Government of Saskatchewan

Integrated Resource Information System (IRIS)
Ministry of Energy and Resources

Industry Tip

New IRIS Security Features

Date	Module/Application/Functionality	Notes
June 6, 2018	Security; Security Administrator	Initial Release

With the implementation of IRIS Release 5.14 on June 6, new functionality will be introduced to the IRIS security application. The new concept of Roles, improvements to permission descriptions, new and improved reports, and many other enhancements will change the overall Security Administrator (SA) experience. This is Information Security best practice and allows a more effective and flexible way to manage user access. Also, this is in line with Ministry of ER's compliance with principle of least privilege – meaning user is given just enough access so they can do what they need to do. This document is intended to provide the user a high level overview of some of the key features that have been introduced. Complete details of the new functionality will be available on the online Help System for the Integrated Resources Information System (IRIS), IRIS Help – Security Administration module.

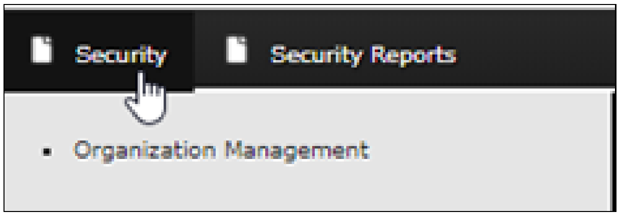
About Roles

Roles are a new function introduced in the 5.14 IRIS Release to make the SA role easier. Roles are optional; if an organization decides not to use Roles, permission sets may continue to be managed individually.

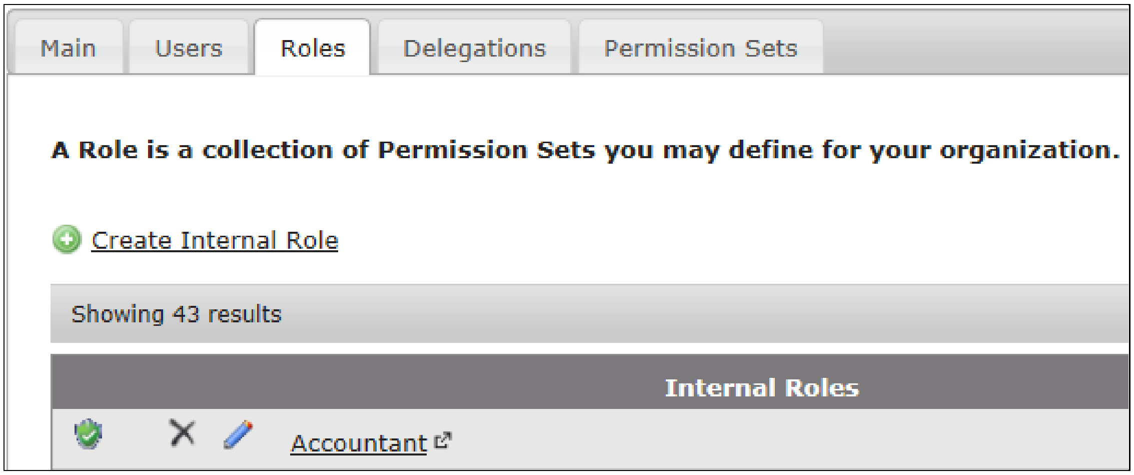
A Role is simply a collection of permission sets that can be assigned to multiple users. Roles have not been pre-determined for IRIS; each Business Associate can define their own roles, as appropriate for their organization. For example, roles might be created for Billing, Production Accounting, Well Licensing, Consultant, etc. A large BA may need more roles than a smaller BA. A user can be granted multiple roles; they can also be granted a combination of Roles and individual Permission Sets.

Overview of New Role Process

a. When a user with SA access logs in, they will see the menu bar with two options, From ‘Security’, select ‘Organization Management’.



b. Select ‘Roles’, ‘Create Internal Roles’ to create a role for each of the logical groups.



