Oracle® Communications Performance Intelligence Center

Management Security Guide

Release 10.4.0

F26322-01

November 2020

Oracle® Communications Performance Intelligence Center Management Security Guide, Release 10.4.0

CAUTION: Use only the guide downloaded from Oracle Help Center.

Table of Contents

List of Figures

List of Tables

Chapter 1: About this Help Text

Overview

The Management Application Security Application enables the user to manage user access at login to the Management Application Platform and user access to data through profile and role definitions.

Scope and Audience

This help text provides information about Security concepts. It is designed as a guide for the system administrator or the user who is in charge of setting up users, groups, and roles in Management Application.

General Information

You can find general information about Oracle® Communications Performance Intelligence Center, such as product overview, list of other guides, workstation requirements, login and logout procedures, user preference settings, in the Quick Start Guide. This document is available from the Portal menu or can be downloaded from Oracle Help Center (OHC).

Chapter 2: About Management Application Security

Management Application Security Principles

The Management Application Security application provides the means to authorize user access to Management Application and features and to maintain data integrity. The Security application enables the System Administrator to apply the following:

- Authentication (System Access) - Makes sure users are who they claim to be. Authentication is controlled by
  - User IDs created in an underlying LDAP directory or an external LDAP database
  - Passwords
- Authorization (Application Access) - Makes sure the user has access only to specified applications or features within applications. Several mechanisms are used: system operating mode, token availability, and role definitions. The user must first be authenticated. Each user is identified by a profile, which contains that user's authorization role.
- Privacy (Data Access) - Protects the sensitive data objects from unauthorized use by assuring that only users with the appropriate Read/Write/Execute privileges gain access.

Management Application employs a Web-based interface to control system access. This facility controls:

- User login and logout
- Management Application Administrator's ability to force disconnect and set access level
- Oracle Customer Service's setting values for purchased user tokens (licenses)

Security Menu and Toolbar

For details about what these Menu options and toolbar icons provide, see Chapter 3: Using Security Application

Menu Option	Description
Users	Displays the list of the users with the username, description, email address, profile, restricted access status, date and time of last login, and the number of active sessions. From this page you can perform the actions such as add users, modify existing users, and unlock accounts.
Privacy roles	Displays the list of Privacy roles, including description, number of users in that role, and number of objects to which that role has access.
Profiles	Displays the list of defined Profiles, with description and the number of users within each profile
Objects	Displays the list of objects within Management Application, including the type of object, owner, and the date created.

Table 1: Security Menu

Menu Option	Description
Password settings	Displays a dialog for configuring password criteria. Examples are number and type of characters, lifetime of the password (before it must be changed), and whether the password is generated automatically or manually.
Filter access	Displays a dialog to define which subset of users can access Management Application during times of restricted access.
Transfer ownership	Displays a dialog to change ownership for all of an individual's objects.
Manage tokens	Displays a read-only dialog that shows the number of purchased tokens (licenses) and the maximum number allowed per user.
Security notice	Displays a dialog for security text to be used on the login page.

Table 2: Action Menu

Menu Option	Description
Export users	Displays a dialog for generating a list of existing Management Application user definitions, passwords, email addresses, and profiles.
Export profiles	Displays a dialog for generating a list of existing Management Application profiles with descriptions and associated roles.
Export roles	Displays a dialog for generating a list of existing Management Application roles and their descriptions.

Table 3: File Menu

Menu Option	Description
User manual	Opens on-line help text for the Management application in use.
About security	Provides version and copyright information about Management Application as well as contact information for Oracle support.

Table 4: Help Menu

Icons	Lists	Description
	All	Navigation arrow - use to move back and forth among pages. This example is the arrow to move to the next page. Other combinations of arrows move to the next page, final page, etc.
	User Role Profile	Add Record - adds a record to the list
	User Role Profile	Edit Record - modifies the selected record
	User Role Profile	Delete Record - deletes the selected record
	All	Filter - displays a dialog enabling you to define filters for the list of users
	User	Unlock - unlocks the selected user account
	User	Reset password - resets the selected user's password. Resetting can be by manually entering a new password or by having the system automatically generate a password.
	User	Logout - logs the selected user out of the application.
	All	Refresh - resets the display to include the most current data
	All	Records per Page - sets the number of records to view per page
	All	Record Number/Total Number of Records - shows the number of the selected record / total number of records available
	Object	Privacy - modifies the privacy settings of the selected object
	Object	Owner - changes the owner of the selected object

Table 5: Security Toolbar Icons

Note: Do not use the Function Keys (F1 through F12) when using Management Application. Function keys work in unexpected ways. For example, the F1 key does not open Management Application help but opens the help for the browser in use. The F5 key does not refresh a specific screen, but refreshes the entire session and results in a loss of any entered information.

