WorldSpace Assure 1.4
for System Administrators

Quick Reference Guide

Edition: v.1.4

Last Updated: 10/12/2014

Synopsis and Scope: This document covers how to perform the administrative tasks that are available from the user interface of the WorldSpace Assure application itself for those with sufficient privileges. These include using the Admin. Console, setting the Deque Way version and available standards, managing some session settings, and all tasks related to managing users. It does not cover the technical aspects of installation, database setup, configuration, or deployment of the application.

This document online: https://dequeuniversity.com/guide/assure/1.4/system-administration/

Contents

Admin Settings Screen

The Admin Settings screen is used by System Administrators to manage configuration settings pertaining to the Assure application. Deque Administrators use the Admin Settings screen to get to the Admin Console screen to manage multiple organizations and their users, while System Administrators at client sites use it to set the Deque Way version, standards available for selection in test runs, and to manage users for their organization.

In this topic are the following three main procedures:

- Navigating to the admin console
- Setting the Deque Way version
- Setting the available standards

Access: When a user has been granted appropriate security access group role membership for application administration, the **Admin Settings** option will appear on the main horizontal menu bar after successful sign-in.
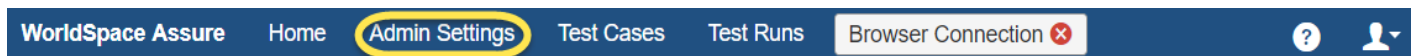
Roles: Organization and User Settings (Administration Console) Access may be granted to one or both of the following types of administrative roles:

- **Deque Admins (System Administrators at Deque)**: Typically, Deque personnel are the only system administrators for WorldSpace Assure. Whether your hosting is in the Deque cloud or a local installation on an on-premises server, designated Deque employees with these types of UI access permissions are always available to provision user accounts and manage organizations and domains. When a user is a member of the Client Security Admin Console role, this is a SuperAdmin who can manage both Organization Realms and Users on behalf of multiple clients. Only designated Deque employees involved in WorldSpace Assure product implementation, application instance configuration and system

administration tasks responsible for Deque's customers are permitted to use the majority of functionality in the Keycloak Admin Console.

- **Client Admins (System Administrators within your organization)**: Under certain circumstances, system administration capabilities are given to delegated individuals at your organization. If this is the case, there are areas of the WorldSpace Assure user interface that are dedicated to system administration tasks. Designated individuals employed by Deque's client organizations may be permitted, at the client's request, to use the Admin Console to adjust things such as the Session Idle Timeout for the organization.

Help: We recommend you first contact Deque Technical Support (Help Desk) for any concerns or questions you may have regarding WorldSpace Assure system administration tasks using any of the following ways most convenient to you:

- **Contact Us page**: Contact Deque Today form
- **Product/Service Support Form**: Support Email Contact form
- **Email Address**: support@deque.com
- **Telephone Number**: 877-225-3932
- **Service Hours**: 9 a.m. to 5 p.m. EST
- **Response Time**: Within 1 (one) working day of receiving your email

Overview

Administration of the WorldSpace Assure software application system includes the ability to manage:

- Organizations within the system
- Their associated domains
- Administrator user accounts
- Standard end user accounts

These types of of administration tasks can all be accomplished from within the user interface via the **Admin Settings** screen and **Keycloak Admin Console** screens that are initially accessed via the main horizontal menu for those with appropriate access permissions.

1. **Go to admin console** button: Causes the Assure Keycloak realm to appear, which allows you to:
   - Adjust the session timeout
   - Manage users for the organization – add, delete, edit, impersonate, unlock, disable, enable (Deque personnel only)

1. **Deque Way version** drop-down list menu: Required. The release version of the checkpoint content displayed on the individual checkpoint test screens when using as a guide during manual accessibility testing.
2. **Available standards** checkbox group: Populates the Standard drop-down menu on the Details (Step 1 tab) of the New Test Case screen with a list of available standards from which to select when creating a new test case.
3. **Save settings** button: Saves to the database your selections made in both the Deque Way version and Available standards fields above.

Navigating to the admin console

Users and other organization settings are managed in the Deque admin console, which is accessed via the following button on the Admin Settings screen:
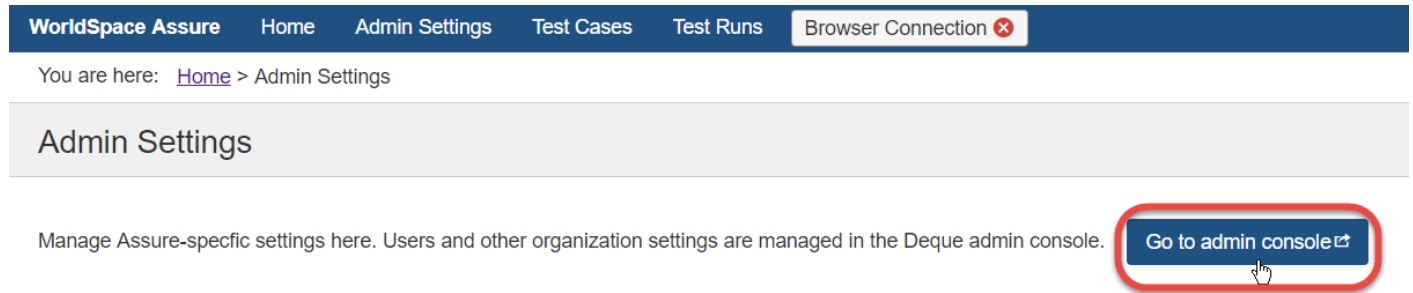
For detailed information about the available system, organization, and user administration options in the Admin Console, refer to the following subtopics:

- Managing Session Settings
- Managing User Settings

Setting the Deque Way version

Since test cases and test runs can span a long period of time, you may want to preserve the version of the Deque Way checkpoint tests for manual testing guidance until complete. So, even though a newer version becomes available, a System Administrator can set the default Deque Way for the system, which will apply to all new test cases created.

