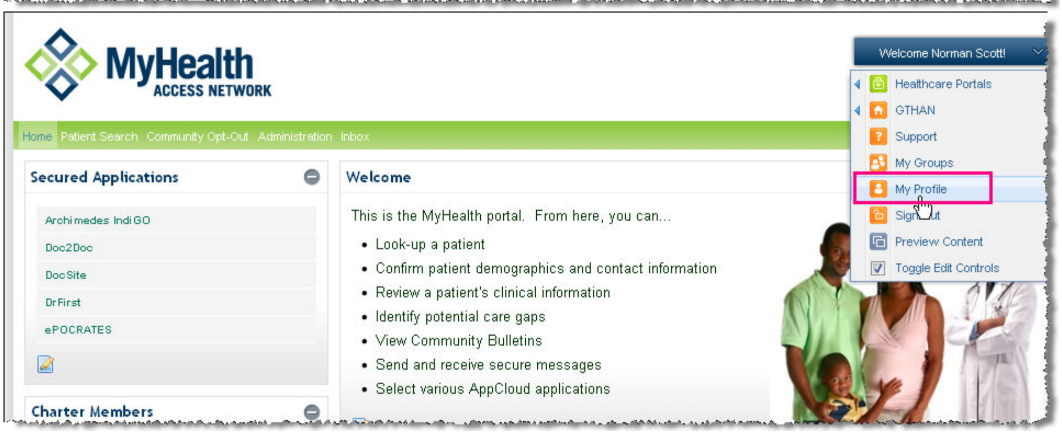
Security Administrator's User Guide

Table Of Contents

ALL USERS

Accessing the "My Profile" Administration Application

1. Sign on to your portal.



2. Click **My Profile** from the Welcome drop down menu. The Home page of the Account Administration application is displayed.

RESULT:

You have successfully accessed the My Profile account administration application.

Reset Your Password

A password reset is a multi-step process that includes:

- answering a security question
- obtaining a temporary password in two parts (one on the screen and one via email)
- entering your temporary password
- resetting to a new, chosen password
- logging in with your chosen password

If your organization also uses the IDcipher™ card premium service, in addition to password login, then your existing IDcipher™ card will become null and void upon successfully resetting your password via "forgot password" link. The system will automatically send you a new IDcipher™ card upon password reset.

1. Navigate to the Sign On screen.

2. **Forgot Your Password?** link.
3. In the open text box, key in your User ID.
4. Click **Submit**. The Challenge Question screen is displayed.

5. Key in the answer to the Challenge Question, exactly as you did during registration.
6. Click **Submit**. The first half of your temporary password is displayed on the screen. The remaining four digits of your temporary password are sent to the email address with which you registered.
7. Write down the four numbers displayed on your screen on a sheet of paper.
8. Retrieve the remaining four digits from your email Inbox.
9. Key in your User ID in the open text field.
10. Key in your eight digit temporary password in the open text field.
11. Click **Sign On**. You are immediately prompted to change your password.
12. Key in the eight digit temporary password in the Old Password open text field.
13. Create a new password, and key it into the New Password open text field. Passwords must be adhere to specific rules. Refer to the password rules on your screen if necessary.
14. Key in your new password again in the Confirm New Password open text field.
15. Click **Update**.

If the IDcipher™ card is required in addition to password sign on, then your existing IDcipher™ card will become invalid upon successfully resetting your password. The system will automatically send you a new IDcipher™ card upon password reset.

RESULT:

You have successfully reset your password and are now ready to sign on to the portal.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

Unlocking Your Account

For security purposes, your user account will become locked if you unsuccessfully attempt to sign on to the portal beyond the predetermined login attempt limit. When this is the case, perform the Password Reset function to unlock your account.

If an IDcipher™ card is required to sign on, your existing IDcipher™ card will become invalid when your account is unlocked and the system will automatically send you a new IDcipher™ card.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

How Do I Get An IDcipher TM Card?

The IDcipher™ card is used as a method for authentication that may optionally be used within Portals that require up-level authentication.

The process for obtaining an IDCipher™ Card is dependent upon your user status. Click on the link that best describes you:

I am an existing user, I can already log in to the portal, but I need a new IDcipher™ Card >>>

I am new to the portal, and not yet a registered user? (You have not yet registered for the portal) >>>

When you register for portal access, an IDcipher™ card will automatically be generated and emailed to you upon approval of your registration request if the portal you are requesting access to requires the IDcipher™ card for up-level authentication.

After submitting a registration request, users need not perform ad an IDCipher™ card.

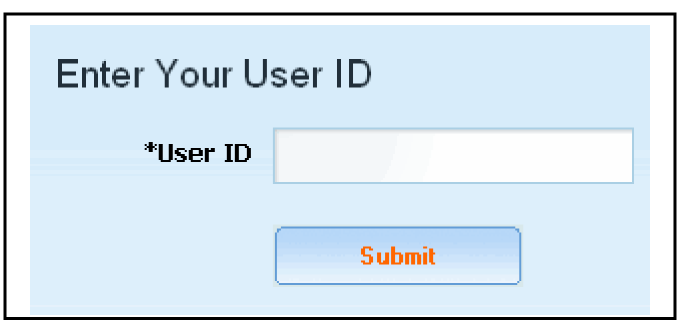
(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

Existing Portal User - I Need a New IDcipherTM Card

If you are not in possession of your IDcipher™ card, you are able to generate a new card. Complete the following steps to generate a new card that will be emailed to the email address you provided during registration as part of your user profile. (The IDcipher™ Card will be sent to the email address that is associated with your profile when the request is made).

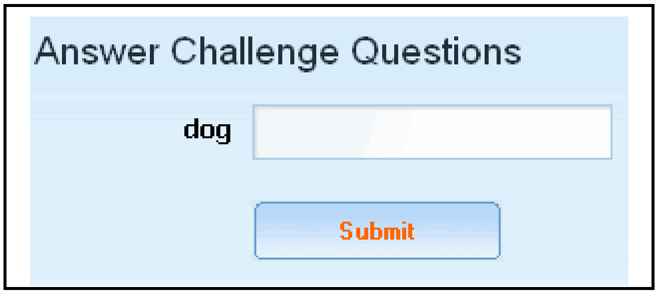
1. Navigate to the portal sign on screen.

2. Click **Request a new IDcipher™ card.** The **enter User ID screen** is displayed.

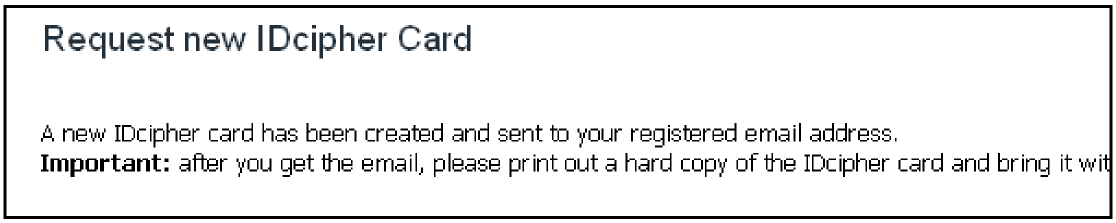


3.
4. Key in your User ID in the open text field.

5. Click **Submit**. The **challenge question screen** is displayed. (***Learn more about a challenge question/answer >>>***)



6.
7. Key in the answer to your challenge question.
8. Click **Submit**. A confirmation screen displays that a **new IDcipher™ card** has been generated and emailed to you.



9.

RESULT:

You have successfully obtained a new IDcipherTM Card.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

About the IDcipherTM Card

The IDcipher™ Card is used as a method for authentication that may optionally be used within Portals that require up-level authentication.

The IDcipher™ card provides two-factor authentication (something the user knows and something the user has) which is one form of authentication that may be used when up-level authentication is required. The card provides a low-cost, easy-to-use, easy-to-deploy authentication mechanism that provides an extra level of assurance when a user is authenticated.

Covisint has trademarked the IDcipher™ Card.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

When Will I Be Prompted To Use An IDcipherTM Card Number?

You will only be prompted to use an IDcipher™ card when up-level authentication is required and the IDcipher™ card was specified as the method of authentication required to complete the up-level authentication.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

Up-Level Authentication

Up-level authentication is an authentication process that prompts the user for an additional, stronger form of authentication than a user name and password, when a user attempts to gain access to a system resource that requires an additional level of protection. Additionally, the user may be prompted for up-level authentication based on specified criteria which can be derived from user provided information (e.g. a specific user name), system collected information (e.g. an unknown PC IP Address), as well as transaction patterns (e.g. time of day the user signs on or how frequently the user is signing on).

Covisint has trademarked the IDcipher™ Card as a means of providing up-level authentication. – Delete from this section and add to section about the IDcipher card.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

Administrator Roles Matrix (Portal and User Security)

Two categories of roles are managed within the Administration too. Those are:

- Covisint Connection and Administration (CCA) Administrator roles
- Health Exchange Roles

The following table lists the privileges that are contained within CCA Administrator roles. When Division Administrators are assigned the Security Admin role perform tasks, each task is only applicable to that division. The role of Security Administrator applies to the division-level as well as the top-level organization. If your company sets up Divisions (aka practices) in this online structure, the Administrator at the Division level is also called a Security Administrator.

CCA Administrator roles are not tied to Health Exchange roles.

Table 1:
Matrix of Privileges Associated Per Role

	Service Admin	Security Admin	Division Admin
Approve / Reject division's service package request	x	x	-
Approve / Reject new user registration requests	-	x	x
Approve / Reject organization service request	-	x	-
Approve / Reject site codes for divisions of your org	-	x	-
Approve / Reject user's service package requests	x	x	x
Audit user grants	x	x	x
Audit users in company (Quarterly & Annually)	-	x	x
Change email preferences for self	x	x	x
Change password of self	X	X	X
Delete a division in your org	-	x	-
Delete a user account	-	x	x
Edit organization and/or division profile	-	x	x
Edit profile of others	-	x	x
Edit profile of self	X	X	X
Generate a service summary report	-	x	x
Generate report of user summary by organization	x	x	x
Generate report of users grants per svc. package	x	x	x
Generate security administrator reports	x	x	x
Grant a service package to a division in your org	-	x	-
Grant a service package to a user	x	x	x
Invite users to register	-	x	x
Modify user roles	-	x	x
Move a user	-	x	x
Remove a service package from a division in your org	-	x	-
Remove service package from a user	x	x	x
Request a service package for my organization	x	x	x
Request a service package for self	x	x	x
Reset password of others	-	x	x
Search /View details for divisions in my organization	x	x	-
Search for users in my organization	x	x	x
Specify password for self	-	x	x
Specify password of others	-	x	x
Suspend a division in your org	-	x	-
Suspend a user account	-	x	x

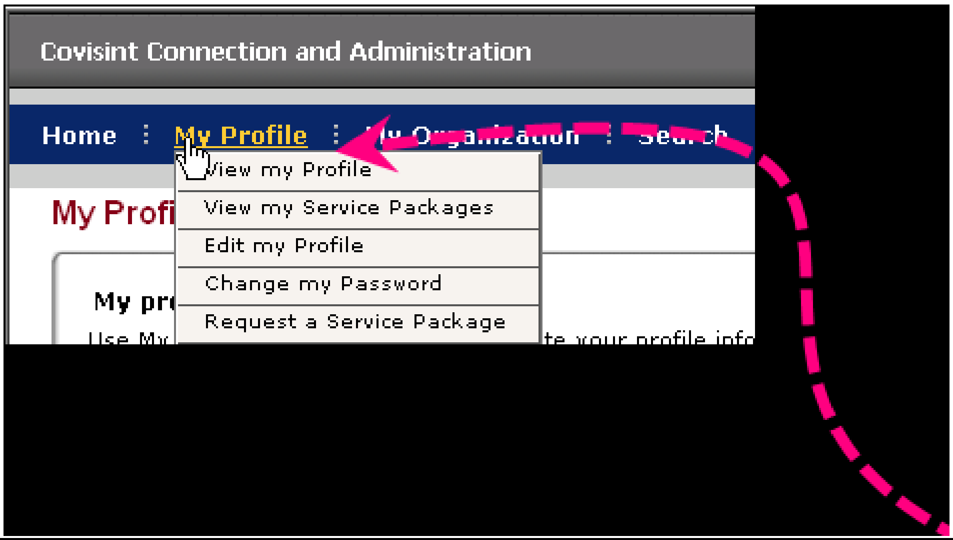
General Users

Cancel a Pending Request

1. From the **My Profile drop-down menu**, click **View my profile.**

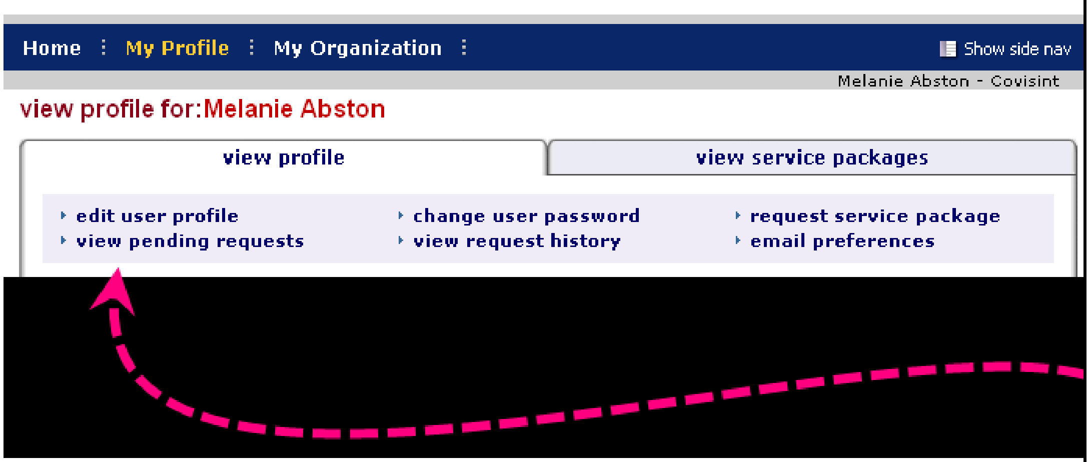
Where is the My Profile Drop-down Menu?

My Profile is located toward the top left of the toolbar.



2.
3. Click **view pending requests**.

Where is the View Pending Requests link?



4.
5. Enable the checkbox of each request you wish to cancel.

6. Click **cancel pending request**.
7. Click **Submit decision.**

RESULT:

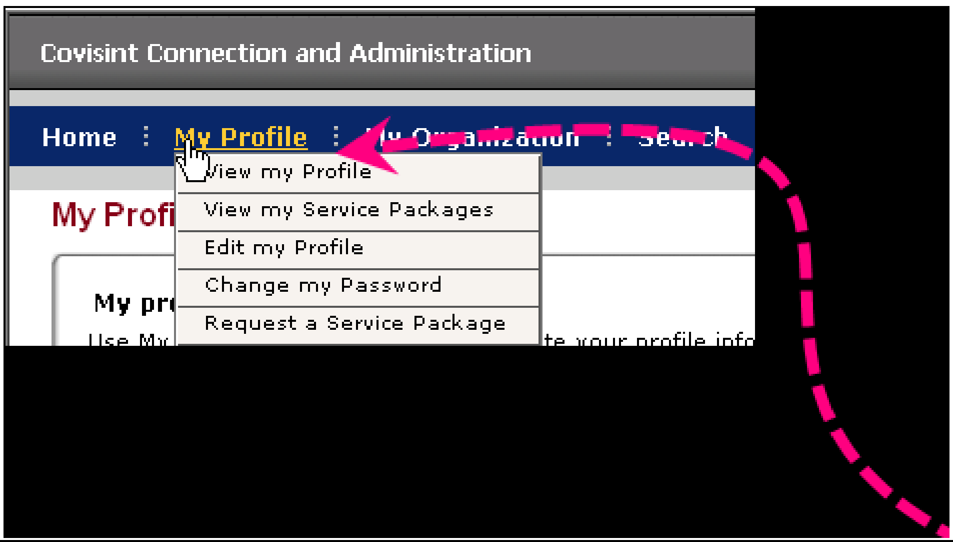
You have successfully cancelled a pending request.

Change Your Password

1. From the **My Profile drop-down menu**, click **Change Password**.

Where is the My Profile Drop-down Menu?

My Profile is located toward the top left of the toolbar.

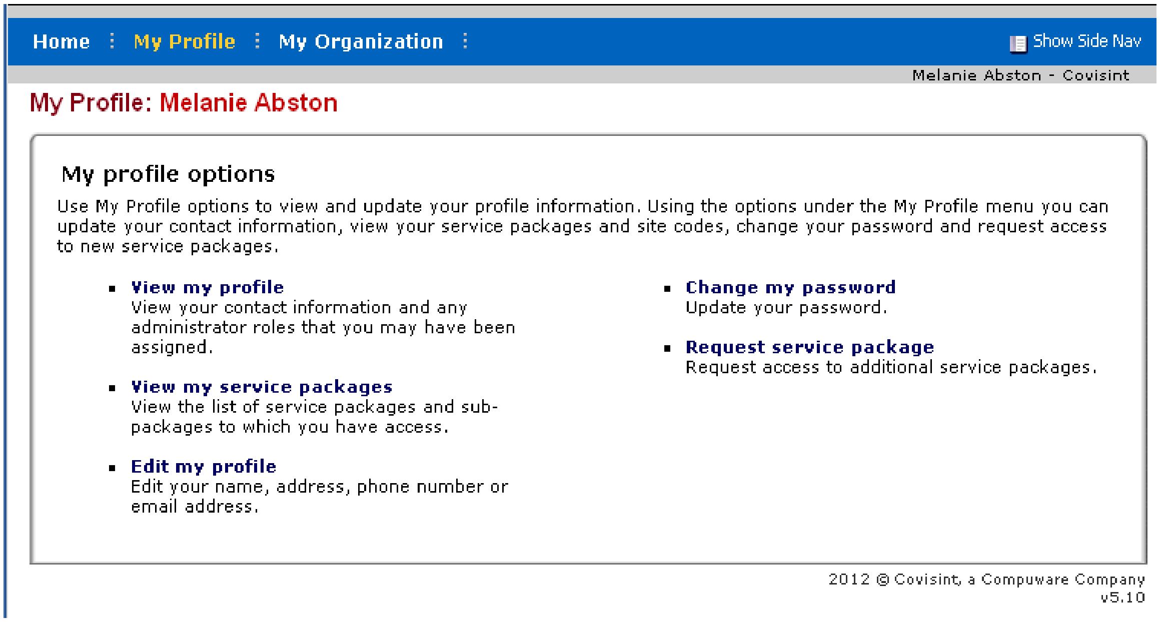


2. In the New Password open text field, create a new password that adheres to specific rules. Refer to the password rules on your screen if necessary.
3. In the Re-enter New Password open text field, k*ey in the newly created password* to verify that you have typed it correctly.
4. Click **Submit password change**.

RESULT:

You have successfully changed your password.

