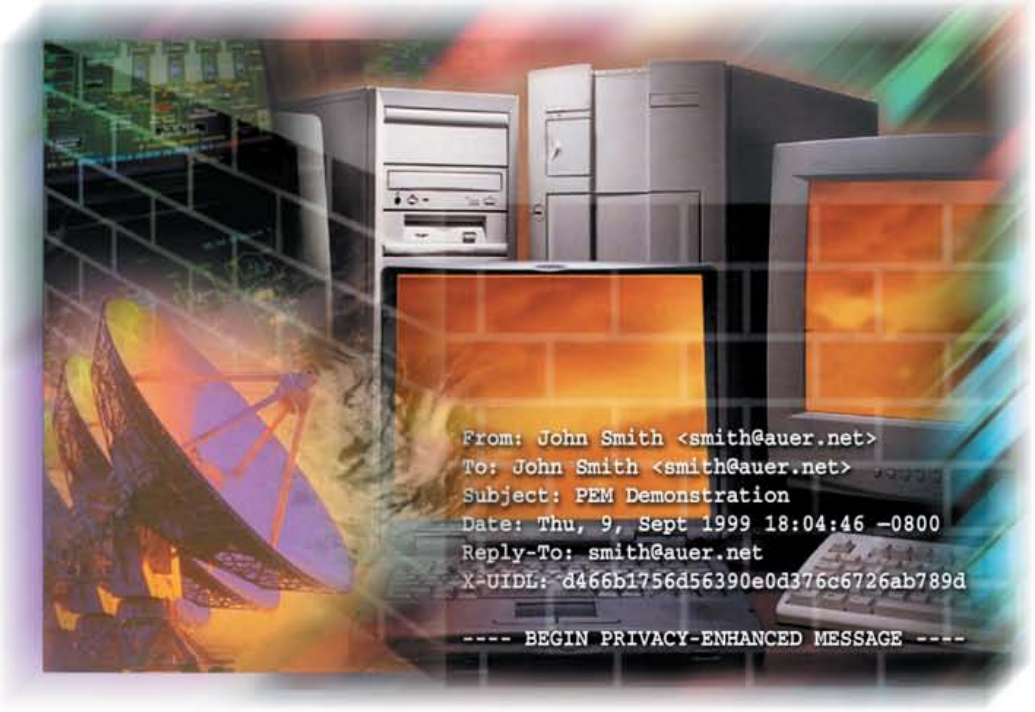
VOLUME 2

Information Security Management

HANDBOOK

4TH EDITION



Harold F. Tipton
Micki Krause

EDITORS

AUERBACH

Contributors

CHRISTINA BIRD, PH.D, CISSP, *Senior Security Analyst, Counterpane Internet Security, San Jose, California*

STEVE BLANDING, *Regional Director of Technology, Arthur Andersen LLP, Houston, Texas*

MICHAEL J. CORBY, *Vice President, Netigy Corp., San Francisco, California*

Eran Feigenbaum, *Manager, PricewaterhouseCoopers LLP, Los Angeles, California*

BRYAN FISH, *Network Systems Consultant, Lucent Technologies, Dallas, Texas*

STEPHEN FRIED, *Senior Manager, Global Risk Assessment and Secure Business Solutions, Lucent Technologies, Warren, New Jersey*

CHRIS HARE, CISSP, ACE, *Systems Auditor, Internal Audit, Nortel, Ottawa, Ontario, Canada*

JAY HEISER, CISSP, *Senior Security Consultant, Lucent NetworkCare, Washington, D.C.*

CARL B. JACKSON, CISSP, *Director, Global Security Practice, Netigy Corp., San Francisco, California*

MOLLY KHEHNKE, CISSP, *Computer Security Analyst, Lockheed Martin Energy Systems, Inc., Oak Ridge, Tennessee*

BRYAN T. KOCH, CISSP, *Principal Security Architect, Guardent, Inc., St. Paul, Minnesota*

ROSS LEO, CISSP, CBCP, *Director, Information Assurance & Security, Omitron, Inc., Houston,Texas*

BRUCE LOBREE, CISSP, *Security Manager, Oracle Business Online, Redwood Shores, California*

JEFF LOWDER, *Chief, Network Security Element, United States Air Force Academy, Colorado Springs, Colorado*

DOUGLAS C. MERRILL, PH.D., *Senior Manager, PricewaterhouseCoopers LLP, Los Angeles, California*

WILLIAM HUGH MURRAY, *Executive Consultant, Deloitte and Touche LLP, New Canaan, Connecticut*

SATNAM PUREWAL, B.SC., CISSP, *Manager, PricewaterhouseCoopers LLP, Seattle, Washington*

SEAN SCANLON, *e-Architect, fcgDoghouse, Huntington Beach, California*

KEN SHAURETTE, CISSP, CISA, *Information Systems Security Staff Advisor, American Family Institute, Madison, Wisconsin*

SANFORD SHERIZEN, PH.D., CISSP, *President, Data Security Systems, Inc., Natick, Massachusetts*

ED SKOUDIS, *Account Manager and Technical Director, Global Integrity, Howell, New Jersey*