To set the Deque Way version:

1. To the right of the **Deque Way version** field, click the **down arrow**.

   The menu expands downward to display available list option version numbers.

2. Click on the desired **version number** (for example, 1.4.4) option in the list to highlight and select it.

The drop-down menu collapses (closes) and the field becomes populated with your selection.

3. Click the **Save settings** button.

A confirmation message appears at the top, right of the Admin Settings screen to indicate successful completion of the setting change(s):
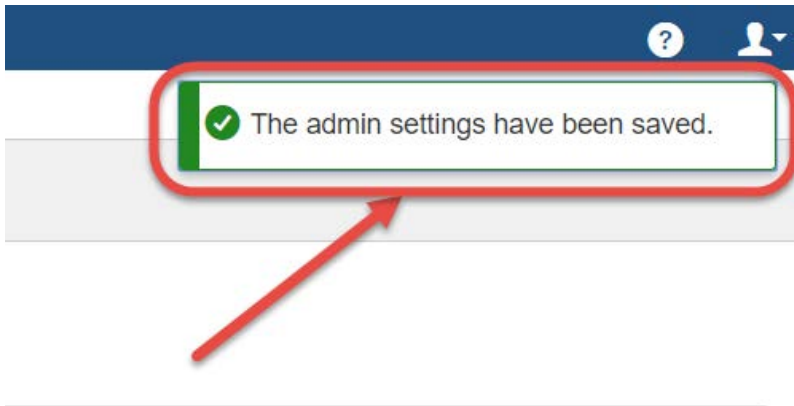
Setting the available standards

The available standard(s) admin setting populates the Standard drop-down menu on the Details (Step 1 tab) of the New Test Case screen with a list of available standards from which to select when creating a new test case. When you want to restrict which rule sets are available to test against for Assure users (for example, if you only wanted to test for Section 508 compliance), follow this procedure.

To set the Available standards:

1. On the Admin Settings screen, scroll down to the right of the **Available standards** field.
2. Click the desired **checkbox** (for example, Section 508) option(s) in the list to check and select.
3. Click the **Save settings** button.
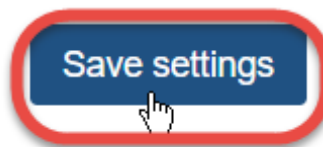
A confirmation message appears at the top, right of the Admin Settings screen to indicate successful completion of the setting change(s):
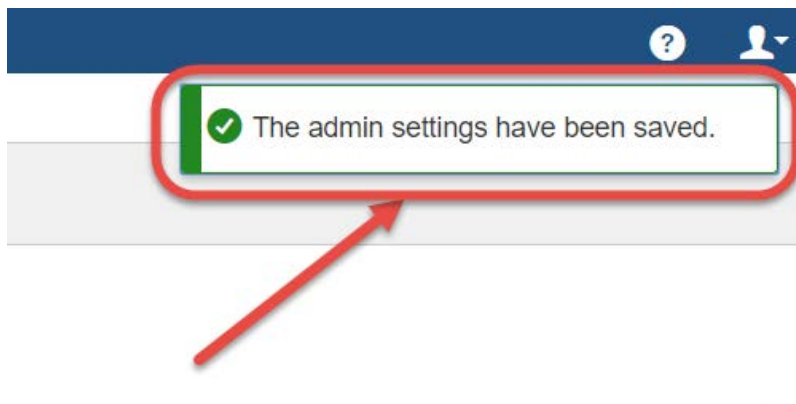
The list of available items is restricted accordingly in the Standard drop-down menu list on the Details tab of the New Test Case screen.
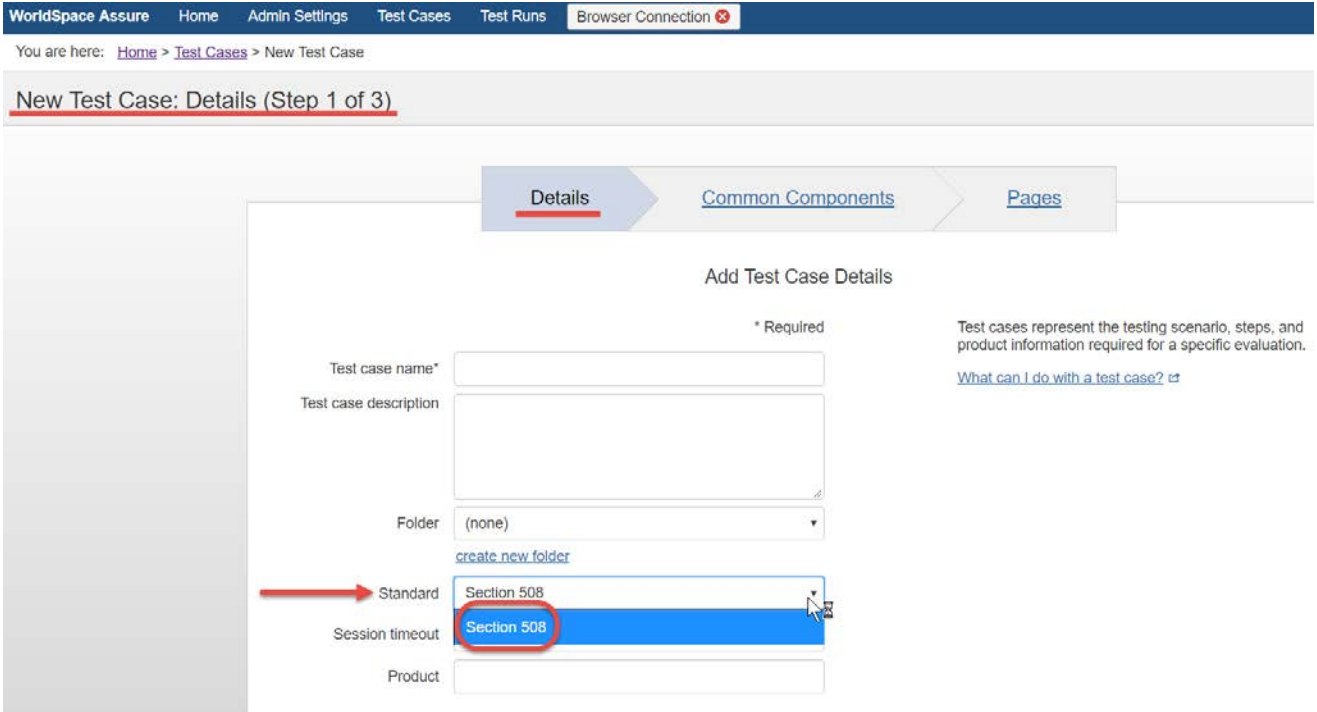
Subtopics:

