CCA Energy
My Profile & Administration

Table Of Contents

About "My Profile" Administration

My Profile (CCA) enables users to manage their user profiles in order to gain secured access to their applications.

It also enables organization administrators to manage their divisions, users, and application access. As organizations are confronted with the requirements of providing access to critical information across divisions within the organization, CCA application provides secure access to this information.

Important Note: The screenshots in this support material may display links to more tasks then you see when you are logged in, depending on your role/privileges/organization configuration.

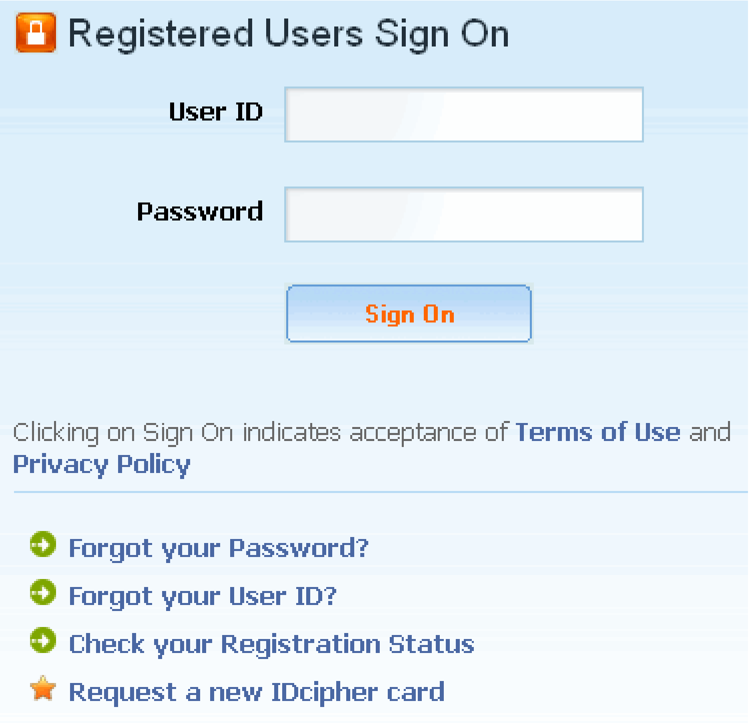
Reset Your Password

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.



Clicking on Sign On indicates acceptance of Terms of Use and Privacy Policy

2. Click **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^{TM} card is required to sign on, your existing IDcipher^{TM} card will become invalid when your account is unlocked and the system will automatically send you a new IDcipher^{TM} card.

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

Administrator Roles Matrix

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 in this online structure, the Administrator at the Division level is also called a Security Administrator.

Table 1: Matrix of Privileges Associated Per Role

	Application Administrator	Security Administrator
Administer All Company Owned Packages	x	-
Grant	x	-
Invite Organization (Modify No Fly List)	x	-
SO Grant Organization Package	x	-
SO Grant User Package	x	-
SO Permanently Remove Package From Division	x	-
SO Permanently Remove Package From Organization	x	-
SO Permanently Remove Package From User	x	-
SO Suspend Package From Division	x	-
SO Suspend Package From Organization	x	-
Edit Organization	-	x
Edit User	-	x
Grant User Roles	-	x
Invite Users	-	x
Permanently Remove User	-	x
Reset/specify user password	-	x
Approve Division	-	x
Manage users	-	x
Manage divisions	-	x
Security Admin - View User Reports	-	x
View hierarchy	-	x

