



Open Range
S O F T W A R E

CTS499 Access Control Overview and Considerations

Last Edited: 01 July 2022

This document discusses the Open Range access control design and provides suggestions for roles that may be useful as starting points to consider.

CONTENTS

Introduction 3

Chapter 1: What is Access Control..... 3

Chapter 2: Access Control Basics 8

Chapter 3: Access Control Reports 14

Introduction

This document discusses the Open Range access control design and provides suggestions for roles that may be useful as starting points to consider.

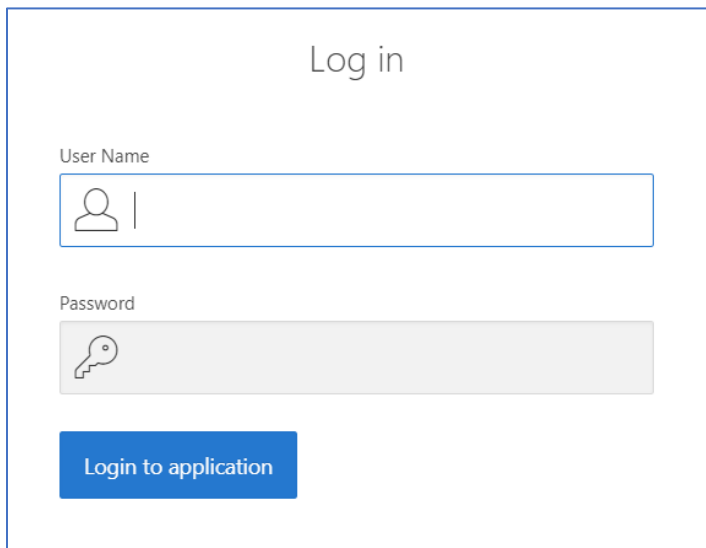
Chapter 1: What is Access Control

In the Open Range software application, there are two key security services that come into effect when a user attempts to access the program:

- Authentication verifies the identity of the user, ensuring that they have a valid user account and password that gives them permission to access the system.
- Authorization controls what each user is allowed to do. Users can only access the programs and features that they have explicitly been given permission to use. In addition, users will only be able to add, view and edit information for the site(s) and company(s) that have been added to their user profile.

Authenticating Users

Each person who will access the Open Range application must authenticate on your internal network with a user identifier that is provided to Open Range either through a logon window, or directly passed through a single sign-on mechanism. The default authentication method is using a standard Logon screen where the username is entered, along with the authentication passcode.



The image shows a login window titled "Log in". It features two input fields: "User Name" with a person icon and "Password" with a key icon. Below the fields is a blue button labeled "Login to application".

If the username and password do not match a valid user account, access to the system will be denied.

Authorizing

Each user account is linked to a security profile in Open Range that outlines exactly what the user is permitted to do.

This information is categorized into three types:

- Feature Access Codes specify exactly which programs and features the user is allowed to use. Each feature code starts with CTS followed by a 3-digit number that represents that feature. Example: CTS499 is the access control by role feature code. Anyone assigned that feature code can add/edit/delete users in the CTS499 screens.
- Company/Site Data information controls which organizations' data the user is able to see and manipulate
- Specialty Flags indicate which special administrative functions the user is permitted to perform, if any.

Feature Access Codes

The initial feature codes list was added to your system when you installed the software, entered a license key and selected the available modules. When you clicked save it build a features list in the CTS478 Menu List which is used for assigning features to users.

CTSADMIN / CTS484: Configuration Option Select /
CTS484: System - Licensing Configuration

Cancel Save and Continue

Core Product License

- Exposure Assessment and Compliance (IH Module)
- Medical Interface (IH Module)
- Electronic Document Retrieval (EDR)
- Job Hazard Analysis (JHA)
- Injury-Illness and Safety Programs
- Chemical Safety-Hazardous Material Inventory and SDS (HMIS)

Specialty Product License (add-on purchase to licensed core product)

- AOP Injury-Illness Reports
- AOP Safety and IH Reports
- AOP JHA Reports
- AOP HMIS Reports
- AOP Occ-Med Reports

Specialty Product License (add-on purchase to licensed core product)

- Occ-Med Questionnaire

The CTS Menu List will show all possible features you can choose to assign to users, or simply leave unassigned until you have a use interest. Example: If you are not implementing a confined space inventory, there is no reason to assign those features for production use. However, any feature you find adds value to your usage of the system should find a home on one more user’s access profile

To see only items in CTS478 that are assignable filter where the APEX ID column is not null, and the Hide column is null.