- Managing Session Settings
- Managing User Settings

Managing Session Settings

WorldSpace Assure uses Keycloak as a single sign-on provider to manage user accounts and authentication. Deque Admins will handle the configuration of and connection with Keycloak for your organization's instance of Assure.

Realm Name note: Upon first accessing the Keycloak Admin Console, you will see on the General tab of the Realm Settings page a **Name** field that displays the realm name for your organization. Since Assure takes the first subdomain of a request URL as the realm of the acting user's organization, this means that given a URL of "http://foo.wsassure.com", the user will have to authenticate against the "foo" realm in Keycloak. Therefore, it is important that you do not change this name field value!
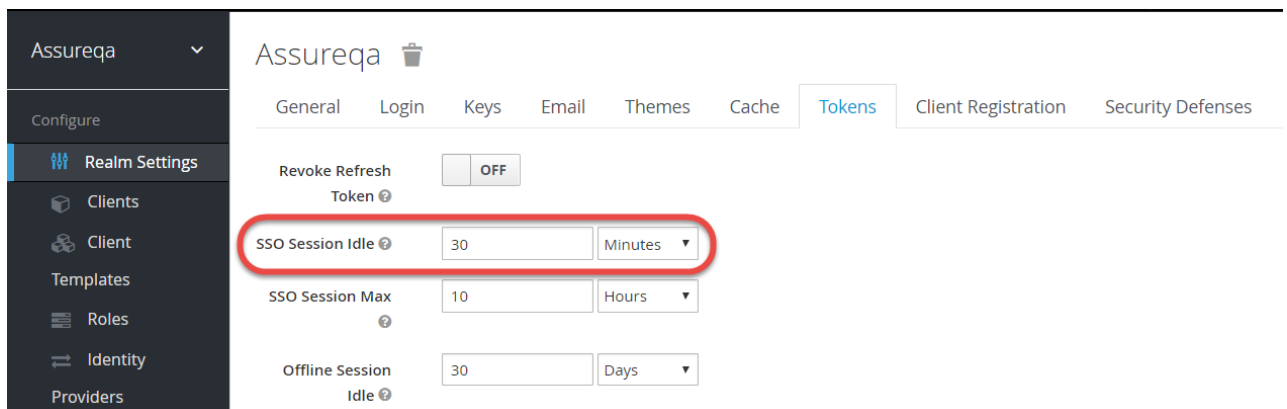
Changing the SSO Session Idle

One thing you are able to change is the SSO Session Idle setting. Although you have the capability to make changes elsewhere within the Tokens tab, we recommend you do not change any of the other available settings. Leaving a user's application session established for an indefinite period of time increases the risk of session hijacking. The SSO Session Idle value is the time a session is allowed to be idle before it expires. Tokens and browser sessions are invalidated when a session is expired.

Warning: Every 10 minutes, Assure asks Keycloak for the timeout for your organization's realm. It is for this reason that we recommend you only change the session timeout during non-business hours or at least during non-peak times to prevent potential loss of user data due to timeout without warning.

To change the SSO Session Idle:

1. Ensure the **Realm Settings** option is selected under the Configure heading in the left sidebar menu.
2. Select the **Tokens** tab in the right pane.
3. On the Tokens panel, in the **SSO Session Idle** field, adjust the value numeric entry field and time unit drop-down menu settings as desired.