All Users

About "My Profile" Administration

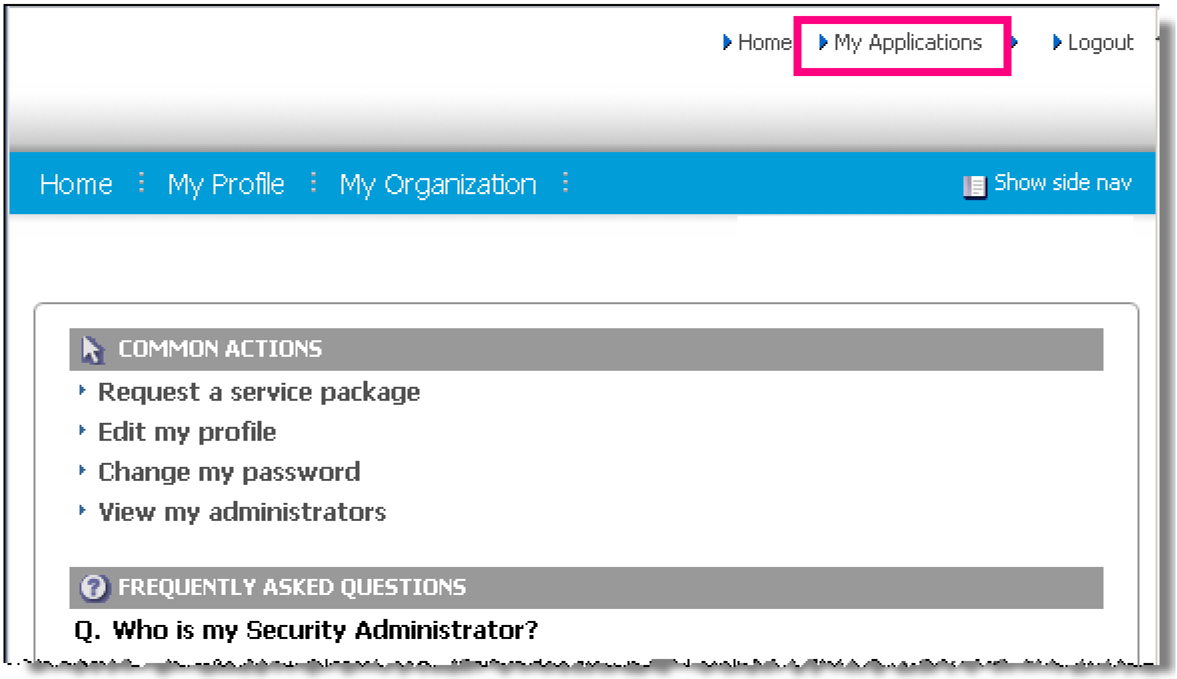
My Profile (CCA) enables users to manage their user profiles in order to gain secured access to their applications.

It also enables organization administrators to manage their divisions, users, and application access. As organizations are confronted with the requirements of providing access to critical information across divisions within the organization, CCA application provides secure access to this information.

Important Note: The screenshots in this support material may display links to more tasks then you see when you are logged in, depending on your role/privileges/organization configuration.

Accessing Your Applications

If your organization does not federate outbound to applications, you may skip this topic, and you will not see a link to My Applications.



Q. Who is my Security Administrator?

1. Click the **My Applications** link in the upper right corner of the screen. The My Applications page displayed a list of all applications to which you have approved access.

2. Click on the *name of the application* you wish to access. The application is displayed in a new window, and you are logged in with your user credentials.

RESULT:

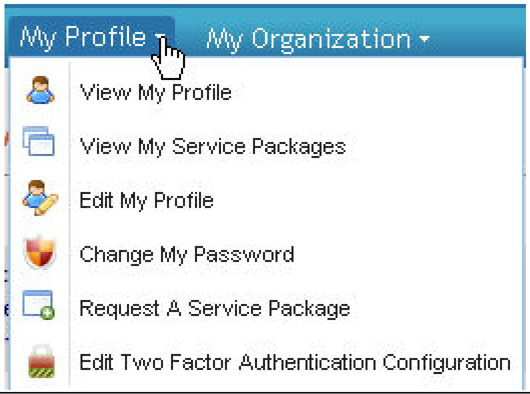
You have successfully accessed your applications.

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.

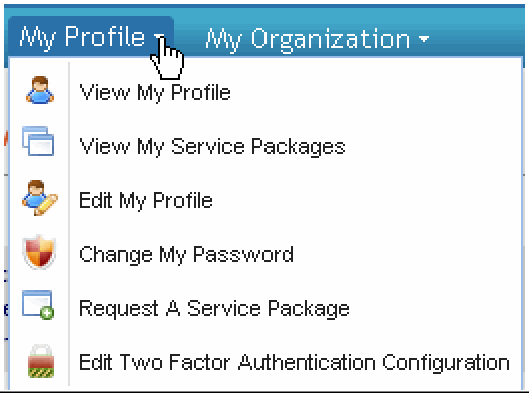
Edit Two-Factor Authentication Settings

Some organizations do not allow options for two-factor authentication. When this is the case, you will not see the "Edit Two-Factor Authentication Settings" menu option.

