Unified User Management System Guide

7.13.2

Tektronix communications

Copyright

Tektronix Communications
3033 W President George Bush Highway
Plano, Tx 75075 USA
+1 469-330-4000 (voice)
www.tektronixcommunications.com

992-0453-08-001-140228

Customer Support

Plano, Texas USA - serves North America, South America, Latin America
+1 469-330-4581 (Customer Support voice)
uaservice@tek.com (Customer Support USA email)

London, England UK - serves Northern Europe, Middle East, and Africa
+44-1344-767-100 (Customer Support voice)
uaservice-uk@tek.com (Customer Support UK email)

Frankfurt, Germany DE - serves Central Europe and Middle East
+49-6196-9519-250 (Customer Support voice)
uaservice-de@tek.com (Customer Support DE email)

Padova, Italy IT - serves Southern Europe and Middle East
+39-049-762-3832 (Customer Support voice)
uaservice-it@tek.com (Customer Support IT email)

Melbourne, Australia - serves Australia
+61-396-330-400 (Customer Support voice)
uaservice-ap@tek.com (Customer Support APAC and Australia email)

Singapore - serves Asia and the Pacific Rim
+65-6356-3900 (Customer Support voice)
uaservice-ap@tek.com (Customer Support APAC and Australia email)

Table of Contents

What's New in UUMS 7.13.2? **10**

Chapter 1 UUMS Architecture and Components **11**

Unified User Management System Architecture 11

Unified User Management System Components 12

UUMS Components 12

User Management Dashboard 12

User Management Components 12

Chapter 2 Workflows **13**

UUMS Workflows 13

UUMS Configuration Workflows 13

UUMS Configuration Workflow for Iris LDAP 14

UUMS Configuration Workflow for Existing (Corporate) LDAP 15

Assigning Licensable User Roles 16

To Assign a Licensable User Role 16

Configuring UUMS for an Existing LDAP 17

To Configure Existing LDAP Settings 17

To Provision Users 17

User Management Workflows 18

User Management Workflow for Iris LDAP 18

User Management Workflow for Existing (Corporate) LDAP 19

Role Management Workflow for Iris and UACN/RIA 20

Role Management Workflow 20

Role Management Workflow for GeoProbe 21

Geo Role Management Workflow 21

Activity Log Workflow 22

Activity Log Workflow 22

Chapter 3 User Interface **23**

UUMS User Interface 23

User Management Dashboard 24

Status Bar 24

User Management Dashboard 25

User Management Window 26

Status Bar 26

User Management 27

Users Pane 27

Columns 27

Column Filter Controls 28

User Pane Controls 28

Users Pane 29
Users Pane Inactivity 29
Viewing Inactive Accounts 29
Configuration Controls 30
User Details Pane 31
User Details Pane Controls 32
User Details Area 32
Authorization Area 33
Role Selection Area 33
User Details Pane 34
Password Area (Iris LDAP) 35
Authorization Pane 36
Authorization Pane 36
Role Selection Pane 36
Role Selection Pane 37
Import LDAP Users Dialog Box 38
Columns 38
Column Filter Controls 38
Search Filter Controls 38
Role Selection Area 38
Import LDAP Users Dialog Box 39
User Management Configuration Window 40
User Management Tabs 40
Configuration Controls 40
User Management Configuration (Iris LDAP) 41
General Tab 42
Configuration Controls 43
General Tab (Existing LDAP) 44
General Tab (Iris LDAP) 45
Password Policy Tab 46
Configuration Controls 46
Password Policy Tab 47
Password Quality Tab 48
Configuration Controls 48
Password Quality Tab 49
Subsystem Defaults Tab 50
Preferences Pane 50
Configuration Controls 50
Subsystem Defaults Window 51

Login Advisory 52
Advisory Message Area 52
Window Controls 52
Advisory Message Area 53
Login Advisory Message Example 54
Digit Masking 55
Digit Masking Area 55
Configuration Controls 55
Digit Masking Area 56
Geo User Settings 57
Geo User Settings Area 57
Configuration Controls 57
Geo User Settings Area 58
Subsystem Access 59
Subsystem Enabled Area 59
Configuration Controls 59
Subsystem Access Area 60
Default Synchronization 61
Synchronization Area 61
Configuration Controls 61
Synchronization Area 62
User Inactivity 63
Interval Configuration Area 63
Configuration Controls 63
User Inactivity Area 64
Synchronization Tab 65
Configuration Controls 65
Synchronization Tab 66
UUMS Role Management 67
Role Management Tabs 67
Role/Profile Pane 67
Role Area Controls 67
Role or Profile Management Pane 68
Role Management Window 69
Role Management Window 69
Iris Role Management Window 70
Role Pane Controls 70
Iris Role Management Window 71
Iris Licensable Role Management Window 71

UACN/RIA Role Management Window 71
Role Pane Controls 72
UACN/RIA Role Management Window 72
Role Details Pane 72
Role Details Pane Controls 73
Members Area 73
Privileges Selection Area 73
Role Details Pane Example 74
Geo Role Management Tab 75
Geo Role Management Window 75
Geo Role Management Profiles Tab 75
Profile Pane Controls 76
Geo Role Management Window Profiles Tab 76
Profile Details Pane 77
Profile Details Pane Controls 77
Members Area 77
Classmarks Selection Area 77
Profile Details Pane Example 78
Geo Role Management Administration Groups Tab 79
Admin Group Pane Controls 79
Geo Role Management Window Administration Groups Tab 79
Geo Role Management Alarm Groups Tab 80
Alarm Group Pane Controls 80
Geo Role Management Window Alarm Groups Tab 81
Group Pane 82
Group Area Controls 82
Group Management Pane 82
Assign Users Pane 82
Assign Users Pane Controls 83
Members Area 83
Assign Users Pane Example 84
Activity Log Window 85
Activity Log Window 85
Filters Pane 85
Filters 86
Filter Controls 86
Filters Pane 86
Log Browser 86
Columns 87

Column Filter Controls 87
Browser Controls 87
Log Browser 87
Column Filter 88
Export Dialog Box 88
Export Dialog Box 88
Chapter 4 References 89
UUMS References 89
Inactivity Timeout 89
Enforcing Login Inactivity Time 89
User Inactivity Area 90
User Management Window Example 91
UUMS Supported LDAPs 92
User Management Functions 92
Setting Up GeoProbe User Accounts for Iris ISA and PA Applications 93
TMF615 API 94
UUMS User Privileges and Roles 95
Available Subsystem Privileges 95
Default Roles 95
Iris Role Management Example 96
Iris User Privileges 96
UACN/RIA Roles and Privileges 101
Cognos Roles and Privileges 103
GeoProbe Classmarks 104
myIrisView Roles 108
Activity Types 109
Activity Log Storage and Aging 109
Export File Formats 110
File Format Details 110
Sample CSV File (ACTIVITY-LOGS-20110714-145600-20110715-145659.csv) 110
Sample PDF File (ACTIVITY-LOGS-20110714-145600-20110715-145659.pdf) 110
Account Migration Rules 111
Role and Privilege Migration 112
Relationship Types Imported 112
Import UACN/RIA Users, Roles and Privileges 113
Define Users Example 113
Define Roles Example 113
Defined Privileges Example 113
Import GeoProbe Users, Profiles, Classmarks, and Groups 114

Define Users Example 114
Define Alarm Groups Example 114
Define Administration Groups Example 115
Define Profiles Example 115
Define Classmarks Example 115
Password Migration 116
Password Reset Prompt Window 116
Single System Administrator Functions 116
System Administrator Access 116
Functions of the System Administrator 117
CLI Commands 117

What's New in UUMS 7.13.2?

Feature ID	Description	Section
F-02250	**SIP Message with SMS Full Content Stored Short-term** A new SMS Full Content privilege has been added to enable full SMS payload content, within SIP messages, to be stored in the G10 probe for a short-term duration and is only visible with the PA and ISA application. This allows PA and ISA users to see all SMS content for troubleshooting purposes.	Iris User Privileges

Chapter 1 UUMS Architecture and Components

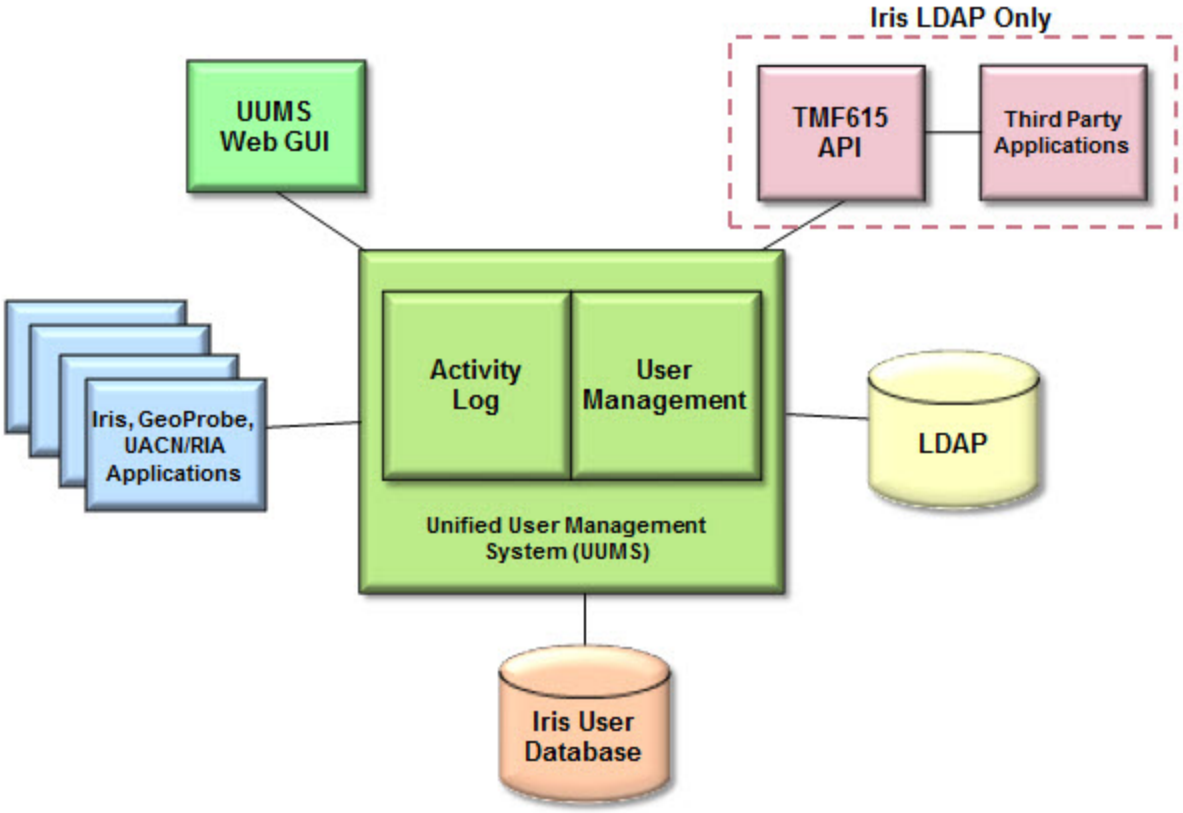
This chapter provides an overview about UUMS system architecture and system components.

Unified User Management System Architecture

UUMS enables system administrators to provision users for the Iris system. UUMS includes the following components:

- UUMS - engine that controls the following components:
  - User Management - processes user data and manages data storage and retrieval for use in Iris and third party applications.
  - Activity Log - provides detailed history of user activities for Iris applications.
  - Role Management - provides user access privileges by functional roles.
- UUMS Web GUI - provides the main user interface for provisioning Iris users.
- LDAP - UUMS supports two LDAP options
- Iris User Database - stores all user credentials (excluding passwords) regardless of implemented LDAP
- Iris, GeoProbe, and UACN/RIA applications - UUMS provides user authentication, authorization and audit logging for the Iris, GeoProbe, and UACN/RIA applications.
- TMF615 API - UUMS supports remote user management using the TMF615 interface when the Iris LDAP is implemented.

Click on any of the following UUMS components for more details.



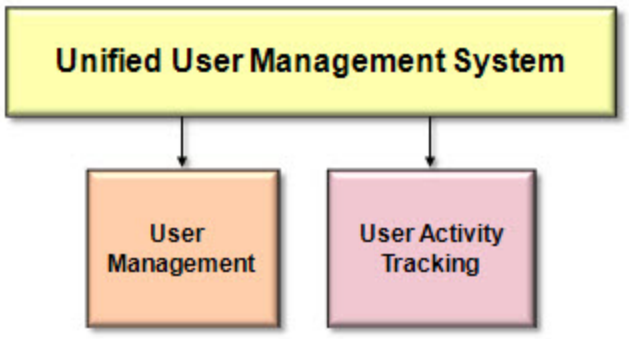
Unified User Management System Components

UUMS enables system administrators to perform the following tasks:

- Configure UUMS and provision user profiles and access
- Track user activities using the Activity Log

UUMS Components

Click on the components in the following graphic to view additional details.



User Management Dashboard

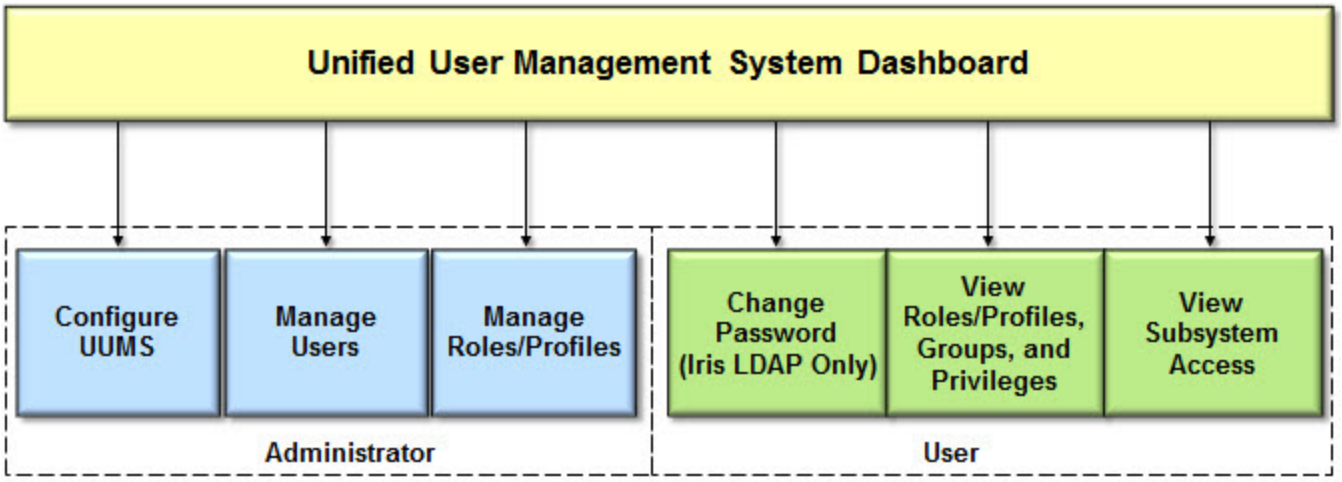
User Management enables system administrators to perform the following tasks:

- Configure settings including LDAP server settings, password policies and password qualities for Iris LDAP, default inactivity timeout, default user settings, default subsystem access, default synchronization, and an advisory login message
- Manage user profiles and assign user roles and privileges

User Management enables users to view their user data, currently defined roles, and to change their password.

User Management Components

Click on the Admin components in the following graphic to view additional details.



Chapter 2 Workflows

This chapter provides diagrams for UUMS and Activity Log workflows.

UUMS Workflows

Click on these workflows for step-by-step instructions:

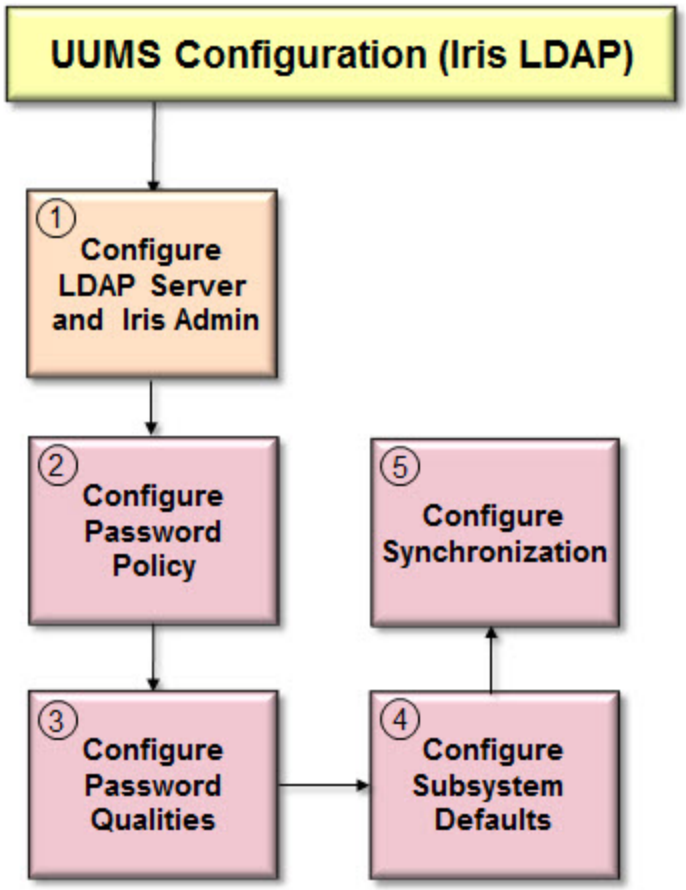
User Management	• Configuration Workflows • User Management Workflows • Role Management Workflow • GeoProbe Role Management Workflow
Activity Log	• Activity Log Workflow

UUMS Configuration Workflows

The UUMS Configuration window enables you to manage LDAP server settings, define global password policy and quality settings for Iris LDAP, and set up the security advisory login and inactivity timeout for all users. You access this window by clicking the Configuration button on the User Management window status bar. The configuration workflow differs depending on which LDAP is implemented.

Additional configuration for Users and Roles is available from the Role Management window.

UUMS Configuration Workflow for Iris LDAP

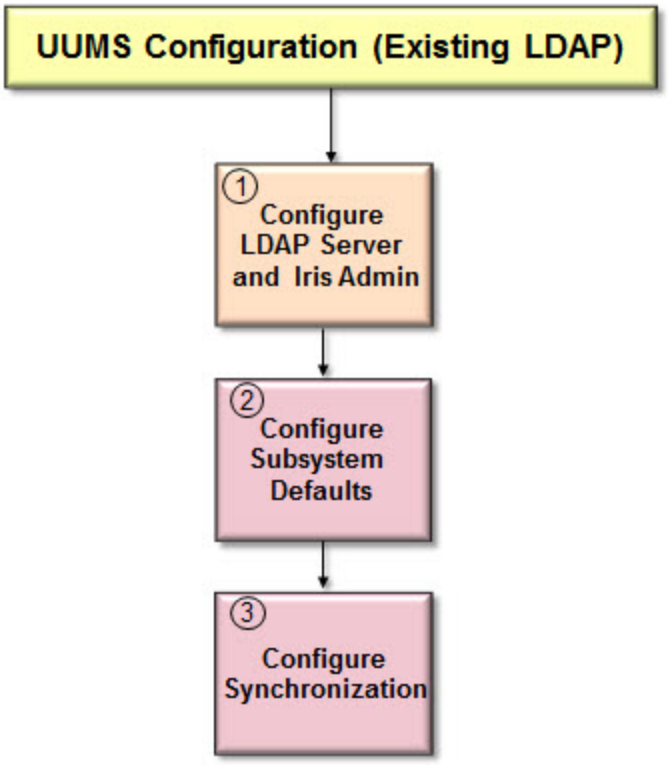


The following steps describe the UUMS Configuration workflow for the Iris LDAP.

1. Tektronix configures the LDAP server and an Iris Admin during system installation. You can modify these settings on the General tab of the Configuration window.
2. Set global password policy parameters relating to password expiration and user account lockout.
3. Set password quality parameters relating to password length and form.
4. Configure the subsystem defaults for the advisory message, Geo user settings, digit masking and user content visible, subsystem access, and inactivity timeout.
5. Configure synchronization between UUMS, GeoProbe, and UACN/RIA users.

Refer to User Management Workflows for user provisioning details.

UUMS Configuration Workflow for Existing (Corporate) LDAP



The following steps describe the UUMS Configuration workflow for an Existing (Corporate) LDAP. See Configuring UUMS for an Existing LDAP.

1. Configure your LDAP server settings and define an Iris Admin on the General tab.
2. Configure the subsystem defaults for the advisory message, Geo user settings, digit masking and user content visible, subsystem access, and inactivity timeout.
3. Configure synchronization between UUMS, GeoProbe, and UACN/RIA users.

Refer to User Management Workflows for user provisioning details.

Assigning Licensable User Roles

This topic illustrates how to assign myIrisView and Cognos user roles with license enforcement.

Each Cognos user role has a separate license, and you cannot assign a user to a Cognos role or the myIrisView role unless there are available licenses. In addition, if the license is not configured on the system, it does not display in the Role list.

To Assign a Licensable User Role

1. On the Iris Role Management window, click on the myIrisView role or one of the four Cognos roles available: Business Analyst, Consumer, Professional, or Web Administrator.
2. In the Role Details section, the list of users displays, along with an indication of the number of licenses available and the number of users assigned to that license.
3. Place a check mark next to the user you wish to assign to this role. The number of users assigned to the license increases by one. If the number of users assigned to the role exceeds the number of licenses available, you receive a tooltip indicating that there are no more licenses left. You need to un-assign some other user from this role before it can be re-assigned.

Configuring UUMS for an Existing LDAP

This use case illustrates how to configure UUMS to support your existing corporate LDAP.

If converting from the Iris LDAP server to an external LDAP server, Tektronix recommends backing up the Iris LDAP data; contact Customer Support for details.

To Configure Existing LDAP Settings

1. On the User Management window, click the Configuration button to open the UUMS Configuration window.
2. Select **Existing LDAP** to configure your specific external LDAP server.
3. Configure the parameters on the General tab using the settings from your existing LDAP. Use the Test Connection button to test the login for LDAP write authentication.
4. Click the Subsystem Defaults tab to configure an advisory login and inactivity timeout.
5. Click the **Submit** button to submit the LDAP and Advisory message settings.

The original admin account Tektronix assigned you is deactivated and the user you define in the LDAP Admin User Selection area is assigned admin privileges.

To Provision Users

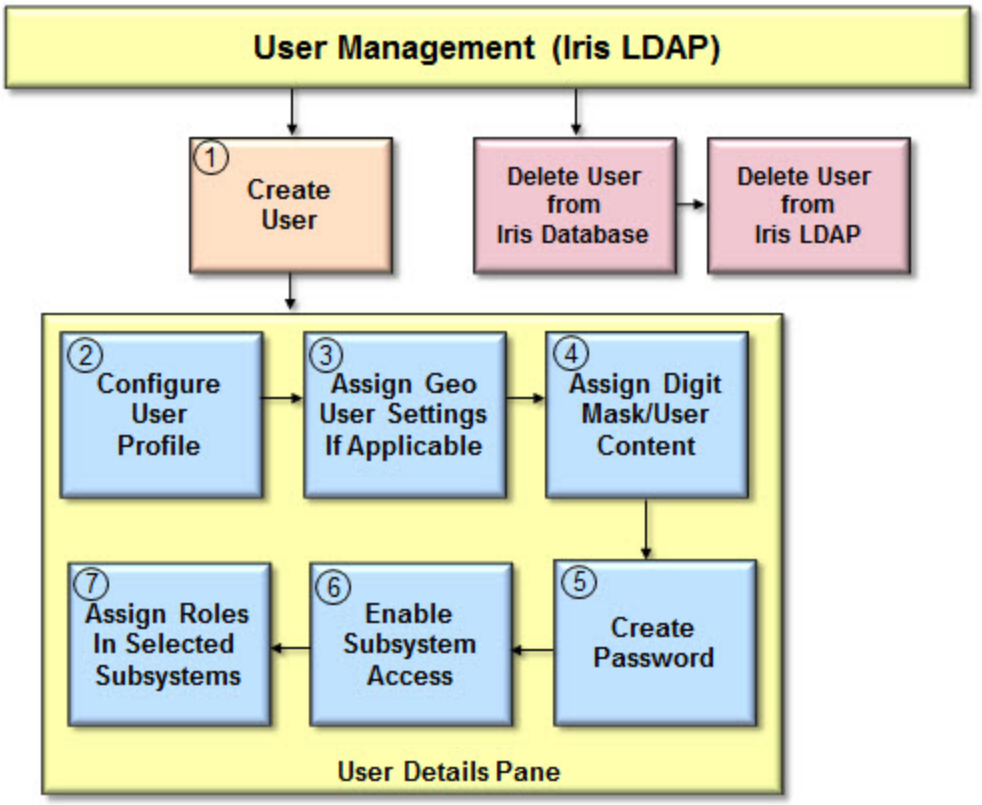
1. On the User Management window, click the **Import Users** button to open the Import LDAP Users Dialog Box.
2. Select the users you want to import. You can use the search filters to find users.
3. Assign user roles to configure the selected users' access to the system. If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary on the GeoProbe system.
4. After import, you can modify the user profile or the assigned roles in the User Details Pane as needed. By default, imported users are enabled.

User Management Workflows

The User Management window enables you to provision user profiles and user access, as well as create and manage roles for user access. The workflow differs depending on which LDAP is implemented.

If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary on the GeoProbe system.

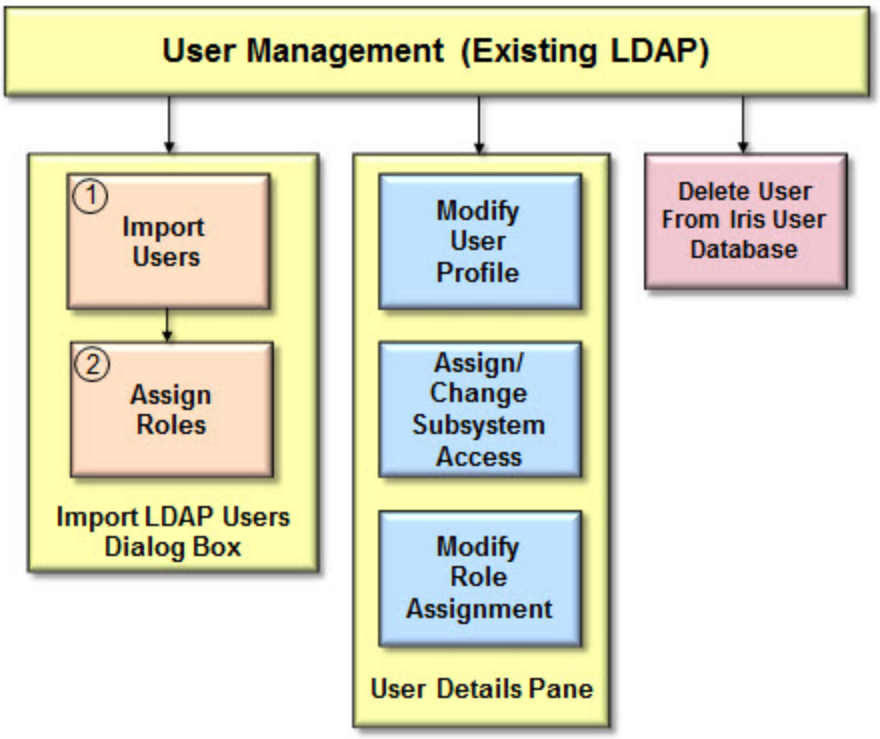
User Management Workflow for Iris LDAP



The following steps describe the User Management workflow for the Iris LDAP.

1. Click the Create User button to open a blank User Details Pane.
2. Configure user details including User ID and email address.
3. Assign the GeoProbe user settings, if applicable.
4. Assign digit masking and user content visible settings.
5. Create a new password for the user using the rules configured in the Password Quality tab. You can create a password policy to force the user to reset their password on their first login.
6. Enable subsystem access; available options are Iris, UACN/RIA, and GeoProbe. If a user is enabled on one subsystem, the Enabled column in the User Pane shows a green checkmark.
7. Assign user roles (or in the case of GeoProbe assign profiles) to configure the user's privileges or classmarks for each subsystem to which they have access.

User Management Workflow for Existing (Corporate) LDAP



The following steps describe the User Management workflow for an Existing LDAP.

1. Click the Import Users button to open the Import LDAP Users Dialog Box. Select the users you want to import. You can use the search filters to find users.
2. Assign user roles to configure the selected users' access to the system.

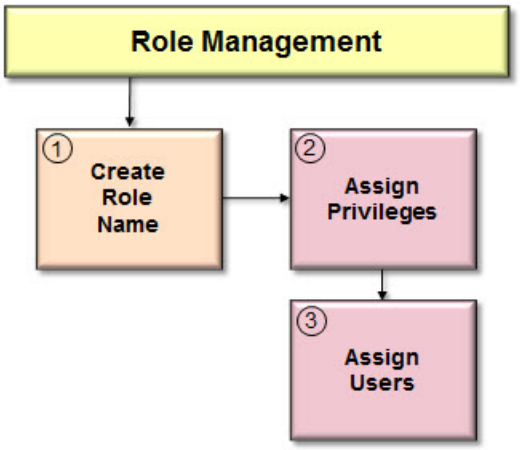
After you import the users, you can modify the user profile or the assigned subsystems and roles in the User Details Pane as needed. By default, imported users are enabled.

Role Management Workflow for Iris and UACN/RIA

The Role Management window enables you to create roles with assigned privileges for Iris and UACN/RIA and manage roles for user access.

If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary.

Role Management Workflow



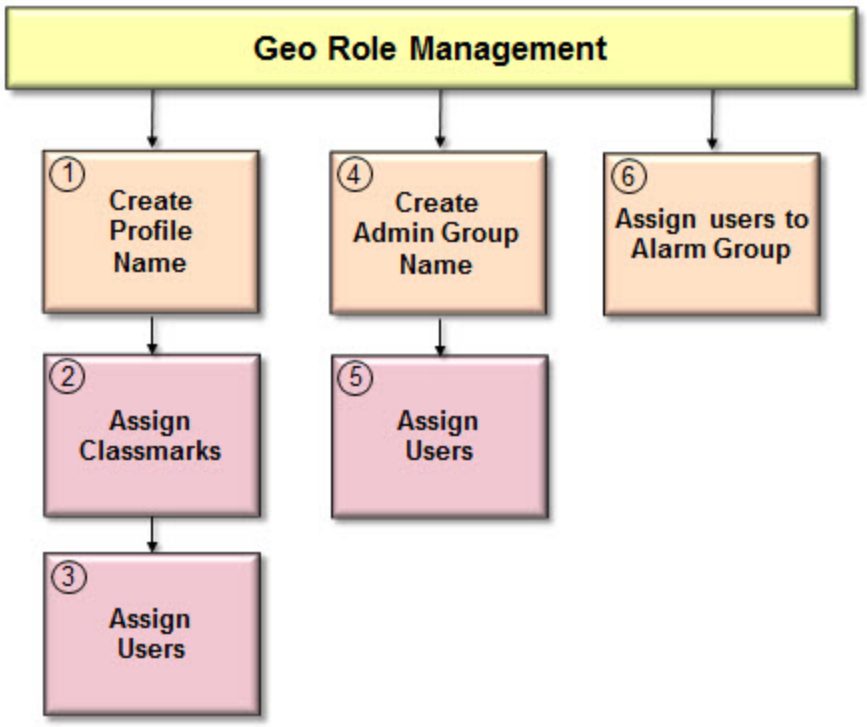
The following steps describe the Role Management workflow.

1. Click the Create button and enter a new role name and optional description in the dialog box. A new role is created with no privileges assigned.
2. Assign privileges to the new role by placing a checkmark next to the privilege in the Privileges area.
3. Assign users to the role by placing a checkmark next to the user name in the Role Details pane..

Role Management Workflow for GeoProbe

The Geo Role Management window enables you to create GeoProbe profiles with assigned classmarks and manage profiles for user access. In addition, you can create and manage administration groups, and manage alarm groups.

Geo Role Management Workflow



The following steps describe the Geo Role Management workflow.

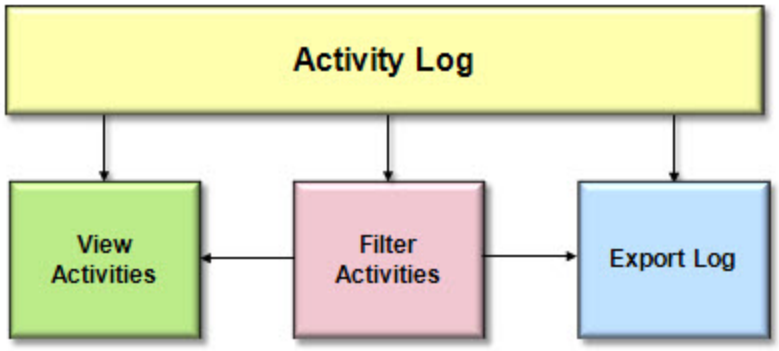
1. Click the Create button and enter a new profile name in the dialog box. A new profile is created with no classmarks assigned.
2. Select a profile and assign classmarks by placing a checkmark next to the classmark in the Classmarks area.
3. Assign users to the profile by placing a checkmark next to the user name in the Profile Details pane.
4. Click on the Administration Group tab, then click the Create button and enter a new Admin Group name in the dialog box. A new group is created.
5. Assign users to the group by placing a checkmark next to the user name in the Assign Users pane.
6. Click on the Alarm Group tab, select an alarm group, and assign users to the group by placing a checkmark next to the user name in the Assign Users pane.