Manage Your User Profile



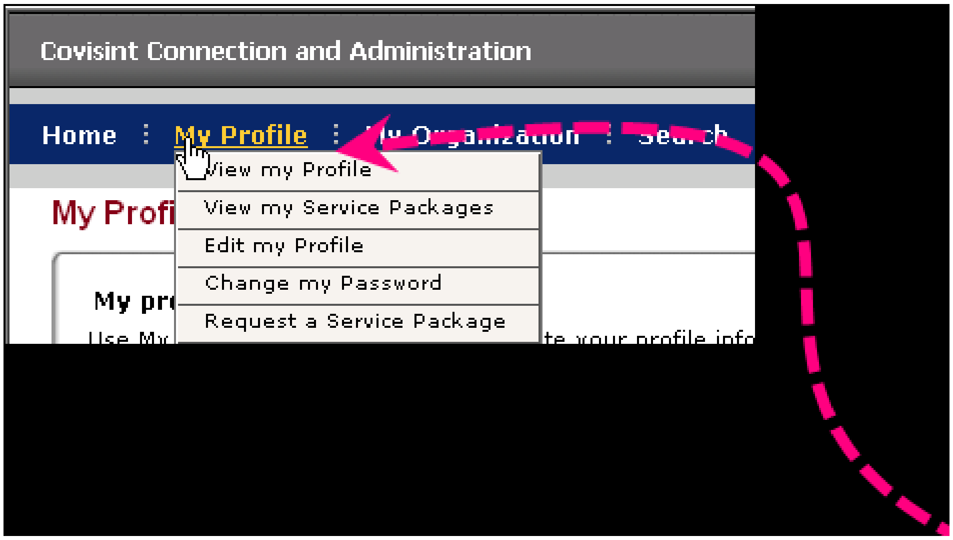
From the My Profile link, you are able to edit your:

- location information
- email address
- security question/answer
- password

- A User ID can never be modified, and can never be reused. Even if a Security Administrator removes your access from the portal, your User ID is invalid forever. If you need to be reinstated to access the portal, you must register for access again, using a different User ID.
- Hover your mouse over a question mark icon to view help text related to that field
- Be sure to enter an email address to which you have access at any time. For example, if your company firewall blocks certain email accounts, such as yahoo.com or aol.com, do not use that email address for your user profile.

---

1. Perform one or more of the following from the **My Profile drop-down menu**:



IF YOU WISH TO...	THEN:
edit your location information	a. Click **Edit my Profile.** b. Modify your address information as required. A User ID can never be modified, and can never be reused. Even if a Security Administrator removes your access from the portal, your User ID is invalid forever. If you need to be reinstated to access the portal, you must register for access again, using a different User ID. c. Proceed to step 2.
edit your email address	a. Click **Edit my Profile.** b. Modify your email address as required. Be sure to enter an email address to which you have access at any time. For example, if your company firewall blocks certain email accounts, such as yahoo.com or aol.com, do not use that email address for your user profile. c. Proceed to step 2.
modify your security question / answer	a. Click **Edit my Profile.** b. Review the details and requirements next to the Challenge Question and Challenge Answer fields. c. Modify your security question / answer as desired, adhering to the rules and policies listed. d. Proceed to step 2.

2. Click **Save Changes**.

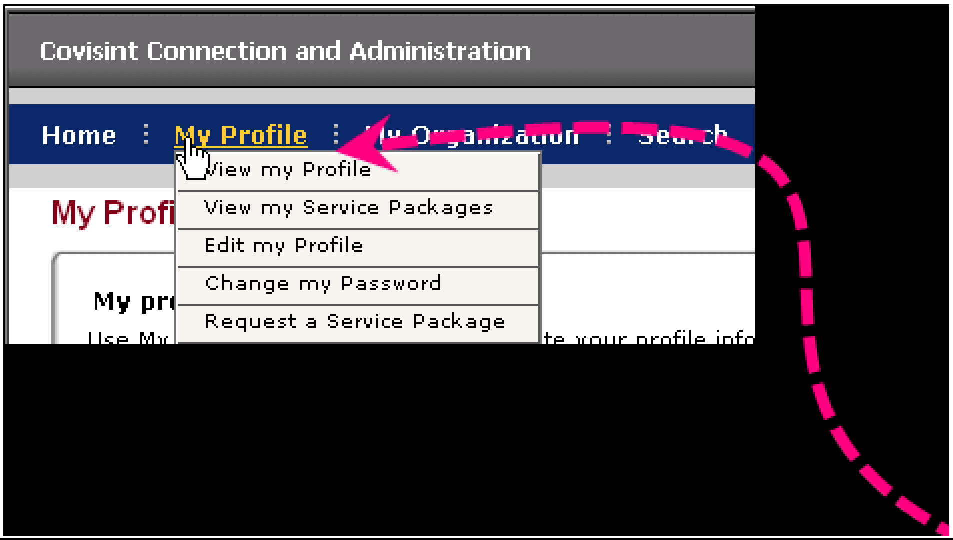
RESULT:
You have successfully edited your User Profile.

Opt Out of email Notices

1. From the **My Profile drop-down menu**, click **View my profile.**

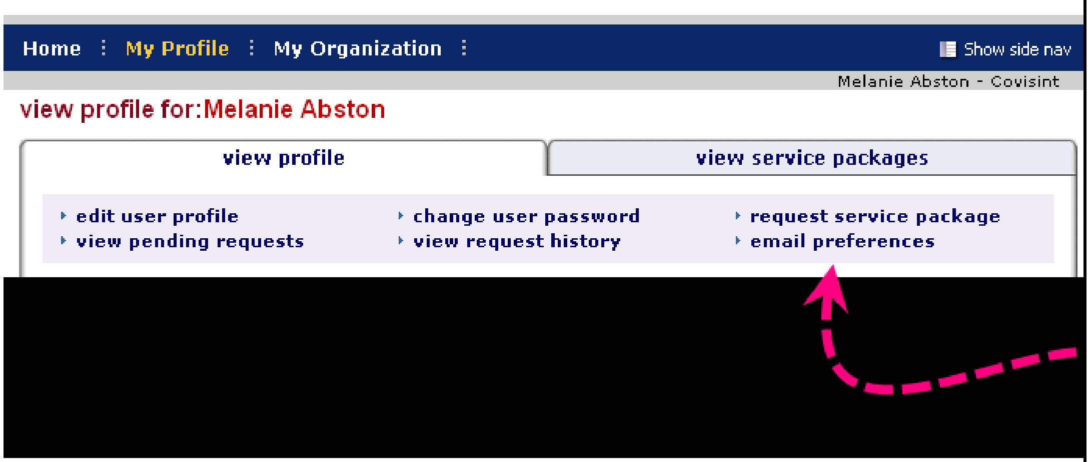
Where is the My Profile Drop-down Menu?

My Profile is located toward the top left of the toolbar.



2. Click **email preferences** link.

Where is the email preferences link?



3. Deselect the checkbox of each item you for which you do not wish to receive notification. (For security purposes, you are not able to opt out of password reset emails. It is important that you receive this alert any time your password is modified.)
4. Click **Save changes.**

RESULT:

You have successfully opted out of email notices.

Request Service Packages

A service package is a defined group of one or more applications to which you may have requested access during registration.

Later, post-registration, you may need to request additional service packages in order to perform your job duties.

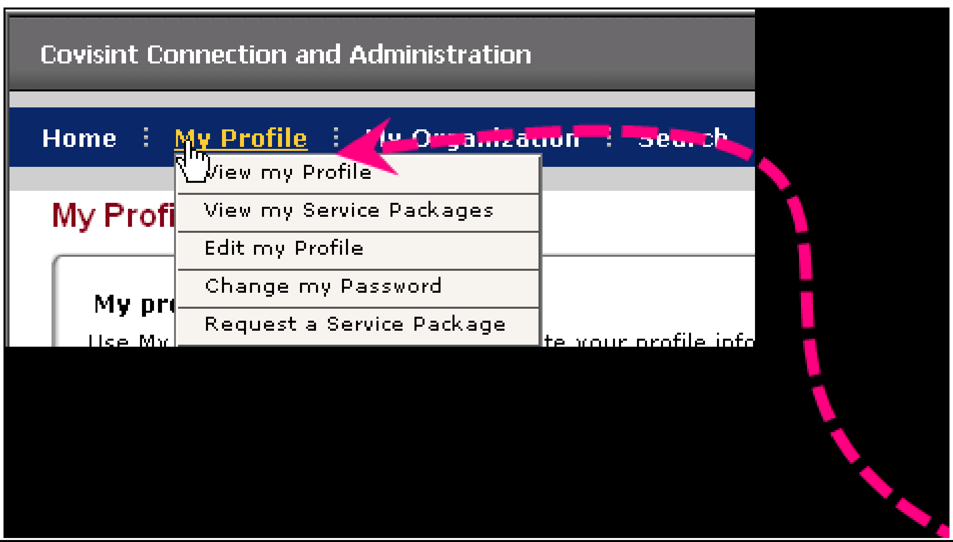
Your Security Administrator will approve/reject your request, and you will be notified of this decision via email. Additionally, your Security Administrator may grant a service package to you, without receiving a request from you.

Watch how to request a service package

1. From the **My Profile drop-down menu**, click **Request Service Package**.

Where is the My Profile Drop-down Menu?

My Profile is located toward the top left of the toolbar.



2. Click **request** next to the package you wish to request.
3. Enter the reason for request in the open text box.
4. Click **continue**.
5. Repeat steps 1 – 4 as necessary for additional service packages.

WHY DON'T I SEE THE PACKAGE OR SUB-PACKAGE I WANT ON THE LIST OF REQUESTABLE PACKAGES?

If you have already have been approved or already have a pending request for that package or sub-package, you will not see the package on the list. Keep in mind that if you are trying to find a specific service, it may be bundled in a package with a different name. Check the package description to view the services it contains.

IF YOU DID NOT RECEIVE A RESPONSE TO MY REQUEST FOR A SERVICE PACKAGE. NOW WHAT?

Your request was routed to your Security Administrator. You can send a reminder email to your Security Administrator by viewing your profile, then clicking the View Pending Requests link inside the application. You will have an opportunity from that screen to remind your Security Administrator to evaluate your request or you can cancel the request.

RESULT:

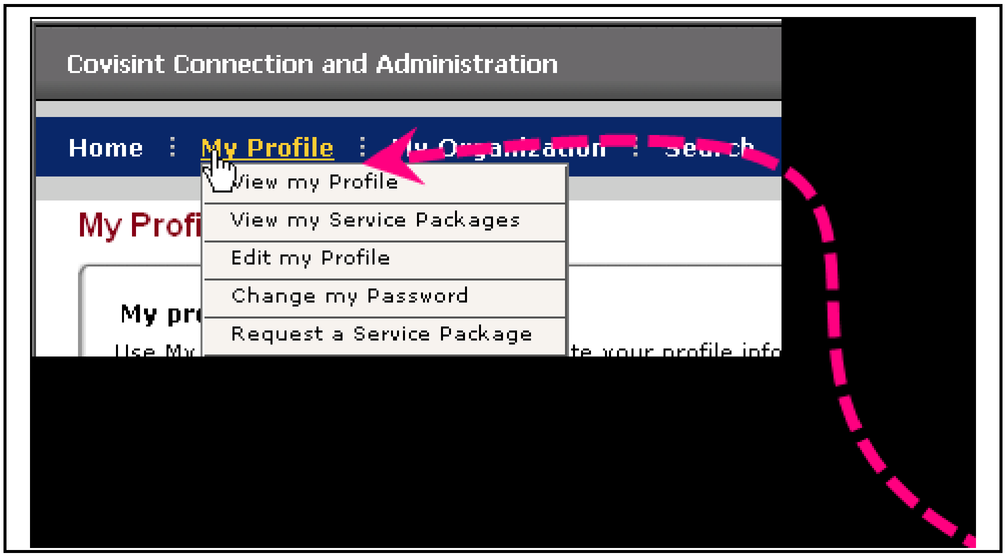
You have successfully requested service packages.

Send Pending Request Reminder to Administrator

1. From the **My Profile drop-down menu**, click **View my profile**.

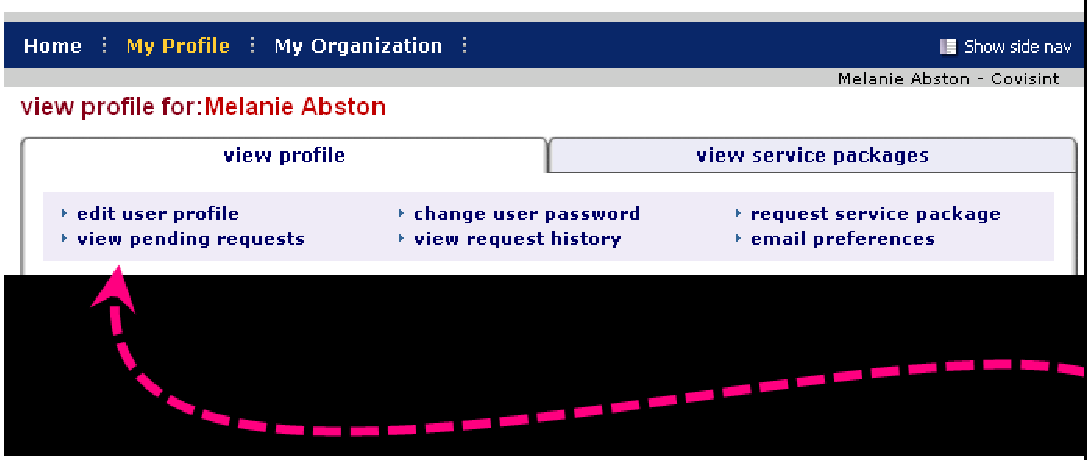
Where is the My Profile Drop-down Menu?

My Profile is located toward the top left of the toolbar.



2. Click **view pending requests**.

Where is the View Pending Requests link?



3.
4. Enable the checkbox of each request
5. Click **Send Reminder.**
6. Key in the *reason for reminder*.
7. Click **Submit**.

RESULT:

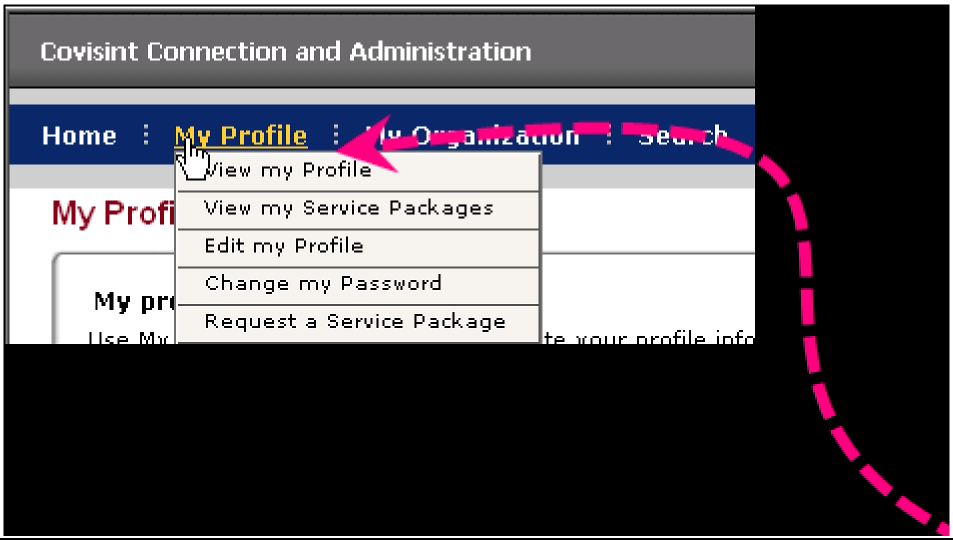
You have successfully sent a reminder to an administrator regarding your pending request.

View History of Your Requests

1. From the **My Profile drop-down menu**, click **View my profile**.

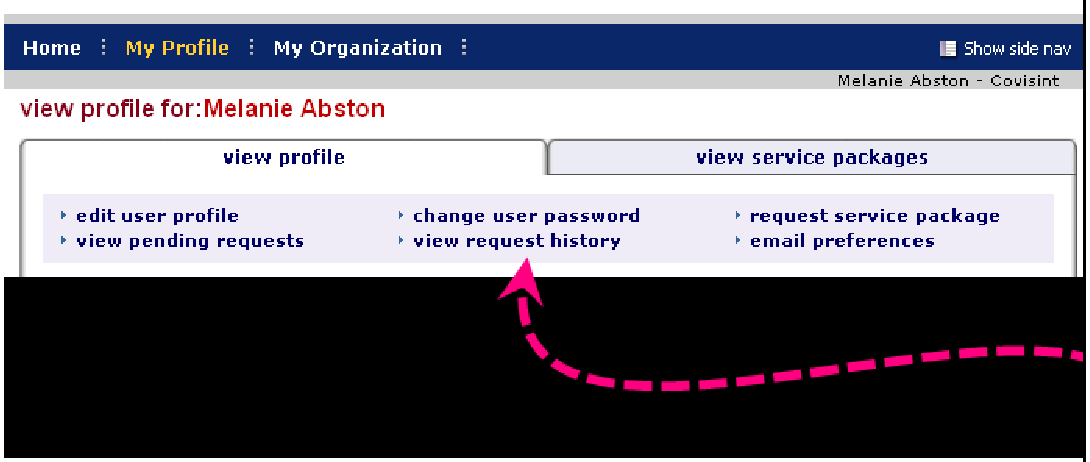
Where is the My Profile Drop-down Menu?

My Profile is located toward the top left of the toolbar.



2. Click **view request history**.

Where is the view request history link?



RESULT:

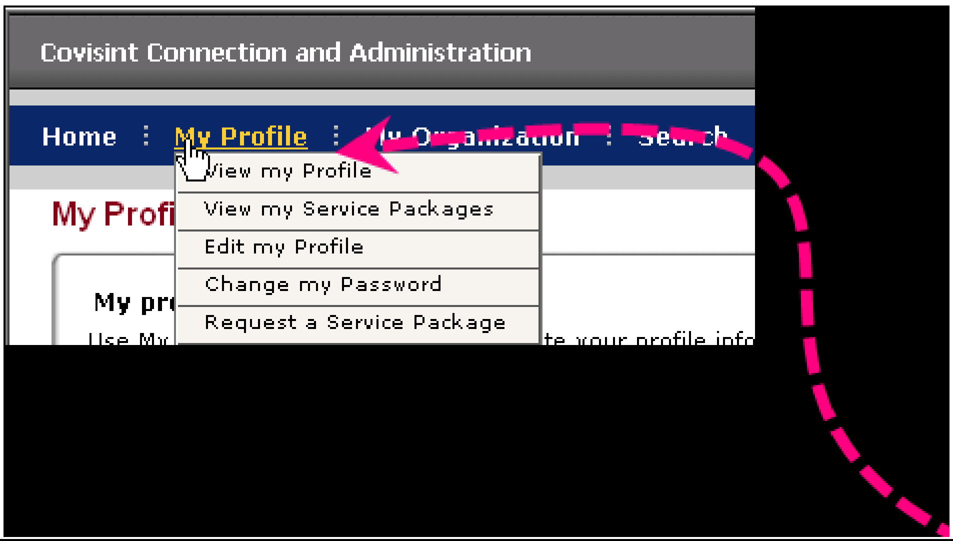
You have successfully viewed a history of your requests.

View Your Current Service Package Grants

1. From the **My Profile drop-down menu**, click **View my profile.**

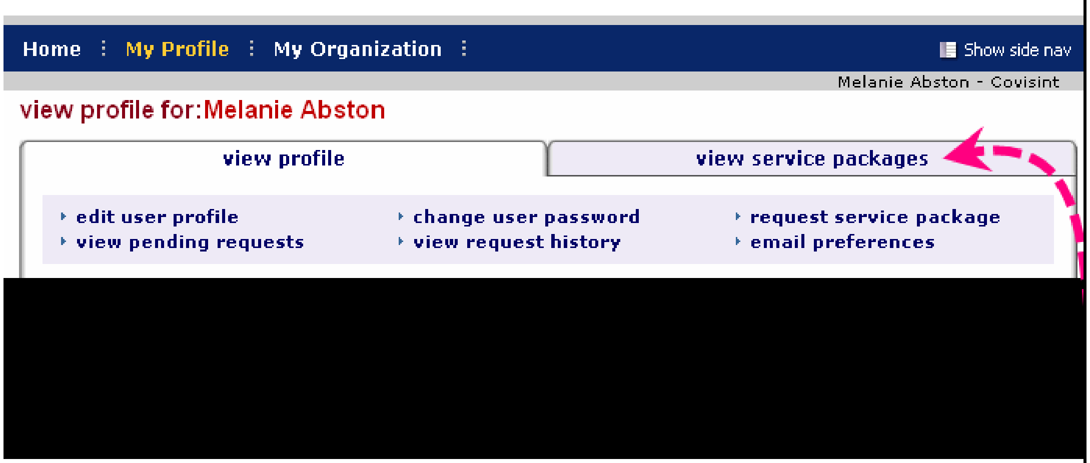
Where is the My Profile Drop-down Menu?