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

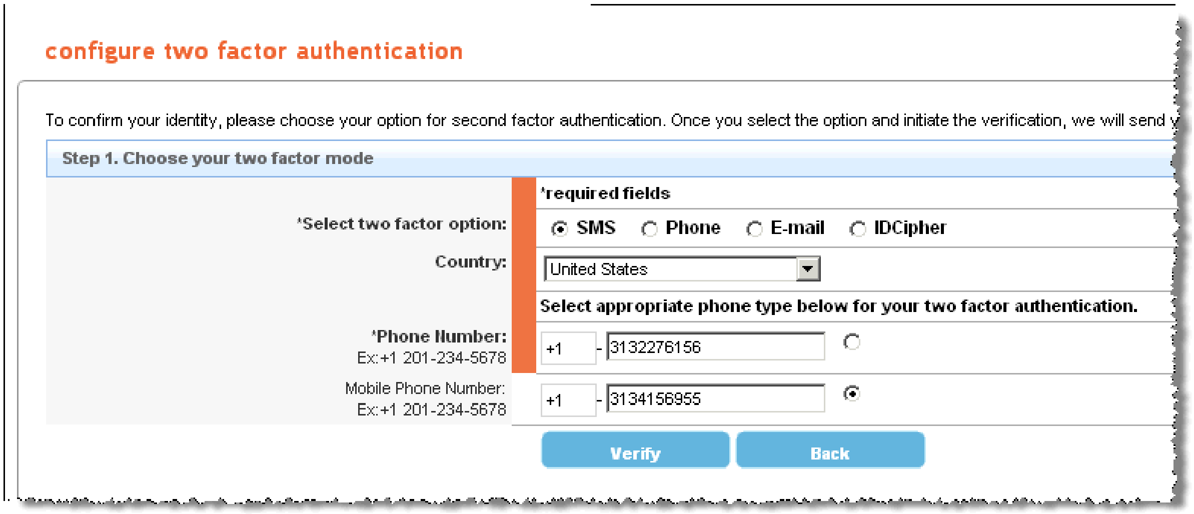
Where is the My Profile Drop-down Menu?

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



2. Click **Edit Two Factor Authentication Configuration** option.

Some customers may not have access to all options indicated below.



configure two factor authentication

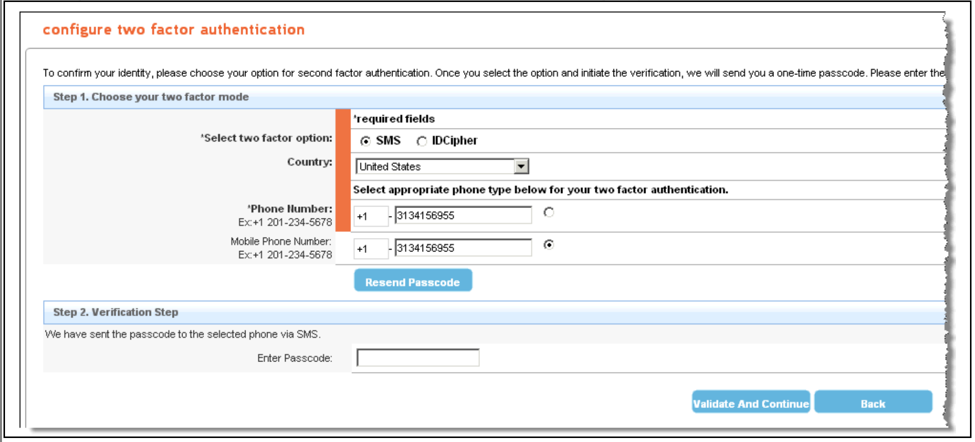
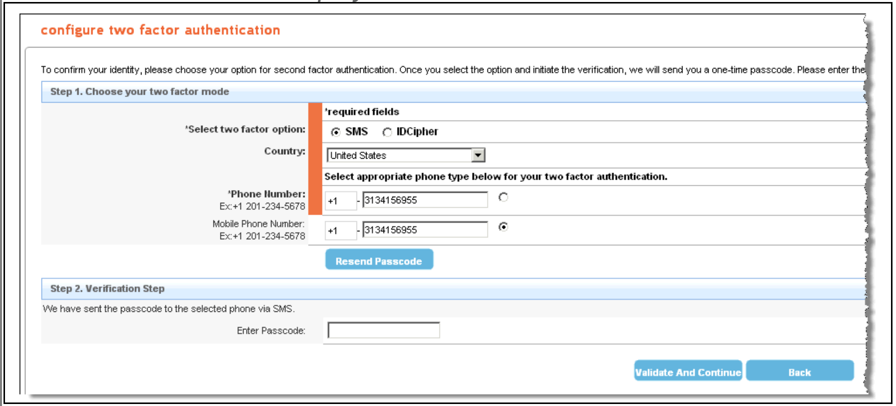
To confirm your identity, please choose your option for second factor authentication. Once you select the option and initiate the verification, we will send y