BILL STACKPOLE, CISSP, *Managing Consultant, InfoSec Practice, Predictive Systems, Santa Cruz, California*

JAMES S. TILLER, CISSP, *Senior Security Architect, Belenos, Inc., Tampa, Florida*

GEORGE WADE, Senior Manager, Lucent Technologies, Murray Hill, New Jersey

Contents

Domain 4
Applications and Systems Development Security

WITH THE INCREASING DEPLOYMENT OF CLIENT/SERVER APPLICATIONS AND THE ADVENT OF INTERNET AND INTRANET APPLICATIONS, USER IDENTIFICATION AND AUTHENTICATION, AND DATA ACCESS CONTROLS ARE DISTRIBUTED THROUGHOUT THE MULTIPLE LAYERS OF A SYSTEM ARCHITECTURE. This decentralized security model differs greatly from the centrally controlled and managed mainframe environment.

The distributed system security architecture demands that protection mechanisms are embedded throughout. The chapters in this domain address the integration and unity of the controls within the application and database design. Further, the concept of the public key infrastructure is featured, which encompasses the policies, procedures, and robust administrative and technical controls required to support and secure scalable applications for potential deployment to millions of users.

Chapter 12
PeopleSoft Security

Satnam Purewal

SECURITY WITHIN AN ORGANIZATION'S INFORMATION SYSTEMS ENVIRONMENT IS GUIDED BY THE BUSINESS AND DRIVEN BY AVAILABLE TECHNOLOGY ENABLERS. Business processes, functional responsibilities, and user requirements drive security within an application. This chapter highlights security issues to consider in a PeopleSoft 7.5 client/server environment, including the network, operating system, database, and application components.

Within the PeopleSoft client/server environment, there are several layers of security that should be implemented to control logical access to PeopleSoft applications and data: network, operating system, database, and PeopleSoft application security. Network, operating system, and database security depend on the hardware and software selected for the environment (Windows NT, UNIX, and Sybase, respectively). User access to PeopleSoft functions is controlled within the PeopleSoft application.

1. Network security controls:
   a. who can log on to the network
   b. when they can log on (via restricted logon times)
   c. what files they can access (via file rights such as execute-only, read-only, read/write, no access, etc.)
2. Operating system security controls:
   a. who can log on to the operating system
   b. what commands can be issued
   c. what network services are available (controlled at the operating system level)
   d. what files/directories a user can access
   e. the level of access (read, write, delete)
3. Database security controls:
   a. who can log on to a database
   b. which tables or views users can access
   c. the commands users can execute to modify the data or the database
   d. who can perform database administration activities

0-8493-0800-3/00/$0.00+$.50

4. PeopleSoft online security controls:
   a. who can sign-on to PeopleSoft (via operator IDs and passwords)
   b. when they can sign-on (via operator sign-on times)
   c. the panels users can access and the functions they can perform
   d. the processes users can run
   e. the data they can query/update

NETWORK SECURITY

The main function of network security is to control access to the network and its shared resources. It serves as the first line of defense against unauthorized access to the PeopleSoft application.

At the network security layer, it is important to implement login controls. PeopleSoft 7.5 delivers limited authentication controls. If third-party tools are not going to be used to enhance the PeopleSoft authentication process, then it is essential that the controls implemented on this layer are robust.

The network servers typically store critical application data like client-executable programs and management reports. PeopleSoft file server directories should be set up as read-only for only those individuals accessing the PeopleSoft application (i.e., access should not be read-only for everyone on the network). If executables are not protected, unauthorized users could inadvertently execute programs that result in a denial-of-service. For this reason, critical applications used to move data should be protected in a separate directory. Furthermore, the PeopleSoft directories containing sensitive report definitions should be protected by only granting read access to users who require access.

DATABASE MANAGEMENT SYSTEM SECURITY

The database management system contains all PeopleSoft data and object definitions. It is the repository where organizational information resides and is the source for reporting. Direct access to the database circumvents PeopleSoft application security and exposes important and confidential information.

All databases compatible with the PeopleSoft applications have their own security system. This security system is essential for ensuring the integrity and accuracy of the data when direct access to the database is granted.

To reduce the risk of unauthorized direct access to the database, the PeopleSoft access ID and password must be secured, and direct access to the database should be limited to the database administrators (DBAs).

The access ID represents the account that the application uses to connect to the underlying database in order to access PeopleSoft tables. For

the access ID to update data in tables, the ID must have read/write access to all PeopleSoft tables (otherwise, each individual operator would have to be granted access to each individual table). To better understand the risk posed by the access ID, it helps to have an understanding of the PeopleSoft sign-on (or logon) process:

1. When PeopleSoft is launched on the user workstation, the application prompts for an operator ID and password. The ID and password input by the operator is passed to the database (or application server in three-tier environments).
2. The operator ID and password are validated against the PSOPRDEFN security table. If both are correct, the access ID and password are passed back to the workstation.
3. PeopleSoft disconnects from the DBMS and reconnects using the access ID and password. This gives PeopleSoft read/write access to all tables in the database.