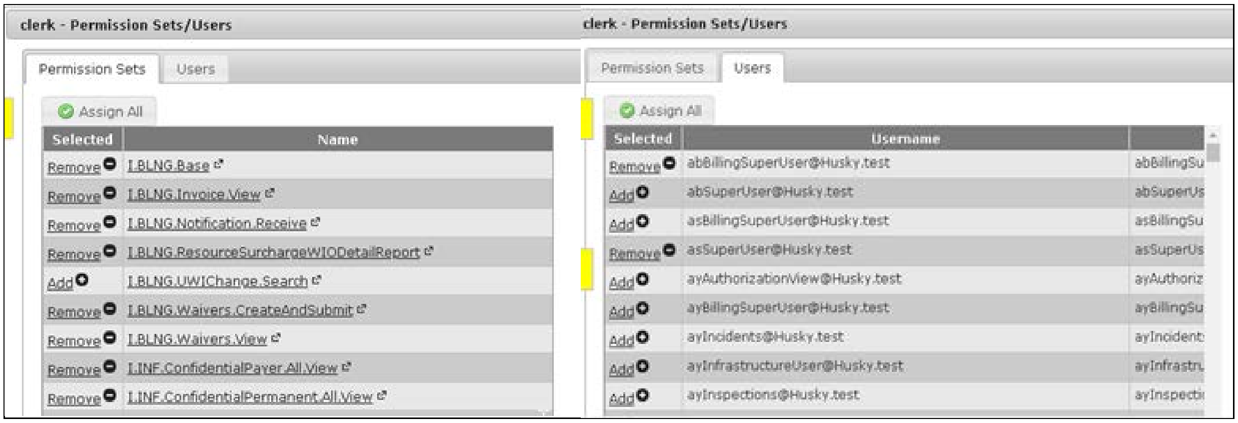
A Role is a collection of Permission Sets you may define for your organization.

Create Internal Role

Showing 43 results

Internal Roles
Accountant

c. Complete the Name and Description fields to describe what the role will enable. Assign the Permission Sets and Assigned Users to the role. These assignments can be done from the Roles Tab, by using the Edit icon ✓ to choose the permission sets and/or users.



clerk - Permission Sets/Users

Selected	Name
Remove ⊖	I.BLNG.Base
Remove ⊖	I.BLNG.Invoice.View
Remove ⊖	I.BLNG.Notification.Receive
Remove ⊖	I.BLNG.ResourceSurchargeWIODetailReport
Add ⊕	I.BLNG.UWIChange.Search
Remove ⊖	I.BLNG.Waivers.CreateAndSubmit
Remove ⊖	I.BLNG.Waivers.View
Remove ⊖	I.INF.ConfidentialPayer.All.View
Remove ⊖	I.INF.ConfidentialPermanent.All.View

clerk - Permission Sets/Users

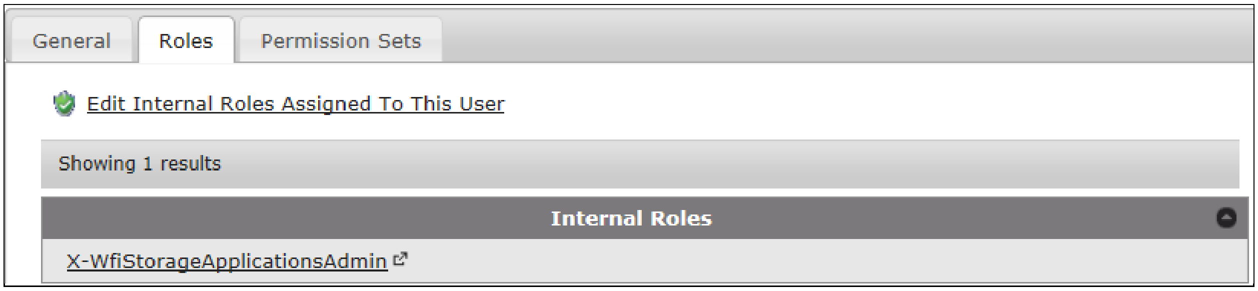
Selected	Username	
Remove ⊖	abBillingSuperUser@Husky.test	abBillingSu
Add ⊕	abSuperUser@Husky.test	abSuperUs
Add ⊕	asBillingSuperUser@Husky.test	asBillingSu
Remove ⊖	asSuperUser@Husky.test	asSuperUs
Add ⊕	ayAuthorizationView@Husky.test	ayAuthoriz
Add ⊕	ayBillingSuperUser@Husky.test	ayBillingSu
Add ⊕	ayIncidents@Husky.test	ayIncident:
Add ⊕	ayInfrastructureUser@Husky.test	ayInfrastru
Add ⊕	ayInspections@Husky.test	ayInspecti

