Administering Users

At a high level, XNAT Administrators need to worry about the site-wide rules for user access. The details of which user has access to what data is typically managed on a project-by-project basis as a responsibility of the project owners themselves. This document contains an overview of site-wide user settings, instructions for adding, enabling or disabling users via the Admin panel, and some under-the-hood explanations of how XNAT manages user sessions, project access requests, and other related concepts.

Managing User Registration Settings

In the Admin UI, you can set site-wide preferences for user registration and account management.

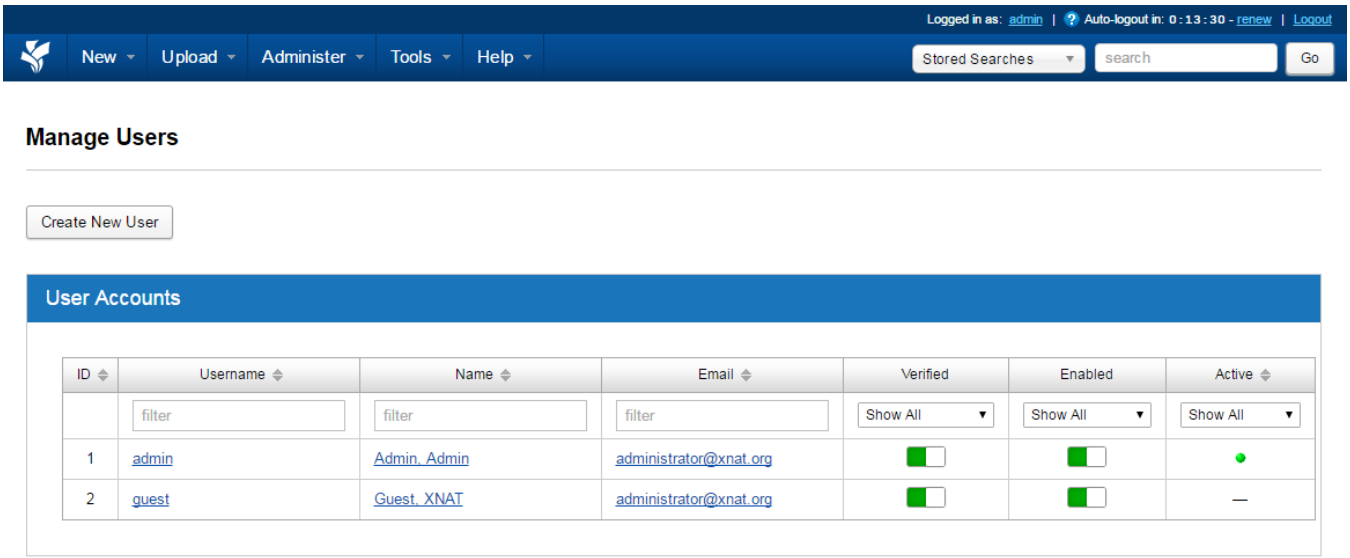
See: Setting User Registration Options in XNAT

Creating a User Account

User accounts can be created in one of three ways:

1. **Users can register for a new account through the login page, by clicking "Register."** By default, these accounts will require an email verification step AND administrator approval before they can get access to your XNAT. Administrators will receive an email notification after each registration.
2. **Users can be invited to join XNAT by an existing XNAT project owner.** This will send a customized registration email containing a **Project Access Request** link. When the recipient clicks on this link, they will be asked to register a new user account. By default, these accounts will not require a separate email verification step OR administrator approval before they can access your XNAT. Additionally, this new account will immediately be granted access to the specified project.
3. **XNAT Administrators can create new user accounts through the XNAT Admin UI.**

