hMetrix Role Manager – POC User Guide

Sep 26, 2023

hMetrix

hMetrix

Table of Contents

hMetrix

1 Overview

This document is a user guide intended for organizational Points of Contact (POCs) using the hMetrix Role Manager to administer users of CRISP data services. It is intended for internal administrative use and reference.

Any questions or recommendations for improvement to this documentation should be directed to the hMetrix Identity & Access Management Team at crisp-iamteam@hmetrix.com.

2 Background

Securely controlling and granting access to protected resources consists of two steps: authentication and authorization.

Authentication is a mechanism for providing proof that a user is who they say they are – typically via a username, password, and multi-factor authentication. In the CRISP application ecosystem, authentication is handled via the HIE Portal Identity Provider (IDP). The HIE Portal is where all account-level management activities take place: user creation, identity verification, password resets, and account recertification. This is done via the HIE Admin Tool. For information on the HIE Admin Tool, see the HIE Admin Tool User Guide.

Authorization takes place after authentication and, now that a user has proven their identity, dictates what data, services, applications, or resources they have permission to access as that individual. The hMetrix Role Manager handles authorization management for all CRISP Reporting Services data and applications, as well as some other ancillary CRISP services. Authorization details can vary by application, from a simple user type designation of 'end user' versus 'administrator' to more nuanced attributes including assigned panel IDs or associated organizational NPIs that correspond to data access relationships. Regardless of the need, such details can be assigned and managed through the hMetrix Role Manager.

The hMetrix Role Manager was developed using a general framework of best practices to accommodate any style of authorization an application or service might require by allowing site administrators to create custom role attributes for each managed service. This same framework allows for efficient, scalable management as more applications, organizations, and users are added to the ecosystem. This user guide is intended to address the standard range of functionality within this framework that organization Points of Contact (POCs) will need to access and understand to provision and manage users at their organization.

2.1 Terminology

2.1.1 Organizations

In the Role Manager, 'organizations' are a mechanism for grouping users according to their affiliation, making it easier to manage roles, permission profiles, and access for those users at scale. While most organizations created in the Role Manager will reflect bodies we traditionally associate as such – e.g., hospitals, group practices, or governmental bodies – the implementation is flexible enough to accommodate any grouping that is useful to CRISP. Technically speaking, an organization is simply a metadata label attached to a user that makes it easy to map bulk operations to all users with that tag.

The most common use for organizations in the Role Manager in its current use is to create and assign default 'Organization Permission Profiles' that are automatically applied to users assigned to that organization, so that common roles do not need to be manually applied to each new user created. This functionality is described in detail under the 'Users' section below.

2.1.2 Applications

Applications are the reports, services, and any other tools whose permissions are managed in the Role Manager. Before users can be assigned roles for and access a new service, the application must first be set up by a super administrator.

2.1.3 Role

A role is an attribute or a collection of attributes that can be used to define access to a resource – be it functionality within an application, an entire application, a dataset, or any combination or parts thereof.

2.1.4 Role Profile

A role profile is a collection of roles that can be applied to an organization or user.

When applied to an organization, users in that organization who have one of the organization's role profile(s) applied will be automatically updated with new permissions when the role profile is updated. This makes it easier to manage and distribute new reports or remove old report access as the resources an organization has access to grows.

3 Accessing the Role Manager

3.1 Granting Role Manager Privileges

To access the Role Manager, an administrative user must first be provided with the correct account permissions. In the CRISP Salesforce instance, the user must have an account in the HIE Portal and be granted the asset corresponding to the 'ReportingRM' product code. Then, in the Role Manager itself, that user needs to be granted the appropriate administrative user role. In the case of POCs, the POC role needs to be provisioned.

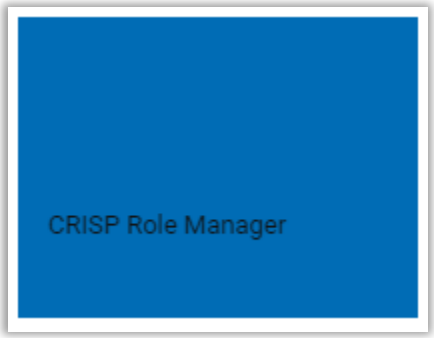
If you feel you should have access to the Role Manager but are not able to view, reach out to your CRISP support team at support@crisphealth.org.