The application has full access to all PeopleSoft tables, but the access granted to the individual operator is restricted by PeopleSoft application security (menu, process, query, object, and row-level security). Users with knowledge of the access ID and password could log on (e.g., via an ODBC connection) directly to the database, circumventing application security. The user would then have full access privileges to all tables and data, including the ability to drop or modify tables.

To mitigate this risk, the following guidelines related to the access ID and password should be followed:

- Procedures should be implemented for regularly changing the access ID password (e.g., every 30 days). At a minimum, the password must be changed anytime someone with knowledge of it leaves the organization.
- Ownership of the access ID and password should be assigned, preferably to a DBA. This person would be responsible for ensuring that the password is changed on a regular interval, and for selecting strong passwords. Only this person and a backup should know the password. However, the ID should never be used by the person to log on to the database.
- Each database instance should have its own unique access ID password. This reduces the risk that a compromised password could be used to gain unauthorized access to all instances.
- The access ID and password should not be hard-coded in cleartext into production scripts and programs. If a batch program requires it, store the ID and password in an encrypted file on the operating system and "point" to the file in the program.

- Other than DBAs and technical support personnel, no one should have or need a database ID and direct connectivity to the database (e.g., SQL tools).

OPERATING SYSTEM SECURITY

The operating system needs to be secured to prevent unauthorized changes to source, executable, and configuration files. PeopleSoft and database application files and instances reside on the operating system. Thus, it is critical that the operating system environment be secure to prevent unauthorized changes to source, executable, and configuration files.

PEOPLESOFT APPLICATION SECURITY

To understand PeopleSoft security, it is first essential to understand how users access PeopleSoft. To access the system, an operator ID is needed. The system will determine the level of access for which the user is authorized and allow the appropriate navigation to the panels.

Many organizations have users with similar access requirements. In these situations, an "operator class" can be created to facilitate the administration of similar access to multiple users. It is possible to assign multiple operator classes to users. When multiple operator classes are used, PeopleSoft determines the level of access in different ways for each component. The method of determining access is described below for each layer when there are multiple operator classes.

PeopleSoft controls access to the different layers of the application using operator classes and IDs. The term "operator profile" is used to refer, in general, to both operator IDs and classes. Operator profiles are used to control access to the different layers, which can be compared to an onion. Exhibit 12-1 shows these layers: Sign-on security, panel security, query security, row-level security, object security, field security, and process security. The outer layers (i.e., sign-on security and panel security) define broader access controls. Moving toward the center, security becomes defined at a more granular level.

The layers in Exhibit 12-1:

- Sign-on security provides the ability to set up individual operator IDs for all users, as well as the ability to control when these users can access the system.
- Panel security provides the ability to grant access to only the functions the user requires within the application.
- Query security controls the tables and data users can access when running queries.
- Row-level security defines the data that users can access through the panels they have been assigned.

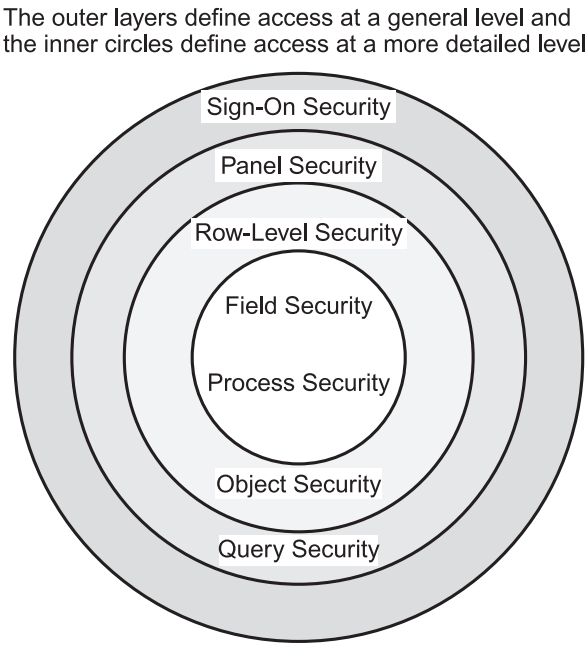


Exhibit 12-1. PeopleSoft security onion.

- Object security defines the objects that users can access through the tools authorized through panel security.
- Field security is the ability to restrict access to certain fields within a panel assigned to a user.
- Process security is used to restrict the ability to run jobs from the PeopleSoft application.

Sign-on Security

PeopleSoft sign-on security consists of assigning operator IDs and passwords for the purpose of user logon. An operator ID and the associated password can be one to eight characters in length. However, the delivered sign-on security does not provide much control for accessing the PeopleSoft application.

PeopleSoft (version 7.5 and earlier) modules are delivered with limited sign-on security capabilities. The standard features available in many applications are not available within PeopleSoft. For example, there is no way to limit the number of simultaneous sessions a user can initiate with an operator ID. There also are no controls over the types of passwords that can be chosen. For example, users can choose one-character passwords or they can set the password equal to their operator ID. Users with passwords equal to the operator ID do not have to enter passwords at logon. If these users are observed during the sign-on process, it is easy to determine their passwords.