My Profile is located toward the top left of the toolbar.



2. Click **view service packages** tab. A list of all service packages to which you currently have access is displayed.

Where is the view service packages tab?



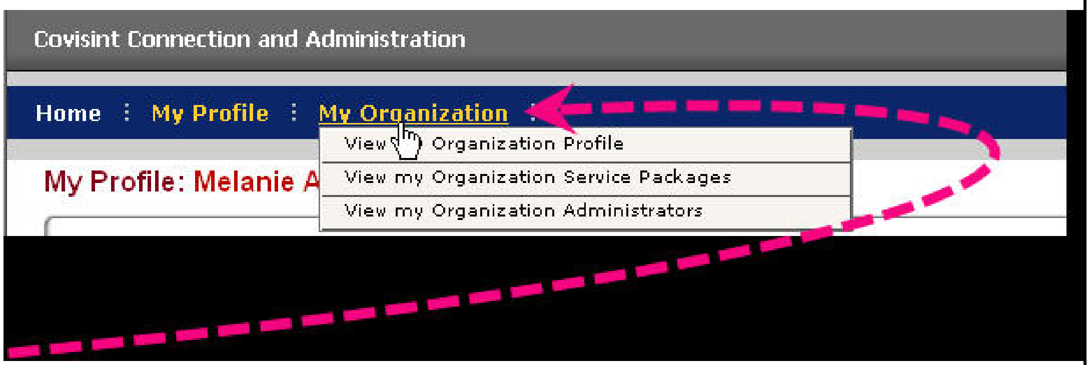
RESULT:

You have successfully viewed your service package grants.

View Your Organization Profile

1. Click **My Organization drop down menu**.

Where is the My Organization drop-down menu?



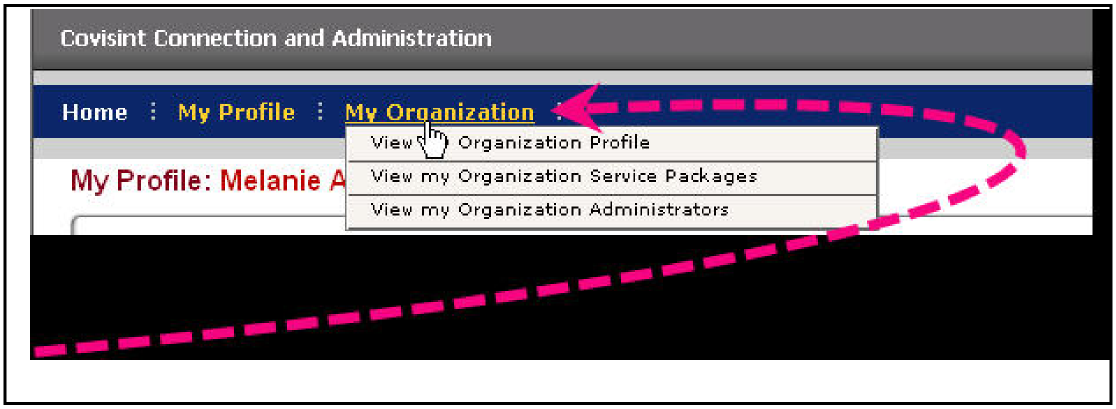
2.
3. Click **view my organization profile.**

RESULT:
You have successfully viewed your organization profile.

View Your Organization Services

1. Click **My Organization drop down menu**.

Where is the My Organization drop-down menu?



2.

3. Click **view my organization services**. A list of all services to which your organization currently has access is displayed.

RESULT:

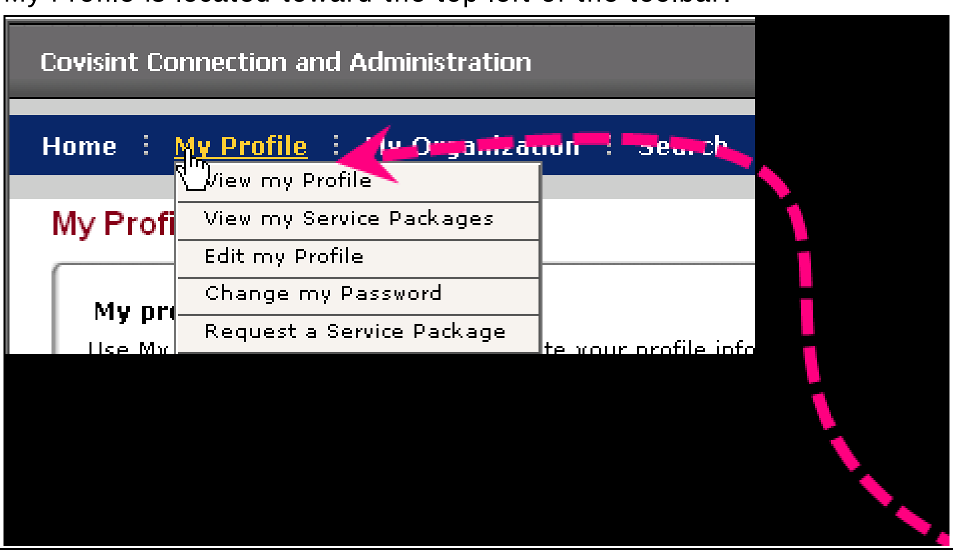
You have successfully viewed your organization services.

View Your Pending Requests

1. From the **My Profile drop-down menu**, click **View My Profile**.

Where is the My Profile Drop-down Menu?

My Profile is located toward the top left of the toolbar.



2. Click view pending requests.

RESULT:

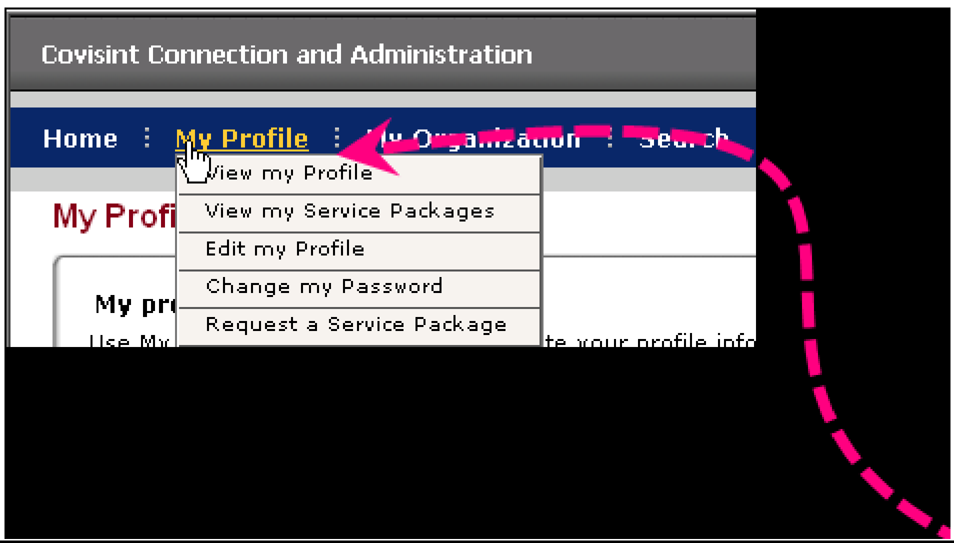
You have successfully viewed your pending requests.

View Your User Roles

1. From the **My Profile drop-down menu**, click **View my profile**.

Where is the My Profile Drop-down Menu?

My Profile is located toward the top left of the toolbar.



2. Scroll to the bottom of the screen to view the "user assigned roles" section. If you have roles assigned, they will be listed here.

RESULT:

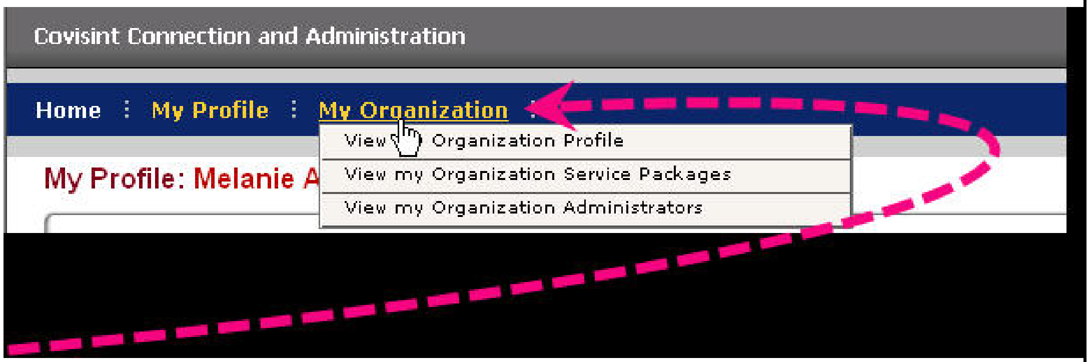
You have successfully viewed your user roles, if any are applicable.

Who are my Organization Security Administrators

Your organization Security Administrators are responsible for approving / rejecting your requests to service packages and suspending your account, among other things. They are also able to assist you with navigation and other questions.

1. Click **My Organization drop down menu**.

Where is the My Organization drop-down menu?



2.

3. Click **View my organization administrators**.

What if the Security Administrator is no longer valid? You can change your administrator by submitting the Security Administrator Change form.

RESULT:

You have successfully viewed your Security Administrators.

SECURITY ADMINISTRATORS

What is a Security Administrator?

The Security Administrator is responsible for the establishment and management of your organization and its divisions, and serves as the main point of contact for your organization. Security administrators also manage the organizations users and access rights. Those with the Security Administrator role decide who gets to use the portal, and what they get access to in the portal.

Managing Users

The checklist below is provided to help you get started managing your organization's **users** as a Security Administrator. (Also view the checklist for managing your organization.)

Tasks are **listed in the order in which they are typically performed**. (This is not a comprehensive list of everything you can do... just a list to help get you started with in your new role.)

SECURITY ADMINISTRATOR - MANAGING USERS

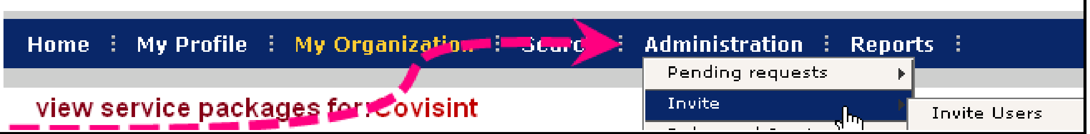
- ☐ Invite users to register for access to the portal
- ☐ Approve pending new user access requests
- ☐ Approve pending service package requests from users
- ☐ Search for users in your Organization
- ☐ Grant a service package to a user
- ☐ Modify a user's role
- ☐ Suspend a user's account
- ☐ Specify a user's password
- ☐ Edit a user's profile

Managing Your Organization's Users

Invite User to Register for Access to the Portal

1. Click **Invite Users** from the **Administration -> Invite drop-down menu**.

Where is the Administration / Invite drop-down menu?



2. Key in the *email address for each recipient* you wish to invite, **separated by semi-colon (;)**
3. Click **send invitation.**
4. Click **OK**.

- The system does not validate the accuracy of the email addresses that you key in. If an email invitation cannot be delivered for any reason, you will not be notified of this failure.
- A good rule of thumb is that you do not modify the text of the email invitation, as editing the actual invitation URL within the subject text could break the link.

RESULT:

You have successfully invited a user to register for portal access.

What happens next?

- User will receive the invitation via email, and complete the steps for registration.
- You will receive an email regarding the user's pending request after the user submits the registration request.
- Approve the user request
- Optionally, grant service packages
- Optionally, modify user roles

Approve Pending New User Request

1. Click **User Requests** from the Administration -> Pending requests drop-down menu.
2. Click to view details of request.
3. Enable the ‘approve’ radio button.
4. Click **submit decision**.
5. Click **OK**.

If your organization also uses the IDcipher™ card in addition to a user name and password for authentication, then the system will automatically generate and email an IDcipher™ card to the user upon your new user request approval.

RESULT:

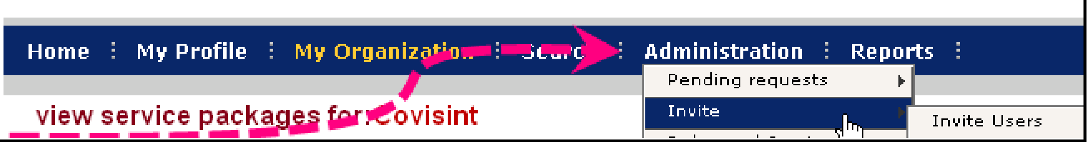
You have successfully approved a pending account request. The user will receive an email notification regarding this approval, along with an IDcipher™ card, if applicable.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

Approve User’s Pending Service Package Request

1. Click **User Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration / Pending requests drop-down menu?



2.
3. Click the **User Service Package** tab.
4. Click to view details of request.
5. Enable the ‘approve’ radio button.
6. Click **submit decision.**
7. Click **OK**.

RESULT:

You have successfully approved a user's service package request.

Edit a User's Profile

1. Perform a user search.
2. From the search results, click on the *name of the user*.
3. Click **edit user profile**.
4. Modify the profile as necessary.
5. Click **Save changes.**

RESULT:

You have successfully edited a user's profile.

Create a New IDcipherTM Card for User

This task is only performed by Security Administrators that are responsible for users that require an IDcipher™ card.

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **Create a New IDcipher™ Card for User.** The user's security question and answer set is displayed.
4. Validate the user's identity via the security questions. The screen refreshes, and a new IDcipher™ card is sent to the user.

RESULT:

You have successfully created a new IDcipherTM card for a user.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

Grant Service Package to User

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **add service package.**
4. Enable the checkbox of each service package you wish to grant to this user.
5. Click **add checked...**

6. Click **continue.**
7. Click **submit.**

Some service packages are not grantable.

RESULT:

You have successfully granted a service package to a user.

Modify a User's Role

Please review the details when on assigning the Health Exchange Role Manager in the topic Managing the Health Exchange Role Manager role.

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **modify roles.**
4. Enable the checkbox of each role you wish to grant to the user.
5. Click **submit**.
6. Click **OK**.

RESULT:

You have successfully modified a user's role.

Move a User

In order to move a user, you must be the administrator at or above the current and target organizations / practices involved in the move.

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **move user.**
4. Enable the radio button of the target for this user.
5. Click **continue**.
6. Click **OK**.

When you move a user, all service packages to which the user currently has access will be transferred to the new organization / division. When making such a move the target organization will automatically receive access to the service package.

RESULT:

You have successfully moved a user.

Suspend a Service Package from User

1. Search and select the name of the user for whom you wish to suspend a service package.
2. Click on the *name of the service package*.
3. Click **suspend**.
4. Key in the *suspension reason.*
5. Click **yes, proceed with suspension.**

RESULT:

You have successfully suspended a service package. You are also able to permanently remove the service package, or to unsuspend it.

Unsuspend a User's Service Package

1. Perform a user search.
2. From the search results, click on the *name of the user*.
3. Click on the *name of the service package* you wish to unsuspend.
4. Click **unsuspend.**

5. Key in the *reason for activating the service package for this user* in the open text box.
6. Click **yes, activate service package..**

RESULT:
You have successfully unsuspended a user's service package.

Permanently Remove a User Account

1. Perform a user search. The user must be Suspended before the user can be permanently removed. Follow the steps in the section Suspend a User's Account if you have not already done so.
2. From the search results, click on the *name of the user.*
3. Click **permanently remove user.**
4. Key in the *reason for removing the user account* in the open text box.
5. Click **yes, permanently remove user.**

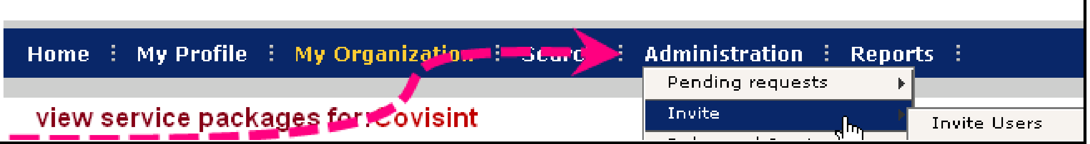
Once a user is permanently removed, that user can not be reactivated, and the user's id can never be reused.

RESULT:
You have successfully permanently removed a user account.

Reject Pending New User Account Requests

1. Click **User Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration / Pending requests drop-down menu?



2.

3. Click to view details of request.
4. Enable the ‘reject’ radio button.
5. Key in the *rejection reason* in the open text box.
6. Click **submit decision**.
7. Click **OK**.

When you reject a new user request, all service package requests for that user are automatically rejected.

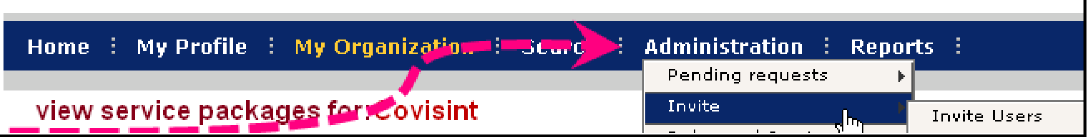
RESULT:

You have successfully rejected a pending request for a new user account. The user is notified via email of this decision.

Reject User’s Pending Service Package Request

1. Click **User Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration / Pending requests drop-down menu?



2.
3. Click the **User Service Package** tab.
4. Click to view details of request.
5. Key in the *rejection reason* in the open text box.
6. Enable the ‘reject’ radio button.
7. Click **submit decision.**
8. Click **OK**.

RESULT:

You have successfully rejected a user's request for service package(s).

Permanently Remove Service Package from User

A Service Package must be suspended before it can be permanently removed from a user.

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **view service packages** tab.
4. Click on the *name of the service package* you wish to remove.
5. Click **permanently remove service package**.
6. Key in the *reason for removing package.*
7. Click **continue**. The package is removed.

RESULT:

You have successfully removed a service package from a user.

Reset a User's Password

1. Perform a user search.
2. From the search results, click on the *name of the user*.
3. Click **reset user password**.
4. Validate the user's identity via the security questions.
5. Click **reset password**.
6. Read first half of password to user.
7. Instruct user to obtain second half of password from his/her email account.
8. Inform user that after signing on with this newly created, temporary password, the user will be prompted / required to change the password.

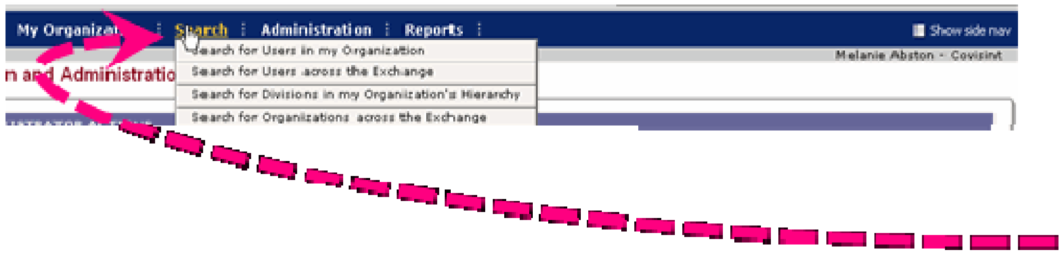
RESULT:

You have successfully reset a user's password.

Search for Users in My Organization

1. From the **Search drop-down menu**, click **Search for Users in my Organization.**

Where is the Search drop-down menu?



2. Select search criteria.
3. Click **Search**.

RESULT:

You have successfully searched for users in your organization

Specify a User's Password

1. Perform a user search.
2. From the search results, click on the *name of the user*.
3. Click **specify user password**.
4. Validate the user's identity via the security questions.
5. In the first New Password open text field, *key in a new password* for this user.
6. In the second New Password open text field, *key in the password again*.
7. State the password to the user.
8. Click **Submit Password Change**. Inform user he/she will be forced to change this temporary password upon the next login.

RESULT:

You have successfully specified a user's password.