Security Components

Users

From the system's viewpoint, each user has a unique identity. This identity is created by combining a user id and a password. A user can be a person or a software entity, such as a Java client.

When users are added to the Performance Intelligence Center system, the system administrator assigns each user a password and a user profile. Authorization roles and privacy roles are assigned to a user profile. The Authorization roles and privacy roles control the level of user access to Management Application, features, and data objects.
Passwords are typically alphanumeric, with a minimum and maximum number of characters.
This guide explains security procedures performed by the Management Application Administrator.

Roles

Roles used to define application and feature access are:

- Pre-defined - Roles used to establish access to application resources. These are mapped to Management Application-defined users in LDAP (Users, Power Users and Managers).
- Organizational - Roles defined by the customer. These are defined as global roles (for example: GPRS, UMTS, PSTN, Lyon, Mulhouse, and so on).

Management Application Security involves two types of roles: Authorization Roles and Privacy Roles.

Authorization Roles

In Management Application, there are ten pre-defined user Authorization roles: The Management Application Administrator is the supervisory role that can assign roles to other users. In addition, the Management Application Administrator has all the privileges of the other roles.

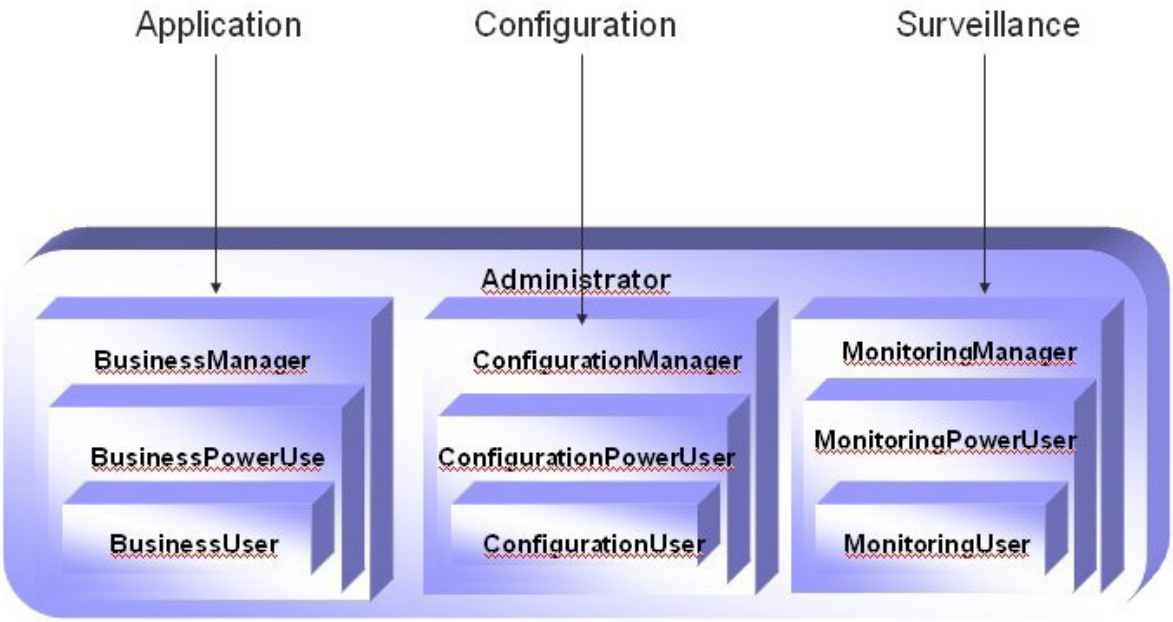

Figure 1: User Matrix

Management Application's user policy divides Authorization roles into a matrix of families and levels, which are assigned to profiles at the time of profile creation. The role families are

- Application (Business) - provides full or partial access to the following applications: Dashboard, Alarm Viewer, Troubleshooting, Report InfoView, SS7 Surveillance, On Demand UP Capture, Sigtran Surveillance, and Browser Export.
- Configuration - provides full or partial access to the following applications: Dashboard, KPI, Alarm Configuration, Alarm Forwarding, Report Administrator, Browser Export Scheduler, On Demand UP Capture, Reference Data, and Mediation Data Feed.
- Surveillance (Monitoring) - provides access to System Alarm, Diagnostic Utility, and Audit Viewer.

