Creating and Managing User Accounts

Overview

In VIVO, the basic functions of browsing and searching are open to anyone. However, if a VIVO user wants to edit items on their profile, view restricted data, or to manage VIVO, they must log in via a User Account.

When a user logs in, they provides their credentials and are associated with a User Account. The credentials are often an Email address and password, but might be different information, depending on how VIVO is configured.

Each User Account has a Role assigned to it. The Role determines how much the user is authorized to do. The lowest Role will permit the user to edit his own profile page. Higher Roles permit editing additional data properties, modifying the ontologies, and administering the VIVO application.

Authentication

Internal Authentication

Every VIVO system allows users to log in to an existing User Account by supplying the Email Address and password to the account. Even in an installation that relies on external authentication, there are administrative pages that allow a user to login with Email Address and password.

External Authentication

VIVO can be configured to work with an External Authentication system like Shibboleth or CUWebAuth. In that case, the user provides whatever information the External Authentication system requires, and the External Authentication system passes an ID value to VIVO. VIVO recognizes that the user is logged in to the User Account whose "External Authentication ID" field matches that ID.

If a user passes External Authentication, but no User Account matches the ID, VIVO prompts the user to enter his Email Address, First Name, and Last Name, and creates a User Account with that information.

NOTE: To configure VIVO for an External Authentication system, please consult the section entitled 'Enable an External Authentication System'. Note also that the value of the property (the designated External Authentication ID field) must be an **exact match** for the username/email of the user.

External-Only Accounts

When creating an account, an administrator may indicate that it is for external authentication only. In that case, no password is assigned to the account, since the External Authentication system manages its own passwords or other credentials.

What is a User Account?

Each User Account is identified by the user's Email address. Each account will have the user's first name and last name, and a role. The account will have additional information, depending on how it is used.

- External Authentication ID – permits logging in by the External Authentication system.
  NOTE: Two User Accounts may not have the same External Authentication ID
- Password – permits logging in by the Internal Authentication system.
- Matching ID – value can be used to associate the User Account with a profile page.

Associating User Accounts with Profile Pages

Each User Account may be associated with an Individual in the VIVO data model. The display page for that Individual is known as the “profile” for that User Account.

A common use of this feature is matching a profile to each member of the campus community. When a user logs in to VIVO, they are directed to their profile page, and are authorized to edit the information on that page.

To associate profiles with user accounts,

1. set selfEditing.idMatchingProperty in runtime.properties to the URI of the datatype property whose values will be used to associate profiles to accounts. A common choice is the university "net id" or other local identifier.
2. For each user that will have a corresponding account, set the value of the idMatchingProperty on the user's profile.
3. Set the value of Matching ID on the user's account to the value on the user's profile.

User Roles

In VIVO there are four user roles that can be assigned: administrator, curator, editor, and self-editor. Future releases will allow VIVO administrators to create additional roles. Permissions provided to roles will determine access options available to user accounts within VIVO. It is important to consider what a new user’s role may be, prior to setting up the new account.

Self-Editor -– The self-editor may create data properties, relationships and entities directly associated to his or her profile.

Editor -– The editor may add, delete and modify entities, object properties and data properties.

Curator -– In addition to performing the tasks of the Editor, the Curator may modify the ontologies, class groups, property groups, and edit site information, including the text displayed on the About page and contact email address.

System Administrator –- In addition to the abilities of the Curator, the Administrator may access the menu management, user accounts, and advanced data tools features. The advanced data tools section include the ingest menu, Add/Remove RDF data, RDF export, SPARQL query, and SPARQL query builder privileges.

The Root User Account

Each VIVO installation has a special User Account, called the root account. The root account has no Role. Nonetheless, the root account is authorized:

- to see all data elements
- to edit all data elements
- to view any page
- to modify the ontologies

Since the root account can do all of these things, it can be particularly useful and particularly dangerous. It can also give you a distorted view of what your VIVO site looks like. Use the root account to create other User Accounts or to access VIVO in emergencies, and use it with deliberation.

The email address for the root account is specified as part of the VIVO installation process.

NOTE: To configure the root account, please consult the Installation Guide, and refer to the section entitled 'Specify Runtime Properties'.

Managing User Accounts

Normal workflow

In normal operation, users will receive an Email message when a VIVO account is created for them, when their password is reset by an administrator, or when the Email address on their User Account is changed. One benefit of this is that the administrator does not need to know the user’s password, and does not need to tell the user his password.

As noted above, when a new account is created, or when an administrator resets the user’s password, the user receives an Email message. The message describes the action that has occurred, and includes a link for the user to click, to set the password on the account.

Note: *User Accounts that are created for External Authentication do not require passwords, so no such link is sent.*

Workflow without Email

Email notifications can be disabled by configuring VIVO without a “Reply-To” address. In that case, users are not notified when User Accounts are created or changed.

When creating a new User Account, the administrator must set a password, and must inform the user of the password (unless the account is to be used for External Authentication only). When the user first logs in to the account, he will be prompted to change the password. Resetting the password on an account involves a similar process.

Note: *To disable Email notifications, please consult the Installation Guide, and refer to the section entitled 'Specify Deployment Properties'.*

External Authentication

In many VIVO installations, the creation of most User Accounts is simple and routine. A user presents credentials to the External Authentication system, and VIVO creates an account with minimal privilege, prompting the user for name and Email Address. In this case, an administrator may edit such an account to assign a higher Role, if desired.

Alternatively, an administrator may create a User Account, add an External Authentication ID, and assign a high-level Role. When the user log in for the first time, they will already have an account with the desired level of privilege.