Suspend a User's Account

1. Perform a user search.

2. From the search results, click on the *name of the user.*
3. Click **suspend user**.
4. Key in the *reason for suspending the account* in the open text box.
5. Click **yes, suspend user.**

RESULT:

You have successfully suspended a user's account.

Unsuspend a User’s Account

1. Perform a user search.
2. From the search results, click on the *name of the user*.
3. Click **unsuspend user.**
4. Key in the *reason for activating the user account* in the open text box.
5. Click **yes, activate user.**

RESULT:

You have successfully unsuspended a user's account.

View My Organization's Users

1. From the **My Organization drop-down menu**, click **View My Organization Users.**

Where is the My Organization drop-down menu?

2. Optionally, click on a *User Name* to view details of that user profile.

RESULT:
You have successfully viewed a list of your organization's users.

MANAGING YOUR ORGANIZATION

Edit Your Organization Profile

1. Click **view my organization profile** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?

2. Click **edit organization profile.**
3. Edit as desired.
4. Click **submit changes.**

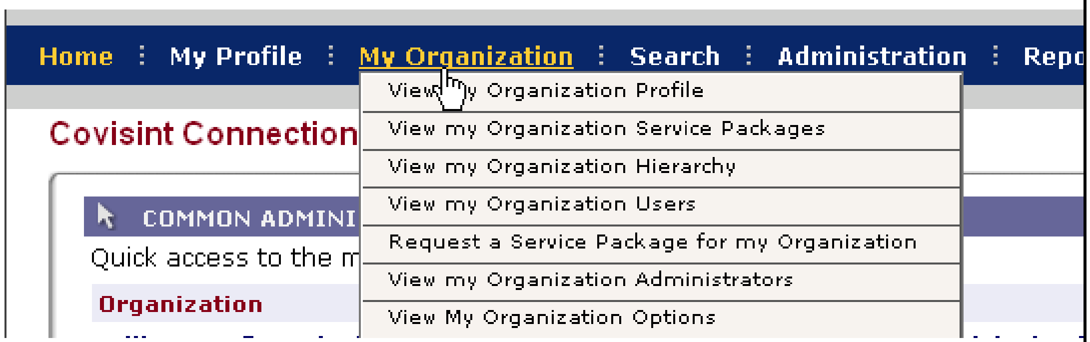
RESULT:
You have successfully edited your organizational profile.

Permanently Remove a Suspended Service Package

A service package must first be suspended before being removed. If you have not already done so, complete the steps for Suspending a Service Package from Organization before proceeding with this task.

1. Click **view my organization service packages** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?



2. Click on the *name of the suspended service package.*
3. Click **permanently remove organization's grant for service package.**
4. Key in the *reason for removing the service package* in the open text box.
5. Click **yes, proceed with removing.**

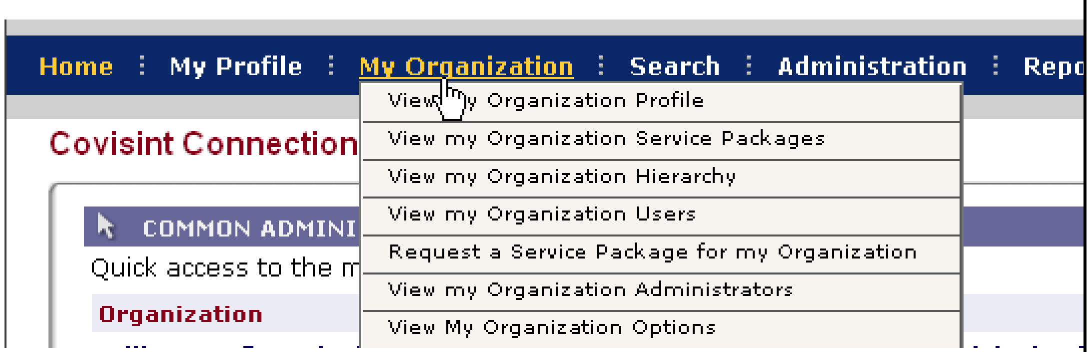
RESULT:

You have successfully removed a service package from the organization.

Request a Sub-Package for Your Organization

1. Click **Request a Service Package for my organization** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?



2. Click **request sub package** next to the desired package.
3. Click **request**. This request for sub- package is submitted to the approving administrator.

RESULT:
You have successfully requested a sub-package for your organization.

Request Service Package for your Organization

1. Click **Request a Service Package for my organization** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?

2. Click **request** next to the desired package.
3. Key in the *reason for request* in the open text box.
4. Click **continue**. This request for service packages is submitted to the approving administrator.

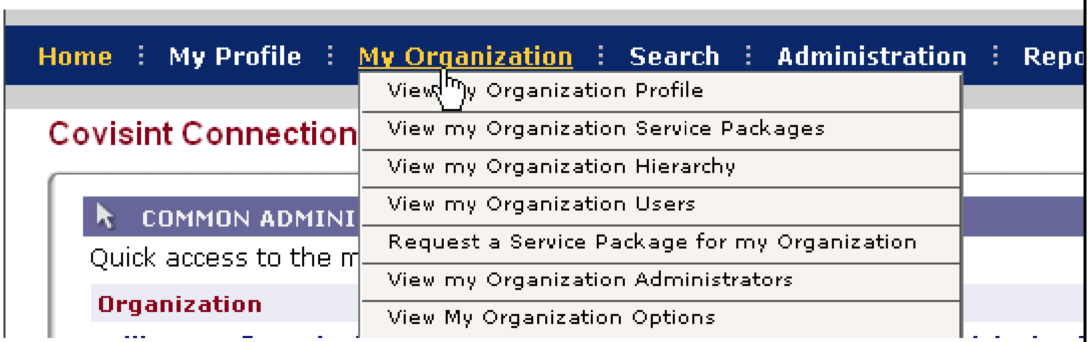
RESULT:
You have successfully requested a service package for your organization.

Suspend a Package from Organization

Suspending a service package from your organization is not easily undone. Once you suspend your organization's access to a service package, it can only be reinstated by contacting Covisint. You may prefer to suspend the service package from individual users in your organization. In so doing, you remain in control of access to the service package, and can easily 'un-suspend' a user's access to a service package.

1. Click **View my organization service packages** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?



2. Click on the *name of the service package*.
3. Click **suspend**.
4. Key in the *suspension reason.*
5. Click **yes, proceed with suspension.**

Suspending a Service Package from your organization locks all users out of that package during the time of suspension.

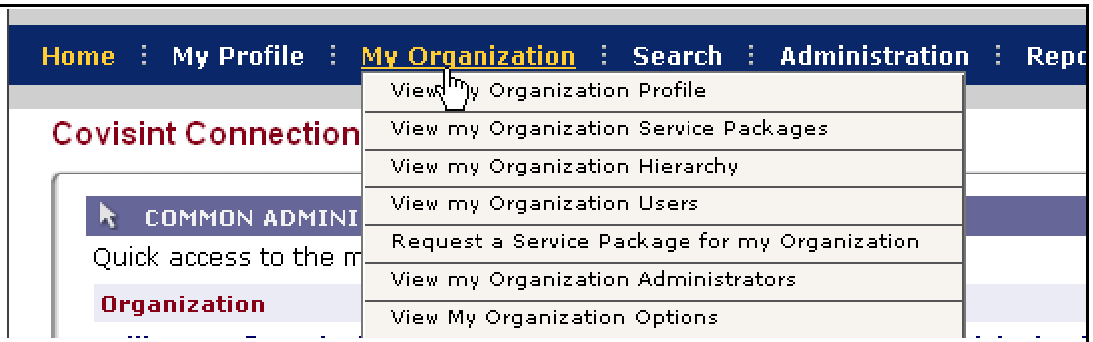
RESULT:

You have successfully suspended a service package.

View Organization Administrators

1. Click **View my Organization Profile** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?



2. Click the **view administrator** tab. All administrators in the organization are displayed.

RESULT:

You have successfully viewed all administrators in your organization.

View Organization Hierarchy (within CCA)

1. Click **View my Organization Profile** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?

2. Click the **view hierarchy** tab. (To view an organization, click on its name within the tree).

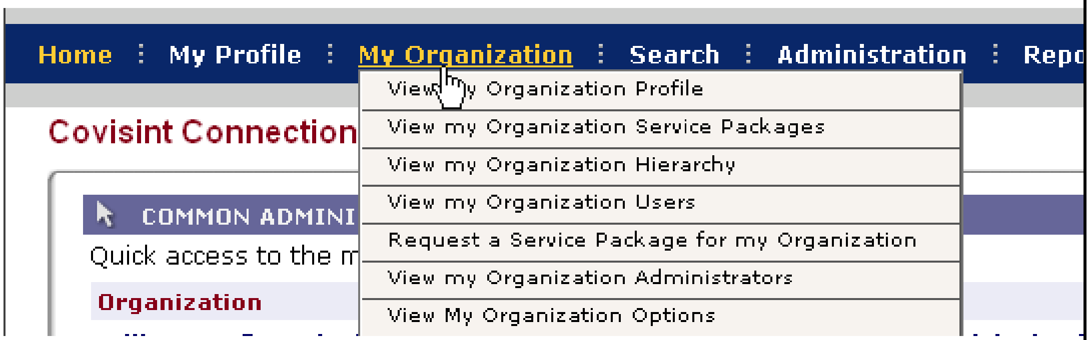
RESULT:

You have successfully viewed your organization's hierarchy.

View Organization Service Packages

1. Click **View my Organization Profile** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?



2. Click the **view service packages** tab. From this screen, you are able to view packages and sub packages to which your organization currently has access.

RESULT:

You have successfully viewed your organization's service packages.

View Organization Users

1. Click **View my Organization Profile** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?

2. Click the **view user** tab. All users registered in the organization are displayed.

RESULT:

You have successfully viewed all users in your organization.

View Pending Organization Requests

1. Click **view my organization profile** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?

2. Click **view pending requests.**

RESULT:

You have successfully viewed your organization's pending requests.

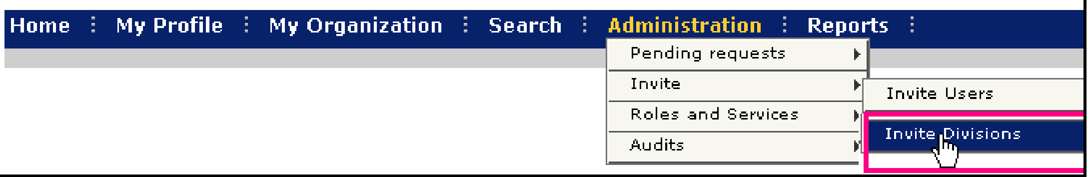
Invite Division (aka Practice) to Register for Access to the Portal

What is a Division?

A division is a part of your organization's hierarchy, such as a business unit, or practice. When inviting a division to your organization, it is important to understand that you are creating a hierarchy for your organization with a delegated administration model. This gives the security administrator of that division the authoritative power over the users of that division. Although the security administrator of the top level organization will still have authority over the users of the division all requests for services and new user accounts will be handled at the division level by the appropriate administrator. You should only create divisions in your organization if you believe your organization would benefit by delegating the administrative responsibilities to an entirely new organization (the division), which will be managed by its own administrators.

1. Click **Invite Division** from the **Administration -> Invite drop-down menu.**

Where is the Invite Divisions drop-down menu?



2.
3. Key in the *email address for each division's recipient* you wish to invite, **separated by semi-colon (;)**
4. Click **send invitation.**
5. Click **OK**.

- The system does not validate the accuracy of the email addresses that you key in. If an email invitation cannot be delivered for any reason, you will not be notified of this failure.
- A good rule of thumb is that you do not modify the text of the email invitation, as editing the actual invitation URL within the subject text could break the link.

RESULT:

You have successfully invited a division to register for portal access.

MANAGING PRACTICES IN YOUR ORGANIZATION

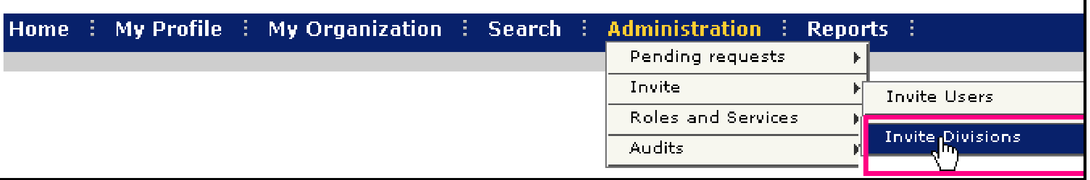
Invite Division (aka Practice) to Register for Access to the Portal

What is a Division?

A division is a part of your organization's hierarchy, such as a business unit, or practice. When inviting a division to your organization, it is important to understand that you are creating a hierarchy for your organization with a delegated administration model. This gives the security administrator of that division the authoritative power over the users of that division. Although the security administrator of the top level organization will still have authority over the users of the division all requests for services and new user accounts will be handled at the division level by the appropriate administrator. You should only create divisions in your organization if you believe your organization would benefit by delegating the administrative responsibilities to an entirely new organization (the division), which will be managed by its own administrators.

1. Click **Invite Division** from the **Administration -> Invite drop-down menu.**

Where is the Invite Divisions drop-down menu?



2.
3. Key in the *email address for each division's recipient* you wish to invite, **separated by semi-colon (;)**
4. Click **send invitation.**
5. Click **OK**.

- The system does not validate the accuracy of the email addresses that you key in. If an email invitation cannot be delivered for any reason, you will not be notified of this failure.
- A good rule of thumb is that you do not modify the text of the email invitation, as editing the actual invitation URL within the subject text could break the link.

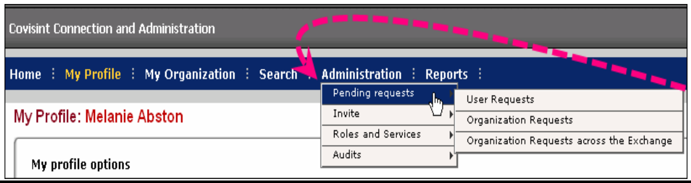
RESULT:

You have successfully invited a division to register for portal access.

Approve Practice's Service Package Request

1. Click **Organization Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration / Pending Requests drop-down menu?



2.

3. Click  next to the practice name.
4. Enable the ‘approve’ radio button next to the selected service package.
5. Click **submit decision**.
6. Click **OK**.

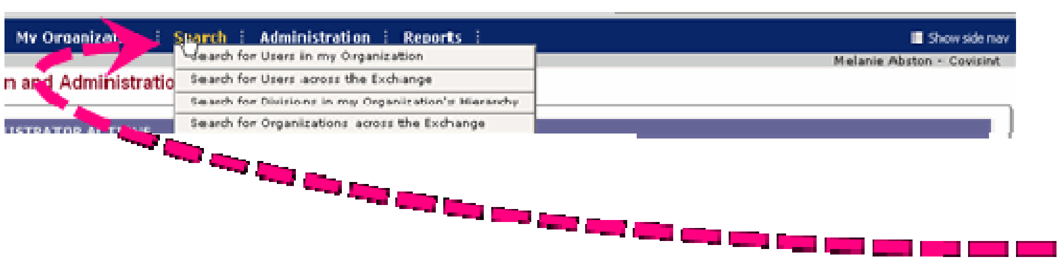
RESULT:

You have successfully approved a practice's service package request.

Edit Practice Profile

1. Click **Search for practices in my hierarchy** from the **Search drop-down menu**.

Where is the Search drop-down menu?



2. From the search results, click on the *practice name*.
3. Click **edit organization profile.**
4. Edit as necessary.
5. Click **save changes**.

RESULT:

You have successfully edited the profile of a practice.

Remove Service Packages from Practice

1. Click **Search for divisions in my organization hierarchy** from the **Search** drop-down menu.
2. Search for the practice from which you wish to remove a package.
3. From the search results, click on the *practice name*.
4. Click **view service packages** tab.
5. Click on the name of the service package you wish to remove.
6. Click
7. Click **add**.
8. Click **continue**.

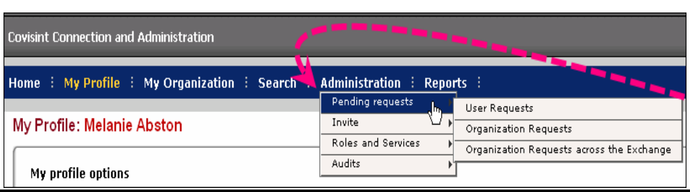
RESULT:

You have successfully granted service packages to a practice.

Permanently Remove Service Package from a Practice

1. Click **View my organization hierarchy** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration / Pending Requests drop-down menu?



2.
3. From the search results, click on the *practice name*.
4. Click **view service packages** tab.
5. Click on the *name of the service package* you wish to remove.
6. Click **permanently remove organization's grant for service package.**
7. Key in the *reason for removal* in the open text box.
8. Click **yes, proceed with removal.**

Once a service package is permanently removed from a practice, it can no longer be reinstated.

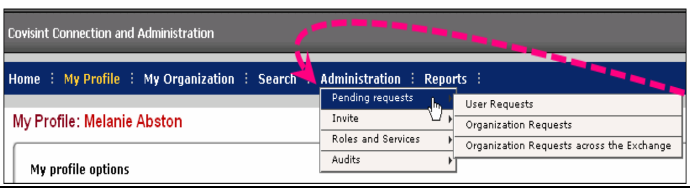
RESULT:

You have successfully removed a service package from a practice.

Reject Practice’s Service Package Request

1. Click **Organization Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration / Pending Requests drop-down menu?



2.
3. Click next to the practice name.
4. Enable the ‘reject’ radio button next to the selected service package.
5. Key in the *rejection reason* in the open text box.
6. Click **submit decision.**
7. Click **OK.**

RESULT:

You have successfully rejected a practice's service package request.

Suspend a Service Package from a Practice

1. Click **View my organization hierarchy** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?

2. From the search results, click on the *practice name*.
3. Click **view service packages** tab.
4. Click on the *name of the service package* you wish to suspend.
5. Click **suspend.**

Where is the Suspend link?

6.
7. Key in the reason for suspension in the open text box.
8. Click **yes, proceed with suspension.**

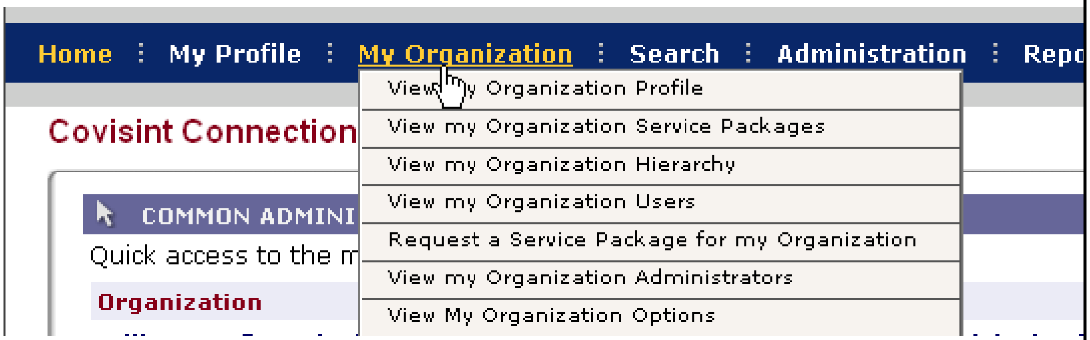
RESULT:

You have successfully suspended a service package from a practice.

View Practice Administrators

1. Click **View my Organization Profile** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?



2. Click the **view hierarchy** tab.
3. Click on the *name of the practice.*
4. Click **view administrator** tab. All administrators in the selected practice are displayed.

RESULT:

You have successfully viewed practice administrators.