The role levels, which define the degree of privilege in application access, are

- User - Allows user access to object data
- Power User - Allows user access to Management Application critical functions

- Manager - Allows a user to manage Management Applications

These tables map authorization roles to specific functions in each application in the Management Application toolbox:
(The ✓ denotes the role that can perform the related function. An empty cell means that role cannot perform the function.)

Application	Feature	Authority	Business Manager	Business Power User	Business User
Troubleshooting	Sessions	List/Execute	✓	✓	✓
	Queries	List/Execute	✓	✓	✓
		Edit/Add/Delete	✓	✓	
	Results	Upload	✓	✓	
		Download	✓	✓	✓
		Delete	✓	✓	
	Roles	Change	✓	✓	
	PDUs	xDR Layout (View)	✓		
		Field Hiding	✓	✓	
	Full Decoding	xDR Layout (View)	✓		
		Field Hiding	✓	✓	
	Decoded SMS	xDR Layout	✓		
		Field Hiding	✓	✓	
	Trace	Start	✓		
	xDR	View	✓	✓	✓
		Field Hiding	✓	✓	✓
Alarm Viewer	Map	List/Execute			
	Alarm List	Terminate alarms			
Dashboard	Dashboard View	List/Execute	✓	✓	✓
SS& Surveillance	Counters	View	✓	✓	✓
		Reset	✓	✓	
Sigtran Surveillance	Counters	View	✓	✓	✓
		Reset	✓	✓	
On Demand UP Capture	Mobile Users	Add/Delete	✓	✓	
		Edit	✓	✓	
		Open/View	✓	✓	✓
		Upload	✓		
		Download	✓		
	APNs	Add/Delete	✓	✓	
		Edit	✓	✓	
		Upload	✓		
		Download	✓		
		Open/View	✓	✓	✓
Browser Export	Export	List/Download	✓	✓	

Table 6: Authorization Role Map for Applications

Application	Feature	Authority	Config Manager	Config Power user	Config User
Alarm Configuration	Configuration	All	✓		
Alarm Forwarding	Configuration	All	✓		
Browser Export Scheduler	Schedule	List	✓		
		Edit/Add/Delete	✓		
KPI	Start Configuration	Consult	✓		
		Create	✓		
		Update	✓		
		Change Rights	✓		
		Delete	✓		
	Applying Configuration	Consult	✓		
		Set	✓		
		Activate	✓		
		Deactivate	✓		
		Change Rights	✓		
		Delete	✓		
Historical KPI	Historical KPI	Create	✓		
		Modify	✓		
		Delete	✓		
		Export	✓		
Dashboard	Dashboard Configuration	Consult	✓	✓	✓
		Create	✓	✓	
		Update	✓	✓	
		Delete	✓	✓	
CCM	Host, Application, Session, Site, Dictionary	Consult	✓	✓	✓
		Modify	✓		
		Delete	✓		
	Applying Configuration	Activate	✓		
		Deactivate	✓		
		Set	✓		
		Delete	✓		
Mediation Data Feed	All functions	All	✓		

Table 7: Authorization Role Map for Configuration Applications

Object	Feature	Authority	Monitor Manager	Monitor Power User	Monitor User
System Alarm	Alarm	List	✓	✓	
		Terminate	✓	✓	
Audit Viewer	User's Actions	List/Filter	✓		

Table 8: Authorization Role Map for Surveillance Applications

Privacy Roles

Privacy roles establish the levels of access to the data objects used by the applications. Profiles link users to privacy roles, which in turn are linked to read/write/execute permissions for the data objects. A given object can offer different permission levels to different roles and indirectly to different profiles.

Object-data access privileges (read/write/execute) imply the following:

- Read (R) - Users can only view an object in a list. They cannot modify or add information in any way.
- Write (W) - Users can modify an object. Write includes read access. This also covers privacy privileges for that object.
- Execute (X) - Users can view, modify, or delete an object in a list

This information is used at the programming level with user authorization roles to define user profiles.