Many organizations have help desks for the purpose of troubleshooting common problems. With PeopleSoft, password maintenance cannot be decentralized to the help desk without also granting the ability to maintain operator IDs. This means that the help desk would also have the ability to change a user's access as well as the password. Furthermore, it's not possible to force users to reset passwords during the initial sign-on or after a password reset by the security administrator.

There are no intrusion detection controls that make it possible to suspend operator IDs after specified violation thresholds are reached. Potentially, intruders using the brute-force method to enter the system will go undetected unless they are caught trying to gain access while at the workstation.

Organizations requiring more robust authentication controls should review third-party tools. Alternatively, PeopleSoft plans to introduce password management features in version 8.0.

Sign-on Times. A user's session times are controlled through the operator ID or the operator class(es). In either case, the default sign-on times are 24 hours a day and 7 days a week. If users will not be using the system on the weekend or in the evening, it is best to limit access to the known work hours.

If multiple operator classes are assigned to operator IDs, attention must be given to the sign-times. The user's start time will be the earliest time found in the list of assigned operator classes. Similarly, the user's end time will be the latest time found in the list of assigned operator classes.

Delivered IDs. PeopleSoft is delivered with operator IDs with the passwords set equal to the operator ID. These operator IDs should be deleted because they usually have full access to business panels and developer tools. If an organization wishes to keep the delivered operator IDs, the password should be changed immediately for each operator ID.

Delivered Operator Classes. PeopleSoft-delivered operator classes also have full access to a large number of functional and development menus and panels. For example, most of these operator classes have the ability to maintain panels and create new panels. These operator classes also have the ability to maintain security.

These classes should be deleted in order to prevent them from being assigned accidentally to users. This will prevent users from getting these operator classes assigned to their profile in error.

Panel Security

There are two ways to grant access to panels. The first way is to assign menus and panels directly to the operator ID. The second way is to assign menus/panels to an operator class and then assign the operator class to

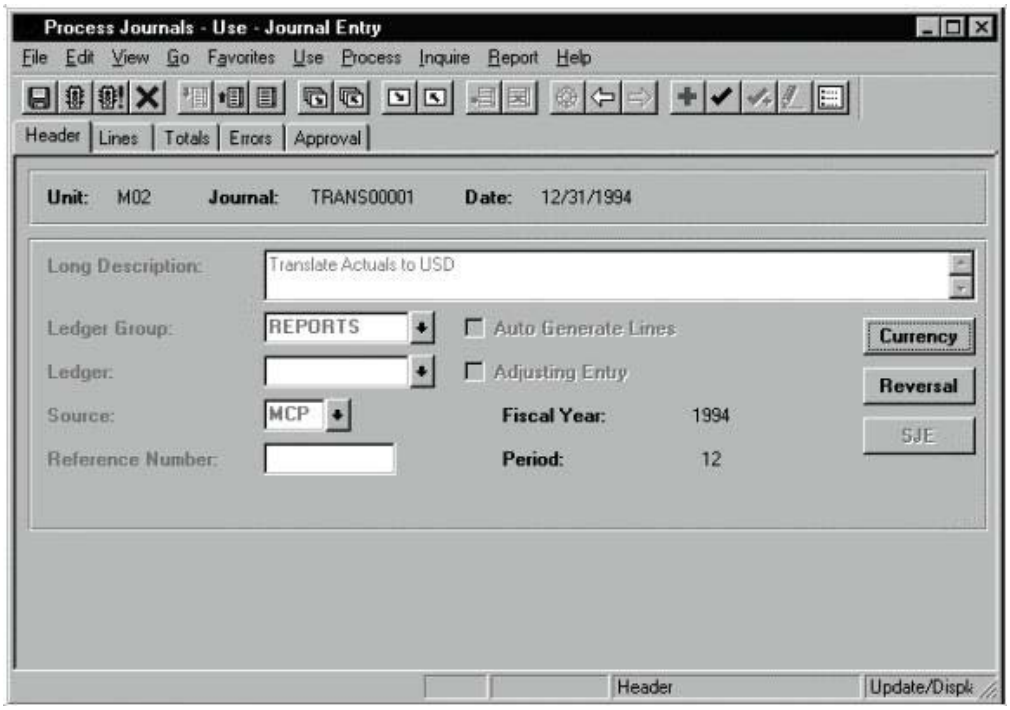


Exhibit 12-2. The PeopleSoft journal entry panel.

the operator ID. When multiple operator classes are assigned to a user, the menus granted to a user are determined by taking a union of all the menus and panels assigned from the list of operator classes assigned to the user. If a panel exists in more than one of the user's operator classes with different levels of access, the user is granted the greater access. This means if in one operator class the user has read-only access and in the other the user has update access, the user is granted update access. This capability allows user profiles to be built like building blocks. Operator classes should be created that reflect functional access. Operator classes should then be assigned according to the access the user needs.

Panel security is essentially column security. It controls access to the columns of data in the PeopleSoft tables. This is best described with an example. The PeopleSoft Journal Entry panel (see Exhibit 12-2) has many fields, including Unit, Journal, Date, Ledger, Long Description, Ledger Group, Ledger, Source, Reference Number, and Auto Generate Lines.

