DTS 4: User Manager Guide

APELON

BECAUSE TERMINOLOGY MATTERS

75 Sgt William B Terry Dr, Suite 2005, Hingham, MA 02043

+1 (203) 431-2530

www.APELON.com

www.ApelonDTS.org

Table of Contents

Introduction

User (logon) access to DTS ("authentication") is controlled by the underlying Application Server, e.g. JBoss, authentication processes. Application Server administrator functions define a User (user account) by creating a username and access password, and associating Application Server roles with the account. DTS Users must be given the *apelondts* (or *apelondtsadmin*, see below) roles to gain access to DTS. See the documentation supplied with your Application Server for details on User account creation. (The **DTS 4 Installation Guide** provides basic account creation instructions for a JBoss installation.)

In addition to this basic user authentication, DTS provides additional, functional, access control facilities, via a multi-level role-based methodology. First, DTS defines a set of atomic *Permissions*. Example Permissions are *Write Permission to MyNamespace*, and *Permission to create and delete Subsets*. These low-level Permissions can be grouped in installation-defined *Roles*. Roles could be defined for System Administrators, content modelers, and clinical browsers. Finally, Application Server *Users* are given one, or more, Roles.

When a User logs in to DTS, their Roles are accessed, and in turn, the Permissions associated with those Roles. The union of all of the User's Role's Permissions define what that User can access/do.

These relationships between Permissions, Roles and Users are maintained via the DTS **User Manager** module. The User Manager is available in the DTS Editor **Options** menu. In order to run the User Manager, however, the User must have the Application Server *apelondtsadmin* role. (Note that *apelondtsadmin* is an Application Server, e.g. JBoss, role and must be assigned by the appropriate Application Server authentication processes. This role must be distinguished from DTS Roles as discussed in this document.)

The following sections provide additional details on Permissions and Roles, and describe how the User Manager can be used to manage access control relationships.

Access Elements

Permissions

DTS defines a variety of access Permissions to enable organizations to tailor their access models to meet individual needs. There are two general types of Permissions: *Admin Permissions* that apply across different DTS object instances, and *Object Permissions* that apply to individual instances of DTS objects.

The three types of Admin Permissions are:

NAMESPACE_ADMIN	Allows the User to create and delete Namespaces. This Permission also allows modification of local Namespace Name, Authority and Writability: changing from Read/Write to Read-Only and from Read-Only to Read/Write.
SUBSET_ADMIN	Allows the User to create and delete Subsets. This Permission also allows modification of local Subset Name, Authority and Writability: changing from Read/Write to Read-Only and from Read-Only to Read/Write.
AUTHORITY_ADMIN	Allows the User to create and delete Authorities. This Permission also allows modification of the Authority Description.

Object Permissions are available separately for each instance of a top-level DTS Object, i.e., Namespaces, Subsets, and Authorities. E.g., a User can be given only Read Permission to the 'States of the Union' Namespace, but Write Permission to the 'Triad' Namespace.

The three Namespace Permissions are:

NAMESPACE_READ	Allows Read access to the specific Namespace
NAMESPACE_WRITE	Allows creation/modification of Concepts and Terms and all of their attributes. Includes NAMESPACE_READ Permission.
NAMESPACE_MANAGE	Allows creation/modification of all Types associated with the specific Namespace, Namespace Publish and creation/modification of Namespace and Version Properties. Includes NAMESPACE_WRITE Permission.

The three Subset Permissions are:

SUBSET_READ	Allows Read access to the specific Subset.
SUBSET_WRITE	Allows creation, modification and building of the specific Subset Expression. Includes SUBSET_READ Permission.
SUBSET_MANAGE	Allows creation/modification of all Types associated with the specific Subset, Subset Publish and creation/modification of Subset and Subset Version Properties. Includes SUBSET_WRITE Permission.

There are only two Authority Permissions:

AUTHORITY_READ	Allows Read access to the specific Authority
AUTHORITY_MANAGE	Allows creation/modification of all Types associated with the specific Authority, and creation/modification of Authority Properties. Includes AUTHORITY_READ Permission.

Note that Object Permissions are additive: MANAGE includes WRITE, which includes READ. Thus one, and only one, of these Permissions can be selected for a given Object.