About Users and Roles

Roles can also be assigned from the Users tab, by using the Action icon from the selected user.

Overview

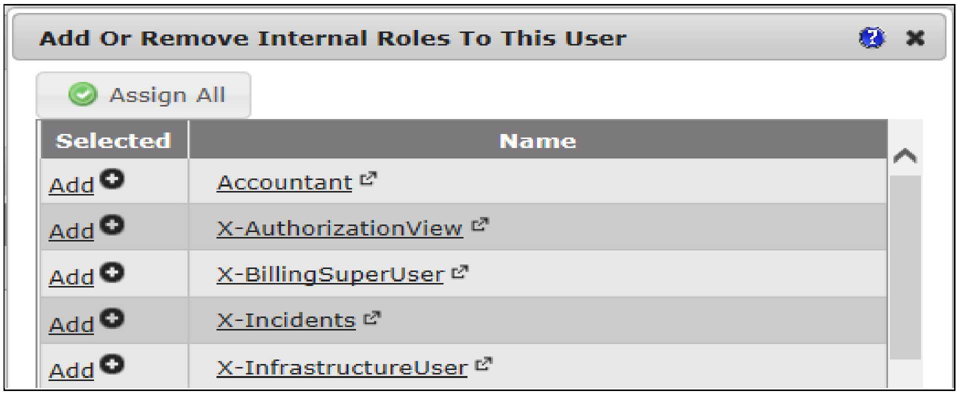
a. Click 'Edit Internal Roles Assigned to this User' from the Roles tab.



Showing 1 results

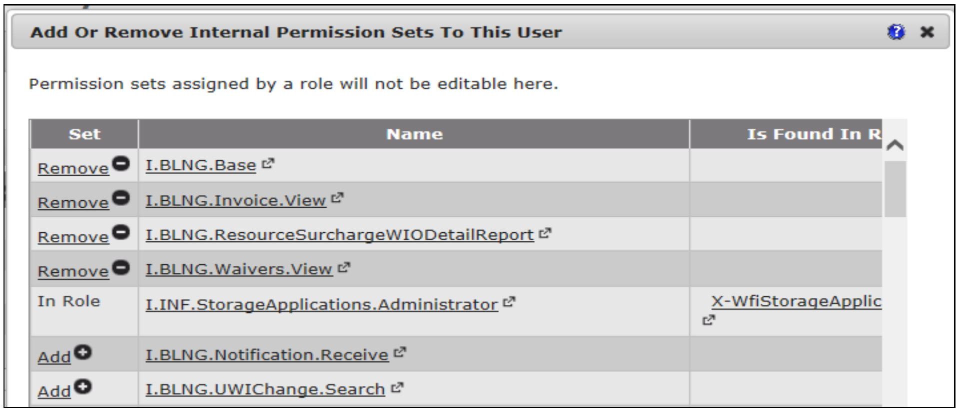
Internal Roles
X-WfiStorageApplicationsAdmin

b. You then Add or Remove roles for that user.


Add Or Remove Internal Roles To This User

Selected	Name
Add	Accountant
Add	X-AuthorizationView
Add	X-BillingSuperUser
Add	X-Incidents
Add	X-InfrastructureUser

If that user needed a combination of roles plus a few individual permission sets, individual permission sets could be selected from their Permission Sets tab. Any permission sets that the user already has as a result of a role will show 'In Role', with the role indicated on the right.