Activity Log Workflow

The Activity Log is a key security and audit component for the Iris system. The Activity Log provides the following features:

- Secure access to a detailed system and user activity history
- Filters for isolating user activity in specific areas of the system
- Export option for saving select log messages for further examination

Activity Log Workflow



The following steps describe the Activity Log workflow.

1. Launch the Activity Log by clicking Admin on the IrisView toolbar and clicking Activity Log from the drop-down menu. The Activity Log appears displaying all log entries for the previous 24 hours.
2. Apply Activity Log filters, as needed, to view user activity for areas of interest. Filters are dynamic; selecting an option in one filter only displays related options in subsequent filters. Filters are data driven; options are only available for data that exists in the database.
3. Export log data to a CSV or PDF file.

Chapter 3 User Interface

This chapter provides a description of the UUMS UI.

UUMS User Interface

UUMS contains the following GUI components.

User Management	• User Management Configuration Window
	  • General Tab
	  • Password Policy Tab
	  • Password Quality Tab
	  • Subsystem Defaults Tab
	  • Synchronization Tab
	• User Management Window
	  • Users Pane
	  • User Details Pane
	  • Import LDAP Users Dialog Box
	  • Authorization Pane
	  • Role Selection Pane
	• Role Management Window
	  • Iris Tab
	  • UACN/RIA Tab
	  • Role Pane
	  • Role Details Pane
	  • Geo Role Management Tab
	  • Profiles Tab
	  • Administration Groups Tab
	  • Alarm Groups Tab

Activity Log	• Activity Log Window
	  • Filters Pane
	  • Log Browser
	  • Export Dialog Box

User Management Dashboard

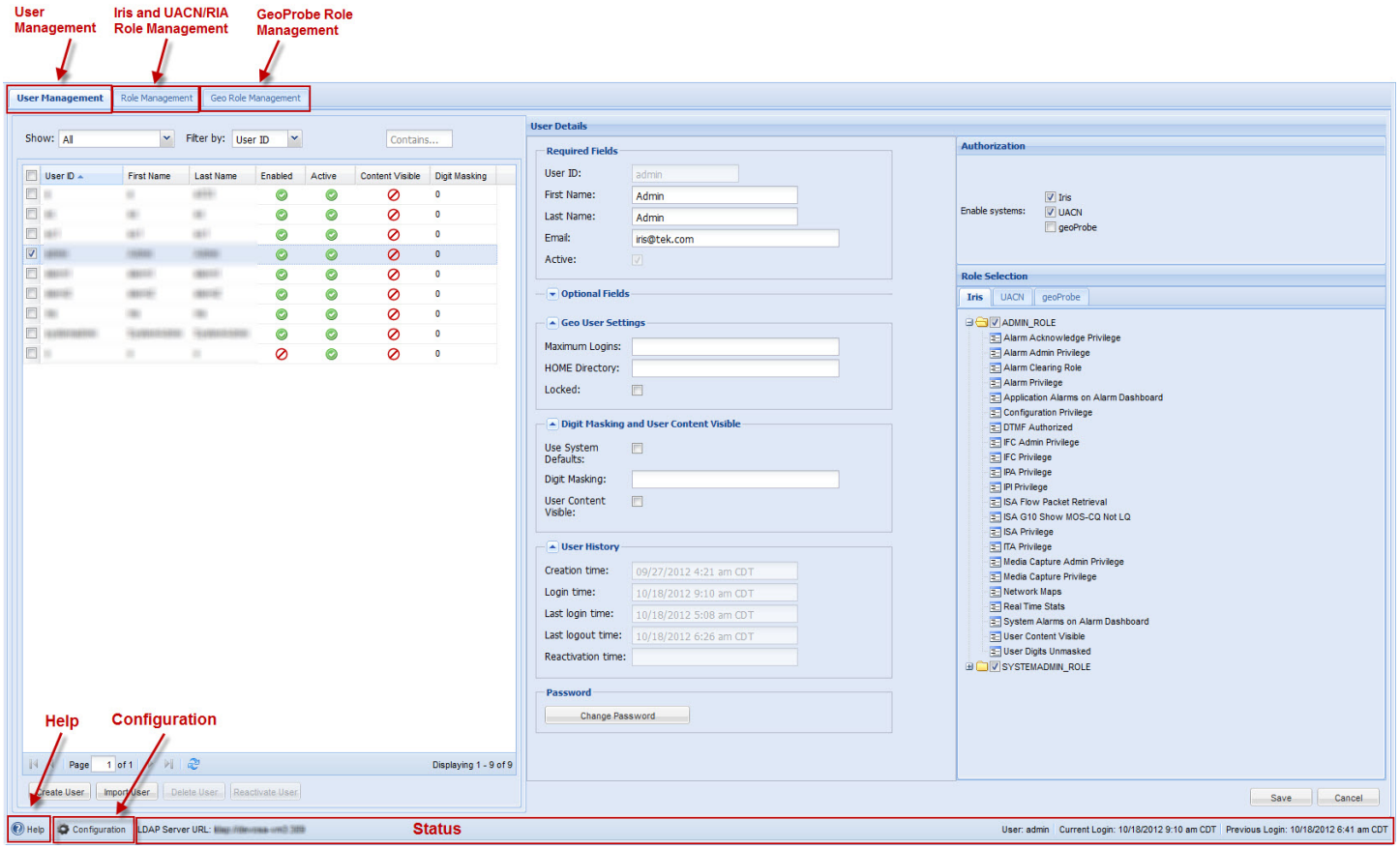
The User Management dashboard is the main window that opens when you access User Management from the Admin button on the Iris toolbar. This window enables you to manage user profiles and user system access. See User Management workflows for details.

Users Management Tab	Enables you to create, edit, or delete users and import users from an existing database.
Role Management Tab	Enables you to manage user roles and privileges for the Iris and UACN/RIA subsystems.
Geo Role Management Tab	Enables you to manage user profiles, classmarks, admin groups, and alarm groups for the GeoProbe subsystem.

Status Bar

Help Button	Open the UUMS Help.
Configuration Button	Access the Configuration window where you can configure LDAP server settings, password policies and qualities for Iris LDAP, and configure an advisory login message for users.
LDAP Server URL Field	Displays the currently installed LDAP server. You can update LDAP server settings on the General tab on the Configuration window.
User Field	Displays your user ID.
Current Login Field	Displays the date and time (client timezone) you logged into the current UUMS session.
Previous Login Field	Displays the date and time (client timezone) of your last login to UUMS.

User Management Dashboard



User Management Window

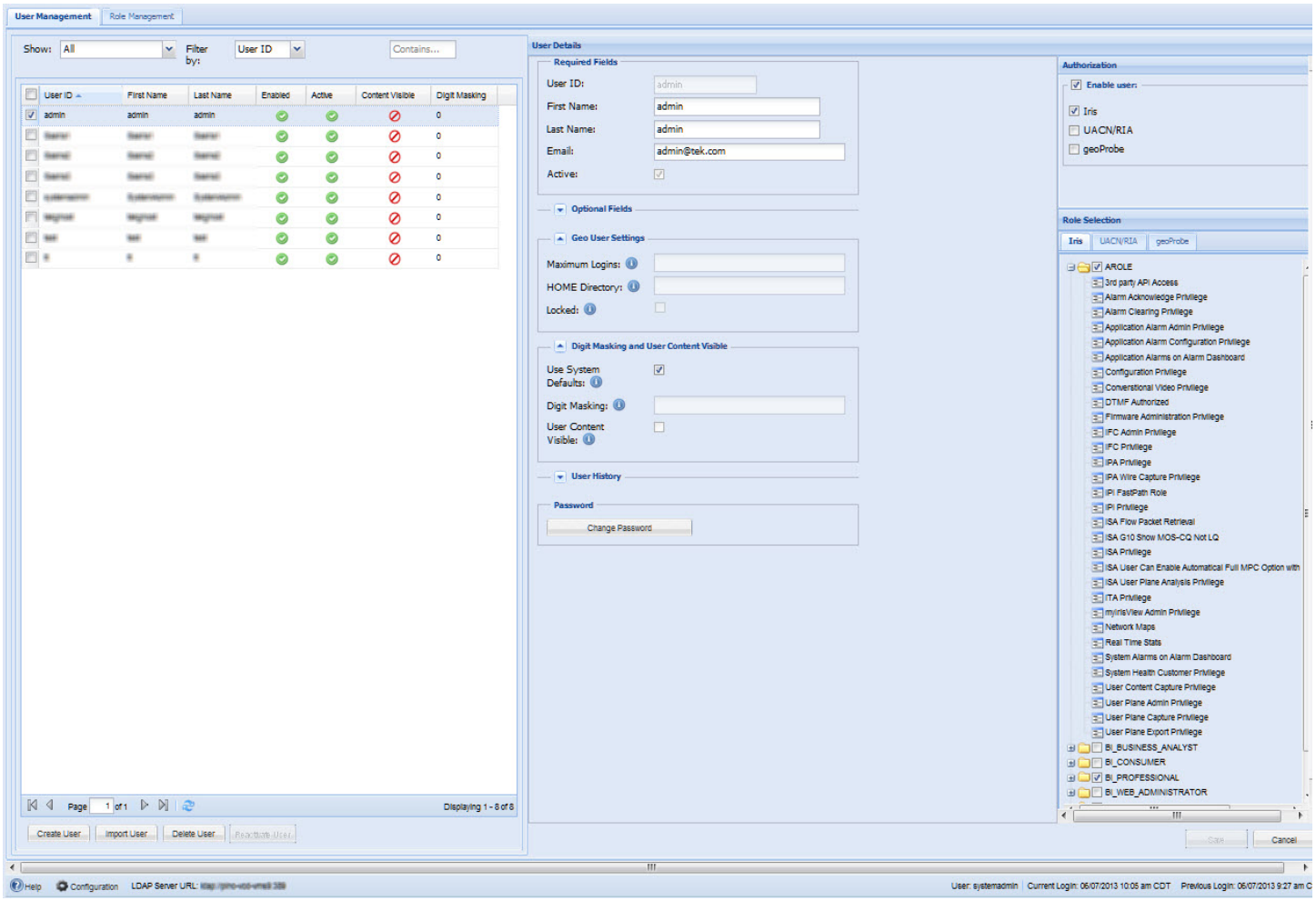
The User Management window is the main window that opens when you access User Management from the Admin button on the Iris toolbar. This window enables you to manage user profiles. See User Management workflows for details.

Users Pane	Enables you to view a list of all currently defined users and their enabled/disabled status.
User Details Pane	View a selected user's profile details, change a user's password, and assign roles to the user profile.
Authorization	Enables you to view and modify the current subsystem access settings for a specific user.
Role Selection Pane	Enables you to view a list of currently defined roles for each subsystem, and assign members to a role.

Status Bar

Help Button	Open the UUMS Help.
Configuration Button	Access the Configuration window where you can configure LDAP server settings, password policies and qualities for Iris LDAP, configure default subsystem access settings, and synchronize user data with UUMS, GeoProbe, and UACN/RIA.
LDAP Server URL Field	Displays the currently installed LDAP server. You can update LDAP server settings on the General tab on the Configuration window.
User Field	Displays your user ID.
Current Login Field	Displays the date and time (client timezone) you logged into the current UUMS session.
Previous Login Field	Displays the date and time (client timezone) of your last login to UUMS.

User Management



Users Pane

The Users Pane enables you to view a list of all user profiles that exist in the Iris database and their current status. You can create, import, and delete user profiles from this pane. Available user management functions depend on the configured LDAP.

Columns

User ID Column	Select a user profile in this list to display the profile data in the User Details pane.
First Name Column	
Last Name Column	
Enabled Column	Displays user profile status as Enabled or Disabled. User accounts are disabled manually using the Enabled check box in the User Details pane. Users with disabled user accounts cannot log in to the system.
Active Column	Displays user profile status as Active or Inactive. User accounts are made inactive when no logins occur for a user ID for a specific number of days (configured using the Inactivity Timeout). You can reactivate multiple users in a single step by selecting each user ID you wish then clicking the Reactivate User button.

Content Visible Column	Displays content status as Visible or Not Visible. You can change this status in the User Details pane.
Digit Masking Column	Displays the number of digits to conceal for this user. You can change this value in the User Details pane.

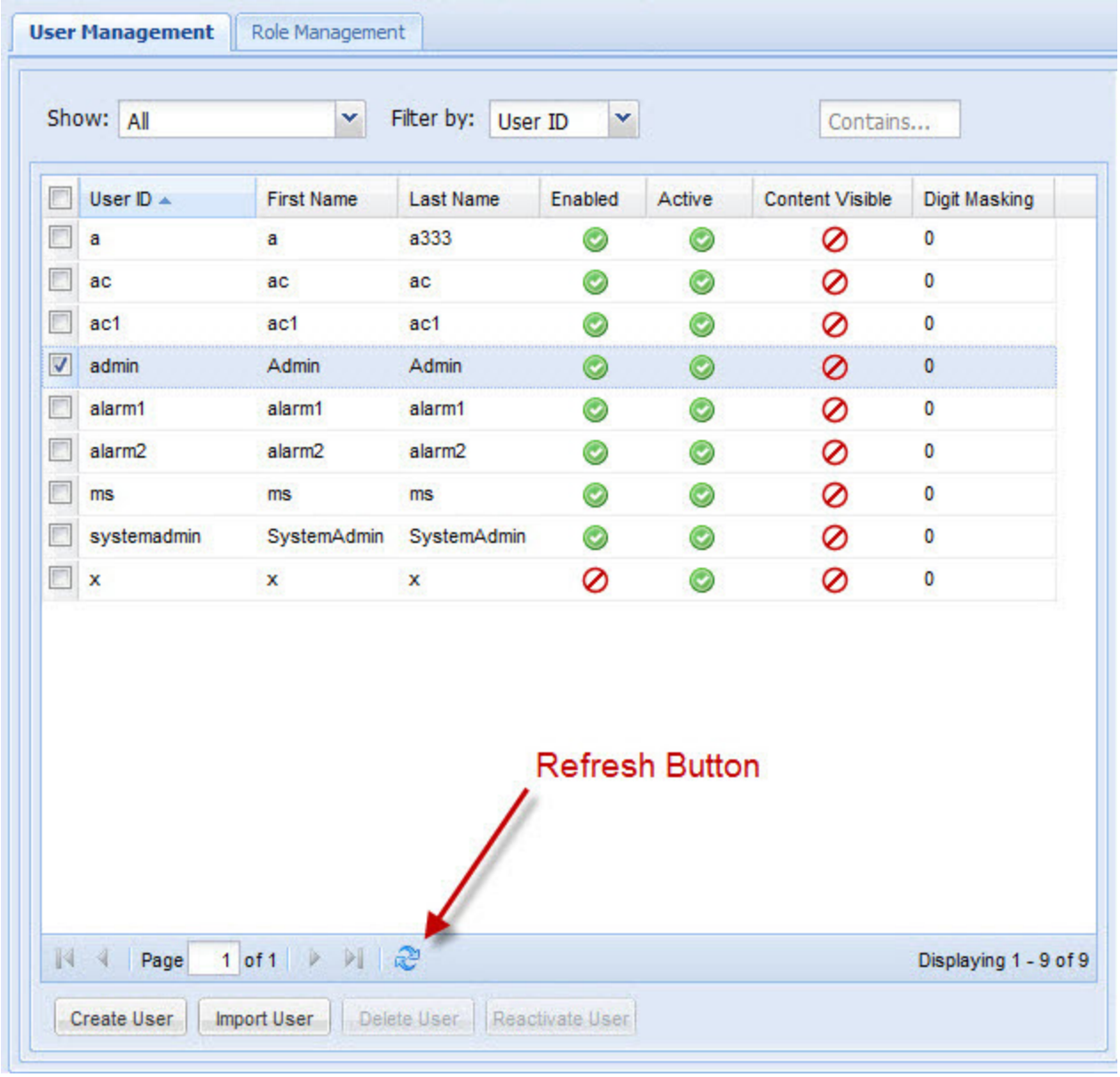
Column Filter Controls

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the checkmark from columns you want to hide. At least one column must remain visible.

User Pane Controls

Last / Next Page Buttons	Navigate to view users in multiple pages.
First / Last Page Buttons	Go to the first or last page of the list of users.
Refresh Button	Manually refresh the data displayed in the User Pane.
Create User Button	This button is only available when the Iris LDAP is configured. Open the User Details Pane with blank fields for entering new user profile data.
Import User Button	Open the LDAP Import List Dialog box to import user profile data from the LDAP.
Delete User Button	Delete selected user profiles (use the CTRL and Shift keys to select multiple profiles). You will be prompted to confirm. Deletion varies depending on the configured LDAP: • Iris LDAP: Deletes all user data from Iris database. On the confirm prompt, you can select the Also Delete LDAP User check box to delete the user credentials (user ID, user name, email address, and password) from the Iris LDAP. • Existing LDAP: Deletes all user data from Iris database only. User credentials (user ID, user name, email address, and password) remain in the existing LDAP.
Reactivate User Button	Manually reactivate one or more users made inactive based on the inactivity timeout configuration.

Users Pane



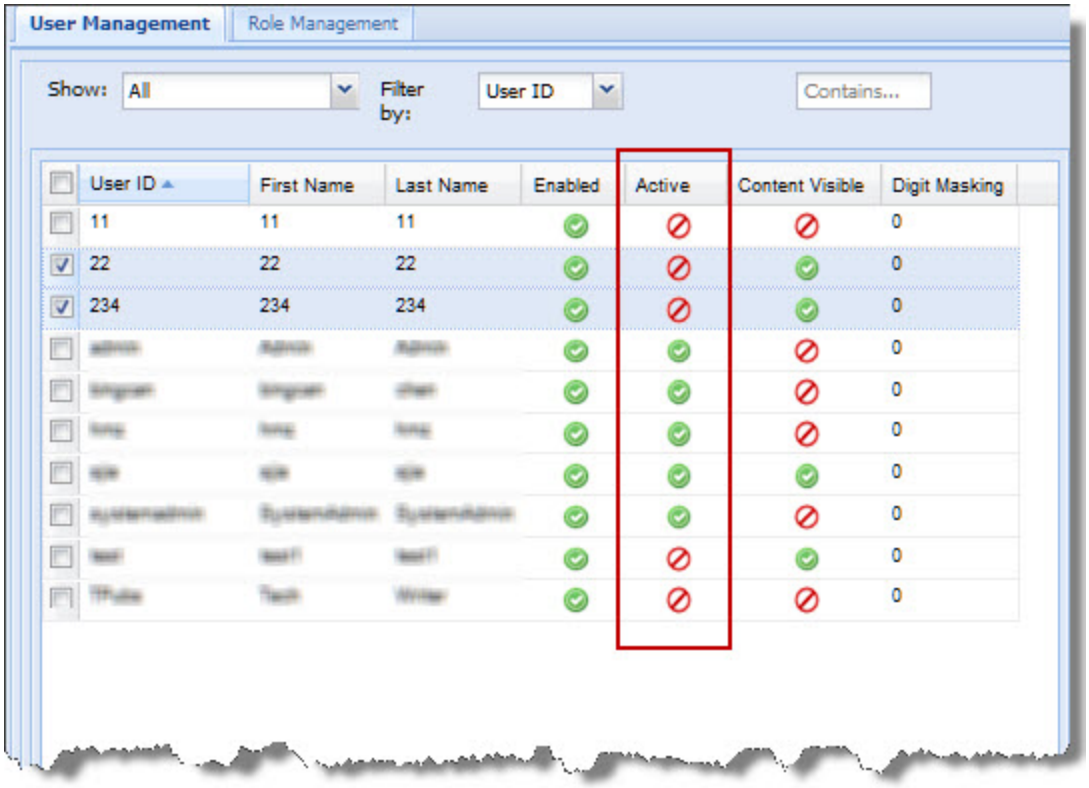
Users Pane Inactivity

The Inactivity Timeout feature allows you to identify and remove inactive users. You can set up a system-wide login inactivity time in number of days that will be applied to all users in the system. By default, this value is 30 days. Once the value is changed, it becomes effective to all subsequent user sessions. There is also a mechanism to disable the feature.

The default administrator users with the Administrator role are exempted from this inactive timeout requirement.

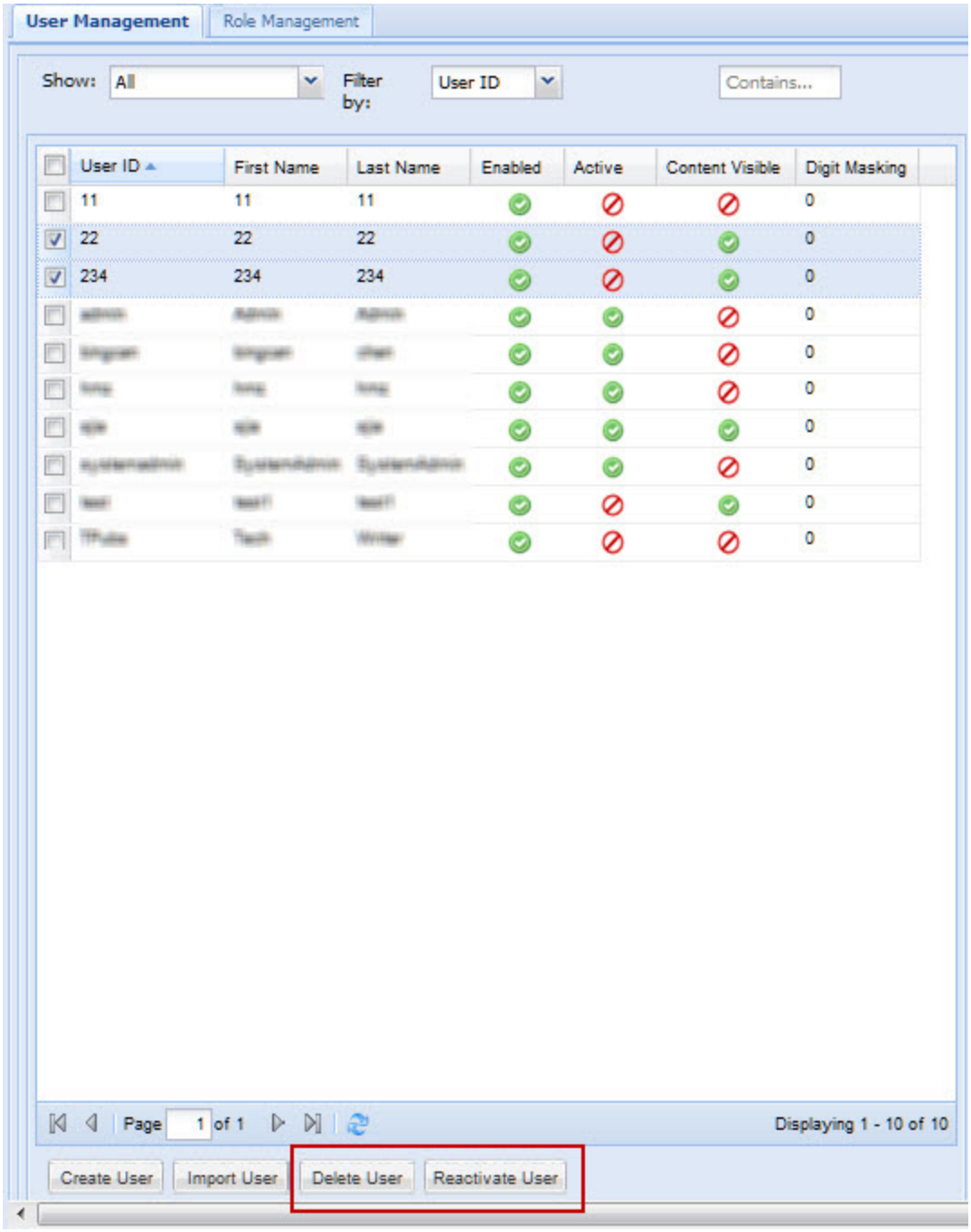
Viewing Inactive Accounts

You can view a list of inactive users from the User Management window. Active users have a green check mark and Inactive users have a red circle with a line through it.



Configuration Controls

Delete User	Administrators can delete one or more inactive users. The user deletion option applies to all LDAP deployments currently supported by UUMS: • Iris LDAP--users deleted in UUMS are also deleted from the LDAP • Corporate LDAP--users deleted in UUMS are not deleted from the LDAP • LDAP shared with GeoProbe and UACN/RIA--the shared LDAP is treated as a Corporate LDAP, so users deleted in UUMS are not deleted from the LDAP The Administrator account performing the delete action cannot be deleted, since there should be at least one Iris user with Administrative privileges at all times.
Reactivate User	Administrators can reactivate one or more inactive accounts. The Reactivate button is grayed out if at least one of the selected users is active.



User Details Pane

The User Details pane enables you to view or modify user profile details and assign roles. Some GUI and data management differences exist, depending on the configured LDAP.

User Details Area	View user profile details and change password (Iris LDAP).
Authorization Area	Assign user access to a specific subsystem and enable users. Valid options are Iris, UACN/RIA, and GeoProbe.
Role Selection Area	Assign user roles for each user. If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary.

User Details Pane Controls

GUI Element	Iris LDAP	Existing Corporate LDAP
Save Button	Save user profile changes to the Iris LDAP and the Iris database. When creating a new user, this button is not enabled until all required fields and a password are entered. Changes take effect the next time the user logs in.	Save user profile changes to the Iris database; modified data is not saved in the existing LDAP. Changes take effect the next time the user logs in.
Cancel Button	Close the User Details Pane without saving changes.	

User Details Area

GUI Element	Iris LDAP	Existing Corporate LDAP
Required Fields		
User ID Field	Enter an Iris system user name using alphanumeric characters. Spaces and special characters are not supported. This field is not editable once the user profile is saved. The system verifies the user ID does not already exist in the Iris database or Iris LDAP.	View imported user ID. This field is read-only.
First Name Field	Enter the user's first and last name. Spaces and special characters are supported.	Modify the imported first name and last name.
Last Name Field		
Email	Enter the user's email address in the user@example.com format.	Modify the imported email address.
Enabled Check Box	Enable or disable selected user account. Users with disabled profiles cannot login to the system.	By default, imported users are enabled. Select check box to disable the selected user account. Users with disabled profiles cannot login to the system.
Active Check Box	A check mark indicates the user is active, no check mark indicates the user is inactive.	
Optional Fields		
Office Number Field	Optional data to describe the user.	Data for these fields is not imported. You can add optional data here for imported users, but the data is only saved to the Iris database.
Mobile Number Field		
Employee ID Field		
Address Field		
Description Field		
Geo User Settings		
Maximum Logins	Configure the number of simultaneous SpImain sessions a user can open.	
HOME Directory	Configure the user's Unix HOME directory. The default is $HOME/$SPI_SERVER_HOST/$SPI_USER_NAME.	
Locked	A checkmark indicates the selected user will not be able to log in to the GeoProbe system.	
Digit Masking and User Content Visible		

GUI Element	Iris LDAP	Existing Corporate LDAP
Use System Defaults	A checkmark indicates you have selected the system defaults for this user (Digit masking set to 0, User Content Visible is NOT checked).	
Digit Masking	Configure digit masking for the specific user. This will override any default settings for this user.	
User Content Visible	Set content to visible for the specific user. This will override any default settings for this user.	
User History		
Creation Time	The User History fields list the times the selected user was created, the current session login time, the last login and logout time, and if the user has been reactivated, the timestamp for reactivation.	
Login Time		
Last Login Time		
Last Logout Time		
Reactivation Time		
Password		
Change Password Button	Access the new password fields.	Not available; passwords are managed on the existing LDAP. For example, password expiration continues to be managed on the existing LDAP; if a user's password expires on the existing LDAP, UUMS will not allow the user to login until the password is updated in the existing LDAP.
New Password Field	Enter a new password using the rules configured in the Password Quality tab (also available in the tooltip). Passwords from UACN/RIA and GeoProbe will be not migrated to the UUMS. UUMS will create a corresponding record in the LDAP and set the default password directly. Default password is equal to the user login name, but will be in lower case. On the first login, the user will be prompted to change their password You can require new users to reset their password after their first login.	
Confirm Password Field	Reenter the new password to confirm.	

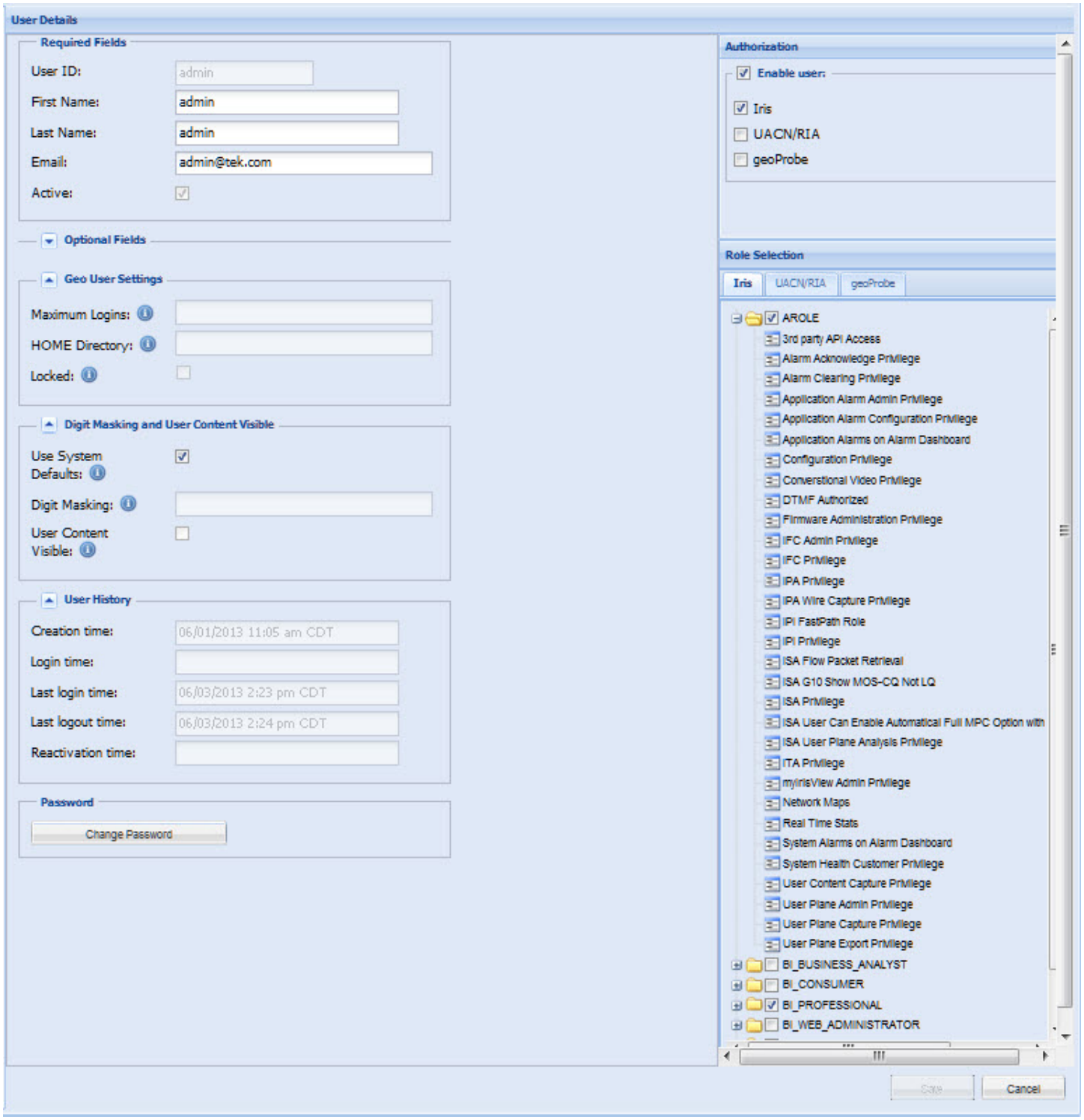
Authorization Area

Enable the subsystem(s) for the selected user. Options are Iris, UACN/RIA, and GeoProbe. Click the Enable Users check box to enable the user in Iris.

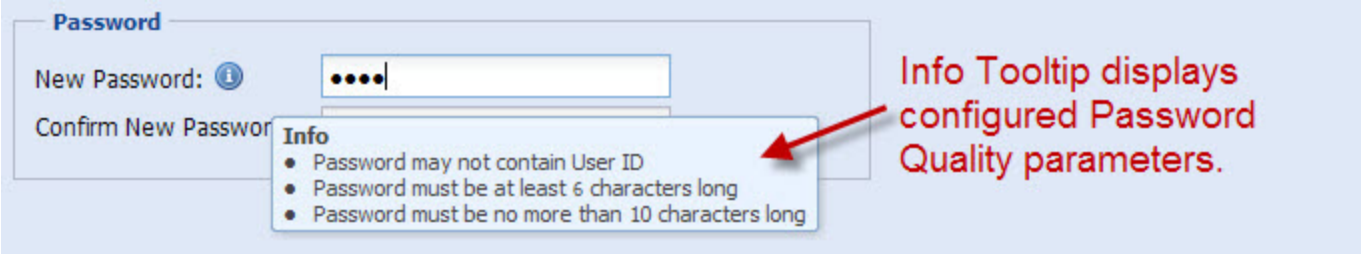
Role Selection Area

GUI Element	Iris LDAP	Existing Corporate LDAP
Subsystem Tab	See the roles available in each subsystem: Iris, UACN/RIA, and GeoProbe.	
Role Tree	Tree view containing role folders and individual privileges for each role. You can expand the role folders to view user privileges contained in a role.	
Role Check Boxes	Select at least one role to assign to the current user.	Roles are assigned when importing users on the Import LDAP Users dialog box. You can modify imported users' assigned roles.