CTSADMIN / CTS478: Menu List

Reset Descriptions Edit Feature View Item Usage Set Track Flag Report Set Invis

Q Go Rows 100 Actions

Hide is null APEX ID is not null

1 - 100 of 352

	Edit Feature	Feature	Menu Title	Module	Number of Users	View Users	Track Usage	Set Invisible	Display on Public Portal	Hide	APEX ID	APEX Alias
<input type="radio"/>		CTS021	CTS021: Qualification Programs	MED: Support	1		-	-	-		102101	CTSMED
<input type="radio"/>		CTS025	CTS025: Confined Space Entry	IH: Confined Space Program	1		-	-	-		102501	CTSIHPRG
<input type="radio"/>		CTS026	CTS026: Confined Space Daily Count Trends	IH: Confined Space Program	1		-	-	-		102601	CTSMETRIC
<input type="radio"/>		CTS028	CTS028: Confined Space Inventory	IH: Confined Space Program	1		-	-	-		102801	CTSIHPRG
<input type="radio"/>		CTS029	CTS029: Confined Space Reports and Metrics	IH: Confined Space Program	1		-	-	-		102901	CTSMETRIC
<input type="radio"/>		CTS032	CTS032: Confined Space Entry Report	IH: Confined Space Program	1		-	-	-		103201	CTSIHPRG
<input type="radio"/>		CTS034	CTS034: Confined Space Evaluation	IH: Confined Space Program	1		-	-	-		103401	CTSIHPRG
<input type="radio"/>		CTS035	CTS035: Confined Space Inventory Report	IH: Confined Space Program	1		-	-	-		103501	CTSIHPRG
<input type="radio"/>		CTS036	CTS036: Confined Space Work	IH: Confined Space	1		-	-	-		103601	CTSIHPRG

Note: There will be feature codes in CTS478 that do not have an APEX ID assignment, and some that do but are hidden by default. Those feature codes do not need to be assigned to anyone as they will not serve any purpose. However, if you do assign them, it will not cause any issue unless you choose to unhide a hidden code. Hidden features are meant for development testing, feedback and review only, not for production use.

Company/Site Data

Another aspect of security authorization is the Company/Site assignment which controls the data a user can see and manipulate.

If a user has a site and company with write permissions, they will be able to enter data for that site and company through features designed for data entry.

If a user has read only permission, they will be able to run report features for the site and company but will not be able to enter or edit records for that site or company.

A single user may have multiple sites, company and read/write combinations. But for any one site and company they will be assigned either read or write.

When you add a site and company you will add a code (max 7 character), and description (max 100 character). The site and company code fields are most displayed for use on data entry and report filters due to their short length. Descriptions are commonly displayed in report headers.

Note: It is important to note that the Company/Site fields work in combination with the feature access codes. In other words, a user must have BOTH the feature access code and the Company/Site codes to use the feature and view/edit data for the company and site. If you assign a reporting feature code that limits by site and company, but do not assign the user any site and company permission they will not see data.

Specialty Flags

Certain program features are more restrictive than simply having access to a button. For example, deleting someone else’s record. Most commonly if you are not flagged as a manager for an area such as sampling, you will not be able to delete other people’s records.

CTSADMIN / CTS499: Access Control By Role /

CTS499 - Specialty Flags

Role ID	Description
0000002	IT ADMINISTRATOR

Cancel Save and Continue

- HMIS Manager
- IH Manager
- CTS Manager
- IT System Support
- HRA Manager
- IH Equipment Manager
- CTS777 Mgr
- EDR Manager
- Training Manager
- Obsv. Manager
- Obsv. Data Entry for Others
- JHA Manager
- INJL Manager
- CTS778 Mgr
- MI Manager
- CAT Manager
- CAT Data Entry for Others
- Support Doc Manager
- Confined Space Manager
- BE Program Mgr
- Create Public Reports