Remember that the ability to perform certain actions in DTS is a function of both the User's Permissions and the state of an Object. For example, if a local Namespace has been set to **Read-Only**, its contents cannot be modified even if the User has **WRITE** or **MANAGE** Permission. The only exception is that a User with **MANAGE** Permission can change the state of the Namespace back to **Read/Write**.

Roles

DTS enables the grouping of the Permissions described above into organization-defined Roles. A DTS Role is a named entity that encapsulates access to a specific set of operations on a specific (set of) top-level DTS Objects: Namespaces, Subsets, and Authorities. Roles are meant to represent "types" of Users, or typical User use-cases. Thus there could be an "Admin" Role that allows creation (and deletion) of Namespaces, Subsets, and Authorities, or a "Lab Manager" Role that gives Manage access to Laboratory Namespaces and Subsets. Roles can have as many, or as few, Permissions as are required.

A DTS Role is created by giving it a name, and assigning a set of DTS Permissions to it. Creation of a Role and assignment of Permissions to Roles can be made via the API or through the User Manager GUI application (see **Using the DTS User Manager** below).

Users

As was described in the Introduction, Users are defined in the Application Server authentication function, not through DTS. DTS identifies Users by the username given to the User by the Application Server administrator. The DTS **User Manager** application, or DTS API, can associate one or more Roles with Users (usernames). The set of Roles associated with the User is called the User's *Profile*.

For security reasons, DTS does not have access to the Application Server usernames. DTS administrators must enter User names into the User Manager, or the API, and assign Roles to these Users. It is the responsibility of the administrator to maintain equivalence between entered DTS User names and the "official" Application Server usernames.

Special Conditions

There are two special access conditions: (a) a new (to DTS) User signs in without a DTS User Profile; and (b) a new Namespace (or Subset or Authority) is created.
For the first case (new User) the User is given default *Read* access to all Namespaces, Subsets, and Authorities. No permanent User Profile, or Role, is created.

In the second case (new Namespace/Subset/Authority), all Users are given default Read access to the new Object. In addition, DTS adds MANAGE access on the object to the User's Roles that has the associated Admin Permission (if more than one Role with Admin Permission exists for the user then only one of these Roles will be given the MANAGE access for the object). Without this latter step, the User, who could be a batch load program, could not continue to populate the new object without separately modifying Roles/Permissions (which they might not be able to do if they were not an *apelondtsadmin*).