Application	Object Class	eXecute	Write	Read
Centralized Configuration Manager	Host	Run discover	Modify & delete	View attributes
	Applications, Data Server MSW, ICP, IMF	Run discover (when applicable)	Modify & delete	View attributes
	xDR session	N/A	Modify & delete	View attributes
	Dictionary, Protocol, Stack	N/A	N/A	N/A
	Session View	N/A	Modify & delete	View attributes
	Link View	N/A	Modify & delete	View attributes
	Network Elements	N/A	Modify & delete	View attributes
	Monitoring Groups	N/A	Modify & delete	View attributes
KPI Configuration	KPI Config	Apply/ activate/...	Modify	View configuration
	Statistic sessions	Open session	N/A	View session in list
	Alarms	N/A	N/A	(See privacy dependencies in Managing Object Privacy.)
Troubleshooting	xDR session	Open session	N/A	View session in list
	Session view	Open all sessions	N/A	View in list tree. (See privacy dependencies in Managing Object Privacy.)
	Link view	Open all sessions	N/A	View in list tree. (See privacy dependencies in Managing Object Privacy.)
	Queries	Execute query	Modify query	View and read query Save it with a new name
Dashboard	Dashboard	View dashboard	Modify config	View panel & KPI list in dashboard
Alarm	Filtering rules	N/A	N/A	N/A

Forwarding				
Alarm	Managed Objects	N/A	N/A	View object on map
	Maps	Display map	Configure map	View map in list
Browser Export Scheduler	Export file	N/A	Delete	Upload & download
	Task	N/A	Modify & delete	View

Table 9: Application Privacy Roles

Profiles

Profiles are structures that make it easier to grant users access to Management applications and data structures. A user is assigned to one profile, which defines the Authorization role and Privacy role for that user. Authorization roles define the user's access to Management applications and its features. Privacy roles link users to Management Application data objects.

Management Application Security Model

Profiles map users to privacy and authorization roles. Before users can access Management applications and data, the following must be defined:

- Users
- Each user is assigned to a profile
- Roles
- In profiles, privacy roles must be associated with users (data object access)
  In profiles, authorization roles must be associated with users (application/feature access) Legend

Figure 2: Profile Overview shows two different profiles linked to two separate sets of users in the hypothetical NET department. The NET department manages SS7 network surveillance. Some users need to perform configuration tasks and other users need to run pre-defined queries and pre-defined dashboards. For more on the hypothetical application of the Management Application Security Model, see **Profile 1** and **Profile 2** below.