View Practice Grant History

1. Click **View my organization hierarchy** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?

2. From the search results, click on the *practice name.*
3. Click **view grant history.**

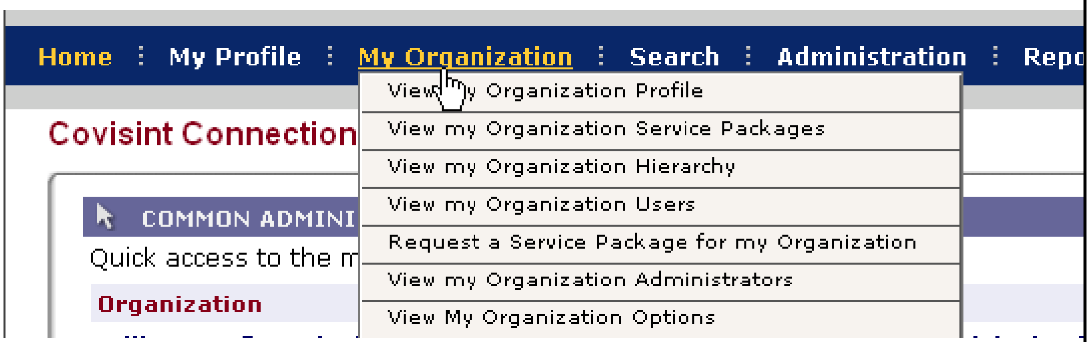
RESULT:

You have successfully viewed the grant history of a practice.

View Practice Hierarchy

1. Click **view my organization hierarchy** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?



2. Click on the *name of the practice*. The practice hierarchy is displayed.

RESULT:

You have successfully viewed the hierarchy of a practice.

View Practice Request History

1. Click **View my organization hierarchy** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?

2. From the search results, click on the *practice name.*
3. Click **view request history.**

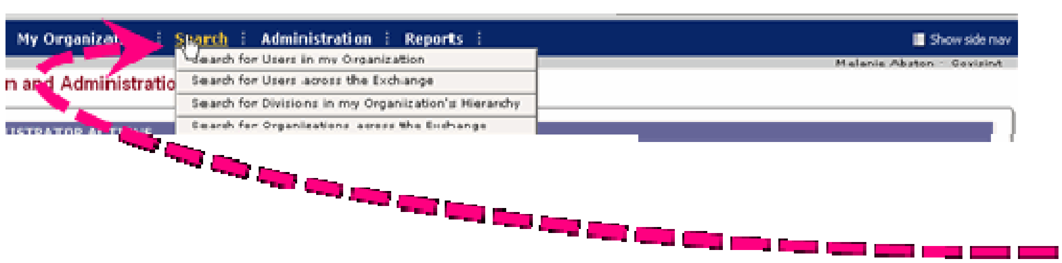
RESULT:

You have successfully viewed the request history of a practice.

View Practice Service Packages

1. Click **Search for practices in my hierarchy** from the **Search drop-down menu**.

Where is the Search drop-down menu?



2. From the search results, click on the *practice name.*
3. Click **view service packages** tab.

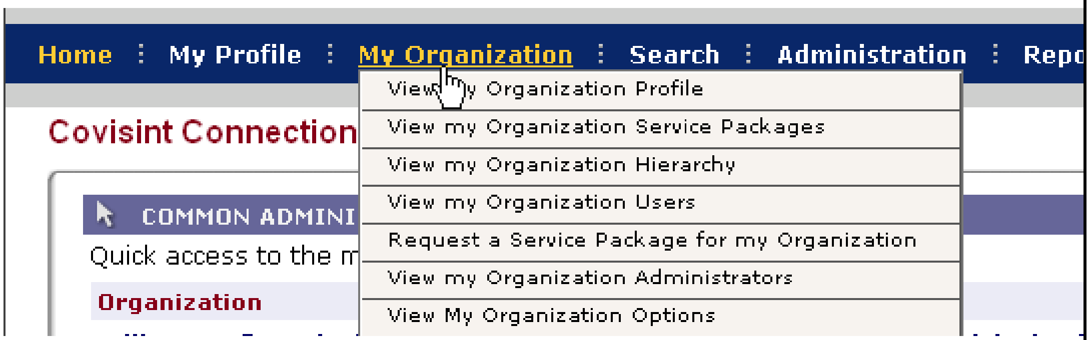
RESULT:

You have successfully viewed service packages of a practice.

View Users in a Practice

1. Click **View my Organization Profile** from the **My Organization drop-down menu**.

Where is the My Organization drop-down menu?



2. Click the **view hierarchy** tab.
3. Click on the *name of the practice.*
4. Click **view user** tab. All users registered in the selected practice are displayed.

RESULT:

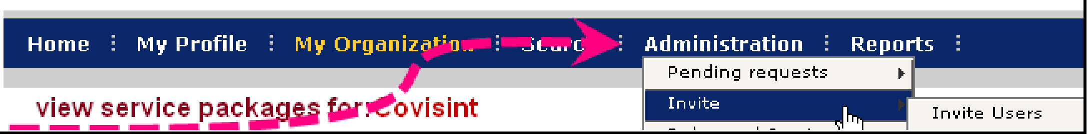
You have successfully viewed all users in a practice.

DIVISION (AKA PRACTICE) ADMINISTRATORS

Invite User to Register for Access to the Portal

1. Click **Invite Users** from the **Administration -> Invite drop-down menu**.

Where is the Administration / Invite drop-down menu?



2. Key in the *email address for each recipient* you wish to invite, **separated by semi-colon (;)**
3. Click **send invitation.**
4. Click **OK**.

- The system does not validate the accuracy of the email addresses that you key in. If an email invitation cannot be delivered for any reason, you will not be notified of this failure.
- A good rule of thumb is that you do not modify the text of the email invitation, as editing the actual invitation URL within the subject text could break the link.

RESULT:

You have successfully invited a user to register for portal access.

What happens next?

- User will receive the invitation via email, and complete the steps for registration.
- You will receive an email regarding the user's pending request after the user submits the registration request.
- Approve the user request
- Optionally, grant service packages
- Optionally, modify user roles

Approve Pending New User Request

1. Click **User Requests** from the Administration -> Pending requests drop-down menu.
2. Click to view details of request.
3. Enable the 'approve' radio button.
4. Click **submit decision**.
5. Click **OK**.

If your organization also uses the IDcipher™ card in addition to a user name and password for authentication, then the system will automatically generate and email an IDcipher™ card to the user upon your new user request approval.

RESULT:

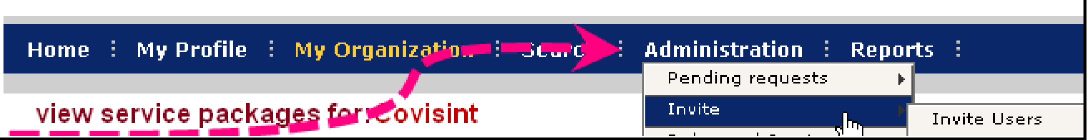
You have successfully approved a pending account request. The user will receive an email notification regarding this approval, along with an IDcipher™ card, if applicable.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

Reject Pending New User Account Requests

1. Click **User Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration / Pending requests drop-down menu?



2.

3. Click to view details of request.
4. Enable the 'reject' radio button.
5. Key in the *rejection reason* in the open text box.
6. Click **submit decision**.
7. Click **OK**.

When you reject a new user request, all service package requests for that user are automatically rejected.

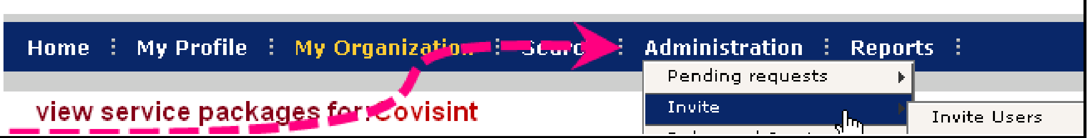
RESULT:

You have successfully rejected a pending request for a new user account. The user is notified via email of this decision.

Approve User's Pending Service Package Request

1. Click **User Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration / Pending requests drop-down menu?



2.
3. Click the **User Service Package** tab.
4. Click to view details of request.
5. Enable the 'approve' radio button.
6. Click **submit decision.**
7. Click **OK**.

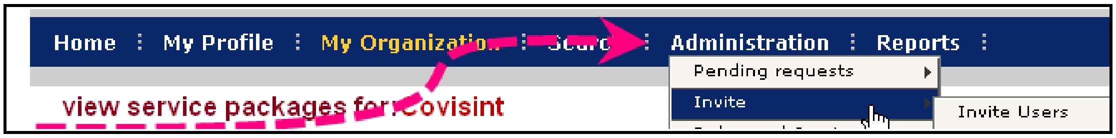
RESULT:

You have successfully approved a user's service package request.

Reject User's Pending Service Package Request

1. Click **User Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration / Pending requests drop-down menu?



2.
3. Click the **User Service Package** tab.
4. Click to view details of request.
5. Key in the *rejection reason* in the open text box.
6. Enable the ‘reject’ radio button.
7. Click **submit decision.**
8. Click **OK**.

RESULT:

You have successfully rejected a user's request for service package(s).

Search for Users in My Organization

1. From the **Search drop-down menu**, click **Search for Users in my Organization.**

Where is the Search drop-down menu?

2. Select search criteria.
3. Click **Search**.

RESULT:

You have successfully searched for users in your organization

Grant Service Package to User

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **add service package.**
4. Enable the checkbox of each service package you wish to grant to this user.
5. Click **add checked...**
6. Click **continue.**
7. Click **submit.**

Some service packages are not grantable.

RESULT:

You have successfully granted a service package to a user.

Suspend a Service Package from User

1. Search and select the name of the user for whom you wish to suspend a service package.
2. Click on the *name of the service package*.
3. Click **suspend**.
4. Key in the *suspension reason.*
5. Click **yes, proceed with suspension.**

RESULT:

You have successfully suspended a service package. You are also able to permanently remove the service package, or to unsuspend it.

Unsuspend a User's Service Package

1. Perform a user search.
2. From the search results, click on the *name of the user*.
3. Click on the *name of the service package* you wish to unsuspend.

4. Click **unsuspend.**
5. Key in the *reason for activating the service package for this user* in the open text box.
6. Click **yes, activate service package..**

RESULT:
You have successfully unsuspended a user's service package.

Permanently Remove Service Package from User

A Service Package must be suspended before it can be permanently removed from a user.

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **view service packages** tab.
4. Click on the *name of the service package* you wish to remove.
5. Click **permanently remove service package**.
6. Key in the *reason for removing package.*
7. Click **continue**. The package is removed.

RESULT:
You have successfully removed a service package from a user.

Modify a User's Role

Please review the details when on assigning the Health Exchange Role Manager in the topic Managing the Health Exchange Role Manager role.

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **modify roles.**

4. Enable the checkbox of each role you wish to grant to the user.
5. Click **submit**.
6. Click **OK**.

RESULT:

You have successfully modified a user's role.

Edit a User's Profile

1. Perform a user search.
2. From the search results, click on the *name of the user*.
3. Click **edit user profile**.
4. Modify the profile as necessary.
5. Click **Save changes.**

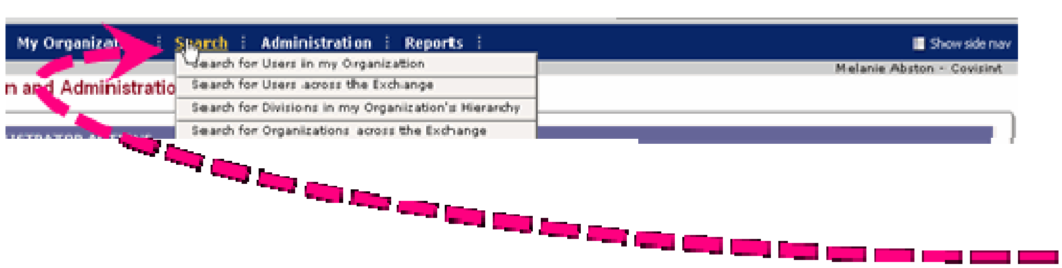
RESULT:

You have successfully edited a user's profile.

Edit Practice Profile

1. Click **Search for practices in my hierarchy** from the **Search drop-down menu**.

Where is the Search drop-down menu?



2. From the search results, click on the *practice name*.
3. Click **edit organization profile.**
4. Edit as necessary.
5. Click **save changes**.

RESULT:

You have successfully edited the profile of a practice.

Suspend a User's Account

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **suspend user**.
4. Key in the *reason for suspending the account* in the open text box.
5. Click **yes, suspend user.**

RESULT:

You have successfully suspended a user's account.

Unsuspend a User's Account

1. Perform a user search.
2. From the search results, click on the *name of the user*.
3. Click **unsuspend user.**
4. Key in the *reason for activating the user account* in the open text box.
5. Click **yes, activate user.**

RESULT:

You have successfully unsuspended a user's account.

Permanently Remove a User Account

1. Perform a user search. The user must be Suspended before the user can be permanently removed. Follow the steps in the section Suspend a User's Account if you have not already done so.

2. From the search results, click on the *name of the user.*
3. Click **permanently remove user.**
4. Key in the *reason for removing the user account* in the open text box.
5. Click **yes, permanently remove user.**

Once a user is permanently removed, that user can not be reactivated, and the user's id can never be reused.

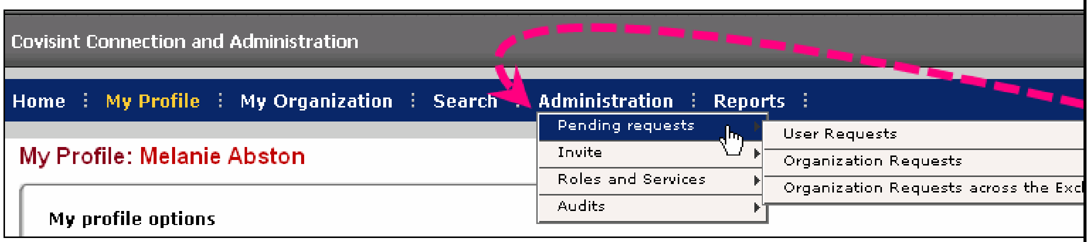
RESULT:

You have successfully permanently removed a user account.

Approving NPI Code Requests Received from a Practice in My Organization

1. Click **Organization Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration -> Pending requests drop-down menu?



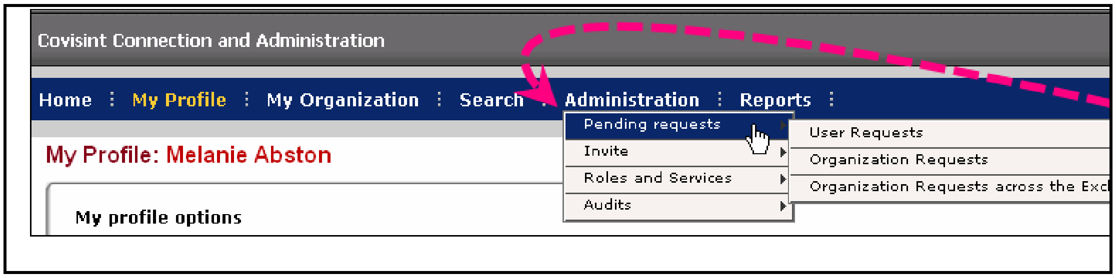
2. Click **Site codes** tab.
3. Click  (the view request icon).
4. Enable the *approve* radio button.
5. Click **submit decision**.
6. Click **OK**.

RESULT:
You have successfully approved an NPI Code request from a practice.

Approving NPI Code Requests Received from My Users

1. Click **User Requests** from the **Administration -> Pending requests drop-down menu**.

Where is the Administration -> Pending requests drop-down menu?



2. Click **User Site codes** tab.
3. Click (the view request icon).
4. Enable the *approve* radio button.
5. Click **submit decision**.
6. Click **OK**.

RESULT:

You have successfully approved an NPI Code request from a user.

How do I Request Access to an NPI Code?

As a user, request access to an NPI code by following the steps for Requesting Service Packages.

As a practice, request access to an NPI code for your practice by following the steps in Requesting Service Package for your Organization

Remember, you must have access to HAP in order to view NPI codes. If you have already been approved for HAP, simply request the NPI codes. If you are not yet approved for HAP, request the HAP service package when you request NPI code access.

I am an Administrator, and I need to Grant NPI Codes to Practices/Users Within My Organization. How Do I Do That?

NPI codes cannot be auto-granted to practices/users within your organization.

The practice/user must request the NPI code, and you can then approve that practice/user request. **Remember, your practices/users must also have access to HAP in order to view NPI codes**. If the practice/user has not yet been approved for HAP, grant the HAP service package when you approve the NPI code access.

My NPI Code Access Request was Approved, but I Still Cannot Log in to HAP

In order to view your approved NPI codes in HAP, you must also be approved for HAP. Request access to HAP by following the steps for "Requesting Service Packages”.

REPORTS - SECURITY ADMIN

Security Administrator Reports

If your role is that of Service Administrator, proceed to Service Administrator Reports

User Summary

The User Summary report allows you to gain at-a-glance information regarding the number of users in your organization and the corresponding status. The report will display the number of pending, rejected, active, suspended and removed users.

User Service Summary

The User Service Summary report allows you to gather information about the numbers and identities of users who have been granted various service packages. You can limit your search to your own organization, or you can broaden it to include all users above or below your organization in your company's hierarchy. You can select a service package to narrow your results to all users with a specific service package or you can search for all users with all service packages. The report displays the User ID, Last Name, First Name, Email Address and Company/Division name of all users who meet the report criteria.

Service Summary

The Service Summary report allows you to gather information about the numbers and identities of users who have been granted various service packages.

Security Administrator

The Security Administrator reports offer three outcomes, including a user report, a service package grant report, and a user portal access by site code report. These reports allow you to gather information about the numbers and identities of users who have been granted various service packages.

Quarterly User Audits

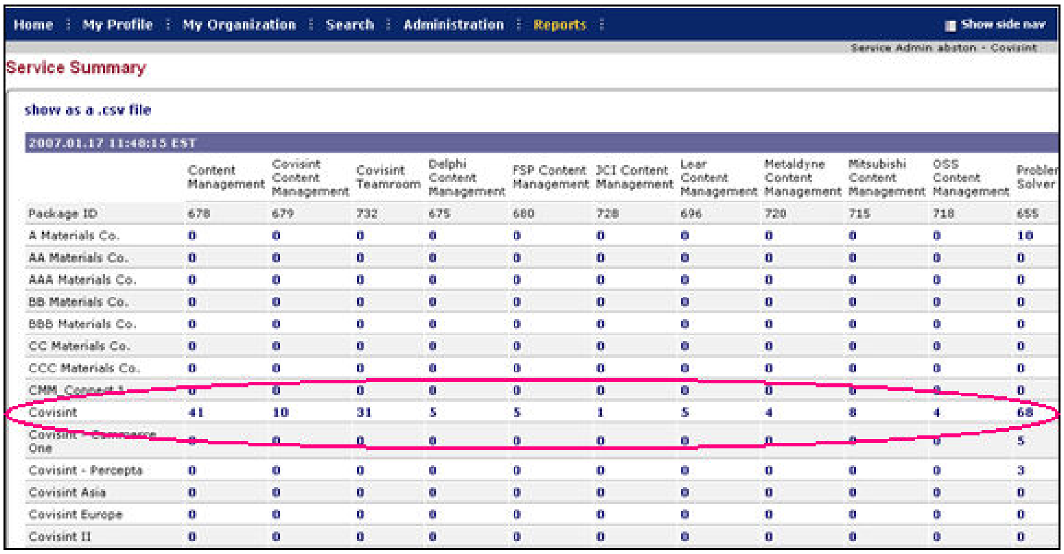
A quarterly audit reminder will be emailed to all Security Administrators reminding them to perform the necessary audit activities. You can view your audit history on the Quarterly User Grant Audit page. The audit history records the date, the type of audit, and the auditor's ID for past audits.

Annual User Audits

An annual User Grant audit reminder will be emailed to all Security Administrators reminding them to perform the User Grant audit. You can view your audit history on the Annual User Grant Audit page. The audit history records the date, the type of audit, and the auditor's ID for past audits.