Exhibit 12-3 shows a subset of the columns in the table JRNL_HEADER. This table is accessible from the panel **Process Journals – Use – Journal Entry Headers** panel. The fields in this panel are only accessible by the user if they are displayed on the panel to which the user has access.

When access is granted to a panel, it is also necessary to assign *actions* that a user can perform through the panel. Exhibit 12-4 shows the actions that are

Exhibit 12-3. A subset of the columns in the table JRNL_HEADER.

Unit	Journal	Date	Long Descr	Ledger Grp	Ledger	Source	Ref No	Auto Gen
M02	TRANS0001	1994-12-31	Translate Actuals to USD	REPORTS		MCP		N
M02	TRANS0001	1995-12-31	Translate Actuals to USD	REPORTS		MCP		N
M02	TRANS0001	1996-01-01	Translate Actuals to USD	REPORTS		MCP		N
M04	0000005185	1995-12-27	Adjusting entries for unexpected Production Scrap - not to be repeated.	ACTUALS		ADJ		N
M04	0000005197	1998-03-13	Inventory Transactions	ACTUALS		INV	INV100	N
M04	0000005259	1998-03-19	Inventory Transactions	ACTUALS		INV	INV100	N
M04	0000005271	1998-01-31		BUDGETS		CFO		N
M04	0000005272	1998-01-01	Budget Journals	BUDGETS		CFO		N

Exhibit 12-4. Common actions in panels.

Action	Capability
Add	Ability to insert a new row
Update/Display	Ability to access present and future data
Update/Display All	Ability to access present, future, and historical data; updates to historical data are not permitted
Correction	Ability to access present, future, and historical data; updates to historical data are permitted

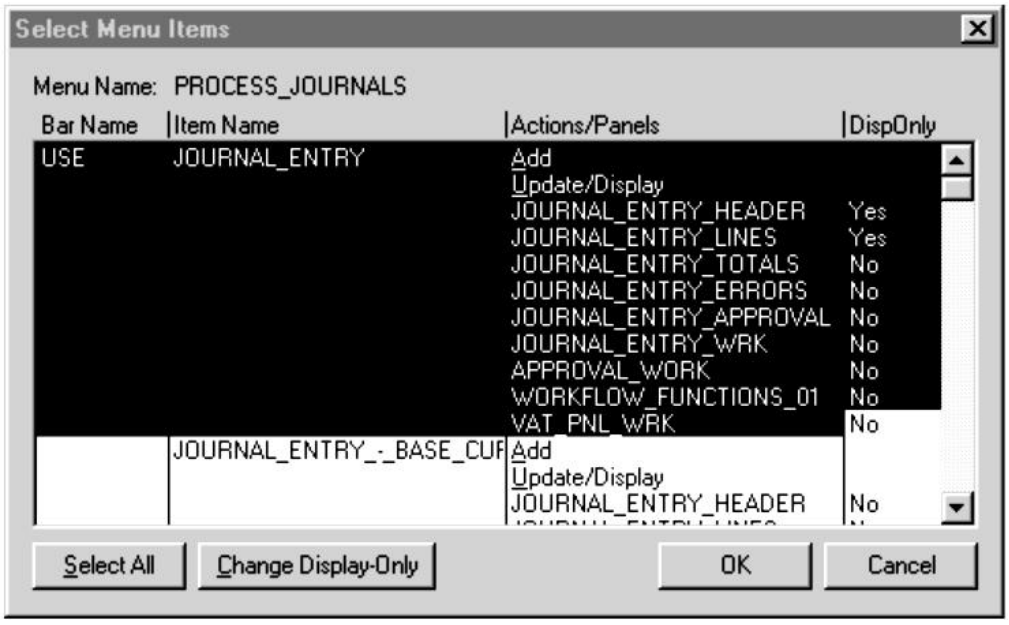


Exhibit 12-5. Assigning read-only access.

common to most panels. This table only shows a subset of all the actions that are available. Furthermore, not all of these actions are available on all panels.

From a security standpoint, correction access should be limited to select individuals in an organization because users with this authority have the ability to change historical information without maintaining an audit trail. As a result, the ability to change historical information could create questions about the integrity of the data. Correction should be used sparingly and only granted in the event that an appropriate process is established to record changes that are performed.

The naming convention of two of the actions (Update/Display, Update/Display All) is somewhat misleading. If a user is granted access to one or both of these actions, the user does not necessarily have update access. Update access also depends on the "Display Only" attribute associated with each panel. When a panel is assigned to an operator ID or operator class, the default access is update. If the user is to have read-only access to a panel, then this attribute must be set to "Y" for yes (see Exhibit 12-5 for an example). This diagram shows that the user has been assigned read-only access to the panels "JOURNAL_ENTRY_HEADER" and "JOURNAL_ENTRY_LINES." For the other highlighted panels, the user has been granted update capabilities.

The panels that fall under the menu group PeopleTools provide powerful authority (see Exhibit 12-6 for a list of PeopleTools menu items). These panels should only be granted to users who have a specific need in the production environment.