Step 1. Choose your two factor mode

*required fields

*Select two factor option:	● SMS ○ Phone ○ E-mail ○ IDCipher
Country:	United States
	Select appropriate phone type below for your two factor authentication.
*Phone Number: Ex:+1 201-234-5678	+1 - 3132276156 ○
Mobile Phone Number: Ex:+1 201-234-5678	+1 - 3134156955 ●

3. Perform one of the following:

If You Wish To:	Then...
receive a SMS (text message) with the second factor authentication required during log in	a. Enable the **SMS** radio button b. Select the *country* in which your cell phone is registered. c. Enable the radio button next to **Mobile Phone Number** field. d. Key in your mobile number to which you will receive SMS text messages required for log in. e. Click **Verify**. The passcode is sent via text to your mobile phone number provided, and the *Enter Passcode field is displayed.*  configure two factor authentication To confirm your identity, please choose your option for second factor authentication. Once you select the option and initiate the verification, we will send you a one-time passcode. Please enter the Step 1. Choose your two factor mode *required fields *Select two factor option: ● SMS ○ IDCipher Country: United States Select appropriate phone type below for your two factor authentication. *Phone Number: Ex:+1 201-234-5678 +1 - 3134156955 ○ Mobile Phone Number: Ex:+1 201-234-5678 +1 - 3134156955 ● Step 2. Verification Step We have sent the passcode to the selected phone via SMS. Enter Passcode: f. Key in the passcode in the Enter Passcode field. g. Click **Validate and Continue.** The Edit Profile screen is displayed. h. Click **Save Changes.**
receive a voice recording via phone with the second factor authentication required during log in	a. Enable the **Phone** radio button b. Select the *country* in which your phone is registered. c. Enable the radio button next to **Phone Number** field d. Key in your phone number to which you will receive voice recorded passcode required for log in. e. Click **Verify**. The passcode is sent phone number provided, and the *Enter Passcode field is displayed.*  configure two factor authentication To confirm your identity, please choose your option for second factor authentication. Once you select the option and initiate the verification, we will send you a one-time passcode. Please enter the Step 1. Choose your two factor mode *required fields *Select two factor option: ● SMS ○ IDCipher Country: United States Select appropriate phone type below for your two factor authentication. *Phone Number: Ex:+1 201-234-5678 +1 - 3134156955 ○ Mobile Phone Number: Ex:+1 201-234-5678 +1 - 3134156955 ● Step 2. Verification Step We have sent the passcode to the selected phone via SMS. Enter Passcode:

f. Key in the passcode in the Enter Passcode field.

g. Click **Validate and Continue.** The Edit Profile screen is displayed.

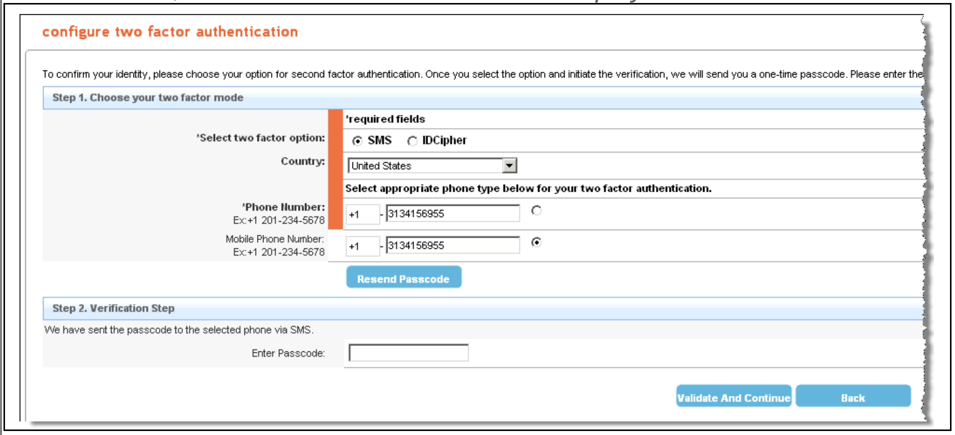
h. Click **Save Changes.**

receive an email with the second factor authenticatio n required during login

a. Enable the **E-mail** radio button

b. Key in the email address to which you will receive the passcode.

