Covisint Connection and Administration (CCA) ~ Security Administrator Guide

April 2008

Using This Help Section

- **<u>Expand a section</u>**: Click the + link next to a bookmark in order to expand it and view contents within the bookmark.
- **<u>Navigate</u>**: Click on a bookmark to jump to that section.
- **<u>Print a specific bookmark</u>**: Print out a particular bookmark by right clicking on the bookmark, and then selecting **Print Page(s).** (If you right click on a 'parent' bookmark, all of the 'child' bookmarks will print as well).
- **<u>Print the entire help document</u>:** Click  (Print icon) in the toolbar, or click **File / Print,** then click **OK**.

Introduction

Delegated Model

CCA is a delegated administration tool designed to give power to people who are best in a position to manage user access and make security decisions. In some companies, this may be accomplished through a central office; while in other companies, this may be accomplished by delegating responsibility to people spread throughout the company. The delegated model allows each company to set up the structure that best fits their needs for managing access grants to their users.

The delegated model allows a single company to set up one or more organizations in CCA. CCA organizations are simply groupings of users with their own administrator(s) and their own available service packages. Organizations that are created below the parent organization are called divisions. Administrators in the parent organization can perform tasks on users in the divisions below.

Defining Administrator Roles

A definition of all Administrator Roles is listed here for informational purposes.

There are several administrator roles available in CCA that can be assigned to users. These roles can be used independently or multiple roles can be combined for a broader variety of administrative options. The available roles include:

Organization Password Administrator - Searches for users' profiles and resets users' passwords.

Organization Security Administrator - Administers a *specific* service package as well as sub-packages associated with it.

User Account Administrator – Rejects or approves new user requests. (This role is appropriate for someone in a position to confirm that the user should have access to the secured portal).

Security Administrator - A superset of all administrator rights and responsibilities. An organization can have as many or as few administrators as desired.

The following section displays roles / privileges in two ways. First, Table 1 is comprised of privileges associated per role in a matrix view. Second, Figure 1 is comprised of privileges associated per role in a list view.

Table 1:

Matrix of Privileges Associated Per Role

	User Roles				
	1. General User	2. Password Admin	3. User Account Admin	4. Service Admin	5. Security 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
Audit User Grants	-	-	X	X	X
Audit Users in Company (Quarterly & Annually)	-	-	X	-	X
Change Email Preferences for Self	X	X	X	X	X
Change Password of Self	X	X	X	X	X
Delete a Division in Your Org	-	-	-	-	X
Delete a User Account	-	-	X	-	X
Edit Organization and/or Division Profile	-	-	-	-	X
Edit Profile of Others	-	-	X	-	X
Edit Profile of Self	X	X	X	X	X
Generate a Service Summary Report	-	-	-	-	X
Generate Report of User Summary by Organization	-	-	-	X	X
Generate Report of Users Grants per Svc. Package	-	-	-	X	X
Generate Security Administrator Reports	-	-	-	X	X
Grant a Service Package to a Division in Your Org	-	-	-	-	X
Grant a Service Package to a User	-	-	-	X	X
Invite Users to Register	-	-	X	-	X
Modify User Roles	-	-	-	-	X
Move a User	-	-	X	-	X
Remove a Service Package from a Division in Your Org	-	-	-	-	X

Table 1:

Matrix of Privileges Associated Per Role

	User Roles				
	1. General User	**2. Password Admin**	**3. User Account Admin**	**4. Service Admin**	**5. Security Admin**
Remove service package from a user	-	-	-	X	X
Request a service package for my organization	-	-	-	X	X
Request a service package for self	X	X	X	X	X
Reset password of others	-	X	X	-	X
Search /View details for divisions in my organization	-	X	-	X	X
Search for users in my organization	-	X	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
View my organizational administrators	X	X	X	X	X
View organization's hierarchy	-	-	-	-	X
View / cancel pending requests of self	X	X	X	X	X
View request history of others	-	-	-	X	X
View request history of self	X	X	X	X	X

Figure 1: List of Privileges Associated Per Role

Role 1: Privileges associated to All Registered Users (General Users)

- Change email preferences for self
- Change password of self
- Edit profile of self
- Request a service package for self
- View my organizational administrators
- View / cancel pending requests of self
- View request history of self

Role 2: Privileges associated to Password Administrator

- *All of General Users* +
- Reset password of others
- Search /View details for divisions in my organization
- Search for users in my organization
- Specify password for self
- Specify password of others

Role 3: Privileges associated to User Account Administrator

- *All of General Users* +
- Approve / Reject new user registration requests
- Audit user grants
- Audit users in company (Quarterly & Annually)
- Delete a user account
- Edit profile of others
- Invite users to register
- Move a user
- Reset password of others
- Search for users in my organization
- Suspend a user account

Role 4: Privileges associated to Service Administrator

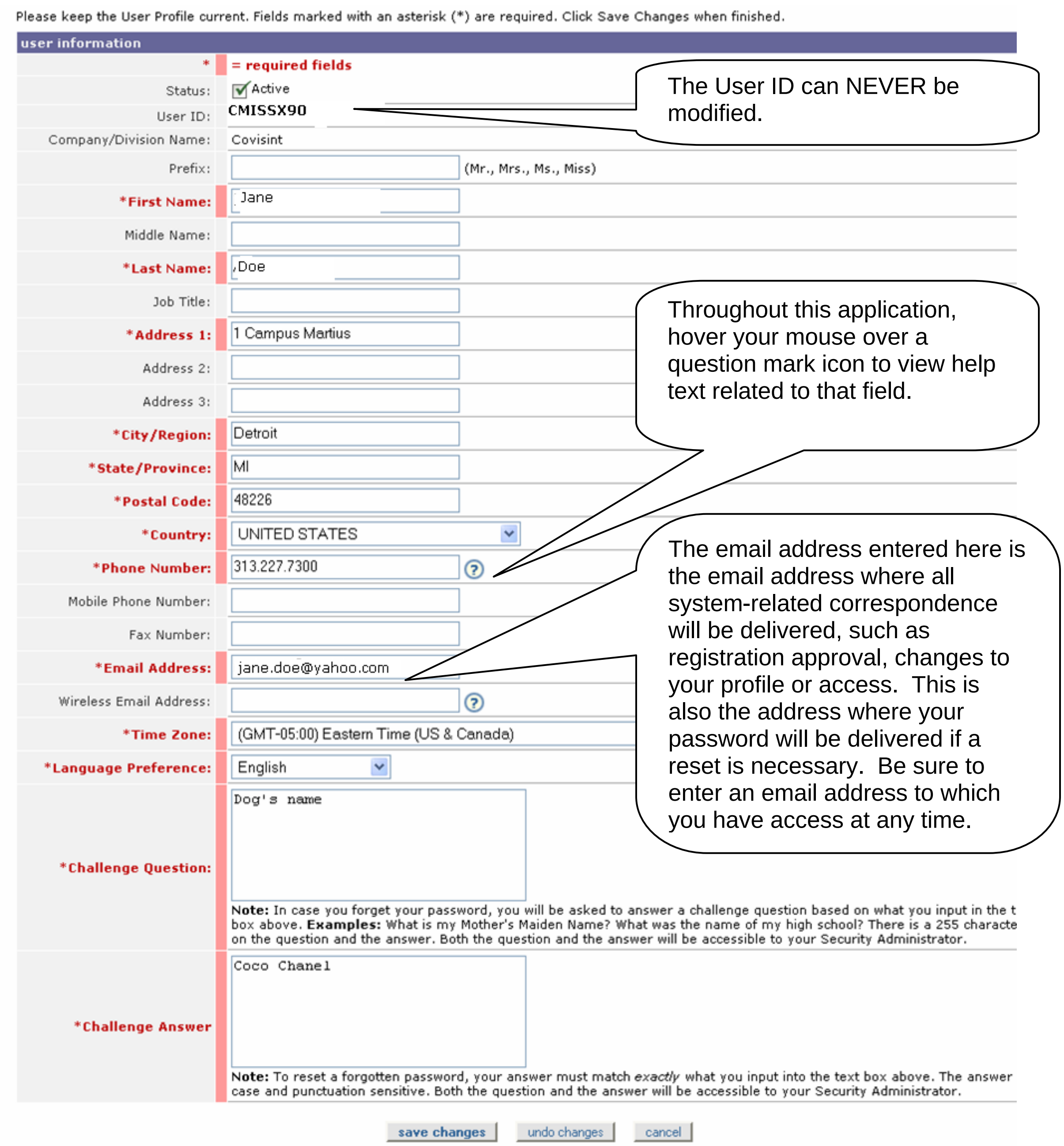
- *All of General Users* +
- Approve / Reject division's service package request
- Approve / Reject user's service package requests
- Audit users in company (Quarterly & Annually)
- Generate report of user summary by organization
- Generate report of users' grants per svc. package
- Generate security administrator reports
- Grant a service package to a user
- Remove service package from a user
- Request a service package for my organization
- Search /View details for divisions in my organization
- Search for users in my organization
- View request history of others

Role 5: Privileges associated to Security Administrator

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

Edit Your User Profile

1. From the **My Profile** drop down menu, click **Edit my Profile**. The Edit Profile screen is displayed. All of the information associated with your user profile can be edited via this screen.



2. Modify the information as desired. Remember that required fields, identified with the bold, red font, red bar, asterisk, must be populated in order to save changes to your profile.

Details about the Challenge Question and Challenge Answer fields.
Security questions are used to verify the identity of a user during password reset. You will be prompted to enter the answer to the security question you create in this field. Important to note that your answer must match exactly as entered here – including upper and lower case.

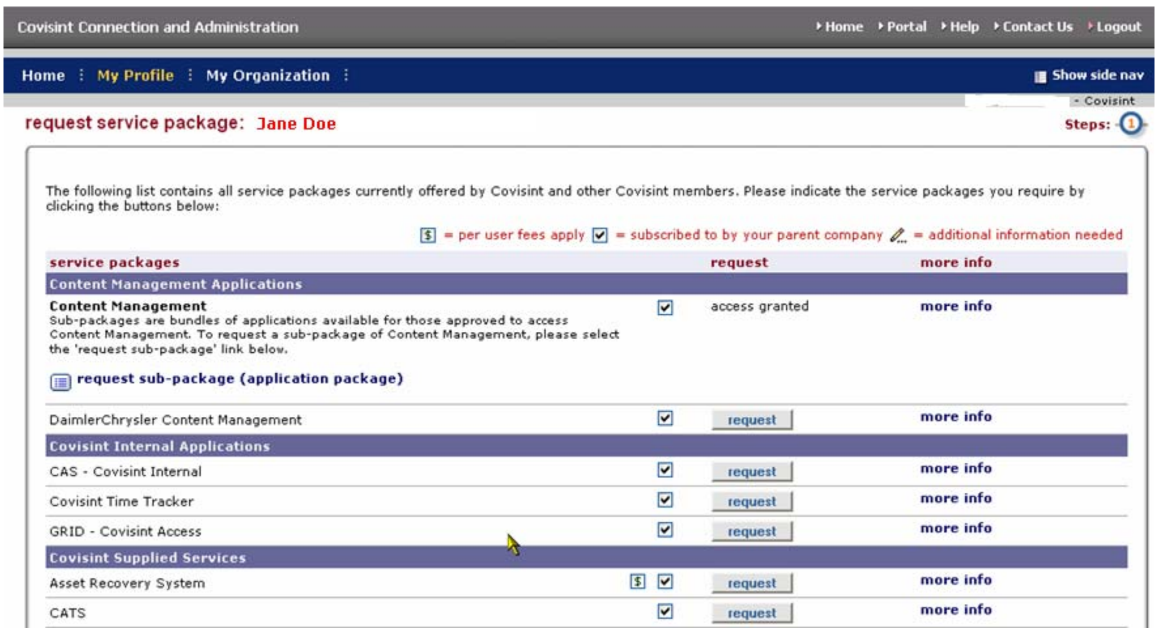
3. Click **Save Changes**. The changes are immediately applied to your profile, and a success message is displayed.

Result
You have successfully modified your user profile.

Request Service Packages

Service Package: a defined group of one or more applications. By requesting a service package, you can obtain access to additional applications.

1. From the **My Profile** drop down menu, click **Request Service Package**. The request service package screen is displayed.



Note: the following symbols will help you understand attributes of certain packages:

Packages already granted to your organization are denoted by a check mark.

Packages that have associated fees are denoted with a dollar sign.

Note: You are only able to be approved for service packages already granted to your organization. If you request a service or sub-package that is not already granted to your organization, your administrator will need to request those services on behalf of the organization before granting them to you.
Click here for steps on how to view the service packages granted to your Org.

2. Click **request** next to the package you wish to request**. Note:** You can request Sub Packages of certain portals by clicking on the **request sub-package** link under the applicable Partner Portal Service. The request details screen is displayed.

3. Enter the reason for the request in the open text box. The request reason will help your administrator make appropriate decisions regarding your request.

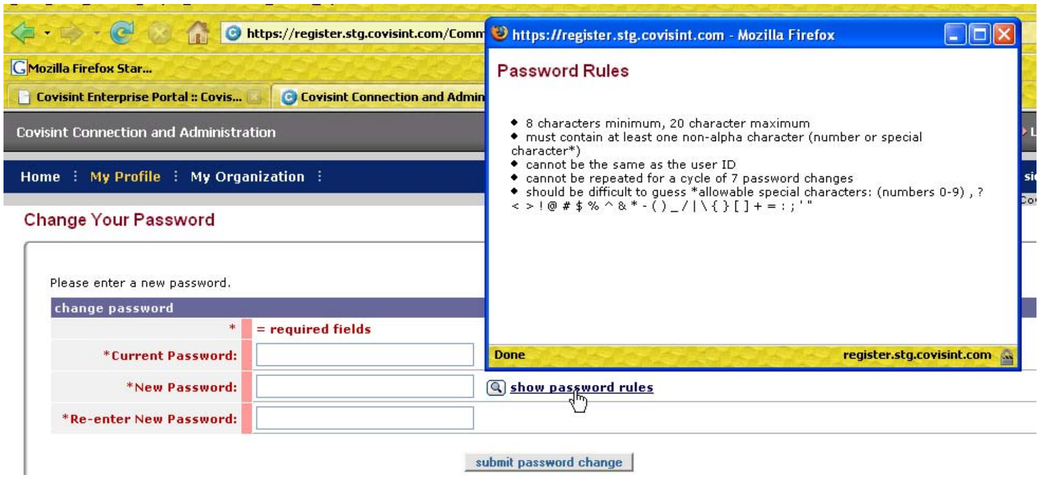
4. Click **continue** to submit the request. Your request is routed to your administrator for approval

5. Repeat steps 1 – 4 as necessary to request additional service packages.

Result
You have successfully requested access to a service package.

Change Your Password

1. From the **My Profile** drop down menu, click **Change my Password**. The Change Your Password screen is displayed.



It is important to change your password every 90 days to keep your account secure. You will be prompted by the system to change your password as the 90 day expiration date approaches. After 90 days, the system will force a password change during the login process.

Your password must adhere to Covisint security standards. You can view the password rules by clicking **show password rules** on the password-reset page, as displayed in the screen above.

2. In the *Current Password* open text field, key in your current password.

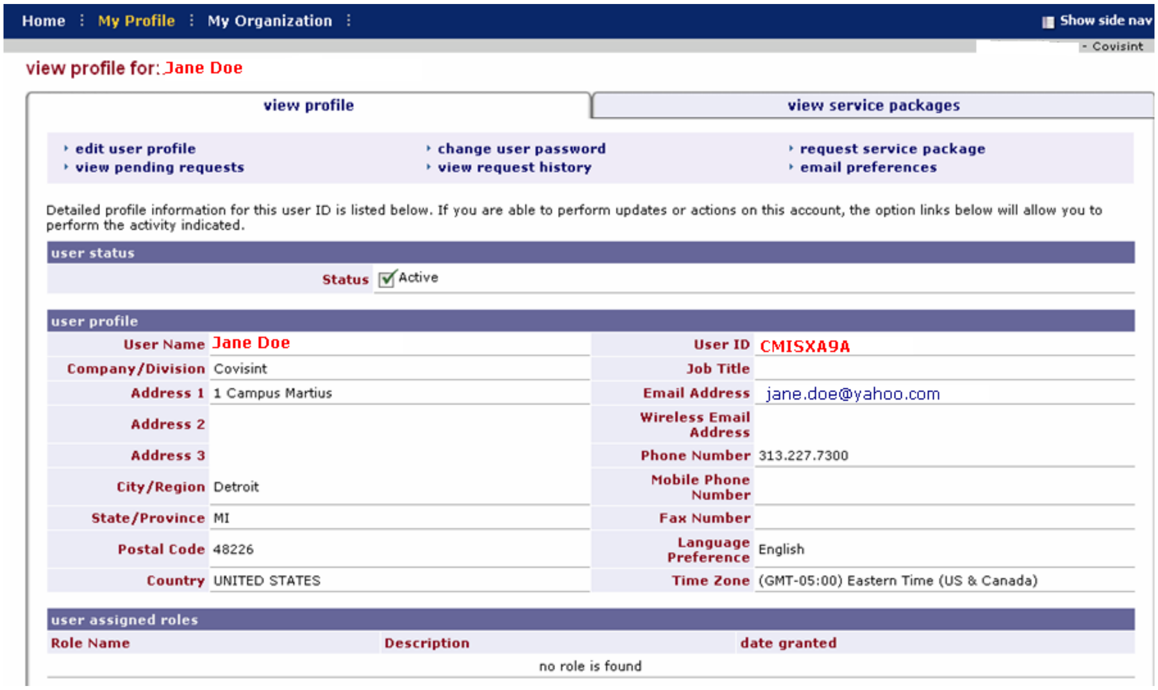
3. In the *New Password* open text field, create a new password that adheres to the Covisint password rules.

4. In the *Re-enter New Password* open text field, key in the newly created password to verify that you have typed it correctly.

5. Click **Submit password change**. The changes are immediately applied to your account.

Result
You have successfully changed your password.

Additional Profile Management Features



If you wish to…	Then…
View your current service package grants	1. Click **My Profile** menu. 2. Click **View my profile option**. 3. Click **View service packages** tab. The View service packages screen is displayed. From this screen, you are able to view packages and sub packages to which you currently have access. To view details of any service package grant, simply click the *package name*.
View user roles assigned to you	1. Click **My Profile** menu. 2. Click **View my profile option**. 3. Scroll to the bottom of the screen to the 'user assigned roles' section to view the list.
View pending requests you have submitted	1. Click **My Profile** menu.

If you wish to…	Then…
	2. Click **View my profile option**. 3. Click **View pending requests**. The View pending request screen is displayed. From this screen, you are able to view packages and sub packages to which you currently have access request pending.
Send a reminder to the administrator regarding a pending request	1. Click **My Profile** menu. 2. Click **View my profile option**. 3. Click **View pending requests**. The View pending requests screen is displayed. 4. Enable the checkbox of each request for which you wish to send a reminder. 5. Click **send reminder.** 6. Key in the reason for the reminder. 7. Click **submit**. The reminder is sent to the appropriate Administrators.
Cancel a pending request	1. Click **My Profile** menu. 2. Click **View my profile option**. 3. Click **View pending requests**. The View service packages screen is displayed. 4. Enable the checkbox of each request you wish to cancel. 5. Click **cancel pending request**. 6. Click **submit decision**. The request is removed from the Administrator's queue.
Opt out of auto-generated email	**(The system automatically sends email notifications for many items. You may**

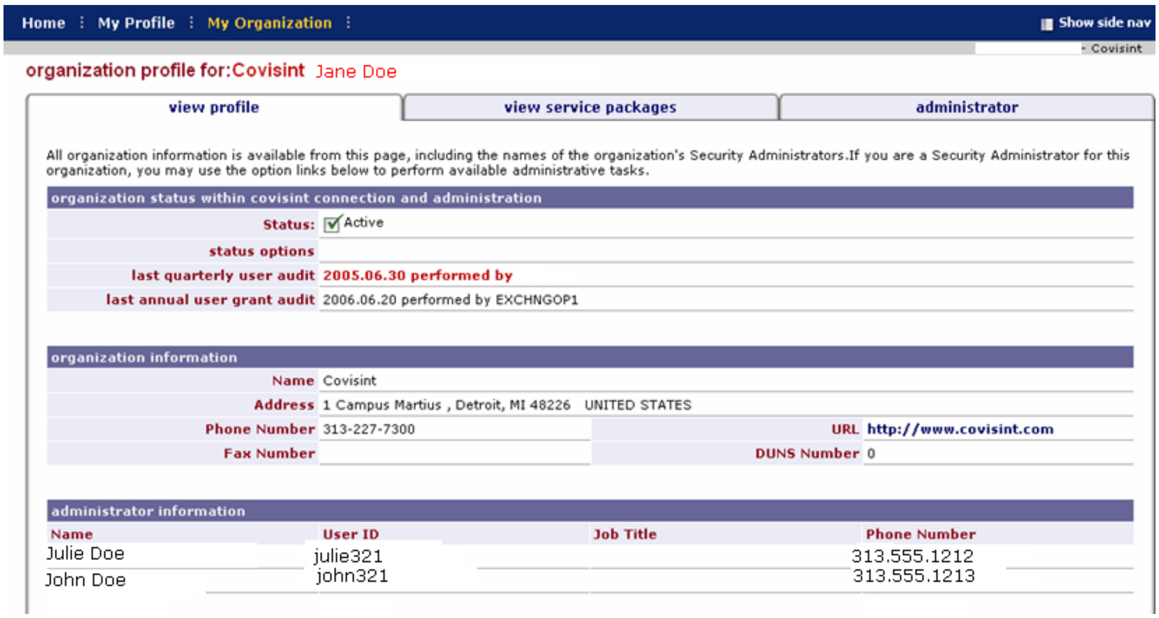
If you wish to…	Then…
	opt out of certain email notification by following the steps provided here) 1. Click **My Profile** menu. 2. Click **View my profile option**. 3. Click **email preferences**. The Update your email preferences screen is displayed. 4. Deselect the checkbox of each item for which you do not wish to receive notification. (You are not able to opt out of password reset emails for security reasons). 5. **Click Save** changes.
View the history of your requests	1. Click **My Profile** menu. 2. Click **View my profile option**. 3. Click **view request history**. A log of your request history is displayed. This log contains the request and approval dates, as well as the approver's name and decision

Result
You have successfully performed additional profile management options.

View Your Organization Profile

1. From the Home screen, click **My Organization**. The Organization Profile screen is displayed for the logged in user.

2. Click **View my organization profile**. Your Organization Profile Screen is displayed.

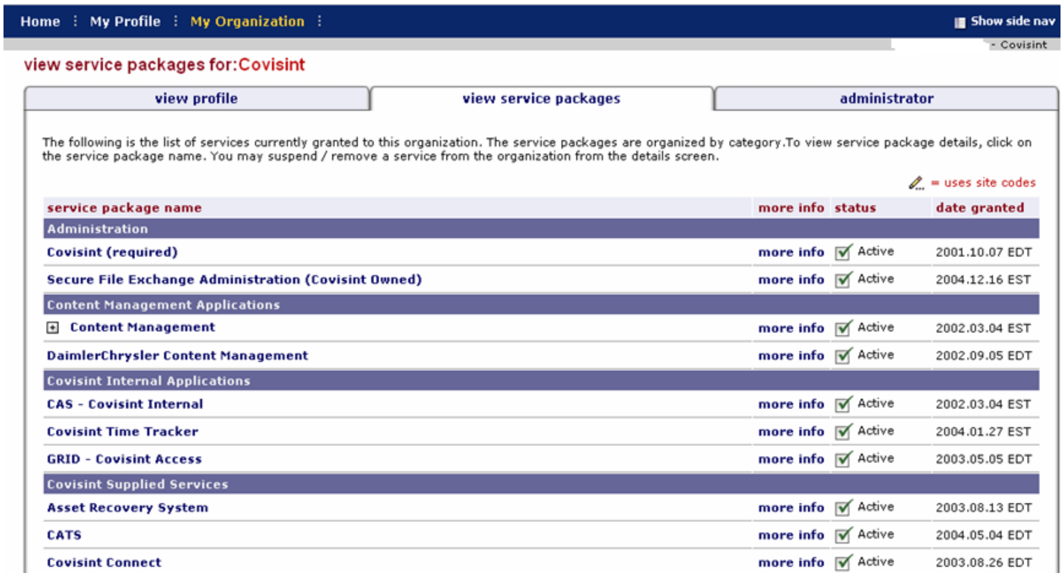


Result
You have successfully viewed organization profile details.

View Your Organization Services

1. From the Home screen, click **My Organization**. The Organization Profile screen is displayed for the logged in user.

2. Click **View my organization services**. Your Organization Services Screen is displayed.



Click the + sign next to a service package to view additional portal customers that have a unique view of that service package. Some portal customers may have a 'customized' view of a given service package.

Result
You have successfully viewed your organization services.

Performing Security Administrator Tasks for your Users

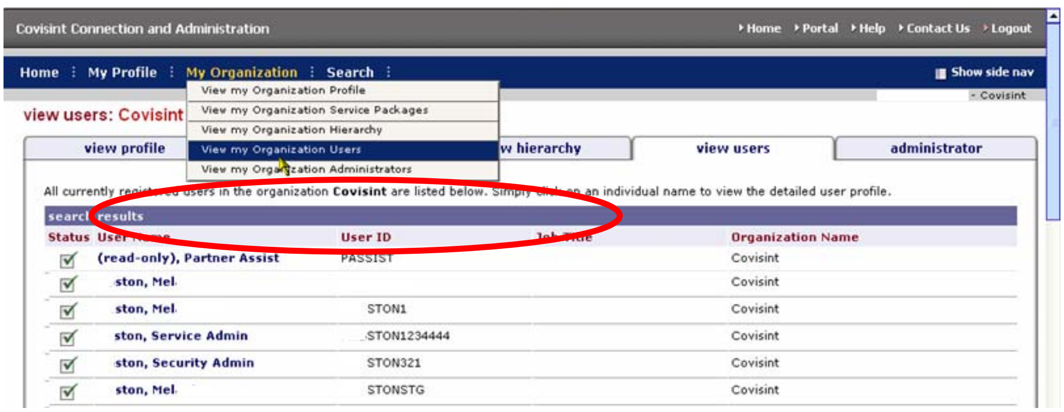
Viewing Users in your Organization

There are two ways for an Administrator to access user accounts. Those are:

- View Users (generally used when quantity of users is less than 50)
- Search for users (generally used when quantity of users is greater than 50)

Complete the following steps to view users in your organization.

1. Click **View my Organization Users** from the *My Organization* drop down menu. The View Users screen is displayed.



User Status Icons Defined:

= Active Status (user account is active)
= Rejected (user registration request was rejected)
= Permanently Removed (user account has been permanently removed from the system)
= Suspended (user account is suspended, and user cannot login until the account is unsuspended)

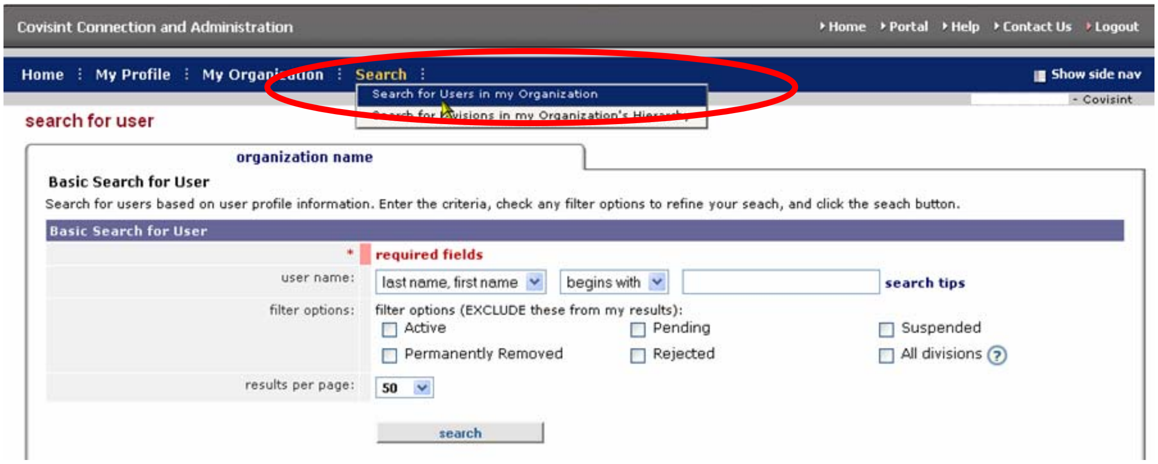
2. Optionally, click on a User Name to view details of that user profile.