User Details Pane



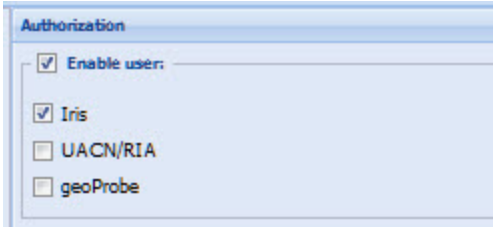
Password Area (Iris LDAP)



Authorization Pane

The Authorization Pane allows you to view the subsystem a selected user can access and enable/disable the user. You can change subsystem access for the selected user by checking the box next to the desired subsystem. Default subsystem access is Iris enabled, GeoProbe and UACN/RIA disabled. Changes to subsystem access will not take effect until the next time the user logs in.

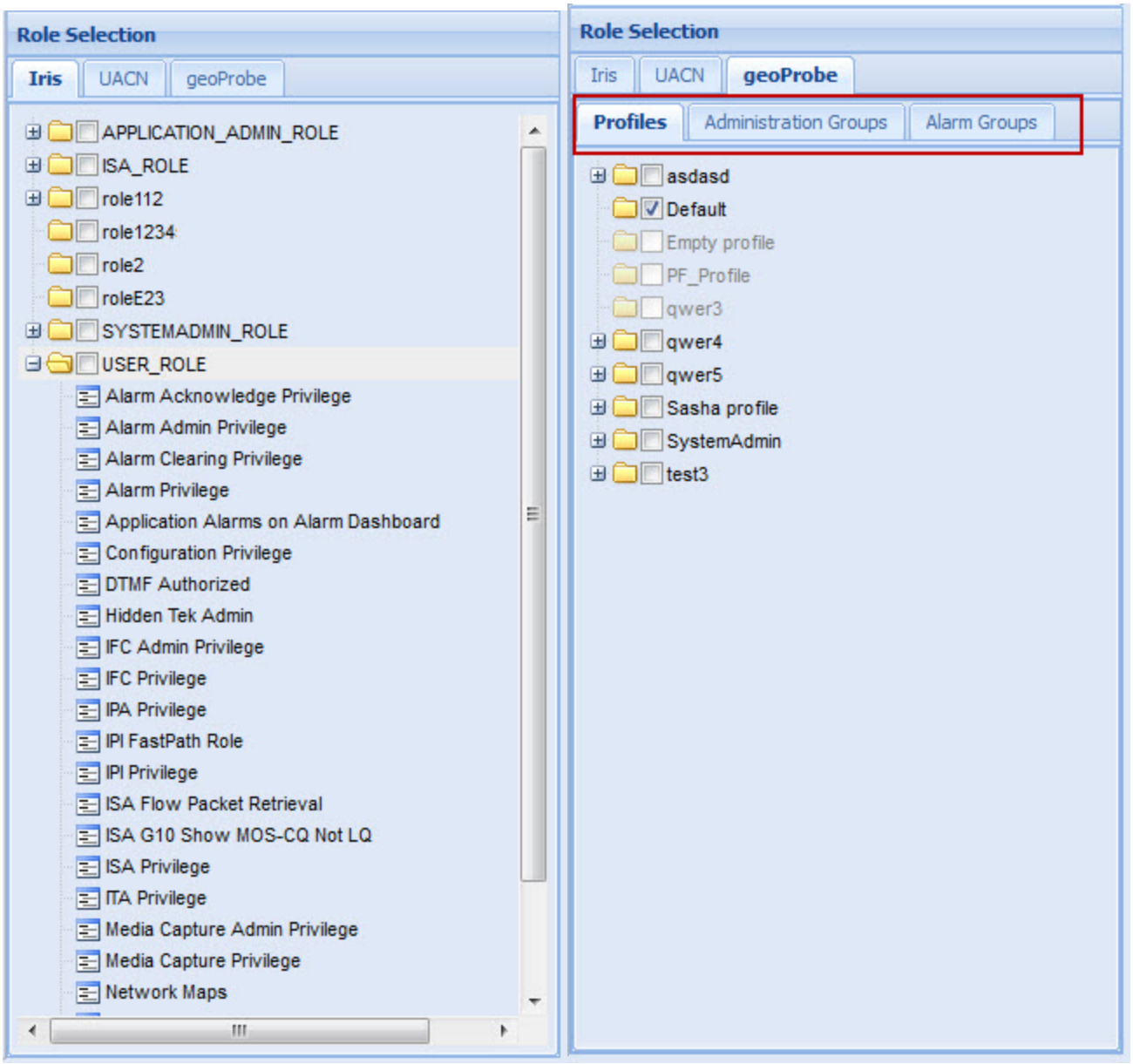
Authorization Pane



Role Selection Pane

The Role Selection Pane enables you to assign roles that control system access for all subsystems based on user functional privileges. You assign users with similar functional duties to appropriate roles on the Role Management Window. View all roles defined by the System Administrator and the privileges assigned to each role. The GeoProbe tab contains additional roles for GeoProbe Profiles, Administration Groups, and Alarm Groups.

Role Selection Pane



Import LDAP Users Dialog Box

The Import LDAP Users Dialog Box enables you to import user profile data from the configured LDAP into the Iris Database.

Columns

Check Box Column	Select the top check box in the column to choose all LDAP users in the list for import. Or, select specific users by clicking on their corresponding check box.
User ID Column	View the profile information of LDAP users. UUMS imports these fields into the Iris database.
First Name Column	
Last Name Column	
Email Column	
Organization Column	This user data is for search purposes only and is not imported into the Iris database.
Organization Unit Column	

Column Filter Controls

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the checkmark from columns you want to hide. At least one column must remain visible.

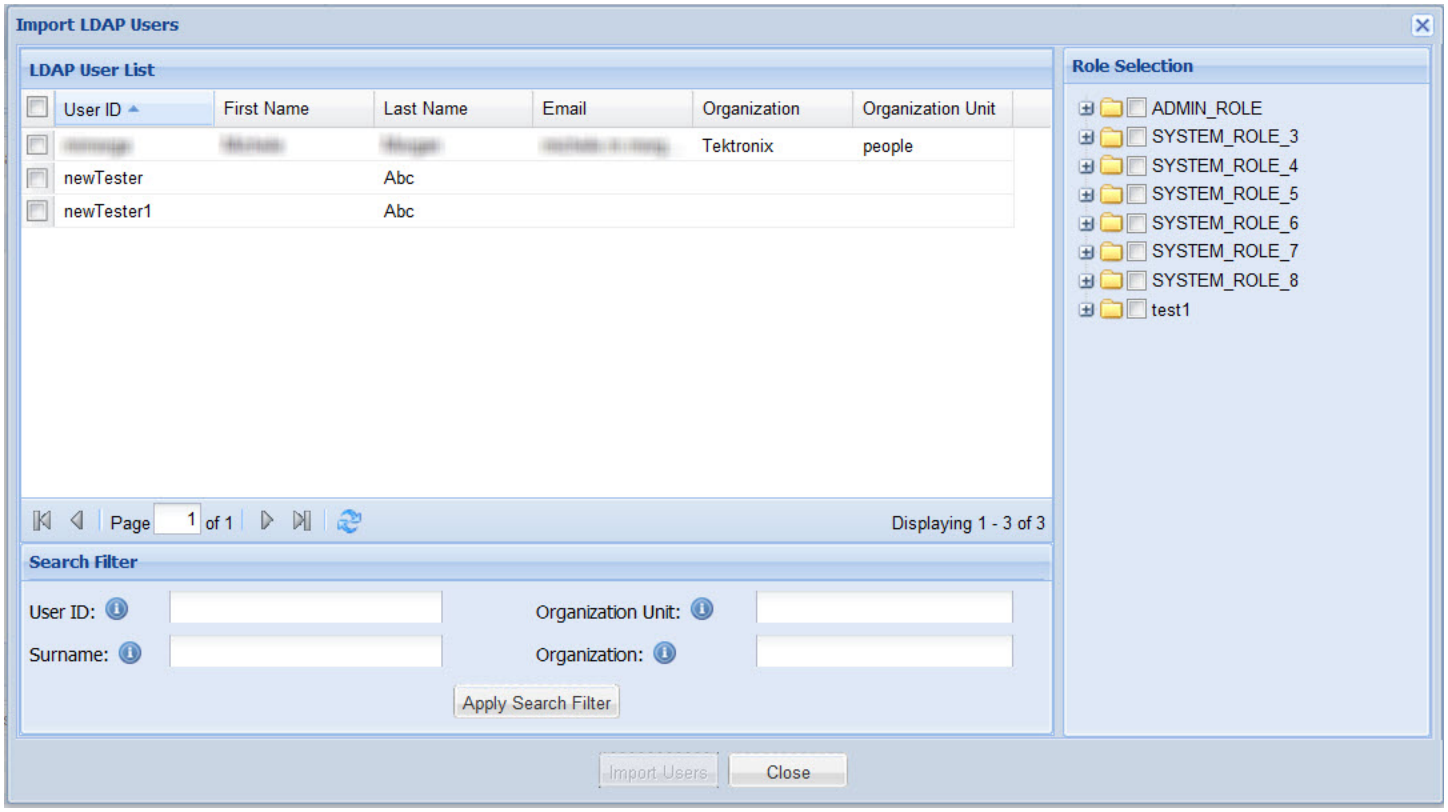
Search Filter Controls

User ID Field	Use one of the following methods to search for users by User ID, surname (last name), organization or organization unit: • Enter the entire name you want to search for. • Enter one or more letters in the name followed by an asterisk (*). Click the Apply Search Filter button to search based on your criteria.
Surname Field	
Organization Field	
Organization Unit Field	
Apply Search Filter Button	

Role Selection Area

Role Tree	Tree view containing role folders and individual privileges. You can expand the role folders to view user privileges contained in a role.
Role Check Boxes	Select at least one role to assign to all users you select to import.

Import LDAP Users Dialog Box



User Management Configuration Window

The User Management Configuration window enables you to manage LDAP server settings, set password policy and quality parameters for Iris LDAP, and define a login advisory message for users. You access this window by clicking the Configuration button in the User Management window status bar. Available tabs vary depending on the selected LDAP Server. See User Management Configuration workflows for details.

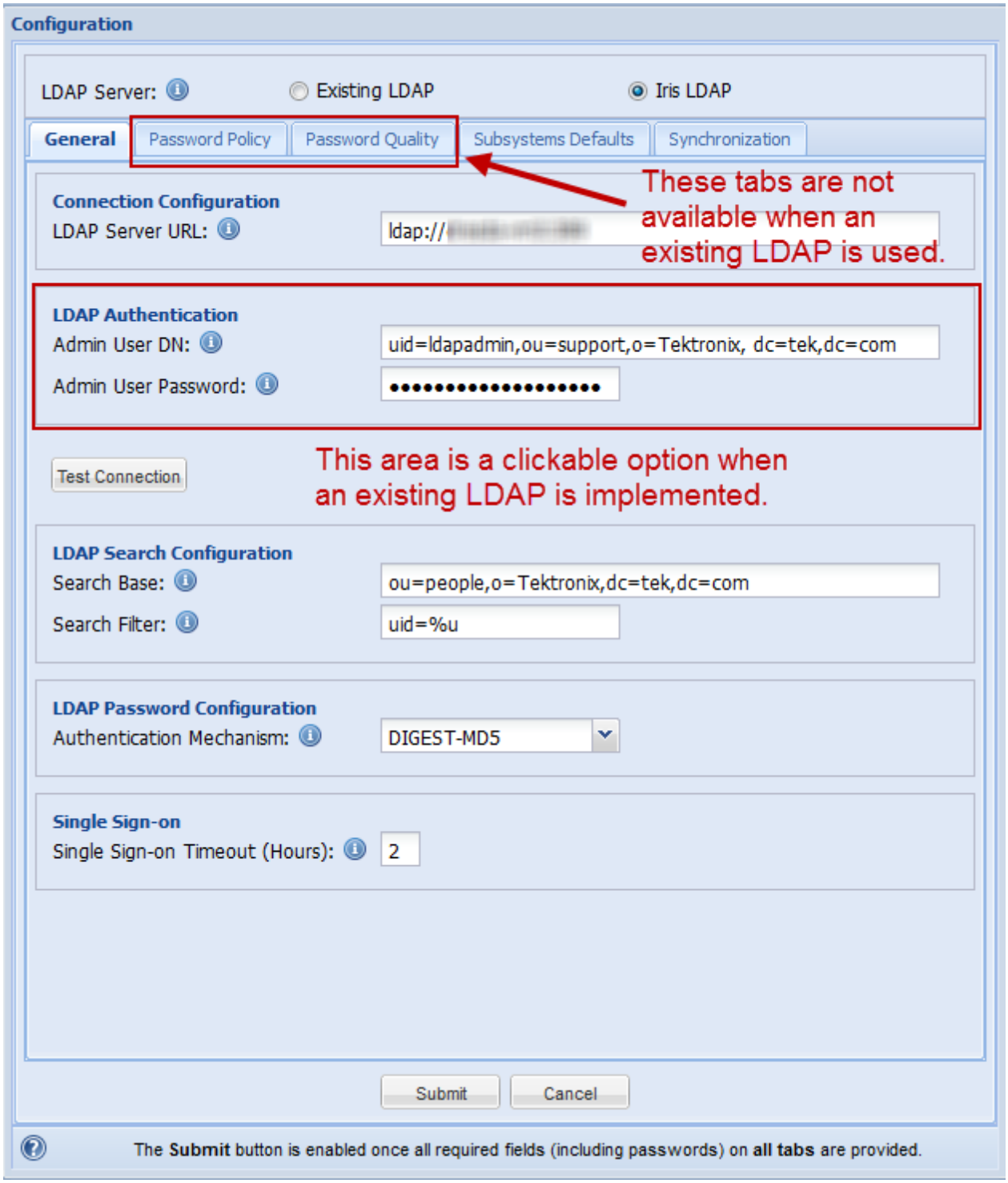
User Management Tabs

General Tab	Configure the LDAP server settings, Admin login, and user session duration.
Password Policy Tab	Configure policies such as number of days until expiration and number of allowable login attempts. If using an existing LDAP, this tab is unavailable because password policies are managed on the existing LDAP.
Password Quality Tab	Configure qualities such as allowable characters, syntax, and password length. If using an existing LDAP, this tab is unavailable because password quality is managed on the existing LDAP.
Subsystem Defaults Tab	Configure the Subsystem defaults, include an advisory login, digit masking, Geo user settings, default user data synchronization, and an inactivity timeout.
Synchronization Tab	Manually synchronize user, role, and classmark data between UUMS and GeoProbe and UACN/RIA.

Configuration Controls

Existing LDAP Option	These options are set up by Tektronix at installation. The Existing LDAP option is selected when your existing corporate LDAP is used. The Iris LDAP option is selected if the Iris LDAP was installed on initial system setup.
Iris LDAP Option	Iris LDAP Option
Submit Button	Submit and apply all UUMS configuration settings. This button is not enabled until all required fields are populated on all tabs.
Cancel Button	Close the window without making any changes.
Help Button	Open the UUMS Help.

User Management Configuration (Iris LDAP)



General Tab

The General tab provides the LDAP server settings, Admin login configuration, and the global session duration setting. For Iris LDAP, Tektronix configures LDAP server settings and creates your admin account at installation. You can access this tab when you select the Configuration icon in the User Management window. Iris supports LDAPv3.

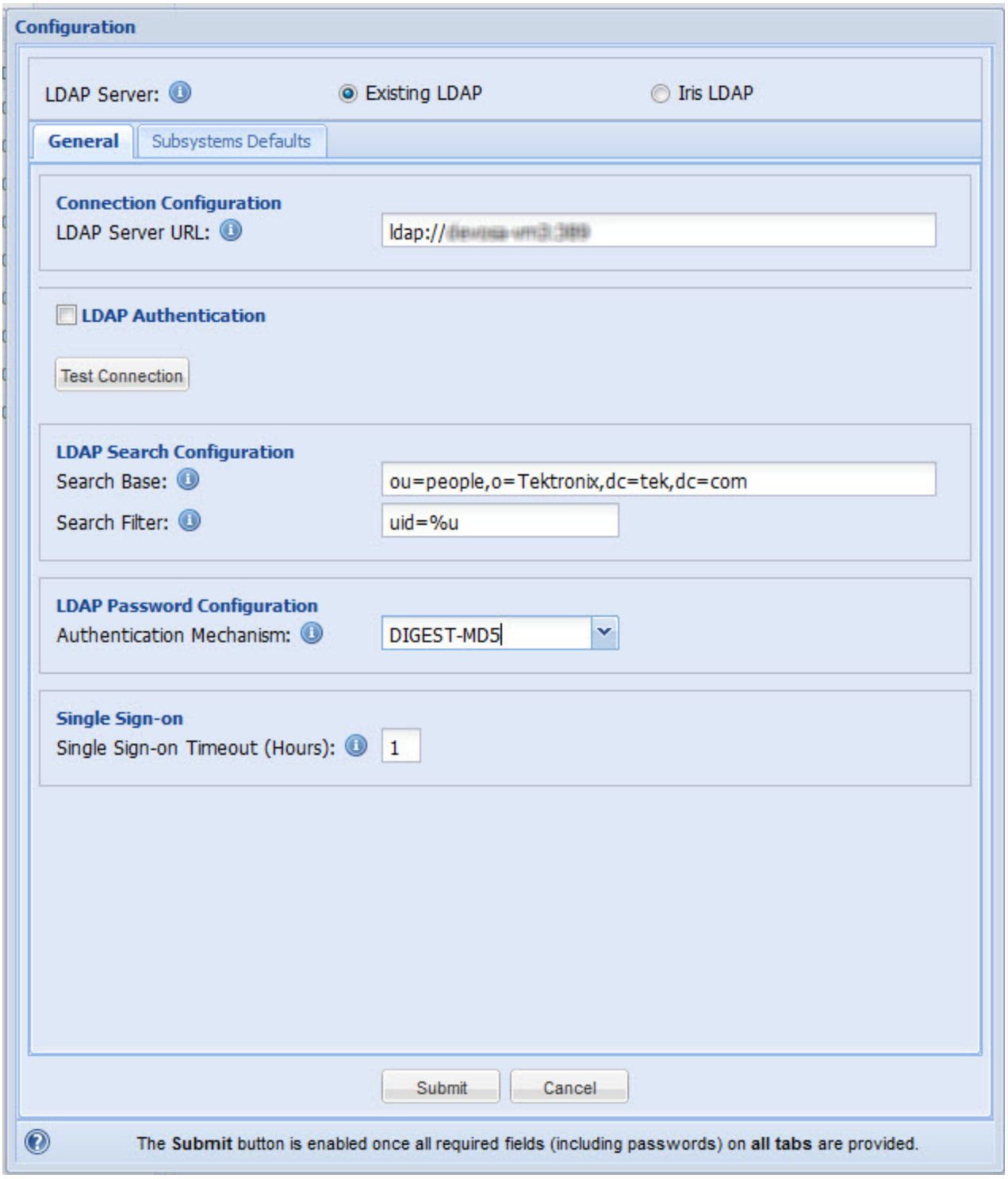
LDAP Server URL Field	Enter URL and port for the LDAP server you want Iris to communicate with; for example, http://sunshine:389, where 389 is the expected port. Iris supports either an existing corporate LDAP server or the installed Iris LDAP server.
LDAP Authentication Check Box	For an Existing LDAP, select this option if your LDAP server requires authenticated connections. When you select this option the Admin User DN and Password fields appear for you to enter data. Clear this option if your LDAP server does not require authenticated connections to LDAP. The Iris LDAP requires authenticated connections.
Admin User DN Field	For Existing LDAP, this field appears only if the LDAP Authentication check box is selected. Enter the Admin User Distinguished Name (DN) of an LDAP user who has write privileges to the LDAP. The LDAP connection must be authenticated with a valid user in order to perform LDAP writes. Use the syntax configured in your LDAP server. Iris LDAP uses the syntax: uid=jsmith,ou=people,o=tektronix,dc=tek,dc=com: • uid=valid user ID • ou=organizational unit • o=organization; you can enter one or more separated by commas • dc=domain or company name; you can enter one or more values separated by commas
Admin User Password Field	For Existing LDAP, this field appears only if the LDAP Authentication check box is selected. Enter the exact password associated with the Admin user who has write privileges to the LDAP. This is for connectivity purposes only, the password will not be changed.
Test Connection Button	Test the login for LDAP write authentication. If connection is successful, a success confirmation message appears and a green checkmark icon appears next to this button. If connection fails, a failure message appears and a red icon appears next to this button. Verify the LDAP Server URL and Admin User DN and password entries are valid and try again.
Search Base Field	Enter the exact search base values configured in the LDAP server. The search base defines the starting point for the search in the LDAP directory tree.
Search Filter Field	Enter the exact search filter values configured in the LDAP server. The search filter defines the scope of the data to retrieve for authentication. For example, uid=%u returns only the user ID such as "jsmith".

Authentication Mechanism Drop-Down	Select the authentication mechanism used on your Existing LDAP. The Iris LDAP uses DIGEST-MD5. • GSSAPI - Generic Security Services Application Program Interface that allows the client to pass GSSAPI tokens to the server to establish their credentials. • CRAM-MD5 - a Challenge-Response Authentication Mechanism (CRAM) based on Hash-based Message Authentication Code (HMAC)-MD5 algorithm. • Simple - consists of sending the LDAP server the fully qualified DN of the client (user) and the client's clear-text password; used within an encrypted channel for security. • Digest-MD5 - used with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. • External - allows the client to request that the server use credentials established by a means external to the mechanism to authenticate the client. • Login - transfers authentication data as plain unencrypted text. • Plain - transfers authentication data as plain unencrypted text.
Single Sign-on Timeout (Hours)	Enter the number of hours users will remain authenticated after initial login. For example, if this value is set to 4, users will not be required to log in again for at least 4 hours. Single Sign-on Timeout does not apply to ISA and PA; users of these applications do not require reauthentication.

Configuration Controls

Existing LDAP Option	These options are set up by Tektronix at installation. The Existing LDAP option is selected when your existing corporate LDAP is used. The Iris LDAP option is selected if the Iris LDAP was installed on initial system setup.
Iris LDAP Option	Iris LDAP Option
Submit Button	Submit and apply all UUMS configuration settings. This button is not enabled until all required fields are populated on all tabs.
Cancel Button	Close the window without making any changes.
Help Button	Open the UUMS Help.

General Tab (Existing LDAP)



General Tab (Iris LDAP)

Password Policy Tab

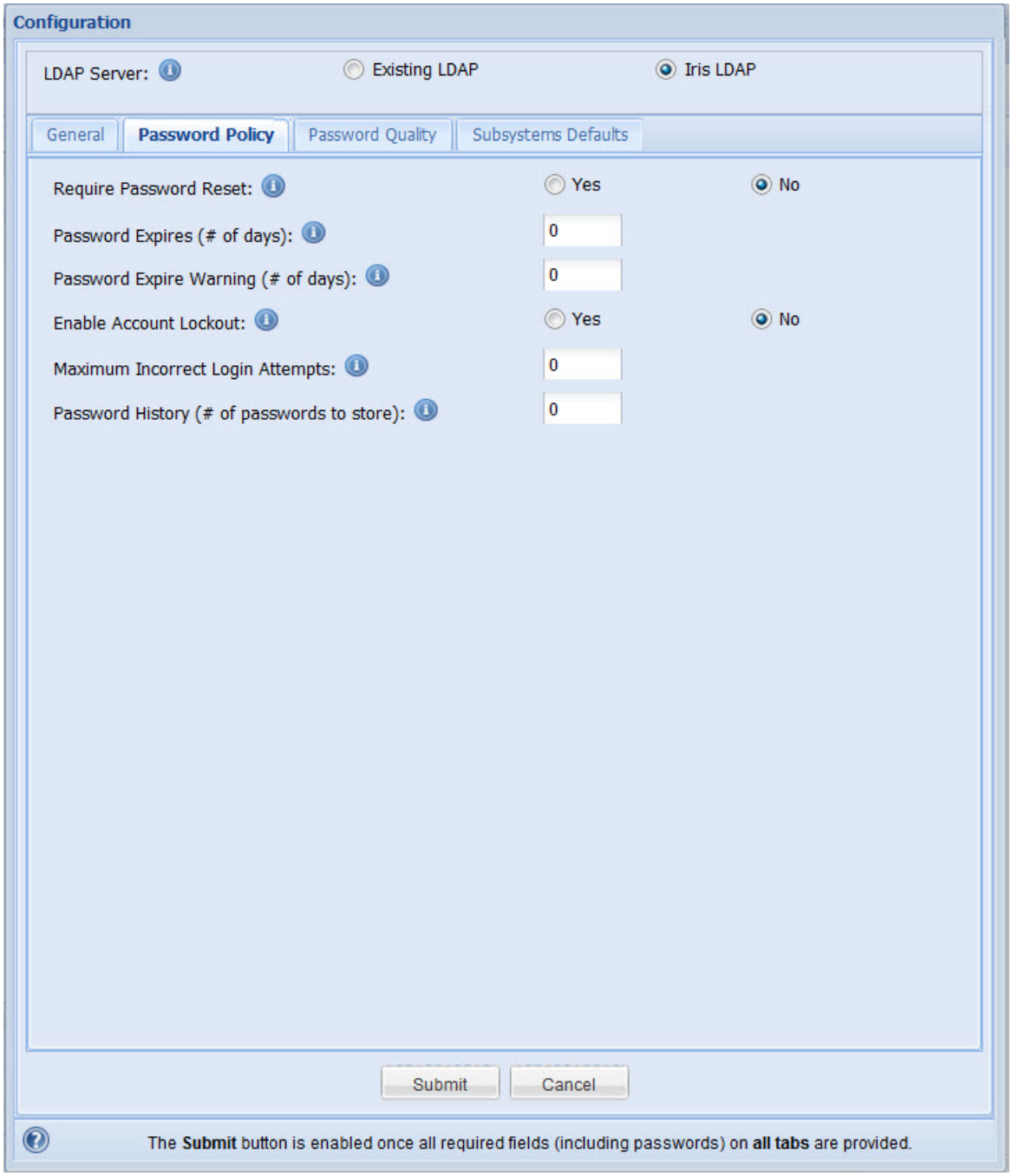
The Password Policy tab enables you to define various password control parameters relating to password expiry, login attempts, and history. This tab is not available if connecting to an existing corporate LDAP because password policies are managed in the existing LDAP. You can access this tab when you click the Configuration icon in the User Management window.

Require Password Reset Option	Select Yes to force new users to reset their password on their first login. New users initially log in using the password you configure on the User Details Pane. After successful login, new users will then be prompted to reset their password. This option only applies to newly created users. When you change an existing user's password in the User Details Pane, and this option is set to Yes, the existing user will **not** be prompted to change their password at login; the user will log in using the password you configured.
Password Expires (# of days) Field	Set the number of days a password is valid before expiring. This option requires the Enable Account Lockout option to be set to Yes. When a password expires, the account is locked and you must reset the password on the User Details Pane. A value of 0 indicates passwords never expire.
Password Expire Warning (# of days) Field	Set the number of days prior to password expiration that a warning will appear to the user at login. A value of 0 indicates no warnings will appear.
Enable Account Lockout Option	Select Yes to enable accounts to be locked through password expiration and failed login attempts. If an account is locked, you must reset the user's password on the User Details Pane so the user can log in.
Maximum Incorrect Login Attempts Field	Set the number of failed logins allowed prior to a user's account being locked. This option requires the Enable Account Lockout option to be set to Yes. A value of 0 indicates user accounts are allowed an unlimited number of failed logins.
Password History (# of passwords to store) Field	Set the number of unique new passwords that must be stored in a user account before a previously used password can be reused. This feature ensures that old passwords are not continually reused. When users change their password, the new password is checked against the password list and rejected if present in the list. A value of 0 indicates that no password history is retained.

Configuration Controls

Existing LDAP Option	These options are set up by Tektronix at installation. The Existing LDAP option is selected when your existing corporate LDAP is used. The Iris LDAP option is selected if the Iris LDAP was installed on initial system setup.
Iris LDAP Option	Iris LDAP Option
Submit Button	Submit and apply all UUMS configuration settings. This button is not enabled until all required fields are populated on all tabs.
Cancel Button	Close the window without making any changes.
Help Button	Open the UUMS Help.

Password Policy Tab



Password Quality Tab

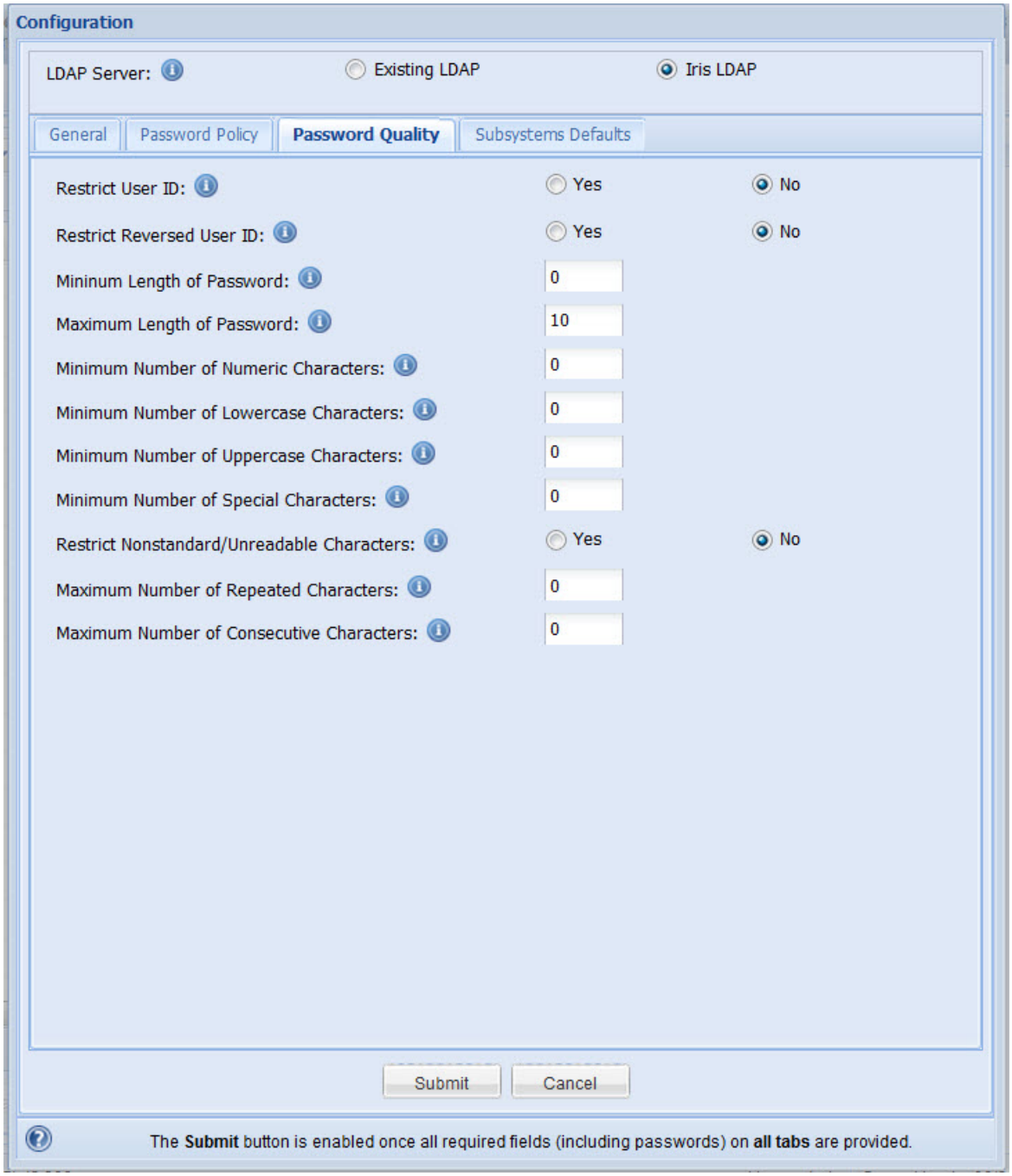
The Password Quality tab enables you to define various password quality parameters relating to password length and syntax rules. This tab is not available if connecting to an existing corporate LDAP because password quality is managed in the existing LDAP. When Iris LDAP users change their password on the User Management window, a Password Info tooltip appears summarizing the configured password syntax rules. You can access this tab when you click the Configuration icon in the User Management window.

Restrict User ID Option	Select Yes to prevent users from choosing a password that contains their user ID.
Restrict Reversed User ID Option	Select Yes to prevent users from choosing a password that contains the reverse spelling of their user ID.
Minimum Length of Password Field	Set the minimum number of characters a password must contain.
Maximum Length of Password Field	Set the maximum number of characters a password may contain.
Minimum Number of Numeric Characters Field	Set the minimum number of numeric characters a password must contain.
Minimum Number of Lowercase Characters Field	Set the minimum number of lower case characters a password must contain.
Minimum Number of Uppercase Characters Field	Set the minimum number of uppercase characters a password must contain.
Minimum Number of Special Characters Field	Set the minimum number of special characters (!"@$%&/()=?#+') that a password must contain.
Restrict Nonstandard/Unreadable Characters Option	Select Yes to prevent users from using nonstandard or unreadable characters, such as spaces, in their password.
Maximum Number of Repeated Characters Field	Set the maximum number of allowable repeated consecutive characters a password may contain. For example, if the value is set to 2, the following passwords would not be valid: smith222, johnnny99.
Maximum Number of Consecutive Characters Field	Set the maximum number of allowable ascending or descending alphanumeric characters a password may contain such as ABCDEF and 12345.

Configuration Controls

Existing LDAP Option	These options are set up by Tektronix at installation. The Existing LDAP option is selected when your existing corporate LDAP is used. The Iris LDAP option is selected if the Iris LDAP was installed on initial system setup.
Iris LDAP Option	Iris LDAP Option
Submit Button	Submit and apply all UUMS configuration settings. This button is not enabled until all required fields are populated on all tabs.
Cancel Button	Close the window without making any changes.
Help Button	Open the UUMS Help.