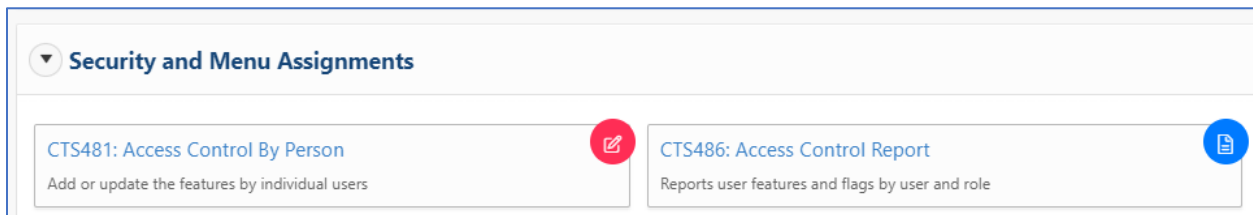
Check All Uncheck All

Note: These flags are not usually needed for everyday users. Site and system administrators will often use these roles for their program areas. For example an IH program lead would tend to have IH Manager flag checked so they could help manager other people’s records for them.

Chapter 2: Access Control Basics

To create a user profile in Open Range you must first choose the method which you will use to manage user profiles. There are two options:

- **CTS481 Access Control By Person** where assignments are to each user independent of other users, or
- **CTS499 Access Control By Role** where assignments are made to an access role, then people are assigned to the role.



Open Range recommends you use CTS499 manage by role if you have more than 2 users as it will make the process of management much easier as people switch to different positions and need different access. Plus, once you have a role set it is very quick to add another user and simply apply the role versus picking individual assignments for each person each time. You can add people to multiple roles, which become additive for the unique features combined.

Regardless of which option you choose to manager user profiles, there is always a user specific profile for the logged-on person.

The examples below will only use CTS499 for demonstration.

Deciding Roles and Feature Assignments

There is no 'right' answer for which role you will want to establish. It is about your team and how you want them to interact with the system, and your data.

The general approach for how many roles to create will often be dictated by how many unique users you have.

If you only have 1 or 2 people and want full access to everything you only need one role and assign that role everything.

More practically, it is likely you have a group of people who do similar things (like IH Sampling), and some people who do very specific things (like confined space evaluations). Also, it is likely you have a few power users who will help manage data for others.

You should always create at least one role to which you assign all features, specialty flags and all sites and at least one person who you will consider your system administrator. This will help ensure all feature options are available for consideration.

When the system was installed, it created an IT Administrator role and assigned all features to it, but if you choose not to keep that role create one that is similar and only assigned to one or a few power users.

From a normal user perspective, It is often beneficial to assign a limited number of features focused on areas of interest to help prevent them from feeling overwhelmed by the large number of feature options in the system.

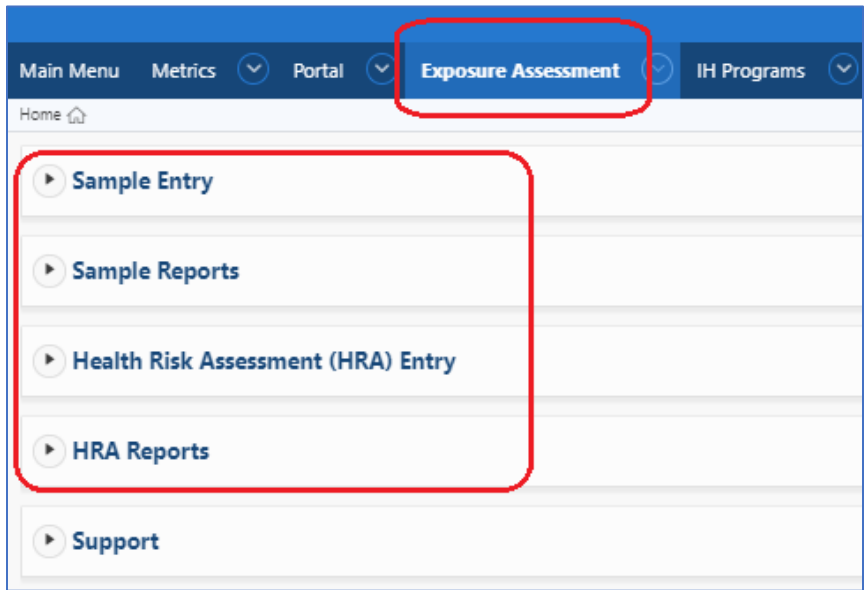
Below are a set of roles you may consider for use and examples for how you might set them up initially.