Result
You have successfully viewed users for your organization.

Searching for Users in your Organization

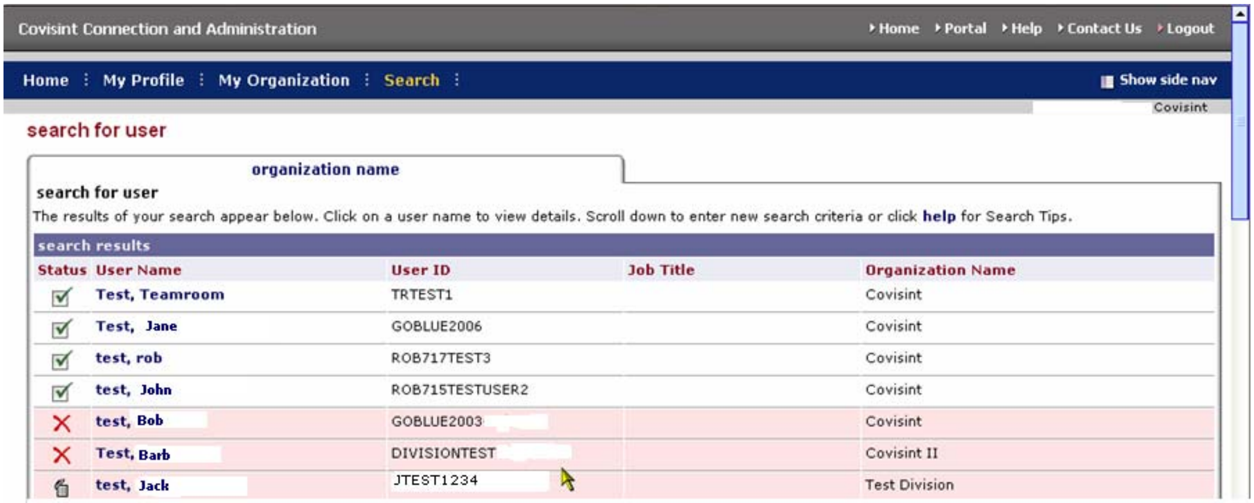
Complete the following steps to search for users in your organization.

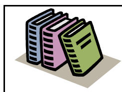
1. Click **Search for Users in my Organization** from the search drop down menu. The Search for Users screen is displayed.



2. From the User Name drop box, select the search criteria regarding the user that you wish to search:
    a. last name, first name
    b. phone number
    c. user id
    d. email address
3. Select either ‘begins with’ or ‘contains’.
4. Key in the search criteria in the open text box.
5. Optionally, narrow search results by enabling the checkbox of each filter you wish to apply. This will *exclude* the checked item from the search results.
    a. Active
    b. Pending
    c. Suspended
    d. Permanently Removed
    e. Rejected
    f. All divisions

6. Click **Search**. The Search results screen is displayed.





User Status Icons Defined:

= Active Status (user account is active)

= Rejected (user registration request was rejected)

= Permanently Removed (user account has been permanently removed from the system)

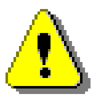
= Suspended (user account is suspended, and user cannot login until the account is unsuspended)

Result
You have successfully searched for a user in your organization.

Resetting a User's Password

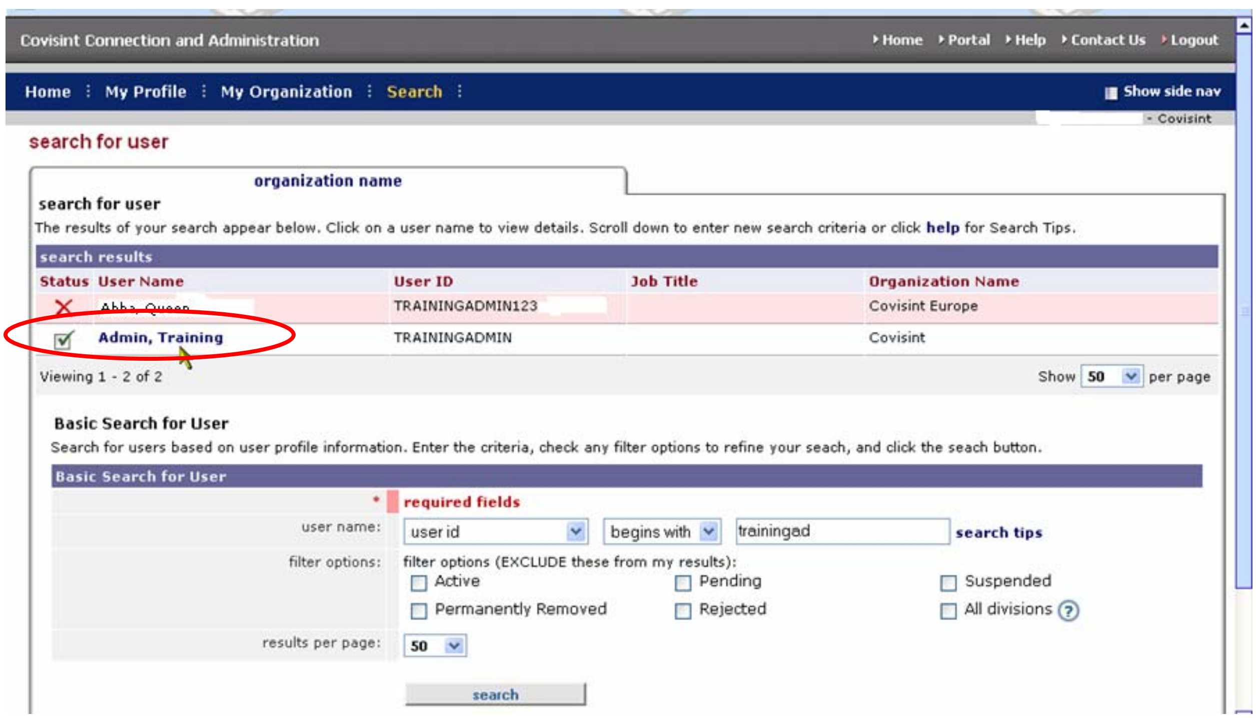
The following section describes the steps involved in resetting a user's password. The steps are similar to the steps a user would take if the user selected the *Forgot my password* link at the login screen.

After locating the user account via view or search (described in a previous section), the Security Administrator can reset the user's password using the steps below.

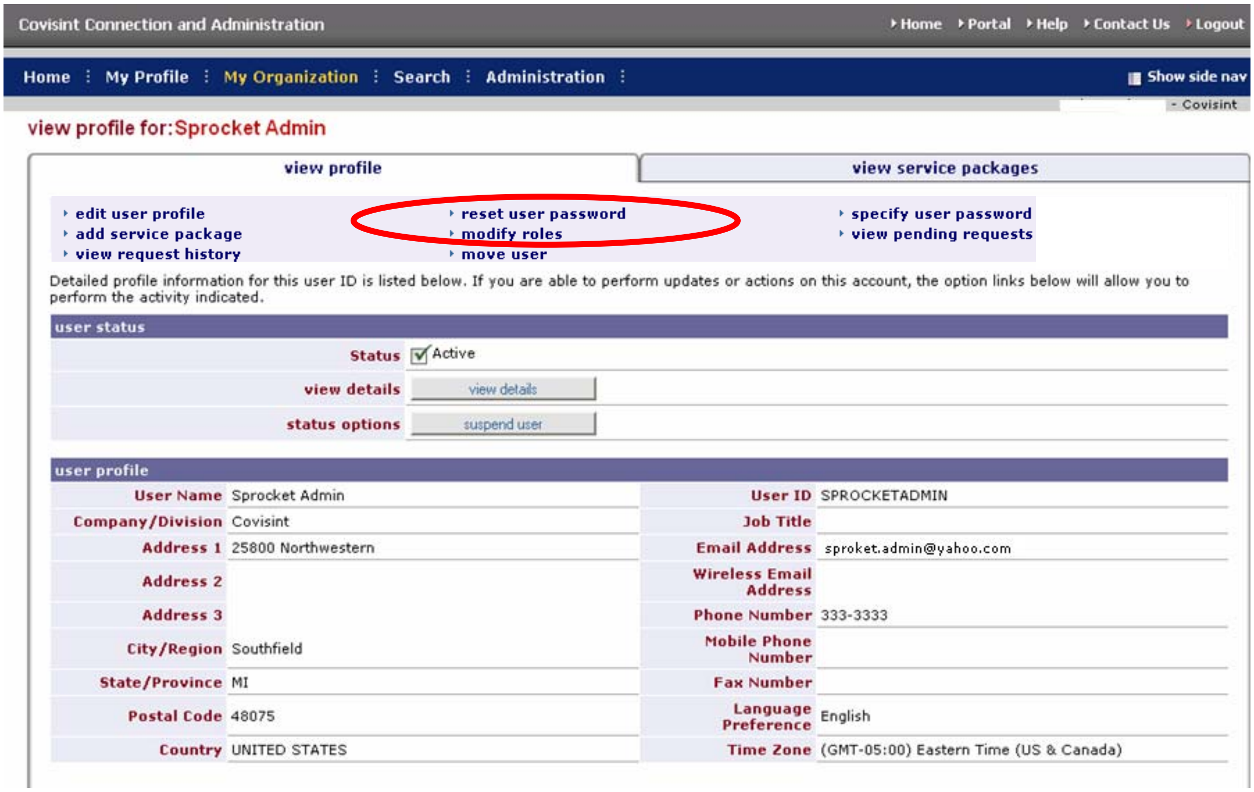


You may notice a "Specify Password" link in addition to the Reset Password option. The specify password process is less secure than the reset password process. It does allow the user assigned the Security Administrator role the ability to know the user's entire password and thus could be exposed to risk / liability. It is recommended that the Specify Password process be used only in exceptional circumstances and not as a general practice. Standard operating procedures should include resetting passwords and not specifying passwords.

1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.



2. Click on the user name of the user for whom you searched. The View Profile screen is displayed.



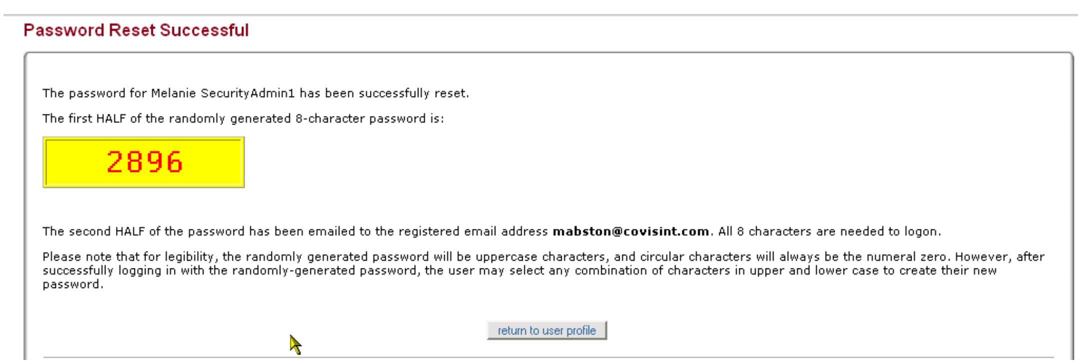
3. Click **reset user password**. The Reset User Password screen is displayed.

4. Validate the user's identity:

    a. Read the "challenge question" to the user.

    b. Ask the user for the answer to the question, and validate the answer to this question. It must match the answer exactly as it appears on the screen.

5. Click **Reset Password**. The screen is refreshed, and the first half of the new password is displayed.



6. Inform the user that you are going to provide the first half of the new password, and ask the user to write down this information.

7. Remind the user that passwords are case-sensitive.

8. Instruct the user to obtain the second half of the new password from the user's email account.

9. Inform the user that after logging in with this newly created, temporary password, the user is prompted / required to change the password.

Result
You have successfully reset a user's password.

Specifying a New Password

Security Administrators are able to specify a password for a user, only on an exception basis. As a standard procedure, the user should reset a password via the Reset Password functionality. However, when that is not possible, the Security Administrator can explicitly state a new password to a user.

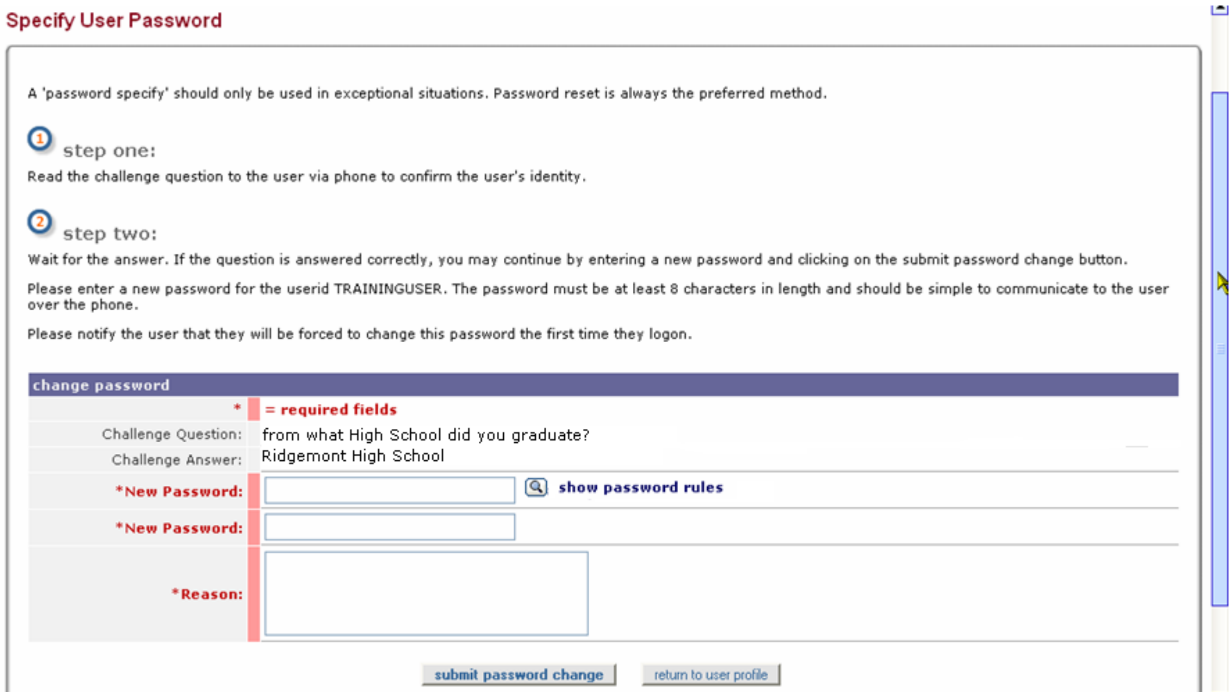
After locating the user account, the user assigned the Security Administrator role can specify a new password for the user using the steps below

> The *specify password* process is less secure than the reset password process. It does allow the Security Administrator to know the user's entire password and thus could be exposed to risk / liability. It is recommended that the *Specify Password* process be used only in exceptional circumstances and not as a general practice. Standard operating procedures should include resetting passwords and not specifying passwords.

1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.

2. From the search results, click on the name of the user for whom you wish to specify a password. The User Profile screen is displayed.

3. Click **specify user password**. The Specify User Password screen is displayed.



4. Validate the user's identity by prompting the user for the answer to the security question.

5. In the first *New password* open text field, key in a new password for this user. This password must adhere to the existing password rules, and should be simple to communicate to the user over the phone.

6. In the second *new password* open text field, key in the newly created password for this user.

7. State the password to the user and inform the user to write down this new, temporary password. Also inform users that they are forced to change this temporary password upon the next login.

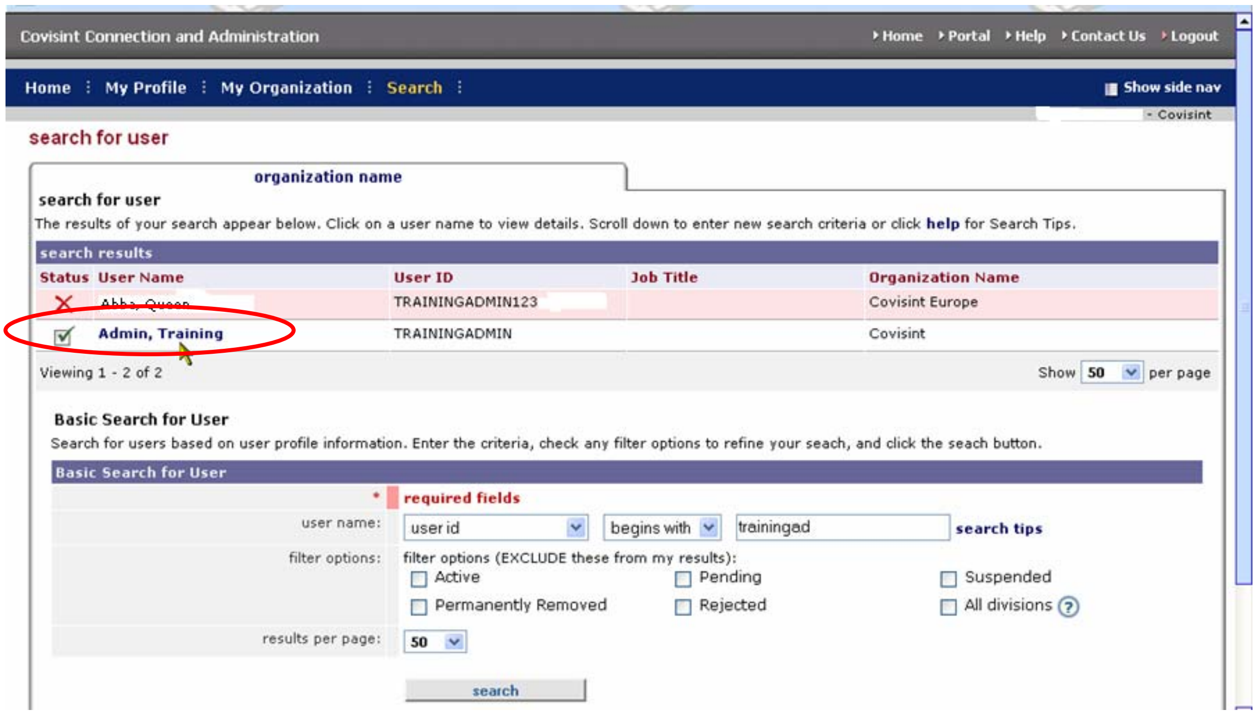
8. Click **submit password change**.

Result
You have successfully specified a user's password.

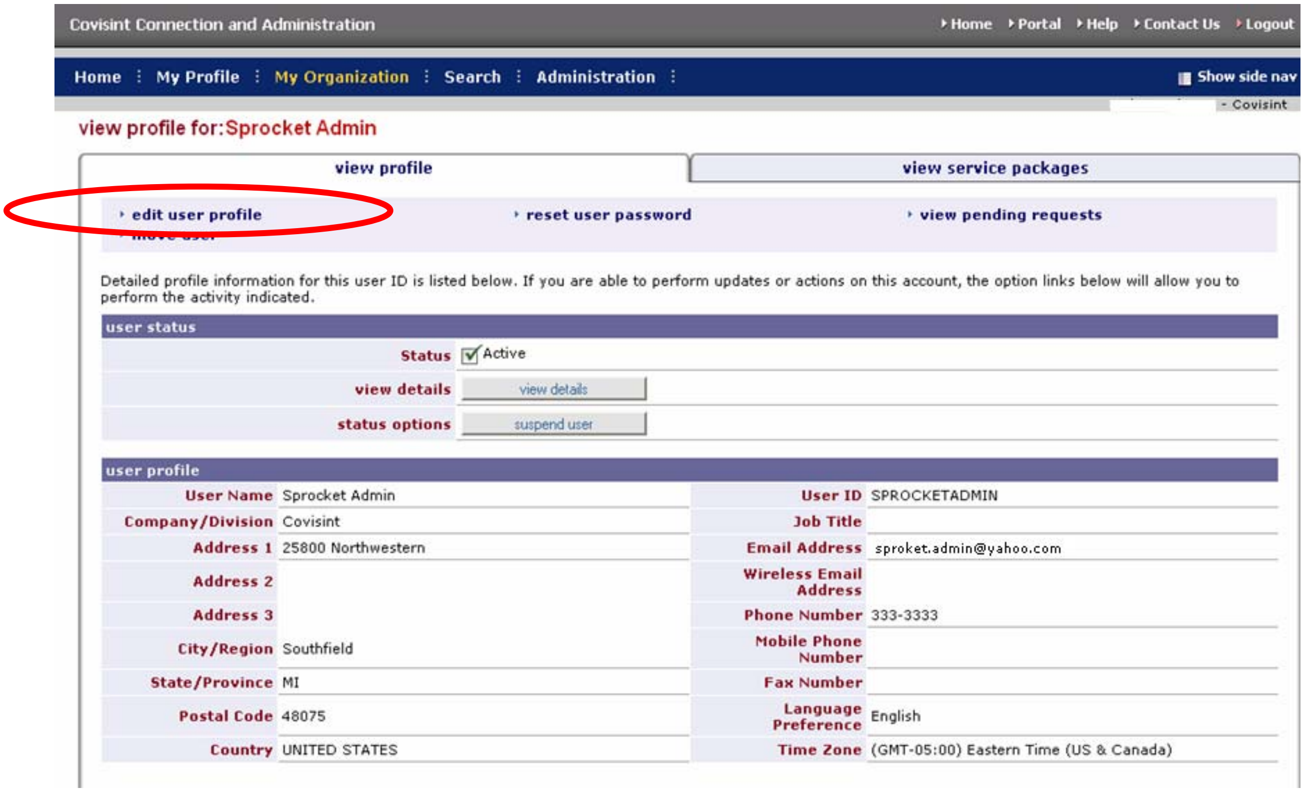
Editing a User's Profile

Users are able and expected to manage their own profiles. However, the Security Administrator is able to update user's profiles as needed. Complete the following steps to edit a user's profile (user must belong to your organization).

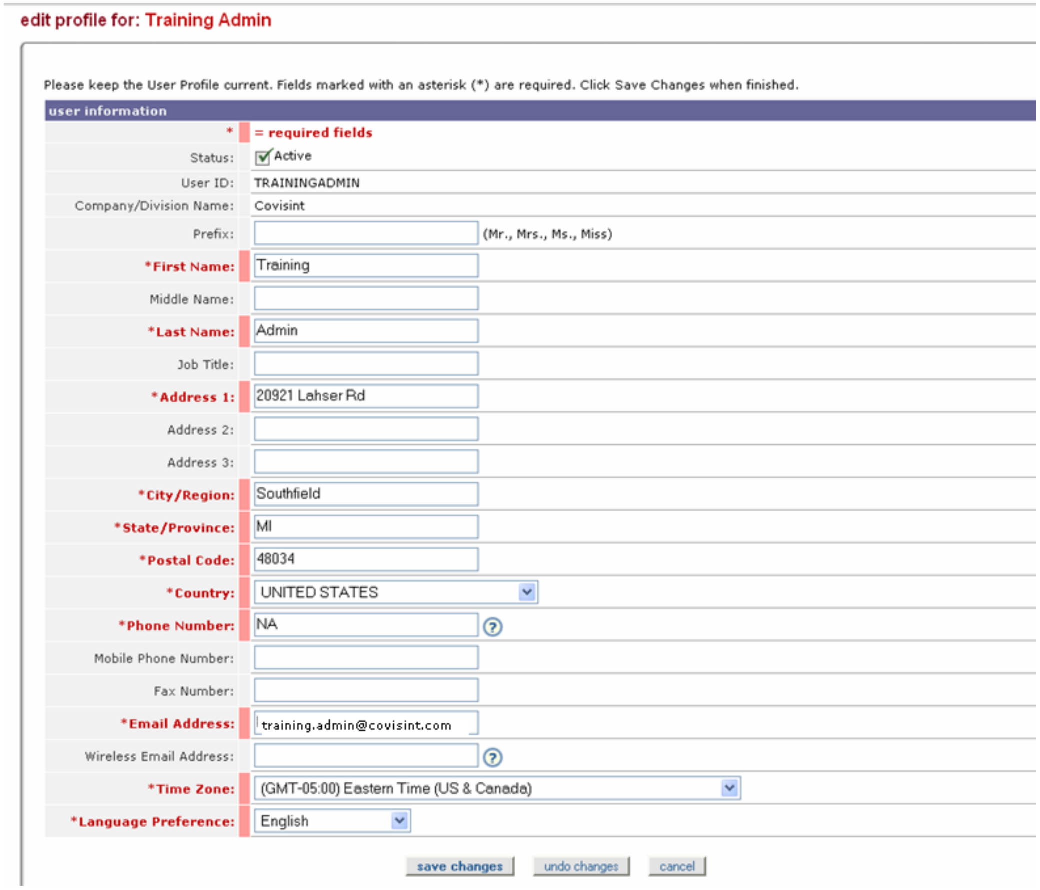
1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.



2. Click on the user name of the user for whom you searched. (This example uses a user named **Admin, Training**) The View Profile screen is displayed.



3. Click **edit user profile**. The Edit User Profile screen is displayed.



4. Edit the profile for the user selected as you wish. Required fields must be populated in order to apply the changes to this profile.

5. Click **save changes**.

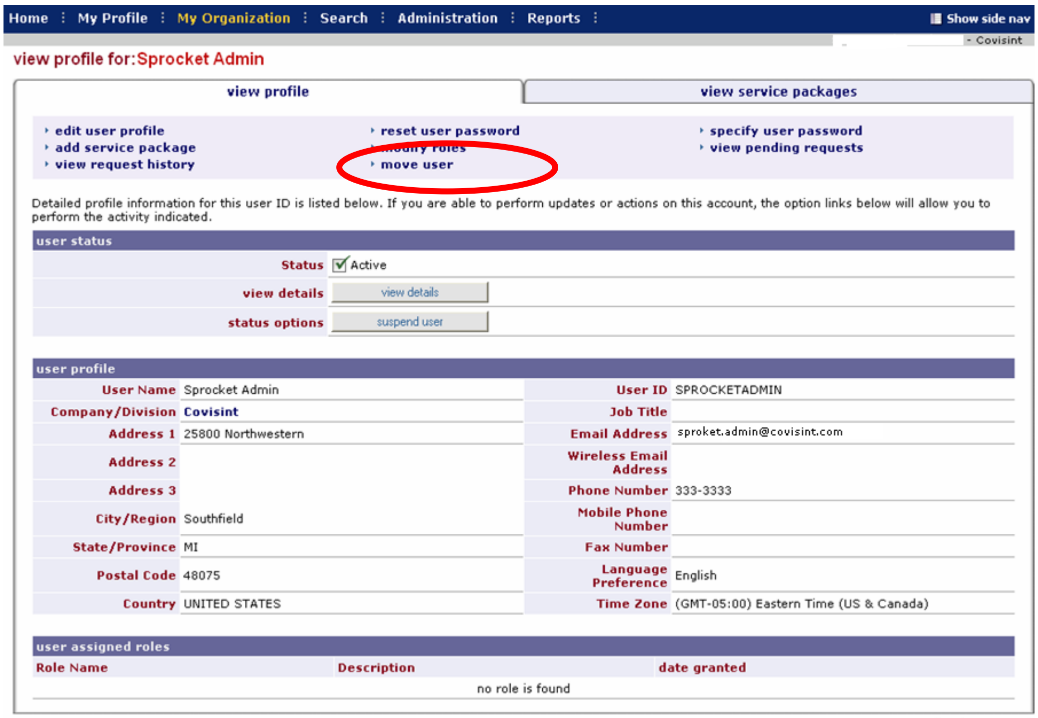
Result
You have successfully edited a user's profile. The user will receive an email notification stating that their profile has been modified by the administrator.