Managing User Accounts



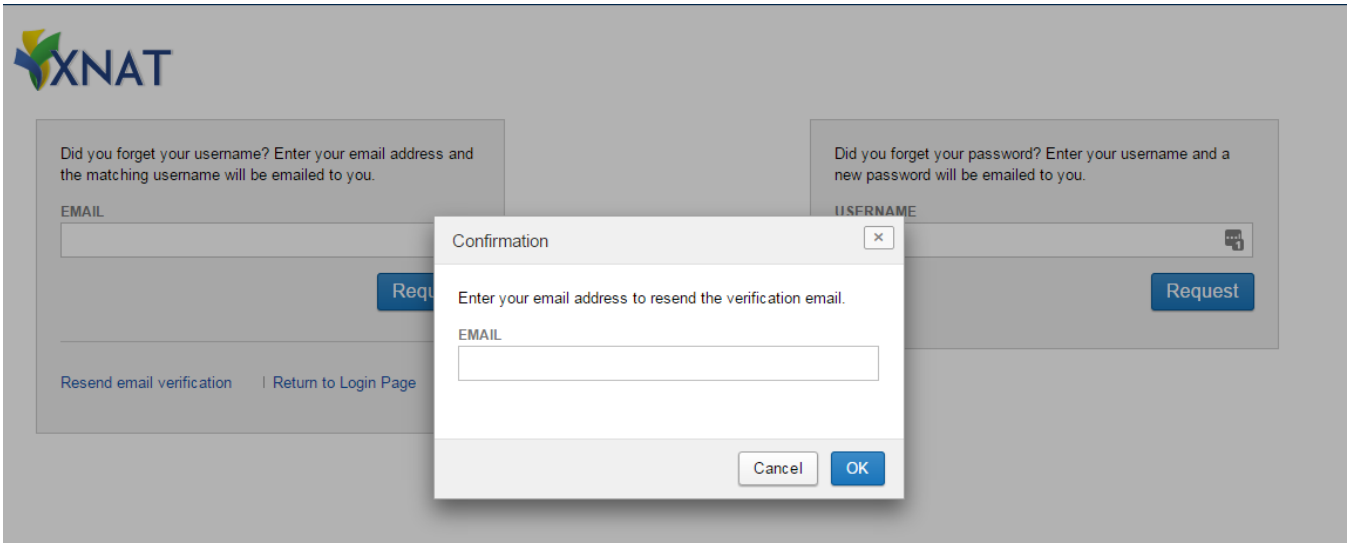
XNAT Administrators can manage all user accounts by navigating to **Administer > Users** in the top navigation.

New in XNAT 1.7.1

This page contains a user listing which shows you which users are currently active in the site. You can also disable site access to any user (including yourself, so be cautious) through the Enabled controls in this table.

Verified / Unverified Users

If you require an email verification step during account registration, this will affect the setting of the "Verified" flag on a user's account. An unverified user account cannot log in to the web application, and will need their email to be verified again. Users can do this for themselves by going to the site login page, clicking "Forgot Login or Password?", then clicking "Resend email verification."



Enabled / Disabled Users

Regardless of other user registration security settings, all XNATs allow Administrators to control the "Enabled" or "Disabled" status of a given user account. In this way, Administrators can disable the user account of a person who does not require or should not have access to your web application.

> **User accounts cannot be deleted.** Doing so would invalidate any audit trail entry of that user's activity in your XNAT.