4. At the bottom of the panel, cick the **Save** button.
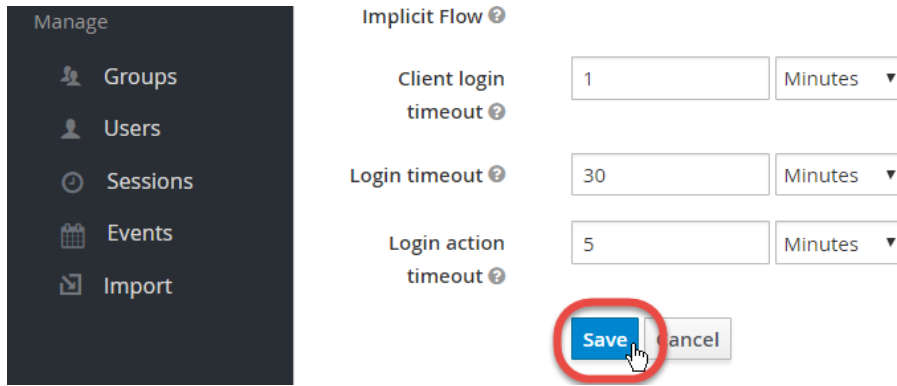
A system response message appears to confirm the changes you made were saved to the realm.
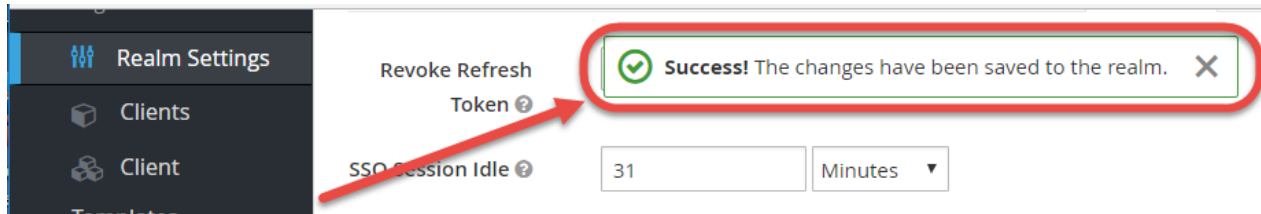
Managing User Settings

Follow the procedures on this page to manage users within your organization. When you have a large organization and do not want to have Deque configure Assure for automated user federation (for example, via LDAP or Active Directory), you can elect to have a System Administrator staff member at your organization manage Assure users via the following procedures.

In this topic:

- Accessing the Manage Users functionality
- Adding a user
- Deleting a user
- Editing a user
- Impersonating a user
- Unlocking a user
- Disabling a user
- Enabling a user

Accessing the Manage Users functionality

1. On the Admin Settings screen of Assure, click the **Go to admin console** button.
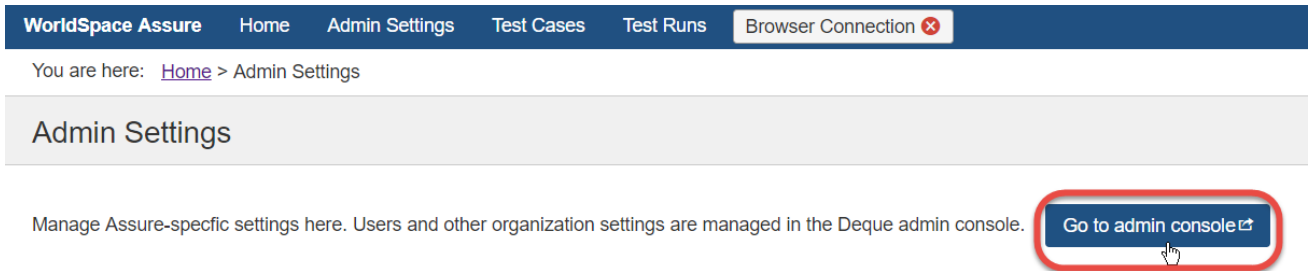
2. On the left sidebar menu of the Keycloak Admin Console screen, under the **Manage** menu heading, select the **Users** item.
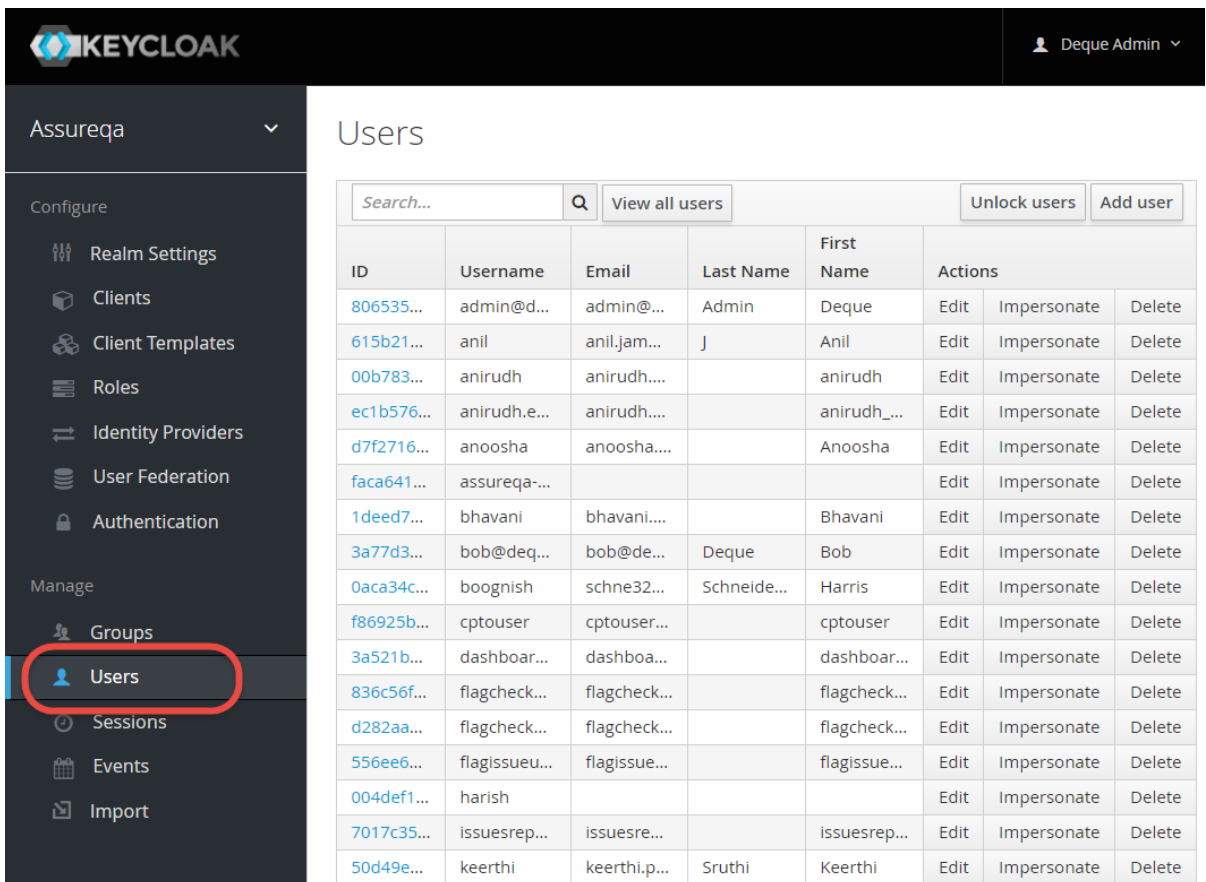
The Users page is displayed on the right pane.