Password Quality Tab



Subsystem Defaults Tab

The Subsystem Defaults feature allows you to configure defaults for the login Advisory message, digit masking, Geo user settings, subsystem access, synchronization, and default inactivity timeout for all users.

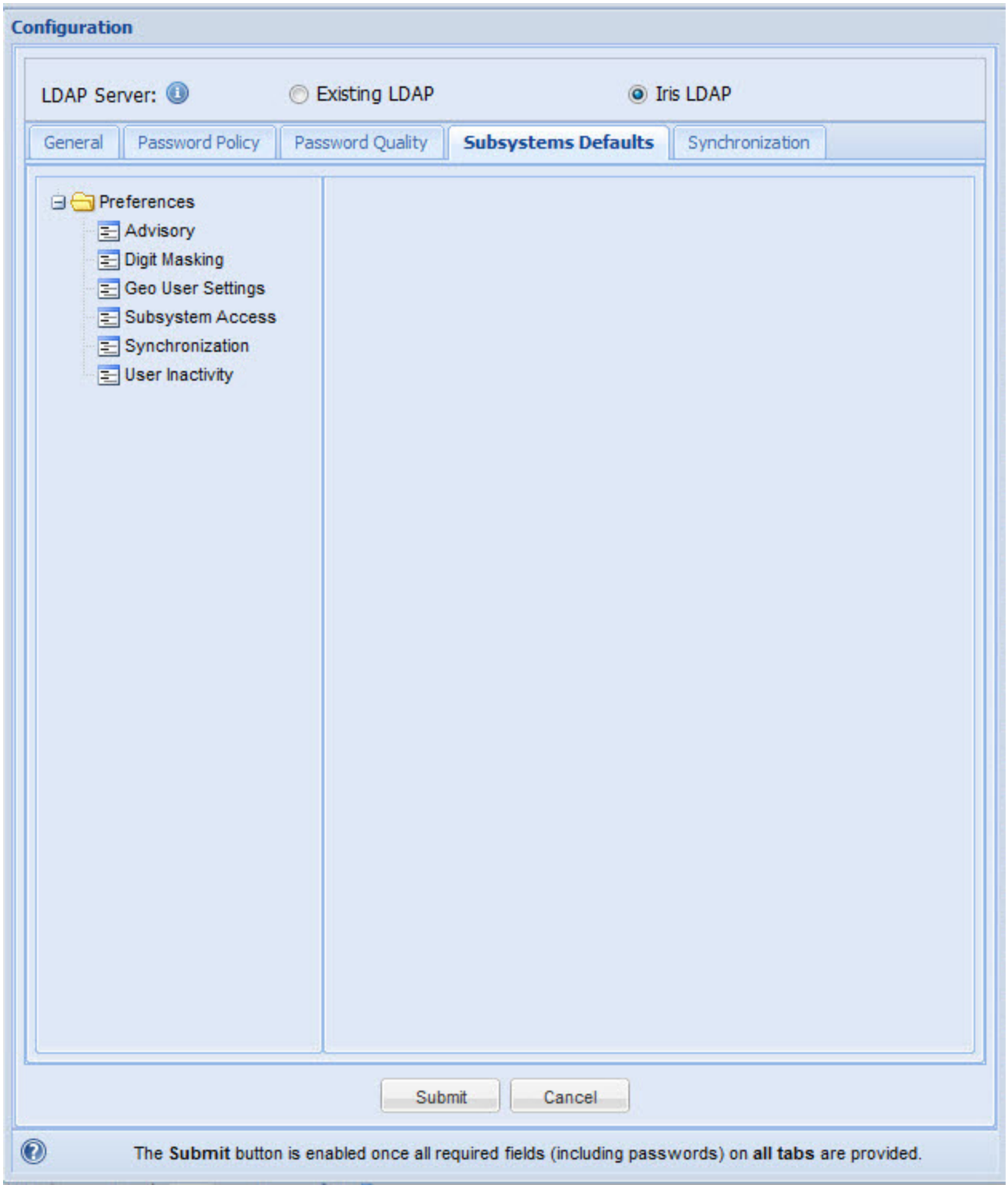
Preferences Pane

Advisory	Configure the advisory login available to all users.
Digit Masking	Configure the default value for digit masking and enable/disable user content visibility.
Geo User settings	Configure the default maximum logins and HOME directory settings for GeoProbe users.
Subsystem Access	Configure the default user access to the Iris, GeoProbe, and UACN/RIA systems. The default is Iris enabled, UACN/RIA and GeoProbe disabled.
Synchronization	Enable automatic synchronization of GeoProbe and UACN/RIA user imported data.
User Inactivity	Configure the default timeout values for inactive users.

Configuration Controls

Cancel	Cancels any changes to the window.
Submit	Submit button becomes active once all required fields on all tabs are provided.

Subsystem Defaults Window



Login Advisory

The Login Advisory feature allows you to create a custom notice to be seen by users when they log in to the system. This notice allows you to notify users of your corporate IT policies. You can configure that data protection statement to align with your company policies, and select whether this statement will be displayed upon user login. The system defaults to this statement ON. If you leave the default ON and do not provide a custom policy statement, the default message is displayed.

The default statement is intended for example purposes only. You should have your company legal department approve any login advisory statement you use.

The advisory message is a global option, so it is either on or off for all users. To turn the message off, simply leave the Advisory Message area blank.

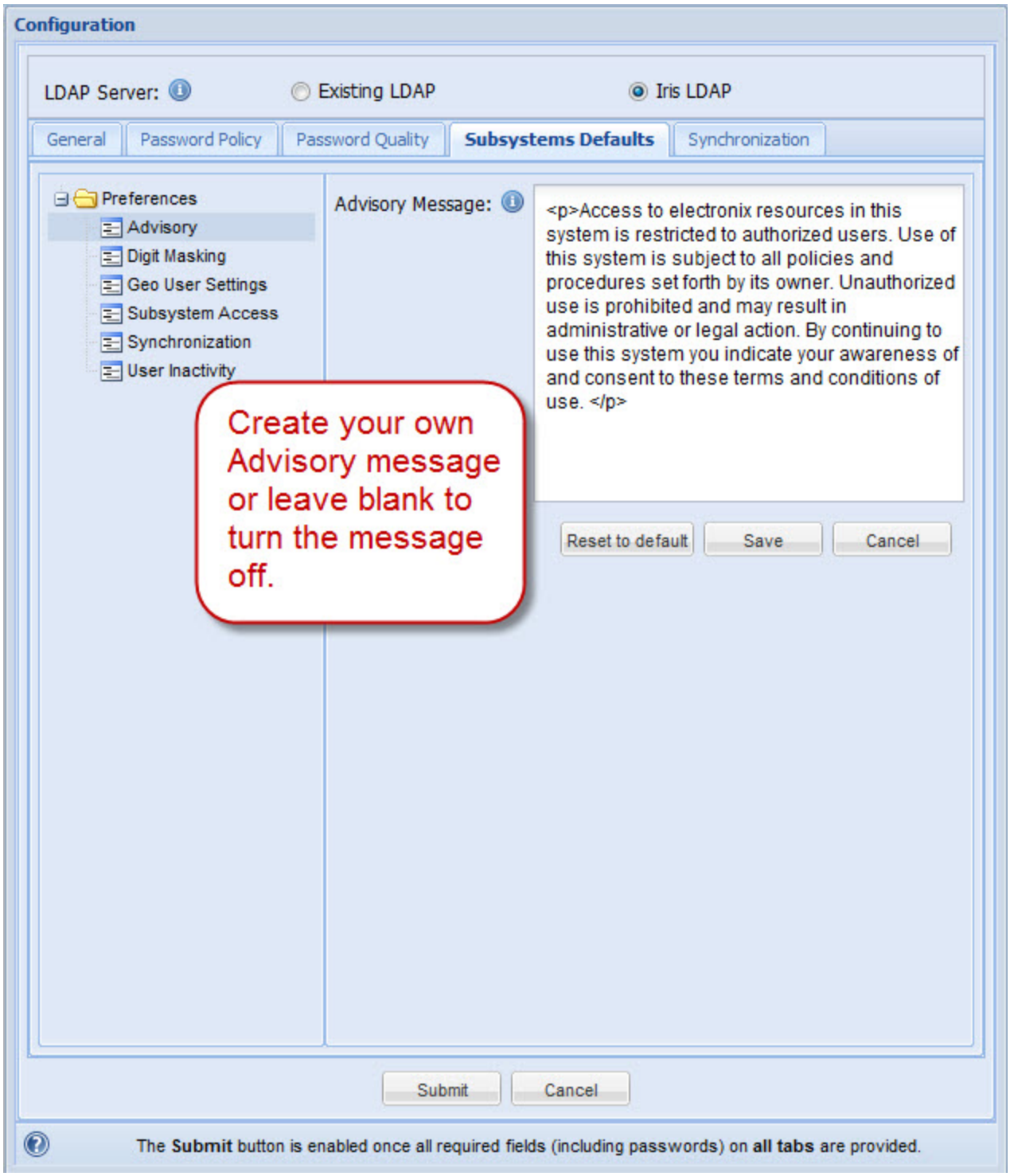
Advisory Message Area

Advisory Message	Shows you the default message.
Reset to Default Button	Reset to the default advisory message.
Save Button	Save your settings.
Cancel Button	Cancel out of the Advisory Message preferences.

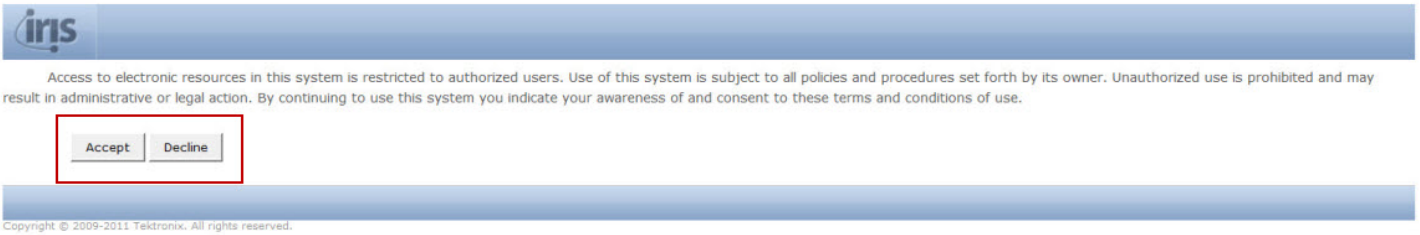
Window Controls

Submit Button	Submit and apply settings.
Cancel Button	Close the window without making any changes.

Advisory Message Area



Login Advisory Message Example



Digit Masking

The Digit Masking feature allows you to configure default digit masking settings for new users. Digit and content masking conceals network traffic and call content from unauthorized access and protects the privacy of a customer's personal information. Digits are masked with the letter X and content is masked with an asterisk (*). Individual digit masking can be changed on the User Details window.

Digit Masking Area

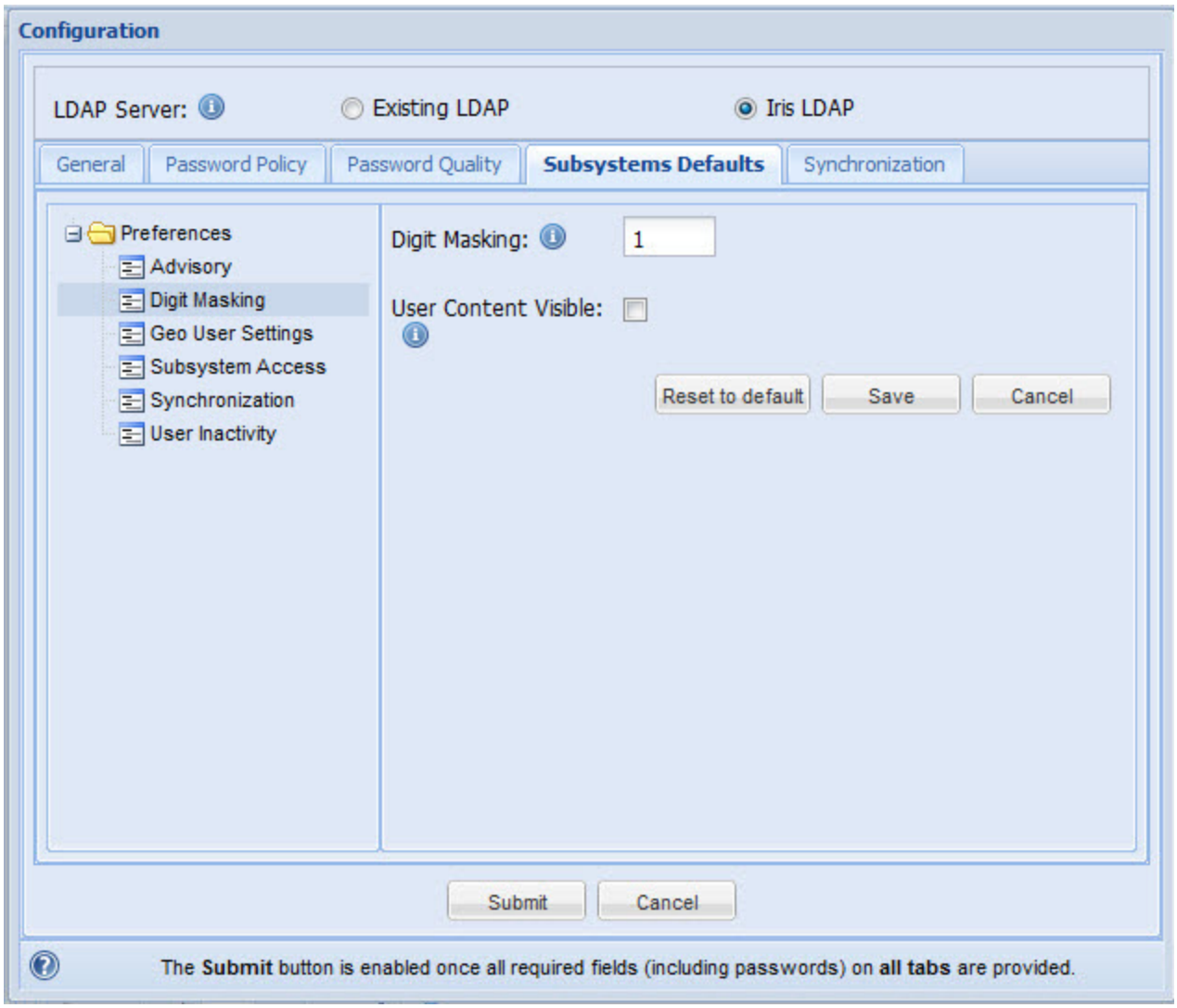
You can set the default masking for new users in this area.

Digit Masking	Sets the number of digits to conceal. To make all digits accessible to users, enter 0. You can enter a value between 0 and 20.
User Content Visible	When checked, user content is visible.

Configuration Controls

Reset to Default	Resets the default to 0 digits for masking and disables User Content Visible.
Save	Saves the changes you made to the Digit Masking.
Cancel	Cancel any changes you have made.

Digit Masking Area



Geo User Settings

The Geo User Settings feature allows you to configure default maximum logins and the HOME directory for those users who will also access GeoProbe. By default, new users have 999999 maximum logins and a default GeoProbe HOME directory. Individual user settings can be changed on the User Details window.

Geo User Settings Area

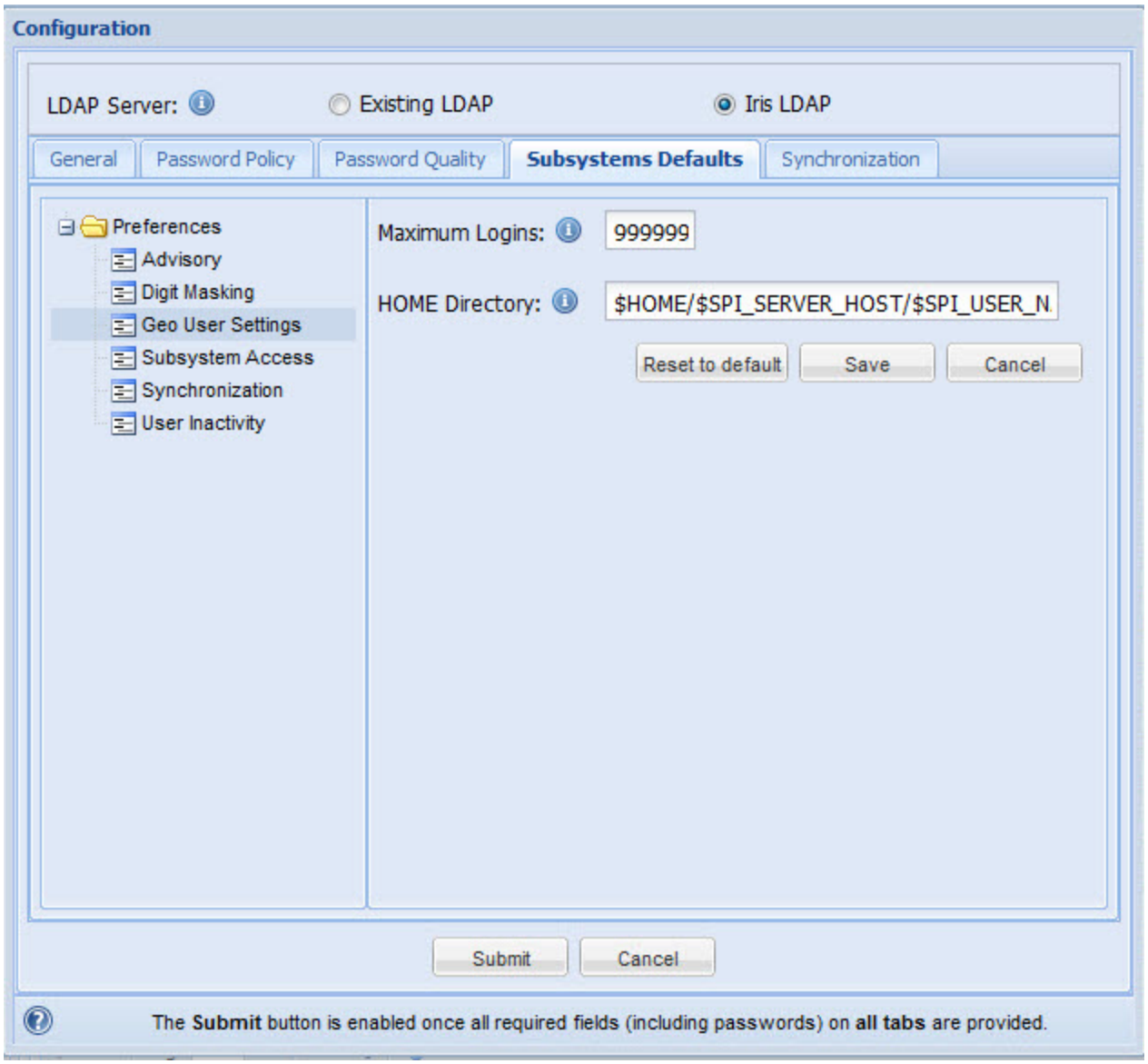
You can set the default Geo User settings for new users in this area.

Maximum Logins	Configure the number of simultaneous SpImain sessions a user can open.
HOME Directory	Configure the user's Unix HOME directory. The default is $HOME/$SPI_SERVER_HOST/$SPI_USER_NAME.

Configuration Controls

Reset to Default	Resets the Geo User Settings to 999999 and the default HOME directory.
Save	Saves the changes you made to the Geo User Settings.
Cancel	Cancel any changes you have made.

Geo User Settings Area



Subsystem Access

The Subsystem Access feature allows you to configure default subsystem access for new users. Subsystems available are: Iris, UACN/RIA, and GeoProbe. By default, new users have access to Iris, with UACN/RIA and GeoProbe access disabled. Individual user access can be changed on the User Details window.

Subsystem Enabled Area

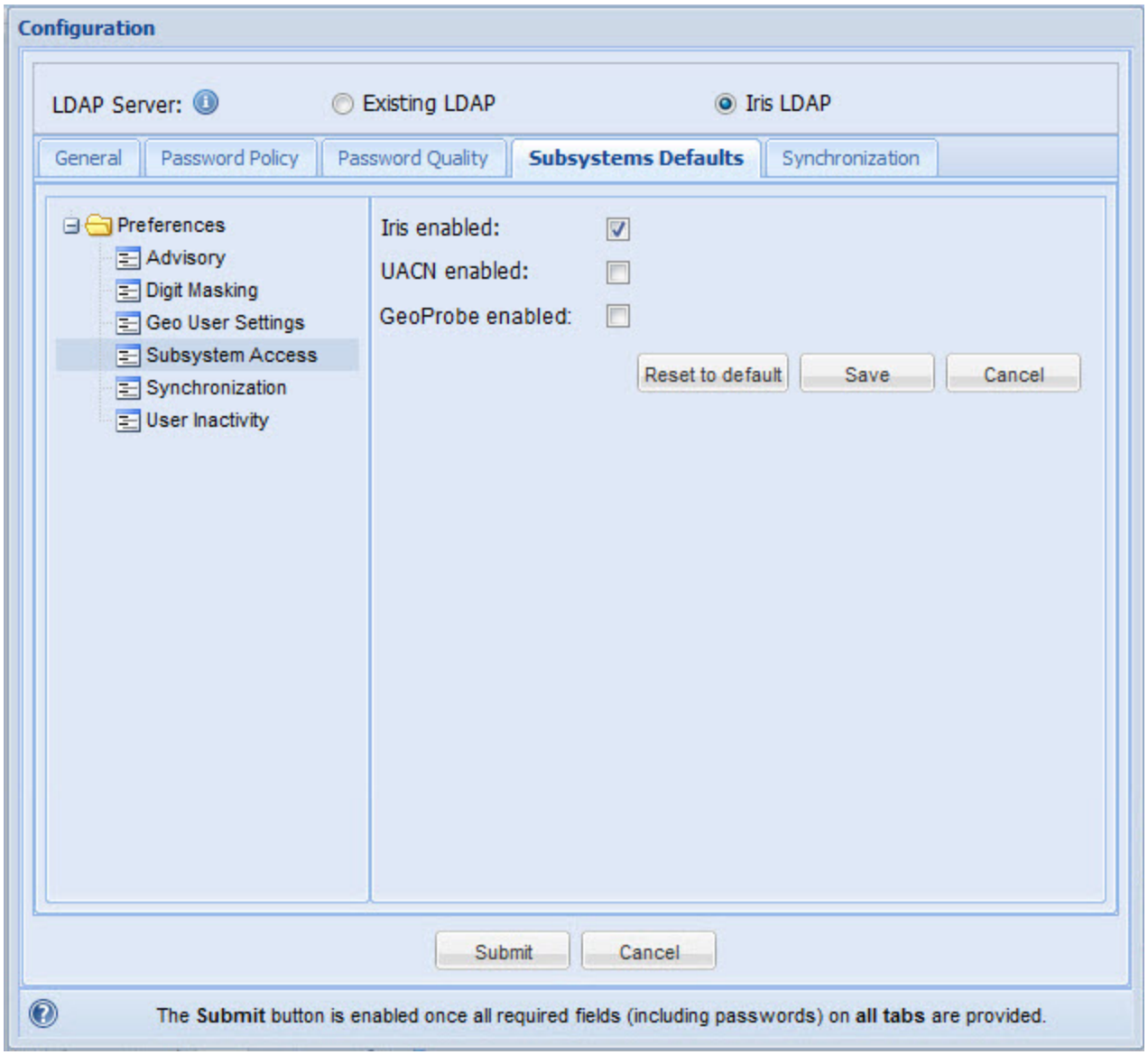
You can set the default system access for new users in this area.

Iris enabled	User has access to the Iris system.
UACN/RIA enabled	User has access to the UACN/RIA system.
GeoProbe enabled	User has access to the GeoProbe system.

Configuration Controls

Reset to Default	Resets the subsystem access to Iris enabled, UACN/RIA and GeoProbe disabled.
Save	Saves the changes you made to the subsystem access.
Cancel	Cancel any changes you have made.

Subsystem Access Area



Default Synchronization

The Synchronization feature on the Subsystem Defaults allows you to enable synchronization of the Geo and UACN/RIA imported user data automatically. You can synchronize manually using the Synchronization tab.

Synchronization Area

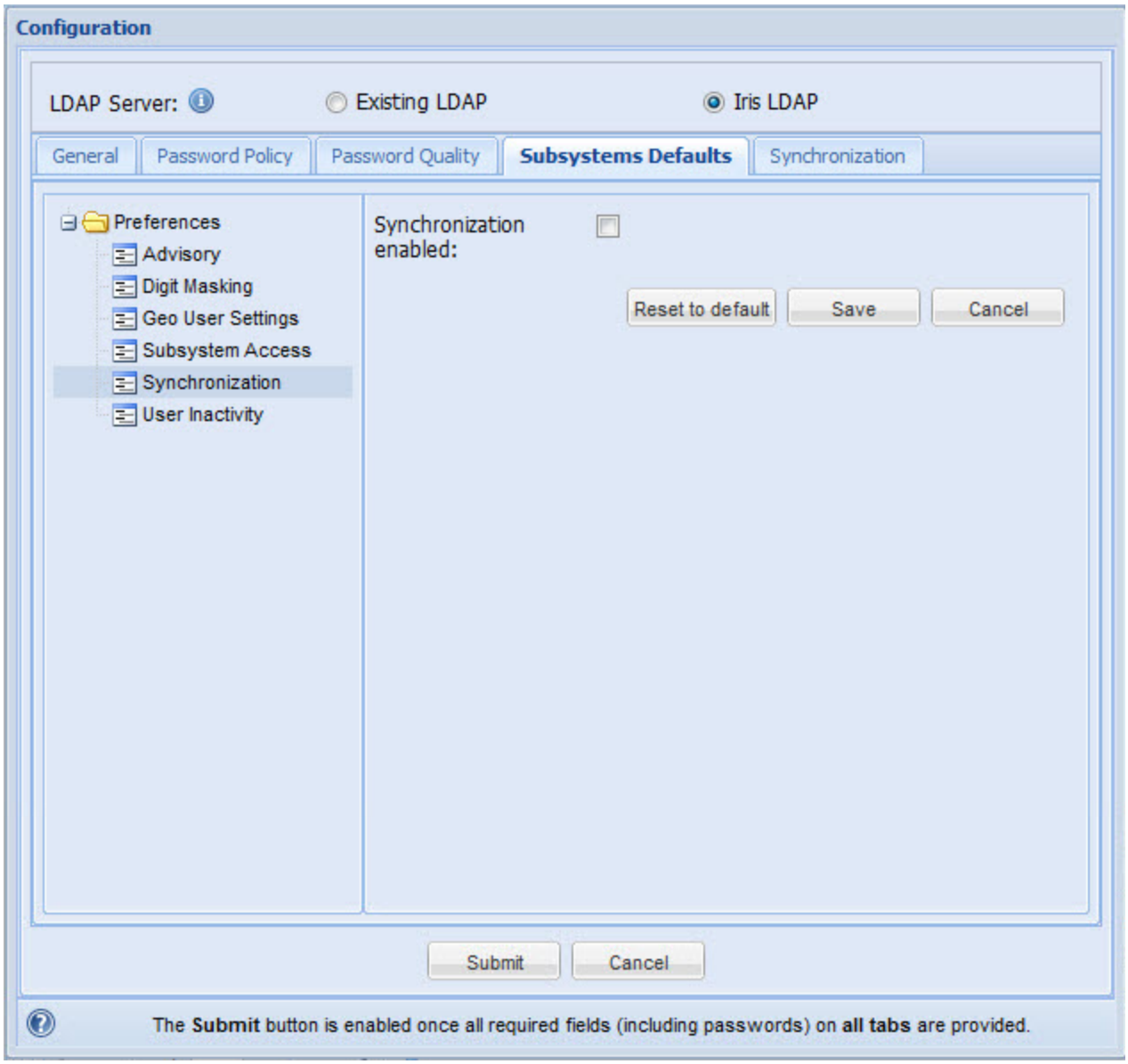
You can set the default synchronization in this area.

Synchronization enabled	You can check this option to automatically synchronize Geo and UACN/RIA user data.

Configuration Controls

Reset to Default	Resets the subsystem access to Iris enabled, UACN/RIA and GeoProbe disabled.
Save	Saves the changes you made to the subsystem access.
Cancel	Cancel any changes you have made.

Synchronization Area



User Inactivity

The User Inactivity feature allows you to configure default an inactivity timeout for users. You can set up a system-wide login inactivity time in number of days that will be applied to all users in the system. By default, this value is 30 days. Once the value is changed, it becomes effective to all subsequent user sessions. There is also a mechanism to disable the feature.

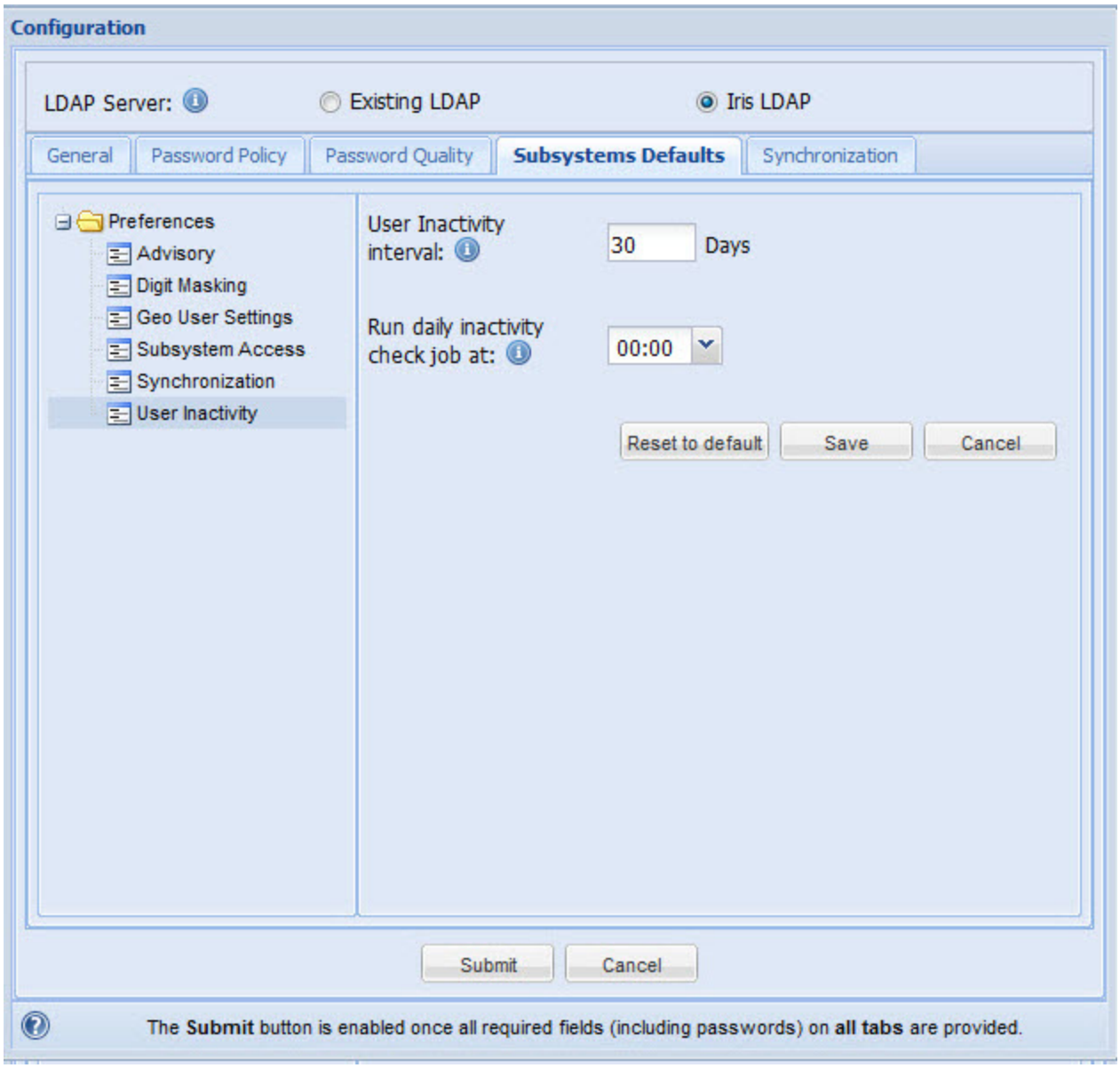
Interval Configuration Area

User Inactivity Interval	The number of days the user must be inactive before the account becomes Inactive. The default is 30 days.
Run daily inactivity check job at	The time the system will run checks on inactivity status. It is the local time for the server's location zone.

Configuration Controls

Reset to Default	Resets all settings to a default of 30 days.
Save	Saves the changes you made to the inactivity timeout settings.
Cancel	Cancel any changes you have made.