Exhibit 12-6. PeopleTools menu items.

APPLICATION DESIGNER
SECURITY ADMINISTRATOR
OBJECT SECURITY
APPLICATION REVIEWER
UTILITIES
IMPORT MANAGER
PROCESS SCHEDULER
EDI MANAGER
nVISION
REPORT BOOKS
TREE MANAGER
QUERY
APPLICATION ENGINE
MASS CHANGE
WORKFLOW ADMINISTRATOR
PROCESS MONITOR
TRANSLATE
CUBE MANAGER

Query Security

Users who are granted access to the **Query** tool will not have the capability to run any queries unless they are granted access to PeopleSoft tables. This is done by adding *Access Groups* to the user's operator ID or one of the operator classes in the user's profile. Access Groups are a way of grouping related tables for the purposes of granting query access.

Configuring query security is a three-step process:

1. Grant access to the **Query** tool.
2. Determine which tables a user can query against and assign **Access Groups**.
3. Set up the Query Profile.

Sensitive organizational and employee data is stored within the PeopleSoft application and can be viewed using the **Query** tool. The challenge in setting up query security is consistency. Many times, organizations will spend a great deal of effort restricting access to panels and then grant access to view all tables through query. This amounts to possible unauthorized access to an organization's information. To restrict access in query to the data accessible through the panels may not be possible using the PeopleSoft delivered access groups. It may be necessary to define new access groups to enable querying against only the tables a user has been authorized to view. Setting up customized access groups will facilitate an organization's objective to ensure consistency when authorizing access.

The **Query Profile** helps define the types of queries a user can run and whether the user can create queries. Exhibit 12-7 displays an example of a profile. Access to the Query tool grants users the ability to view information that resides within the PeopleSoft database tables. By allowing users to create ad hoc queries can require high levels of system resources in order to run complex queries. The Query Profile should be configured to reduce the risk of overly complex queries from being created without being tuned by the database administrators.

The Query Profile has several options to configure. In the **PS/Query Use** box, there are three options. If a user is not a trained query user, then access should be limited to *Only Allowed to run Queries.* Only the more experienced users should be given the authority to create queries. This will reduce the likelihood that resource intensive queries are executed.

Row-level Security

Panel security controls access to the tables and columns of data within the tables but a user will be able to access all data within the columns of the tables on the panel. To restrict user access to data on a panel, row-level security should be established. Access is granted to data using control fields. For example, in Exhibit 12-8 the control field is "Unit" (or Business Unit). If a user is assigned to only the M02 business unit, that user would only be able to see the first four lines of data.

Row-level security is implemented differently in HRMS and Financials.

Human Resource Management System (HRMS) Row-level Security. In HRMS, the modules are delivered with row-level security activated. The delivered row-level security is based on a Department Security Tree and is hierarchical (see Exhibit 12-9). In this example, if a user is granted access to ABC manufacturing department, then the user would have access to the ABC manufacturing department and all of the child nodes. If access is granted to the department Office of the Director Mfg, then the user would have access to the Office of the Director Mfg as well as Corporate Sales, Corporate Marketing, Corporate Admin/Finance, and Customer Services. It is also possible to grant access to the department Office of the Direct Mfg. and then deny access to a lower level department such as Corporate Marketing.

It is important to remember that the organizational tree and the security tree in HRMS need not be the same. In fact, they should not be the same. The organizational tree should reflect the organization today. The security tree will have historical nodes that may have been phased out. It is important to keep these trees in order to grant access to the associated data.

Financials Row-level Security. In the Financials application, row-level security is not configured in the modules when it is delivered. If row-level