Modifying a User's Role

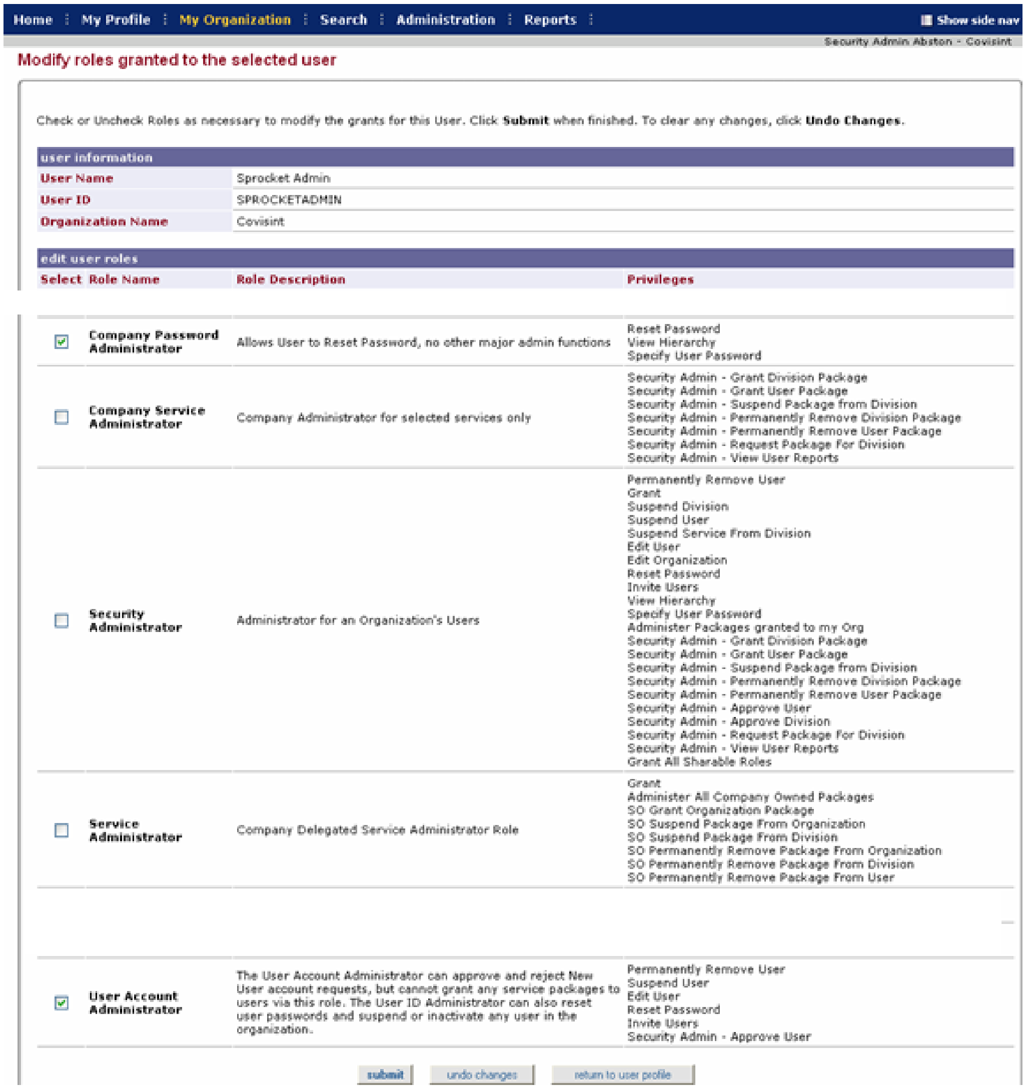
Complete the following steps to modify a user's role. [(Refer to Figure 1 for role definitions)].

1. Perform a User Search. Refer to the previous section entitled Searching for Users in your Organization for details. The User Search result screen is displayed.

2. Click on the *user name* of the user for whom you searched. The View Profile screen is displayed.



3. Click **modify roles**. The Modify Roles Granted to User screen is displayed.



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

Result
You have successfully modified a user's role. The user will receive an email notification stating that the role has been modified by the administrator.

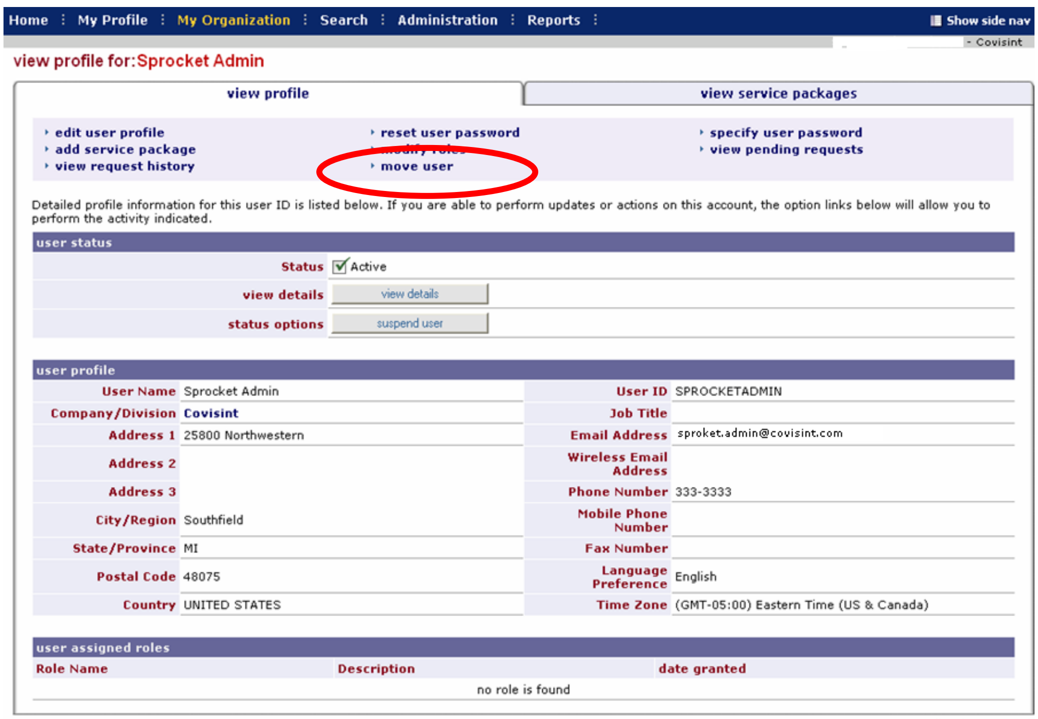
Moving a User

Complete the following steps if you wish to move a user to a different division so that they can be managed by a different administrator.

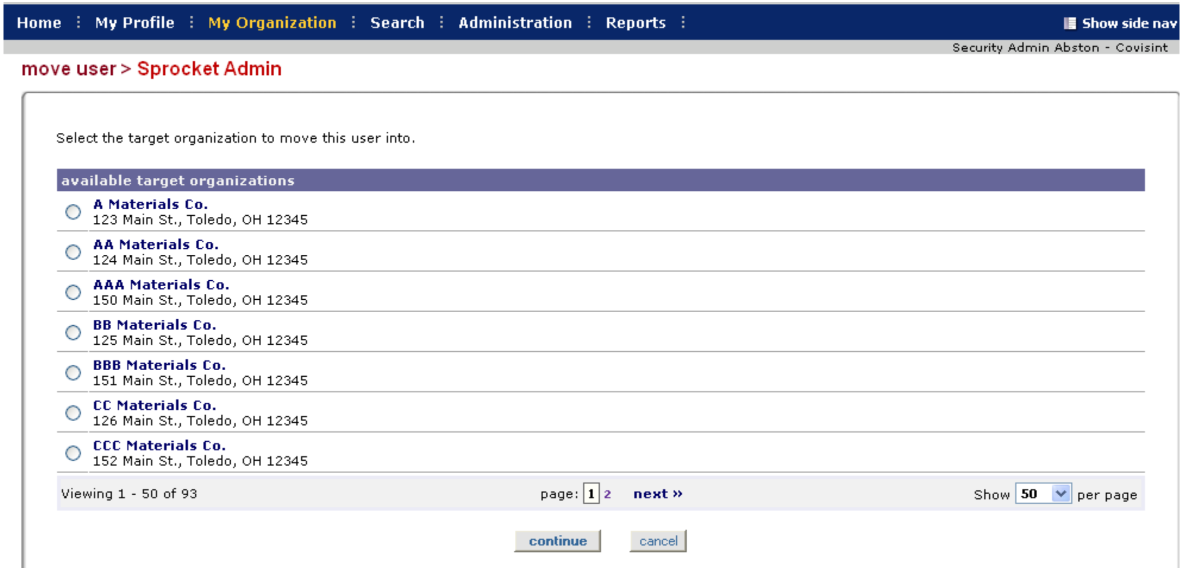
In order to move a user, you must be the administrator at or above the current and target organizations / divisions involved in the move.

1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.

2. Click on the user name of the user for whom you searched. The View Profile screen is displayed.

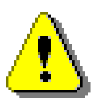


3. Click **move user**. The Move User screen is displayed.

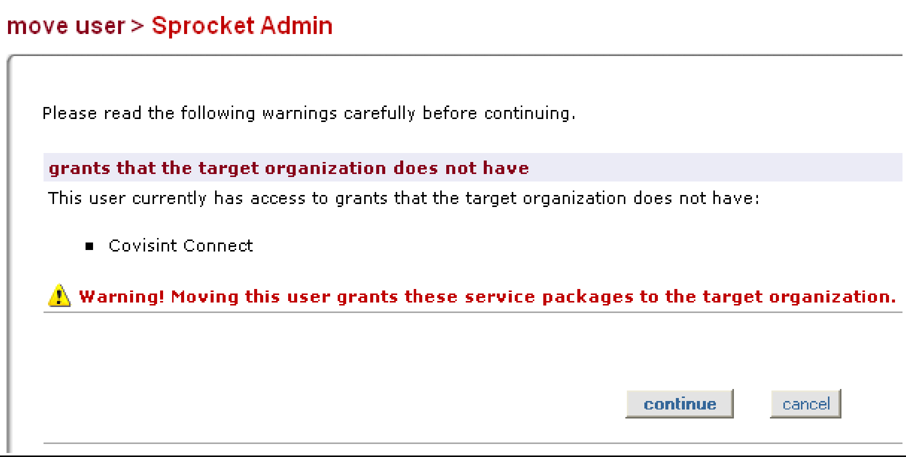


4. Enable the radio button of the target for this user.

5. Click **continue**.



In the event that this user currently has access to grants that the target organization does not have, then moving this user will auto-grant the additional service packages to the target organization. If this is the case, and you are satisfied, click continue. The following is an example of the screen warning:



6. Click **OK** to confirm.

Result
You have successfully moved a user. The user will receive an email notification stating this move/

Granting a Service Package or Sub-Package to a User in your Organization

Packages are grantable groups of one or more applications. Some Service Packages contain Sub-Packages. Sub-packages are designed such that the parent package must be granted before the sub-packages become available.

Service Package – a grantable container that contains at least one application or tool accessed via Covisint portal. Some Service Packages contain sub-packages.

Sub-package – a grantable container that contains at least one sub-service application. The sub-package requires that the parent package be granted first. For example, Covisint provides an application called Content Management.

- Customer A has purchased from Covisint a version of Content Management customized with Customer A's logo.
- Customer B has purchased from Covisint a version of Content Management customized with Customer B's logo.
- Customer C has purchased from Covisint a version of Content Management customized with Customer C's logo.

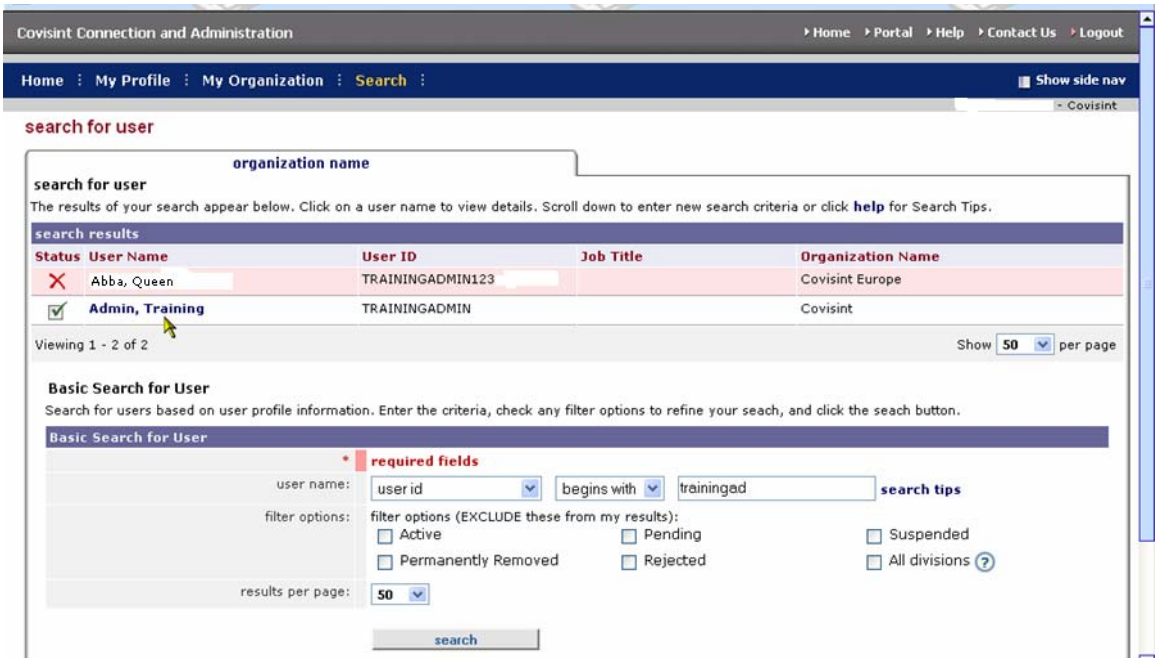
Users must be approved access to the Service Package called "Content Management", and then must request access to the sub-package for the appropriate 'customer version' of the Content Management Application. Therefore, the user would perform the following process to gain access to a 'customer version' of the application:

1. request access to **service package** Content Management Service Package.
2. receive approval for **service package** Content Management Service Package.
3. request access to **sub-package** "Customer-C Content Management"
4. receive approval for **sub-package** "Customer-C Content Management"

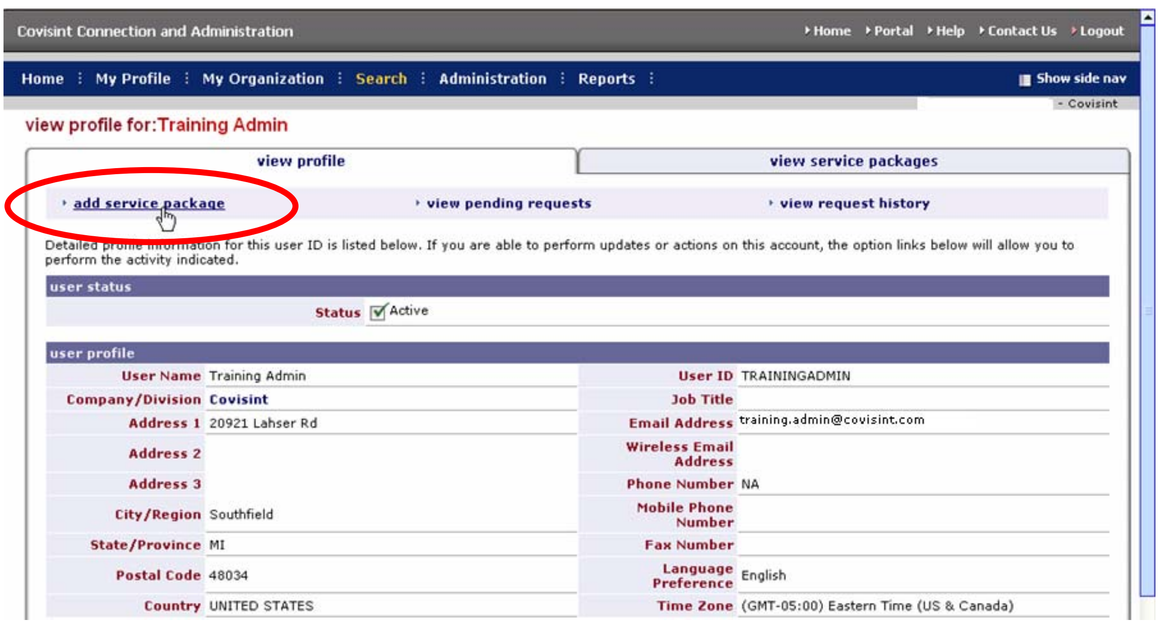
Complete the following steps to grant service packages to users in your organization.

You are only able to grant service package(s) to which your organization has access.

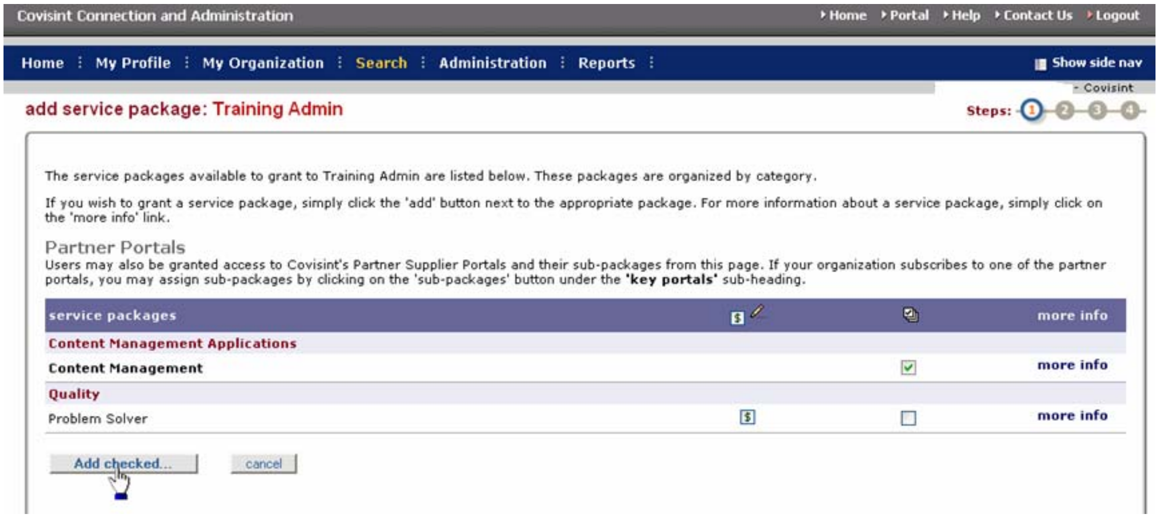
1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.



2. Click on the user name of the user for whom you searched. (This example uses a user named **Admin, Training**) The View Profile screen is displayed.



3. Click **add service package**. A list of all Services Packages to which your organization has access.



4. Enable the checkbox of each service package you wish to grant to this user.

5. Click **Add checked**…

	Some sub-packages may require additional Site Codes. Sub-packages that require additional Site Codes are denoted with the barcode icon. To request site codes, which may be associated with certain service packages or sub-packages, click on the sub-package name to view the details. Click **View Current Site Codes** to view the codes currently associated with this sub-package or click **Request Site Code** to request access to additional codes. Once you have requested access to site codes, your request will be routed to your administrator for approval.

6. Click **continue**

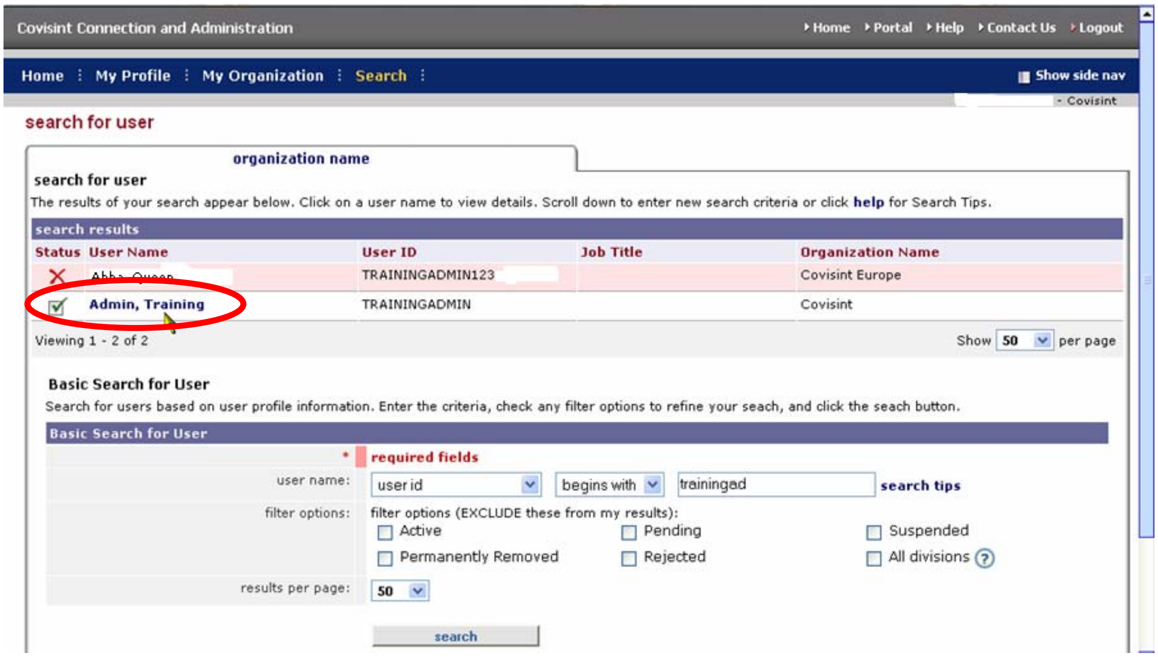
7. Click **submit**.

Result
You have successfully granted service package(s) to a user in your organization.

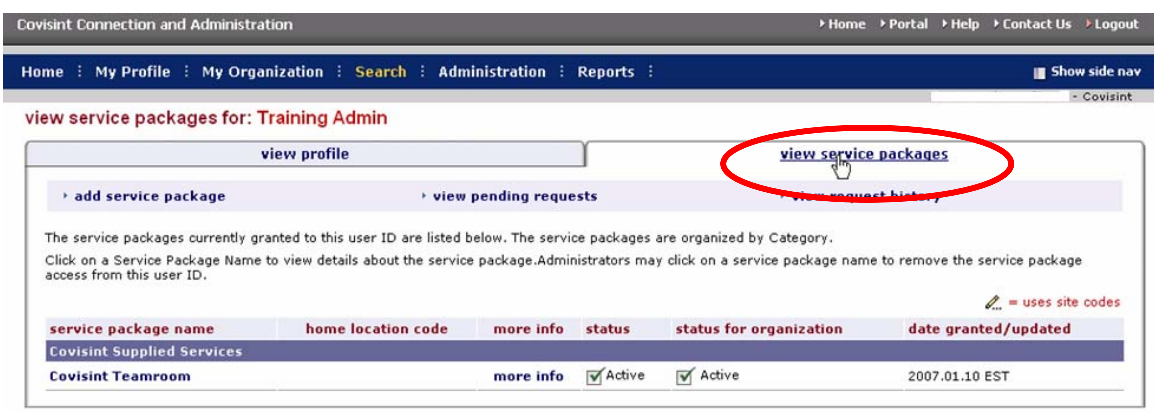
Removing a Service Package from a User in your Organization

Complete the following steps to remove service package(s) from users in your organization.

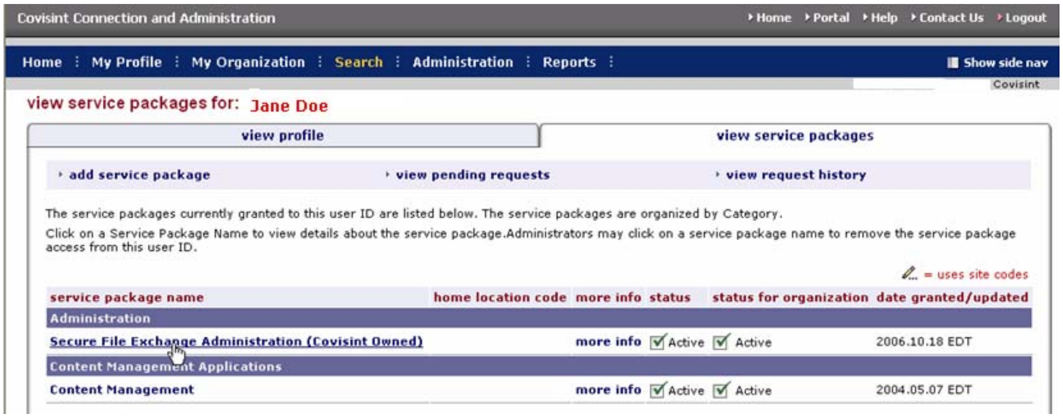
1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.



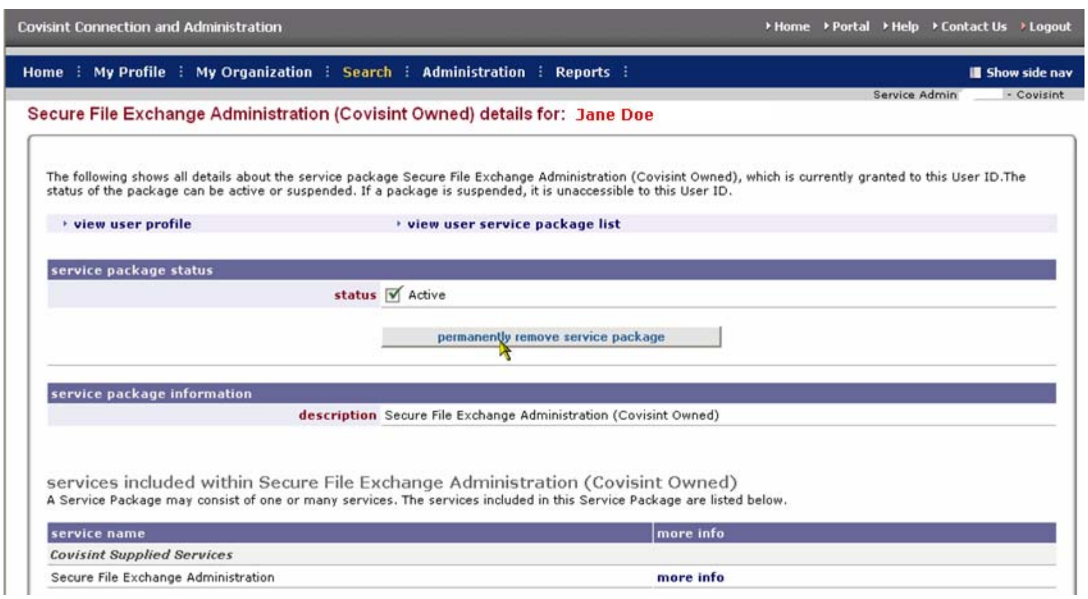
2. Click on the user name of the user for whom you searched. The View Profile screen is displayed.



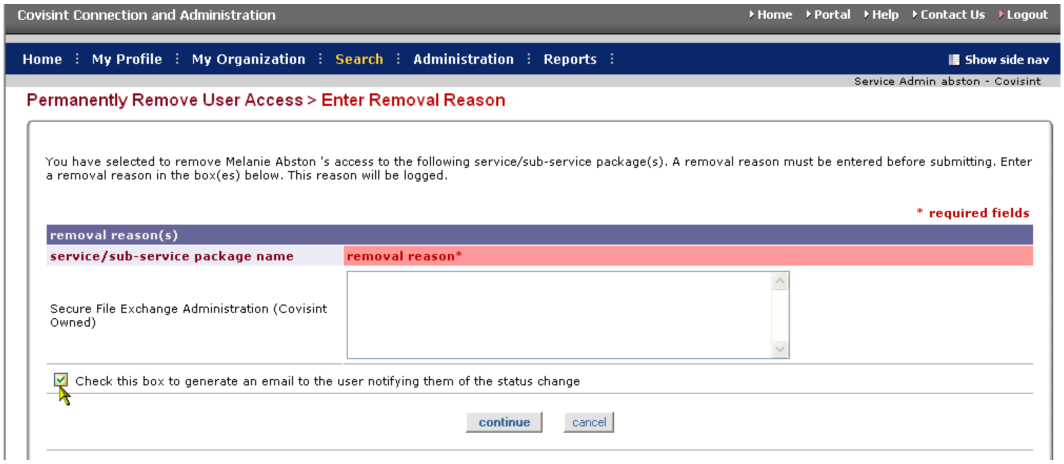
3. Click **view service packages** tab. A list of all Services Packages assigned to this user is displayed.