User Inactivity Area



Synchronization Tab

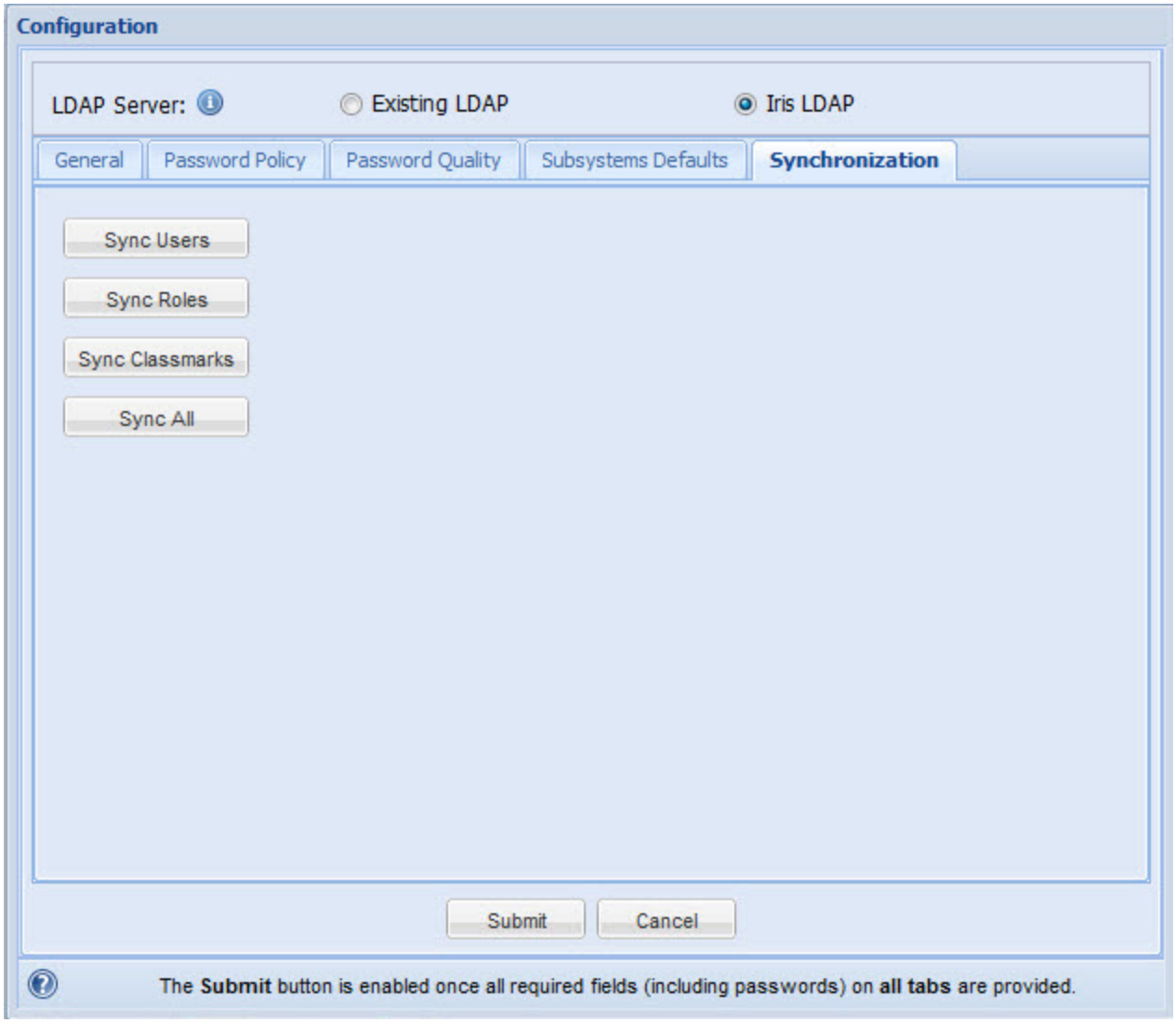
The Synchronization tab enables you to synchronize UACN/RIA and GeoProbe user data.

Sync Users button	Synchronize UACN/RIA and GeoProbe user lists.
Sync Roles	Synchronize UACN/RIA and GeoProbe roles.
Sync Classmarks	Synchronize GeoProbe classmarks.
Sync All	Synchronize all UACN/RIA GeoProbe user data, including user lists, roles, and GeoProbe classmarks.

Configuration Controls

Existing LDAP Option	These options are set up by Tektronix at installation. The Existing LDAP option is selected when your existing corporate LDAP is used. The Iris LDAP option is selected if the Iris LDAP was installed on initial system setup.
Iris LDAP Option	Iris LDAP Option
Submit Button	Submit and apply all UUMS configuration settings. This button is not enabled until all required fields are populated on all tabs.
Cancel Button	Close the window without making any changes.
Help Button	Open the UUMS Help.

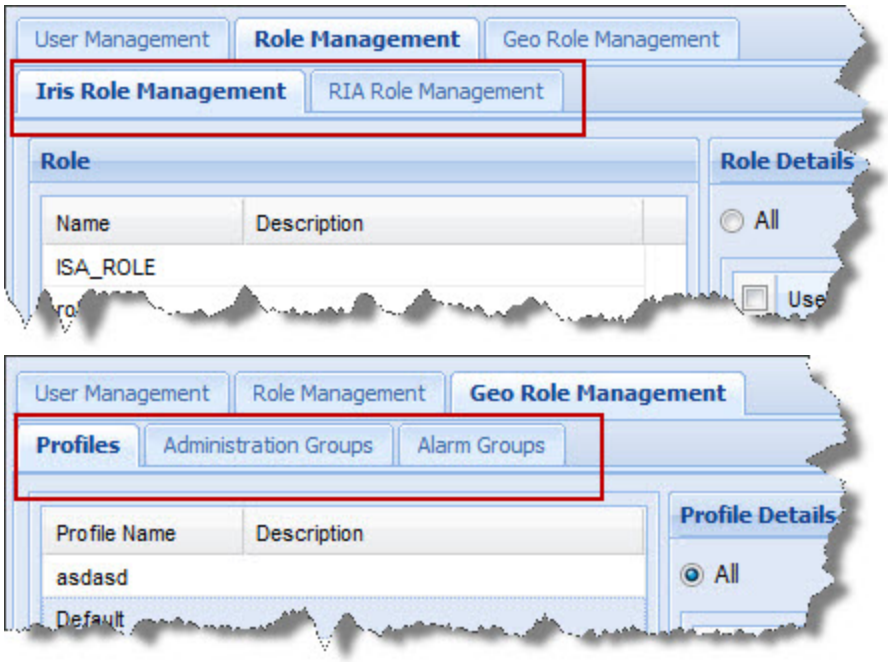
Synchronization Tab



UUMS Role Management

Role Management for Iris, UACN/RIA, and GeoProbe is accessed through the Role Management and GeoProbe Role Management tabs. From those tabs, you can configure roles, assign users, and for GeoProbe you can assign profiles, administration groups, and alarm groups.

Role Management Tabs



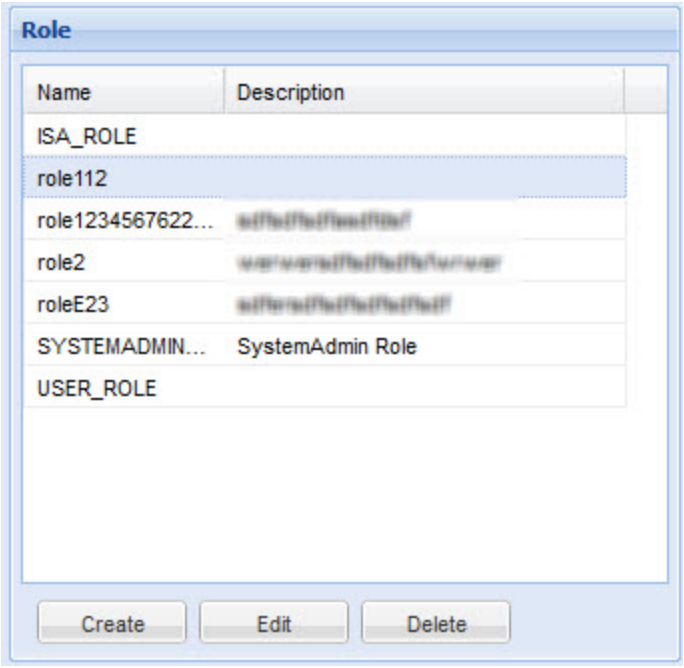
Role/Profile Pane

The Role/Profile pane enables you to create, rename, or delete roles that control system access with privileges. You assign users with similar functional duties to appropriate roles, using either the Role Management window or the User Management window. For Iris and UACN/RIA users this pane is called Roles; for GeoProbe users it is called Profiles, and is found under the Profiles tab under Geo Role Management.

Role Area Controls

Create Button	Open the Create Role or Create Profile dialog box, enter a name and description, and click OK to add a new role or profile. Role and Profile names can only contain alphanumeric characters; spaces and special characters are not allowed. The name is limited to 50 characters. Once a new role or profile is created, you can assign users and privileges to it.
Edit Button	Open a dialog box and change the name and description for the role or profile.
Delete Button	Open a dialog box and click OK to delete the selected role or profile. Any users assigned to the role or profile are unassigned to it once it is deleted.

Role or Profile Management Pane

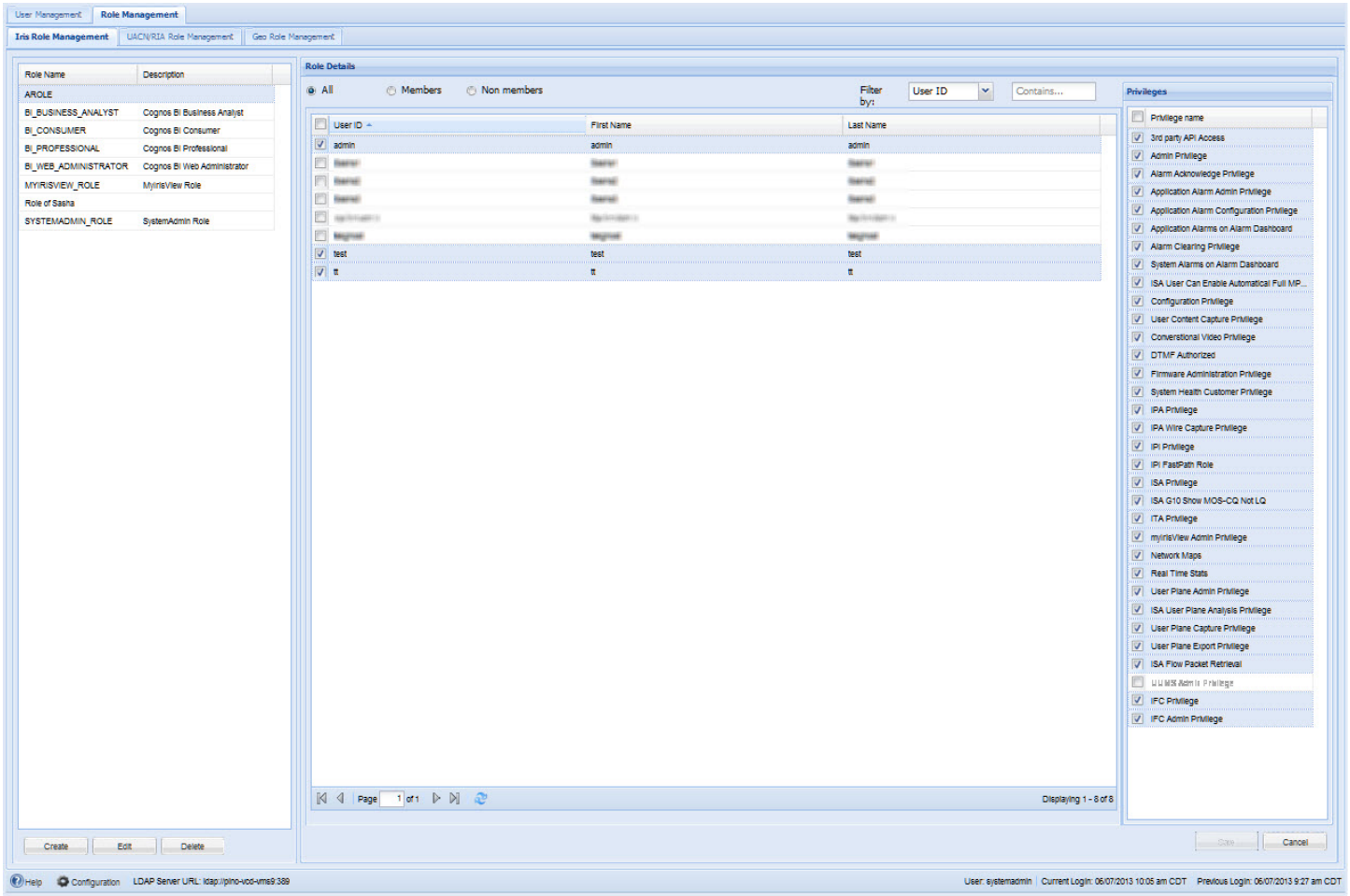


Role Management Window

The Role Management window helps you to manage roles that organize system access privileges for Iris, UACN/RIA, and GeoProbe. You assign users with similar functional duties to appropriate roles, using either the Role Management window or the User Management window.

Tab	Function
Iris Role Management Tab	View, create, edit, delete, and assign roles for the Iris subsystem.
UACN/RIA Role Management Tab	View, create, edit, delete, and assign roles for the UACN/RIA subsystem.
Geo Role Management Tab	View, create, edit, delete, and assign roles for the GeoProbe subsystem.
Role Pane	View the list of current roles. Click on a role to display the members and privileges in the adjacent panes. For an existing user database, a role migration script can be run to create functional roles using existing role assignments.
Role Details Pane	Assign user roles. If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary.
	Privileges: Lists the available privileges you can assign to a role.

Role Management Window



Iris Role Management Window

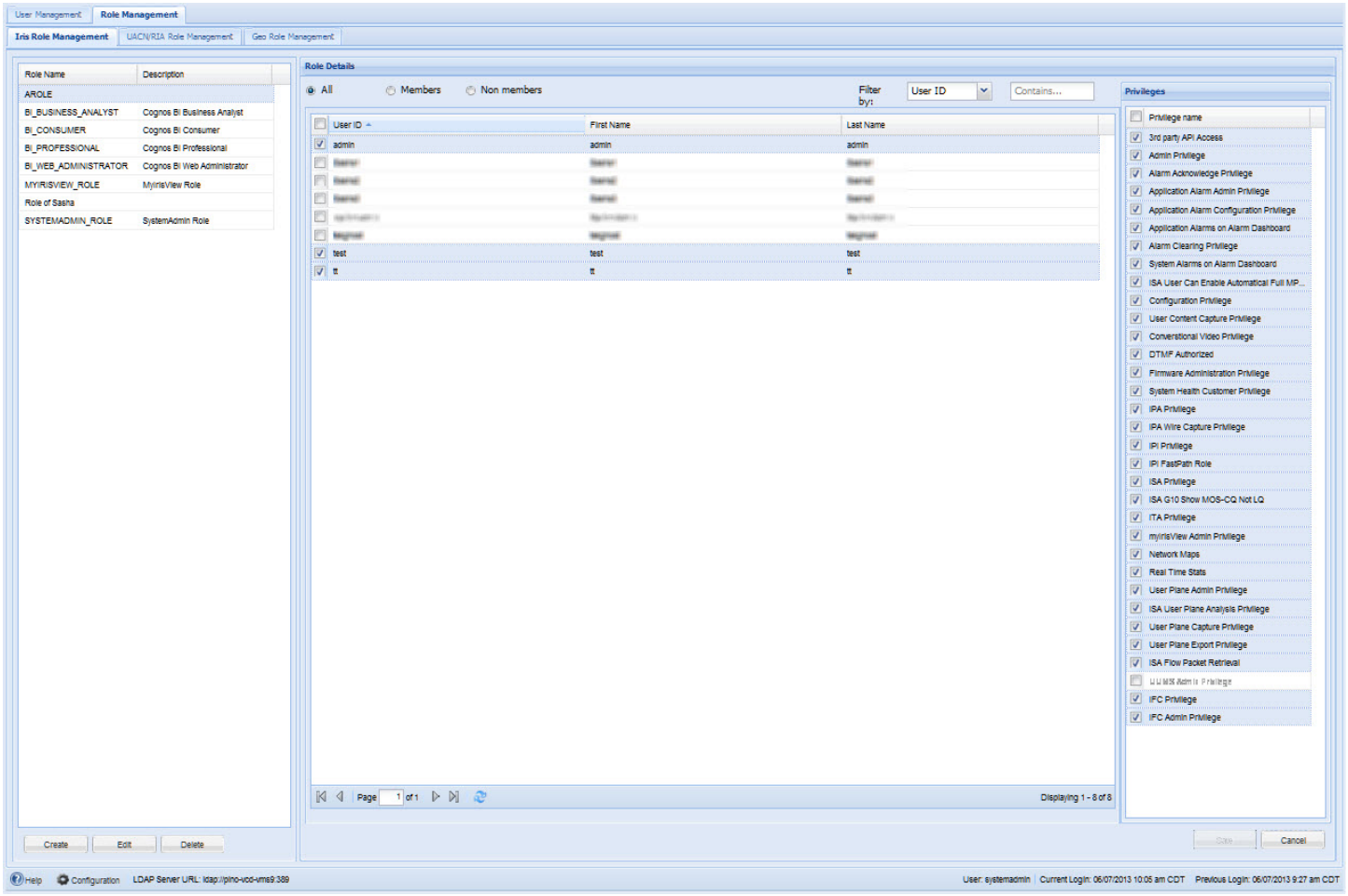
The Iris Role Management window enables you to create roles that control system access with privileges for the Iris subsystem. You assign users with similar functional duties to appropriate roles, using either the Role Management window or the User Management window.

Role Pane	View the list of current roles. Click on a role to display the members and privileges in the adjacent panes. For an existing user database, there is a role migration script as part of the installation that creates functional roles using existing role assignments.
Role Details Pane	Assign user roles. If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary. When you select either the mylrisView role or one of the Cognos roles: BI_Business_Analyst, BI_Consumer, BI_Professional, or BI_Web_Administrator, there is a slight difference in the information available.Because licenses define how many users can have access, you cannot assign users beyond the number of licenses available. There is an indicator for each role that tracks the number of licenses available and the number of users assigned to it. Refer to Assigning Licensable User Roles for more information.
	Privileges: Lists the available Iris privileges you can assign to a role.

Role Pane Controls

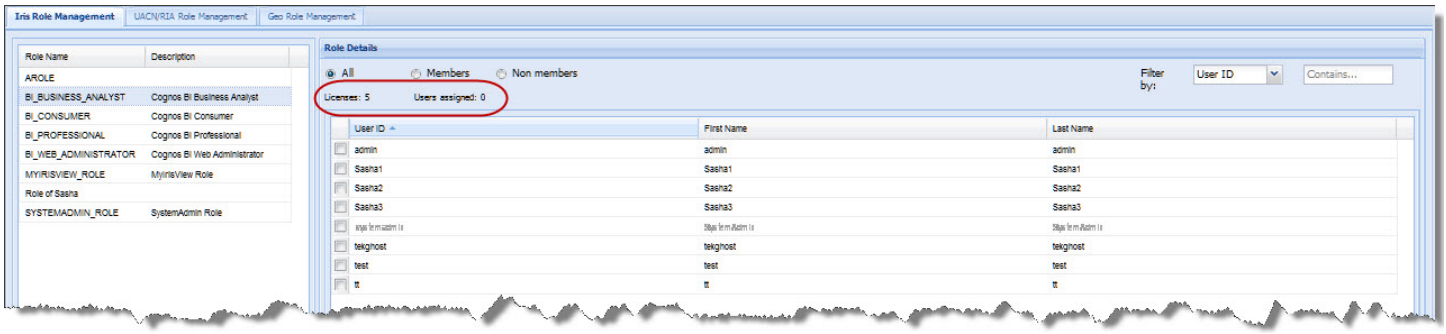
Create Button	Create a new role and add a description.
Edit Button	Edit the selected role name and description.
Delete Button	Delete the selected role.

Iris Role Management Window



Iris Licensable Role Management Window

When you select either the myIrisView role or a Cognos role, the license indicator is there to help you track how many licenses are available. In addition, you cannot change the privileges associated with a Cognos role, so no privileges are listed for those.



UACN/RIA Role Management Window

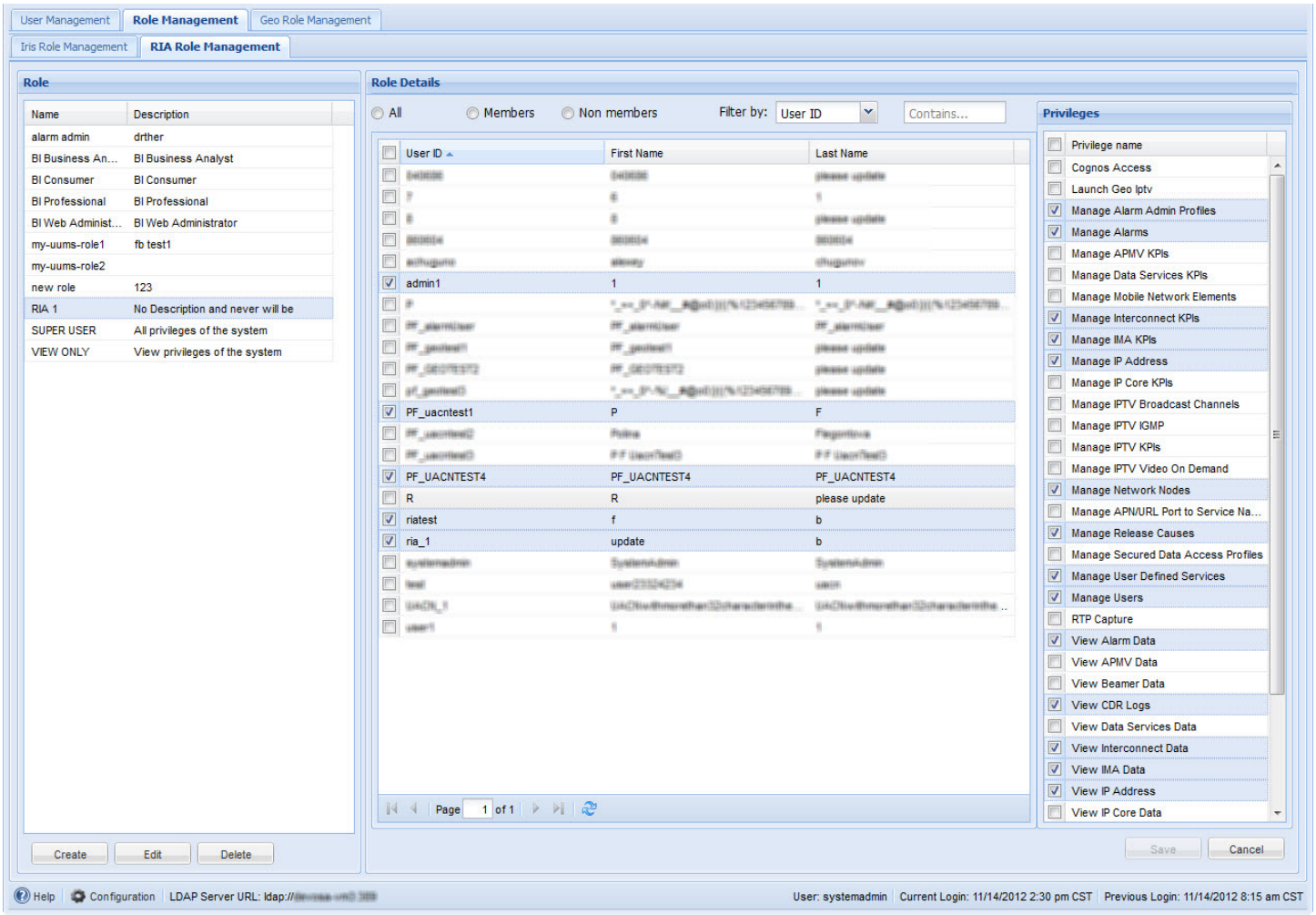
The UACN/RIA Role Management window enables you to create roles that control system access with privileges for the UACN/RIA subsystem. You assign users with similar functional duties to appropriate roles, using either the Role Management window or the User Management window.

Role Pane	View the list of current roles. Click on a role to display the members and privileges in the adjacent panes. For an existing user database, a role migration script can be run to create functional roles using existing role assignments.
Role Details Pane	Assign user roles. If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary.
	Privileges: Lists the available UACN/RIA privileges you can assign to a role.

Role Pane Controls

Create Button	Create a new role and add a description.
Edit Button	Edit the selected role name and description.
Delete Button	Delete the selected role.

UACN/RIA Role Management Window



Role Details Pane

The Role Details pane enables you to view or modify user role details and assign privileges. Some GUI and data management differences exist, depending on the configured LDAP.

Members Area	View the members and nonmembers assigned to each role, as well as a complete list of members in the database.
Privileges Selection Area	Assign Iris user privileges and UACN/RIA privileges. If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary on the GeoProbe system.

Role Details Pane Controls

GUI Element	Iris LDAP	Existing Corporate LDAP
Save Button	Save user role changes to the Iris LDAP and the Iris database. When creating a new role, this button is not enabled until at least one privilege is assigned to a role. Changes take effect the next time the user logs in.	Save user profile changes to the Iris database; modified data is not saved in the existing LDAP. Changes take effect the next time the user logs in.
Cancel Button	Close the Role Details Pane without saving changes.	

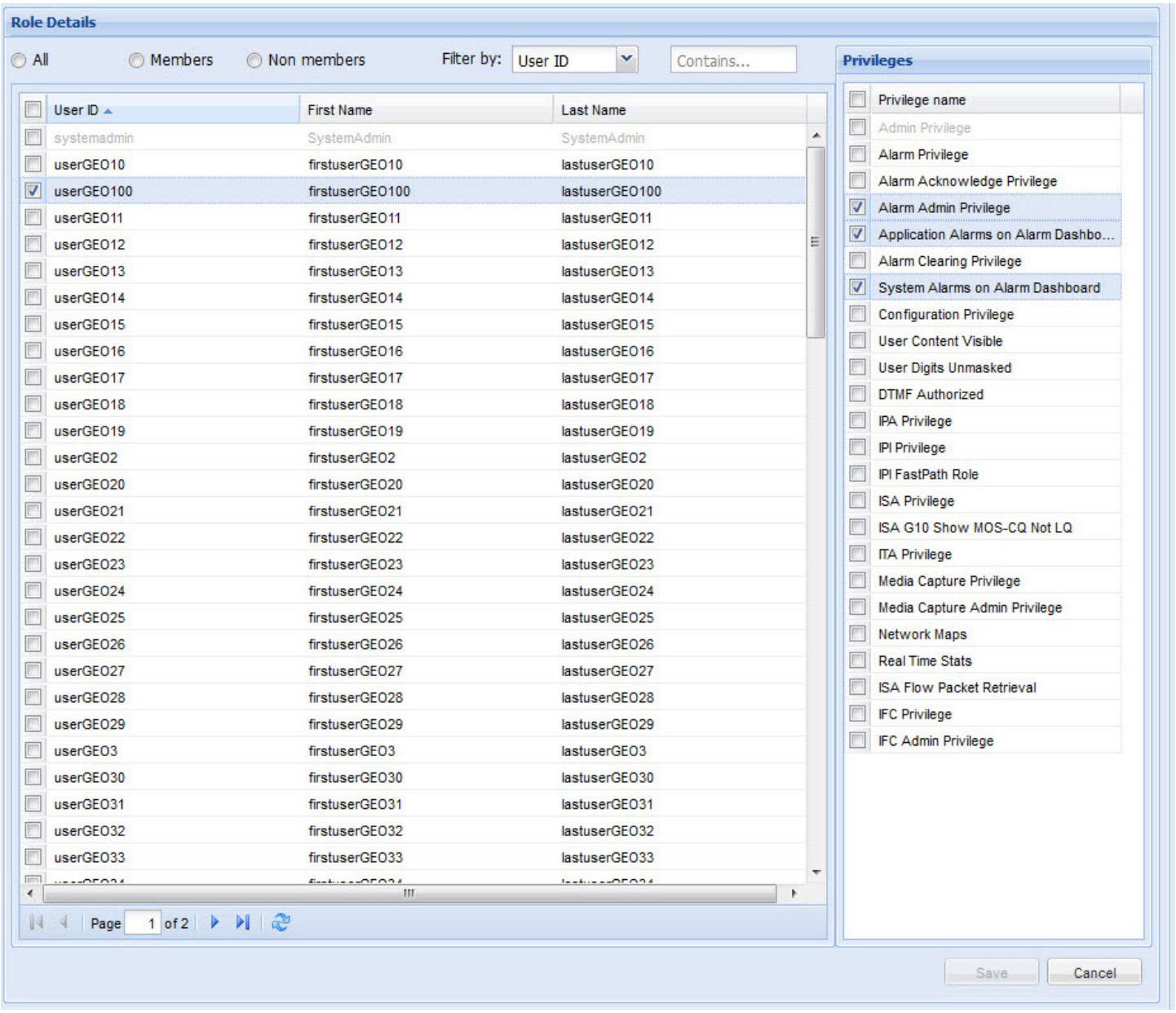
Members Area

GUI Element	Description
All radio button	View all of the users in the system.
Members radio button	View only the members of the selected group.
Non members radio button	View members NOT in the selected group.
Filter by:	Drop-down menu: You can filter by User ID, First Name, or Last Name.
	Contains field: You can enter a partial of the search criteria, and members meeting that criteria are displayed.

Privileges Selection Area

GUI Element	Iris LDAP	Existing Corporate LDAP
Privileges list	A list of all available privileges.	
Privilege Check Boxes	Select at least one privilege to assign to the currently selected role.	Roles (and thus privileges) are assigned when importing users on the Import LDAP Users dialog box. You can modify imported users' assigned roles.

Role Details Pane Example

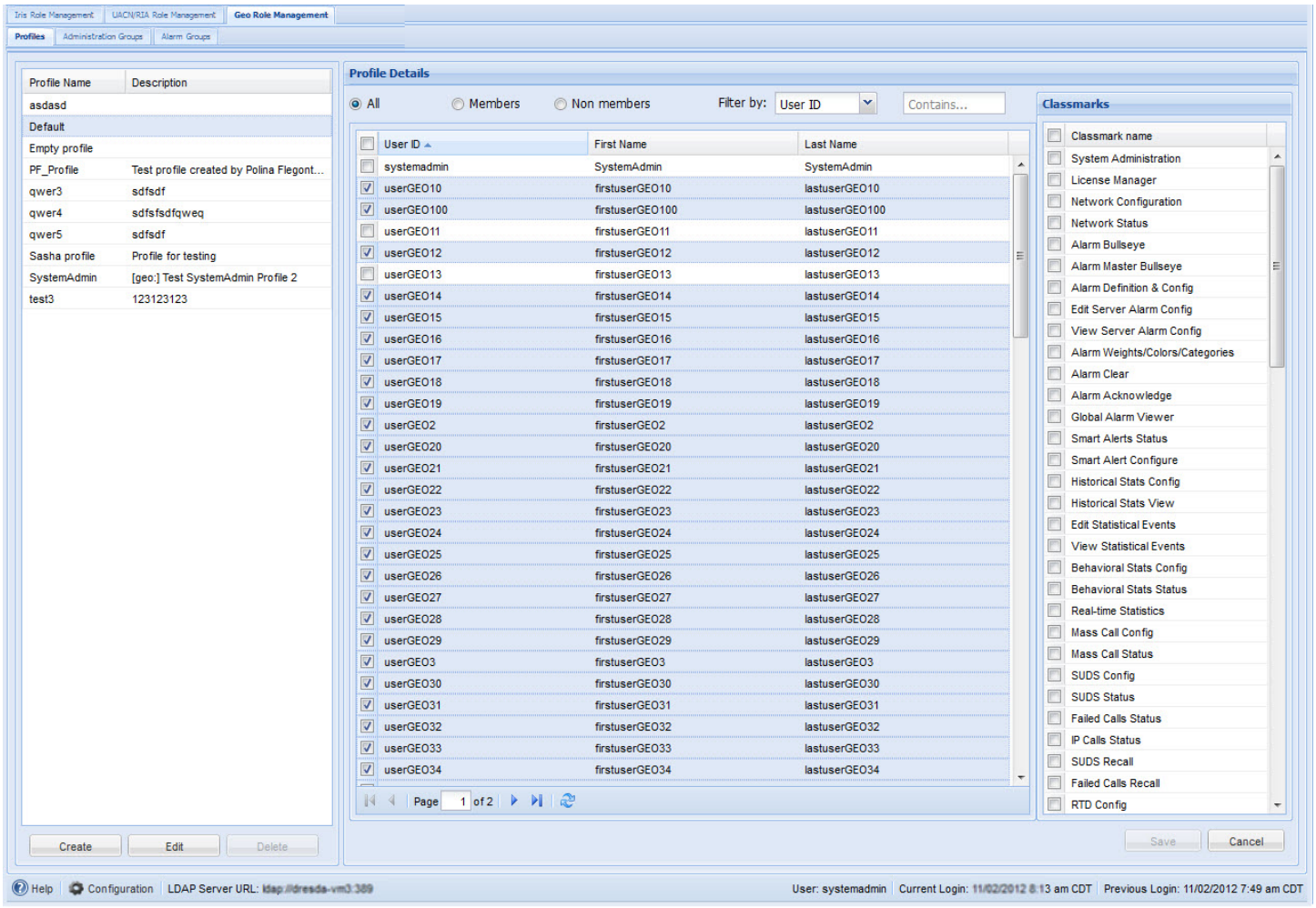


Geo Role Management Tab

The Geo Role Management tab enables you to create roles that control system access with profiles, classmarks, Administration Groups, and Alarm Groups for GeoProbe. You assign users with similar functional duties to appropriate profiles, using either the Geo Role Management window or the User Management window.

Profiles Tab	Lists the available profiles, and add, edit, or delete profiles.
Administration Groups Tab	Lists the available administration groups, and add, edit, or delete groups.
Alarm Groups Tab	Lists the sixteen available alarm groups. You can edit the alarm group name, but you cannot create or delete one.
Profile Details Pane	Assign user Profiles, Administration Groups, and Alarm Groups. If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary.
	Classmarks: Lists the available classmarks you can assign to a profile.