- IT Administrator
- General IH User
- Site Administrator

This set of roles focuses on Exposure Assessment. If you plan to use other features such as IH Program Inventories, or Equipment Tracking etc.. you will want to consider if those assignments are part of a general role or if those assignments need a role of their own. You can have as many roles as makes sense for your needs. People are added to roles and when applied, their profile is built in an additive fashion so they will get the maximum rights of all the roles they are on combined.

Below is an example for how you might describe and assign features

Functional Role	Description
<p>General IH User <i>(note – if you have multiple sites and want the general user to have different sites you can create a general IH user role – and then a site specific role where you add the sites. Add people as appropriate to both roles. The roles assignments are additive.</i></p>	<p>Person who will enter and report sampling and health risk assessment information. Note: This role will not have any specialty flags (i.e. no CTS or IH manager flags)</p>



General IH User Feature Assignments		
Menu	Region	Minimum Key Features
Exposure Assessment	Sample Entry Region	CTS041, CTS047, CTS050, CTS052, CTS343, CTS344, CTS345
Exposure Assessment	Sample Report Region	CTS056, CTS064, CTS121, CTS122, CTS153, CTS560
Exposure Assessment	Health Risk Assessment (HRA) Entry	CTS068, CTS081, CTS084, CTS094, CTS108, CTS116;, CTS124, CTS155
Exposure Assessment	HRA Reports	CTS107, CTS118, CTS656, CTS669
Exposure Assessment	Support	CTS080

Functional Role	Description
<p>Site Administrator</p> <p><i>(note – if you have multiple sites and want the administrators to have different sites you can create a general admin role – and then a site-specific role where you add the sites. Add people as appropriate to both roles.</i></p>	<p>This person will be assigned to the General User Role, or have all features duplicated to this role.</p> <p>Additionally, this person-role will have the IH Manager specialty flag checked and the Create Public Report flag checked.</p>

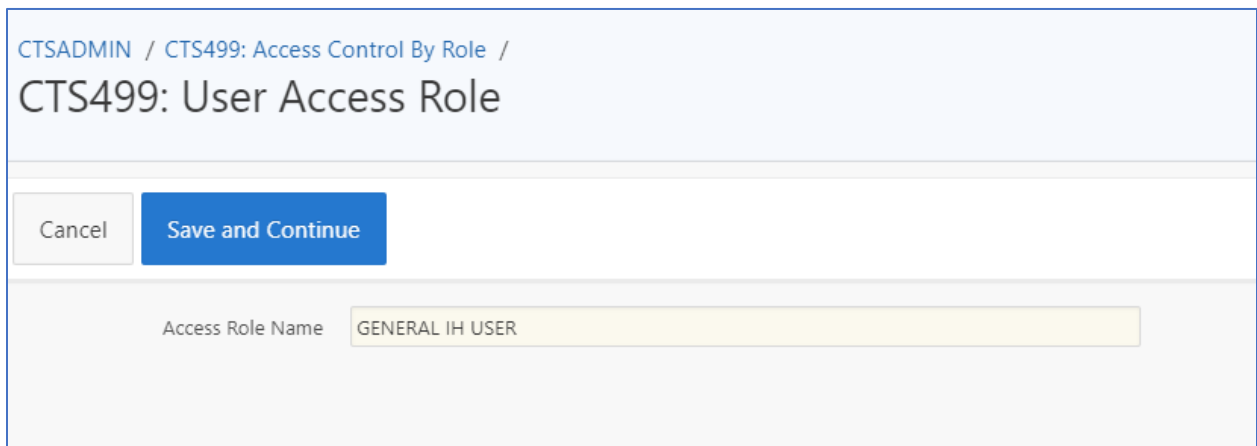
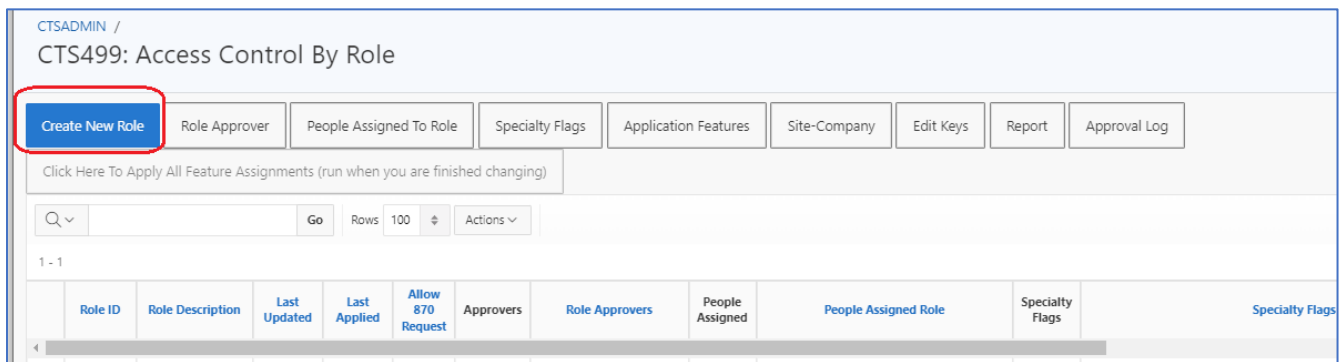
Site Administrator Feature Assignments (with assumption they are already assigned to the general user role – or you have assigned those features to this role)		
Menu	Region	Minimum Key Features
Exposure Assessment	Support	CTS044, CTS045, CTS046, CTS061
Toolkit	Configuration and Reference List	CTS851, CTS852
Toolkit	Support	CTS497
Master Lists	Master List Entry and Edit	CTS401, CTS402, CTS403, CTS404, CTS405, CTS407
Maser Lists	Master List Reports	CTS411, CTS412, CTS414, CTS426, CTS429, CTS431
Maser Lists	Support	CTS396, CTS422, CTS437, CTS847, CTS856
Administration	Security and Menu Assignments	CTS486, CTS495, CTS499
Administration	Support	CTS476, CTS994