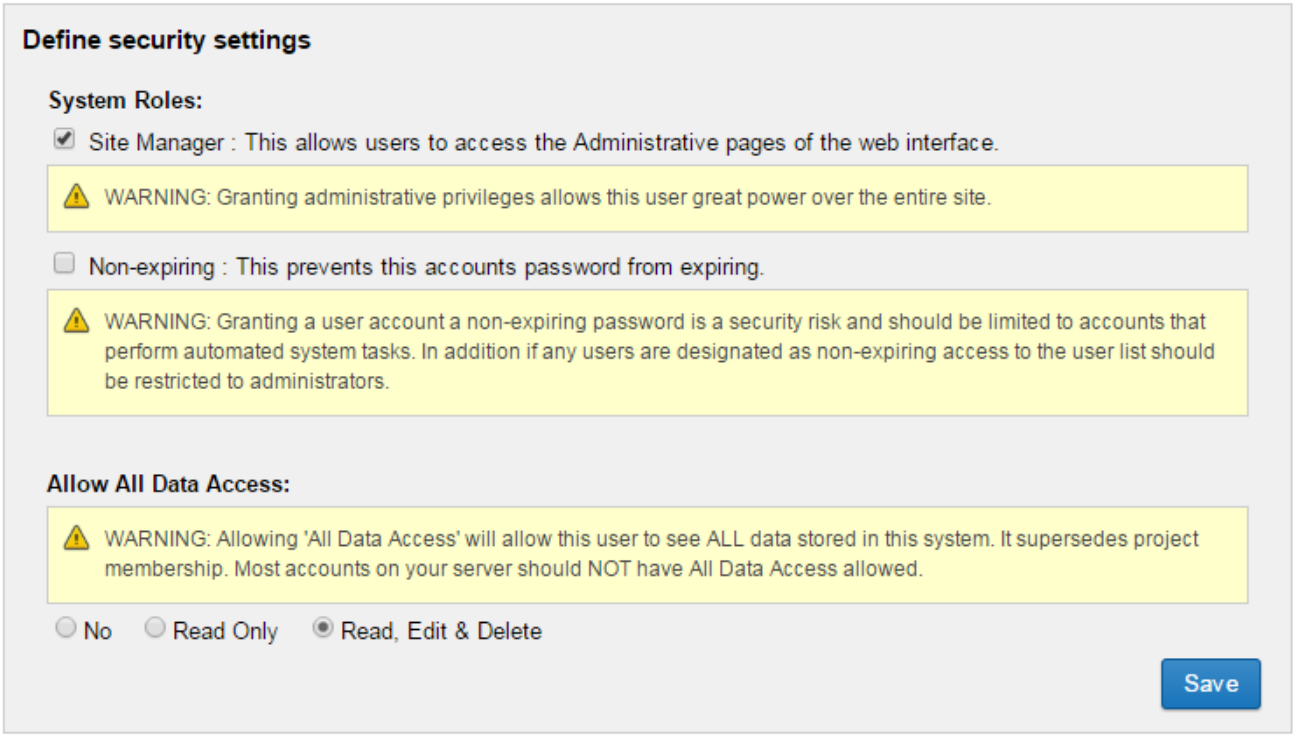
Granting or Revoking Project Access to Users

Clicking on an individual user id in the user table will open a modal window that allows you to edit the user account information. In addition to setting enabled and verified settings, you can also add or remove access to existing projects. As an XNAT Administrator, you can manage access to projects whether or not you have been explicitly added to those projects yourself.

Granting Administrative Privileges to Users

In addition to project access, XNAT's user management tools also give you the opportunity to apply site-wide roles. Chief among those are administrative privileges. There are two levels of administrative privilege that a user account can have, by default.

- **Site Manager** - This setting allows the user account to access the Administrative pages of the web interface. By proxy, any account with this privilege can grant itself or others total data access. Please apply this role judiciously.
- **Non-Expiring** - This setting circumvents the password expiration security setting in **XNAT Security Settings**.
- **Allow All Data Access** - This setting allows the user account to see ALL data stored in this system. It supersedes project membership. Most accounts on your server should NOT have All Data Access allowed.