Geo Role Management Window



Geo Role Management Profiles Tab

The profile assigned to a user determines the user's restrictions and capabilities in the GeoProbe system. You can assign profiles to users in the Profiles window. You can the same profile to multiple users. Changes to the profile affect all users with that profile. This enables you to define or change restrictions or capabilities for multiple users in one step.

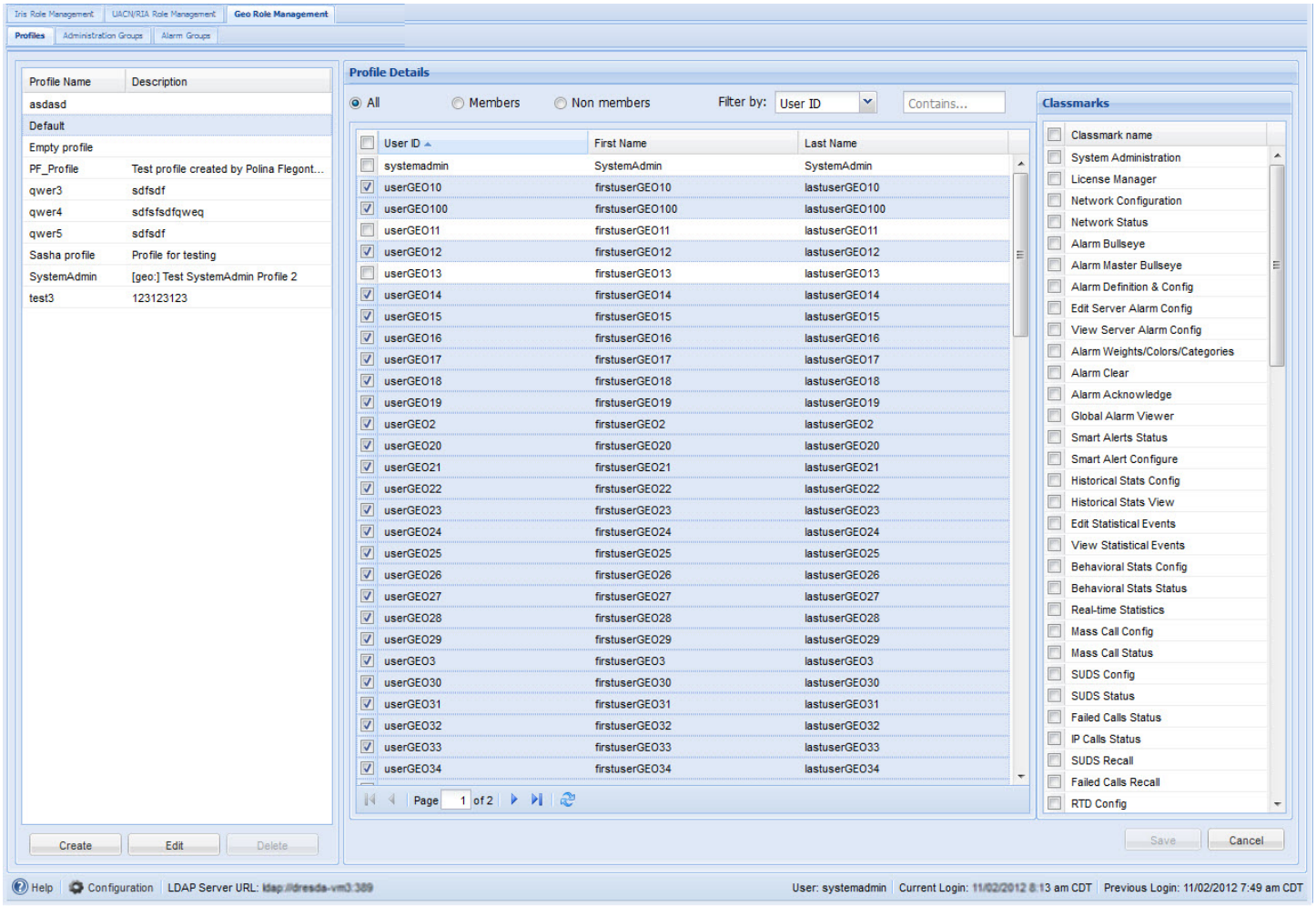
You assign users with similar functional duties to appropriate profiles, using either the Geo Role Management Profiles window or the User Management window.

Profile Pane	View the list of current profiles. Click on a profile to display the members and classmarks in the adjacent panes.
Profile Details Pane	Assign user profiles. If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary.
	Classmarks: Lists the available classmarks you can assign to a profile.

Profile Pane Controls

Create Button	Create a new profile and add a description.
Edit Button	Edit the selected profile name and description.
Delete Button	Delete the selected profile.

Geo Role Management Window Profiles Tab



Profile Details Pane

The Profile Details pane enables you to view or modify user profile details and assign classmarks. Some GUI and data management differences exist, depending on the configured LDAP.

Members Area	View the members and nonmembers assigned to each role, as well as a complete list of members in the database.
Classmarks Selection Area	Assign GeoProbe classmarks. If ISA and PA users will need access to SpIprobes for data capture and filtering, additional user administration is necessary on the GeoProbe system.

Profile Details Pane Controls

GUI Element	Iris LDAP	Existing Corporate LDAP
Save Button	Save user role changes to the Iris LDAP and the Iris database. When creating a new role, this button is not enabled until at least one privilege is assigned to a role. Changes take effect the next time the user logs in.	Save user profile changes to the Iris database; modified data is not saved in the existing LDAP. Changes take effect the next time the user logs in.
Cancel Button	Close the Profile Details Pane without saving changes.	

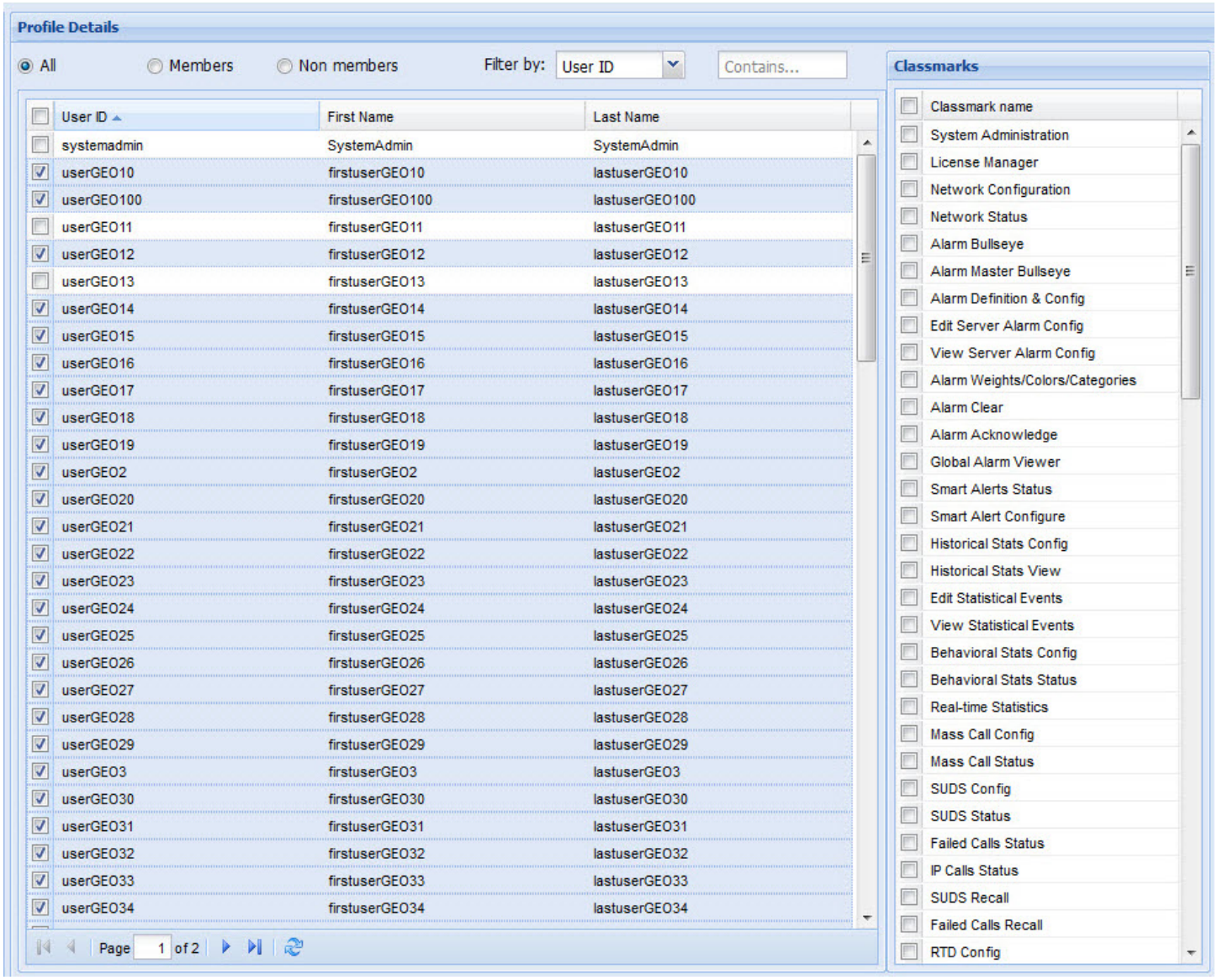
Members Area

GUI Element	Description
All radio button	View all of the users in the system.
Members radio button	View only the members of the selected group.
Non members radio button	View members NOT in the selected group.
Filter by:	Drop-down menu: You can filter by User ID, First Name, Last Name, or Role Name.
	Contains: You can enter a partial of the search criteria, and members meeting that criteria are displayed. Role Name allows you to view users for the selected role.

Classmarks Selection Area

GUI Element	Description
Classmarks list	A list of all available classmarks.
Classmark Check Boxes	Select at least one classmark to assign to the currently selected profile.

Profile Details Pane Example



Geo Role Management Administration Groups Tab

Admin Groups enable you to set configurations for multiple users in one step. Users belonging to the same group share group views for GeoProbe maps. Regional administrators belonging to the same group share administration privileges for the same regional networks.

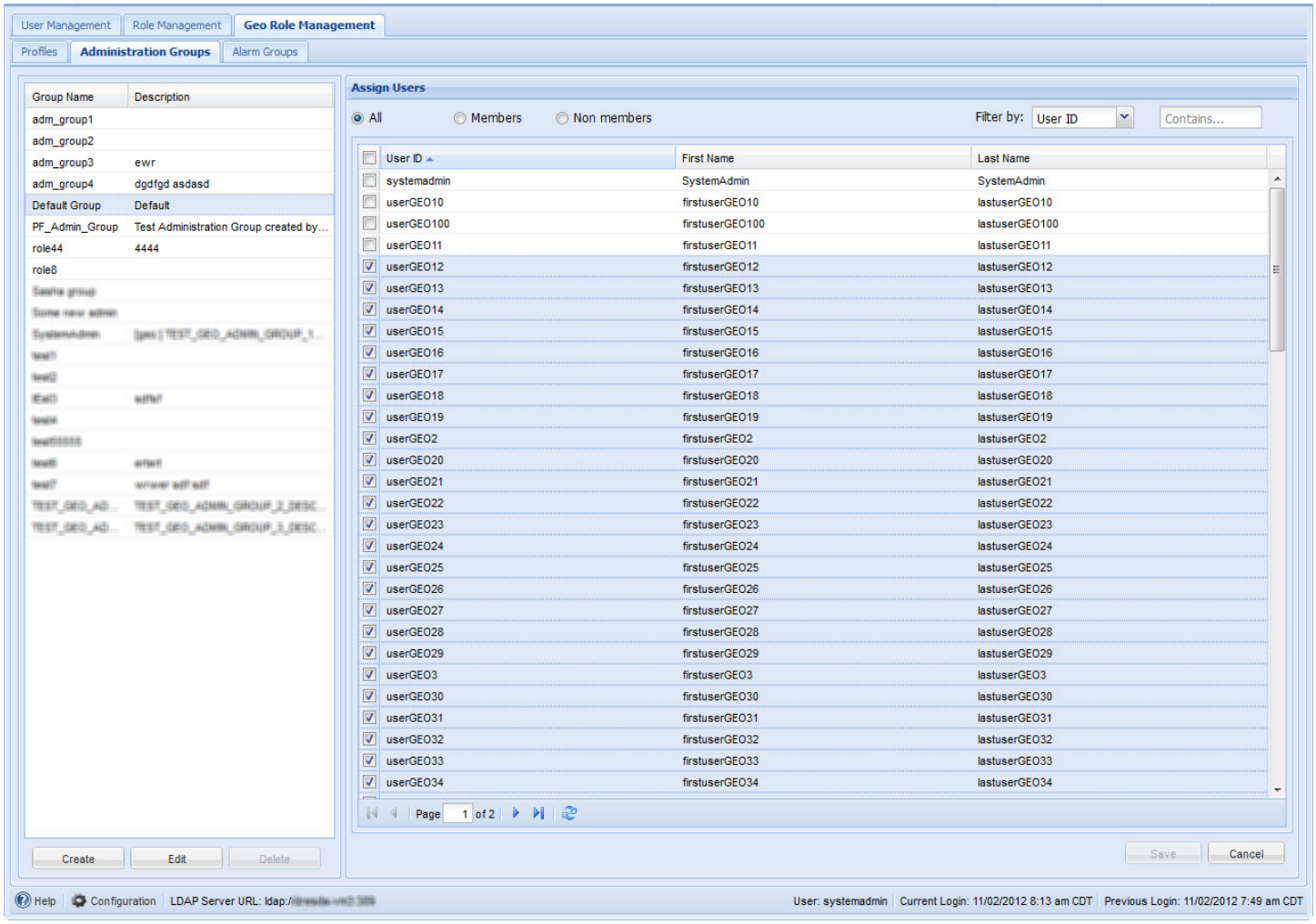
You assign users with similar functional duties to the appropriate Admin Group, using either the Geo Role Management Administration Groups window or the User Management window.

Group Pane	View the list of current Admin Groups. Click on a group to display the members in the adjacent pane.
Assign Users Pane	Place a check mark next to a user name to assign that user to an Admin Group.

Admin Group Pane Controls

Create Button	Create a new group and add a description.
Edit Button	Edit the selected group name and description.
Delete Button	Delete the selected group.

Geo Role Management Window Administration Groups Tab



Geo Role Management Alarm Groups Tab

Alarms appear on GeoProbe network maps based on defined alarm severity levels and alarm colors. You can assign users to specific alarm groups to control how alarms appear to the user on the network maps. Users in the same alarm group see the same alarms and alarm displays.

Sixteen alarm groups are available. They are numbered 2 through 16; Alarm Group 1, by default, is named Default Group.

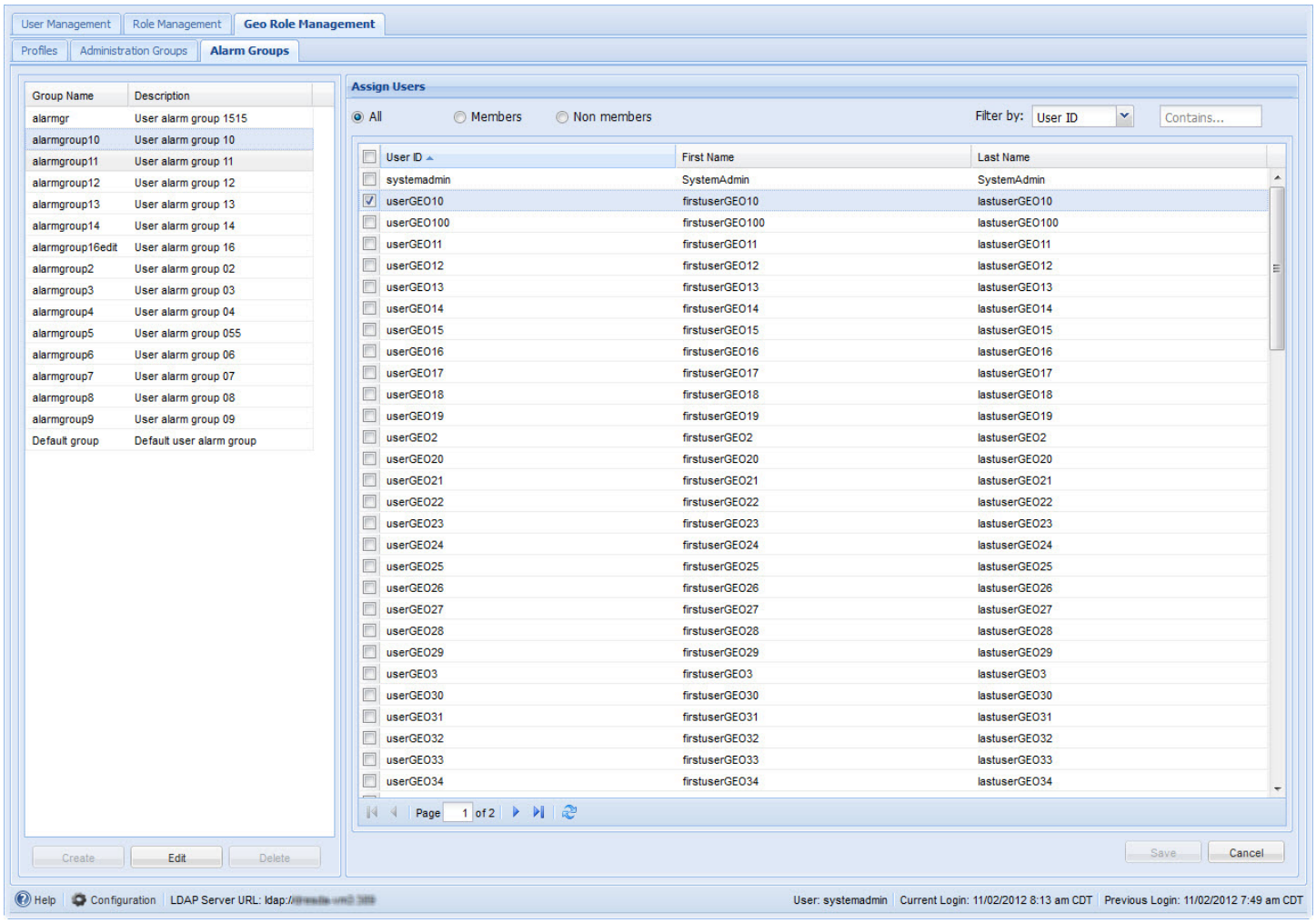
You assign users with similar functional duties to an appropriate Alarm Group, using either the Geo Role Management Alarm Groups tab or the User Management window.

Group Pane	View the list of current Alarm Groups. Click on a group to display the members in the adjacent pane.
Assign Users Pane	Place a check mark next to a user name to assign users to an Alarm Group.

Alarm Group Pane Controls

Create Button	The Create button is inactive; no new groups can be created. Alarm Groups 1-16 are available.
Edit Button	Edit the selected group name and description.
Delete Button	The Delete button is inactive. Alarm Groups cannot be deleted.

Geo Role Management Window Alarm Groups Tab



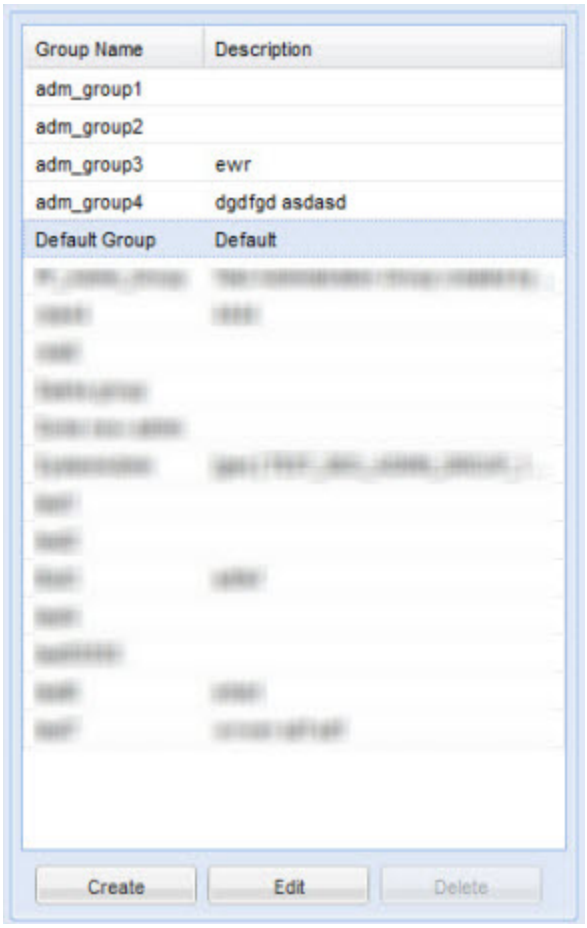
Group Pane

The Group pane enables you to create, rename, or delete Administration and Alarm Groups that control system access for GeoProbe users. You assign users with similar functional duties to appropriate groups, using either the Role Management window or the User Management window.

Group Area Controls

Create Button	Open the Create Group dialog box, enter a name and description, and click OK to add a new group. Group names can only contain alphanumeric characters; spaces and special characters are not allowed. Once a new group is created, you can assign users to it.
Edit Button	Open a dialog box and enter the new name or description for the group.
Delete Button	Open a dialog box and click OK to delete the selected group.

Group Management Pane



Assign Users Pane

The Assign Users pane enables you to view or modify members of the GeoProbe administration groups and alarm groups. Some GUI and data management differences exist, depending on the configured LDAP.

Members Area	View the members and nonmembers assigned to each role, as well as a complete list of members in the database.

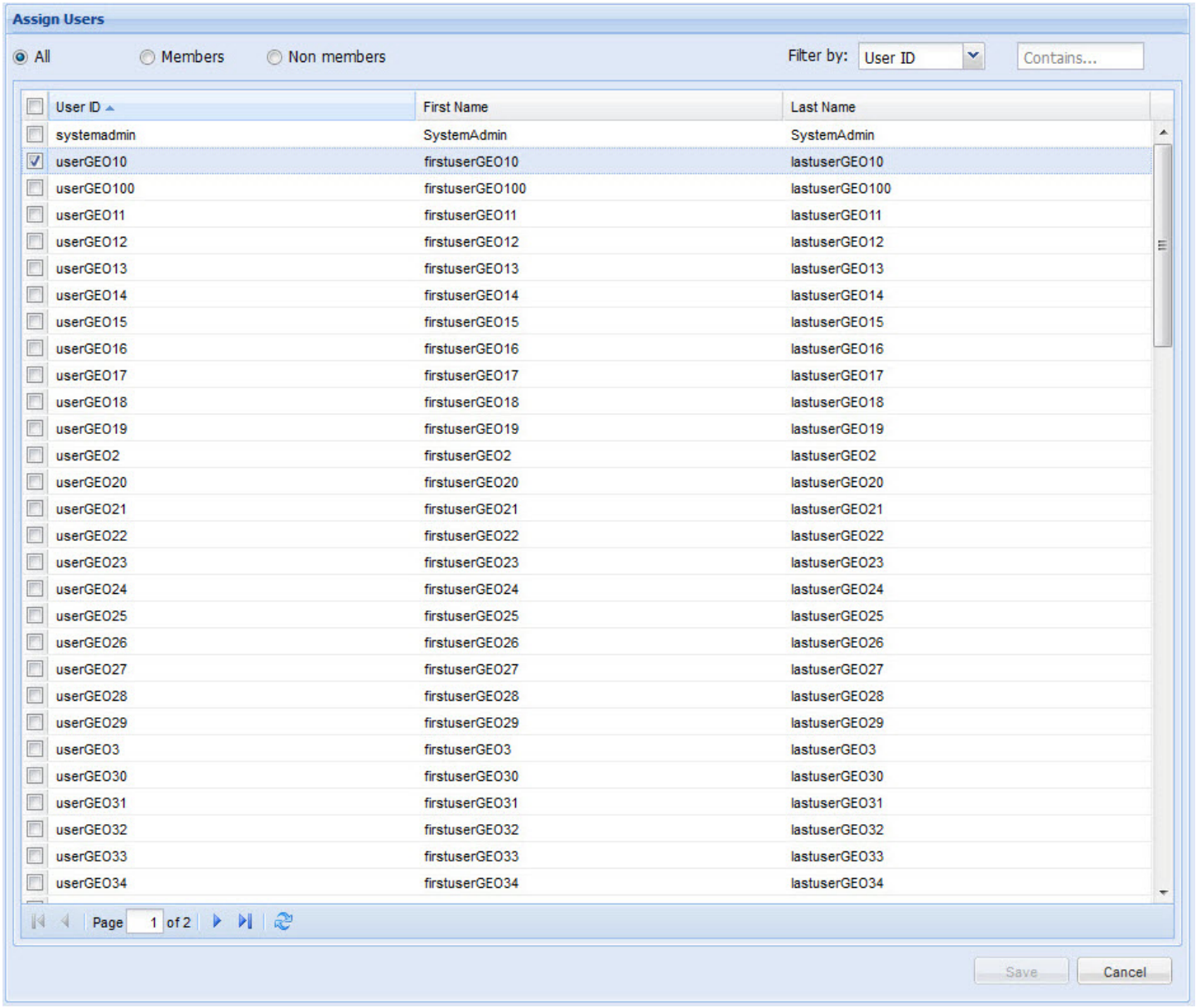
Assign Users Pane Controls

GUI Element	Iris LDAP	Existing Corporate LDAP
Save Button	Save user role changes to the Iris LDAP and the Iris database. When creating a new role, this button is not enabled until at least one privilege is assigned to a role. Changes take effect the next time the user logs in.	Save user profile changes to the Iris database; modified data is not saved in the existing LDAP. Changes take effect the next time the user logs in.
Cancel Button	Close the Assign Users pane without saving changes.	

Members Area

GUI Element	Description
All radio button	View all of the users in the system.
Members radio button	View only members of the selected group.
Non members radio button	View members NOT in the selected group.
Filter by:	Drop-down menu: You can filter by User ID, First Name, or Last Name.
	Contains field: You can enter a partial of the search criteria, and members meeting that criteria are displayed. Role Name allows you to view users for the selected role.

Assign Users Pane Example

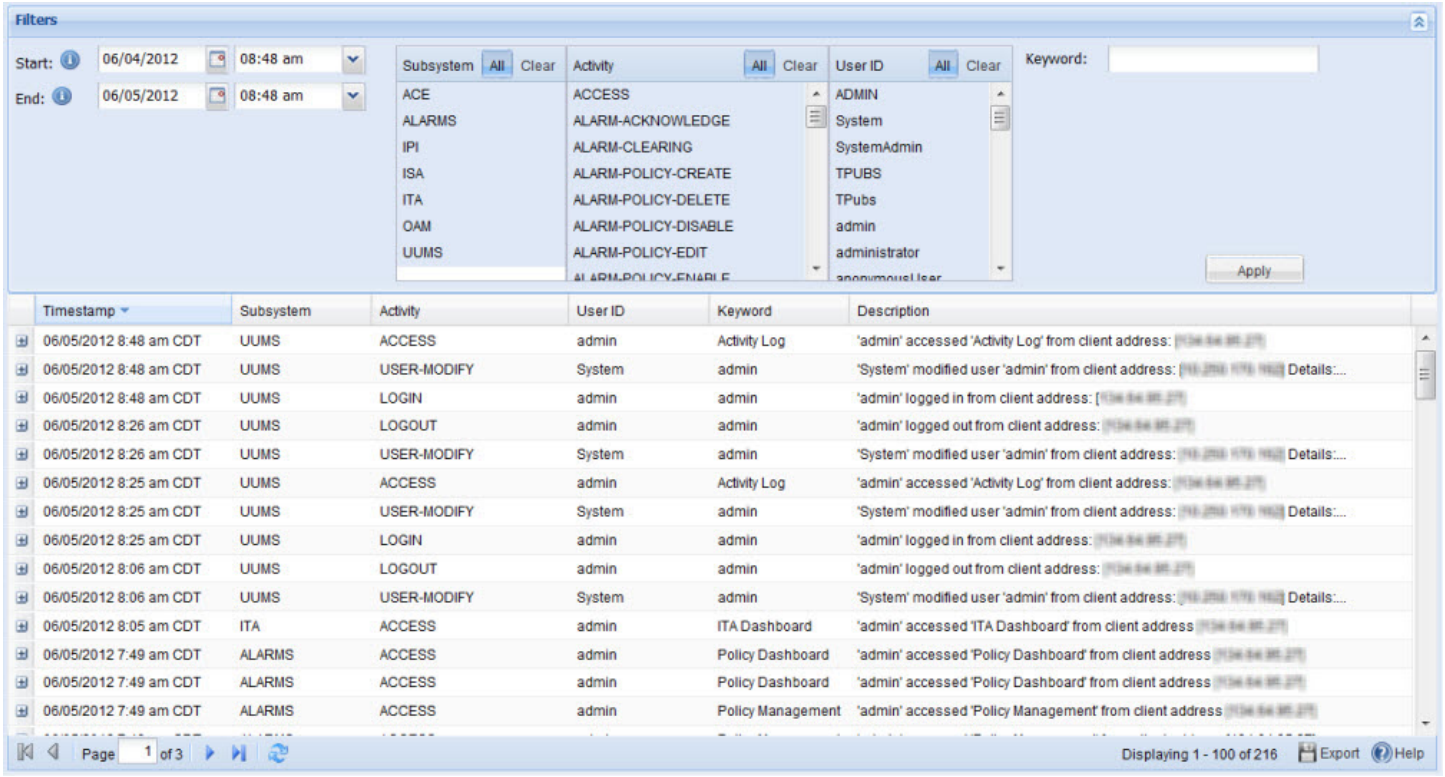


Activity Log Window

You use the Activity Log Window to monitor user activity for different Iris applications. You access this window by clicking the Admin button on the IrisView toolbar and clicking Activity Log. There is a delay of about 15 minutes for the list filter of activities in the top panel of the Activity Log to be updated to include all of the activities. After the time delay, if the list still does not automatically update, you can refresh the browser to update the list or run a query on another subsystem, then re-run it on the original subsystem for the list to be updated.

Filters Pane	Contains filters to control the activities displayed in the Log Browser.
Log Browser	Contains a table listing all activities that have occurred in the selected time frame.

Activity Log Window



Filters Pane

You use the Filters Pane to control the activity data displayed in the Log Browser. You access this window by clicking the Admin button on the IrisView toolbar and clicking Activity Log from the drop-down menu.

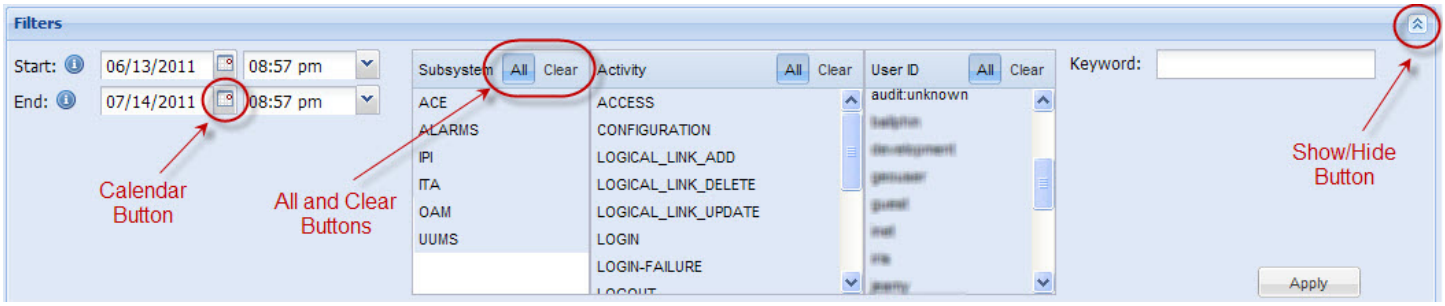
Filters

Start/End Date Field Calendar Button Start/End Time Drop-down Menu	• The Start Date/Time field is set to the previous day's date and the End Date/Time field is set to the current date (both set with current time), so the Activity Log shows all logged events for the previous 24 hours. • Enter the filter Start or End Date by changing the value in the field or by selecting it from a calendar. • To open the calendar, click the Calendar button and then click the Start or End Date. • End Date and Time cannot be greater than the current Date and Time.
Subsystem	Select one or more Iris subsystems as a filter. Data availability during the selected time frame and licensed applications affect which subsystem filters are available.
Activity	Select one or more user or system activities as a filter. Previous filter selections and data availability affect which Activity filters display in the list. There may be a delay of as much as 15 minutes for the list of Activity filters to reflect all current activities. You can update the list by refreshing your browser, or you can run a query on another subsystem, then re-run the query on the subsystem you are interested in.
User ID	Select one or more User IDs as a filter. Previous filter selections and data availability affect which User ID filters are available. **Note:** The User ID filter not only includes valid Iris users, but also includes any invalid user names that tried to log in to the Iris system but failed.
Keyword	Enter a keyword to use as a filter. Keywords are not case sensitive, and you can use an asterisk (*) to replace multiple characters in any part of the keyword. Applicable keywords vary by subsystem.

Filter Controls

All Button	Select all elements for a filter (subsystem, activity, User ID).
Clear Button	Clear all elements for a filter.
Show/Hide Button	Hide or show the Filters pane.
Apply Button	Apply your filter settings to the Log Browser.

Filters Pane



Log Browser

You use the Log Browser to monitor system and user activity for different Iris applications. You access this window by clicking the Admin button on the IrisView toolbar and clicking Activity Log from the drop-down menu.

Column Filters	Sort column data using the Column Filter controls.
Expand/Collapse Buttons Activity Details Area	Click plus (+) button in the first column to expand the row and view the associated activity description details.