4. Click on the *name of the service package* you wish to remove from this user. The Service Package Details screen is displayed.



5. Click **permanently remove service package.** The Enter Removal Reason screen is displayed.



6. In the *removal reason* open text box, key in the reason for removing the service package from the user. (The text you enter in this box becomes part of this user's permanent record, and is viewable by all Security Administrators in your company).

7. Optionally, enable the checkbox if you wish to send an auto-generated email to the user, informing the user of the removal of the service package. The text you entered in step 6 will be included in the email.

8. Click **continue**. The Removal Confirmation Screen is displayed.

Result
You have successfully removed service package(s) from a user in your organization. If you wish to remove additional packages for this user, **click view user service package list** from the confirmation screen, and repeat steps 4 – 8 above.

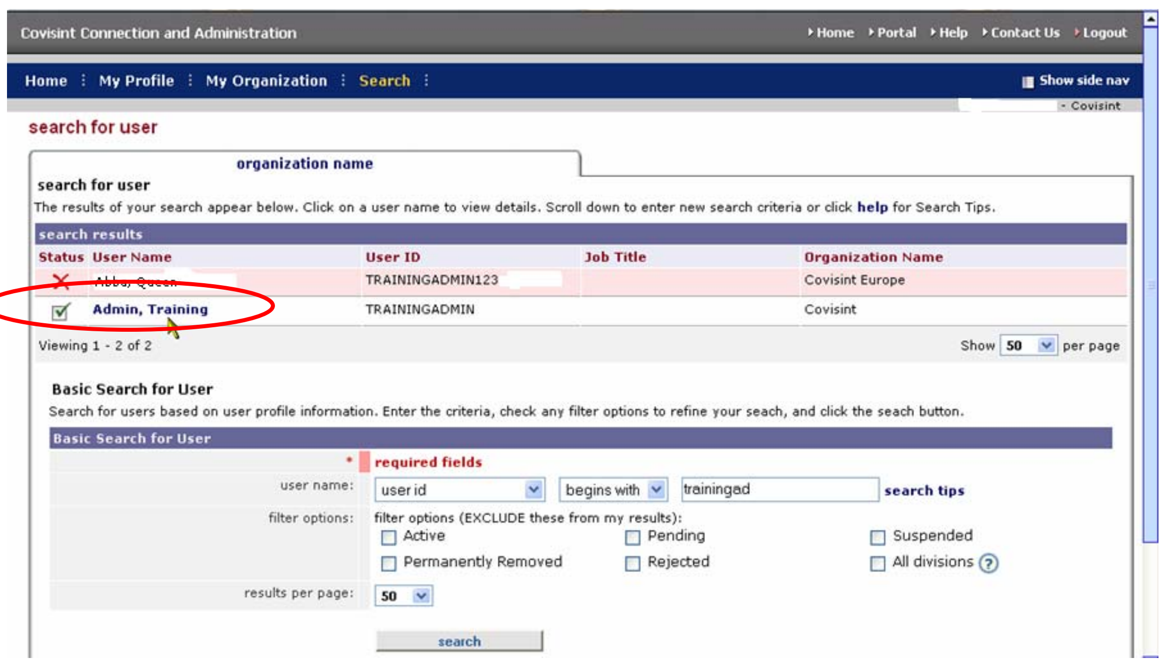
Suspending a User's Account

A suspended account is one whose package grants, roles, etc., remain in tact, but the user is unable to login. For example, organizations may suspend an account of users that are going on extended leave of absence and will not need to login to their accounts. A suspension reason is required and is logged upon completion, and is viewable by Security Administrators in the organization. Complete the following steps to suspend a user's account

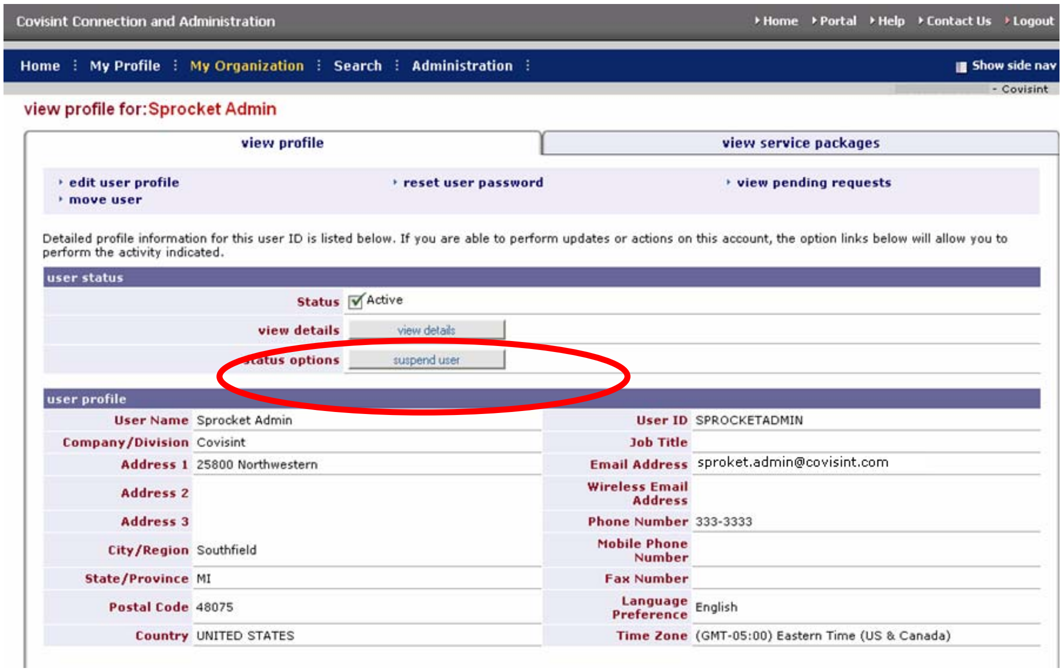
If you are required to suspend users in bulk, proceed to the section entitled performing user audits.

Suspended account: A suspended account is one whose package grants, roles, etc., remain in tact, but the user is unable to login.

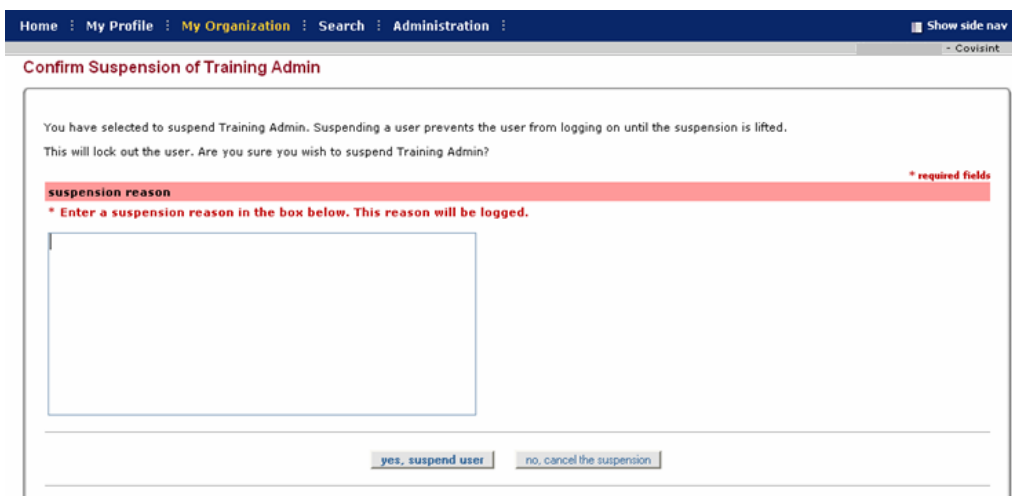
1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.



2. Click on the user name of the user for whom you searched. (This example uses a user named **Admin, Training**) The View Profile screen is displayed.



3. Click **suspend user**. The Suspend User screen is displayed.



4. Key in the reason for suspending the user account in the open text box.

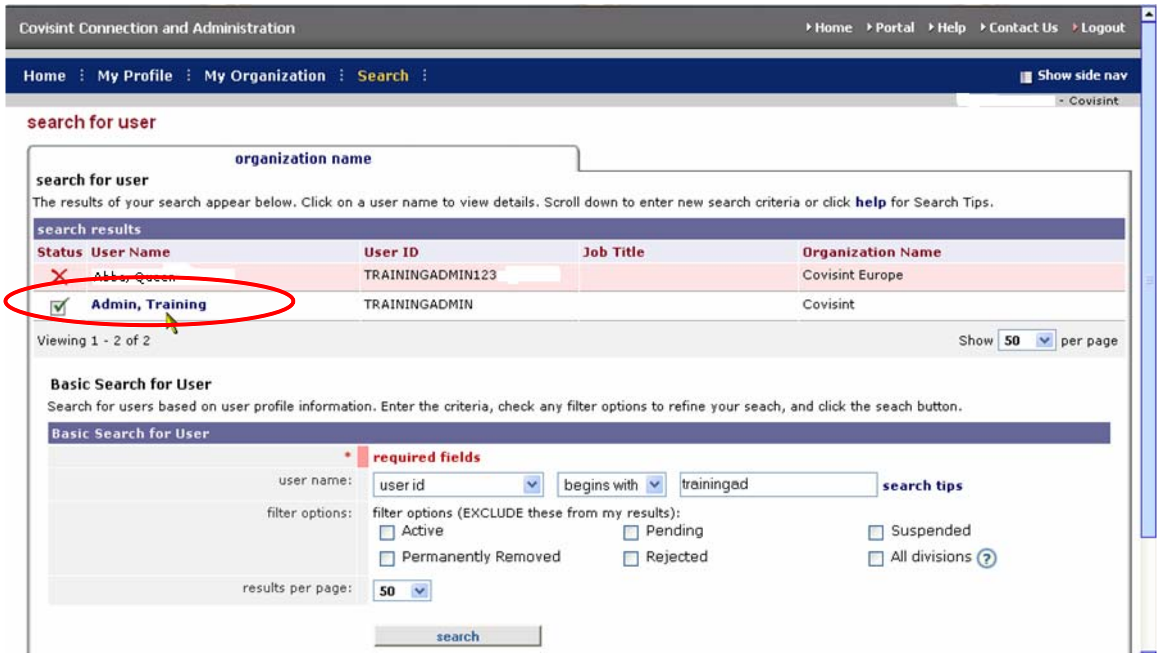
5. Click **yes, suspend user**.

Result
You have successfully suspended a user's account. The user will receive an email notification of the suspension, and is no longer able to login to the portal.

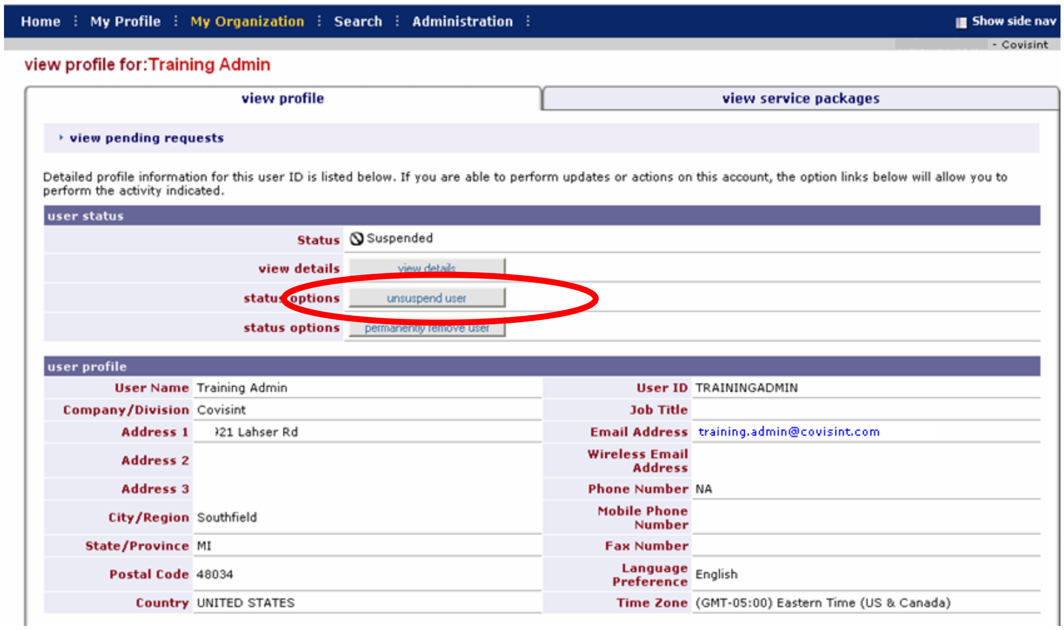
Unsuspending a Suspended User Account

Complete the following steps to reverse the suspension on a user account.

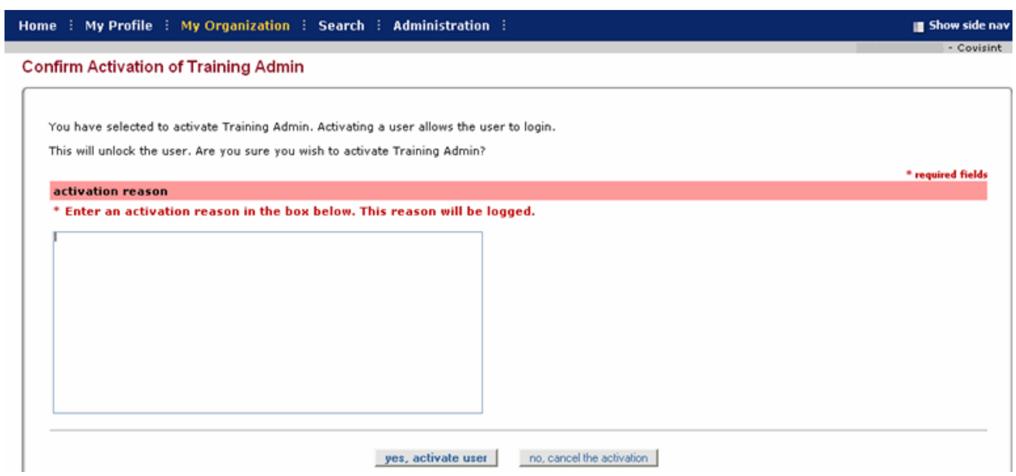
1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.



2. Click on the user name of the user for whom you searched. (This example uses a user named **Admin, Training**) The View Profile screen is displayed.



3. Click **unsuspend user**. The Confirm Activation of User screen is displayed.



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 account. The user will receive an email notification of the status change, and is now able to login to the portal.

Permanently Removing (Terminating) a User Account

The act of permanently removing a user is permanent (cannot be undone) and forever restricts the user account from being used. Users that are permanently removed will lose all roles, all service packages, and will never be able to login to that account.

> You are not able to terminate a user if that user is the only person assigned the Security Administrator role. You must first modify the role of another user and assign the Security Administrator role.
>
> If the user you wish to terminate is the sole Security Administrator and sole user, and there are no other users in that company, you will not be able to terminate the user. You will instead terminate the company. Only the Security Administrator for your organization can terminate a company.

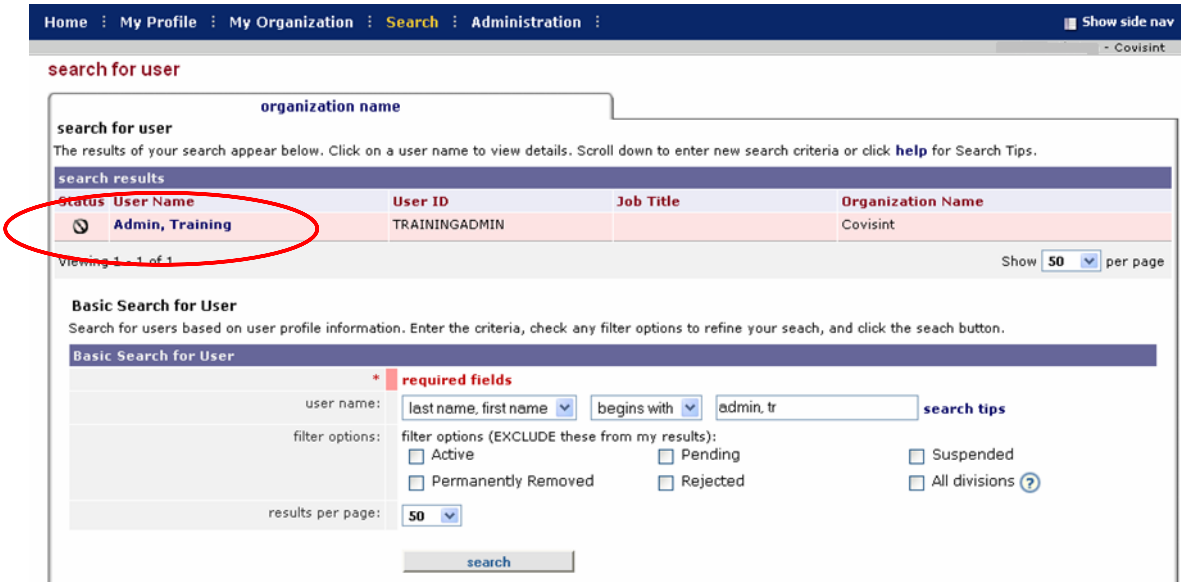
Only suspended user accounts may be removed from the CCA system. Refer to the section entitled Suspending a User Account for details.

> **Permanently Removed User Account:** A user account that can never be used to login. Typically, the permanently remove function is used when a user leaves the company and is not expected to return.

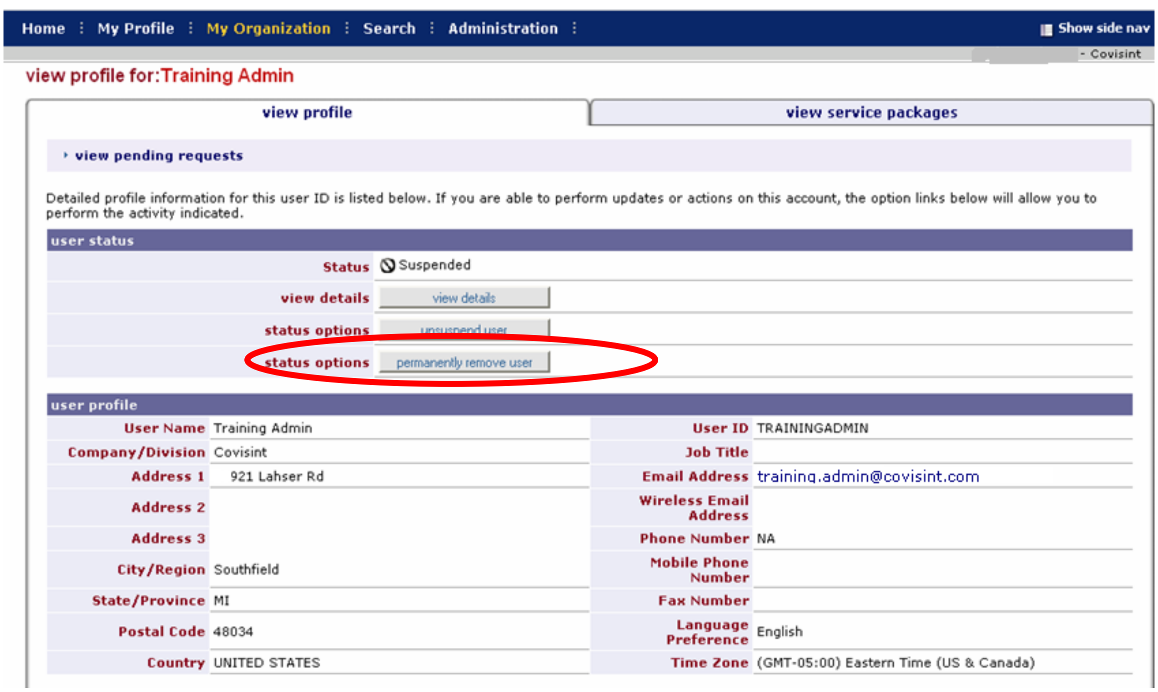
A removal reason is required and is manually entered. The termination reason becomes part of the user's permanent record, and is viewable by other Security Administrators for that company.

Complete the following steps to permanently remove a user's account.

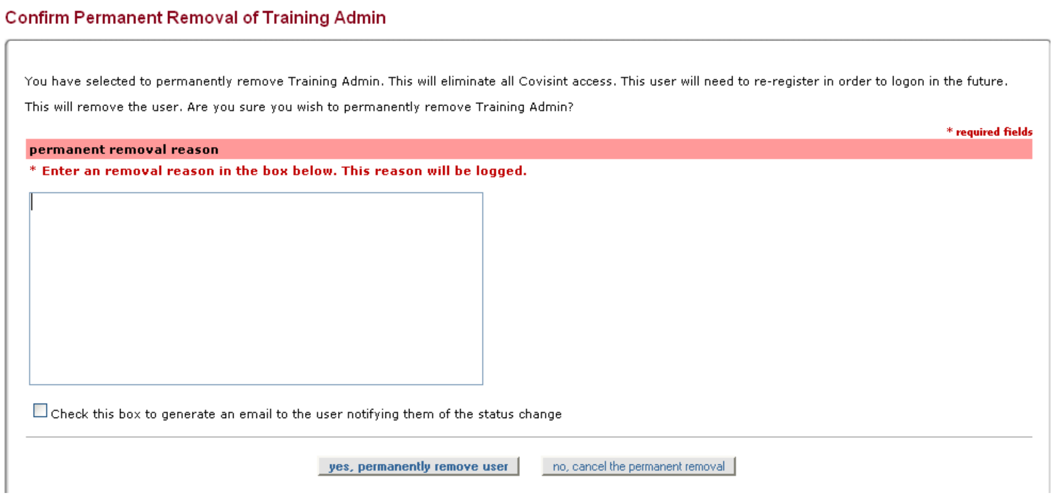
1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.



2. Click on the user name of the user for whom you searched. (This example uses a user named **Admin, Training**) The View Profile screen is displayed.



3. Click **permanently remove user**. The Confirm Permanent Removal of User screen is displayed.



4. Key in the reason for removing the user account in the open text box.

	Recall that the act of termination is permanent (cannot be undone) and forever restricts the user from logging in to the account.

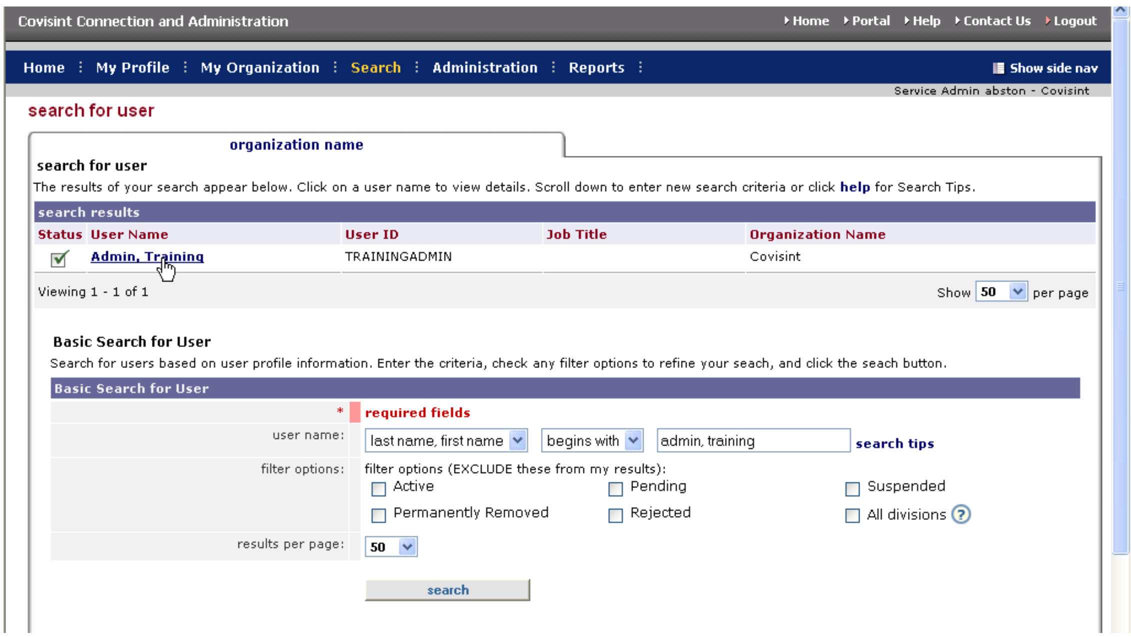
5. Click **yes, permanently remove user**.

Result
You have successfully removed the user account from the CCA system. The user is not able to login to the portal, and can not be reactivated.

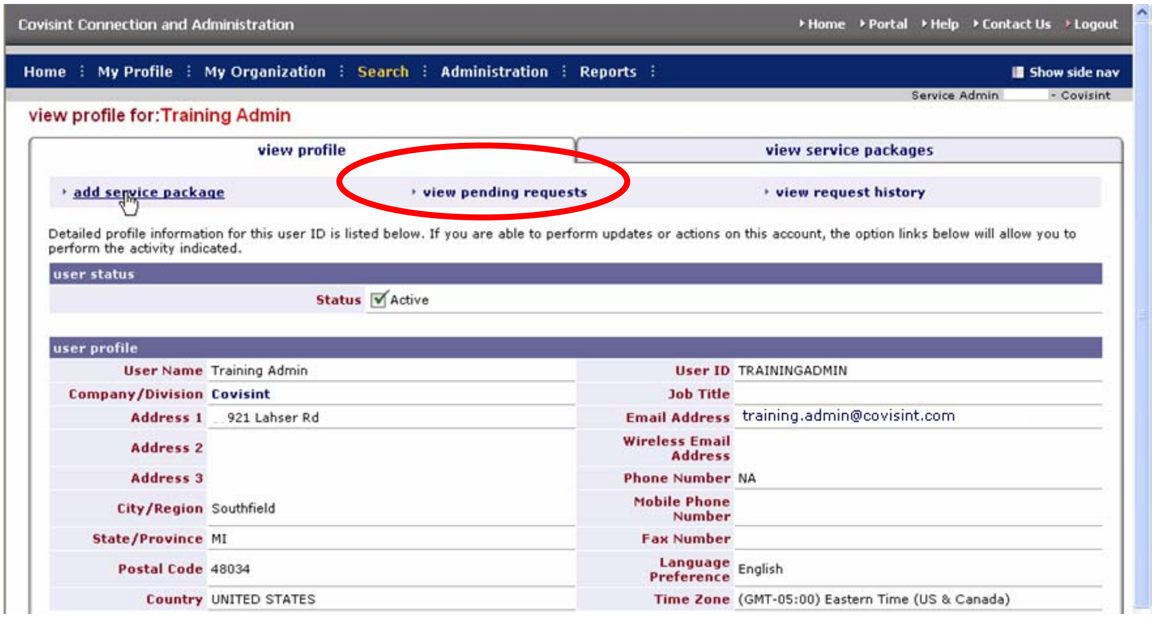
Viewing a User's Pending Requests

Administrators receive email alerts when a new request is submitted. Within the email is a link that takes the Administrator straight to the pending request screen. Alternately, Administrators may complete the following steps to view a user's pending request.

1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.



2. Click on the user name of the user for whom you searched. (This example uses a user named **Admin, Training**). The View Profile screen is displayed.