Add Or Remove Internal Permission Sets To This User

Permission sets assigned by a role will not be editable here.

Set	Name	Is Found In R
Remove	I.BLNG.Base	
Remove	I.BLNG.Invoice.View	
Remove	I.BLNG.ResourceSurchargeWIODetailReport	
Remove	I.BLNG.Waivers.View	
In Role	I.INF.StorageApplications.Administrator	X-WfiStorageApplic
Add	I.BLNG.Notification.Receive	
Add	I.BLNG.UWIChange.Search	

Please Note:

In the new IRIS Security screens, there are no more check boxes for assigning permission sets or users or roles. The word in the 'Selected' column indicates whether an item is assigned or not:

- 'Remove' indicates it is assigned. These sort to the top when the window is opened again.
- 'Add' indicates it is not assigned.
- 'From Role' indicates it is assigned via a role.

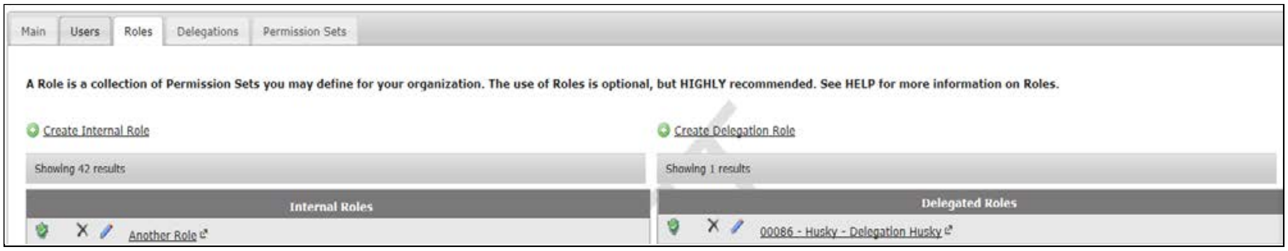
Assignment happens IMMEDIATELY, so there is no SAVE button. If you click 'Add', the user will have that permission the next time they sign on.

About Delegation of Roles

Roles can also be created from Delegated Permissions received from another Business Associate. The right side of the Roles Screen will show Delegated Roles.

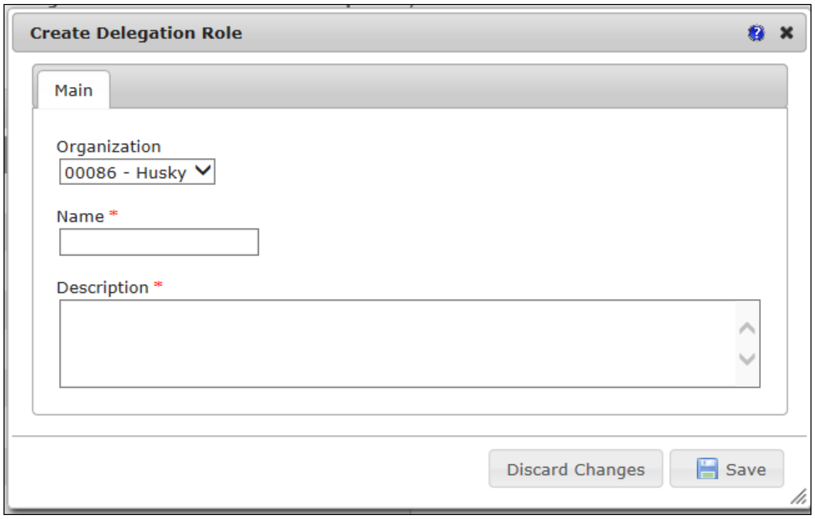
Overview

a. Click 'Create Delegation Role' from the Roles tab.



A Role is a collection of Permission Sets you may define for your organization. The use of Roles is optional, but HIGHLY recommended. See HELP for more information on Roles.

b. Complete the Name and Description fields to describe the role, click Save.