Columns

Timestamp	Time the activity occurred (Iris Client timezone).
Subsystem	Iris application logging the event.
Activity	Event being logged, such as "USER-CREATE" or "LOGIN-FAILURE".
Username	User ID of user performing action.
Keyword	An additional level of detail, which varies per subsystem and on which you can filter.
Description	Additional details about the activity such as topology details, quantity of elements processed during activity, or IP address of the user accessing the subsystem.

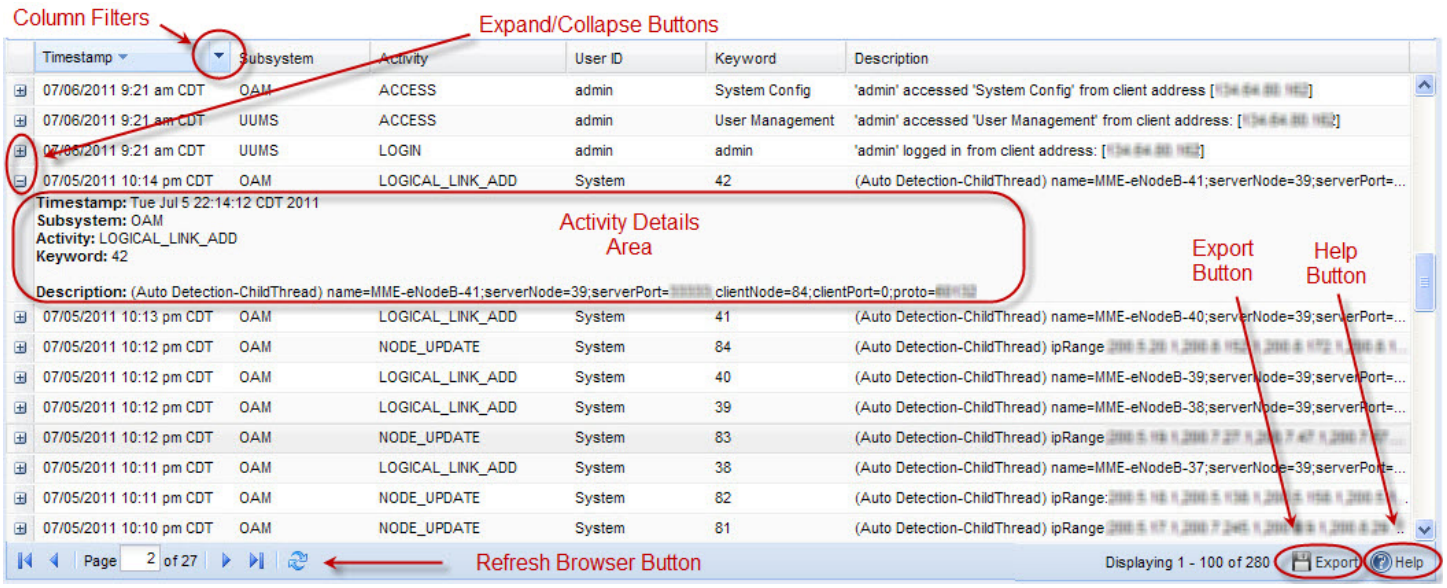
Column Filter Controls

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the checkmark from columns you want to hide. At least one column must remain visible.

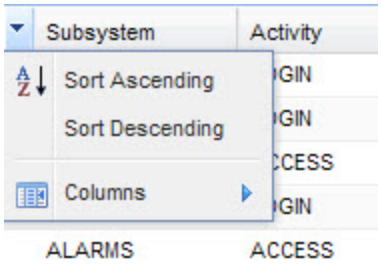
Browser Controls

Last / Next Page Buttons	Navigate to view activities in multiple pages.
First / Last Page Buttons	Go to the first or last page of the Activity Browser.
Browser Refresh Button	Manually refresh the data displayed in the Activity Browser.
Export Button	Open the Export dialog box to export select log data to a CSV file or PDF file.
Help Button	Open the Activity Log Help.

Log Browser



Column Filter

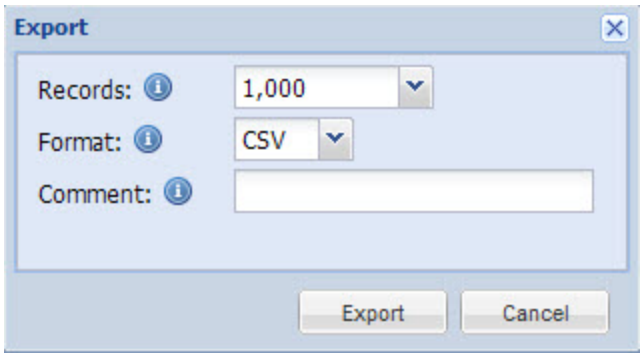


Export Dialog Box

Use the Export dialog box to export Activity Log data to a PDF or CSV file format. You access this dialog box when you click the Export button in the Log Browser. Select specific data for export by applying filters to the Log Browser and configuring export settings.

Records Drop-down Menu	Select the number of records to export: • 1,000 • 10,000 • Current page (default is 100 activities) Records are exported based on current filter and sort settings.
Format Drop-down Menu	Select CSV or PDF file format.
Comment	(Optional) Enter text you want to add at the beginning of the file to describe the exported activity data.
Export Button	Open a File Download dialog box and select either the Open or Save option. • Open - CSV files open in either a text editor or Microsoft Excel; PDF files open in Acrobat Reader. • Save - select a location from the Save As dialog box to save the file.
Cancel Button	Close the dialog box without saving changes.

Export Dialog Box



Chapter 4 References

This chapter provides UUMS reference information.

UUMS References

The following references are included for UUMS:

User Management	• Inactivity Timeout • Supported LDAPs • Setting Up GeoProbe User Accounts for Iris ISA and PA Applications • TMF615 API
Role Management	• UUMS User Privileges Overview • Iris User Privileges • UACN/RIA User Privileges • Cognos User Roles • GeoProbe Classmarks
Activity Log	• Activity Types • Activity Log Aging • Export File Formats
Configuration	• Account Migration • Role and Privilege Migration • Import UACN Roles and Privileges • Import GeoProbe Profiles, Groups, and Classmarks • Password Migration • Single System Administrator Functions • User Management Command Line Interface

Inactivity Timeout

The Inactivity Timeout feature allows you to identify and remove inactive users. You can set up a system-wide login inactivity time in number of days that will be applied to all users in the system. By default, this value is 30 days. After the value is changed, it becomes effective to all subsequent user sessions. There is also a mechanism to disable the feature.

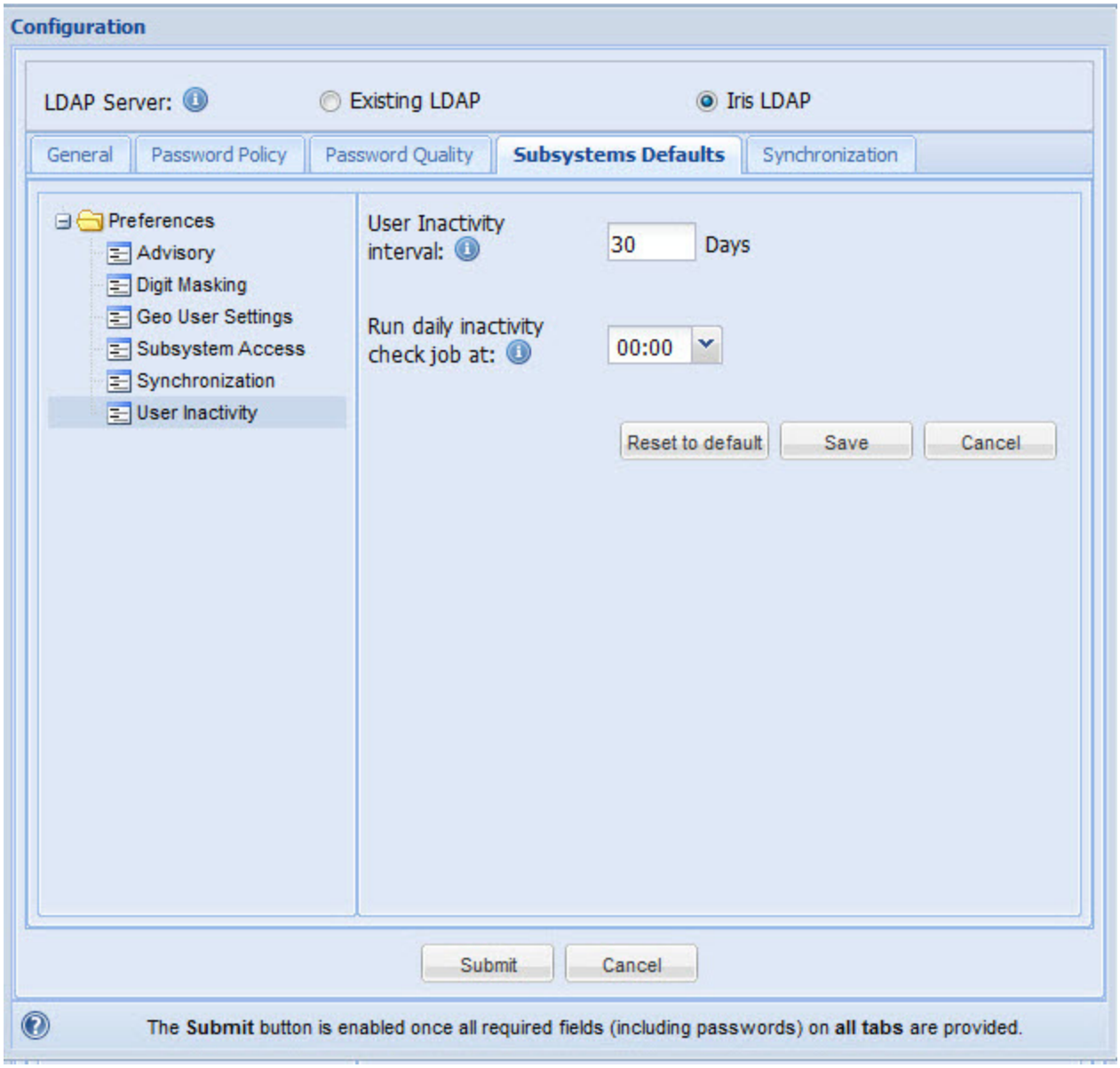
The default administrator users with the Administrator role are exempted from this inactive timeout requirement.

Enforcing Login Inactivity Time

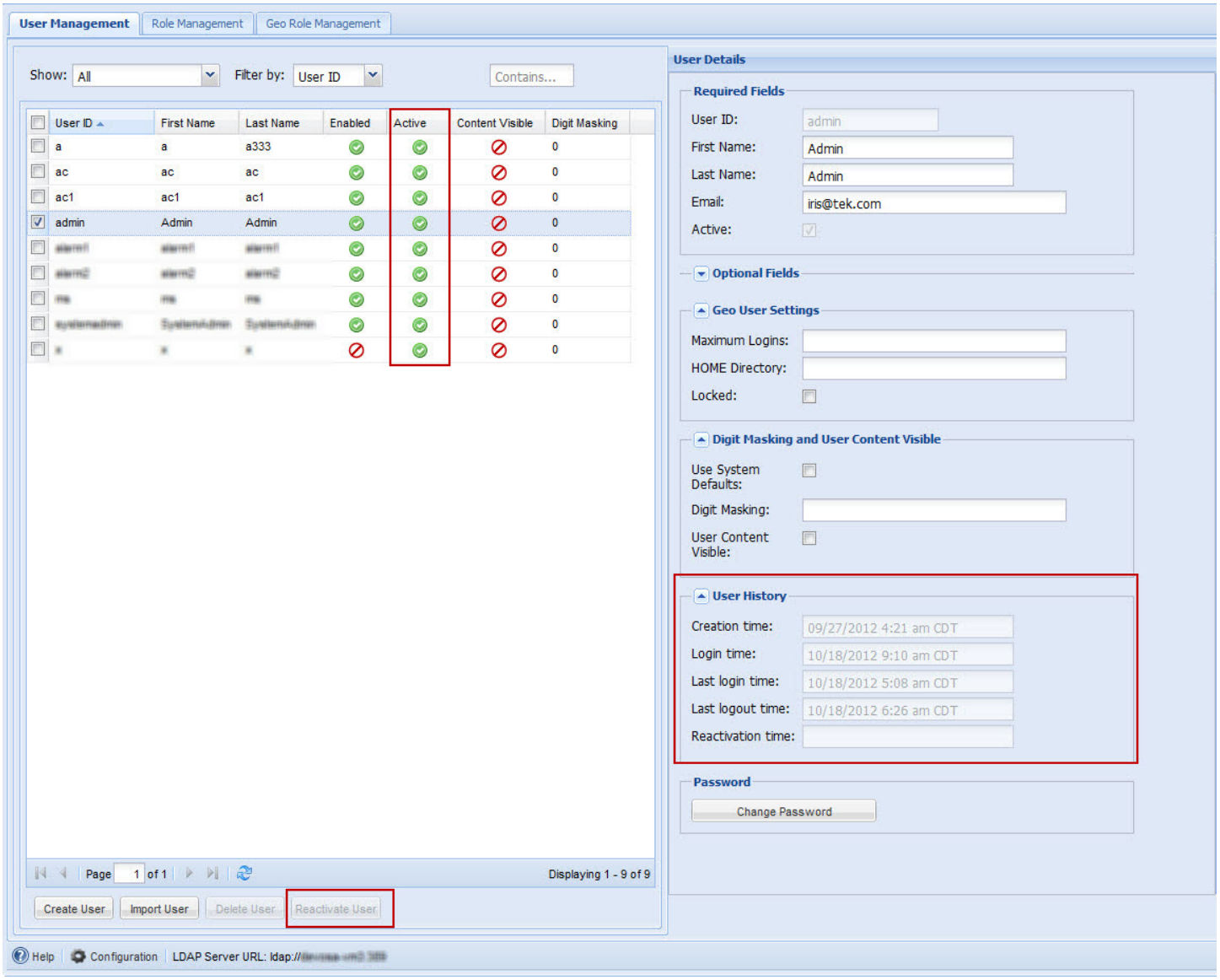
If a user has not logged in to Iris for more days than the configured inactivity time, he or she will become inactive. The inactive interval starts when the user logs out of all sessions. Inactive users cannot log on the system, and a corresponding log is generated when a login attempt is made. An Administrator must reset the user's status back to active.

If a user never logged in to the Iris system, and the account has existed longer than the set login inactivity time, the user account will become inactive.

User Inactivity Area



User Management Window Example



UUMS Supported LDAPs

The following table describes the LDAPs that UUMS supports and summarizes data management for each LDAP.

LDAP	Description	User Profile Data Management
Iris LDAP	• Tektronix-provided LDAP installed during initial system setup. • Remote user administration supported using a TMF615 API.	**Iris LDAP Data (Managed by UUMS):** • User credentials (user ID, user name, email address, and password) **Iris Database Data:** • User ID, user name, email address (password is NOT stored in database) • Enabled status • Optional data including employee ID, mobile number, and address • Assigned user roles
Existing Corporate LDAP	• Customer-provided LDAP that UUMS connects to for user authentication. • Password policy and quality parameters are managed on the Existing LDAP and are not configured in UUMS. For example, password expiration continues to be managed on the existing LDAP; if a user's password expires on the existing LDAP, UUMS will not allow the user to login until the password is updated in the existing LDAP.	**Existing LDAP Data (Not managed by UUMS):** • User credentials (user ID, user name, email address, and password) **Iris Database Data:** • User ID, user name, email address imported from existing database (password is NOT stored in database) • Enabled status • Optional data including employee ID, mobile number, and address • Assigned user roles

User Management Functions

Supported User Management functions differ depending on which LDAP is implemented. Creating users and changing passwords are managed on the existing corporate LDAP rather than within UUMS. The Activity Log tracks user activities within UUMS.

User Management Function	UUMS Options	
	Iris LDAP	Existing LDAP
Import Users	X	X
Create Users	X	
Modify User Details	X	X
Assign Roles	X	X
Set/Change Password	X	
Enable/Disable Users	X	X
Delete Users	X	X

Setting Up GeoProbe User Accounts for Iris ISA and PA Applications

Additional user administration is necessary when ISA and PA users require access to SpIprobes. The Iris Session Analyzer (ISA) and Protocol Analyzer (PA) applications both support data from GeoProbe SpIprobes. In order for Iris ISA and PA users to be able to select SpIprobes within these applications for filtering and data capture, all users that need access to ISA and PA must be assigned at least one role with the privileges identified in the matrix below.

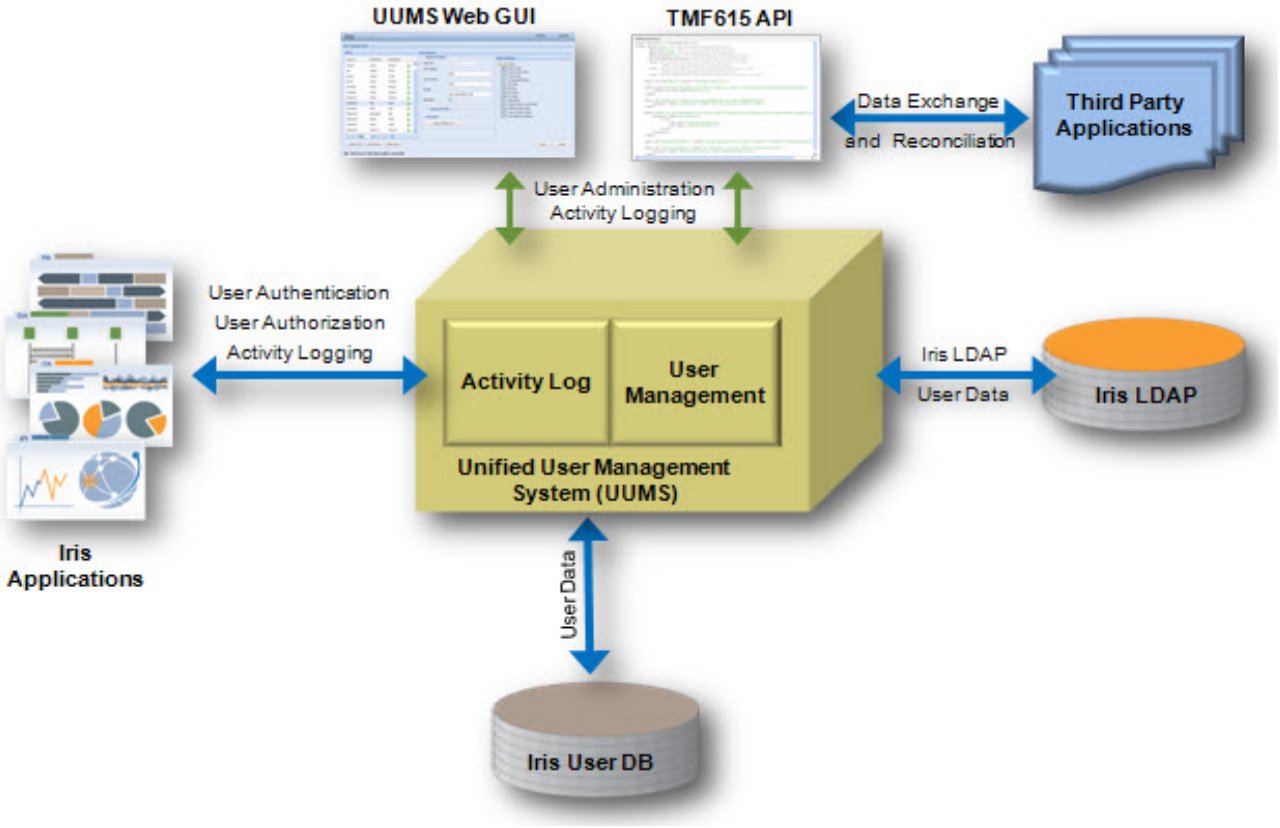
Iris Application	GeoProbe Classmarks	GeoProbe License	Applicable UUMS Iris Privileges	UUMS License
Protocol Analyzer	• Protocol Analyzer	• PA	• IPA Privilege • User Content Visible • User Digits Unmasked	• PA
Iris Session Analyzer	• User Call Trace • SUDS Recall • Failed Calls Recall • Snooping User Call trace	• User Call Trace • SUDS Recall • Failed Calls Recall • Snooping User Call trace	• ISA Privilege • ISA Flow Packet Retrieval • Media Capture Privilege • Media Capture Admin Privilege • User Content Visible • User Digits Unmasked	• ISA

TMF615 API

Service provider environments are comprised of multi-vendor networks that are managed using various Operations Support Systems (OSSs). Service Providers (SPs) require a utility to unify the user management operations across these various OSSs.

The TMF615 specification defines an interface for SPs to consistently provision user's access rights and privileges across the system in a secure manner.

As an OSS, the Iris system supports the TMF615 interface through the UUMS. TMF615 is a purchasable option that is only supported when the Iris LDAP is implemented; it is not supported when an existing corporate LDAP is implemented. See the ***TMF615 API Reference Guide*** for details. Contact Tektronix for purchasing details.



UUMS User Privileges and Roles

Once users log onto the Iris, GeoProbe, or UACN/RIA system, access to the applications and features is controlled by role assignment in the case of Iris and UACN/RIA, and profile assignment in the case of GeoProbe. Each role or profile contains a set of privileges to ensure appropriate access to job-related tasks. The System Administrator assigns defined roles or profiles to each user account.

Available Subsystem Privileges

System Administrators can assign roles/profiles and privileges on the User Details Window or the Role Management (for Iris and UACN/RIA) and Geo Role Management windows.

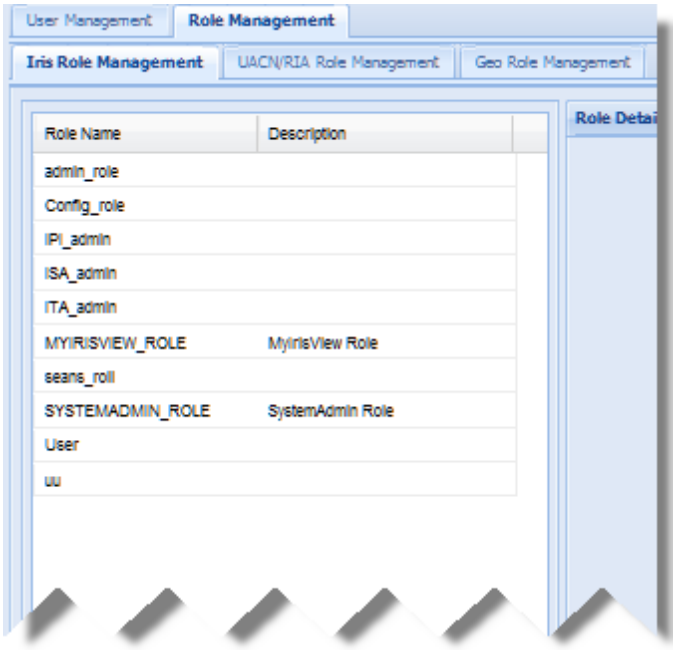
Subsystem	Access
Iris User Privileges	Allows access to the Iris suite of applications.
UACN/RIA User Privileges	Allows access to the UACN/RIA features.
Cognos User Roles	In UACN/RIA, a separate set of Cognos user roles is necessary to manage the reports.
GeoProbe Classmarks	Allows access to the GeoProbe applications and features.
mylrisView Role	Allows access to the mylrisView application.

Default Roles

When Administrators use the Role Management window for Iris Role Management, you will see at least one role called SYSTEMADMIN_ROLE. In the event of an upgrade, you may see the APPLICATION_ADMIN_ROLE.

Role Name	Description
SYSTEMADMIN_ROLE	This role is assigned one privilege, UUMS Admin, which cannot be assigned to any other users. This default role cannot be deleted.
APPLICATION_ADMIN_ROLE	You will see this role in the event of a system upgrade. It is assigned to users who have the current (prior to Version 12.2) SYSTEMADMIN_ROLE, and is assigned the Admin Privilege.

Iris Role Management Example



Iris User Privileges

After Iris users log on to the Iris system, access to the Iris applications is controlled by role assignment. Each role contains a set of privileges to ensure appropriate access to job-related tasks. The Iris System Administrator assigns defined roles to each user account.

The following table describes the privileges available in Iris. The administrator can add different combinations of privileges to create a role. Users can view their assigned privileges in the User Management User Details window.[1]

Privilege	System Access	Tasks
3rd Party API Access	ISA API	Access the ISA API capability.

Privilege	System Access	Tasks
Admin Privilege	System Config • Probes tab • Applications tab • Licenses tab • Software tab • System tab • Topology tab • Location tab	All system configuration tasks: • Configure probe settings • Configure physical device ports • Configure disk arrays • Configure Store to Disk settings • Configure XDR profiles • Configure ISA System Default Node Type Order • Manage Probe Software Updates • Configure server settings • Configure Topology entities • Configure element geographical coordinates using the Map Location Editor dialog in the Network Maps application • Use the Session Management tab to attach to or terminate all non-media sessions • Configure Location rules for geographical coordinates
Alarm Acknowledge Privilege	Displays Acknowledge check boxes and ACK button on Alarm Dashboard	• Acknowledge ITA, IPI, KPI Studio, ACE, and system-level alarms
Application Alarm Admin Privilege	Alarms Policy Management	For ITA, IPI, KPI Studio, and ACE: • Create new policies • Edit any policy or template, public or private • Delete any policy or template, public or private • Configure system level alarms • Export all policies, action templates, schedule templates, and profiles to an XML file • Import policy configuration files (configuration files contain policies, action templates, schedule templates, and profiles) • Display the content of the XML schema file within the default Internet browser
Application Alarm Configuration Privilege	Alarms Policy Management	For ITA, IPI, KPI Studio, and ACE: • Create new policies • Edit their own policies and templates as well as any designated as public • Delete their own policies and templates as well as any designated as public
Alarm Clearing Privilege	View and access Clear check boxes and CLEAR button on Alarm Dashboard	• Clear ITA, IPI, KPI Studio, ACE, and system-level alarms
Application Alarms on Alarm Dashboard	Alarm Dashboard	• Monitor ITA, IPI, KPI Studio, and ACE alarms

Privilege	System Access	Tasks
System Alarms on Alarm Dashboard	Alarm Dashboard	• Monitor System-level alarms
Configuration Privilege	System Config • Probes tab • Applications tab • Licenses tab • Software tab • System tab • Topology tab • Location tab	• Configure probe settings • Configure physical device ports • Configure disk arrays • Configure Store to Disk settings • Configure XDR profiles • Configure ISA System Default Node Type Order • Manage Probe Software Updates • Configure Server settings • Configure Topology entities • Configure element geographical coordinates using the Map Location Editor dialog in the Network Maps application • Use the Session Management tab to attach to or terminate all non-media sessions
Conversational Video Privilege	ISA application	• Can analyze captured conversational video and related audio using the ISA Media Player.
DTMF Authorized	ISA application	• Expand DTMF flows in the Results window to analyze packet decodes • View DTMF digits in the DTMF column and Flow Details window
IFC Privilege	Not applicable	When an IFC profile runs and is configured to save the artifacts to the remote server repository, the artifacts are stored either in the public or private area for the IFC profile on the repository. All users can see the public area. Users with the IFC privilege can see the private area.
Firmware Administration Privilege	Software tab • By Probe - Firmware tab • Firmware Audit Tab • Campaign Details - Firmware Campaign Type	• View/export firmware audit inventory information on a per-probe basis • View/export firmware audit inventory information for all/selected probes • Create, schedule, and activate Firmware campaigns
IFC Admin Privilege	System Config Configure profiles to schedule session traces for customers of interest, and save them to a local disk or a remote server repository.	• Set up schedule options: start, end, frequency • Determine the monitored objects • List the IMSIs of interest • Determine whether the profiles and sessions are to be stored locally or on a remote server • If stored on a remote server, determine whether the profiles and sessions are to be stored in the private area on the repository or a public area

Privilege	System Access	Tasks
IPA Privilege	PA application	• Set up capture filters • Run real-time capture sessions • Run historical capture sessions
IPI Privilege	IPI application To launch ISA from within IPI, user must also have the ISA privilege.	• View dashlets • Set filters • Drill-down to any KPI level
ISA Automatic Full MPC	ISA application	Users can enable full MPC for their ISA sessions.
ISA Flow Packet Retrieval	Retrieve User Plane options in ISA application	• Retrieve and view ISA user plane PDUs in ISA Ladder Diagram and PDU Details Pane
ISA G10 Show MOS-CQ Not LQ Privilege	Not applicable	View either MOS-CQ or MOS-LQ values for PDUs in the ladder diagram for G10 probes: • **Enabled (checked)**: View MOS-CQ values • **Disabled (unchecked)**: View MOS-LQ values
ISA Override MPC Rule-sets	ISA	Users can override default ISA MPC correlation rules and choose one or more custom MPC rule sets. Contact Tektronix Communications Customer Support for information about customizing MPC rule sets.
ISA Privilege	ISA application	• Configure capture filters • Start capture sessions • Drill to decode
ITA Privilege	ITA application To launch PA from within ITA, user must also have the IPA privilege.	• View dashlets • Set filters • Drill-down to any KPI level
mylrisView Admin Privilege	mylrisView	Users can view, edit, and delete any mylrisView dashboard marked Public or Private. See mylrisView Roles for more information.
Network Maps Privilege	Network Maps application	Users can view Network Maps but cannot make configuration changes to maps.
SMS Full Content Privilege	Not applicable	For ISA and PA: • **Enabled (checked)**: Allows the viewing of SIP messages including SMS and MSRP content. • **Disabled (unchecked)**: Allows the viewing of SIP messages with user content concealed with asterisks (*).
System Health Customer Privilege	Iris System Health Reports	Users can view and run Iris System Health reports.
User Content Capture Privilege	Not applicable	For ISA: • **Enabled (checked)**: Allows capture of SMS and MSRP content in the G10 probe for use by Iris applications. • **Disabled (unchecked)**: User content concealed with asterisks (*).

Privilege	System Access	Tasks
User Content Visible Privilege	Not applicable	For ISA and PA: • **Enabled (checked)**: Allows the viewing of content including SMS and MSRP content. • **Disabled (unchecked)**: User content concealed with asterisks (*).
User Digits Unmasked Privilege	Not applicable	For ISA and PA: • **Enabled (checked)**: Can view user digits such as IMSIs. • **Disabled (unchecked)**: User digits are concealed (masked) with Xs in the system. The Admin can set the number of digits to conceal from 0 to 99 digits in the System Tab.
User Plane Admin Privilege	Media and User Plane Capture functionality within ISA application	• Configure filters to identify media streams to capture in ISA • Capture and monitor real-time media streams in ISA • Analyze captured data using Wireshark • In the Session Management page, view, attach, or terminate media capture sessions created by other users
User Plane Capture Privilege	Media and User Plane Capture functionality within ISA application	• Configure filters to identify media streams to capture in ISA • Capture and monitor real-time media streams in ISA • Analyze captured data using Wireshark • Detach captured media sessions so they run unattached
User Plane Analysis Privilege	User Plane export to PCAP and Wireshark functionality within ISA application	Users can export User Plane data to PCAP files and launch Wireshark to view data and play back audio for User Plane flows.
UUMS Admin Privilege	User Management	User management tasks for Admin: • Configure LDAP Server settings • Configure password policy and quality settings • Create roles • Provision users and assign roles Users without the UUMS Admin privilege can only view their user information and currently assigned roles and change their password (Iris LDAP only). This privilege cannot be assigned to any other users.
	Activity Log	• View and filter activity log messages • Export messages to PDF or CSV

[1]User Content Visible and User Digits Unmasked settings can be found on the Subsystem Defaults window for global defaults, and on the User Details pane for individual settings. During migration from version 7.12.1 to 7.12.2, users with the "User Content Visible" and User Digits Unmasked" privileges will retain the settings they had in previous software releases. Users without these privileges will have the default global settings that are configured on the Subsystem Defaults page.

UACN/RIA Roles and Privileges

The System Administrator must assign User Role(s) for each User Account. The role assigned to an account must be relative to the type of work function the user performs. The System Administrator must determine the specific privileges to grant a user depending on their specific responsibilities.

The following table describes the privileges available in UACN/RIA. The administrator can add different combinations of privileges to create a role. Users can view their assigned privileges in the User Management User Details window.

Privilege	Users Can...
Cognos Access	Access Cognos for reporting capabilities. See Cognos User Roles for more information.
Launch Geo IPTV	Launch the GeoProbe IPTV application.
Manage Alarm Admin Profiles	View all alarm profiles, create new profiles, and edit and delete existing profiles.
Manage Alarms	Set up alarm configurations to trigger for each application that allows you to customize KPI thresholds.
Manage APMV KPIs	Configure the APM Voice KPIs.
Manage Data Services KPIs	Configure the Data Services KPIs.
Manage Mobile Network Elements	Configure services for mobile network elements.
Manage Interconnect KPIs	Configure the Interconnect KPIs.
Manage IMA KPIs	Configure the IMA KPIs.
Manage IP Address	Add or edit the IP Address list.
Manage IP Core KPIs	Configure the IP Core KPIs.
Manage IPTV Broadcast Channels	Configure groups of preferred Broadcast channels.
Manage IPTV IGMP	Configure IPTV IGMP data.
Manage IPTV KPIs	Configure IPTV KPIs.
Manage IPTV Video On Demand	Configure IPTV Video on Demand.
Manage Network Nodes	Access the Network Configuration feature to add nodes and sites.
Manage APN/URL Port to Service Name	Configure the APN/URL Port to Service Name feature.
Manage Release Causes	Configure release causes.
Manage Secured Data Access Profiles	Configure the SDA profiles.
Manage User Defined Services	Configure user defined services.
RTP Capture	Launch the RTP Capture application.
View Alarm Data	View the Alarm Browser.
View APMV Data	View APMV Data portlets.
View Beamer Data	View Beamer Data portlets.
View CDR Logs	View the CDR logs.
View Interconnect Data	View Interconnect portlets.
View IMA Data	View IMA portlets.
View IP Address	View the IP address list.