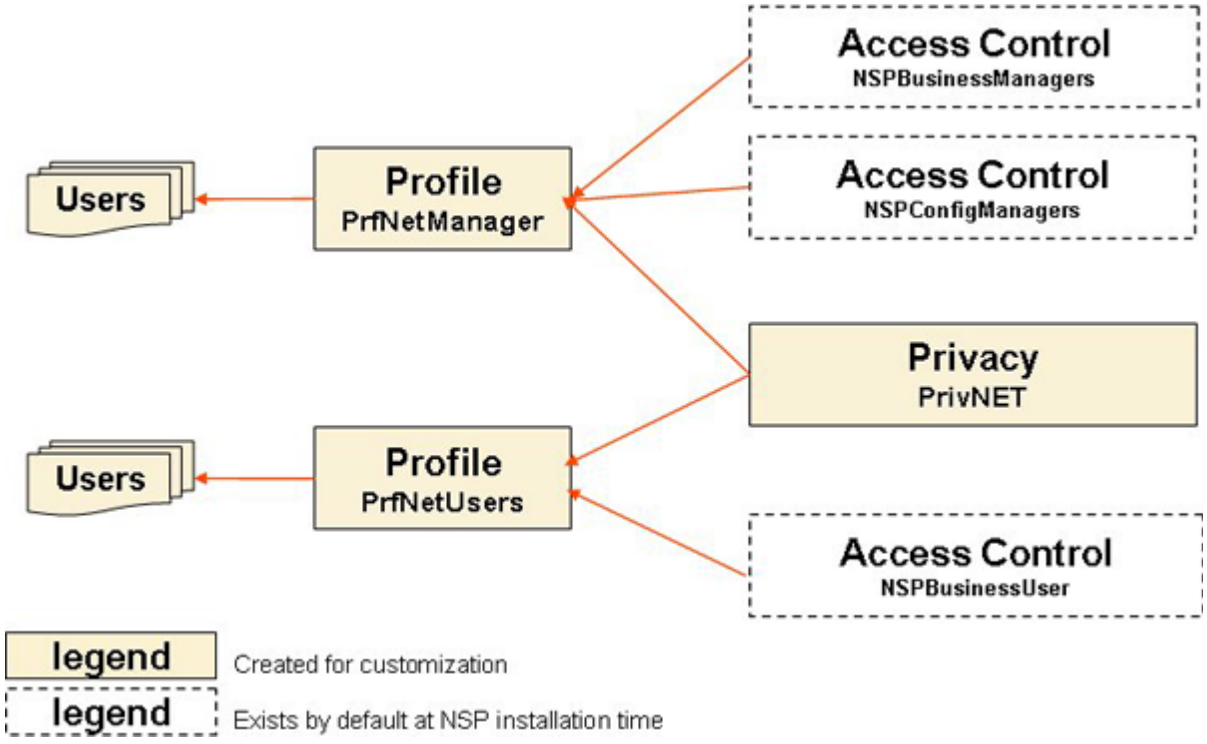

Figure 2: Profile Overview

Notes:

- A role can be mapped to more than one profile.
- A profile should include, at the minimum, one role for application/feature access and one role for data access.
- Many users can share the same profile.

For information on setting up Security in Management Application, see Chapter 3: Using Security Application

Profile 1
Profile - PrfNetManager
Access Control privileges - for authorization roles NSPConfigManager and NSPBusinessManager. (These roles have almost no restriction on feature access.)
Privacy role - PrivNET

Profile 2
Profile - PrfNetUsers
Access Control privileges - for authorization role NSPBusinessUser. (Users with this profile can execute queries on sessions and can view dashboards.)
Privacy role – PrivNET

Chapter 3: Using Security Application

Overview

Management Application Security features are created and managed directly through the Web interface using the Security application. Once profiles, roles, and users have been defined, you can configure Privacy settings for the data.
Users must be authenticated to use Management Application. A user is an individual or a group that has a unique userid and password.

Note: Do not use the Function Keys (F1 through F12) when using Management Application. Function keys work in unexpected ways. For example, the F1 key does not open Management Application help but opens the help for the browser in use. The F5 key does not refresh a specific screen, but refreshes the entire session and results in a loss of any entered information.

Opening the Security Application

To open the Management Application Security application, follow these steps:

Note: Management Application only supports latest versions of IE and Firefox. Before using Management Application, turn off the browser pop up blocker for the Management Application site.

- Log in to Management Application.
  The Application Board is displayed.

- Click the Security icon.
  The Security application is opened and the Users page is displayed.

Managing Users

In the Management Application Security application, you can manage users by

- Viewing users
- Adding users
- Modifying users
- Removing users

For more information about the role of users in Management Application Security, see Users

Viewing Users

The Management Application Administrator can see a list of all defined users on the Users page.

- In the Security menu, select **Security ► Users**.
  The Users page is displayed.

Note: The Users page is the default view when the Security application is activated.

Column Name	Description
User Name	The user's name as defined when the record is created.
Description	A brief explanation entered when the record is created.
Mail	The user's email address
Profile	The profile to which user is assigned. For more information, see Managing Profiles
Access Status	 Restricted access (user allowed to log in Management Application under controlled access conditions). This status is useful for troubleshooting.  Built-in (profile cannot be modified).  Locked (too many invalid login attempts). Use the unlock button to reset.  Inactive (password is expired). Use the reset password bottom to reset.  Externally managed user.
Last Login	Date and time stamp for user's most recent login.
Sessions	Number of tokens the current user has in use.

Table 10: Columns in the Users

Adding Users

The Management Application Administrator can add users for the Management applications. Complete these steps to create a new user.

- Click the **Add** Record icon. 
  The User settings window is displayed.
- Enter the appropriate values in the fields. The options are described below:

Field or Option	Explanation
Name	User Name. The system allows a maximum of 30 alphanumeric characters. Special characters (e.g., + or *) are not allowed, with the exception of a period (.) or hyphen (-).
Description	Optional description The system allows a maximum of 255 alphanumeric characters
Password	Initial password. Password settings may hide this field and require specific content (see Configuring Password Requirements) You can make up a password or click the Automatic password icon  for a system-generated password.
Confirm password	Confirm above password
Profile	Unique user profile from defined ones to give access rights to user (authorization and privacy)
Restricted access	Allowed login when system is in restricted mode (see Setting Access Level)

Table 11: User Properties

- Click Apply to save the data.

You are returned to the User page, and the new user record is displayed at the bottom of the Users list.

Modifying Users

The Management Application Administrator can modify existing user records.