Adding a user

To add a user:

1. In the Manage section of the left sidebar menu of the Keycloack Admin Console, click the **Users** link.

   The Users screen appears, displaying a Search... field and three action command buttons (View all users, Unlock users, and Add user).

2. Click the **Add user** button at the top, right of the Users screen.
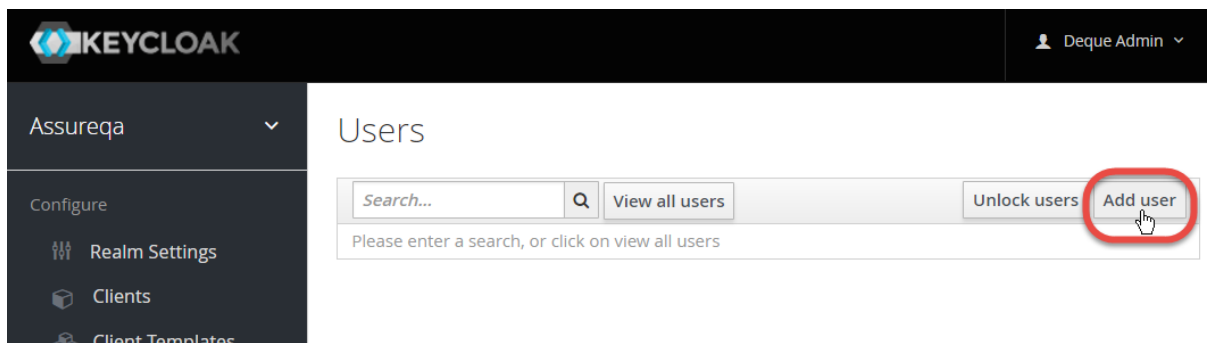
   The Add user screen displays with an editable form.

3. Populate at a minimum the fields marked required, then click the **Save** button.

A message appears to confirm the successful addition of a new user record.

Deleting a user

Warning: After deleting a user, when any Test Runs previously assigned to that user are accessed, the name is replaced with `(deleted user)`, which may not be as desirable to you as simply disabling them, which preserves the name. In the case of multiple deleted users around the same time frame, this could prove to be confusing for organizational purposes.

To delete a user:

1. In the Manage section of the left sidebar menu of the Keycloack Admin Console, click the **Users** link.

   The Users screen appears, displaying a Search... field and three action command buttons (View all users, Unlock users, and Add user).

2. To the right of the search field at top, left of the screen, click the **View all users** button.

   The Users screen is refreshed to display a paginated table with a row for each user in the system.

3. On the Users screen of the Keycloak Admin Console, click the **Delete** button in the Actions column within the row of the user you want to delete.

A confirmation prompt appears in a popup window.