Organization
00086 - Husky

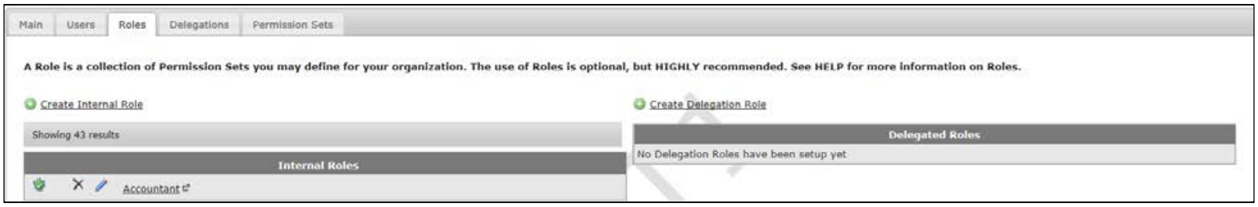
Name *

Description *

<u>Please Note:</u>

The right side of the Roles tab shows Roles created from Delegations received from other organizations. If your BA does not have any delegations from other BAs, this side of the screen will show no delegated roles assigned. Delegated roles must be specific for each organization.

To see Delegations initiated by the organization, see the Delegations Tab.



A Role is a collection of Permission Sets you may define for your organization. The use of Roles is optional, but HIGHLY recommended. See HELP for more information on Roles.

Showing 43 results

Internal Roles
Accountant

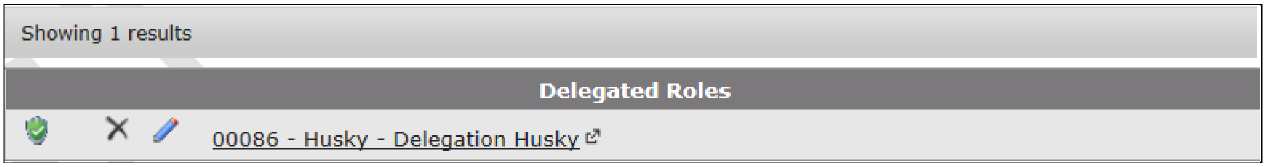
Delegated Roles
No Delegation Roles have been setup yet

About Modifying Delegated Role Permission Sets and User (Received Delegations

Permission set or users may be added or removed from the Delegated Role. The Permission sets and Users that have been assigned should sort to the top, and are indicated with the word 'Remove' in the Selected column. Those not assigned show 'Add'.

Overview

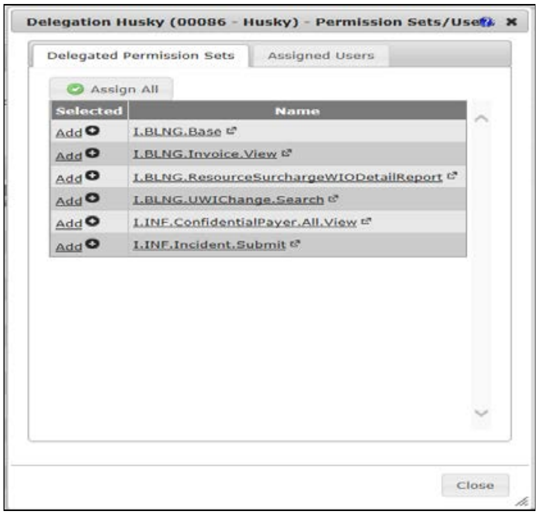
a. Click the Edit ✓ icon next to the Delegated Role to be changed.



Showing 1 results

Delegated Roles
00086 - Husky - Delegation Husky

b. Click 'Add' to add the permission set to the role **AND/OR** Click 'Add' to add a role to the user .