- Select the user record to be modified. Click the **Edit** Record icon. 
- The User settings window is displayed with data fields populated.
- Make the necessary changes to the record.
- Adding Users for an explanation of the fields.
- Click Apply.
- The record displayed in the list reflects the changes.

Removing Users

The Management Application Administrator can remove user records. Complete these steps to remove a user.

Note: A user who owns objects cannot be deleted until the ownership is transferred. The following error message is displayed: "Unable to delete an owning user (try to transfer ownership)." To transfer ownership, see Changing Overall Ownership

- In the Security menu, select **Security ► Users**.
  The Users page is displayed.
- In the Users list, select the User record to be removed.
- Click the **Delete** Record icon. 
- Click OK at the prompt.
- The record for that User is deleted from the Users list.

Managing Privacy Roles

The Management Application Security application supports Privacy Role management through the following activities:

- Viewing Privacy Roles
- Adding Privacy Roles
- Modifying Privacy Roles
- Removing Privacy Roles

For more information about the purpose of Privacy Roles in Management Application Security, see Privacy Roles

Viewing Privacy Roles

The Management Application Administrator can view all defined Privacy Roles. Follow these steps to open the Privacy roles page:

- In the Security menu bar, select **Security ► Privacy Roles**.
  The Privacy roles list is displayed.

Column Name	Description
Role	The name of the privacy role as defined when the record is created.

Description	A brief summary entered when the record is created.
Users	The number of users granted this role through their profiles.
Objects	The number of data objects linked to this role.

Table 12: Privacy Roles Columns

Creating Privacy Roles

The Management Application Administrator can add new Privacy Roles. Complete these steps to create a Privacy Role:

- Click the Add Record icon 
  The Privacy role settings window is displayed.
- Enter the appropriate values in the fields. The options are described below:

Field or Option	Explanation
Name	Privacy role name
Description	Optional description

Table 13: Privacy Roles Properties

- Click **Apply** to save the Privacy role data.
- You are returned to the Privacy roles page, where the new record is listed.

Modifying Privacy Roles

The Management Application Administrator can modify existing Privacy Role records. Complete these steps to modify a privacy role:

- Select the Privacy Role record to be modified.
- Click the Edit Record icon 
- The Privacy roles settings window is displayed with data fields populated.
- Make the necessary modifications.
- Click Apply to save the updated information. You are returned to the Privacy roles page, where the list reflects the changes.

Removing Privacy Roles

The Management Application Administrator can remove Privacy Roles. Complete these steps to remove a privacy role:

- Select the Privacy Role record to be removed.
- Click the Delete Record icon.
- Click OK at the prompt.
  The Privacy roles list is modified to remove the record.

Managing Profiles

The Management Application Security application supports Profile management through the following activities:

- Viewing Profiles
- Adding Profiles

- Modifying Profiles
- Removing Profiles

For more information about profiles in Management Application Security, see Profiles

Viewing Profiles

The Management Application Administrator can view all defined profiles.

- In the Security menu bar, select **Security ► Profiles**.
  The Profiles list is displayed.

The three columns in the Profiles page are described below:

Column Name	Description
Profile Name	The name given to the profile when the record is created
Description	A brief summary entered when the record is created
Users	The number of users assigned to each profile

Table 14: Columns in Profiles List

Creating Profiles

The Management Application Administrator can create new profiles. Authorization roles and privacy roles are assigned to a profile in the system (but are not visible in the profile record in the Profiles listing). Complete these steps to create a profile:

- Click the Add Record icon 
  The Profile settings window is displayed with the General page active by default.
- Enter the appropriate values in the fields. The options are described below:

Field or Option	Explanation
Name	Profile Name. The system allows a maximum of 30 alphanumeric characters. Special characters (e.g., + or *) are not allowed, with the exception of a period (.) or hyphen (-).
Description	Optional description
Authorization	Predefined authorization roles to access features
Privacy	Custom privacy roles to access data
Applications	Application from authorized list (according selected authorization roles) to be excluded

Table 15: Privacy Roles Properties

- Click Apply to save the profile data.
  The new record is displayed at the bottom of the Profiles list.

Modifying Profiles

The Management Application Administrator can modify existing profile records. Complete these steps to modify a profile:

- In the Security menu bar, select **Security ► Profiles**.
- Select the record to be modified.

- Click the Edit Record icon 
- The Profile settings window is displayed.
- Make the necessary modifications.
  See previous paragraph for information on the options in the Profile Setting Window.
- Click Apply to save the updated information. The record, with changes, is displayed in the list.