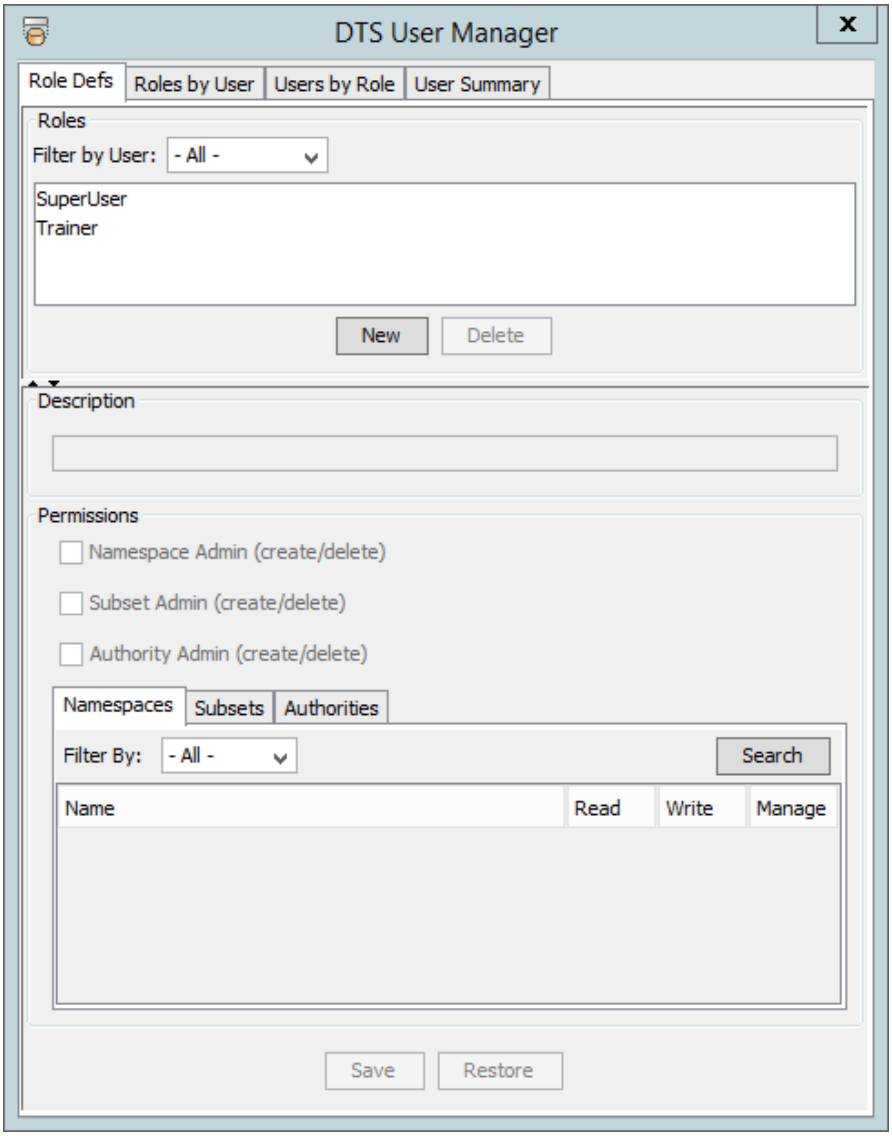
Using the DTS User Manager

The DTS **User Manager** is a GUI application (actually a DTS Editor Module) that manages Roles and User Profiles. The User Manager enables (1) the creation of DTS Roles and their association with Permissions, and (2) the creation of DTS User Profiles and assignment of the Roles to these Users.

The User Manager application is available from the **Options** menu in the standard DTS Editor layout. As described earlier in this document, the User Manager is only enabled for users having the *apelondtsadmin* Application Server role.

Starting the User Manager

After selecting the User Manager, the dialog shown below is displayed.



This window consists of a pane with four tabs:

Role Defs	Create and manage DTS Role definitions
Users by Role	View and edit the Roles associated with a given User
Roles by User	View and edit the Users associated with a given Role
User Summary	View all object permissions associated with a selected User

Typically, a DTS administrator would first create a set of Roles and assign each Role's individual Permissions using the first tab, then assign these Roles to Users using the second or third tab. Note that since the **Users by Role** tab and **Roles by User** tab simply provide different "views" into the User Profiles, once any edits are pending in either tab, the other tab is no longer available for selection.

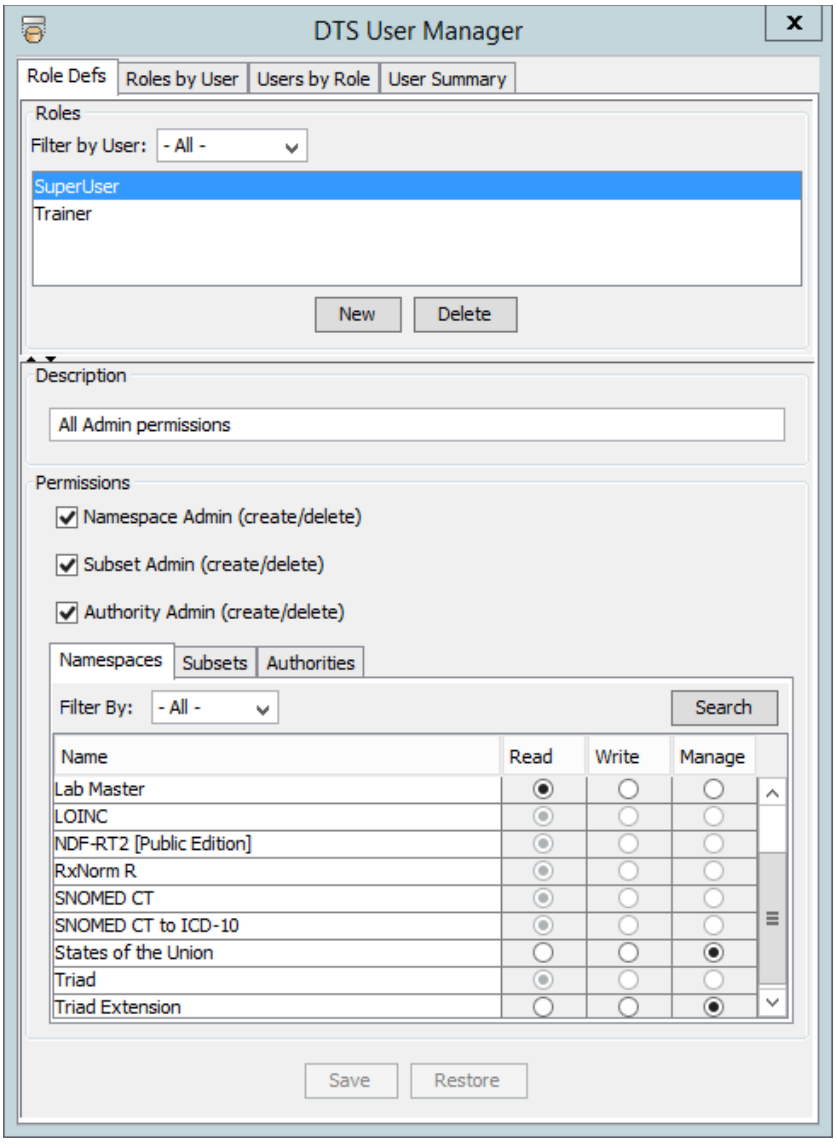
The following sections describe operation of these panels.