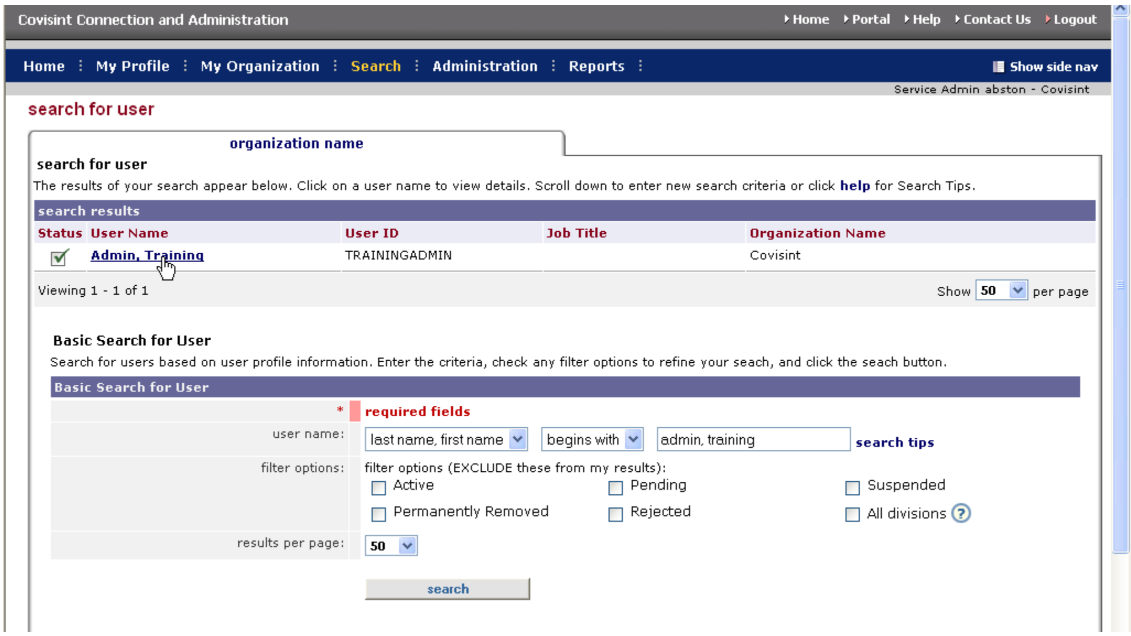
3. Click **view pending requests.** A list of all pending service package requests is displayed.

Result
You have successfully viewed pending service package requests for a user in your organization. If you wish to approve the request from this screen, click on the request name in the request type column. Click here to view work steps for approving pending requests.

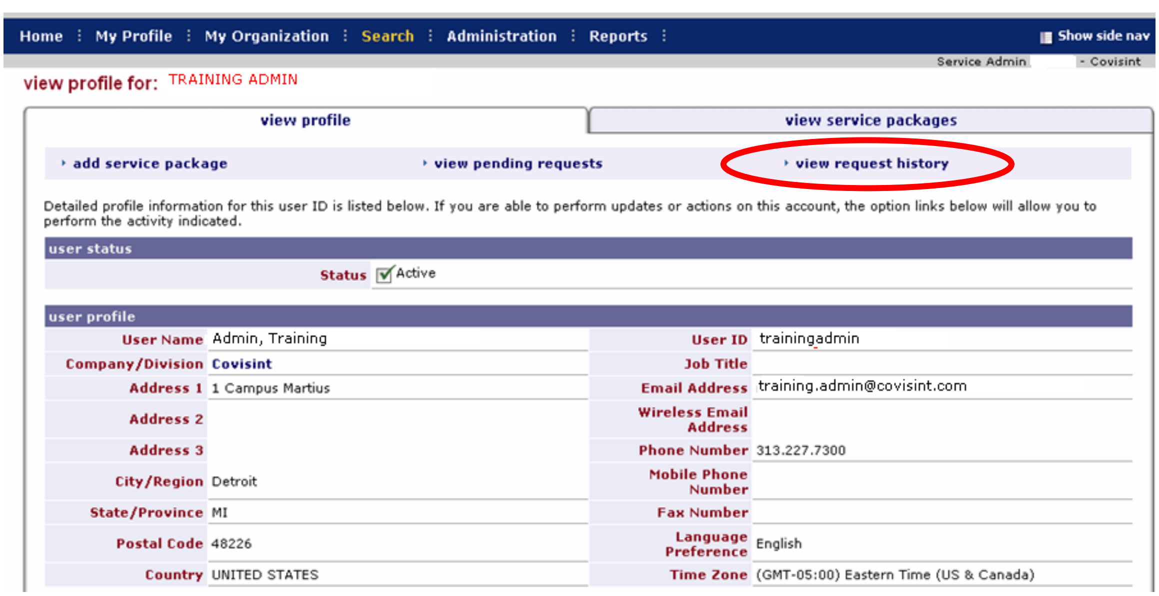
Viewing a User's Request History

Complete the following steps to view a user's request history.

1. Perform a User Search. Refer to the previous section entitled *Searching for Users in your Organization* for details. The User Search result screen is displayed.



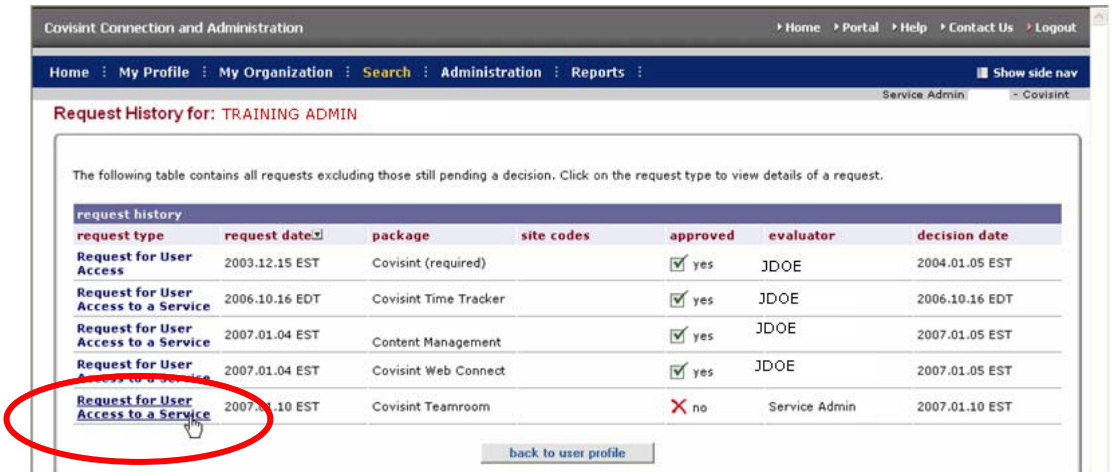
2. Click on the user name of the user for whom you searched. (This example uses a user named **Admin, Training**) The View Profile screen is displayed.



3. Click **view request history.** A list of all requests submitted by this user is listed.

The history screen displays the following information:

- Type of request
- Date of request
- Service package requested
- Site code(s) requested (if applicable)
- Approval status
- Name of the deciding Administrator
- Date of decision



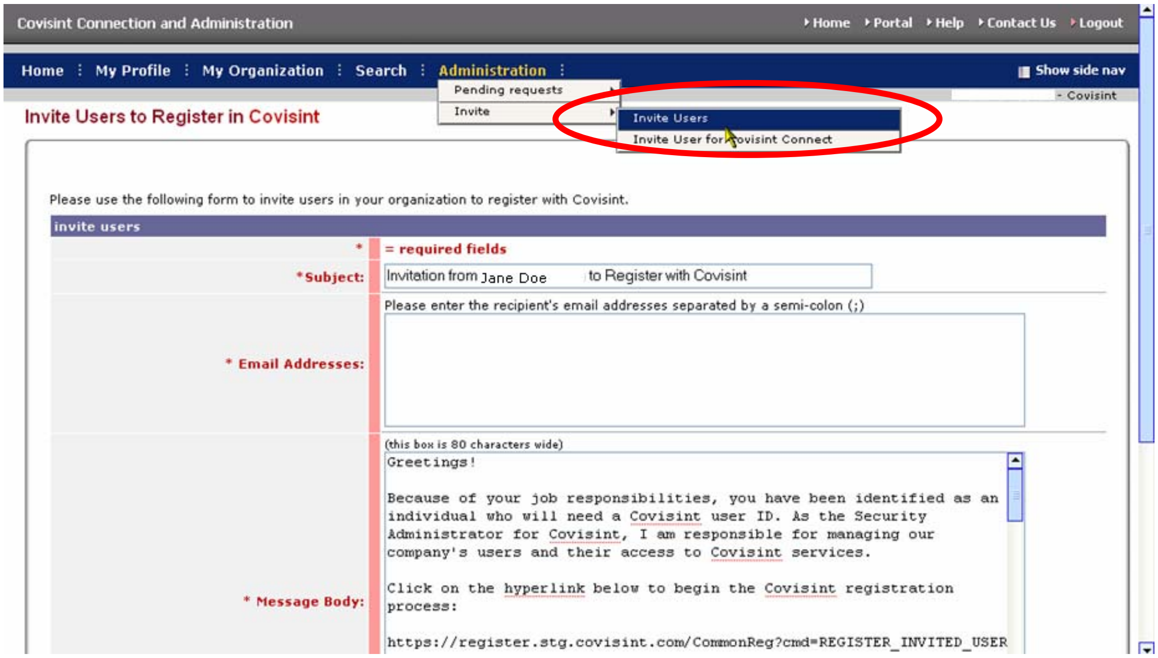
4. If you wish to view additional details for an item, click on that item name in the 'request type column.

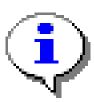
From this screen, you are able to view additional details, such as the reason for rejection submitted by the deciding administrator.

Result
You have successfully viewed a request history for a user in your organization.

Inviting User to Register for a New User Account

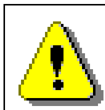
1. Click **Invite Users** from the *Administration -> Invite* drop down menu. The invitation screen is displayed.





The *Subject line* and the *Message body* fields are populated by default. While these fields are editable, it is recommended that you do not modify the text as editing the actual invitation URL within the invitation text could break the link.

2. In the Email Address open text field, key in the email address for each recipient you wish to invite, separated by a semi-colon (;) (For example, a list of users: user1@mycompany.com; user2@bluecompany.com; user3@pinkcompany.com).



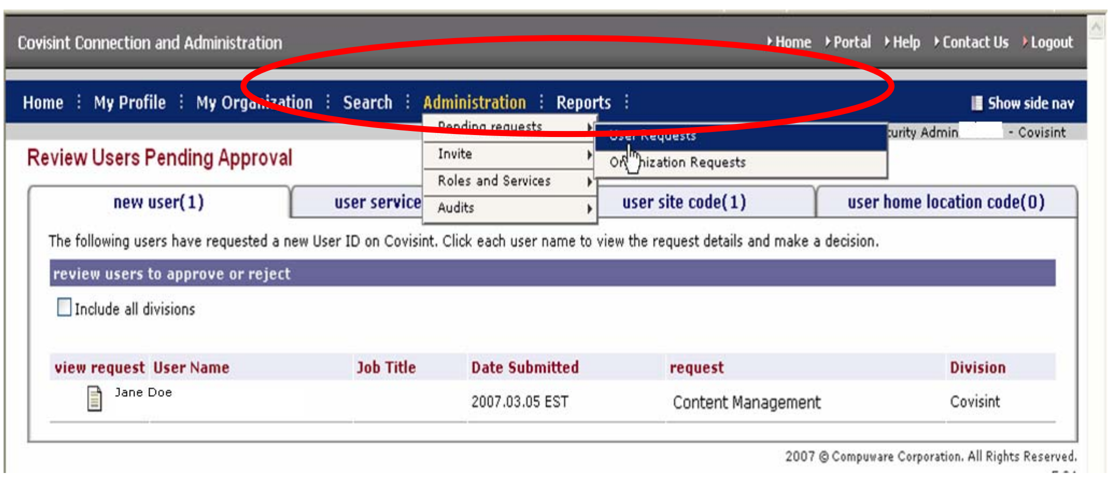
The system does not validate the accuracy of the email addresses that you key in. If an email invitation cannot be delivered for any reason, the administrator will ***not*** be notified of this failure.

3. Click **Send Invitation**.

4. Click **OK** to confirm. The email invitations are sent to the email addresses. You will receive email notification of each registration request. The Pending User Requests queue displays all users who have registered and are pending approval.

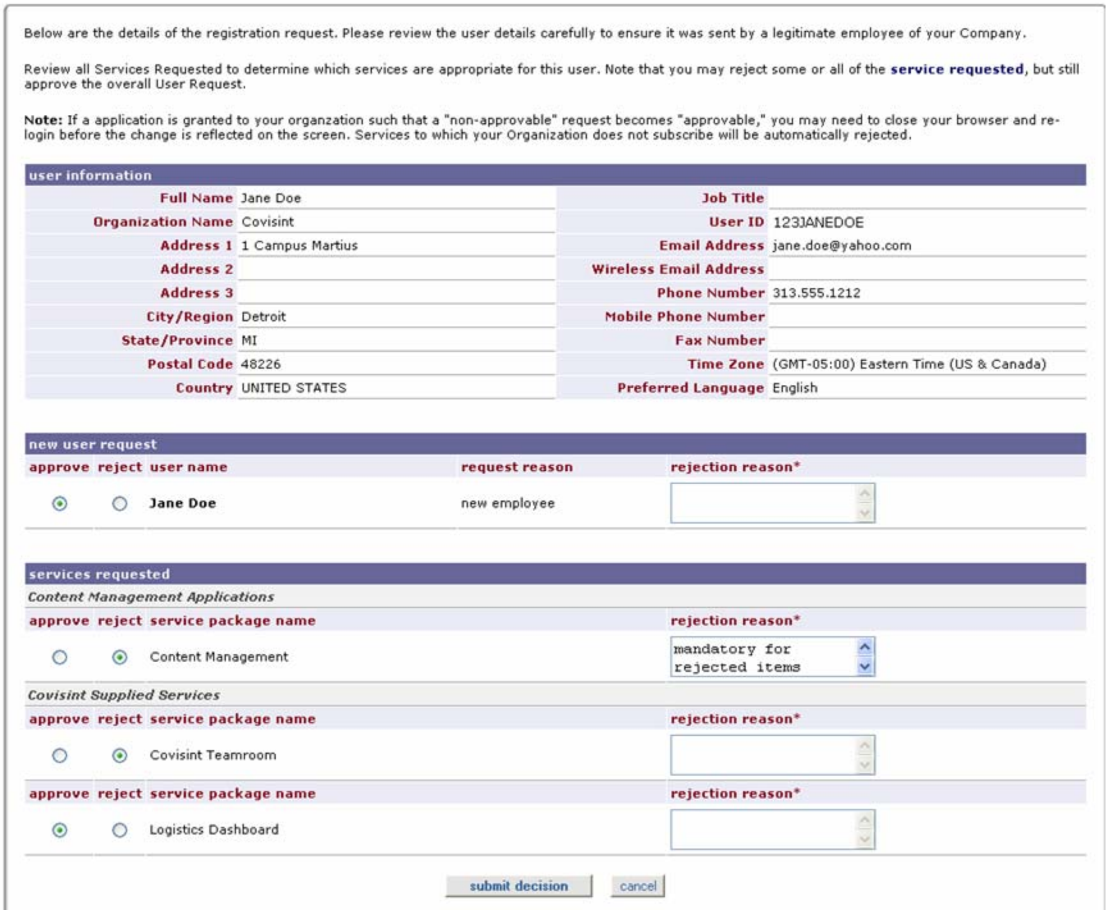
Result
You have successfully invited a user to register. You will receive an email notification once the user has successfully registered. At that time, you shall log in to issue a decision on the pending user requests.

Managing Pending New User Account Requests



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

2. Click  to view the details of the request.



3. Perform one or more of the following:

If you wish to…	Then…
approve the new user request	Enable the Approve radio button for the request.

If you wish to…	Then…
reject the new user request	a. Enable the Reject radio for the request. a. As required, key in the reason for the rejection in the open text field. (The text you enter in this box becomes part of this user's permanent record, and is viewable by all Security Administrators in your company). **Note**: If you reject a new user request, all service package requests for that user are automatically rejected.
approve the service requested by the new approved user (Note that new users and new service packages are listed together in the same tab)	Enable the Approve radio button for the service.
reject the new user's service package request	a. Enable the Reject radio for the service package request. b. As required, key in the reason for the rejection in the open text field. (The text you enter in this box becomes part of this user's permanent record, and is viewable by all Security Administrators in your company).
approve site code requests	Enable the Approve radio button for the site code.
reject site code requests	a. Enable the Reject radio for the site code request. a. As required, key in the reason for the rejection in the open text field. (The text you enter in this box becomes part of this user's permanent record, and is viewable by all Security Administrators in your company).
approve home location code requests	Enable the Approve radio button for the home location code.

If you wish to…	Then…
reject home location code requests	a. Enable the Reject radio for the home location code request. b. As required, key in the reason for the rejection in the open text field. (The text you enter in this box becomes part of this user's permanent record, and is viewable by all Security Administrators in your company).

Supplier Code/Location Code: The supplier code associated with a user's grant to the parent portal package (i.e. Ford Supplier Portal) is typically known as the user's location code. Note: Each portal owner may have a slightly different term that they use (i.e. home location code). The location code designates the user's primary office location. Some applications within the portal use the location code to determine what items the user can view in the application. Other applications refer to the specific supplier codes associated with the user's grant to that application to determine what items the user can view.

4. Click **submit decision**.
5. Click **OK** to confirm issuing a decision regarding the new user account request.

Result
You have successfully managed a new user's pending requests.

Service Authority Organization (SAO)

Service Authority Organization: The Covisint Connection and Administration (CCA) tool allows companies to create multiple administrative organizations for a single Legal Corporation. For example, a company's European offices may have a completely separate CCA organization from the North American offices' CCA organizations. Most Portal packages, such as the Ford and DaimlerChrysler Supplier Portals, require relationships between these organizations based on the Supplier Code. The Service Authority Organization is a designation of primary responsibility for all organizations with the same parent supplier code.

Service Authority Organization Responsibilities

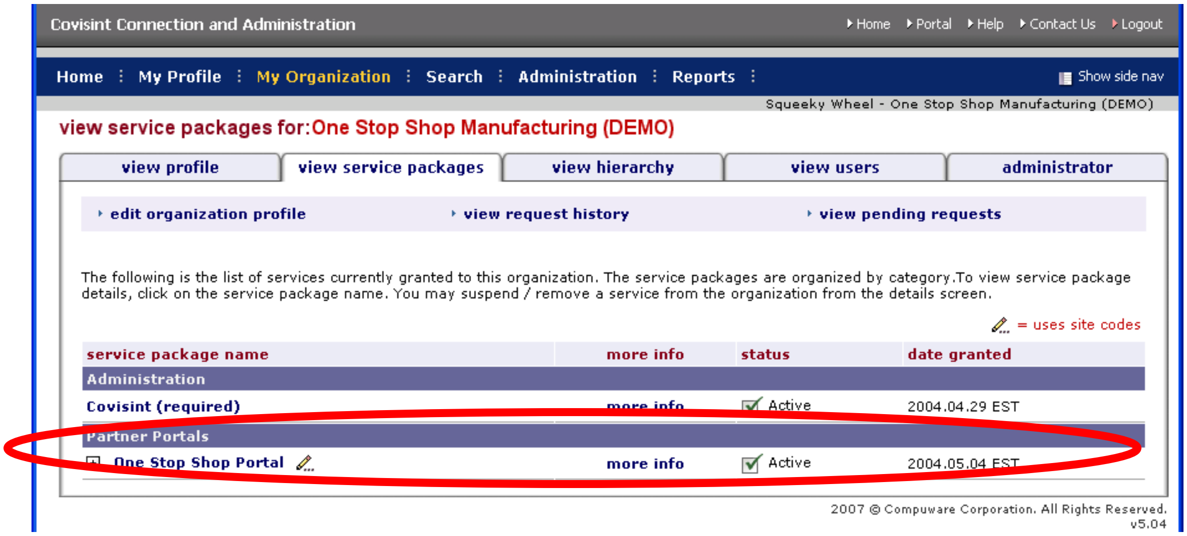
- Approve Requests for the service submitted by related organizations
- Approve and Revoke Site Codes grants to related organizations
- Revoke access to the service from related organizations

For details on pending requests for organizations, refer to the section entitled "Who Approves an Organization Request?"

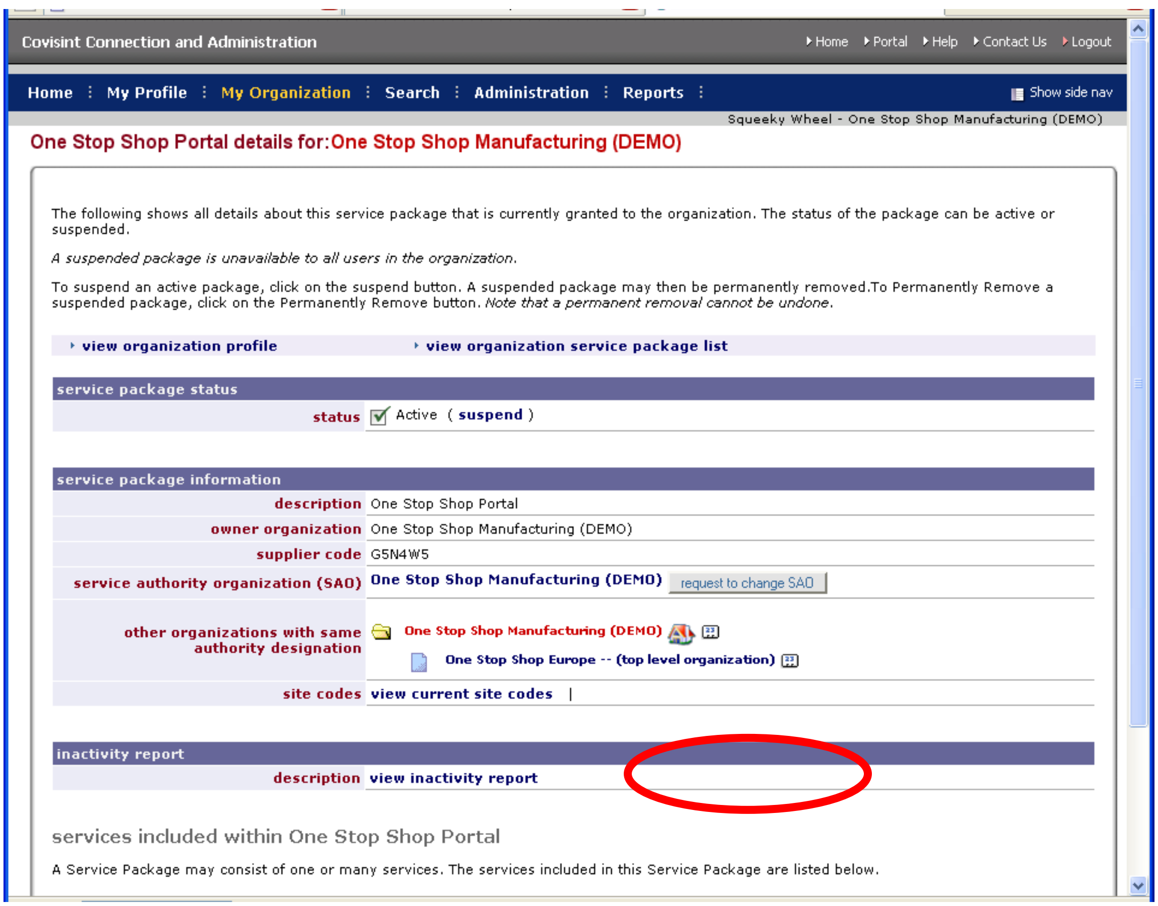
Changing the SAO Designation

In the case where multiple distinct CCA organizations have the same parent supplier code attached to a portal grant, the SAO designation can be switched between those related organizations. The organization that currently has the SAO designation must initiate the process.

1. Click **View my Organization Service Packages** from the My Organization drop down menu. The View Service Package Screen is displayed.



2. Click on the *name of the portal service package* for which you wish to change the SAO designation. The Details Screen for that service package is displayed.



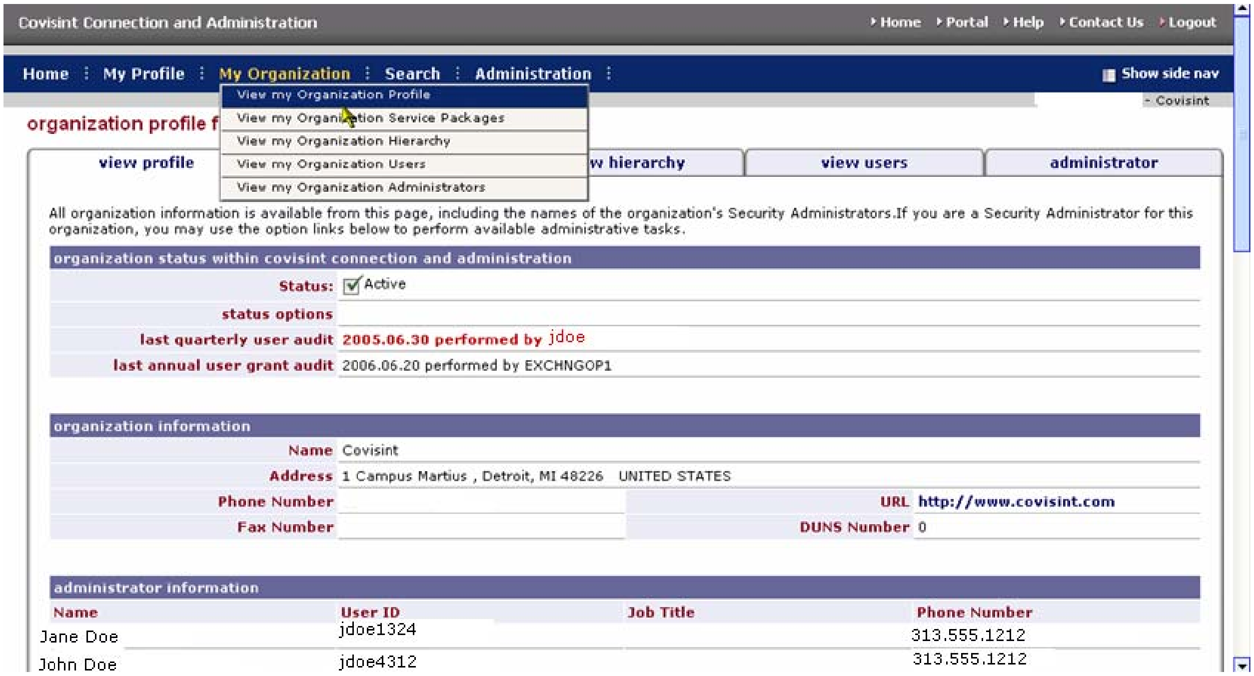
3. Click **request to change SAO**.

4. Select the organization to receive the SAO designation. If there are no organizations listed, it means that no other CCA organization has the same parent supplier code for the portal package selected.

5. Review the change and click **submit**.

Result
You have successfully changed the SAO designation for a service package for your organization.

Viewing the Administrator's view of Organization Profile



Perform one or more of the following:

If you wish to…	Then…
View the current service packages to which your organization subscribes	a. Click **View my Organization Profile** from the My Organization drop down menu. The View Profile tab is displayed. This tab provides a detailed view of the parent level of your organization. b. Click **view service packages** tab. The View service packages screen is displayed. From this screen, you are able to view packages and sub packages to which your organization currently has access. To view details of any service package grant, simply click the package name.
view the current hierarchy of your organization within CCA	a. Click **View my Organization Profile** from the My Organization drop down menu. The View Profile tab is displayed. This tab provides a detailed view of the parent level of your organization. b. Click **view hierarchy** tab. This page reflects the Covisint user administration model, not necessarily the legal or physical structure of your organization. To view an organization, simply click on its name within the tree.

If you wish to…	Then…
view users within your organization	a. Click **View my Organization Profile** from the My Organization drop down menu. The View Profile tab is displayed. This tab provides a detailed view of the parent level of your organization. b. Click **view user** tab. All users registered in the organization are displayed.
view users in a particular division of your organization	a. Click **View my Organization Profile** from the My Organization drop down menu. The View Profile tab is displayed. This tab provides a detailed view of the parent level of your organization. b. Click **view hierarchy** tab. c. Click on the name of the division. d. Click **view user** tab. All users registered in the selected division are displayed.
view all administrators in your organization	a. Click **View my Organization Profile** from the My Organization drop down menu. The View Profile tab is displayed. This tab provides a detailed view of the parent level of your organization. b. Click **administrator** tab. All administrators in your organization are displayed.
view administrators in a particular division of your organization	a. Click **View my Organization Profile** from the My Organization drop down menu. The View Profile tab is displayed. This tab provides a detailed view of the parent level of your organization. b. Click **view hierarchy** tab. c. Click on the *name of the division*. d. Click **administrator** tab. All users registered in the selected division are displayed.
edit your organization profile	a. Click **edit organization profile**. b. Edit as desired. c. Click **submit changes**.

