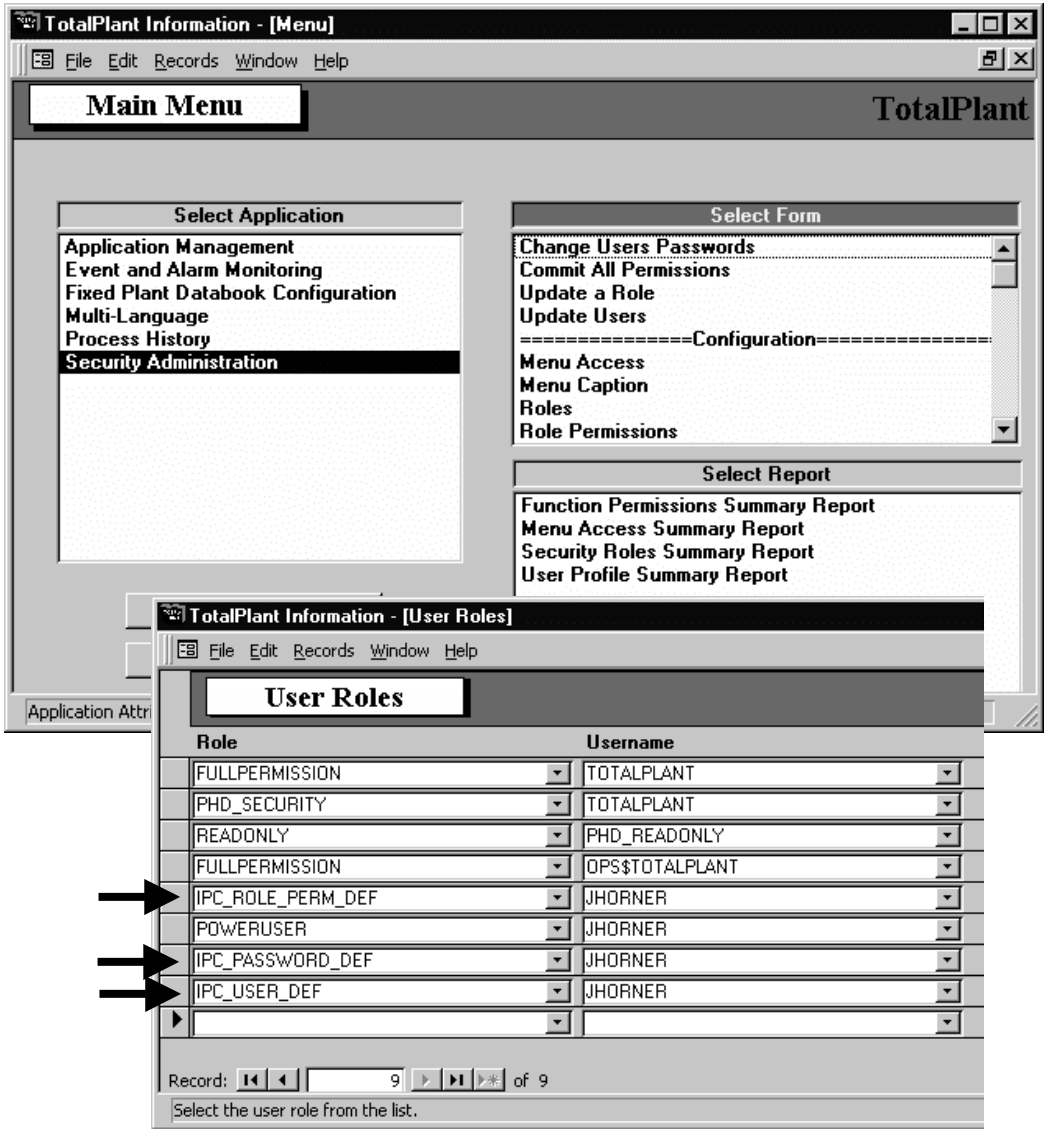
Tag Configuration Rules

The following rules apply to tag configuration:

- If you do not define PHD Security Configuration, there is no security applied to tag configuration. If you define at least one entry on a tag, then a role must have explicit access to perform operations on a tag.
- In order to add a tag to a collector (RDI), the role must have configuration access to the collector.
- If configuration is enabled on a collector for a role, users within the role can modify or delete all tags on the collector, except those tags that have been set to no-configure for the role.
- If a role has access to configure a tag, but no access to configure the collector, the tag can be modified or deleted. In this scenario, the collector name on the tag cannot be changed.
- To move a tag from one collector to another, the role must have configuration access to both collectors.
- Any role with “Insert” access to the Tag Configuration form can create a tag which is not on a collector (virtual tags and manual input tags). A role’s access to forms (a.k.a. functions) is defined on the Role Permissions form.