c. Click **Resend Passcode**. The passcode is sent via text to your email address, and the *Enter Passcode field is displayed.*



configure two factor authentication

To confirm your identity, please choose your option for second factor authentication. Once you select the option and initiate the verification, we will send you a one-time passcode. Please enter the

Step 1. Choose your two factor mode

*required fields

*Select two factor option: ● SMS ○ IDCipher

Country: United States

Select appropriate phone type below for your two factor authentication.

*Phone Number: Ex:+1 201-234-5678 +1 - 3134156955 ○

Mobile Phone Number: Ex:+1 201-234-5678 +1 - 3134156955 ●

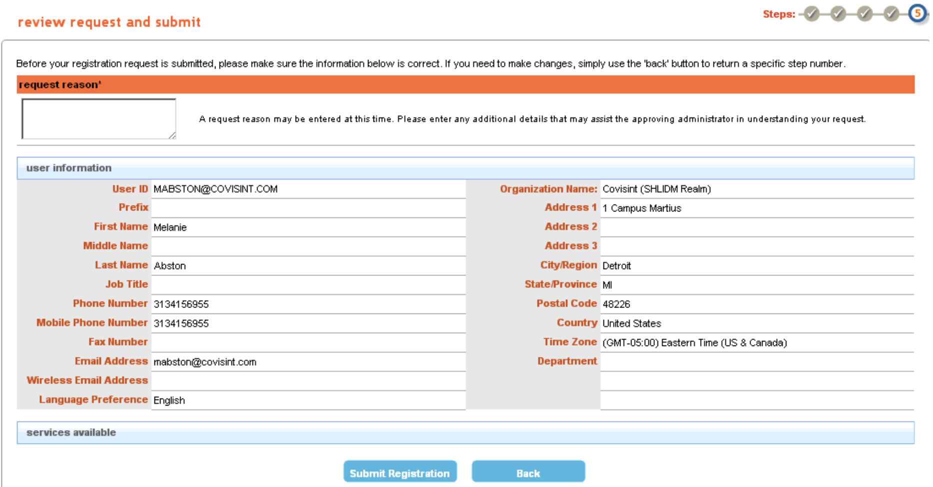
Step 2. Verification Step

We have sent the passcode to the selected phone via SMS.

Enter Passcode:

d. Key in the passcode in the Enter Passcode field (retrieved from your email).

e. Click **Validate and Continue.** The *Review Request and Submit* screen is displayed.



review request and submit

Before your registration request is submitted, please make sure the information below is correct. If you need to make changes, simply use the 'back' button to return a specific step number.

request reason*

A request reason may be entered at this time. Please enter any additional details that may assist the approving administrator in understanding your request.

user information

User ID	MABSTON@COVISINT.COM	Organization Name:	Covisint (SHLIDM Realm)
Prefix		Address 1	1 Campus Martius
First Name	Melanie	Address 2	
Middle Name		Address 3	
Last Name	Abston	City/Region	Detroit
Job Title		State/Province	MI
Phone Number	3134156955	Postal Code	48226
Mobile Phone Number	3134156955	Country	United States
Fax Number		Time Zone	(GMT-05:00) Eastern Time (US & Canada)
Email Address	mabston@covisint.com	Department	
Wireless Email Address			
Language Preference	English		

services available

f. Click **Save Changes**.

use the IDCipher card as your second factor authenticatio

a. Enable the **IDCipher** radio button

b. Enable the checkbox in Step 2. Verification Step.

c. Click **Continue**.