Role Definitions Tab

DTS Roles are named "envelopes" that hold a set of Permissions. The use of Roles facilitates matching an organization's actual DTS activities, e.g., "Laboratory Data Manager", with specific Users.

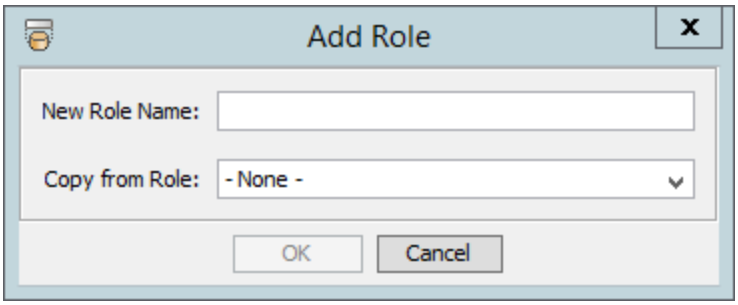
The **Role Definitions** tab is used to create and manage the Permissions associated with a Role. The panel consists of a list of all DTS Roles at the top, a resize divider, and a Permissions panel for editing Permission participation for a selected Role at the bottom. Drag the divider to reapportion space between the Role list and the Permissions panel.

To view, or edit, the Permissions associated with a Role, select the Role from the Role list. The Permissions Panel is then populated as shown below:



The Role Description is shown first, followed by the Admin Permissions. At the bottom of the panel is another tabbed panel with tabs for **Namespaces**, **Subsets**, and **Authorities**. To add, or remove, an Admin Permission, click the associated Permission box. To change the Permission level for a Namespace, select the **Namespaces** tab, and click the desired Permission radio button for the Namespace. The Permissions for Read-Only Namespaces will be grayed and unavailable for selection. You can set the same Permission on all (writable) Namespaces by clicking on the table column header for that Permission. The **Subset** and **Authority** tabs operate similarly. Finally, click **Save** to persist the updated Permission settings for the Role.

To create a new Role, click the **New** button. This opens the **Add Role** window:

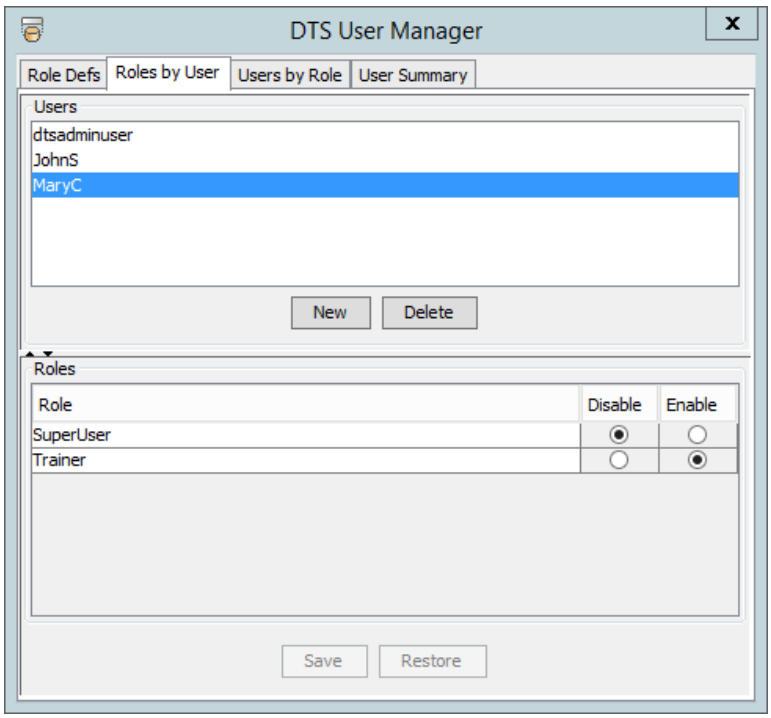


Enter the desired name of the Role and click **OK**. Note that Role names must be unique. You will not be allowed to create a Role with the same name as an existing Role. The new Role's Permissions can also be copied directly from an existing Role's Permissions using the Copy from Role dropdown. Modifications to the copied Role can be completed after Role creation.

To delete an existing Role, select the Role in the Role list and click **Delete**. A confirmation dialog is shown. When a Role is deleted, all references to the Role in User Profiles are removed.

Roles by User Tab

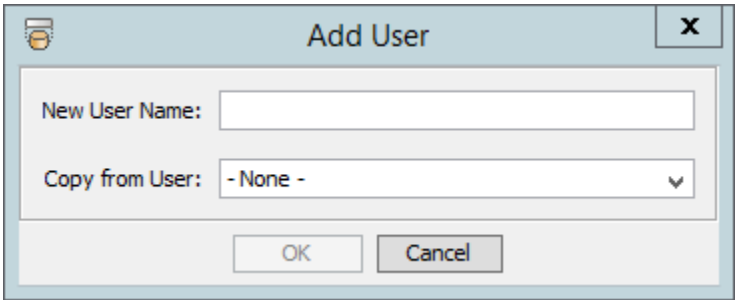
The **Roles by User** tab shows what Roles are enabled, i.e. active, for a specific User. To see a User's Profile, select the User from the User list.



Click the **Enable** or **Disable** radio button across from any Role to enable, or disable, that Role in the User's Profile. You can enable or disable all Roles on the selected User by clicking on the **Enable** or **Disable** table column header.

Click **Save** to persist any Role changes for the User Profile or click **Reload** to discard changes and restore the original Profile.

To create a new User Profile, click the **New** button. This opens the **Add User** window:

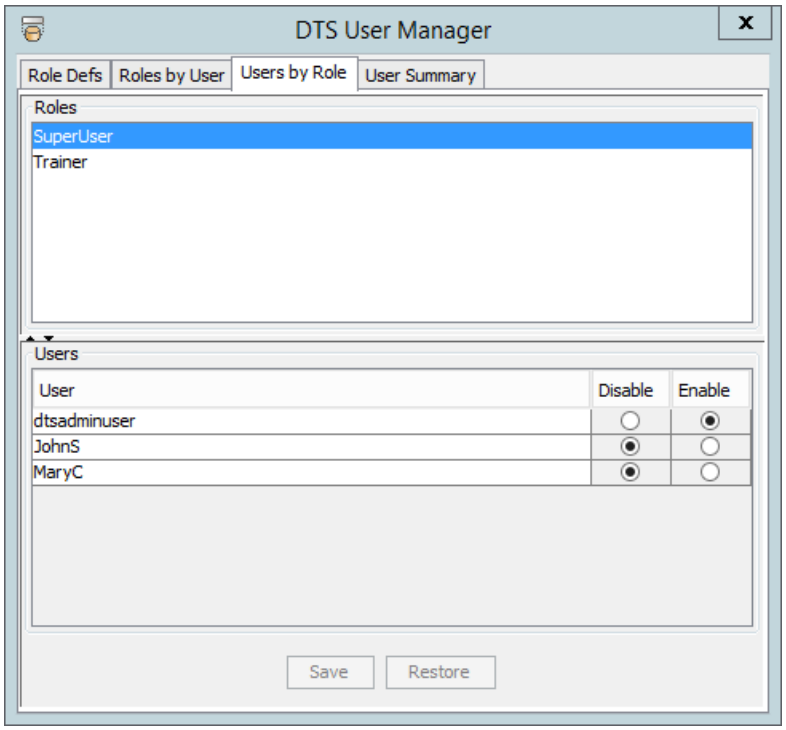


Enter the desired User name and click **OK**. Note that User names must be the same as the usernames created in your Application Server. User names also must be unique. You will not be allowed to create a User with the same name as an existing User. The new User's Role designations (Disable/Enable) can also be copied directly from an existing User using the Copy from User dropdown. Modifications to the copied User's Role designations can be completed after User creation.