4. On the Delete User dialog box, click the red **Delete** button again to confirm.

Digital equality. It's our mission, our vision, and our passion.
We believe that websites, mobile applications, and digital content should be accessible to people with disabilities - and we're passionate about creating technology that can make that vision a reality.
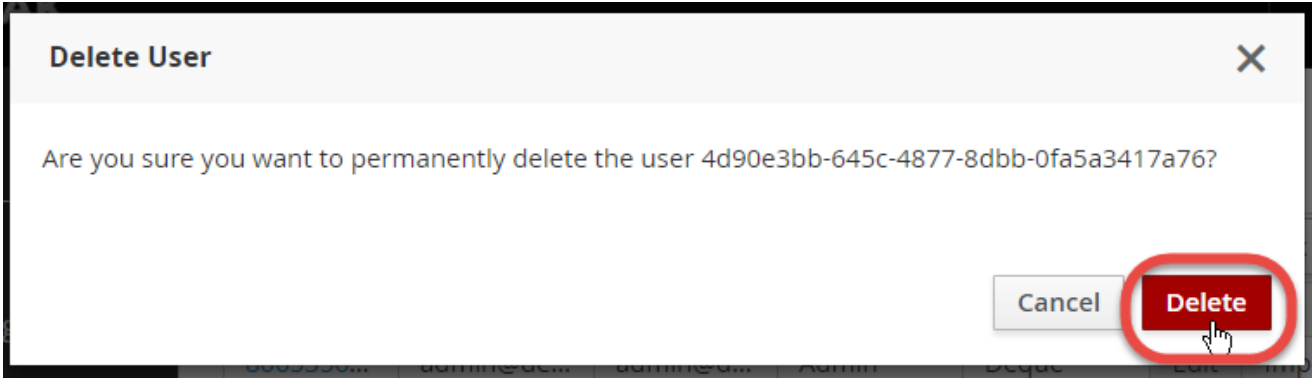
A system response message appears at the top, center of the screen to indicate successful deletion.
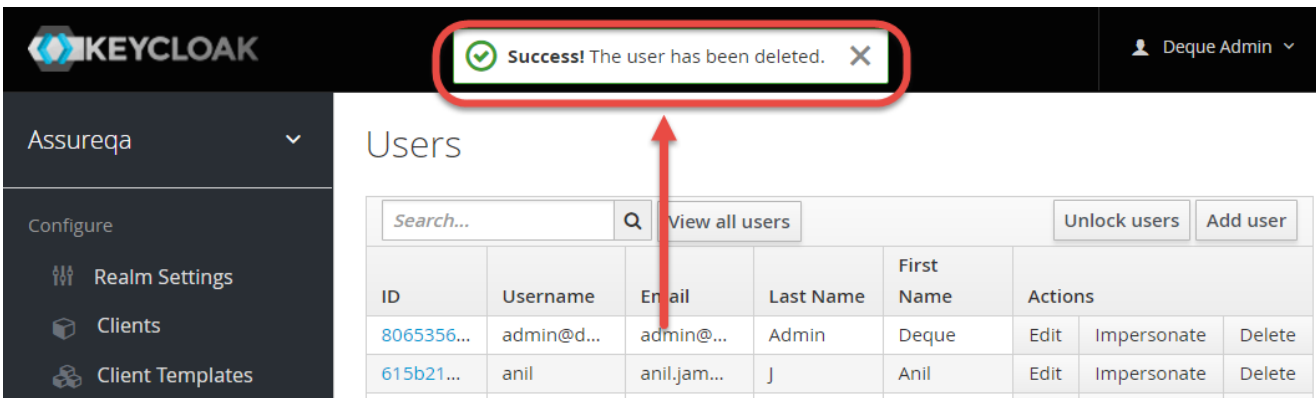
The corresponding row is removed from the Users screen table.

Note: The name is replaced with `(deleted user)` in the application anywhere the user name appears (for example, in the Assigned User columnn on the Test Runs screen for a test run that had previously been assigned to that user).

Editing a user

To edit a user:

1. In the Manage section of the left sidebar menu of the Keycloack Admin Console, click the **Users** link.

   The Users screen appears, displaying a Search... field and three action command buttons (View all users, Unlock users, and Add user).

2. To the right of the search field at top, left of the screen, click the **View all users** button.

   The Users screen is refreshed to display a paginated table with a row for each user in the system.

3. Within the desired user row of the Users screen table, click the **Edit** button in the Actions column.

The username screen appears with editable fields.

4. Make changes to the text entry field values as necessary (for example, to change the Email address).

   Note: As soon as you click the cursor within an editable field to begin to make an edit to an existing value, the Save button at the bottom of the screen changes from grey to blue as an indicator that unsaved changes have been made to the form.