End users of services managed via the Role Manager should not be provisioned with access to the Role Manager, do not need a Salesforce Role Manager asset and will always have a Role Manager user type of End User.

3.2 Launching the Role Manager via the HIE Portal

Once you have the correct permissions, you can access the Role Manager via the HIE Portal in the same fashion as any other integrated service provider, as follows:

1. Sign into the HIE Portal for the appropriate environment you wish to administer using a modern web browser at https://portal.crisphealth.org.
2. Click the "*CRISP Role Manager*" tile (shown at right).
3. The Role Manager will open in a new tab of the browser.



4 Users

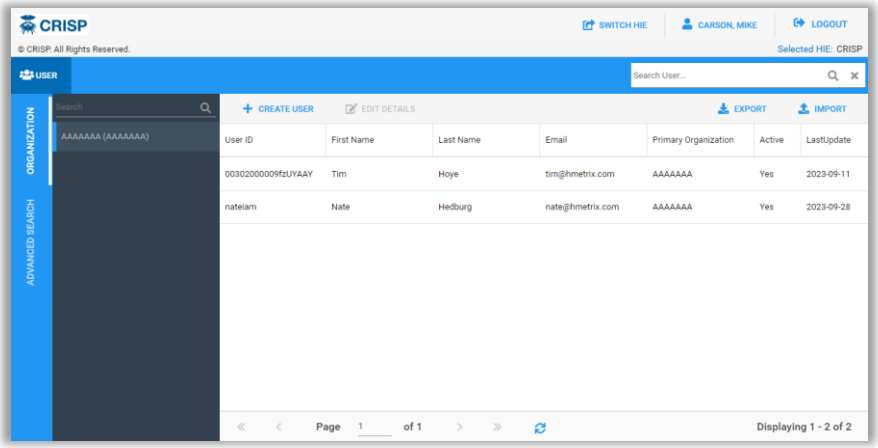
The user section of the site allows for the assignment of roles, role profiles, and/or organization role profiles to a user or group of users. This is where the bulk of POCs workflows will take place.

Key Features:

1. Searching for users and organizations
2. Creating, editing, activating and deactivating users
3. Exporting and Importing Users

4.1 Overview of the User Screen

The User Screen is where the bulk of day-to-day work in the Role Manager will take place and is shown below. The User screen is visible and accessible to all Role Manager administrative user types.

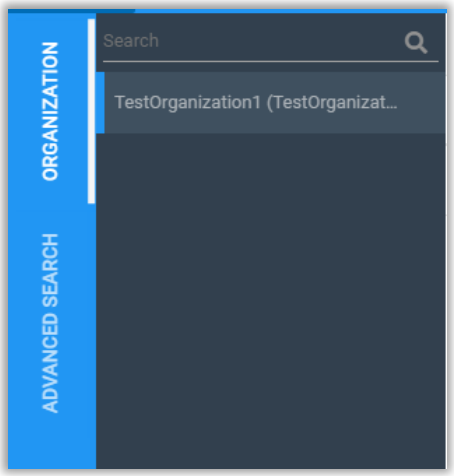


4.2 Left Menu Bar (Organization View and Advanced Search View)

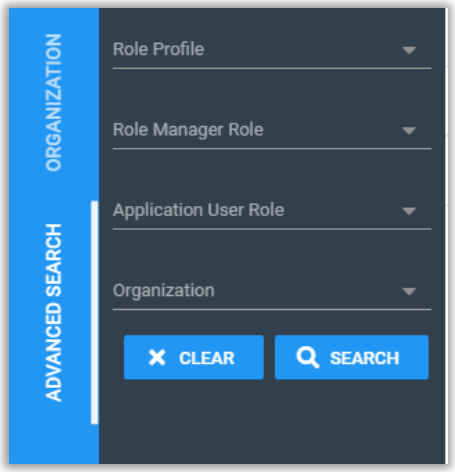
Along the left-hand side of the screen is a vertical navigation bar that contains two panes: Organization View and Advanced Search, as described below.