n during log in	

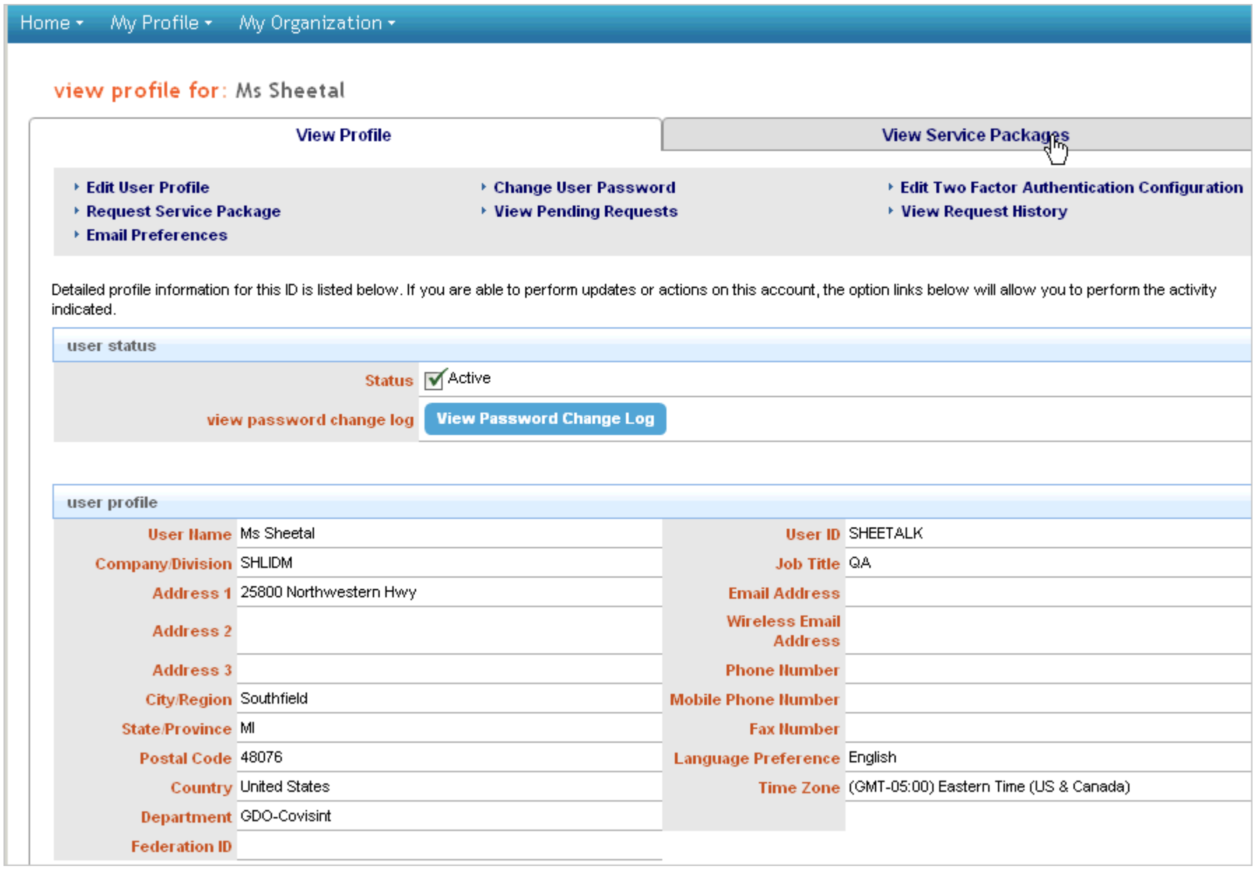
RESULT:

You have successfully edited your two-factor authentication settings.

Manage Your User Profile

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

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



view profile for: Ms Sheetal

Detailed profile information for this ID is listed below. If you are able to perform updates or actions on this account, the option links below will allow you to perform the activity indicated.

user status

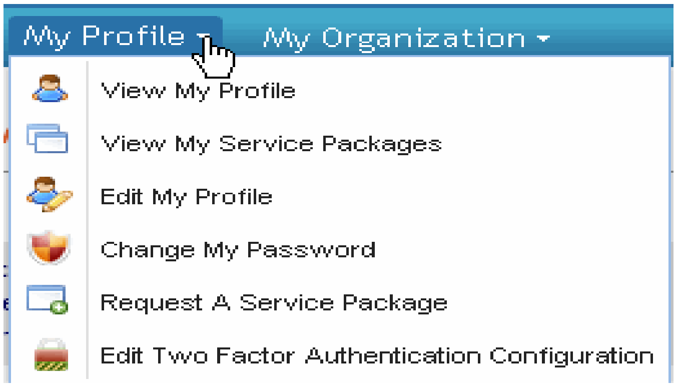
Status	☑ Active
view password change log	View Password Change Log

user profile

User Name	Ms Sheetal	User ID	SHEETALK
Company/Division	SHLIDM	Job Title	QA
Address 1	25800 Northwestern Hwy	Email Address	
Address 2		Wireless Email Address	
Address 3		Phone Number	
City/Region	Southfield	Mobile Phone Number	
State/Province	MI	Fax Number	
Postal Code	48076	Language Preference	English
Country	United States	Time Zone	(GMT-05:00) Eastern Time (US & Canada)
Department	GDO-Covisint		
Federation ID			

- 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.