Removing Profiles

The Management Application Administrator is permitted to remove profile records. Complete these steps to remove a profile.

- In the Security menu bar, select Security ► Profiles.
- Select the record in the list to be modified.
- Click the Delete Record icon. 
- Click OK at the prompt. The profile is deleted.

Managing Object Privacy

When a user tries to access an object in an Management Application, Management Application checks access rights. Access rights are established by one of the following:

- System defaults (RWX for owner and administrator), or
- Settings customized by the object owner

Note: R=Read, W=Write, and X=eXecute.

Privileges for one object are automatically calculated based on other related objects. One change in Privacy for an object can be cascaded to many others. Thus, to perform a task,

Object	Dependency
Node	Signaling Point (SP)
Signaling Point	Connected Linksets
Network View	Contained XDR session or view
Statistic session	KPI configuration
KPI alarms	KPI configuration

Table 16: Privacy Dependencies in Management Application

You may have to verify privileges of multiple objects. This chain of Privacy is called "Privacy dependencies."
The following tables list the cases in which there is a Privacy dependency.

Object	Configure	Execute	Comment
Session	R	R+X	Applies to all sessions of the view if the view is used
Query	R+W	R+X	N/A

Table 17: Configure and Execute a Query

Object	Configure	Execute	Comment
Dashboard	R+W	R+X	N/A

Session	R	R	N/A

Table 18: Configure and Display Dashboard

Object	Configure	Comment
KPI Configuration	R+W	N/A
Session	R	N/A
IXP	R	N/A

Table 19: Associate a KPI Configuration

Object	View	Comment
Map	R+X	N/A
Managed Object	R	N/A

Table 20: View Alarms in Map

Note: If a case is not listed in one of the tables, the object just depends on Simple Privacy.

Viewing Data Objects

The Management Application Administrator can display summary records for all defined data objects. When data objects are created in Management applications (for example, maps in Alarm Configuration), the Security application adds the object records to a list. When the owner removes that object, the object's record is removed from the list. Complete these steps to view a list of data objects:

- Select **Security ► Objects**.
  The Objects list is displayed.

Column Name	Description
Object	The name of the object as defined when the record is created.
Type	A brief summary entered when the record is created.
Owner	The user who creates the object or to whom ownership is transferred. The owner has full access privileges to that record.
State	The status of the object: M=Modified, N=Normal, O=Obsolete.
Created	Date stamp showing when the object was created.

Table 21: Columns in Object List

Setting Default Privileges for Objects

See Quick Start Guide Chapter 2, Setting Default Object Privacy

Changing Object Privacy

The Management Application Administrator and data object owners can modify existing Object Privacy settings using the Security application. The Administrator has access to all listed objects. The owner has access to those records which identify him or her as the owner.
Complete these steps to change data object access privileges.

- In the Security menu bar, select **Display ► Objects**.
  The Objects page is displayed.
- Select the Object record or records.
  If you are using Internet Explorer, select multiple records by pressing CTRL while selecting the records.
- Click the Privacy icon. 

- The Change privacy window is displayed.
  Note: If an individual record is selected, the current settings are shown. If multiple records are selected, the initial view of the settings shows unselected boxes because the individual settings vary.

- Click the box for the appropriate Privacy setting.
- Click Apply to save the changes.

Managing Login

The Management Application Security Application supports user authentication in the following activities:

- Configuring passwords
- Setting restricted access groups
- Monitoring purchased tokens (licenses)
- Setting the Security notice

For more information about user authentication, see Management Application Security Model

Configuring Password Requirements

The Management ApplicationAdministrator can set password requirements for the Management Application system, including number and type of characters, lifetime of the password before it must be changed, and whether it is generated manually or automatically.

- In the Security Menu, select **Action ► Password Settings**.
  The Password settings dialog is displayed.
- Enter the appropriate values in the fields. The options are described below:

Field or Option	Explanation
Minimum length	Minimum number of characters for password; must be at least 8.
Check quality	Defines what aspects of the password the system should check: default is to check on password length and strong is to check length, mix of characters, and history. "Mix" must include uppercase and lowercase letters, numbers, and special characters. "History" check means the password has not been used for the last x times.
History size	Number of previously used passwords to check for (in Check quality).
Minimum age	Minimum delay between two password changes. (To change the password again, the user must wait at least this amount of time.)
Maximum age	Password lifetime before it expires.
Grace period	Delay for changing expired password. After the password expires, the grace period allows the user to login, but requires the password to be changed. After the password expires, and after the grace period expires, the user will not be able to login (the account is locked).
Expire warning	Time (prior to password expiration) when the user begins to get warning notices.
Mode	Defines whether a password (initial or reset) is set manually or automatically.
Must change	Denotes whether a password (initial or reset) is temporary. A temporary password must be reset when the user first uses it.