If you wish to…	Then…
View pending organization requests	Click **view pending requests**.

Result
You have successfully viewed organization details from an administrator perspective.

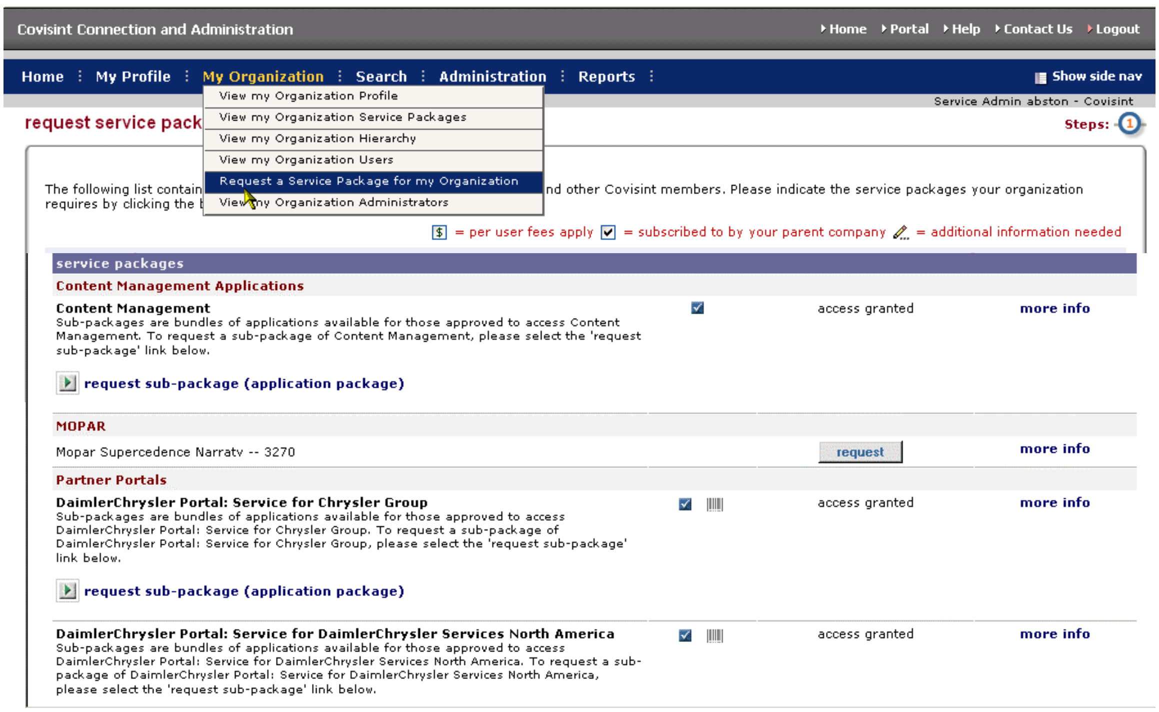
Managing Your Organization Service Packages

As the Security Administrator, you are able to manage your organization's service packages.

Icons indicating the following functionality are noted next to each service package as appropriate:

- Packages already owned by your parent company (if applicable) are denoted by a check mark
- Packages that require additional information are indicated with a pencil icon
- Packages that will cause the user to incur fees are denoted with a dollar sign
- Packages that require site codes are indicated with the barcode icon

Requesting a Service Package for Your Organization



Perform one or more of the following

If you wish to…	Then…
Request a service package	1. Click **Request a Service Package for my Organization** from the My Organization drop down menu. The Request Screen is displayed. A list of all service packages are displayed. 2. Click **request**. 3. Key in the reason for the request in the open text box. 4. Click **continue**. This request for service package is submitted to the approving administrator.
Request a sub-package of a service package (The package must be granted to the organization before the sub-package can be requested or granted).	1. Click **Request a Service Package for my Organization** from the My Organization drop down menu. The Request Screen is displayed. A list of all service packages are displayed. 2. Click **request sub package**. This request for sub package is submitted to the approving administrator.

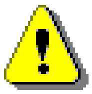
Result
You have successfully requested a package or sub-package for your organization. For details on pending requests for organizations, refer to the section entitled "Who Approves an Organization Request?"

Who Approves an Organization Request?

Organization Approval Matrix

If the Requestor is…	And the Package Owner is…	Then the Approver is the…
an SAO	a Portal Partner	Portal Partner Admin
a top-level non-SAO	a Portal Partner	SAO Admin
a Top-level Org	Covisint	Covisint Admin
a Division	any	Division's Parent Company Admin

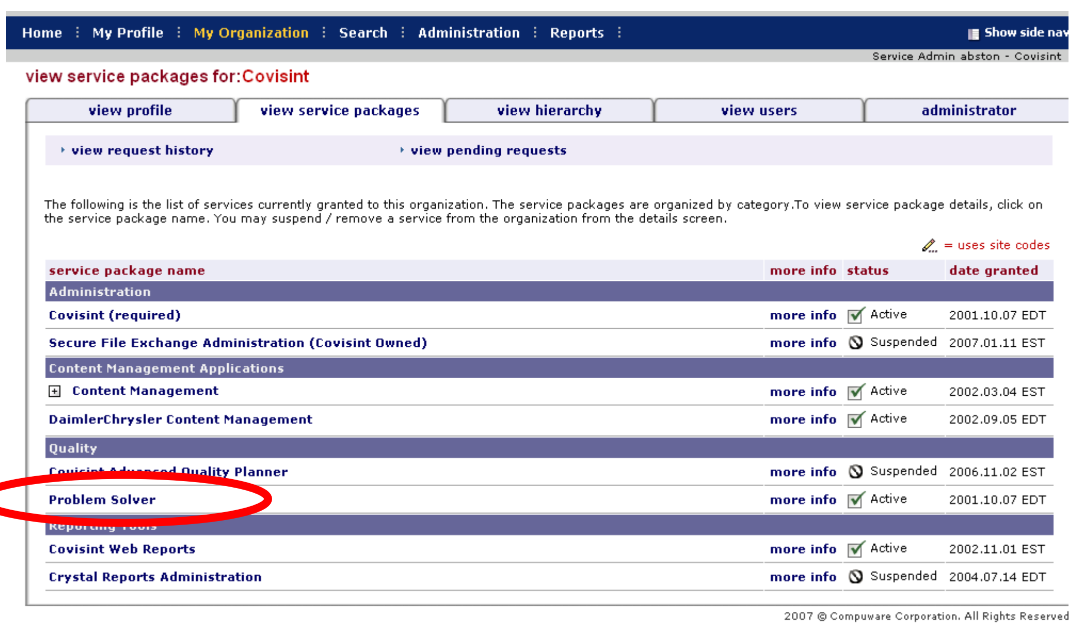
Suspending a Service Package From Your Organization



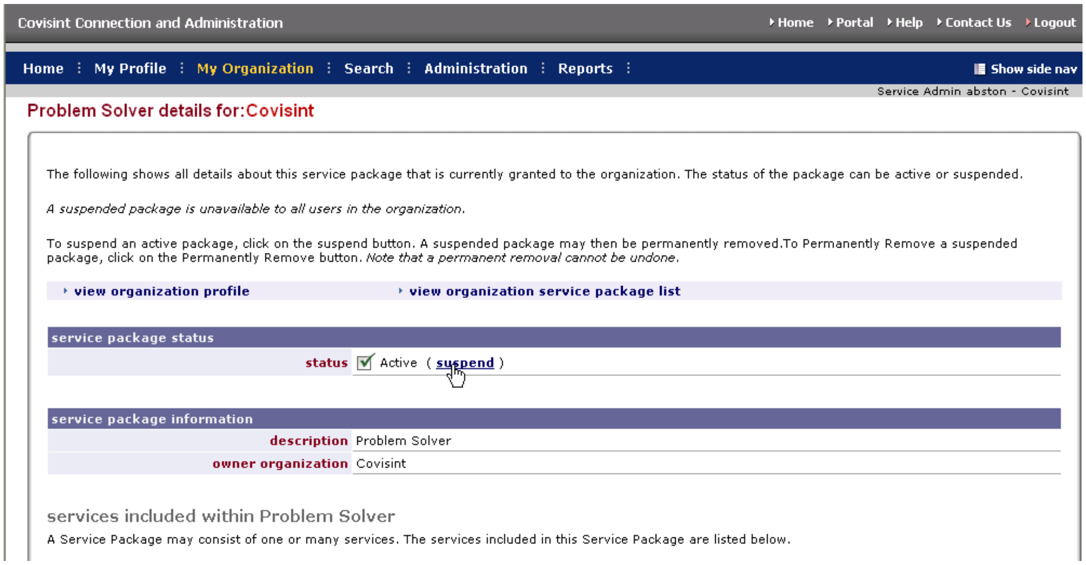
Warning: Suspending a service package from your organization is not easily undone. Once you suspend your organization's access to a service package, it can only be reinstated by contacting Covisint. Once you suspend your organization's access to a service package, it can only be reinstated by requesting the package for your organization. This includes packages that were auto-granted to your organization. For details on pending requests for organizations, refer to the section entitled "Who Approves an Organization Request?" **You may prefer to suspend the service package from individual users in your organization.** By 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.

Security Administrators are able to suspend the Organization's access to any service for which they are assigned as Administrator. The locked state prevents all users in the organization from logging in to the suspended service. If users try to login, they receive an "unauthorized" message. Once a service package is suspended, it can only be reinstated by Covisint. You are not able to reactivate a suspended service package.

1. Click **View my Organization Service Packages** from the My Organization drop down menu. The View Service Package Screen is displayed.



2. Click on the *name of the service package* you wish to suspend. The Details Screen for that service package is displayed.



3. Click **suspend**.

Warning: 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. This includes packages that were auto-granted to your organization. For details on pending requests for organizations, refer to the section entitled "Who Approves an Organization Request?" **You may prefer to suspend the service package from individual users in your organization.** By 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.

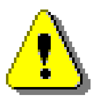
4. Key in the *reason for suspension* in the open text box.

5. Click **yes, proceed with suspension**. The suspension is logged in the history along with the name of the Administrator performing the task.

Result
You have successfully suspended a service package for your organization.

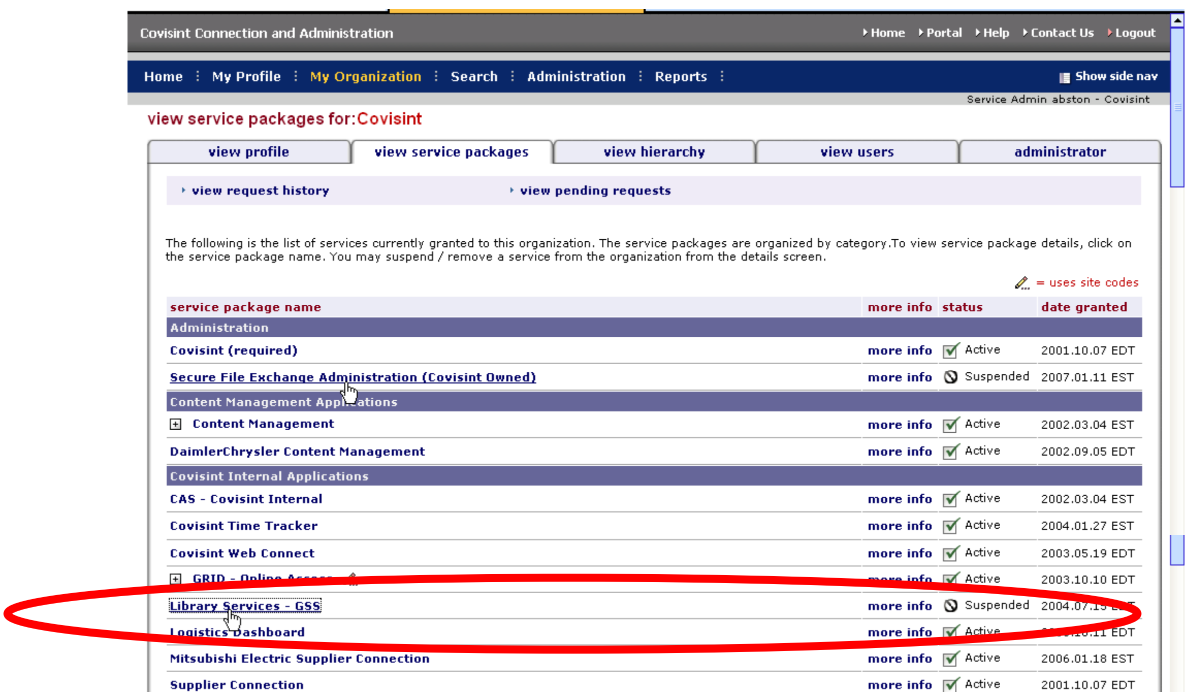
Permanently Removing a Suspended Service Package For Your Organization

Security Administrators are able to permanently remove a suspended service package for the Organization for any service to which they are assigned as Administrator. Once removed, the service package can no longer be reinstated by Covisint.

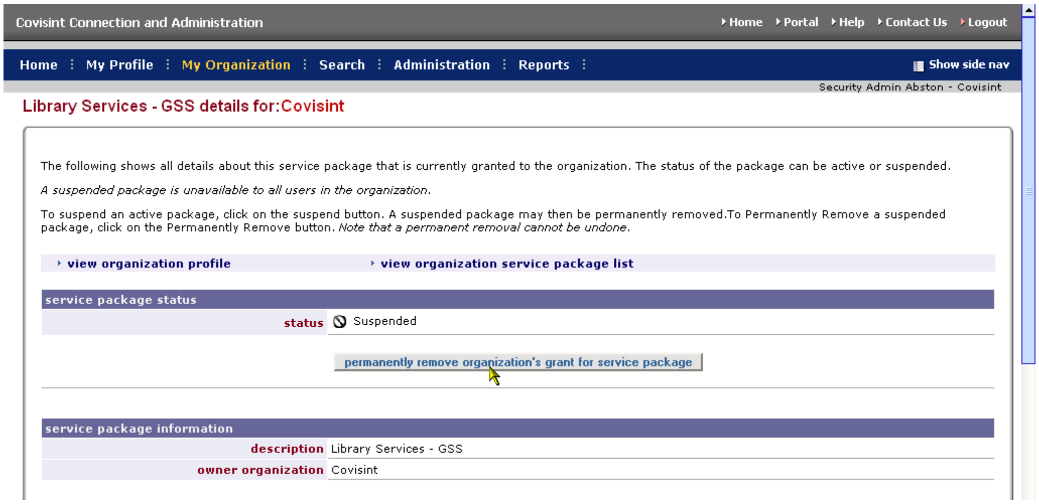


Once permanently removed, the service package is permanently removed from all users in the organization, and all divisions below. The service package cannot be reinstated. This includes packages that were auto-granted to your organization. For details on pending requests for organizations, refer to the section entitled "Who Approves an Organization Request?"

1. Click **View my Organization Service Packages** from the My Organization drop down menu. The View Service Package Screen is displayed.



2. Click on the *name of the suspended service package* you wish to permanently remove. The Details Screen for that service package is displayed.



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. The permanent removal is logged in the history
along with the name of the Administrator performing the task.

Result
You have successfully removed a suspended service package for your organization.

Managing Service Packages for Divisions of Your Organization

As the Security Administrator, you are able to manage service packages for divisions in your organization. You are able to grant, suspend, and remove service packages from divisions in your organization.

Granting a Service Package to a Division in your Organization

Security Administrators are able to grant some Service Packages as well as Sub-Packages to divisions in their organization. The division must be at a lower tier in the hierarchy, and the parent organization must have access to the service package. (Sub-packages are designed such that the parent package must be granted before the sub-packages become available).

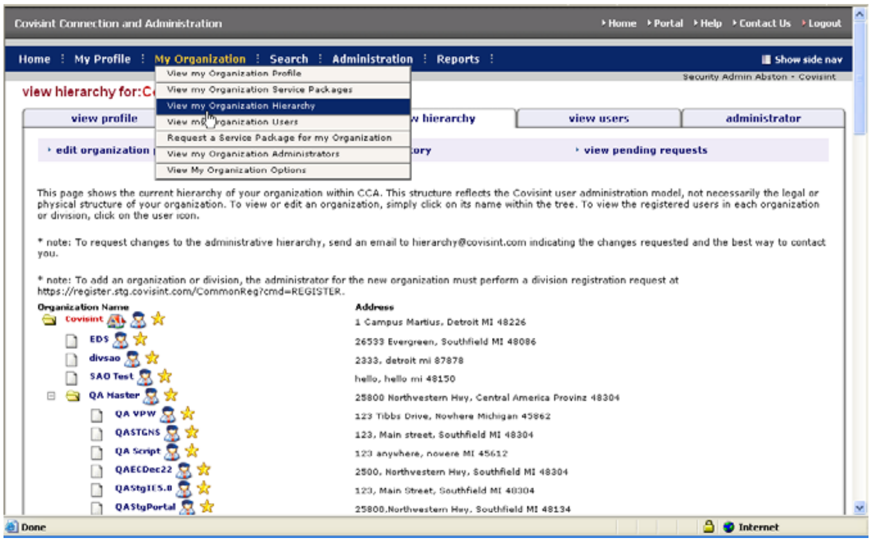
The division must be at a lower tier in the hierarchy, and the parent organization must have access to the service package.

Service Package – a grantable container that contains at least one application or tool accessed via Covisint portal. Some Service Packages contain sub-packages.

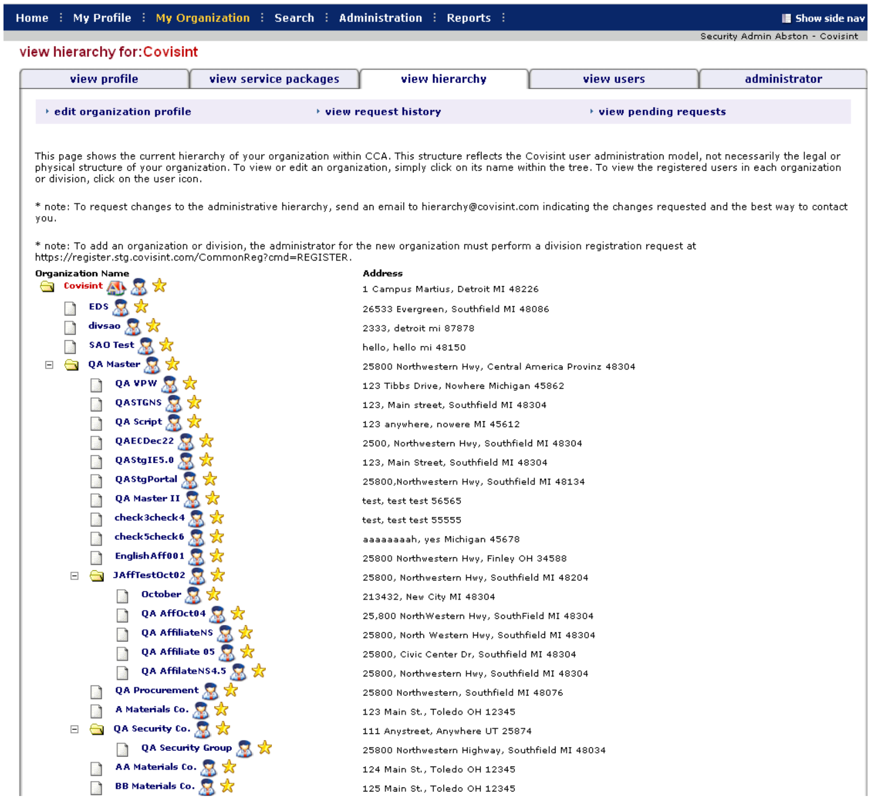
Sub-package – a grantable container that contains at least one sub-service application. The sub-package requires that the parent package be granted first.

Complete the following steps to grant service packages to divisions in your organization.

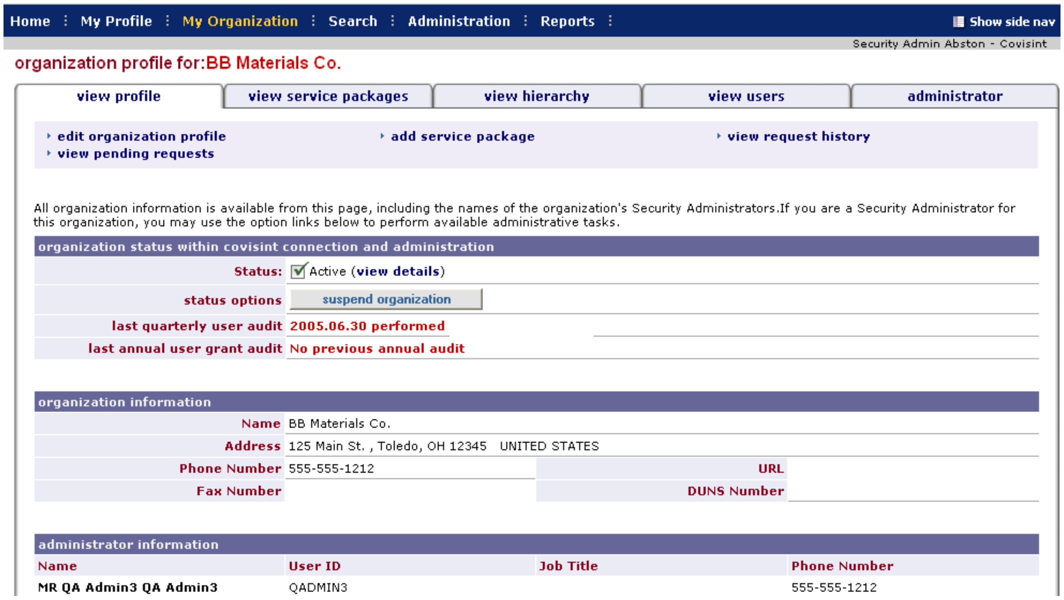
You are only able to grant service package(s) to which your organization has access.



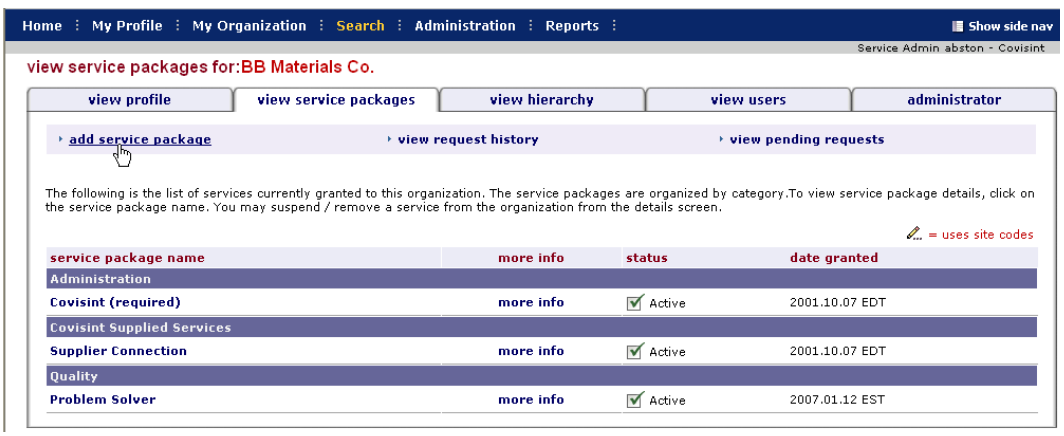
1. Click **View my Organization Hierarchy** from the My Organization drop down menu. The View Hierarchy screen is displayed.



2. Click on the *name of the division* for which you are searching. The Division Profile is displayed.



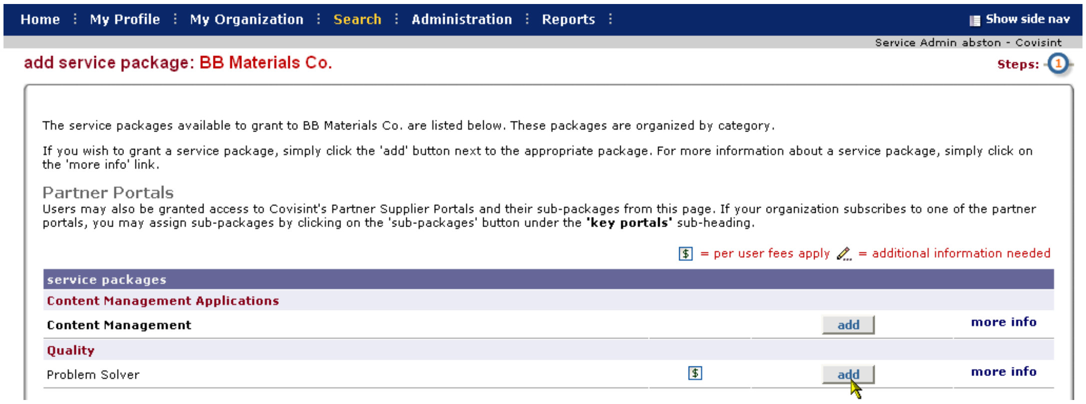
3. Click **view service packages** tab. All list of all service packages granted to the division is displayed.



4. Click **add service package**. A list of all Services Packages for which you are the Security Administrator is listed.

Icons indicating the following functionality are noted next to each service package as appropriate:

- Packages already owned by your parent company will be denoted by a check mark
- Packages that require additional information are indicated with a pencil icon
- Packages that have associated fees are denoted with a dollar sign



5. Click **add**.

6. Click **continue**.

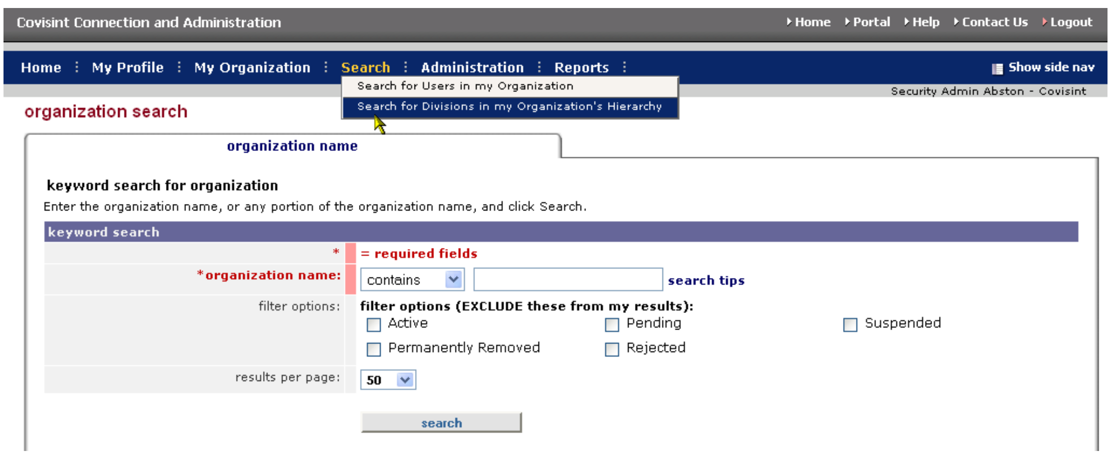
Result
You have successfully granted a service package to a division in your organization.

Suspending a Service Package from a Division of Your Organization

Complete the following steps to suspend a service package from a division. This will prevent all users in the selected division from accessing the applications contained within the package.