4.2.1 Organization View

The organization view shows the organizations in role manager that the user has permissions to view. Users can search for an organization using the search bar to the right of the menu.



4.2.2 Advanced Search



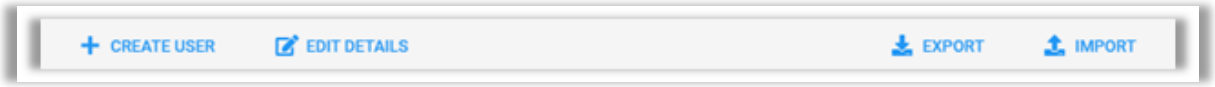
Advanced search gives users the ability to search for users whom they have permission to view, that match the search criteria. Any combination of fields can be searched on. Search fields include:

1. Role Profile
2. Role Manager Role
3. Application User Role
4. Organization

4.3 Central Control Bar

The central control bar includes the following functions:

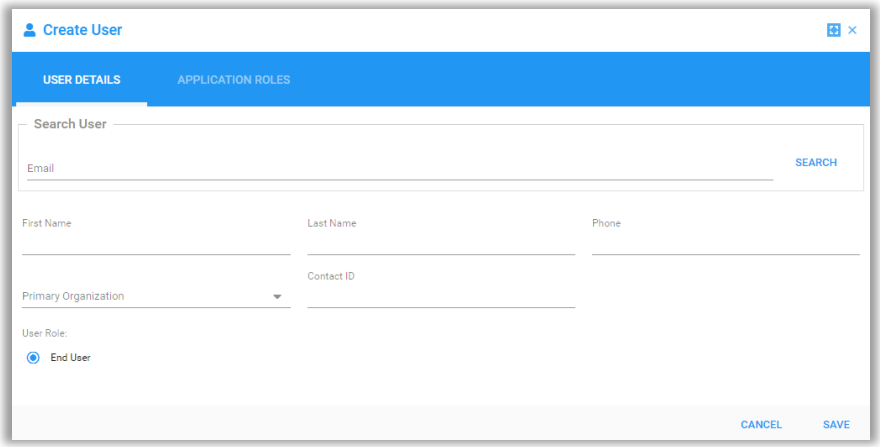
1. **Create User:** Create a new rule, assign role manager permissions, and assign roles, role profiles, or organization role profiles.
2. **Edit Details:** Edit user details, role manager permissions, and assign roles, role profiles, or organization role profiles.
3. **Export:** Exports the users currently shown in the Users table to Excel.
4. **Import:** Opens the User Import interface and allows the user to bulk import new users or bulk modify existing users.



4.3.1 Create User

To create a user in the Role Manager, they must first have an HIE Portal account. You can verify this in the Role Manager during the user setup process as follows:

1. Click "*Create User*".
2. Enter the email address of the user you want to create and press "*Search.*"



3. First Name, Last Name, Phone, and Contact ID should auto populate. If the user is not present in the HIE Portal, a notification will appear instructing you to first set up an account for that user in the HIE Admin Tool, then return to the Role Manager for further provisioning.
4. Select the primary organization of the user.
5. Click the "*Save*" button.

4.3.2 Add Roles

To add roles to a user:

1. Click the "*Application Roles*" button.
2. Select whether you want to add a role, role profile, or organization (role profile).
3. Click the "*Save*" button.