Delegation Husky (00086 - Husky) - Permission Sets/Use
Delegated Permission Sets
Assigned Users
Assign All
Close

Selected	Name
Add	I.BLNG.Base
Add	I.BLNG.Invoice.View
Add	I.BLNG.ResourceSurchargeWIODetailReport
Add	I.BLNG.UWIChange.Search
Add	I.INF.ConfidentialPayer.All.View
Add	I.INF.Incident.Submit

About User Cloning permissions

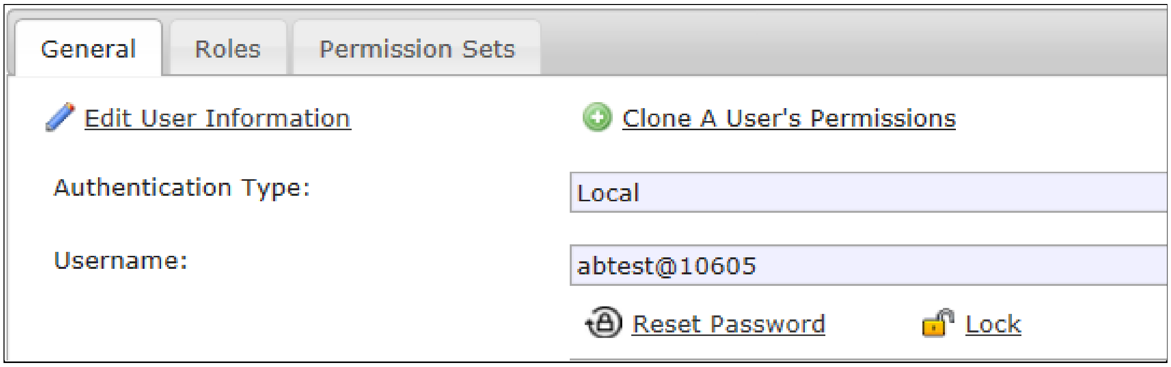
Rather than creating identical permissions for multiple users, the Security Administrator may now clone a user's permissions (both internal and delegated roles, and both internal and delegated directly assigned permissions).

Please Note:

- To clone **to a New User**, the user must first be created. From the User General screen, select **Clone A User's Permissions.**
- To clone **to an existing user who had permissions**, all their original permissions will be wiped out and replaced with the permissions from the clone source.
- This screen will NOT clone an SA setting – that is done by simply editing the user, and checking the appropriate box. If a SA account is cloned to an existing user, all IRIS permissions of the existing user will be removed. If the intention is to give a user both IRIS permissions and SA rights, they will need to have 2 accounts.