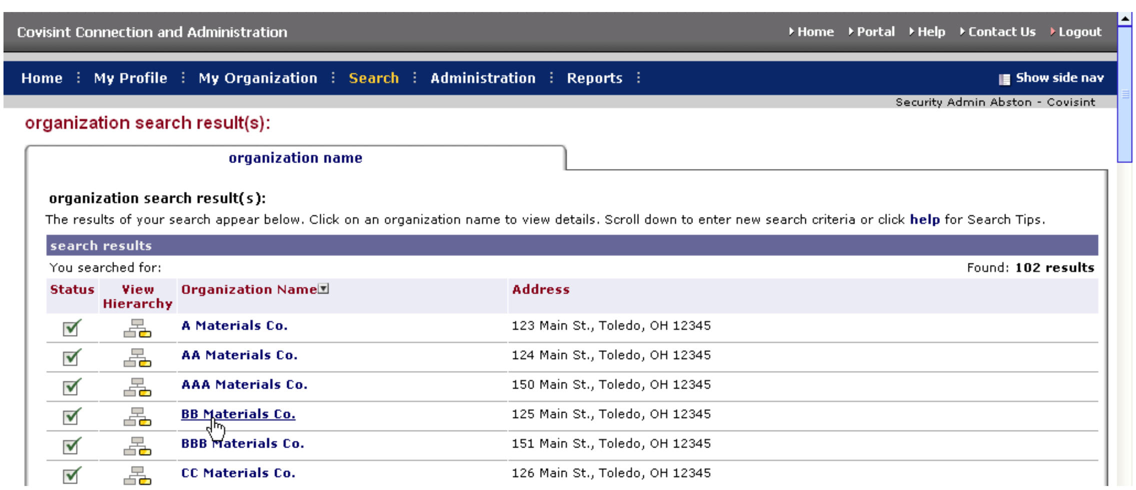
> The division must be at a lower tier in the hierarchy than your own organization.

1. Click **Search for Divisions in my Organization's Hierarchy** from the Search drop down menu. The Search Screen is displayed.



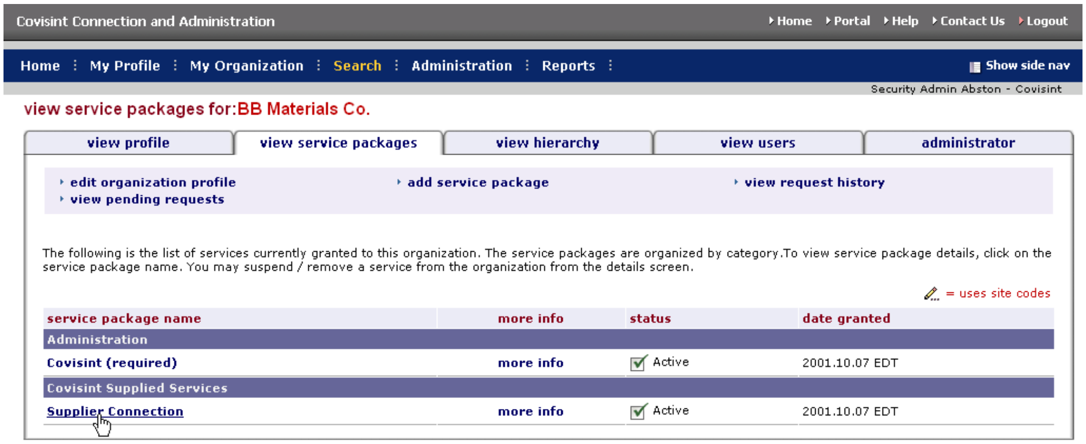
2. Key in search criteria and set filters as desired.

3. Click **Search**. The Search Results screen is displayed.

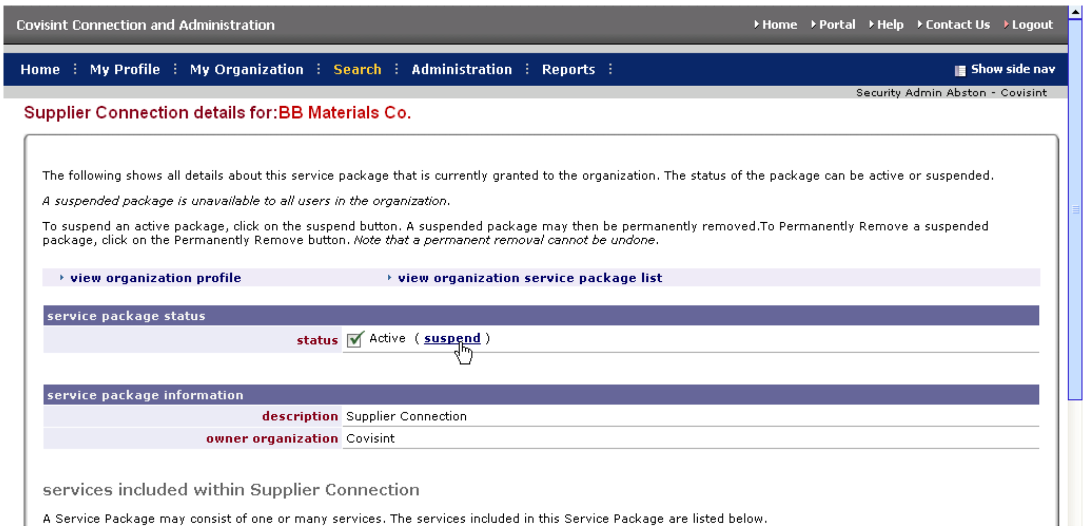


4. Click on the *name of the division* for which you are searching. The Division Profile is displayed.

5. Click **view service packages** tab.



6. Click on the name of the service package you wish to suspend.



7. Click **suspend.**

8. Key in the *reason for suspension* in the open text box.

9. Click **yes, proceed with suspension**. The suspension is logged in the history along with the name of the Administrator performing the task.

Result
You have successfully suspended a service package for a division's your organization.

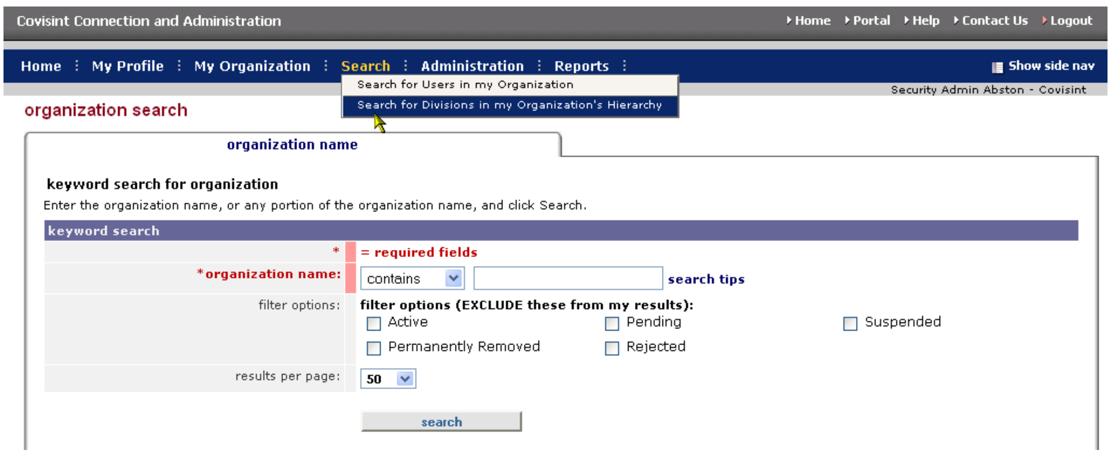
Permanently Removing a Suspended Service Package from a Division of Your Organization

Security Administrators are able to permanently remove a suspended service package from a division in the Organization.

> Once removed, the service package can no longer be reinstated by the Administrator.

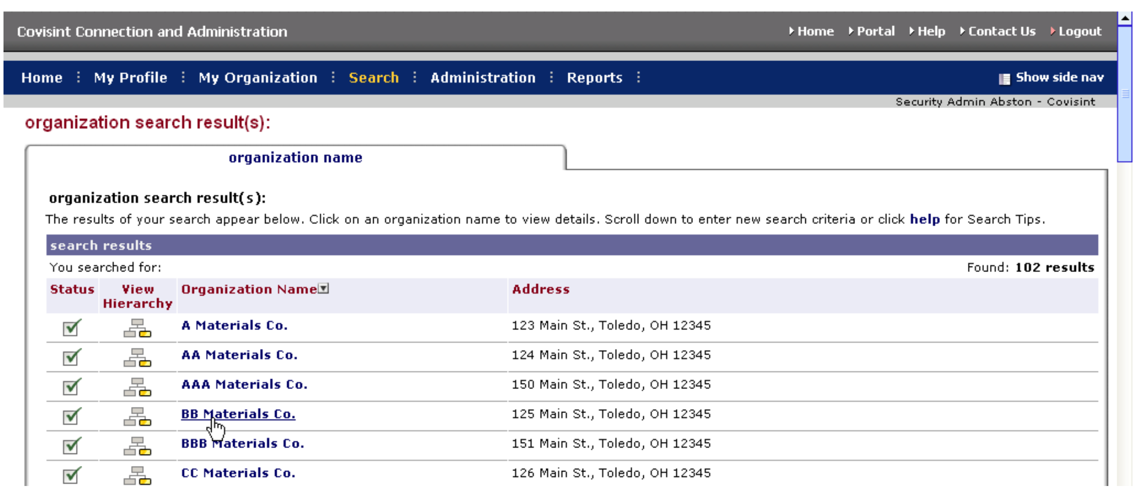
Complete the following steps to permanently remove a service package from a division.

1. Click **Search for Divisions in my Organization's Hierarchy** from the Search drop down menu. The Search Screen is displayed.



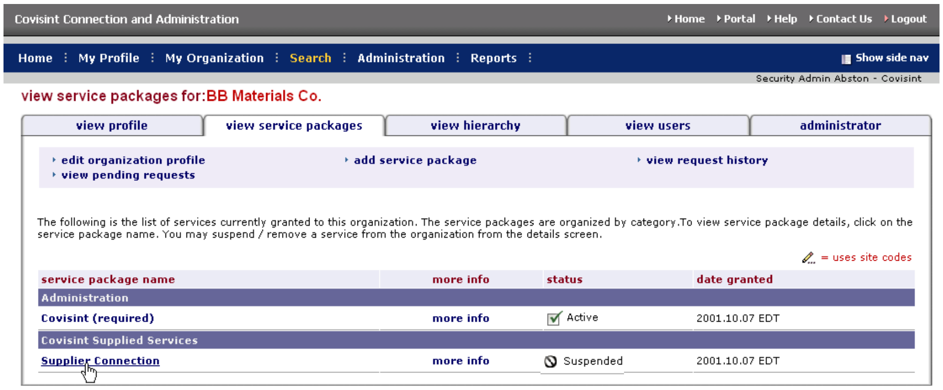
2. Key in search criteria and set filters as desired.

3. Click **Search**. The Search Results screen is displayed.



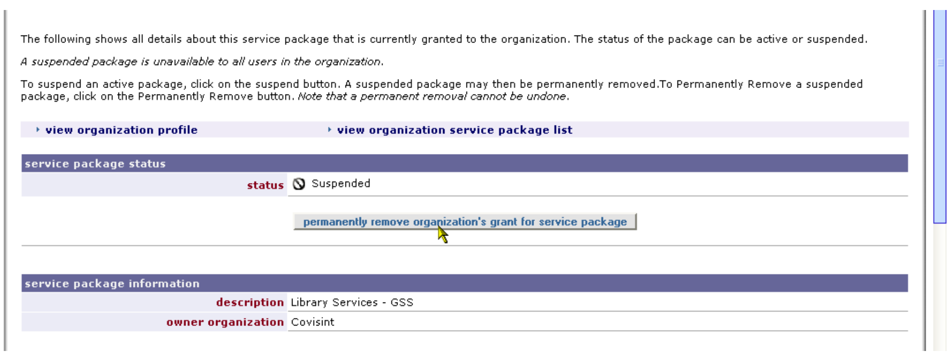
4. Click on the *name of the division* for which you are searching. The Division Profile is displayed.

5. Click **view service packages** tab.



6. Click on the *name of the suspended service package* you wish to permanently remove. The Details Screen for that service package is displayed.

You are only able to permanently remove suspended service packages for which you are the Administrator.



7. Click **permanently remove organization's grant for service package**.

8. Key in the *reason for removing the service package* in the open text box.

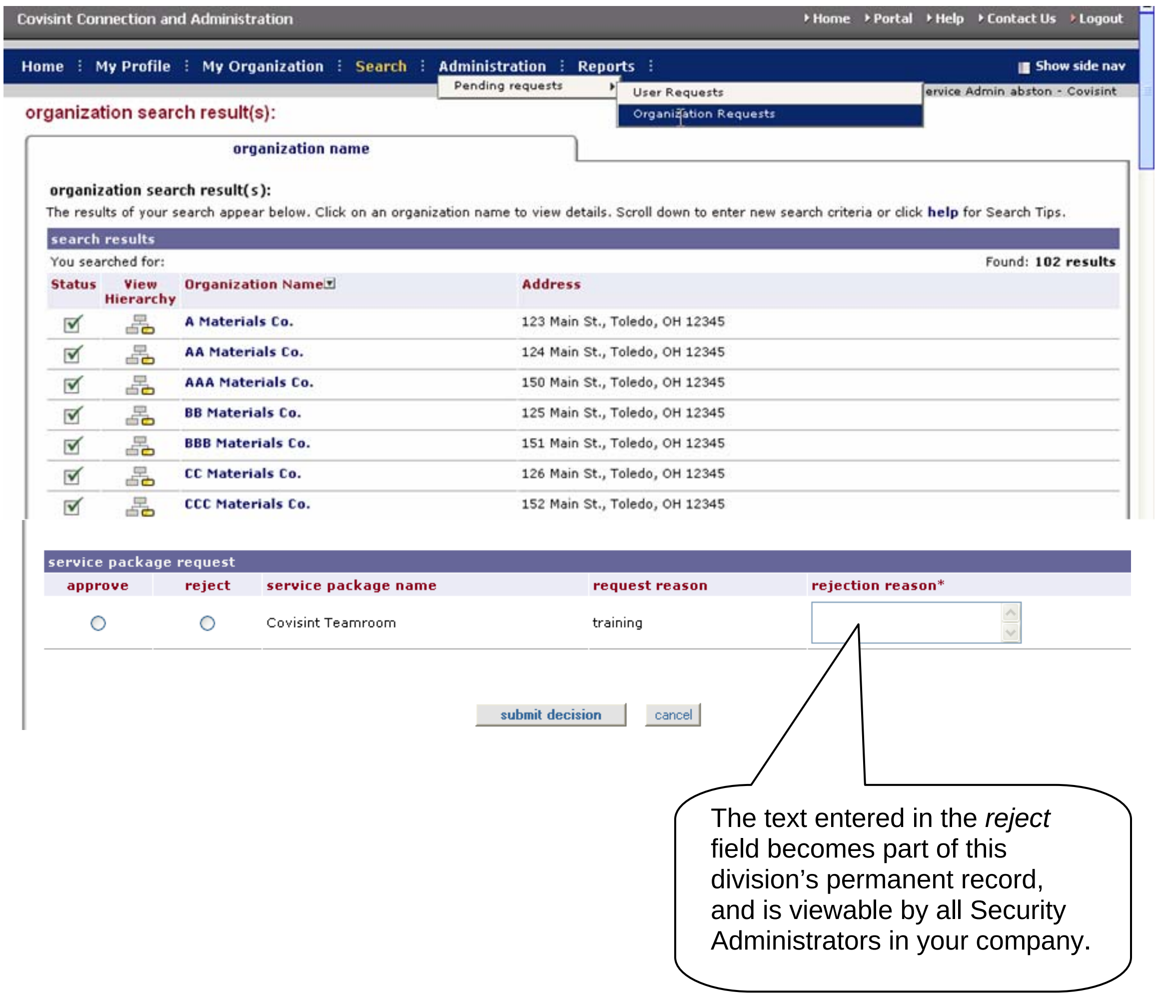
9. Click **yes, proceed with removing**. The permanent removal reason is logged in the history along with the name of the Administrator performing the task.

Result
You have successfully removed a suspended service package for a division in your organization.

Managing a Division's Request for Service Package(s)

Complete the following steps to manage a division's request for service package(s).

> ***Note***: All requests have a 30-day expiration period. If the request is not acted upon in 30 days, the request will be auto-rejected and an explanatory email will be sent back to the user. Requests that are close to expiring automatically trigger a reminder email to the approving administrator(s) five days before the request expires. These rules apply to all pending requests.



Perform one or more of the following:

If you wish to…	Then…
approve the division's access request to a service package	1. From the Administration -> Pending Requests menu, click **Organization Requests**. The Review Pending Approval screen is displayed. 2. Click  next to the division name for whom you wish to review the request. The Details screen is displayed. 3. Enable the approve radio button next to the selected service package. 4. Click **submit decision.** 5. Click **OK** to confirm.
reject the division's access request to a service package	1. From the Administration -> Pending Requests menu, click **Organization Requests**. The Review Pending Approval screen is displayed. 2. Click  next to the division name for whom you wish to review the request. The Details screen is displayed. 3. Enable the reject radio button next to the selected service package. 4. Key in the reason for the rejection in the open text box. The text you enter in this box becomes part of this division's permanent record, and is viewable by all Security Administrators in your company. 5. Click **submit decision.** 6. Click **OK** to confirm.

Generating Reports

Reports Defined

Reports allow a Security Administrator to view CCA real-time reports, customized for their roles. Within the reports options Administrators can view:

* User Summary Report
* User Service Summary Report
* Service Summary Report
* Security Administrator Reports
* Quarterly and Annual User Audits

Each of these report types are defined in the following section.

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.

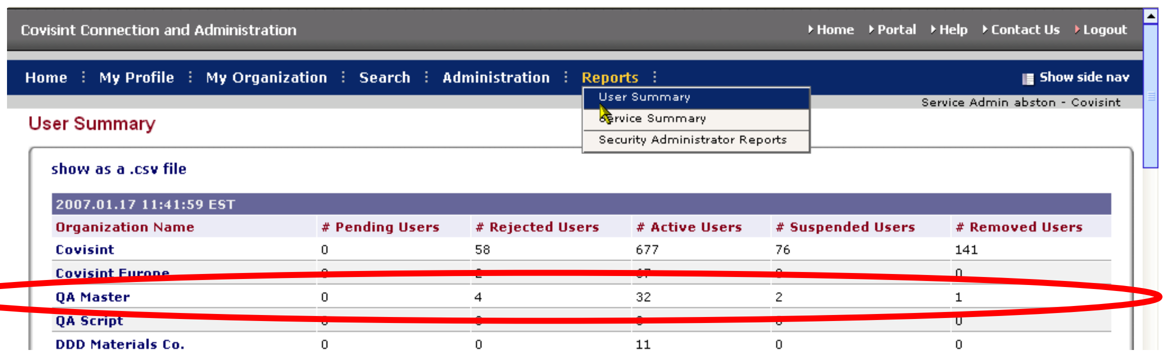
Generating Reports

Generating a User Summary Report

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

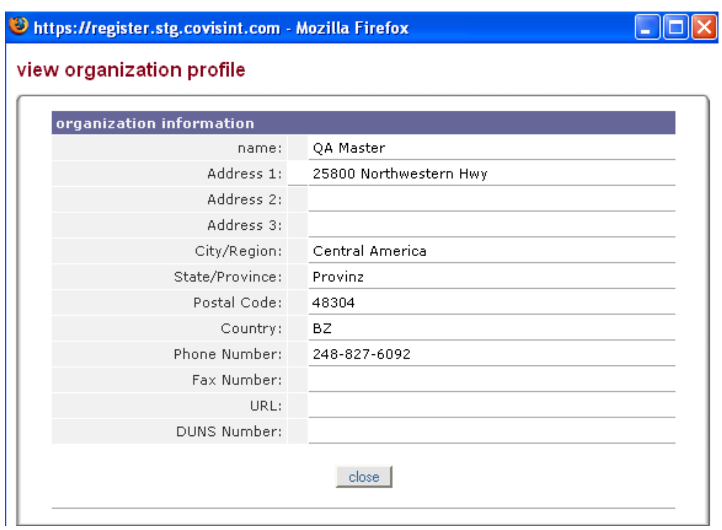
Complete the following steps to generate a User Summary report.

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



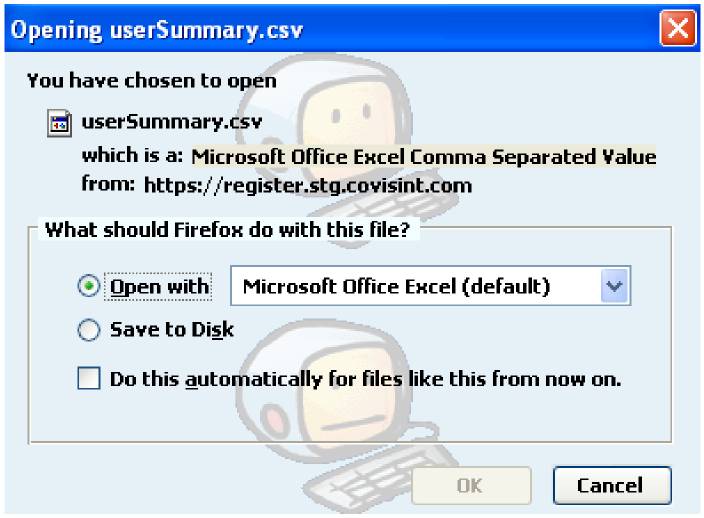
2. View the number of users by status type. For example, in the QA Master organization, you see that there are 0 pending users, 4 rejected users, 32 active users, 2 suspended users, and 1 removed user.

3. If desired, click on the *name of a division* in the organization by clicking on the division name. (This example users QA Master). The profile screen is displayed in a separate window.



   a. Click **close** in the pop-up window when you are done viewing details.

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.



   a. Identify if you wish to open the file or save the file to disk by clicking the appropriate radio button.

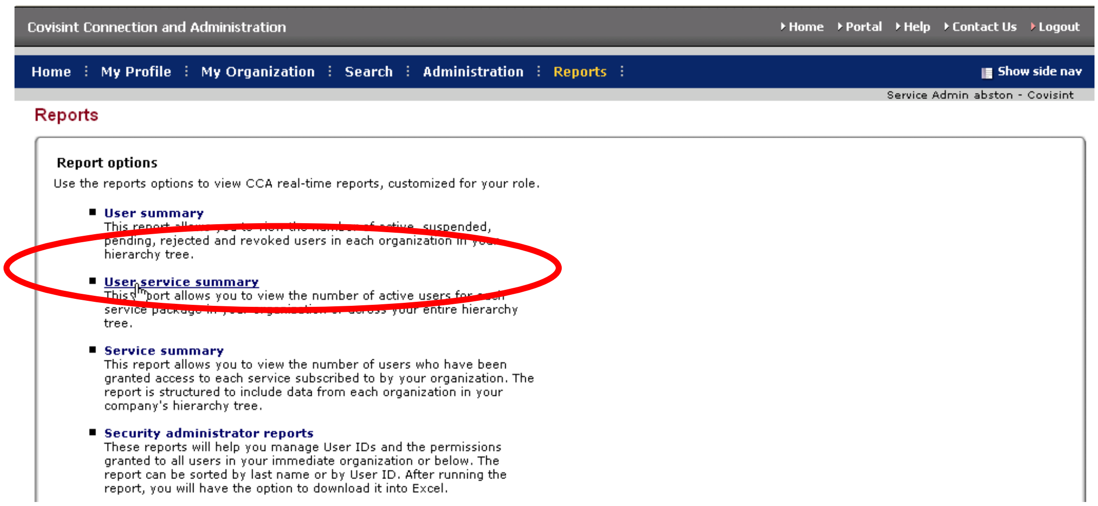
   b. Click **OK**.

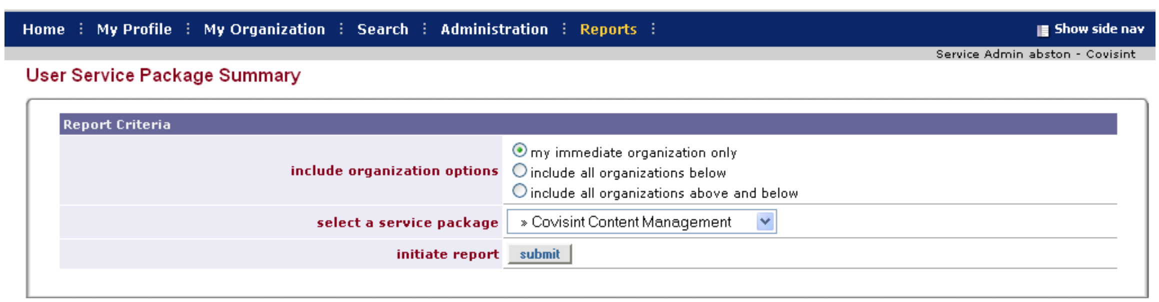
Result
You have successfully generated a user summary report.

Generating a User Service Summary Report

The User Service Summary report allows you to gather information about the numbers and identities of users who have been granted various service packages. In this report, you are able to specify the service package, as well as the level in the organizational hierarchy you wish to include.

Complete the following steps to generate a User Service Summary Report.

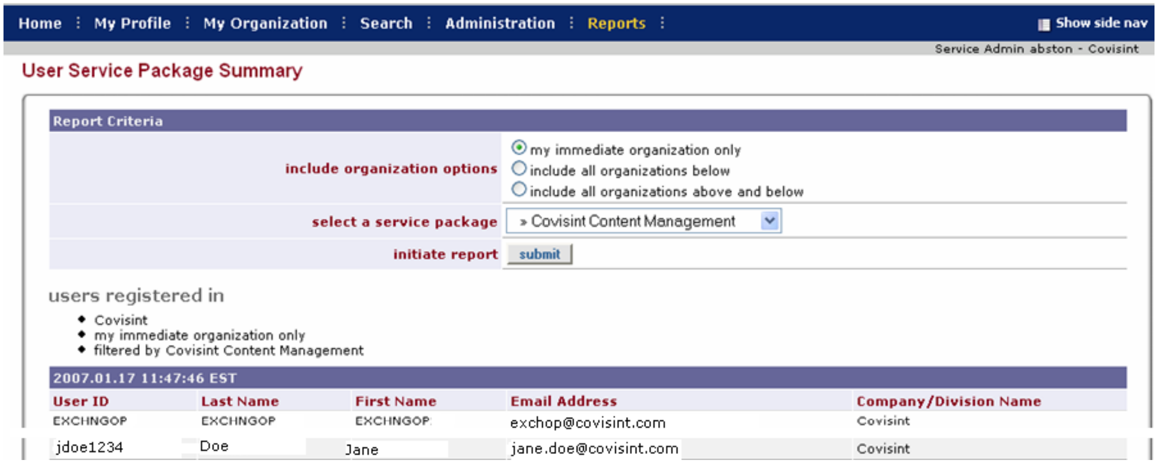




Perform one or more of the following:

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

If you wish to…	Then…
	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.



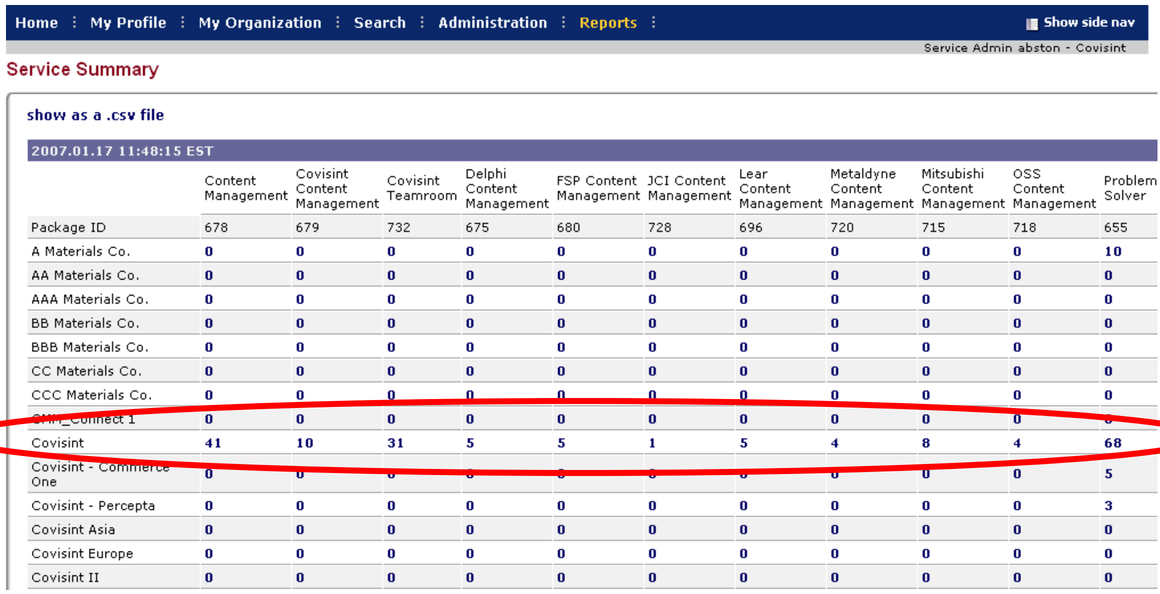
Result
You have successfully generated a user service summary report.