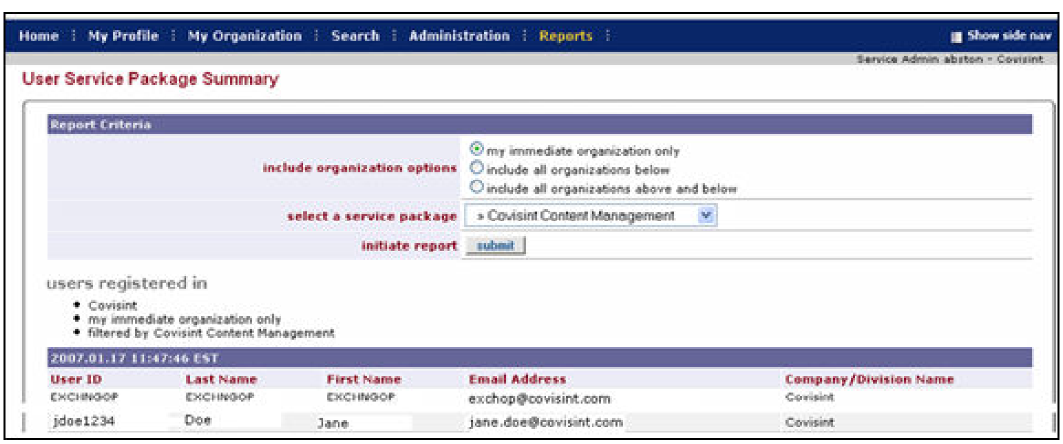
Generate a Service Summary Report

1. Click **Service Summary** from the Reports drop down menu. The Service Summary screen is displayed.



	Content Management	Covisint Content Management	Covisint Teamroom	Delphi Content Management	FSP Content Management	JCI Content Management	Lear Content Management	Metaldyne Content Management	Mitsubishi Content Management	OSS Content Management	Problem Solver
Package ID	678	679	732	675	680	728	696	720	715	718	655
A Materials Co.	0	0	0	0	0	0	0	0	0	0	10
AA Materials Co.	0	0	0	0	0	0	0	0	0	0	0
AAA Materials Co.	0	0	0	0	0	0	0	0	0	0	0
BB Materials Co.	0	0	0	0	0	0	0	0	0	0	0
BBB Materials Co.	0	0	0	0	0	0	0	0	0	0	0
CC Materials Co.	0	0	0	0	0	0	0	0	0	0	0
CCC Materials Co.	0	0	0	0	0	0	0	0	0	0	0
CMM_Connect 1	0	0	0	0	0	0	0	0	0	0	0
Covisint	41	10	31	5	5	1	5	4	8	4	68
Covisint - Commerce One	0	0	0	0	0	0	0	0	0	0	5
Covisint - Percepta	0	0	0	0	0	0	0	0	0	0	3
Covisint Asia	0	0	0	0	0	0	0	0	0	0	0
Covisint Europe	0	0	0	0	0	0	0	0	0	0	0
Covisint II	0	0	0	0	0	0	0	0	0	0	0

2. View the number of users by service package type. For example, in the Covisint organization, you see that there are 41 users of Content Management, 10 users of Covisint Content management, 31 users of Covisint Teamroom, etc.
3. If desired, click on the number in the column of the Service Package to view additional details. (This example users the number "10" in the Covisint Content Management column). The Details Summary screen is displayed in a separate window.



4. From this view, you are able to view all users in your immediate organization that are able to access this service package. (This is essentially the same output as the user service package grant report).
    a. If you wish to filter the results to view only users in organizations 'below' yours in the hierarchy, enable the radio button next to 'include all organizations below'.
    b. If you wish to filter the results to view all organizations above and below yours in the hierarchy, enable the radio button next to 'include all organizations above and below'.
    c. Optionally, you may select a different service package from the dropdown menu.
    d. Click **Submit**. The screen refreshes and results are displayed.

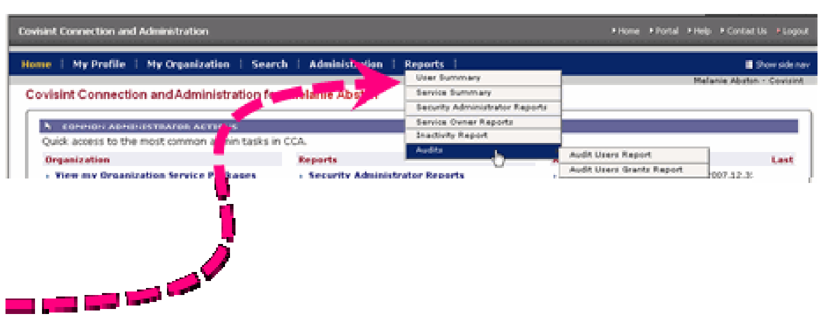
RESULT:

You have successfully generated a service summary report.

Generate a User Report

1. Click **Security Administrator Reports** from the **Reports drop-down menu**.

Where is the Reports drop-down menu?



2. Click **User Reports.** The User Reports screen is displayed.

3. Configure the filters for the report enabling the appropriate radio button for each required field, including:
   a. Organization options – (determines where in the hierarchy you wish to obtain information, for your immediate organization only, or all organizations below yours)
   b. Sort by – (determines how you want the report sorted, by user last name, or user id)
   c. Results – (determines how you wish to view the generated report)
4. Click **Submit**.

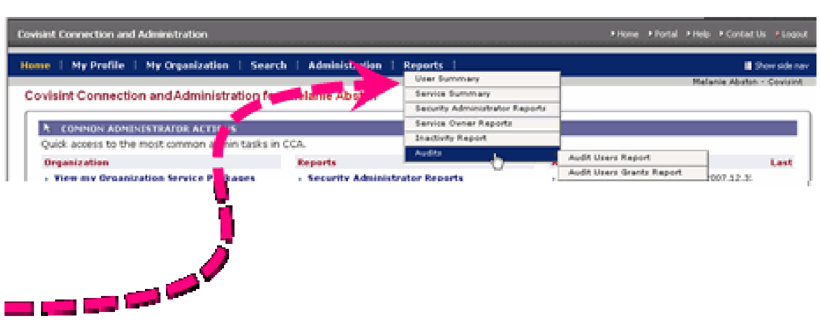
RESULT:

You have successfully generated a user report.

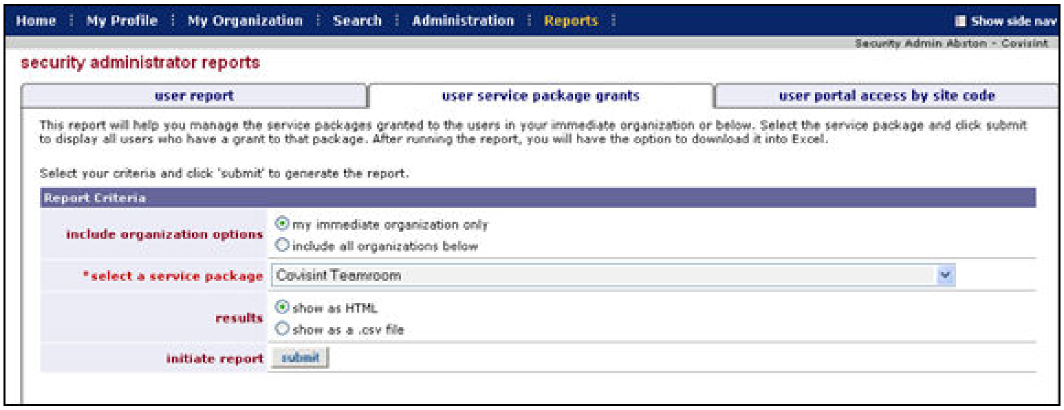
Generate a User Service Package Grant Report

1. Click **Security Administrator Reports** from the **Reports drop-down menu**.

Where is the Reports drop-down menu?



2. Click **user service package grants**. The User Service Package Grants Reports screen is displayed.



3. Configure the filters for the report by selected an option for each required field, including:
   a. Organization options – (determines where in the hierarchy you wish to obtain information, for your immediate organization only, or all organizations below yours)
   b. Select a service package – (from the drop down list, click the service package for which you wish this report to generate)
   c. Results – (determines how you wish to view the generated report)
4. Click **Submit**.

RESULT:

You have successfully generated a user service package grant report.

Generate a User Service Summary Report

If you wish to…	Then…
view only users in your immediate organization,	1. Click **Reports.** The Report Options screen is displayed. 2. Click **User Service Summary**. The User Service Package Summary screen is displayed. 3. Enable the radio button next to 'include all organizations below'. 4. Select the service package for which you wish to view users from the dropdown menu. 5. Click **submit**. The screen refreshes and results are displayed.
view only users in organizations 'below' yours in the hierarchy,	1. Click **Reports**. The Report Options screen is displayed. 2. Click **User Service Summary**. The User Service Package Summary screen is displayed. 3. Enable the radio button next to 'include all organizations below'. 4. Select the service package for which you wish to view users from the dropdown menu. 5. Click **submit**. The screen refreshes and results are displayed.
view only users in organizations 'above and below' yours in the hierarchy,	1. Click **Reports**. The Report Options screen is displayed. 2. Click User Service Summary. The User Service Package Summary screen is displayed. 3. Enable the radio button next to 'include all organizations above and below'. 4. Select the service package for which you wish to view users from the dropdown menu. 5. Click **submit**. The screen refreshes and results are displayed.

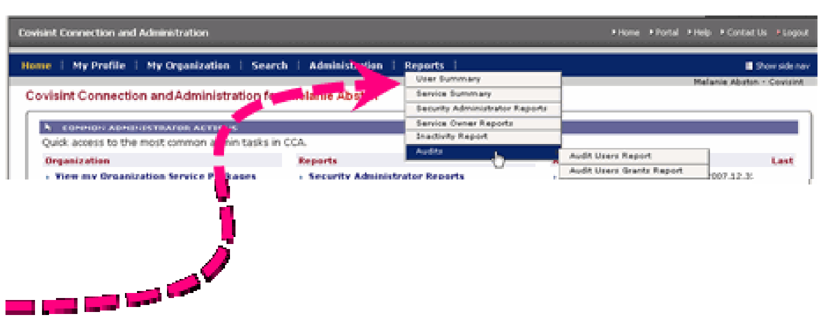
RESULT:

You have successfully generated a user service summary report.

Generate a User Summary Report

1. Click **User Summary** from the **Reports drop-down menu**. The User Summary screen is displayed as an html report for your organization.

Where is the Reports drop-down menu?



2. View the *number of users by status type*.
3. If desired, click on the *name of a division* in the organization by clicking on the division name. The profile screen is displayed in a separate window.
4. If you wish to view this report as a .csv file, click show as .csv file in the upper left corner of the screen. An open file dialog box is displayed.
5. Identify if you wish to open the file or save the file to disk by clicking the appropriate radio button.
6. Click **OK**.

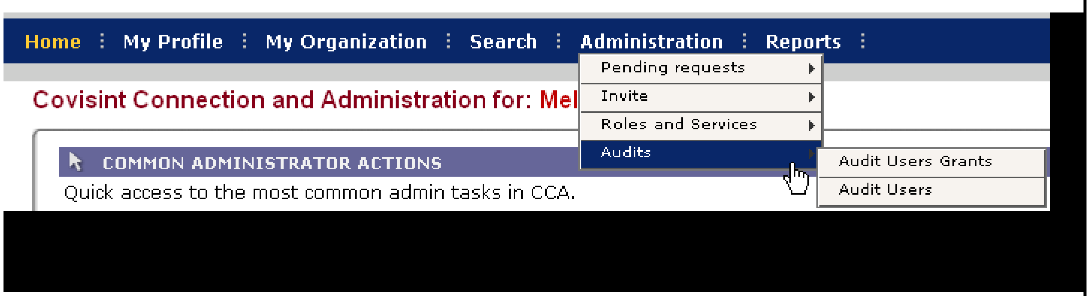
RESULT:

You have successfully generated a user summary report.

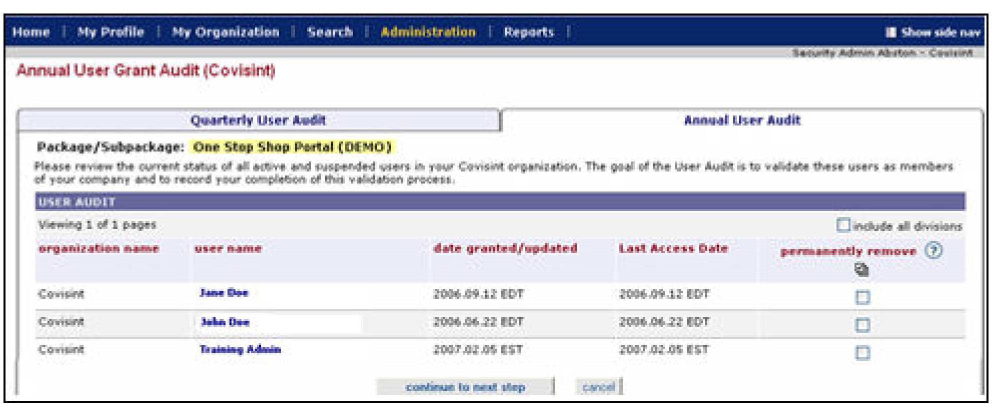
Perform Annual User Audits

1. From the **Administration menu**, click **Audits**.

Where is the Administration drop-down menu?



2. Click **Annual User Audits** from the Audits drop down menu. The Annual User Audit screen is displayed.
3. Click on one *service package name* to view a list of users in your organizations that have access to the service.



4. Optionally, you can click the *show all divisions* checkbox to conduct the audit for all organizations at or below your organization in your organization's hierarchy.
5. Enable the checkbox of each service you wish to permanently remove from the targeted user.
6. Click **continue to next step**.
7. Repeat steps 4 – 7 to verify the grants for each additional service package.
8. Perform one of the following:
   a. Click **confirm and log audit completion** if you have finished your audit.
   b. Click **audit another package** if you need to audit users in an additional service package
   c. Click **I will log my compliance later** if you are not finished and wish to save your audit at this point and finish the audit at a later time.

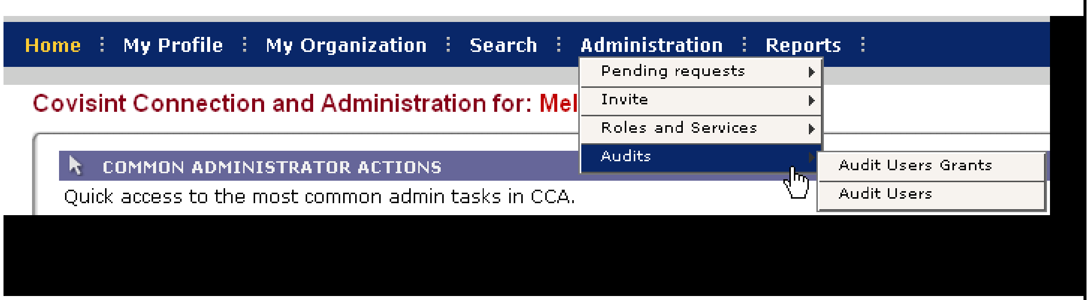
RESULT:

You have successfully performed an annual user audit.

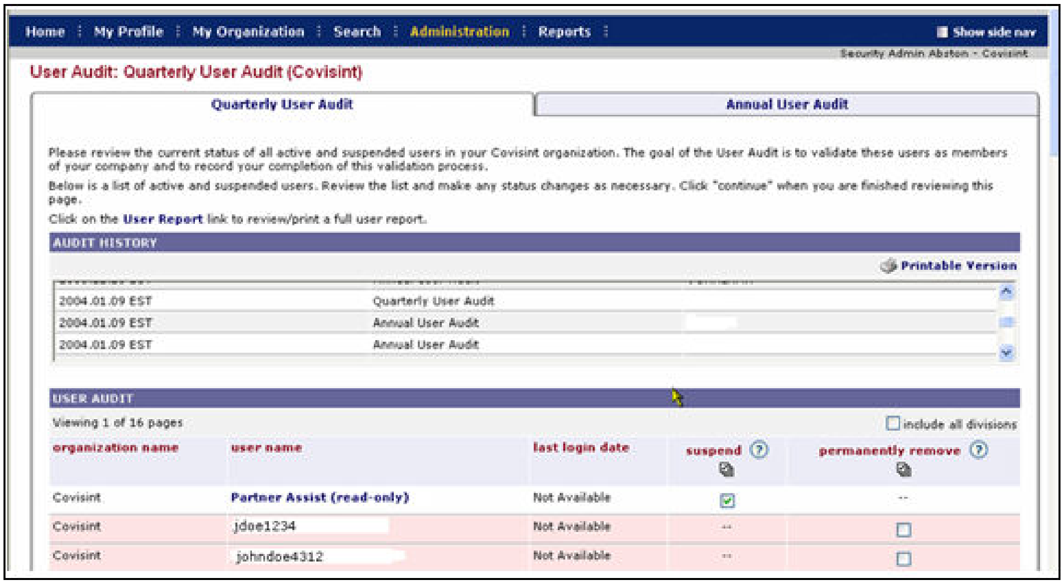
Perform Quarterly User Audits

1. From the **Administration menu**, click **Audits**.

Where is the Administration drop-down menu?



2. Click **Quarterly User Reports** from the Audits drop down menu. The User Audit screen is displayed.
3. Review the list of all users in the organization that is displayed. (Note: Enabling the *include all divisions* check box will enable you to audit all organizations at your level or below on your company's hierarchy tree).



4. Enable the checkbox in the Suspend or Permanently Remove column of each user on the list as necessary. (Note: A user must be 'suspended' before the user can be 'permanently removed').
5. Key in the *reason for suspension or permanent removal* in the open text box. (Note: A default suspension/permanent removal reason will auto-populate).
6. Optionally, enable the checkbox if you choose to send an email to the user(s) notifying them of the change in their account status.
7. After you have examined each page of the audit, confirm the audit and log completion on the last screen by clicking **confirm and log audit completion.**

RESULT:

You have successfully performed quarterly user audits.

SERVICE ADMIN - REPORTS

Service Administrator Reports

If your role is that of Security Administrator, proceed to Security Administrator Reports

Summary Report

The Summary report allows you to gather information about the numbers and identities of users who have been granted various service packages. You can select a service package to narrow your results to all users with a specific service package or you can search for all users with all service packages. The report displays the Service Package name, total user count, total organization count, and total unique parent code count.

User Details Report - as HTML or .CSV File

The User Details report allows you to gather information about the numbers and identities of users who have been granted various service packages and can be filtered by location code. The report displays the User SSO ID, last and first name, email address, location code, and organization / division per user.

Administrator Details Report

The Administrator Details report is designed to provide the service owner with a list of supplier administrators who have the ability to grant user's access to their service. This report may be useful for sending communications to these administrators.

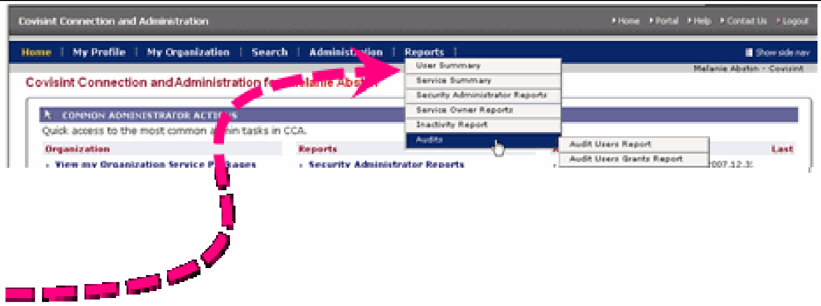
The report may be broken out by administrator type. The security administrator has a larger set of administrative privileges than the service administrator.

To locate the administrators for a single parent supplier code, please enter the full parent supplier code. Although the code is not case sensitive, the search will otherwise look for an exact match of the code entered

Generate a Summary Report

1. Click **Service Owner Reports** from the **Reports drop-down menu**.

Where is the Reports drop-down menu?



2. Click **Summary Report** tab.
3. Select a *service package* in the service package drop-down menu, if desired.
4. Enable the radio button to indicate how you wish to view the results, either HTML or as a .CSV file.
5. Click **submit**. The report displays the total user count, total Covisint organization count, and total unique parent supplier code count for a given service package.