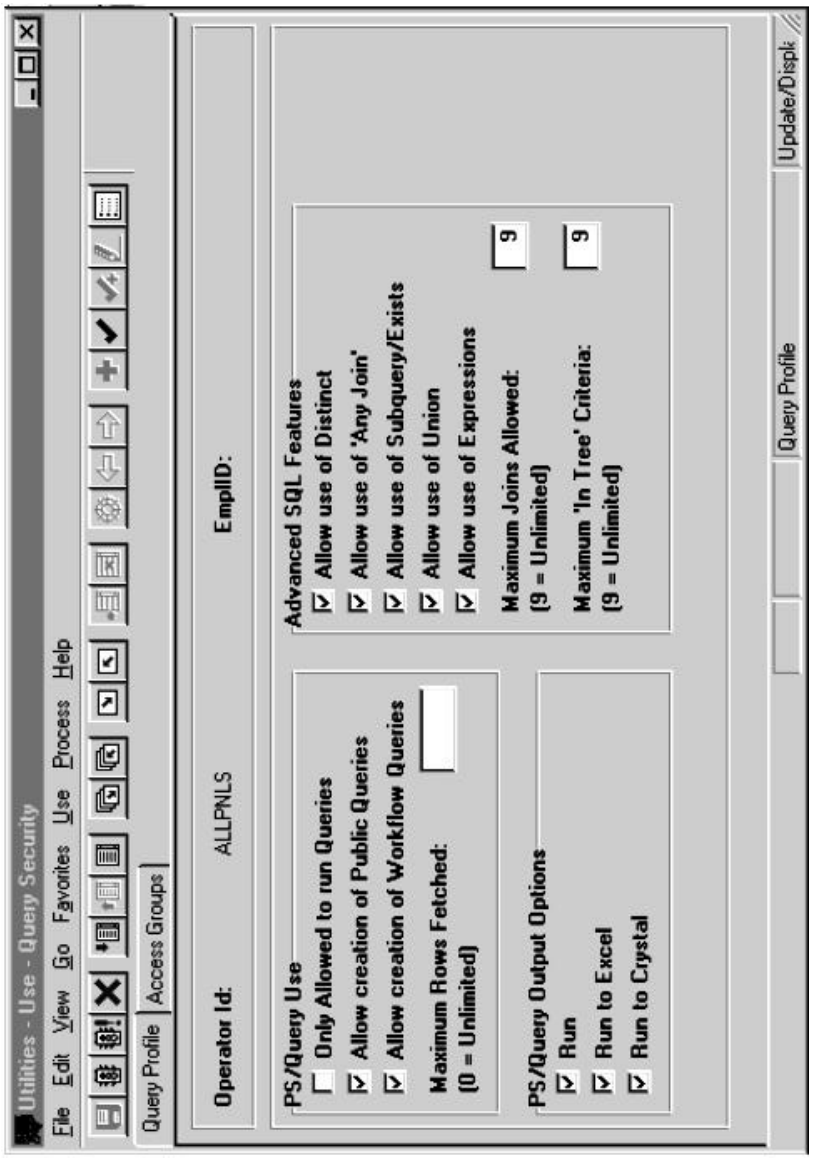


Exhibit 12-7. Query profile.

Exhibit 12-8. Row-level security.

Unit	Journal	Date	Ledger	Unit	Currency	Foreign Curr.	Debits	Credits
M02	**AP00005168**	**1995-12-31**	**ACTUALS**	**M02**	**CAD**	**CAD**	**50000.00**	**50000.00**
M02	BI00005216	1998-03-16	ACTUALS	M02	CAD	USD	10149.30	10149.30
M02	BI00005258	1998-03-18	ACTUALS	M02	CAD	USD	20298.60	20298.60
M02	TRANS00001	1995-12-31	REPORTS	M02	USD	USD	3470257761.27	3470257761.27
M04	0000005185	1995-12-27	ACTUALS	M04	USD	CAD	60362.91	60362.91
M04	0000005185	1995-12-27	ACTUALS	M04	USD	USD	6345.00	6345.00
M04	0000005197	1998-03-13	ACTUALS	M04	USD	USD	525145.27	525145.27
M04	0000005271	1998-01-31	BUDGETS	M04	USD	CAD	69075.08	69075.08