5. Click the **Save** button.
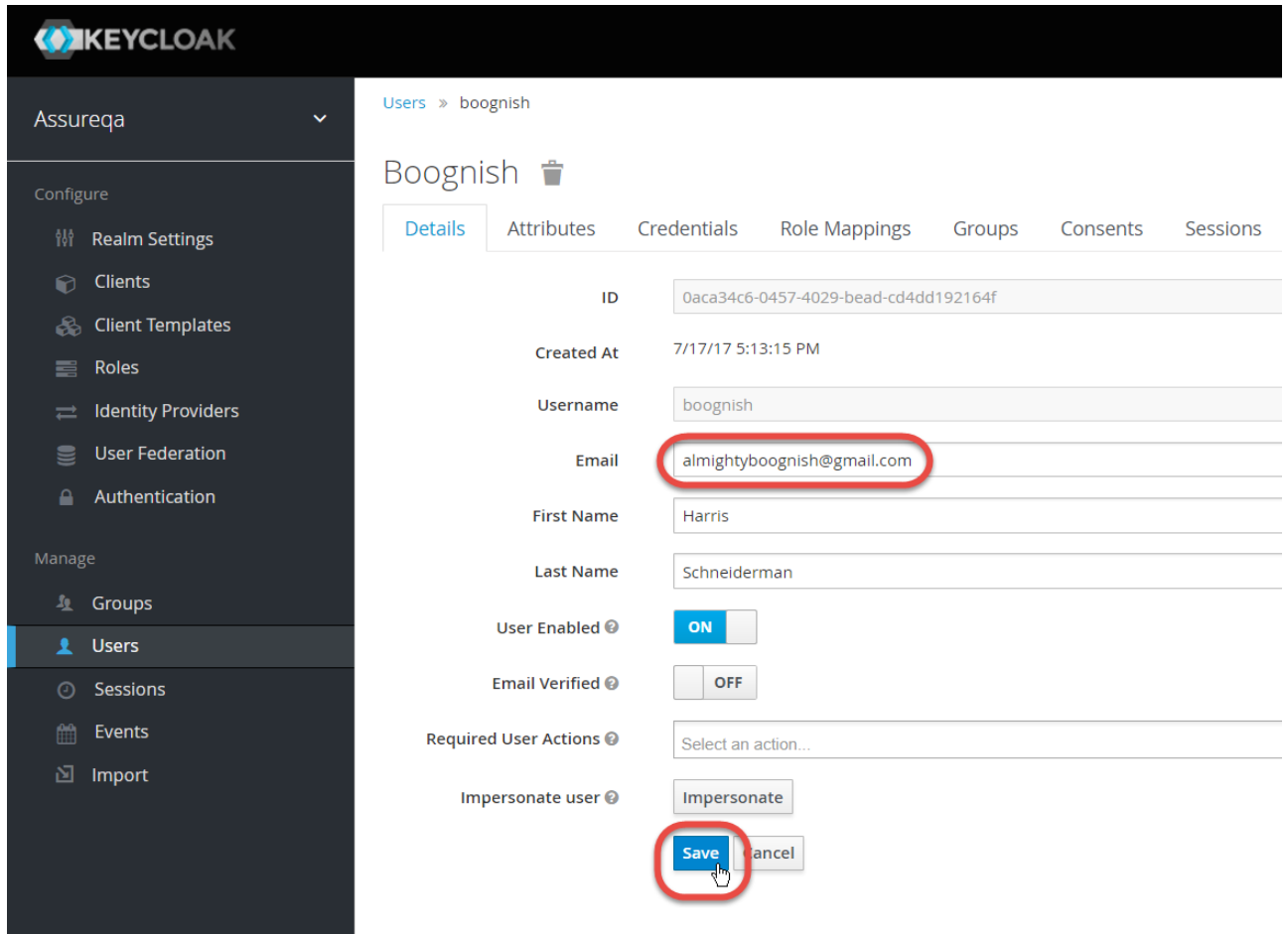
The system displays a success message at the top, center of the screen.
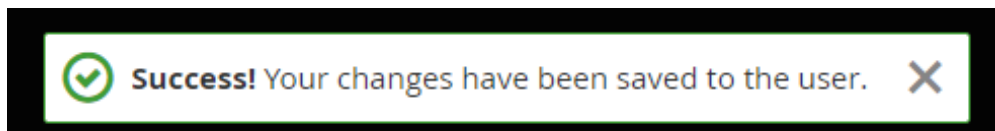
Impersonating a user
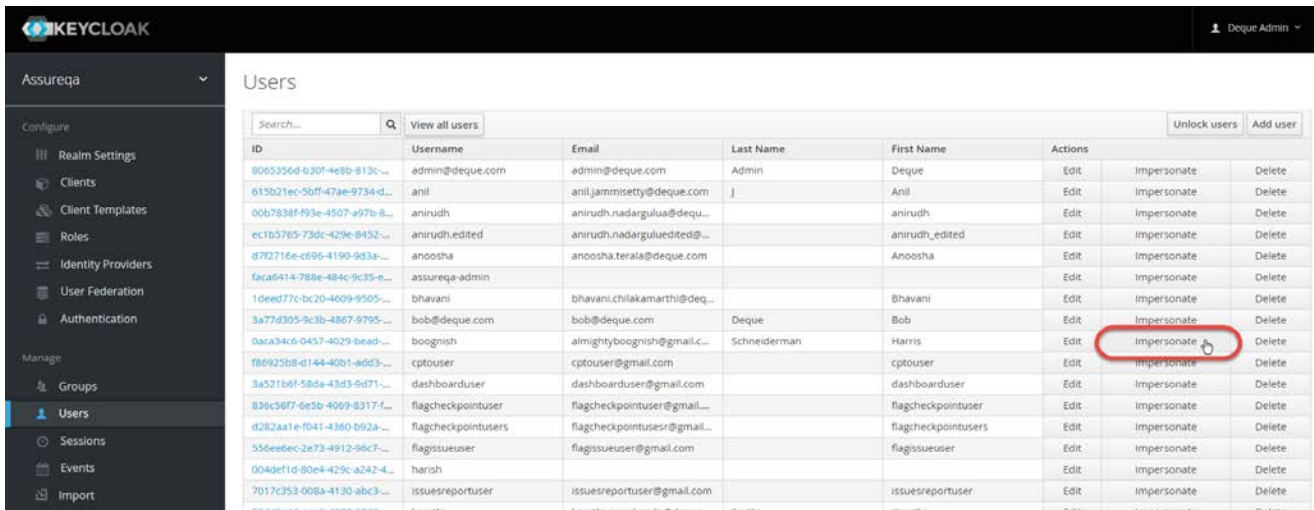
To impersonate a user:

1. In the Manage section of the left sidebar menu of the Keycloack Admin Console, click the **Users** link.

   The Users screen appears, displaying a Search... field and three action command buttons (View all users, Unlock users, and Add user).

2. To the right of the search field at top, left of the screen, click the **View all users** button.

   The Users screen is refreshed to display a paginated table with a row for each user in the system.

3. Within the row of the user you want to impersonate, click the **Impersonate** button under the Actions column.

You are now signed in to the application as the person you are impersonating.
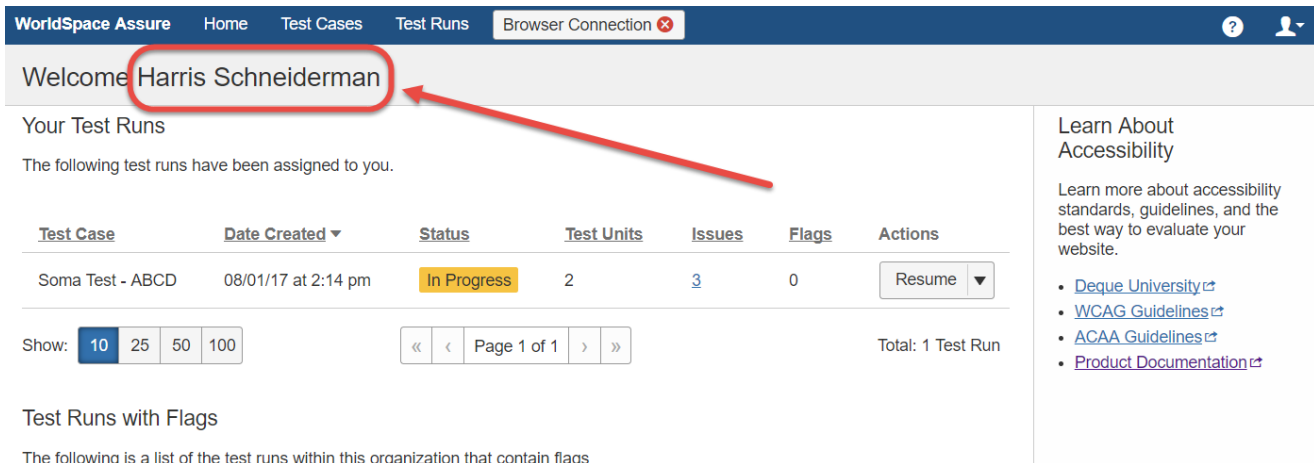
Unlocking a user