Privilege	Users Can...
View IP Core Data	View IP Core portlets.
View IPTV Broadcast Channels Data	View the IPTV portlets.
View IPTV IGMP Data	View IPTV portlets.
View IPTV Video On Demand Data	View IPTV portlets.
NGPA	Launch the Protocol Analyzer application.
View On Demand Data	View On Demand portlets.
Web Call Trace	Launch the Web Call Trace application.

Cognos Roles and Privileges

Tektronix provides four pre-defined user roles for managing IPI Cognos users, based on the four purchasable Cognos licenses of the same names. Each purchased license controls the tasks each role can perform and the applications the role can access. You can edit these roles by adding and removing users for each role; however, you cannot add any privileges to the roles or delete any of the Cognos roles.

Each license controls the corresponding user role type. If the license is absent, you will not see the role in the GUI list. You will not be able to assign users to Cognos user roles if you exceed the number of named users allowed for that license.When you assign multiple Cognos roles to a user, that user retains the privileges of the most restrictive role.

.

The following table describes the Cognos user roles.

Role	Description
BI Consumer	Any user with this role can: • Browse any folder that they have permission to access • Access Cognos Viewer to view and run Management reports This role does not have permissions to use any Studio product (Analysis or Query). User access is limited to the number of licenses purchased for named users.
BI Business Analyst	Any user with this role can: • Browse any folder that he has permission to access • Access Cognos Viewer to view and run Management reports • Access Cognos Viewer to view and run Analysis reports • Access Analysis Studio to change Analysis reports This role does not have permissions to use Query or Event Studio products. User access is limited to the number of licenses purchased for named users.
BI Professional	Any user with this role can: • Browse any folder that he has permission to access • Access Cognos Viewer to view and run reports • Access Analysis Studio to edit/modify Analysis • Access Query Studio to edit/modify Query reports • Access Event Studio to edit/modify Event reports This role does not have permissions to perform any administrative tasks. User access is limited to the number of licenses purchased for named users.
BI Web Administrator	This role is required for the Cognos administrator to be able to perform basic administrative tasks. This role does not have permissions to run any reports.

GeoProbe Classmarks

You can assign classmarks to user profiles to define their access level. You can assign system functions to users with this feature to display only those functions. You can access the classmarks through the Profile tab of the Geo Role Management window.

The following table describes the classmarks available in GeoProbe. The administrator can add different combinations of privileges to create a profile. Users can view their assigned classmarks in the User Management User Details window.

Category	Classmark	Users Can...
Alarms	Alarm Acknowledge	Acknowledge alarms
	Alarm Bullseye	View the alarm Bullseye
	Alarm Clear	Clear alarms
	Alarm Definition & Config	Add, delete, configure, and modify alarms
	Alarm Master Bullseye	View the master alarm Bullseye
	Alarm Weights/Colors/Categories	Modify the weights, colors, and categories the SpIstation uses to depict alarms on the network maps
	Edit Server Alarm Config	Add, delete, configure, and modify server alarms
	View Server Alarm Config	View server alarm configurations
Alerts	Alert Notification	Display an alert notification box with a message. For example, a notification box might appear when an alarm log is auto-aging or a user notification box appears for Graphical User Interface (GUI) Network configuration errors.
	Broadcast Alerts	See an alert message through a dialog box. For example, if a problem occurs and corrective actions interrupt service to other users, the alert message serves as a warning of the pending interruption.
CDR	Activate Rtp Capture	Activate or deactivate the RTP Capture profiles
	CDR Config	Configure a CDR profile
	CDR Status	Launch the profile status for the CDR application
	Edit Rtp Capture	Add, delete, configure, and modify RTP Capture profiles
IT:seven	IT:seven User	Run the IT:seven client software. This classmark is only used with the IT:seven GeoCare product.
Mass Call Applications	Mass Call Config	Configure mass calling events
	Mass Call Status	Monitor mass calling events
Miscellaneous Applications	Filter Editor	Create, modify, or delete filters when using the Filter Editor feature.
	Filter Viewer	View with a read-only capability in the Filter Editor feature
	Usage Measurement Config	Access the Usage Measurement application to configure usage measurement data and send it to a remote system.

Category	Classmark	Users Can...
Network Applications	License Manager	Access the License Manager function to monitor the available SpIstation licenses.
	Network Configuration	Access the Network Configuration mode. Assign users a profile with this classmark who are responsible for setting up network maps or defining and configuring network elements and protocols.
	Network Status	Access the Network Status mode. Assign users who are responsible for monitoring the network a profile with this classmark.
Pointcode Editor	Edit Pointcodes	Add, delete, and modify pointcodes in the database.
	View Pointcodes	Have read-only capability for pointcodes contained in the database.
Probe Run Time/Monitor Port	Edit Monitor Port	Configure and modify monitor ports.
	View Monitor Ports	View monitor ports.
	Probe Run-Time Status	View SpIprobe status.
Protocol Analyzer	Protocol Analyzer	Access the Protocol Analyzer application.
ReMon to Disk/Recall	RTD Automatic Daily Archive	Archive automatically on a daily basis files to another location or remote site.
	RTD Config	Add, delete, and modify an RTD profile.
	RTD Recall	Recall RTD data.
	RTD Status	View a ReMon to Disk (RTD) profile. It also allows users to view how they allocate RTD profiles across SpIprobes.
ReMon/User Call Trace	Call in Progress	Track calls currently in progress in User Call Trace.
	Remote Monitoring	Access the ReMon application.
	Save Turbo—7 Binary	Save the binary content of MSUs.
	User Call Trace	Trace calls using the global User Call Trace application. This classmark also enables you to log a user call trace request. Logging the user call trace request enables you to know who is performing a user call trace function.
	Snooping User Call Trace[1]	Utilize the snoop mode for user call trace.
	View Hex Dump	View hex decode information for an expanded ReMon message.
Smart Alerts	Smart Alert Configure	Add, delete, and modify MSU Events and Smart Alerts.
	Smart Alerts Status	Print, exit, view MSU Events, and view a Smart Alerts script from the Smart Alerts Configuration window.
Statistical Applications	Historical Stats Config	Add, delete, and modify historical statistics configurations.
	Historical Stats View	View historical statistics configurations.

Category	Classmark	Users Can...
	Edit Statistical Events	Create, modify, or delete statistical events.
	View Statistical Events	Utilize a read-only capability of statistical events.
	Behavioral Stats Config	Configure behavioral statistics.
	Behavioral Stats Status	Monitor the status of behavioral statistics.
	Real-Time Statistics	Collect and display real-time statistics.
Status/Config Classmarks	Config Color Palette	Configure color palettes used when defining alarm colors and node icons.
	Database Synchronization	Access the Database Synchronization menu option on the SpIstation.
	Edit SS7 and Monitoring Groups	Define, edit, and delete SS7 and Monitoring Equipment groups.
	Edit SU Filter List	Modify the global list of SU filters.
	Use SU Filter List	Use the global list of SU filters.
	Edit Sig Groups	Create and edit signaling groups.
	Edit Bearer Channel	Create, modify, and delete bearer channels from the bearer channel editor.
	View Bearer Channel	View all bearer channels from the bearer channel editor.
	Edit Physical Device	Edit IP information using the Physical Device Editor window.
	View Physical Device	View information in the Physical Device Editor window.
	Edit Physical Device Group Editor	Edit Physical Device Group information using the Physical Device Group Editor window.
	View Physical Device Group	View information in the Physical Device Editor window.
	Edit Application Map	Edit application map information using the Application Map Editor window.
	View Application Map	View information in the Application Map Editor window.
	Edit Layer 2	Edit the layer 2 information using the Layer 2 Editor window.
	View Layer 2	View the information in the Layer 2 Editor window.
	Edit SCTP Association	Edit the SCTP association information using the SCTP Generic Association Editor window.
	View SCTP Association	View the information in the SCTP Generic Association Editor window.
	Edit SCTP End Point	Edit the SCTP End Point information using the SCTP End Point Editor window.
	View SCTP End Point	View the information in the SCTP End Point Editor window.
	Edit Probe Configurations	Edit and configure timers for the SpIprobe.
	Edit Views	Define, edit, and delete views.
	Edit Protocols	Add, modify, and delete protocols.
	Graphics File Maintenance	Create, modify, or otherwise maintain the graphics files used by the SpIstation.
	Edit Maps	Create, delete, copy, or rename a map.

Category	Classmark	Users Can...
	Edit Nodes	Create, modify, and delete system nodes and node groups from your map. If this classmark is disabled, and you have the Network Configuration privilege, you can create, modify, or delete GPRS BSS, RNC, IP Cloud, and GSN Network nodes.
	Edit Probes	Create, modify, and delete SpIprobes, SpIservers, and generic nodes from your map.
	Linkset/Node Type Editor	Control Linkset/Interface/Node type editors on your map.
	Map/Sig Group Access Editor	Enable map and signaling group access configuration privileges for your map.
SUDS/Failed Calls	SUDS Config	Configure the SUDStore profiles.
	SUDS Status	Check the status of a profile and determine the data each SpIprobe processor contributes to the profile.
	Failed Calls Status	Check the status of a Failed Calls profile to determine the data each SpIprobe processor contributes to the profile.
	IP Call Status	Check the status of the SUDS IP Calls profile to determine the data each SpIprobe processor contributes to the profile.
	SUDS Recall	Recall a SUDStore session based on certain criteria.
	Failed Calls Recall	Recall a failed calls session based on certain criteria.
Tools	Reach-Through Capability	Access SpInodes and control them from the SpIstation.
	Access UNIX Tools	Access the UNIX command tool shell through the Utilities window.
	Syslogs Access	Access system logs.
	Root (overriding) Privileges[2]	The Root (overriding) privileges classmark provides superuser capabilities, enabling users to override certain privileges. Use this feature to delete a view belonging to another user in the Network Configuration and Network Status modes.
Wireshark	Wireshark Monitoring	Access the Wireshark Analyzer and Wireshark Analyzer Recall applications

[1]The Snooping Mode option is only available for Gb, GTP, Gi (HTTP and WAP only) call trace session types, and their associated Multi-Protocol Correlation (MPC) call trace types. This option may not be available for all users.

[2]Users with Root privileges have unlimited access to all network data.

mylrisView Roles

Tektronix Communications provides two predefined user roles for managing and accessing mylrisView, based on the purchasable mylrisView license. You can edit these roles by adding and removing users; however, you cannot add any privileges to the roles or delete either of the mylrisView roles.

The following table describes the mylrisView roles.

Role	Description
MYIRISVIEWADMIN	Users with this role can view, edit, and delete any mylrisView dashboard marked as Public or Private. This is not a licensable role; however, you have to have the MYIRISVIEW_ROLE to access mylrisView.
MYIRISVIEW_ROLE	Users with this role can access the mylrisView application. Users can view any dashboard marked as Public, but can only modify their own mylrisView dashboards. The MYIRISVIEW_ROLE is licensed. You will not be able to assign users to this role if you exceed the number of named users allowed for that license.

Activity Types

Activity types and keywords tracked by the Activity Log vary depending on the Iris subsystem.

Subsystem	Activity Types	Keyword Filter	
ACE	• User access	• ACE Dashboard	
Alarms	• User access • Acknowledged Alarms	• Policy Name as shown in the Alarm Browser • Policy Dashboard • Policy Management	
IPI	• Parse and persist activities	• Dashlet • Dashboard • Filter • Service • Measures • kqis • KPI, kpis	• BH Tables • BH Rollup Type • data table • tables
ISA	• User access • Capture activities • Security Logging	• User ID • Capture ID	
ITA	• User access	• ITA Dashboard	
OAM	User Activities • Access • Topology activities using UI • Probe software campaign activities	• System Config • Node ID • Link ID • Group Name • User ID	
	System Activities • Topology auto detection events	• System	
UUMS	• User Access • User updates • Password updates • Role updates • TMF615 API activities	• Activity Log • User Management • User ID	

Activity Log Storage and Aging

All activity data is stored in the Iris database. Activity Log Aging removes old data from the database to allow storage space for the most recent activity data.

Activity data is retained for 366 days and purged daily at 10 p.m. The retention period is configurable; contact Tektronix Customer Support for details.

Export File Formats

File Format Details

- File format can be saved as CSV or PDF
- File name includes Start Time and End Time filter values: ACTIVITY-LOGS-YYYYMMDD-HHMMSS-YYYYMMDD-HHMMSS.csv
- Exported data is sorted and filtered as shown in Log Browser

Sample CSV File (ACTIVITY-LOGS-20110714-145600-20110715-145659.csv)

```
#Daily Logins
#"Timestamp (GMT)","Subsystem","Activity","User ID","Keyword","Description"
"07/15/2011 14:56:28","UUMS","LOGIN","ccb","ccb","'ccb' logged in from client address: [134.64.78.59]"
"07/15/2011 13:57:38","UUMS","LOGIN","aasmi","aasmi","'aasmi' logged in from client address: [134.64.83.40]"
"07/15/2011 06:03:46","UUMS","LOGIN","admin","admin","'admin' logged in from client address: [134.64.222.200]"
"07/15/2011 05:51:28","UUMS","LOGIN","admin","admin","'admin' logged in from client address: [134.64.140.144]"
"07/15/2011 05:37:37","UUMS","LOGIN","jsmith","jsmith","'jsmith' logged in from client address: [134.64.140.144]"
"07/15/2011 05:27:20","UUMS","LOGIN","ayshu","ayshu","'ayshu' logged in from client address: [134.64.222.200]"
"07/14/2011 16:03:54","UUMS","LOGIN","admin","admin","'admin' logged in from client address: [134.64.95.13]"
"07/14/2011 15:41:49","UUMS","LOGIN","admin","admin","'admin' logged in from client address: [134.64.80.81]"
"07/14/2011 15:35:36","UUMS","LOGIN","dshea","dshea","'dshea' logged in from client address: [134.64.78.59]"
```

Sample PDF File (ACTIVITY-LOGS-20110714-145600-20110715-145659.pdf)

Daily Logins

Timestamp (GMT)	Subsystem	Activity	User ID	Keyword	Description
07/15/2011 14:56:28	UUMS	LOGIN	ccb	ccb	'ccb' logged in from client address: [134.64.78.59]
07/15/2011 13:57:38	UUMS	LOGIN	aasmi	aasmi	'aasmi' logged in from client address: [134.64.83.40]
07/15/2011 06:03:46	UUMS	LOGIN	admin	admin	'admin' logged in from client address: [134.64.222.200]
07/15/2011 05:51:28	UUMS	LOGIN	admin	admin	'admin' logged in from client address: [134.64.140.144]
07/15/2011 05:37:37	UUMS	LOGIN	jsmith	jsmith	'jmith' logged in from client address: [134.64.140.144]
07/15/2011 05:27:20	UUMS	LOGIN	ayshu	ayshu	'ayshu' logged in from client address: [134.64.222.200]
07/14/2011 16:03:54	UUMS	LOGIN	admin	admin	'admin' logged in from client address: [134.64.95.13]
07/14/2011 15:41:49	UUMS	LOGIN	dshea	dshea	'dshea' logged in from client address: [134.64.80.81]
07/14/2011 15:35:36	UUMS	LOGIN	admin	admin	'admin' logged in from client address: [134.64.78.59]

Account Migration Rules

As user account information is migrated to UUMS from GeoProbe and UACN/RIA, this table may answer questions you have about what data is migrated.

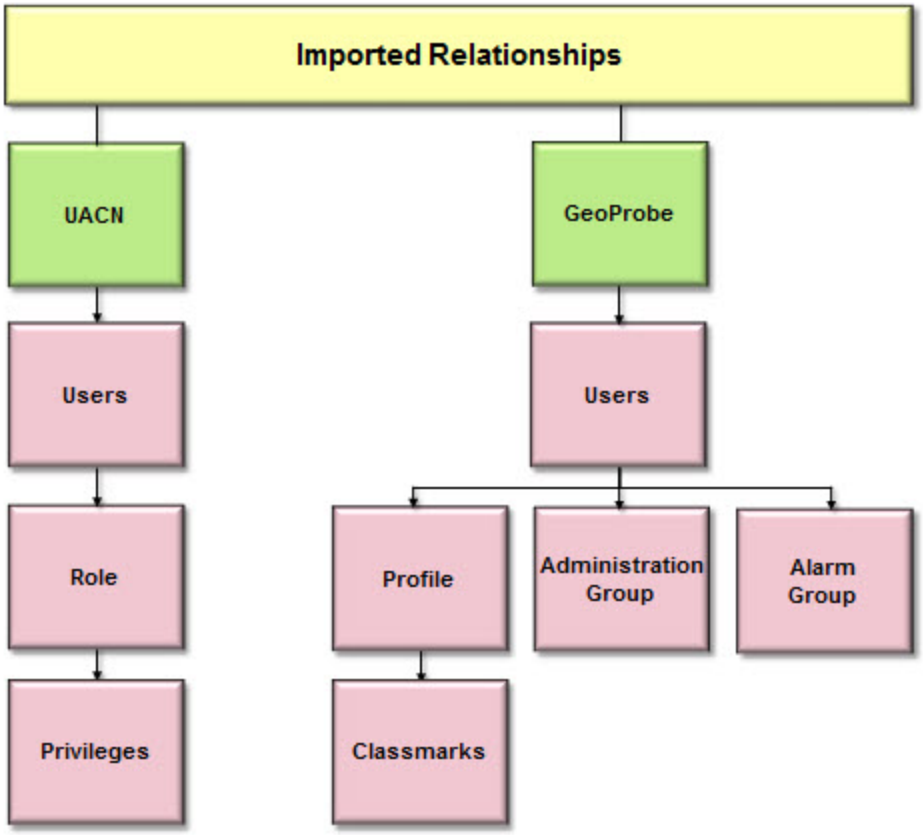
If a User is...	Then...
Only set up in one legacy system	• The user account is created in UUMS and the user is assigned roles corresponding to the level of privileges in the existing legacy system, including the per-user digit and user content masking settings. • The existing user password is migrated, however, it is marked as expired and a new temporary password is assigned, which is the username. Users must reset their password the first time they log in to IrisView. • User enabled/disabled status is migrated; if a user is disabled, the System Administrator must enable the account prior to the user logging in. • User inactivity status is migrated; the time elapsed includes since the user was last active in the legacy system. If the account is inactive, the System Administrator must reactivate the account prior to the user logging in.
Set up in both legacy systems only (GeoProbe and UACN/RIA)	• A single user account is created in UUMS and the user is assigned multiple roles corresponding to the levels of access associated to each legacy system. • The existing user password is migrated, however, it is marked as expired and a new temporary password is assigned, which is the username. Users must reset their password the first time they log in to IrisView. • User enabled/disabled status is migrated; if a user is disabled, the System Administrator must enable the account prior to the user logging in. • User inactivity status is migrated; the time elapsed includes since the user was last active in the legacy system. If the account is inactive, the System Administrator must reactivate the account prior to the user logging in.
Set up in Iris and at least one legacy system	• The Iris user account is updated to include the roles and system-specific settings associated to each legacy system; in case of conflict, the Iris settings prevail (including per-user digit and user content masking). • User password is not changed. • Attributes that are blank in Iris but available in the legacy systems will take the values from the legacy systems. • User enabled/disabled status is based on Iris state. • User inactive/active state is based on Iris state.

Role and Privilege Migration

Tektronix Communications provides a tool to import user management information from UACN/RIA and GeoProbe into UUMS. An existing command line tool called ***irisImportTool.sh*** is updated to handle bulk importing of users into the Iris Oracle database. A text file in XML format is provided from UACN/RIA and GeoProbe to provide input for the tool. The file must be on the same machine where the main OAM JBoss is running. Sample .xml files with the description of the file format and expected fields for GeoProbe and UACN/RIA will be provided as a part of the installation and put under SVN.

User information imported from UACN/RIA and GeoProbe contains the relationship ties between users and privileges, users and profiles, and users and groups.

Relationship Types Imported



Import UACN/RIA Users, Roles and Privileges

User information imported from UACN/RIA is defined in the example .xml files.

Define Users Example

```
<USERS>
    <USER>
        <!-- USER INFO COLUMNS -->
        <ASSIGNED_ROLES>
            <ASSIGNED_ROLE_NAME>...</ASSIGNED_ROLE_NAME>
            ...
        </ASSIGNED_ROLES>
    </USER>
    <USER>
        <!-- USER INFO COLUMNS -->
        <ASSIGNED_ROLES></ASSIGNED_ROLES>
    </USER>
    ...
</USERS>
```

- All Roles (including Roles without any associations with Users) must be specified in the ROLES section.
- User can be defined either having assigned Roles or without any Role.
- To assign a Role only its name should be specified as it is a unique identifier.
- This example covers all possible cases of xml USERS section filling.

Define Roles Example

```
<ROLES>
    <ROLE>
        <!-- ROLE INFO COLUMNS -->
        <ASSIGNED_PRIVILEGES>
            <ASSIGNED_PRIVILEGE_ID>...</ASSIGNED_PRIVILEGE_ID>
            ...
        </ASSIGNED_PRIVILEGES>
    </ROLE>
    <ROLE>
        <!-- ROLE INFO COLUMNS -->
        <ASSIGNED_PRIVILEGES></ASSIGNED_PRIVILEGES>
    </ROLE>
    ...
</ROLES>
```

- This section contains all Roles (including Roles without any associations with Users).
- All Privileges (including Privileges without any associations with Roles) must be specified in the PRIVILEGES section.
- Role can be defined either having assigned Privileges or without any Privilege.
- To assign a Privilege only its ID should be specified as it is a unique identifier.
- This example covers all possible cases of xml ROLES section filling.

Defined Privileges Example

```
<USERS>
    <USER>
        <!-- USER INFO COLUMNS -->
        <ALARM_GROUP_ID>...</ALARM_GROUP_ID>
        <ADMIN_GROUP_NAME>...</ADMIN_GROUP_NAME>
        <PROFILE_NAME>...</PROFILE_NAME>
    </USER>
    ...
</USERS>
```

- This section contains all Privileges (including Privileges without any associations with Roles).
- This example covers all possible cases of xml PRIVILEGES section filling.

Import GeoProbe Users, Profiles, Classmarks, and Groups

User information imported from GeoProbe is defined in the example .xml files.

Define Users Example

```
<USERS>
    <USER>
        <!-- USER INFO COLUMNS -->
        <ALARM_GROUP_ID>...</ALARM_GROUP_ID>
        <ADMIN_GROUP_NAME>...</ADMIN_GROUP_NAME>
        <PROFILE_NAME>...</PROFILE_NAME>
    </USER>
    ...
</USERS>
```

- USER INFO COLUMNS includes user preferences and digit masking, because they can be interpreted as user's attributes.
- ALARM GROUP INFO COLUMNS, ADMIN GROUP INFO COLUMNS and PROFILE INFO COLUMNS are mandatory for an user in terms of Geo.
- ALARM GROUP INFO COLUMNS and ADMIN GROUP INFO COLUMNS can be interpreted as user's attributes as well, because they are mandatory and they do not have underlying dependencies.
- All Profiles (including Profiles without any associations with Users) must be specified in the PROFILES section.
- All AlarmGroups (including AlarmGroups without any associations with Users) must be specified in the ALARM_GROUPS section.
- All AdminGroups (including AdminGroups without any associations with Users) must be specified in the ADMIN_GROUPS section.
- To assign an Alarm Group only its id should be specified as it is a unique identifier.
- To assign an Admin Group only its name should be specified as it is a unique identifier.
- To assign a Profile only its name should be specified as it is a unique identifier.
- This example covers all possible cases of xml USERS section filling.

Define Alarm Groups Example

```
<ALARM_GROUPS>
    <ALARM_GROUP>
        <!-- ALARM GROUP INFO COLUMNS -->
    </ALARM_GROUP>
    ...
</ALARM_GROUPS>
```

- This section contains all AlarmGroups (including AlarmGroups without any associations with Users).
- This example covers all possible cases of xml ALARM_GROUPS section filling.

Define Administration Groups Example

```
<ADMIN_GROUPS>
    <ADMIN_GROUP>
        <!-- ADMIN GROUP INFO COLUMNS -->
    </ADMIN_GROUP>
    ...
</ADMIN_GROUPS>
```

- This section contains all AdminGroups (including AdminGroups without any associations with Users).
- This example covers all possible cases of xml ADMIN_GROUPS section filling.

Define Profiles Example

```
<PROFILES>
    <PROFILE>
        <!-- PROFILE INFO COLUMNS -->
        <ASSIGNED_CLASSMARKS>
            <ASSIGNED_CLASSMARK_ID>...</ASSIGNED_CLASSMARK_ID>
            ...
        </ASSIGNED_CLASSMARKS>
    </PROFILE>
    ...
</PROFILES>
```

- This section contains all Profiles (including Profiles without any associations with Users).
- Profiles can be defined having assigned Classmarks.
- All Classmarks (including Classmarks without any associations with Profiles) must be specified in the CLASSMARKS section.
- This example covers all possible cases of xml PROFILES section filling.
- To assign a Classmark only its id should be specified as it is a unique identifier.

Define Classmarks Example

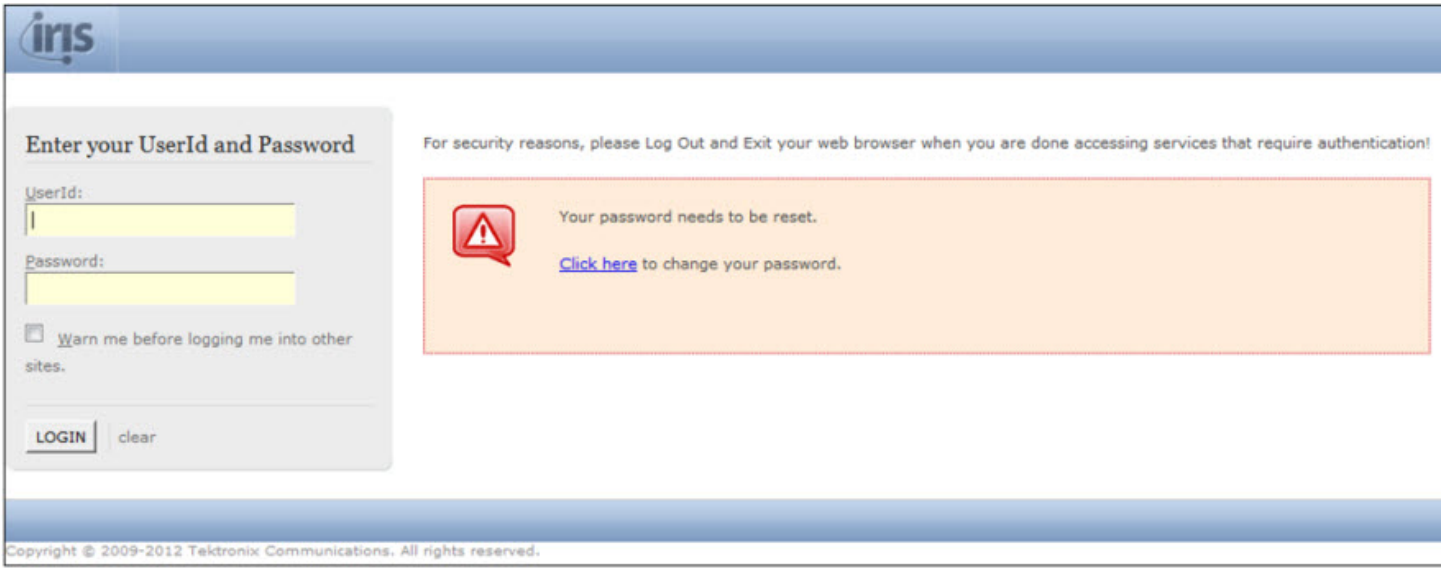
```
<CLASSMARKS>
    <CLASSMARK>
        <!-- CLASSMARK INFO COLUMNS -->
    </CLASSMARK>
    ...
</CLASSMARKS>
```

- This section contains all Classmarks (including Classmarks without any associations with Profiles).
- This example covers all possible cases of xml CLASSMARKS section filling.

Password Migration

Passwords from UACN/RIA and GeoProbe are not migrated to UUMS. UUMS will create a corresponding record in the LDAP (IRIS LDAP mode only) and set a default password directly. The default password is equal to the user login name, but will be in lower case. On the first login the user will be prompted to change the password. If the user account already exists in UUMS, the password will not change.

Password Reset Prompt Window



Single System Administrator Functions

With the integration of UUMS, GeoProbe, and UACN/RIA user management functions, user creation/modification/deletion is now controlled completely in UUMS for all users.

When IrisView/UUMS is down for maintenance, users will not be able to log in to any system since UUMS is the authentication point.

System Administrator Access

Function	IrisView/UUMS	GeoProbe	UACN
Add Users	Yes	No	No
Modify Users	Yes	No	No
Delete Users	Yes	No	No
Manage Passwords	Yes (Iris LDAP Only)	No	No
Admin Access	Full Access	View Only	View Only
Password History	Yes	No	No
System Settings	Full Access	View Only	View Only

Functions of the System Administrator

Feature	Administrators can...
Group User Management	• Rename alarm groups • Add/modify/delete alarm group descriptions • Assign alarm groups to users • Add/delete/rename admin groups • Add/modify/delete admin group descriptions • Assign admin groups to users All pre-existing groups (alarm and admin) defined in the SpIserver are migrated.
GeoProbe Classmarks	• Delete/rename classmark profiles • Add/modify/delete a profile description • Create/modify profiles All pre-existing profiles defined in the SpIserver are migrated.
UACN User Roles	• Create/delete/modify roles[1] • Assign or remove privileges from roles[2] All pre-existing UACN roles defined in the UACN server are automatically discovered.

Digit and User Content Masking Settings	• Set a system default value which can be overridden on a per-user basis. Values are:
	  • User Digit Masking: Default is 0. Zero disables this option, making all digits accessible to the user. A range from 0-20 digits can be set.
	  • User Content Visible: Default is off. If the setting is turned on, the user can see content for protocols like SMS.
	• Users with one or more roles containing the User Content Visible privilege will have the per-user setting User Content Visible enabled.
	• Users with one or more roles having the User Digits Unmasked privilege will be able to access all digits (the per-user setting is zero). If there is no digit masking privilege assigned, the system default applies.
	Pre-existing settings for Iris users are preserved.

User Account Inactivity	User logins through GeoProbe and UACN/RIA count toward the inactivity interval. If the user logs in to GeoProbe and/or UACN/RIA but not IrisView, the user is still considered active. Logins to Cognos do NOT count toward the inactivity interval.

[1]UACN system roles cannot be deleted or modified but they can be added or removed from a user.

[2]Historical PA privileges are only available for assignment when this feature is licensed.

CLI Commands

UUMS Administrators can use command line interface (CLI) commands to perform user management activities. The supported command line options are:

- [--addUser userName password firstName lastName email roleGroup]
- [--removeUser userName]
- [--updateUser userName firstName lastName email]

- [--enableUser userName]
- [--disableUser userName]
- [--listUsers]
- [--listAllRoleGroups]
- [--listUserByRoleGroup roleGroup]
- [--listRoleGroupsByUser userName]
- [--listPrivilegesByUser userName]
- [--addRoleGroupToUser userName roleGroup]
- [--removeRoleGroupFmUser userName roleGroup]
- [--resetPassword userName password]

Option	Required Input	Outcome	Note
addUser	• username • password • firstname • lastname • email • rolegroup	The console displays one of two results: • SUCCESS means a user will be created, and the user is assigned to the designated role group. • UserAlreadyExists means the user already exists in the system.	Only an IrisView user with the ADMIN role is authorized to run this option.
removeUser	• username	The console displays one of two results: • SUCCESS means the user is deleted. • "UserNotExists" means the user cannot be found in the system.	Only an IrisView user with the ADMIN role is authorized to run this option.
updateUser	• username • firstname • lastname • email	The input attributes will replace the user's attributes in the system. If the user does not exists, the execution result is "UserNotExists".	Only an IrisView user with the ADMIN role is authorized to run this option.
enableUser	• username	Enables the designated user. If the user does not exists, the execution result is "UserNotExists" .	Only an IrisView user with the ADMIN role is authorized to run this option.
disableUser	• username	Disables the designated user. If the user does not exists, the execution result is "UserNotExists" .	Only an IrisView user with the ADMIN role is authorized to run this option.

Option	Required Input	Outcome	Note
listUsers		The users info and the last login time are listed. If the user never logged into the system, "LoginInfoNotFounnd" replaces the login time.	
listAllRoleGroups		All role groups defined in the system will be listed.	
listUserByRoleGroup	• rolegroup	All users that belong to the designated role group will be listed.	
listRoleGroupsByUser	• username	All role groups that the designated user belongs to will be listed. If the user does not exist, the execution result is "User not found".	
listPrivilegesByUser	• username	All Privileges the designated user has will be listed. If the user does not exists, the execution result is "User not found".	
addRoleGroupToUser	• username • rolegroup	The console displays one of the following results: • SUCCESS means the designated role group is added to the user • "userRoleNotDefined" means the role group does not exist • "User not found" means the user does not exist.	Only an IrisView user with the ADMIN role is authorized to run this option.
removeRoleGroupFmUser	• username • rolegroup	The console displays one of the following results: • SUCCESS means the designated role group is removed from the user • "userRoleNotDefined" means the role group does not exist • "User not found" means the user does not exist.	Only an IrisView user with the ADMIN role is authorized to run this option.

Option	Required Input	Outcome	Note
resetPassword	• username • password	The console displays one of the following results: SUCCESS means the designated password is set to the designated username account. "userDoesNotExist" means the user cannot be found. If the user was disabled, running this command automatically enables the user account.	Only an IrisView user with the ADMIN role is authorized to run this option.