Table 22: Password Settings

- Click **Apply**.
  The settings are saved.

Resetting User Passwords

The Management Application Administrator uses the **Security ► Users** page in Management Application to reset passwords. To reset a password,

- In the Security Users page, click a User Name in the list of Users. 2.
- Click the reset password icon. 
- The Password Reset dialog is displayed with the current user Name already filled in.
- Type the password in the Password field.
- You can make up a password or click the Automatic password icon  for a system-generated password.
- Type the same new password in the Confirm password field
- Click Apply.
  - The change takes effect the next time the user logs in to Management Application.

Setting Access Level

This procedure gives the Management Application Administrator the ability to restrict access to the Management Application system at login. Users with restricted access can use the system even when access is being controlled. Complete these steps to set the access level for a user.

- In the Security menu, select **Action ► Filter access**.
- To restrict access, select Restricted access users in the drop-down menu. To allow unrestricted access, select All users in the drop-down menu. (All users is the default.)
- Click Apply.
  The change takes effect the next time the user logs in to Management Application.

Monitoring Purchased Tokens (Licenses)

The Management Application Administrator can view system settings for the number of purchased tokens (licenses), the maximum number of tokens allowed per user, and the session timeout. These tokens are assigned to active sessions and control the number of simultaneous users. The session timeout setting ranges from 15 minutes to 8 hours. The session timeout default setting is 1 hour.

Note: The information in the Tokens window cannot be modified in this window. This is a view-only window.

To view the Tokens dialog, perform the following steps:

- In the Security menu, select Action ► Manage tokens.
  The Tokens dialog is displayed.
- Management Application service user may be allowed to enter new value according current contract. Value can only be incremented.
- Click Close to close the window.

Forcing Disconnect

The Management Application Administrator is able to free user tokens (licenses) by forcing disconnection of users.

- In the Security Users page, select the user to be disconnected.

- Click the Logout icon  in the Security toolbar to disconnect the user from the active Management Application session.
- The disconnected user's screen displays an error message on its next Web update. The system returns the session's tokens to the token pool.

Setting the Security Notice

The Management Application Administrator can modify the Security Notice, which is displayed on the login page.

- In the Security menu, select Action ► Security Notice.
  The Security notice window is displayed.
- Enter the appropriate values in the fields. The options are described below:

Field or Option	Explanation
Notice	Text displayed in login page as general security warning. By default: "This is a private computer system. Unauthorized access or use may lead to prosecution". The system allows only 255 alphanumeric characters.
System identifier	Text displayed in page header to identify Management Application system (in case customer has multiple system)

Table 23: Security Notice Properties

- Click Apply.

Transferring Ownership

The Management Application Administrator can change ownership for one or more data objects owned by a particular user. For example, an individual has left the company and a different employee needs to take over all the objects.
The Management Application Administrator can also change the ownership for a selected object or objects. For example, an individual has shifted responsibilities and another employee needs to take over the affected rights.

Changing Overall Ownership

The Management Application Administrator can change ownership for all of an individual's objects. To change the owner Privacy rights, complete the following steps.

- In the Security menu bar, select **Action ► Transfer ownership**.
  The Privacy owner change window is displayed.
- Select the current owner from the Current Owner drop-down list.
- Select the new owner from the New Owner drop-down list.
- Click Apply.

The changes are saved. All of the previous owner's objects are now under new ownership.

Changing Ownership by Object

To change the owner Privacy rights by object, follow these steps:

- In the Security menu bar, select **Display ► Objects**.
  The Objects list is displayed.
- Select the object record or records for which the ownership is to be changed.
- Click the Owner icon. 

- The Privacy owner change window is displayed.
- Select the new owner from the New Owner drop-down list.
- Click Apply.
  The changes are saved. Ownership for the selected record(s) is changed.

Note: This procedure is different from changing all objects from one owner to another. See Changing Overall Ownership.

APPENDIX A: My Oracle Support

MOS (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select 2 for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

MOS is available 24 hours a day, 7 days a week.