Overview

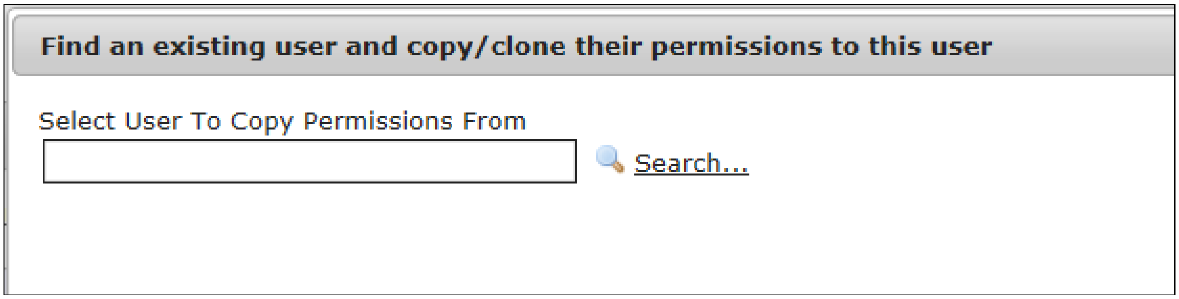
a) Click Clone A User's Permissions



Authentication Type: Local

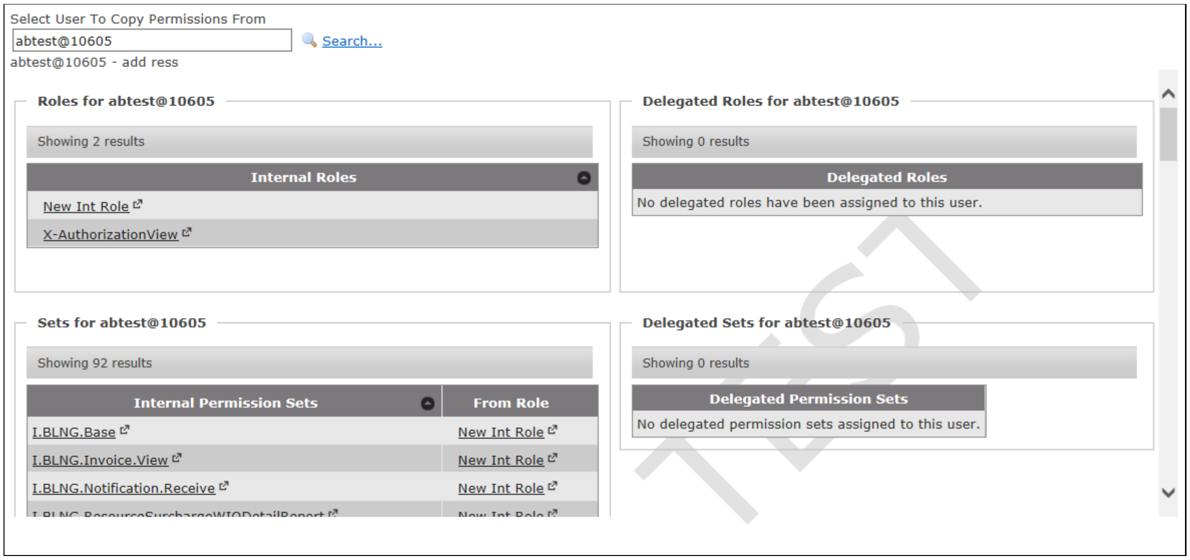
Username: abtest@10605

b) Select user to Copy



Find an existing user and copy/clone their permissions to this user

c) This pop-up displays the permissions that will replace the edited user's current permissions.



Select User To Copy Permissions From

abtest@10605 Search...

abtest@10605 - add ress

Roles for abtest@10605

Showing 2 results

Internal Roles
New Int Role
X-AuthorizationView

Delegated Roles for abtest@10605

Showing 0 results

Delegated Roles
No delegated roles have been assigned to this user.

Sets for abtest@10605

Showing 92 results

Internal Permission Sets	From Role
I.BLNG.Base	New Int Role
I.BLNG.Invoice.View	New Int Role
I.BLNG.Notification.Receive	New Int Role
I.BLNG.ResourceSurchargeWIODetailReport	New Int Role

Delegated Sets for abtest@10605

Showing 0 results

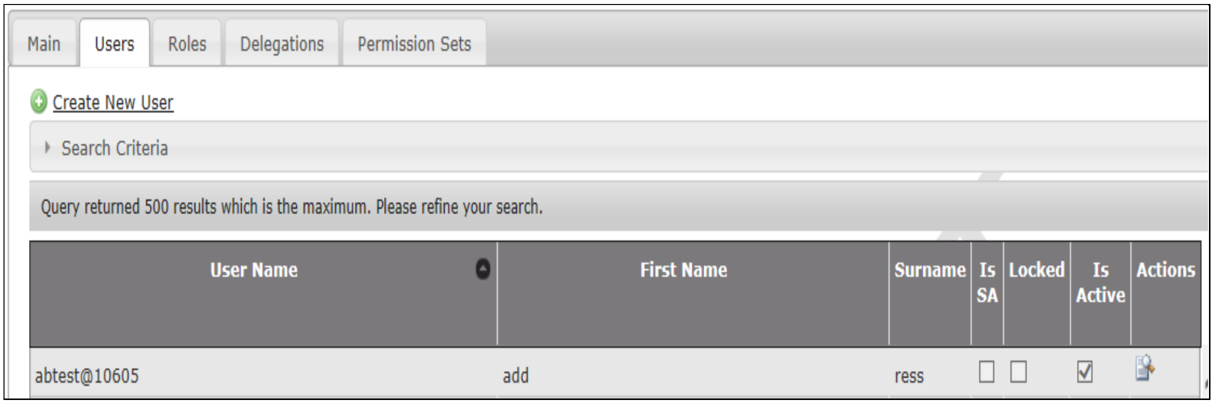
Delegated Permission Sets
No delegated permission sets assigned to this user.