Generating a Service Summary Report

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

Complete the following steps to generate a Service Summary Report.

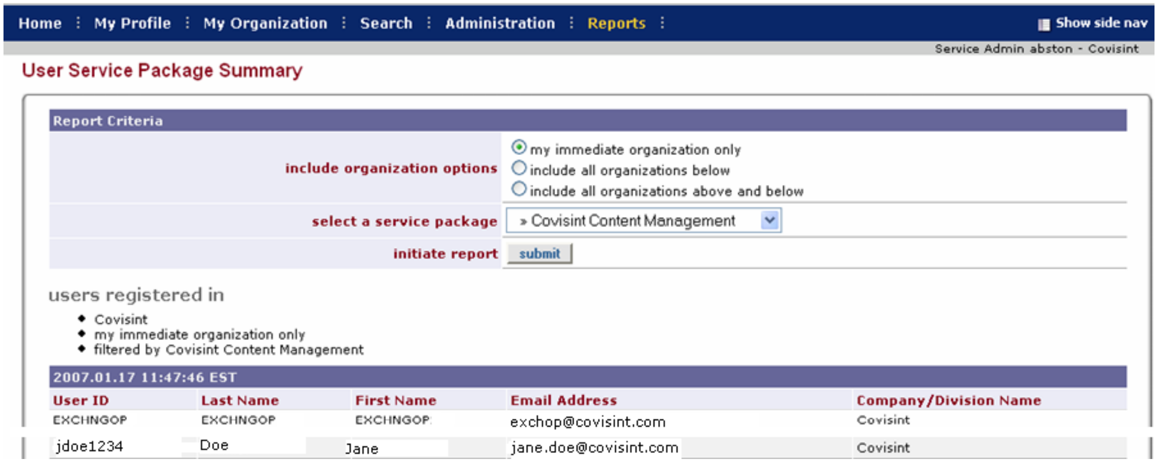
1. Click **Service Summary** from the Reports drop down menu. The Service Summary screen is displayed.



	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
CNH_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.



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.

Security Administrator Reports

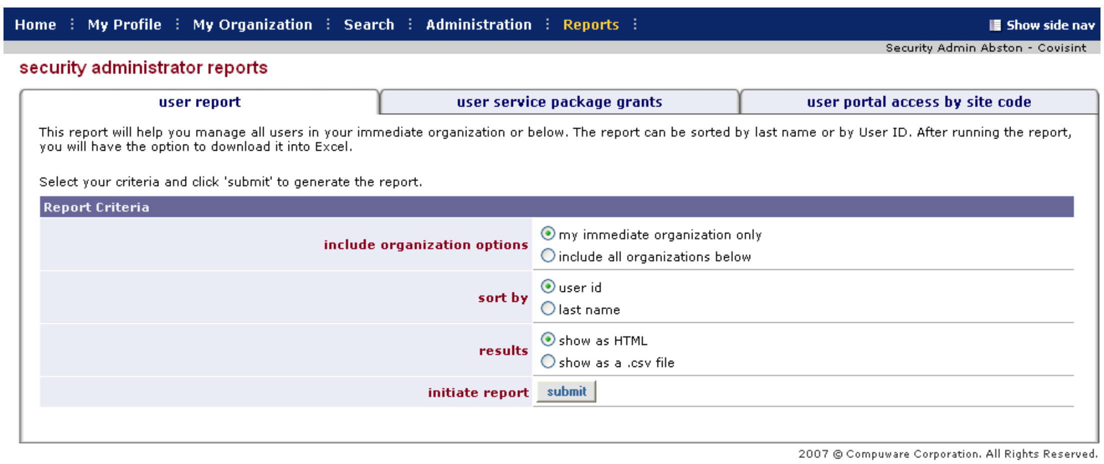
Generating a User Report

The User Report will help you manage all users in your immediate organization or below. The report can be sorted by last name or by User ID, and displays to you the user's SSO ID, first and last name, email address, phone number, organization name, as well as account status (active, suspended, deleted, etc.).

Complete the following steps to generate a User report.

1. Click **Security Administrator Reports** from 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**.

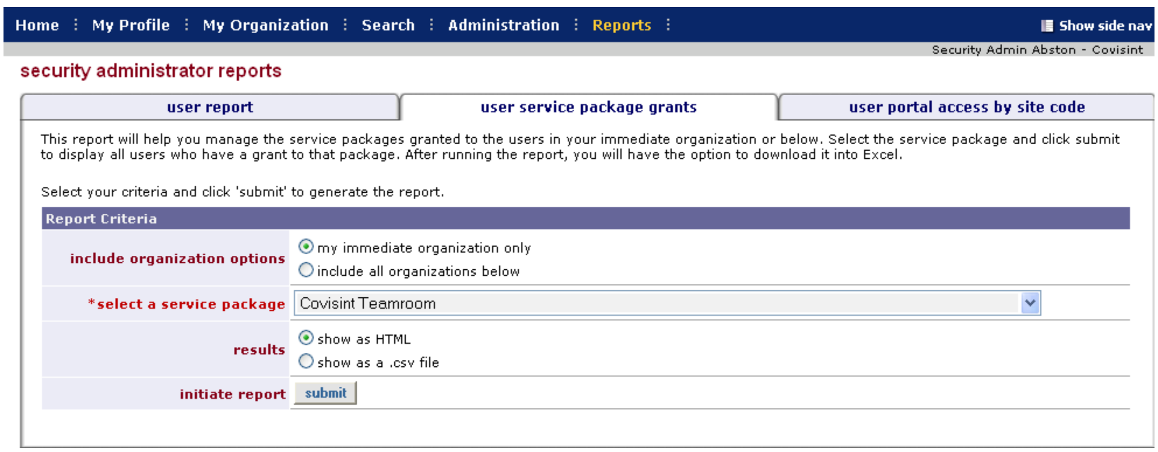
Result
You have successfully generated a user report.

Generating a User Service Package Grant Report

This report will help you manage the service packages granted to the users in your immediate organization or below. By generating this report, you will be able to view all users who have a grant to a selected service package. After running the report, you will have the option to download the report into Excel format.

Complete the following steps to generate a report.

1. Click **Security Administrator Reports** from 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.

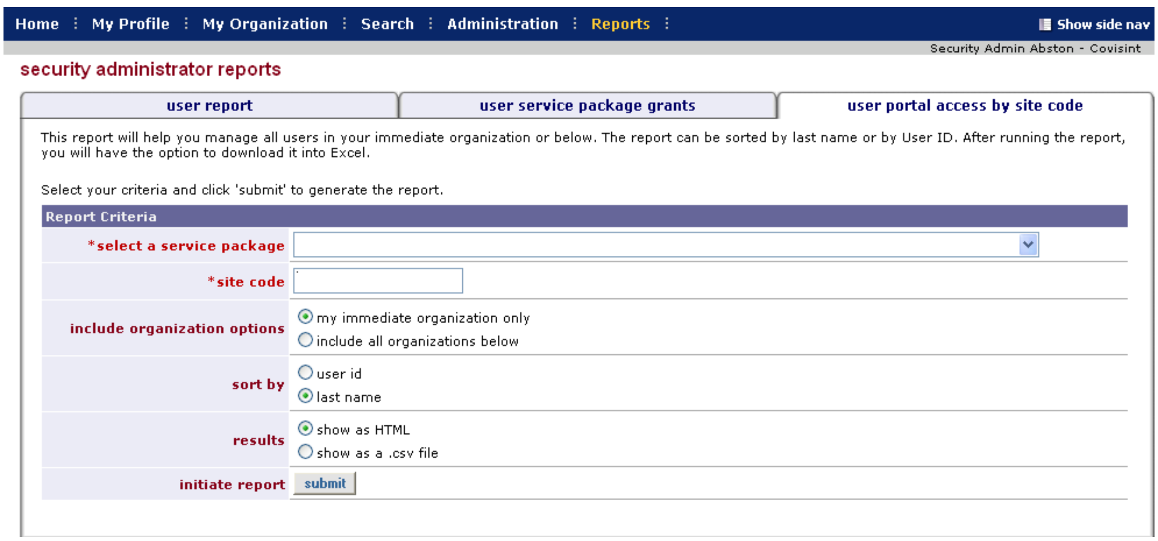
Generating a User Portal Access by Site Code Report

This report will help you manage all users in your immediate organization or below, for a given service package and site code combination. The report can be sorted by last name or by User ID. After running the report, you will have the option to download it into Excel.

Complete the following steps to generate a report.

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

2. Click **user portal access by site code**. The Report screen is displayed.



3. Configure the filters for the report by selected an option for each required field, including:

    i. Organization options – (determines where in the hierarchy you wish to obtain information, for your immediate organization only, or all organizations below yours)

    ii. Select a service package – (from the drop down list, click the service package for which you wish this report to generate)

    iii. Results – (determines how you wish to view the generated report)

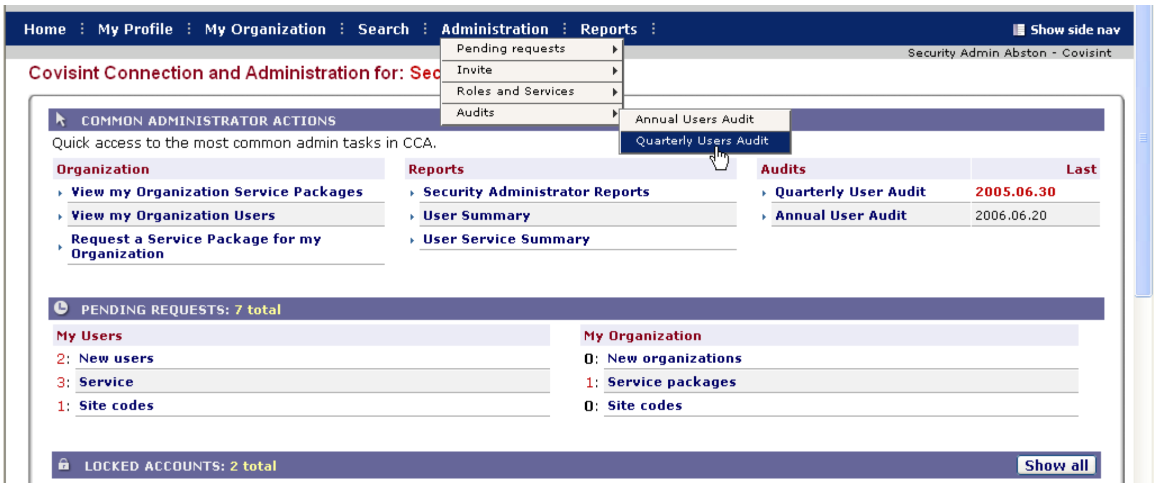
4. Click **Submit**.

Result
You have successfully generated a user portal access by site code report.

Performing Quarterly User Audits

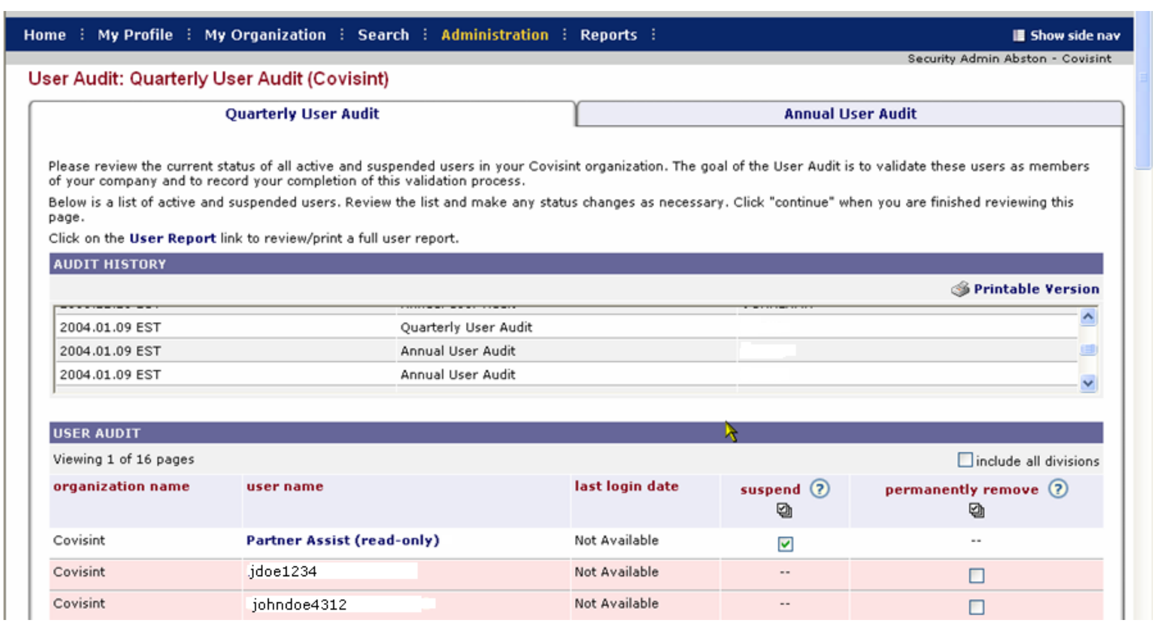
Some of Covisint's portal partners require Security Administrators to perform a periodic audit of their users. A quarterly audit reminder will be emailed to all Security Administrators reminding them to perform the necessary audit activities. You can view your audit history on the Quarterly User Grant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

You can perform the audit at any time using the Audit User functionality in CCA by completing the following steps:



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

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.

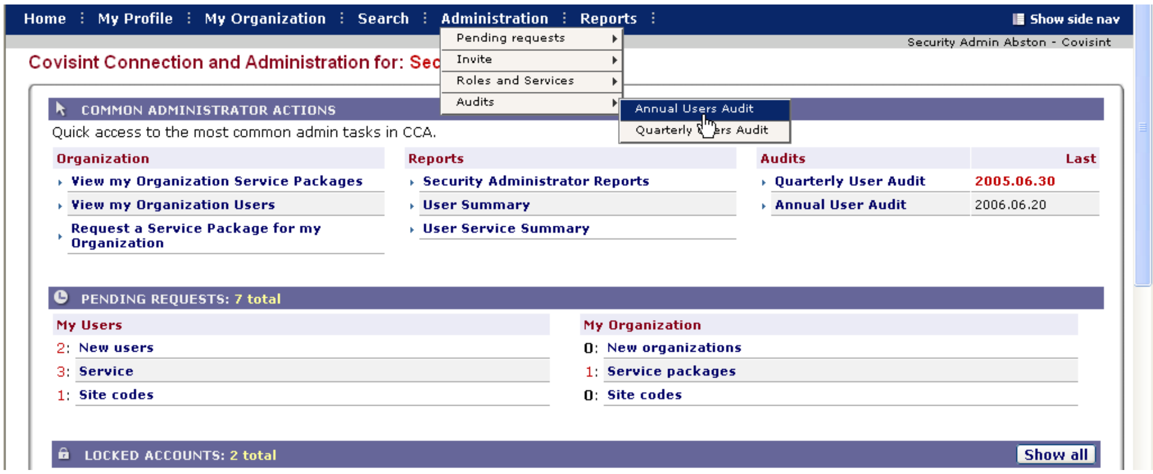
7. After you have examined each page of the audit, confirm the audit and log completion on the last screen by clicking **confirm and log audit completion.**

.

Result
You have successfully logged completion of the quarterly audit requirement. The audit history records the date, the type of audit, and the auditor's ID for past audits.

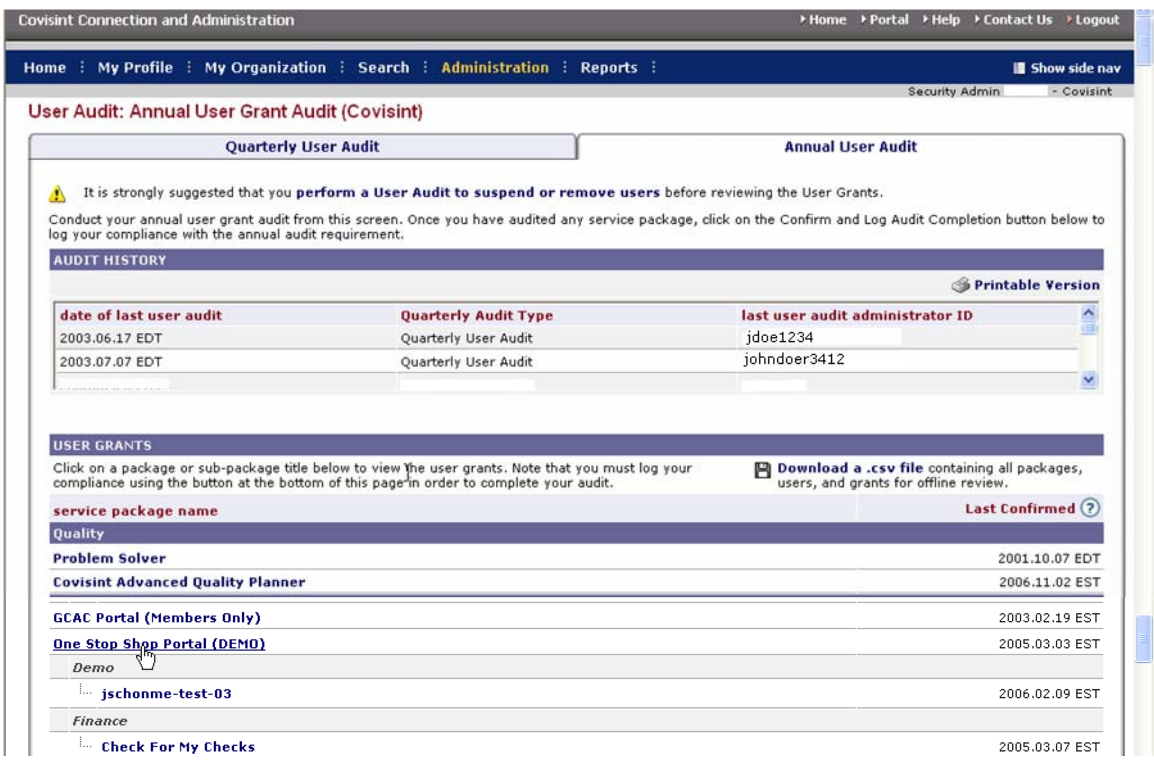
Performing Annual User Audits

Perform an audit at any time using the User Audit functionality in CCA by completing the following steps:

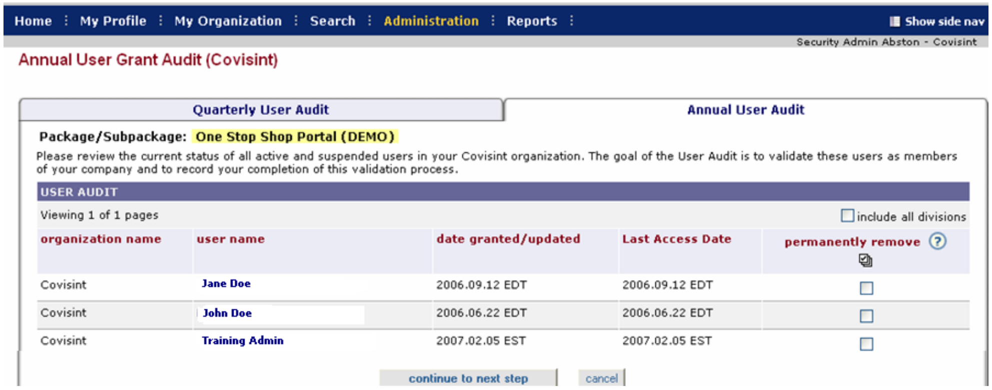


1. From the Administration menu, click **Audits.**

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 user in your organizations that have access to the service.

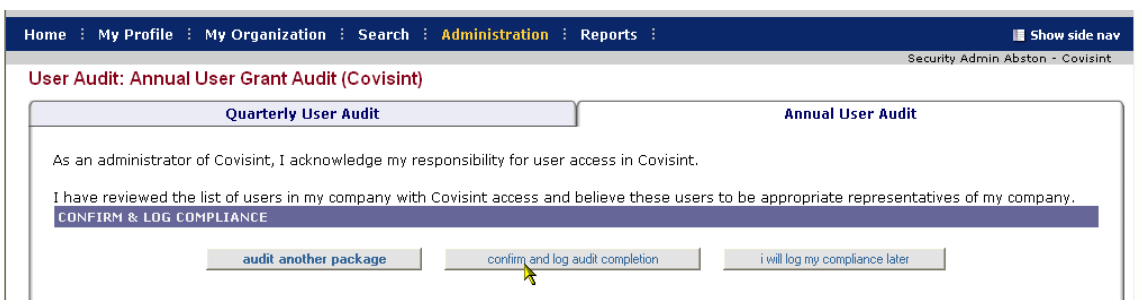


4. Optionally, you can click the *show all divisions* checkbox to conduct the audit for all organizations at or below your organization in your organization's hierarchy.

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 thus far and finish the audit at a later time.

Result
You have successfully logged completion of the annual audit requirement. The audit history records the date, the type of audit, and the auditor's ID for past audits.

Need Additional Support?

Contact your Security Administrator for additional help.

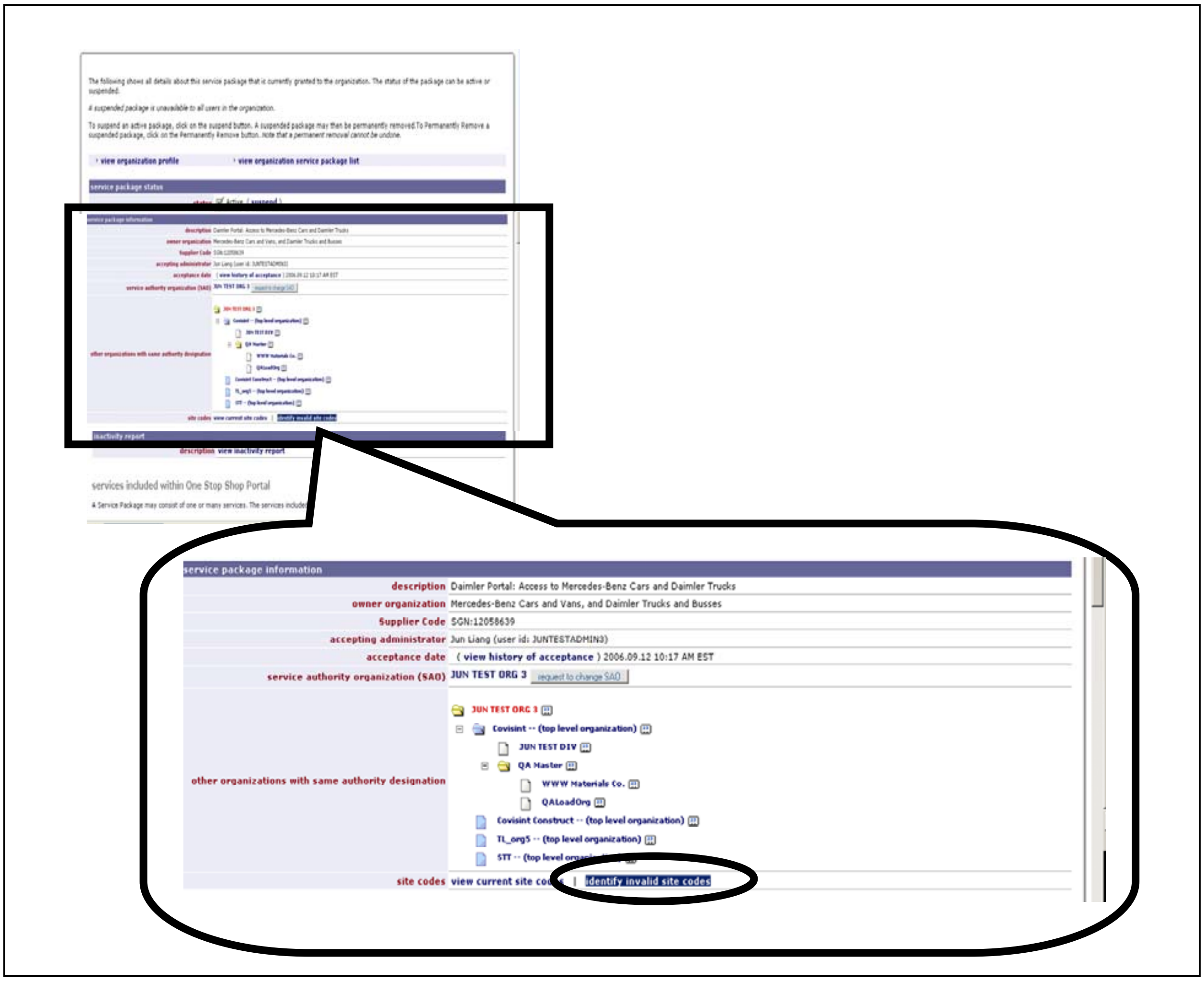
Create a Support Request Ticket

If you are a registered Covisint user, and have questions that are not answered in any of these help guides, you may submit a support request ticket.

Removing Invalid Site Codes

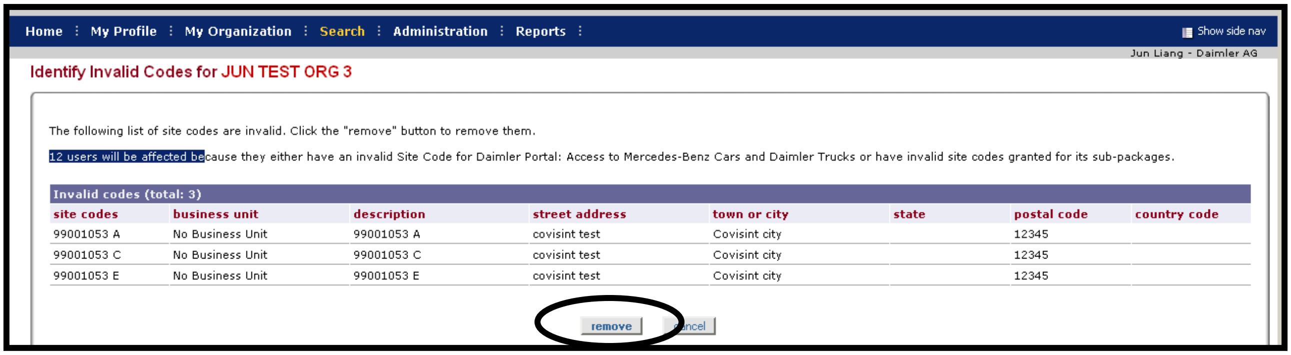
At times, a Portal Owner may review invalid codes in the SAO profile for the portal. This is a list of invalid codes available at the "Identify Invalid Codes for [SAO Organization]" screen.

Organization Service Package Screen (SAO Organization as seen by the Portal Owner)



From the Organization Service Packages screen, navigate to the Invalid Site Code screen by clicking **identify invalid site codes**.

Identify Invalid Codes for [SAO Organization] Screen



From this screen, Portal Owners of an SAO Organization are able to view:

- a list of site codes involved in invalid code grants for users and/or organizations in CCA
- the number of users impacted by the invalid site codes granted on their Portal grant or on application grants (sub-packages).

By clicking the **remove**, the system performs the clean-up actions on invalid grants listed. The system will automatically:

- Revoke the portal grant from each user with an invalid home location code on that portal.
- Revoke a sub-package grant from any user with only invalid associated application site codes remaining.
- Update any user package grant to remove any invalid site code grants.
- Remove any invalid company/division invalid site code from organization portal grants.
- Send sync messages to the portal partner for any effected users.
- Email effected users, notifying them of the changes applied to them.