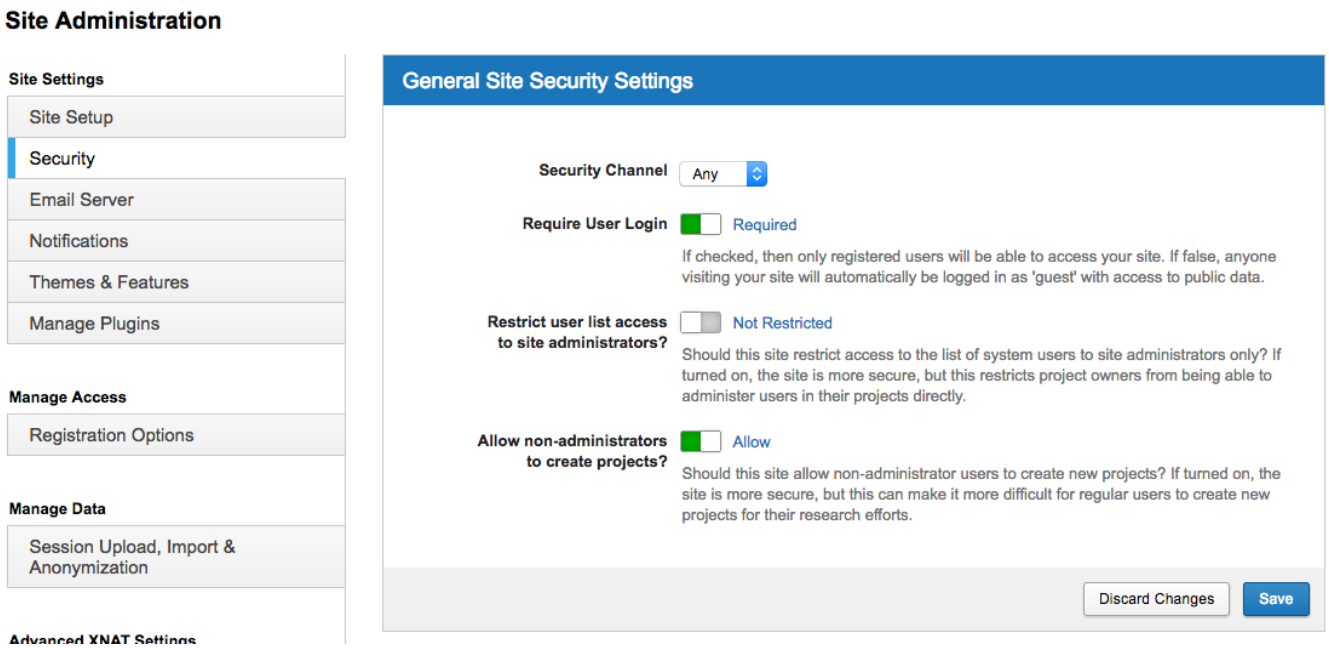
All Data Access

As of XNAT 1.7.4.1, All Data Access is not being properly checked by new XNAT permissions checks (such as permissions checks in XAPI REST calls). If you want these users to be able to use newer REST calls, you must make them a Site Manager (a.k.a. an admin) as well. A refactor of the permissions code is underway and this may change in future versions of XNAT.

Allowing Guest Access

By default, user login is required to view any data in your XNAT application. However, you can allow guest access in XNAT's security settings. Go to the **Se curity** tab and set **Require User Login** to false, or "Not Required."

With this setting disabled, any visitor to your web application will be able to view and download any data that appears in public projects. **See: Setting Project Access to Public, Restricted, or Private**.



Other security settings in this panel also affect user access, from password security to session length and user lockout after a certain period of inactivity. See: **XNAT Security Settings in the Admin UI.**

Working With User Sessions

Login Credential Security and Authentication

Lots of XNAT installations use scripts, batch files, cron jobs, and other command line-based tools to automate or batch data operations. This works well with XNAT's REST API, but also introduces a risk of exposing login names and passwords on command invokation. To mitigate this risk, XNAT provides the alias token service, which provides a set of temporary login credentials suitable for processing a single task.

Creating a new alias token requires valid login credentials to initialize a session from which the alias token can be created. Care should be taken to protect the credentials at that point. XNAT launches pipelines with alias tokens for credentials, so exposure of credentials isn't a concern in that context. You can also reuse an existing valid JSESSIONID (taken from a browser with an active XNAT session, for example) for the command line. Lastly, you can call these REST URLs directly in your browser with an active XNAT session.

```
/data/services/tokens/{OPERATION}
/data/services/tokens/{OPERATION}/user/{USERNAME}
/data/services/tokens/{OPERATION}/{TOKEN}
/data/services/tokens/{OPERATION}/{TOKEN}/{SECRET}
```

Operations include:

- issue
- validate
- invalidate

Viewing and Revoking Active User Sessions

XNAT's new XAPI functions include the ability to view and disable active user sessions in XNAT.

View All Active User Sessions

```
GET - /xapi/users/active
```

View All Active User Sessions For A Given User

```
GET - /xapi/users/active/{USERNAME}
```

Revoke All Active User Sessions For A Given User

```
DELETE - /xapi/users/active/{USERNAME}
```