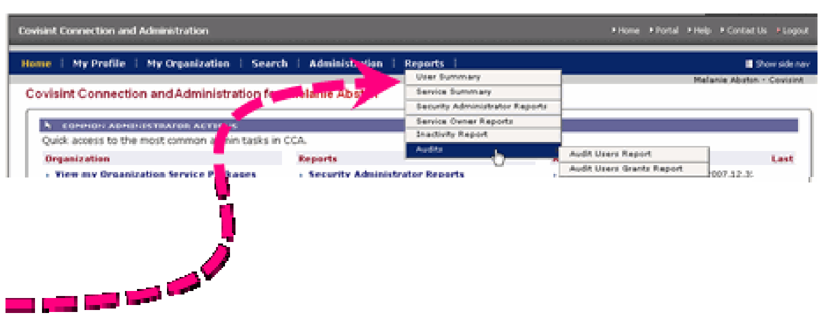
RESULT:

You have successfully generated a Summary report.

Generate a User Detail Report (View as .CSV File)

1. Click **Service Owner Reports** from the **Reports drop-down menu**.

Where is the Reports drop-down menu?



2. Click **user details report** tab.
3. Select a *service package* in the service package drop-down menu, if desired.
4. Optionally, you may narrow the results by identifying the User Location code.
5. Enable the **show as a .csv file** radio button to view the results.
6. Click **submit**.

7. Click **Open in Excel**. Once the data is opened in Excel, you are able to manipulate it to show the data in the manner that is important to you.
   A common use of data is to obtain user count by organization / division. This example is described below:
    1. In the Excel spreadsheet, from the Data drop down menu, click **Sort**.
    2. Sort by the "Company/Division Name" column
    3. From the Data drop down menu, click **Subtotals**.
    4. Select each of the following where prompted:
        a. **At each change in:** Company/Division Name
        b. **User Function:** Count
        c. **Add subtotal to:** <Select just one item from the list, default might be fine>
    5. Click **OK**.
    6. Optionally, if you wish to view only the totals you can collapse the report by selecting the "2" on the left side of the screen just above the first row of the spreadsheet display.

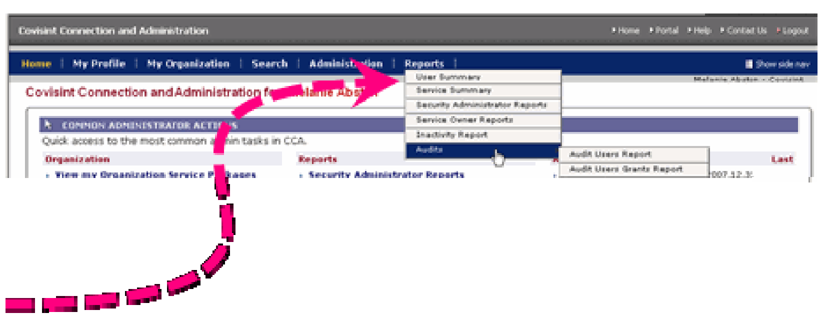
RESULT:

You have successfully generated a User Detail report to view as a .csv file.

Generate a User Detail Report (View in HTML)

1. Click **Service Owner Reports** from the **Reports drop-down menu**.

Where is the Reports drop-down menu?



2. Click **user details report** tab.
3. Select a *service package* in the service package drop-down menu, if desired.
4. Optionally, you may narrow the results by identifying the User Location code.
5. Enable the **HTML** radio button to view the results.
6. Click **submit**.

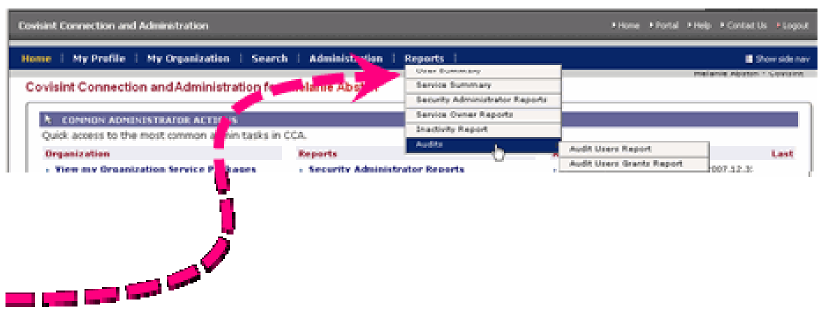
RESULT:

You have successfully generated a User Detail report to view in HTML.

Generate an Administrator Detail Report

1. Click **Service Owner Reports** from the Reports **drop-down menu**.

Where is the Reports drop-down menu?



2. Click **administrator details report** tab.
3. Select a service package in the drop-down menu.
4. Optionally, you may narrow the results by identifying the parent supplier code.
5. Select the *type of administrator* you wish to view in the drop down menu.
6. Enable the radio button to indicate how you wish to view the results, either HTML or as a .CSV file.
7. Click **submit**. The report displays the Organization's name, parent code, and administrator name and contact information for a given service package.

RESULT:

You have successfully generated an Administrator Detail report.

PREMIUM SERVICE: HEALTH EXCHANGE ROLES

Premium Service: Health Exchange Roles

Health Exchange Roles Management is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details on purchasing and enabling Health Exchange Roles Management.

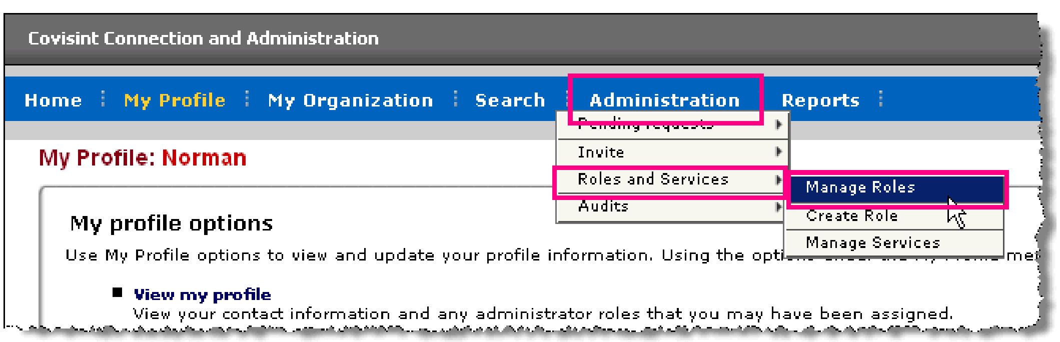
Two categories of roles are managed within the Administration tool. Those are:

- Covisint Connection and Administration (CCA) Administrator roles Security Administration roles (all portal customers)
- Health Exchange Roles (when purchased / enabled by portal customers)

Health Exchange roles allow a Health Exchange Role Manager to create a role based on task-oriented privileges for portal users where the Administrator can control what those users are able to see and do based on privileges selected for inclusion in the role. Roles and privileges, in conjunction with existing service package grants help to achieve fine-grained access control at the application, feature, and data source levels within a portal.

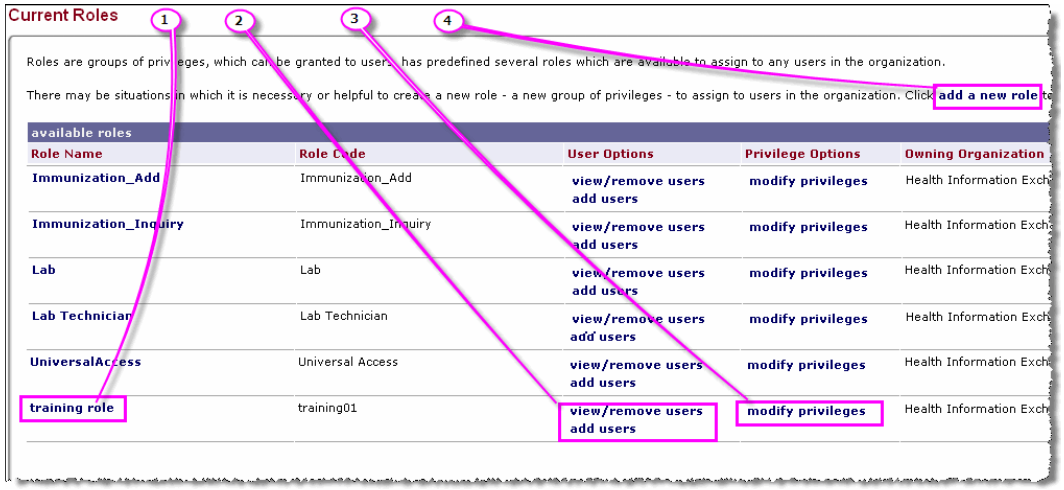
Health Exchange roles are not tied to Administrator roles. The Health Exchange role is owned by the organization that owns the Health Exchange Portal, (GTHAN in this case). The Health Exchange Role Manager (i.e. the administrator of the owning organization) is able to define Health Exchange roles for the Health Exchange Portal. Those roles can only assigned to the users who have the Health Exchange Portal grant.

View Health Exchange Role Details

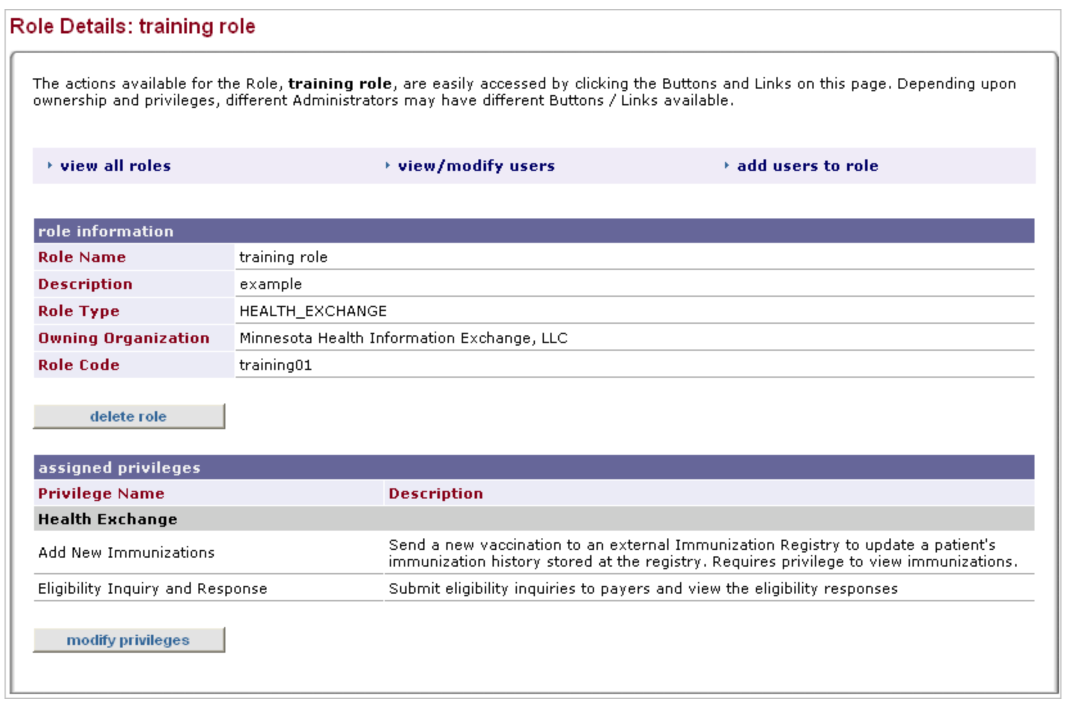


1. From the **Administration** menu, click **Roles and Services.**

2. Click **Manage Roles**. A list of current roles is displayed.



3. Click on the *name of the role* (1) to view details of that role.



4. From this screen you are able to:
   - view / remove users assigned to the role
   - add users to the role
   - delete the role from the system

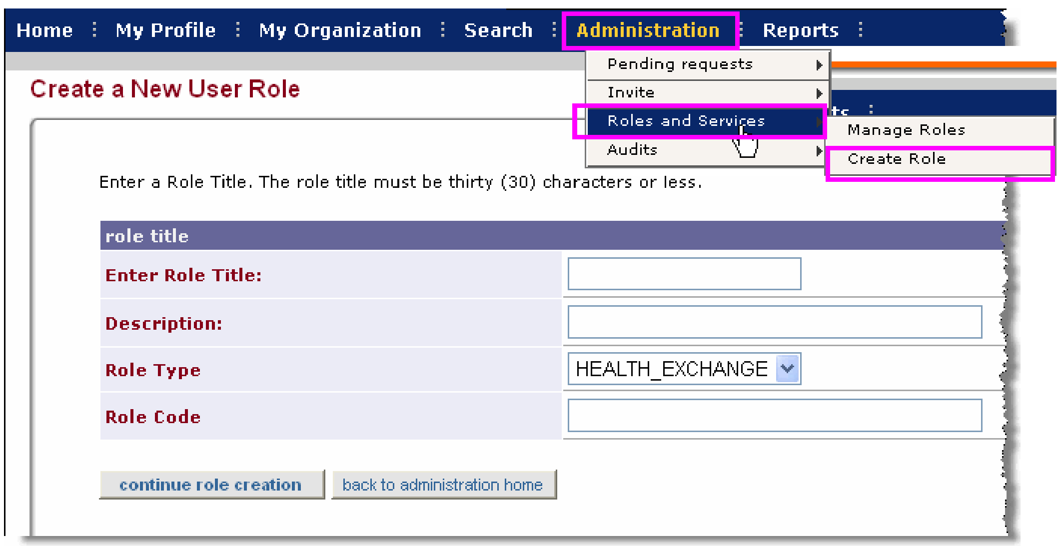
- modify privileges of the role

RESULT:

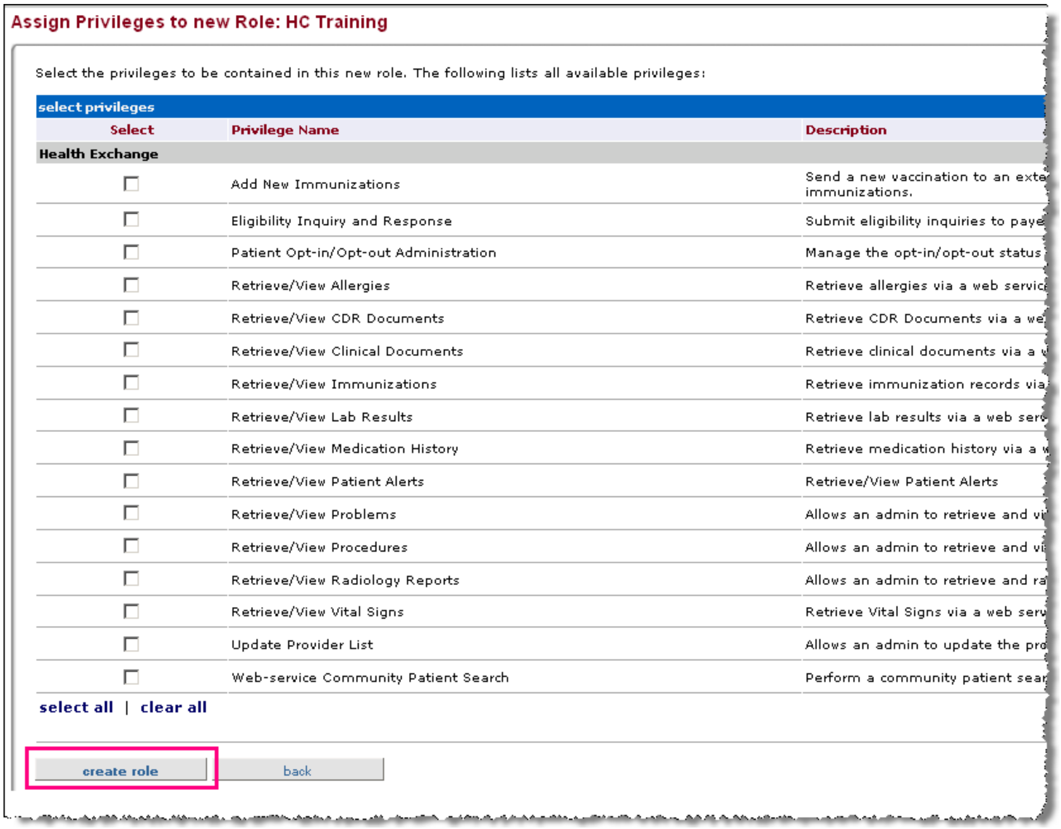
You have successfully viewed details of a Health Exchange role.

Create Health Exchange Role

Before creating a new Health Exchange Role, verify that the role with associated privileges does not already exist by viewing Health Exchange Role details.



1. From the **Administration** menu, click **Roles and Services.**
2. Click **Create Role**.
3. Key in the *Role Title* in the open text field.
4. Key in a *description* of the role in the open text field.
5. Select the *Role Type* from the drop down menu.
6. Optionally key in the ***Role Code*** in the open text field.
7. Click **continue role creation**. The Assign Privileges to Role screen is displayed. (The list of privileges displayed may vary based on your organization's implementation.)



8. Enable the checkbox of each ***privilege*** combination you wish to associate to the role.

Certain privileges must be combined with other privileges in order to provide full functionality, as identified below:

Privilege	Must Also Assign:
Add New Immunizations	+ Retrieve/View Immunizations + Retrieve/View CDR Documents
Eligibility Inquiry and Response	Not applicable
Patient Opt-In/Op-Out Administration	None
Retrieve/View Allergies	+ Retrieve/View CDR Documents
Retrieve/View Clinical Documents	+ Retrieve/View CDR Documents
Retrieve/View Immunizations	+ Retrieve/View CDR Documents
Retrieve/View Lab Results	+ Retrieve/View CDR Documents
Retrieve/View	+ Retrieve/View CDR Documents

Medication History	
Retrieve/View Patient Alerts	+ Retrieve/View CDR Documents
Retrieve/View Problems	+ Retrieve/View CDR Documents
Retrieve/View Procedures	+ Retrieve/View CDR Documents
Retrieve/View Radiology Reports	None
Retrieve/View Vital Signs	+ Retrieve/View CDR Documents
Update Provider List	None
Web-service Community Patient Search	Not applicable for GTHAN

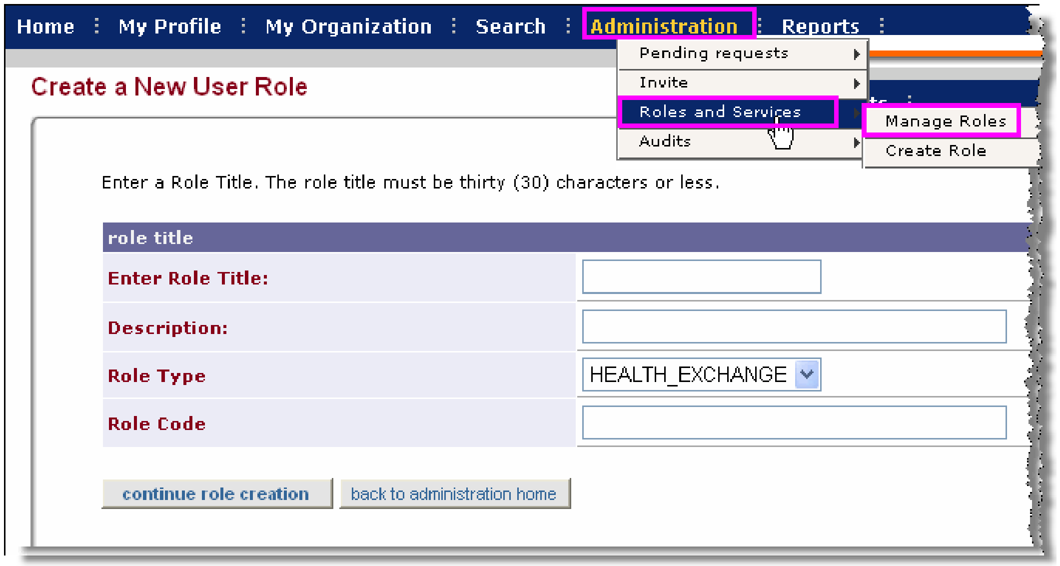
9. Click **create role**. The role is created and the Role Details screen is displayed.