Try to create as few roles as is reasonable to manage but create all you need to have the needs of different groups of people met.

You should always have an IT administrator role - with all access and all features ... and give that role everything. Only assign people to it that should have that level of system management.

Creating an Access Control Role

To create an access role and assign features, flags and site/company go to CTS499 and click the Create New role button.



Click Save and Continue, then then begin assigning people, specialty flags, application features and, sites-companies.

The order you add does not matter.

You can click the pencil in the column or you can click the button above to get to an assignment screen.

CTSADMIN / CTS499: Access Control By Role

Create New Role | People Assigned To Role | Specialty Flags | Application Features | Site-Company | Edit Keys | Report

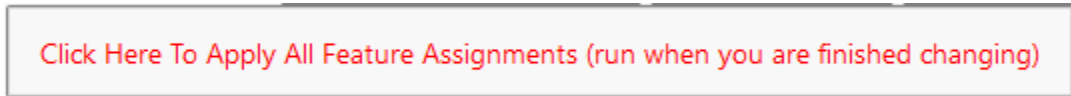
Click Here To Apply All Feature Assignments (run when you are finished changing)

Q v Go Rows: 100 Actions v

1 - 2

Role ID	Role Description	Last Updated	Last Applied	People Assigned	People Assigned Role	Specialty Flags	Specialty Flags	Application Features	Application Features	S-C	Site-Company
0000001	GENERAL BY USER SAMPLING AND EXPOSURE ASSESSMENT	04-MAY-2022 09:47:26 PM			-						
0000002	IT ADMINISTRATOR	04-MAY-2022 08:47:30 PM	04-MAY-2022 08:47:35 PM		LAST NAME, FIRST NAME (BADGE) (CTSONMER)		CTS Mgr, IT Support, Create Public Reports		More than 20 - too many for this display		Write SITE C

When you have completed your entry and wish to apply the assignments to people, click the red titled button



If this button is not red-titled, nothing has changed, and you do not need to click it to apply anything

When the apply button is clicked, the apply routine will go through ALL roles and ALL people and build each unique profile for each unique person (logon id)

Chapter 3: Access Control Reports

If you have a larger number of roles, and/or a larger number of people, using CTS499 to understand what a user has access to can be inefficient.

When you want to review access profiles broadly, use CTS486 and choose the review method of interest.

If you want to see who has a certain management flag, choose the access by user and manager flag.

If you are searching for the total set of people having access to a certain feature, use the User and Feature option.