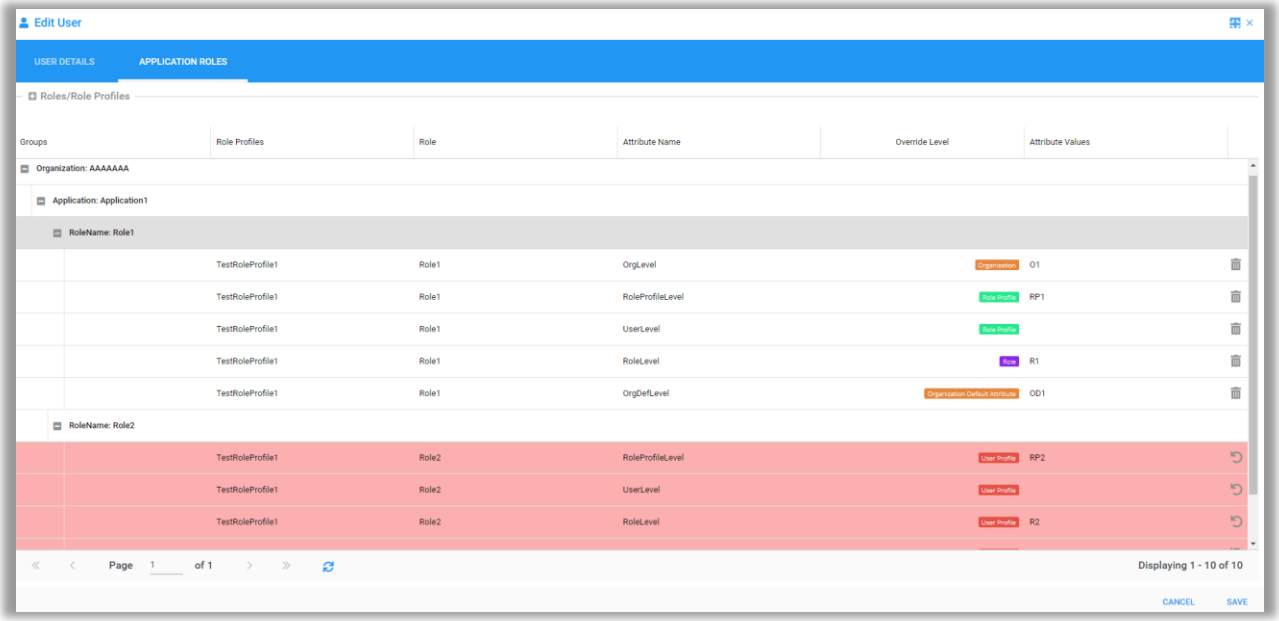
4.3.3 Disable/Enable A Role Within Role Profile / Organization Role Profile for A User

To disable a specific role in a role profile or organization role profile for a given user:

1. Click the "*Application Roles*" button.
2. Expand the Organization and Application sections to show the roles.
3. Click the *"Trash can"* icon.
4. Click *"Remove Role".*
5. This will cause the role background to become red.

To enable a role in a role profile or organization role profile for a user:

1. Click the "*Application Roles*" button.
2. Expand the Organization and Application sections to show the roles.
3. Click the *"Reload"* icon.
4. Click "*Yes"* in the confirmation popup.
5. Press *"Save".*



4.3.4 Edit User

To edit a user's information:

1. Click the user you want to edit.
2. Click the "*Edit Details*" button.
3. Change whatever information you need to change.
4. Click the "*Save*" button.

4.3.5 Export Users

The list of currently displayed users can be exported to a Microsoft Excel file. This list includes users' roles and role attribute values. To do so,

1. Click the "*Export*" button on the right-hand side of the central control bar.
2. An Excel file will start downloading. Depending on the number of users selected to export, this typically takes anywhere from a second to a few minutes (if exporting very large sets of users).

4.3.6 Import Users

Large numbers of users can be added to the Role Manager quickly by using the Import functionality. To import a set of users:

1. Click the "*Import*" button on the right-hand side of the central control bar.
2. Click "*Download Template*" button at the top of the Import screen to download the import template (in Excel format).
3. Completely fill out the import template as required, save and close it.
4. Return to the Role Manager Import screen and click the "*Browse*" button.
5. Select the file you just filled out and press ok.
6. Click "*Upload Users*".
7. The list of users will now be displayed below.
8. Click "*Next*" at the bottom of the screen.
9. Assign the role, role profile, or organization role profile that you want to assign to the users. This functions in the same manner as described for individual users under Section 8.4.2 above. All imported users will be assigned the same roles; individual roles can be modified as needed after the import step is complete.
10. Click "*Save Roles*" when finished.
11. You can hit "*Cancel"* at any time to cancel the import operation and discard any changes made.