Refer to *PHD User Guide*, PHD Security Form

Security Administration Roles (R150 and later)



On R150 and later, administrative roles can be assigned to users.

The administrative roles that can be assigned are:

IPC_USER_DEF
This role has the privileges to maintain user permissions. This role commits user security changes through the **Update Users** form.

IPC_ROLE_PERM_DEF
This role has the privileges to maintain permissions. This role commits role security changes through the **Update a Role** form and commits security changes through the **Commit All Permissions** form.

IPC_PASSWORD_DEF
This role has the privileges to change passwords through the **Change Users Passwords** form.

Reference: *Security Administration User Guide*

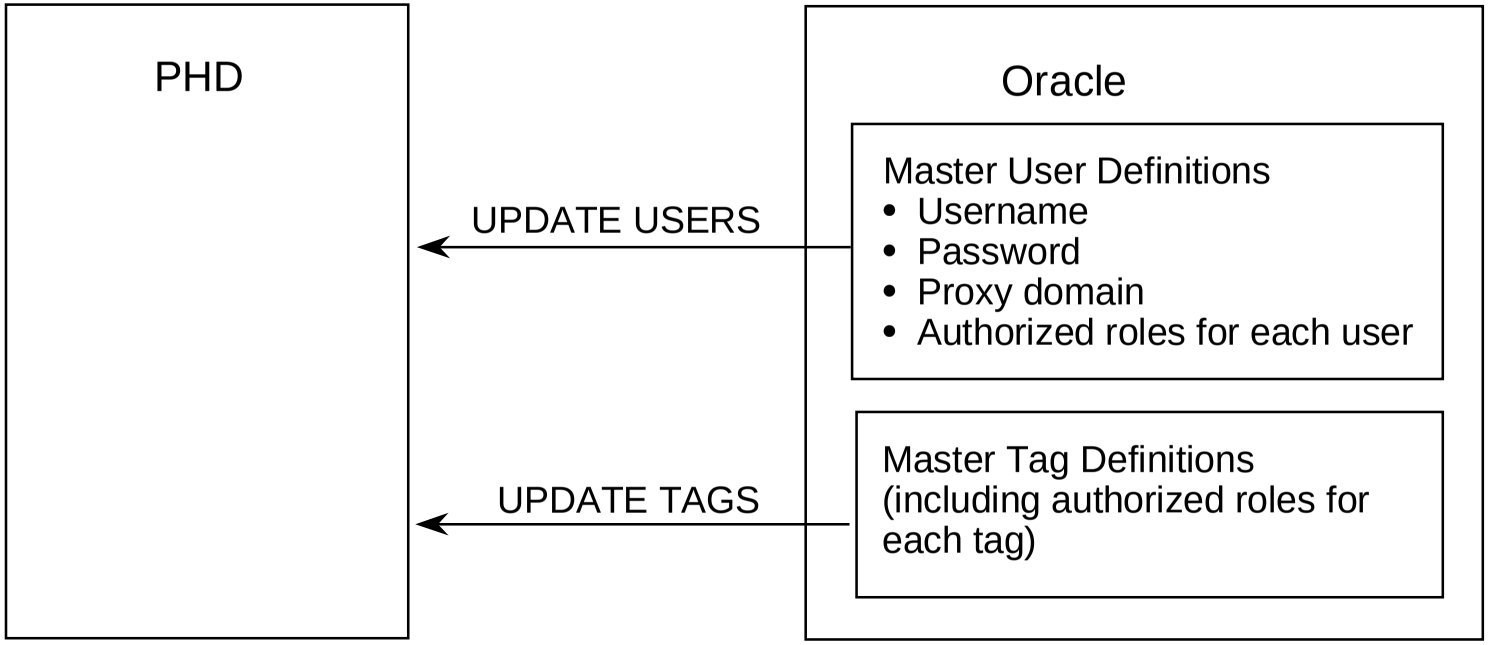
PHDMAN - Update Users and Tags

User definition changes and additions can be updated from Oracle to PHD manually through PHDMAN:

```
PHDMAN> UPDATE USERS
```