About Reset Password

SAs now have the ability to reset passwords for other users.

Overview

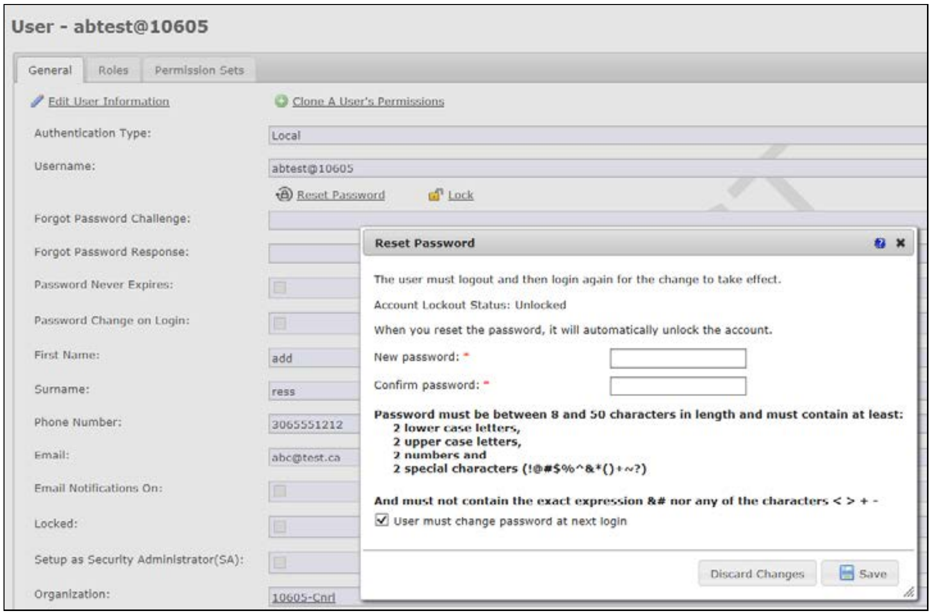
Password can be reset by clicking the Action icon from the selected user.



Query returned 500 results which is the maximum. Please refine your search.

User Name	First Name	Surname	Is SA	Locked	Is Active	Actions
abtest@10605	add	ress	□	□	☑	

a) Click Reset Password from the General tab.



User - abtest@10605

Authentication Type: Local

Username: abtest@10605

Forgot Password Challenge:

Forgot Password Response:

Password Never Expires: □

Password Change on Login: □

First Name: add

Surname: ress

Phone Number: 3065551212

Email: abc@test.ca

Email Notifications On: □

Locked: □

Setup as Security Administrator(SA): □

Organization: 10605-Cnrl

Reset Password

The user must logout and then login again for the change to take effect.

Account Lockout Status: Unlocked

When you reset the password, it will automatically unlock the account.

New password: *

Confirm password: *

Password must be between 8 and 50 characters in length and must contain at least:
2 lower case letters,
2 upper case letters,
2 numbers and
2 special characters (!@#$%^&*()+~?)

And must not contain the exact expression &# nor any of the characters < > + -

☑ User must change password at next login

b) Complete New Password and Confirm Password. The user must logout and then login for the change to take effect.

Please note: Resetting a password will automatically unlock the user account.

Questions?

For more information on:

• Accessing IRIS, or the new IRIS security application functionality implemented in IRIS Release 5.14 on June 6, please call our service desk at 1-844-213-1030 or email er.support@gov.sk.ca.