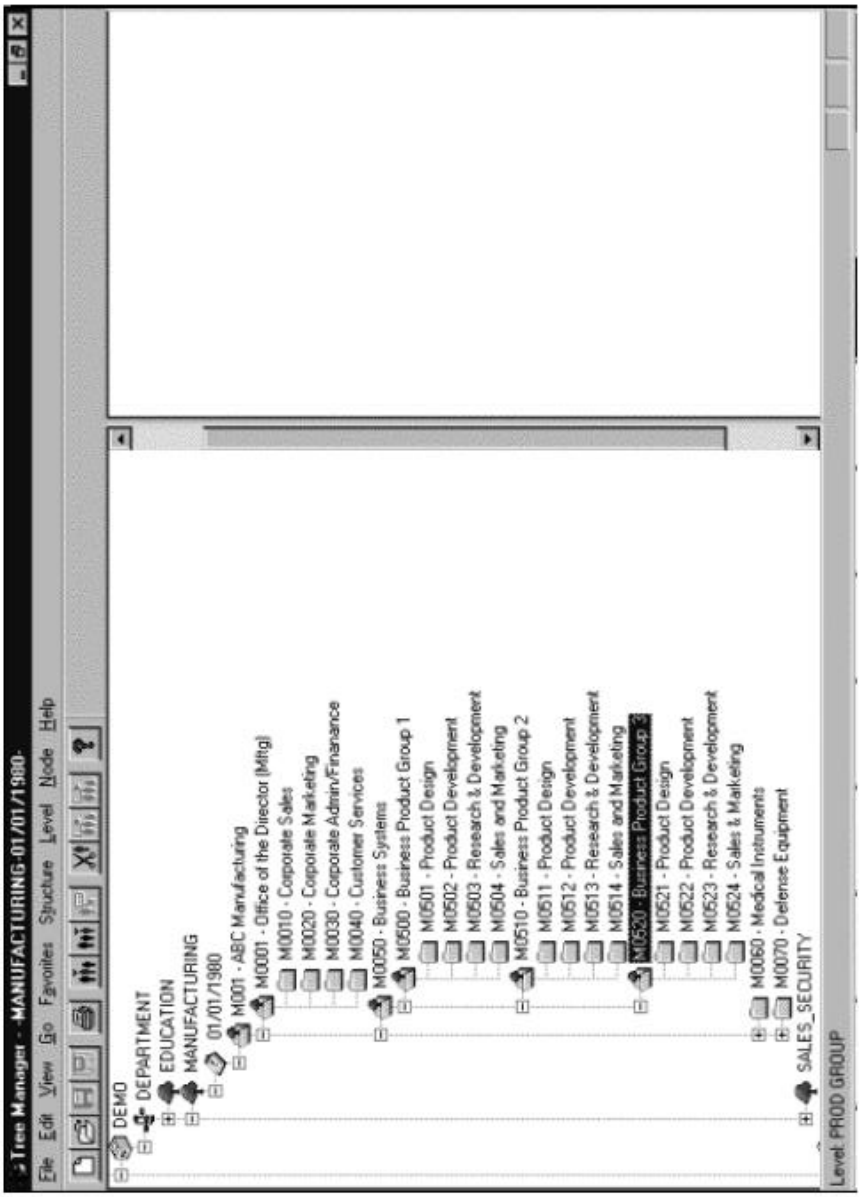


Exhibit 12-9. Department security tree.

security is desired, then it is necessary to first determine if row-level security will be implemented at the operator ID or operator class level. Next, it is necessary to determine the control fields that will be used to implement row-level security. The fields available for row-level security depend on the modules being implemented. Exhibit 12-10 shows which module the options are available in.

Exhibit 12-10. Modules of available options.

Field	Module
Business Unit	General Ledger
SetID	General Ledger
Ledger	General Ledger
Book	Asset Management
Project	Projects
Analysis Group	Projects
Pay Cycle	Accounts Payable

Object Security

In PeopleSoft, an object is defined as a menu, a panel, or a tree. For a complete list of objects, see Exhibit 12-11. By default, all objects are accessible to users with access to the appropriate tools. This should not always be the case. For example, it is not desirable for the security administrator to update the organization tree, nor is it appropriate for an HR supervisor to update the department security tree. This issue is resolved through object groups. Object groups are groups of objects with similar security privileges. Once an object is assigned to an object group, it is no longer accessible unless the object group is assigned to the user.

Exhibit 12-11. PeopleSoft objects.

Import Definitions (I)
Menu Definitions (M)
Panel Definitions (P)
Panel Group Definitions (G)
Record Definitions (R)
Trees (E)
Tree Structure Definitions (S)
Projects (J)
Translate Tables (X)
Query Definitions
Business Process Maps (U)
Business Processes (B)

In production, there should not be any access to development-type tools. For this reason, the usage of object security is limited in production. It is mainly used to protect trees. When users are granted access to the Tree Manager, the users have access to all the available trees. In production HRMS, this would mean access to the organization tree, the department security tree, and query security trees. In Financials, this means access to the query security trees and the reporting trees. To resolve this issue, object security is used to ensure that the users with access to Tree Manager are only able to view/update trees that are their responsibility.

Field Security

The PeopleSoft application is delivered with a standard set of menus and panels that provides the functionality required for users to perform their job functions. In delivering a standard set of menus and panels, there are occasions in which the access to data granted on a panel does not coincide with security requirements. For this reason, field-level security may need to be implemented to provide the appropriate level of security for the organization.

Field security can be implemented in two ways; either way, it is a customization that will affect future upgrades. The first option is to implement field security by attaching PeopleCode to the field at the table or panel level. This is complicated and not easy to track. Operator IDs or operator classes are hard-coded into the code. To maintain security on a long-term basis, the security administrator would require assistance from the developers.

The other option is to duplicate a panel, remove the sensitive field from the new panel, and secure access through panel security to these panels. This is the preferred method because it allows the security administrator control over which users have access to the field and it is also easier to track for future upgrades.

Process Security

For users to run jobs, it is necessary for them to have access to the panel from which the job can be executed. It is also necessary for the users to have the process group that contains the job assigned to their profile.

To simplify security administration, it is recommended that users be granted access to all process groups and access be maintained through panel security. This is only possible if the menus/panels do not contain jobs with varying levels of sensitivity. If there are multiple jobs on a panel and users do not require access to all jobs, then access can be granted to the panel and to the process group that gives access to only the jobs required.

SUMMARY

Within the PeopleSoft client/server environment, there are four main layers of security that should be implemented to control logical access to PeopleSoft applications: network, operating system, database, and application security. Network security is essential to control access to the network and the PeopleSoft applications and reports. Operating system security will control access to the operating system as well as shared services. Database security will control access to the database and the data within the database. Each layer serves a purpose and ignoring the layer could introduce unnecessary risks.

PeopleSoft application security has many layers. An organization can build security to the level of granularity required to meet corporate requirements. Sign-on security and panel security are essential for basic access. Without these layers, users are not able to access the system. Query security needs to be implemented in a manner that is consistent with the panel security. Users should not be able to view data through query that they cannot view through their authorized panels. The other component can be configured to the extent that is necessary to meet the organization's security policies.

Individuals responsible for implementing security need to first understand the organization's risk and the security requirements before they embark on designing PeopleSoft security. It is complex, but with planning it can be implemented effectively.