RESULT:

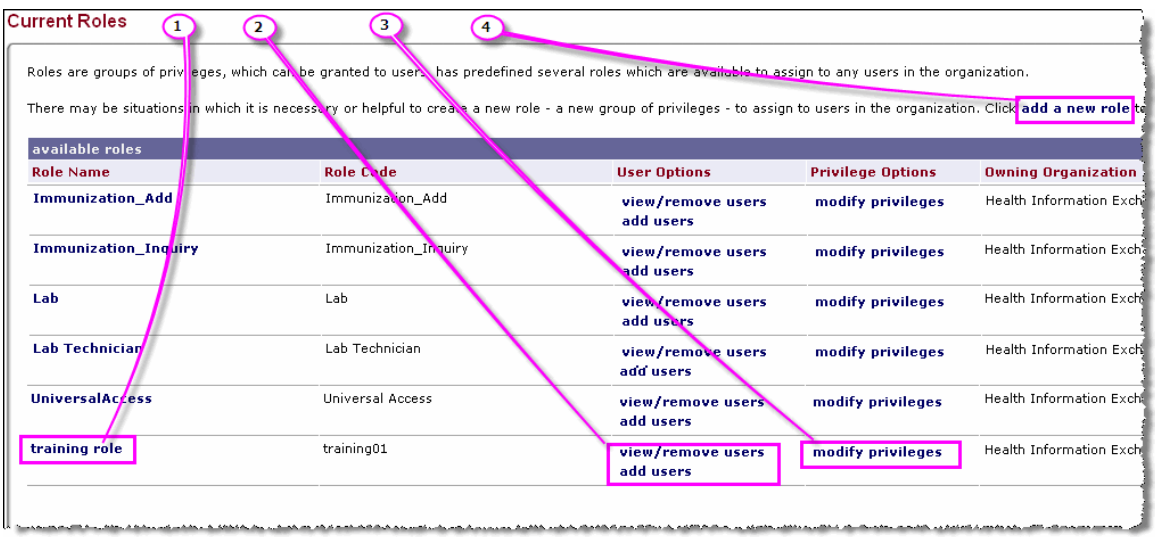
You have successfully created a role. Next, assign the role to users >>>

Modify Privileges of a Health Exchange Role

Before modifying privileges of an existing role, review the required privilege combinations chart >>>



1. From the **Administration** menu, click **Roles and Services.**
2. Click **Manage Roles**. A list of current roles is displayed.



3. Click **modify privileges** (3) of the role you wish to edit.
4. Enable the checkbox of each privilege you wish to add to the role.
5. Disable the checkbox of each privilege you wish to remove from the role.
6. Scroll to the bottom of the screen and click **modify role with updated privilege**. The Confirmation screen is displayed.
7. Click **confirm and save privilege**. The screen refreshes, and the role is updated.

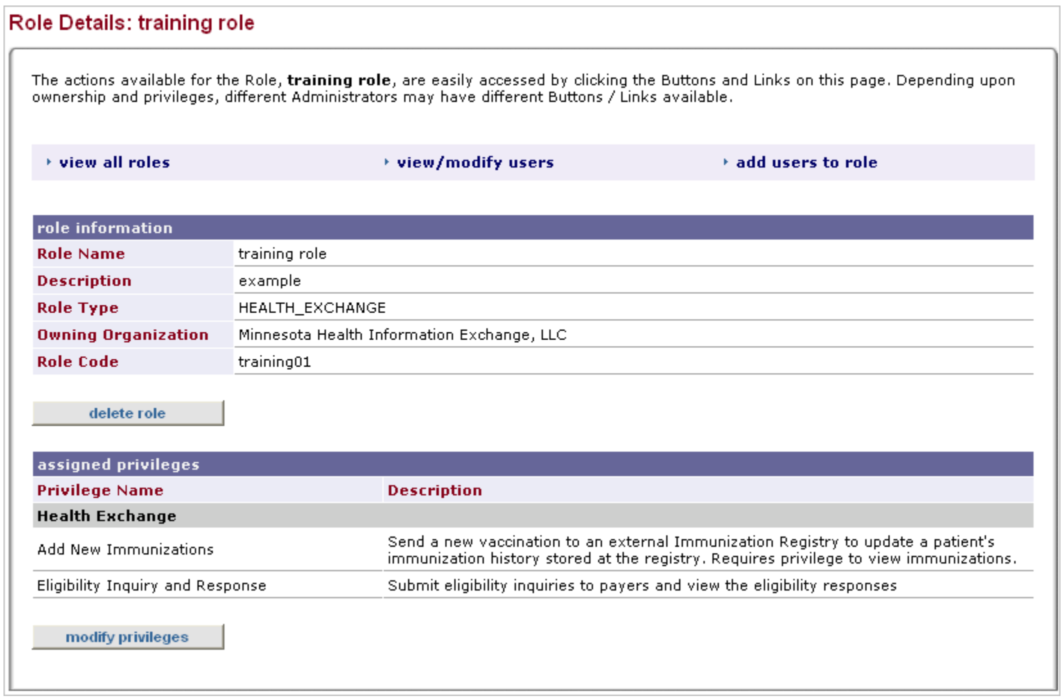
RESULT:

You have successfully modified a role.

Delete Health Exchange Role

When the role is deleted in the system, it is automatically removed from each user associated to the role.

1. Navigate to the View Role Details screen.



Role Details: training role

The actions available for the Role, **training role**, are easily accessed by clicking the Buttons and Links on this page. Depending upon ownership and privileges, different Administrators may have different Buttons / Links available.

view all roles | view/modify users | add users to role

role information	
Role Name	training role
Description	example
Role Type	HEALTH_EXCHANGE
Owning Organization	Minnesota Health Information Exchange, LLC
Role Code	training01

delete role

assigned privileges

Privilege Name	Description
Health Exchange	
Add New Immunizations	Send a new vaccination to an external Immunization Registry to update a patient's immunization history stored at the registry. Requires privilege to view immunizations.
Eligibility Inquiry and Response	Submit eligibility inquiries to payers and view the eligibility responses

modify privileges

2. Click **delete role**.
3. Click **OK** to confirm deletion. When the role is deleted in the system, it is automatically removed from each user associated to the role.

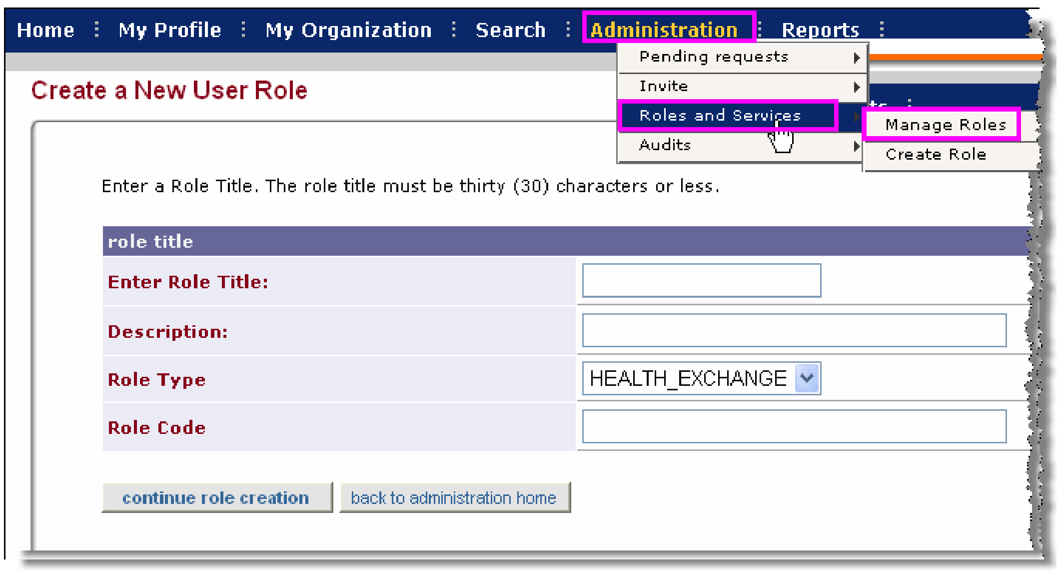
RESULT:

You have successfully deleted a role.

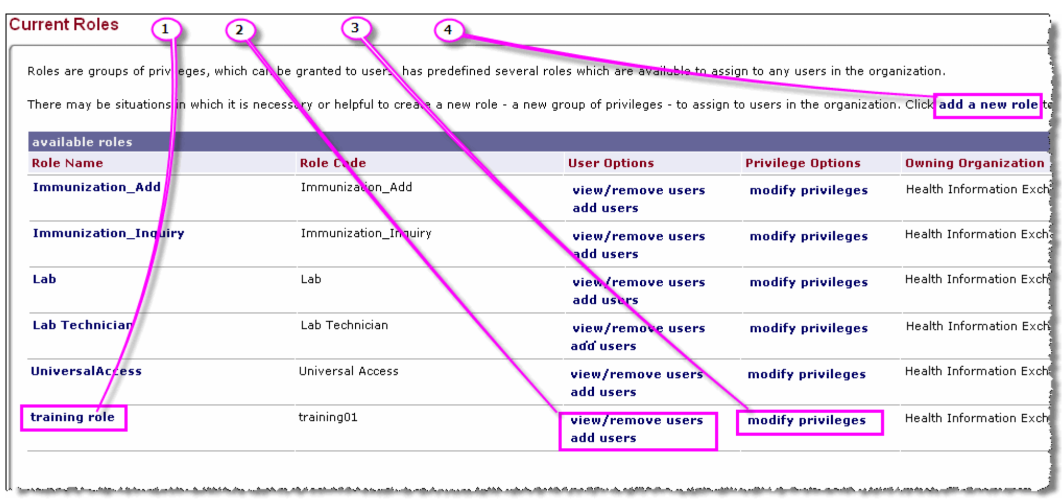
Assign Health Exchange Role to Users

(This task only applies to non-federated users. Federated users are automatically granted Health Exchange role(s) based on the role code(s) in the SAML Assertion).

You must have the Service or Security Administrator Role in order to assign Health Exchange Roles to Users.



1. From the **Administration** menu, click **Roles and Services.**
2. Click **Manage Roles**. A list of current roles is displayed.



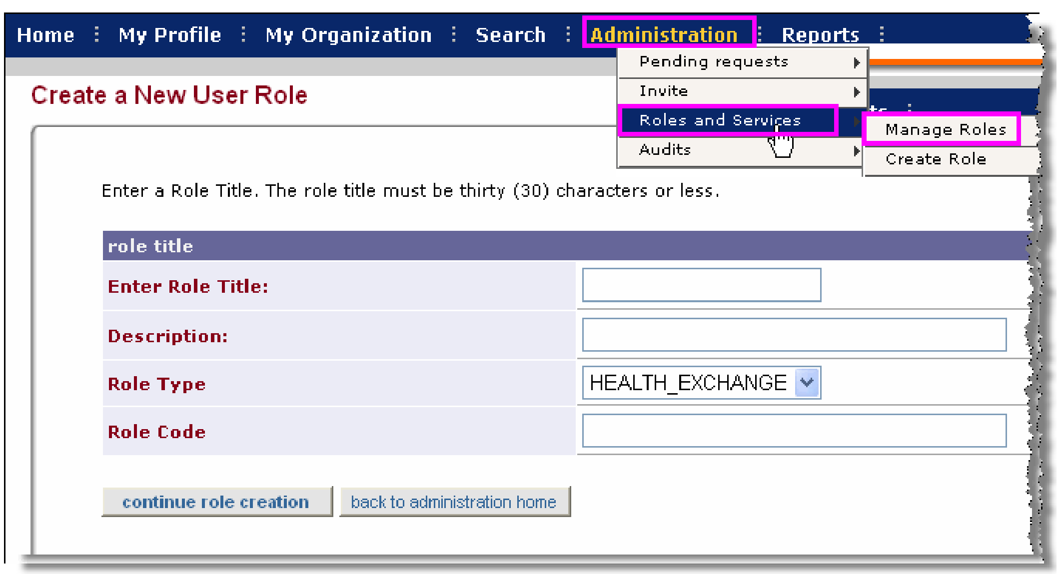
3. Click **add users** (2) in the row of the role to which you wish to assign users. The User Search screen is displayed.
4. Search for the user by keying in search criteria, then click **Search**. (Note: The users who already have the role will not be included in search results).
5. Enable the checkbox of each user you wish to assign to the role.
6. Scroll to the bottom of the screen and click **submit user additions**.
7. Click **OK** to confirm. The screen refreshes, and each user selected is added to the role.

RESULT:

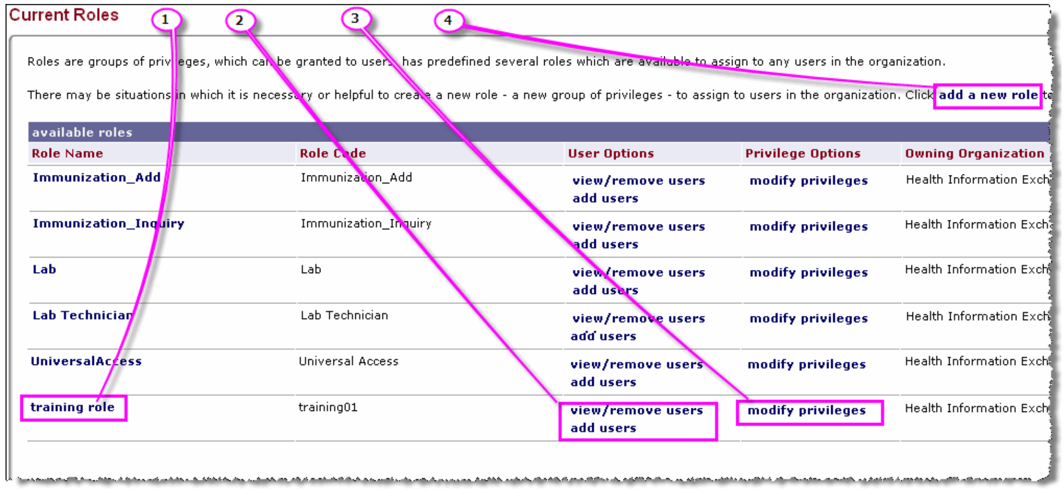
You have successfully assigned a Health Exchange role to a user. The role will be applied to the user's profile the next time the user logs in.

Remove Health Exchange Role from Users

You must have the Service or Security Administrator Role in order to remove Health Exchange Roles from Users.



1. From the **Administration** menu, click **Roles and Services.**
2. Click **Manage Roles**. A list of current roles is displayed.



3. Click **view / remove users** (2) in the row of the role from which you wish to remove users. A list of all users assigned to the role is displayed.
4. Enable the checkbox of each user you wish to remove to the role.
5. Scroll to the bottom of the screen and click **remove selected user(s)**.
6. Click **OK** to confirm. The screen refreshes, and each user selected is removed from the role.

RESULT:

You have successfully removed a Health Exchange role from a user.

PREMIUM SERVICE: IDCIPHER CARD

About the IDcipherTM Card

The IDcipher™ Card is used as a method for authentication that may optionally be used within Portals that require up-level authentication.

The IDcipher™ card provides two-factor authentication (something the user knows and something the user has) which is one form of authentication that may be used when up-level authentication is required. The card provides a low-cost, easy-to-use, easy-to-deploy authentication mechanism that provides an extra level of assurance when a user is authenticated.

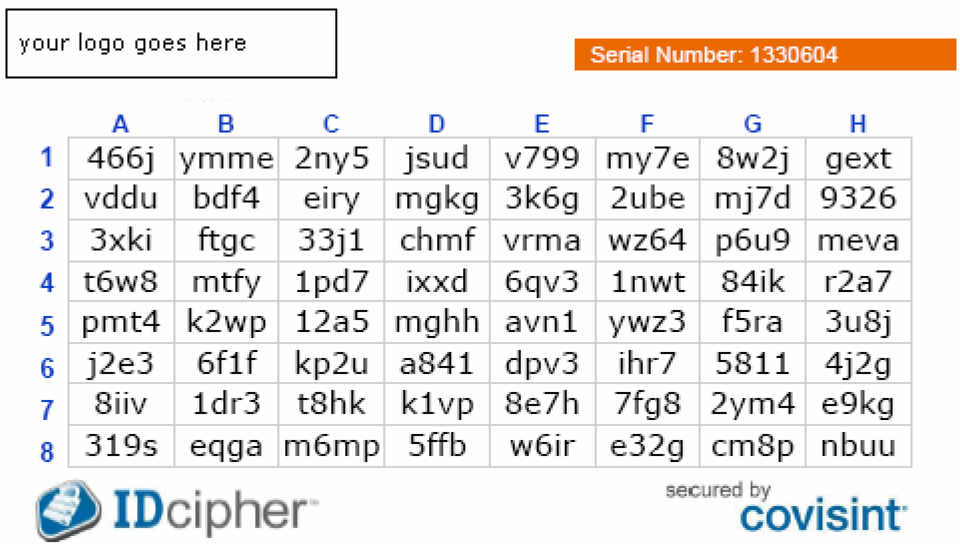
Covisint has trademarked the IDcipher™ Card.

(IDcipherTM card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

More Information About the IDcipherTM Card

The IDcipher™ card is an 8x8 matrix of cells which contain a value that is a randomly generated four-character lower-case alphanumeric string (number 0 and letters o and l are excluded) which is provided by Covisint. Each IDcipher™ card is unique per user.

Picture of a Sample IDcipher Card™



your logo goes here

Serial Number: 1330604

	A	B	C	D	E	F	G	H
1	466j	ymme	2ny5	jsud	v799	my7e	8w2j	gext
2	vddu	bdf4	eiry	mgkg	3k6g	2ube	mj7d	9326
3	3xki	ftgc	33j1	chmf	vrma	wz64	p6u9	meva
4	t6w8	mtfy	1pd7	ixxd	6qv3	1nwt	84ik	r2a7
5	pmt4	k2wp	12a5	mghh	avn1	ywz3	f5ra	3u8j
6	j2e3	6f1f	kp2u	a841	dpv3	ihr7	5811	4j2g
7	8iiv	1dr3	t8hk	k1vp	8e7h	7fg8	2ym4	e9kg
8	319s	eqga	m6mp	5ffb	w6ir	e32g	cm8p	nbuu

IDcipher

secured by covisint

- The card is emailed to the user in PDF format.
- The user prints out a hard copy of the card.
- When a user attempts to sign on to the portal, after keying in the correct User Name and Password, the system may prompt the user for an IDcipherTM card value of a randomly picked cell (for example: column C row 4) The user enters the value as read from the IDcipher™ card when prompted (1pd7 in this example).

When will I be prompted to use an IDcipher™ card? Learn more >>>

(IDcipherTM card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

Up-Level Authentication

Up-level authentication is an authentication process that prompts the user for an additional, stronger form of authentication than a user name and password, when a user attempts to gain access to a system resource that requires an additional level of protection. Additionally, the user may be prompted for up-level authentication based on specified criteria which can be derived from user provided information (e.g. a specific user name), system collected information (e.g. an unknown PC IP Address), as well as transaction patterns (e.g. time of day the user signs on or how frequently the user is signing on).

Covisint has trademarked the IDcipher™ Card as a means of providing up-level authentication. – Delete from this section and add to section about the IDcipher card.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

How Do I Get An IDcipher TM Card?

The IDcipher™ card is used as a method for authentication that may optionally be used within Portals that require up-level authentication.

The process for obtaining an IDCipher™ Card is dependent upon your user status. Click on the link that best describes you:

I am an existing user, I can already log in to the portal, but I need a new IDcipher™ Card >>>

I am new to the portal, and not yet a registered user? (You have not yet registered for the portal) >>>

When you register for portal access, an IDcipher™ card will automatically be generated and emailed to you upon approval of your registration request if the portal you are requesting access to requires the IDcipher™ card for up-level authentication.

After submitting a registration request, users need not perfor
an IDCipher™ card.

(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)