To unlock a user:

1. In the Manage section of the left sidebar menu of the Keycloack Admin Console, click the **Users** link.

    The Users screen appears, displaying a Search... field and three action command buttons (View all users, Unlock users, and Add user).

2. Click the **Unlock users** button at the top, right of the Users screen.

A message appears at the top, center of the screen with a green checkmark icon that reads, 'Success! Any temporarily locked users are now unlocked.'

Disabling a user

Disable a user when you want to prevent them from being able to sign in to the Assure application, but want to preserve their user account in the system.

Warning: Disabling a user has the advantage of preserving the user name in the user interface so that you will still be able to easily identify any test runs assigned to them. Only System Administrators are permitted to disable a user in an organization's realm. For related information, see Deleting a user.
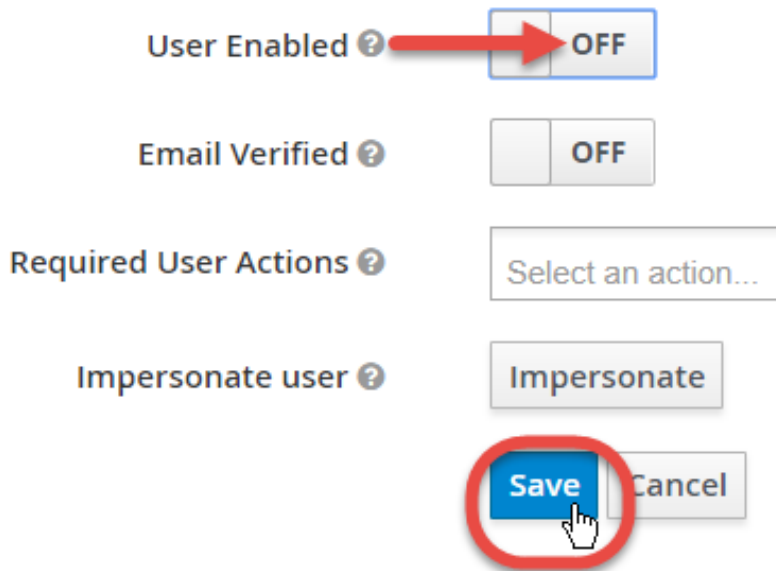
To disable a user:

1. On the Details panel, click to the right of the **User Enabled** field (which is currently displaying 'ON').

   The button toggles to display the 'OFF' position.

2. Ensure 'OFF' is displayed in the toggle button label to the right of the User Enabled field, then click the **Save** button at the bottom of the Details panel.

A message appears at the top to indicate a successful change.

The user will no longer be able to successfully sign in to Assure.

Enabling a user

When a user exists in the system, but has previously been disabled (when the User Enabled field is set to OFF), you can follow this process to make it possible for them to be able to sign in to the Assure application again.
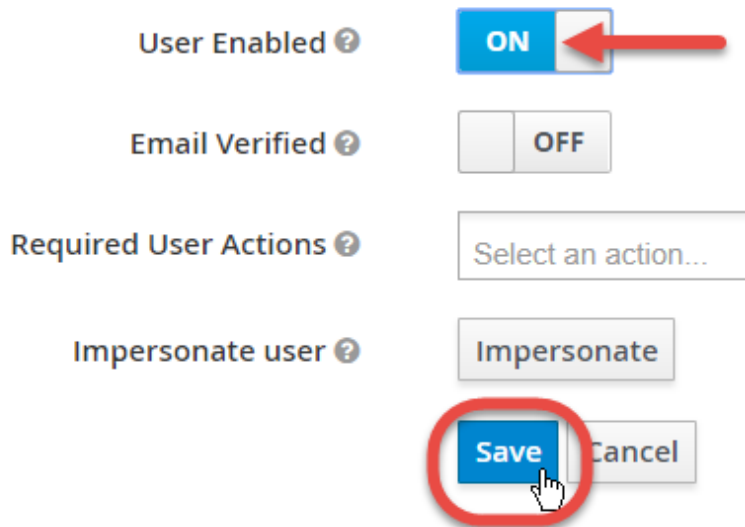
To enable a user:

1. On the Users screen, click the **Edit** button in the Actions column within the row of the user you want to enable.

   For complete details, see Editing a user.

2. On the Details panel, to the right of the **User Enabled** field, click to the left of the OFF toggle slider to switch it to display 'ON'.
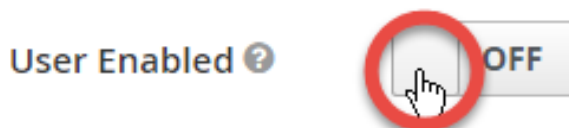
3. Click the **Save** button at the bottom of the panel.

The user will now be able to sign in to the Assure application.