Tag security changes and additions can be updated from Oracle to PHD manually through PHDMAN:

```
PHDMAN> UPDATE TAGS
```



PHD Management Security

The PHDMAN Security Identifier is

- a group under NT
- a rights identifier in VMS (user authorization utility)
- a rights identifier in AIX

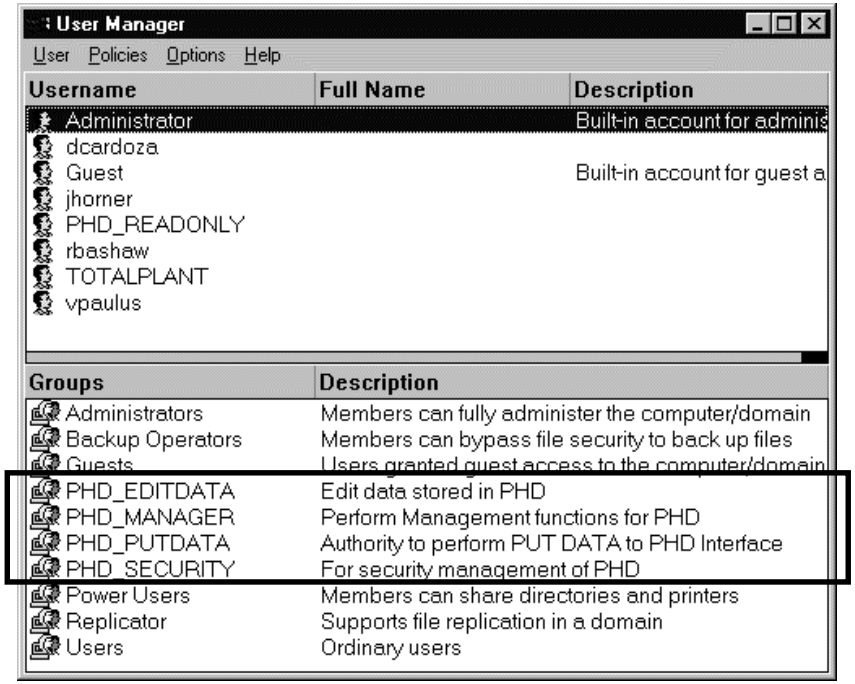
PHD_SECURITY and PHD_MANAGER - Minimum for whoever is going to manage the PHD system.

PHD_SECURITY
For security management of PHD. Allows configuration of tag security, proxies, and parameters, and allows read/configure (but not puts) to any PHD tag.

PHD_MANAGER
Allows access to privileged PHDMAN commands (other users can use SHOW and MONITOR commands only).

PHD_PUTDATA
Allow users to put values to an RDI instance by tag name (tag's Download Enable Flag must be set).

PHD_EDITDATA
Allow users to modify values within the archive system (tag's Data Edit Enable Flag must be set).



Refer to *PHD System Manual*, PHD System Security

Proxy Logins

For systems where Integrated NT Security(INTS) has not been implemented, the PHDMAN PROXY command specifies a proxy logon user for the specified operating system domain and user.

```
PHDMAN> PROXY os_domain os_username phd_username
```

When the NT user performs a proxy login (a login without specifying a username/password), the user will be logged on to the PHD server as the specified phd_username.

Example: Process Trend configured to "Bypass Login" will use a proxy.

Documentation

For information on PHD security, refer to the following documents:

Uniformance Electronic Documentation CD:

- *PHD User Guide*
  - PHD Security
    - PHD Security Form
    - PHDMAN> Update Users, Update Tags
    - Tag Security and PHD Connect
- *TPI Application User Guide*
  - User Profile Configuration
  - Roles
  - User Roles
  - Role Permissions
  - Menu Access
  - Change Passwords
  - Database Attachment
- *PHD System Manual*
  - Tag Security and User Definition
    - Overview
    - Public Security
    - Private Security
    - Role-Based Security
    - PHDMAN>Update User, Update Tags
    - Proxy Logins
  - Operating System Rights Identifiers
- *Security Administration User Guide*

TPS Electronic Documentation CD:

- *TPS System Planning Guide*
  - PHD Considerations

Honeywell

Helping You Manage Your World

www.iac.honeywell.com