To delete an existing User Profile, select the User in the User list and click **Delete**. A confirmation dialog is shown. Note that deleting a User name in the User Manager has no effect on the existence of the username in the Application Server.

Users by Role Tab

The **Users by Role** tab shows what Users have enabled a specific Role. This is a convenience panel that shows an "inverted view" of the same Profile data provided in the **Roles by User** tab. To see the users having a given Role, select the Role from the Role list.



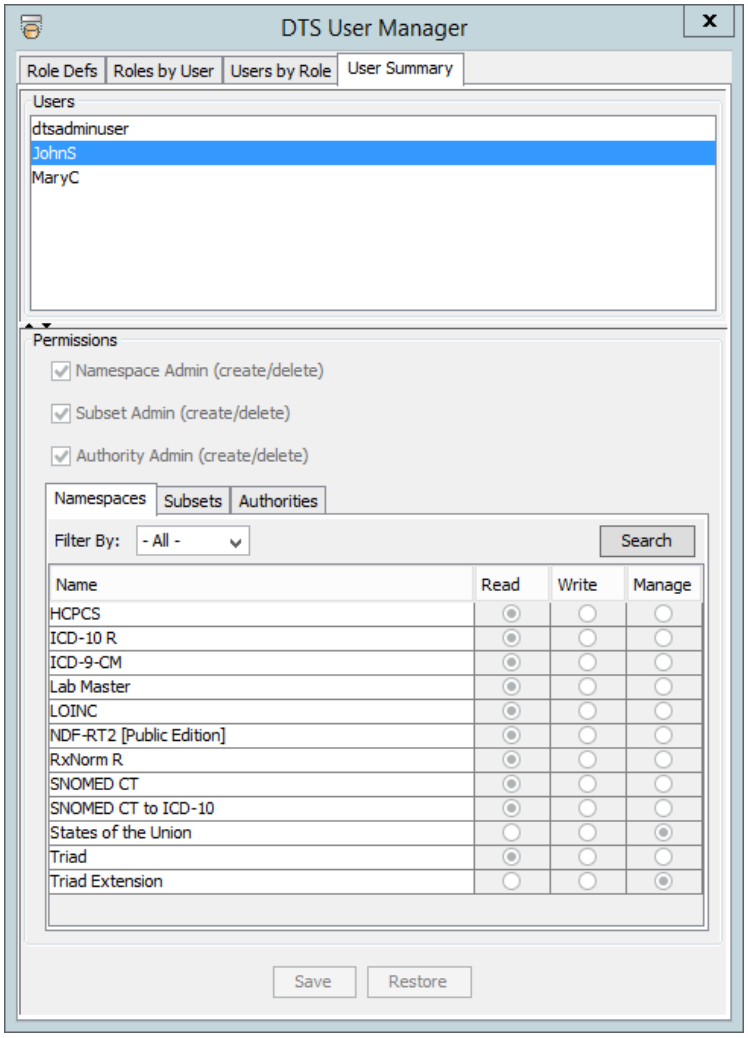
Click the **Enable** or **Disable** radio button across from any User to enable, or disable, the selected Role in that User's Profile. You can enable or disable the selected Role for all Users by clicking on the **Enable** or **Disable** table column header.

Click **Save** to persist any User Profile changes for the Role or click **Reload** to discard the changes and restore the original Profile data.

To add or delete Roles, use the **Role Defs** tab.

User Summary Tab

The **User Summary** tab displays a read-only view of what permissions Users have. This is a convenience panel that shows an overview of a selected User's permissions and can be helpful when determining which objects Users have permissions for if that User has several Roles enabled.



To add, modify, or delete Roles, use the **Role Defs** tab.

To enable or disable Roles from a User, use the **Roles by User** or **Users by Role** tabs.