My User ID is Suspended

If your User ID has been suspended, you are not able to reactivate it on your own. You will need to contact your administrator. Only your security administrator can reactivate your User ID. The Help Desk cannot re-activate suspended IDs, only your administrator can do that.

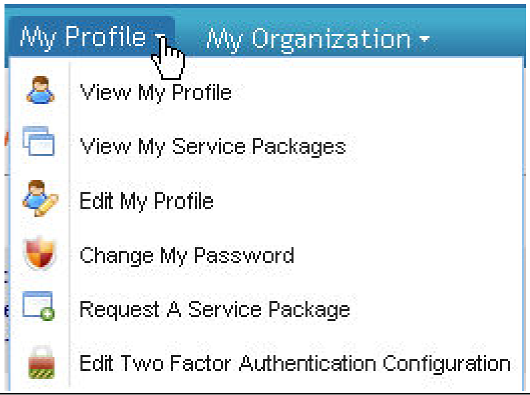
However, if your User ID is locked (from too many login attempts, for example), you are able to unlock your account by resetting your password.

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.
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

Some organizations do not allow users to request service packages. When that is the case, you will not see the "Request Service Package" option.

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

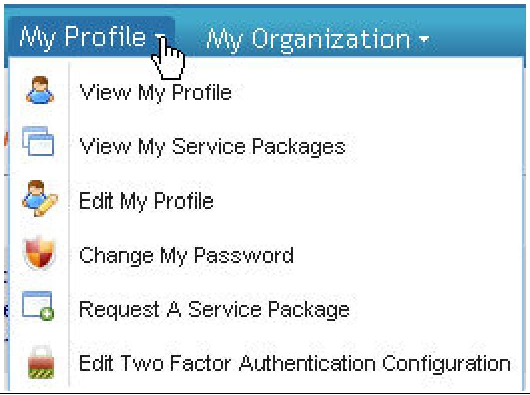
Later, post-registration, you may need to request additional service packages in order to perform your job duties.

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.

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.

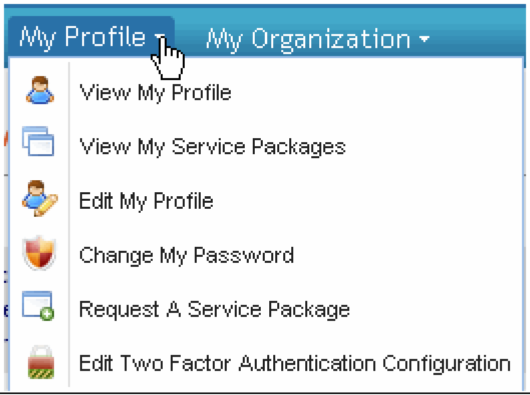
Send Pending Request Reminder to Administrator

Some organizations do not allow users to request service packages. When that is the case, you will not see the "Send Reminder" option.

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

RESULT:

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

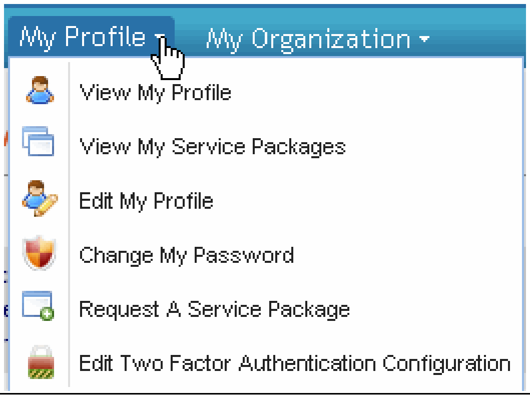
View History of Your Requests

Some organizations do not allow users to request service packages. When that is the case, you will not see the "View request history" option.

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.

RESULT:

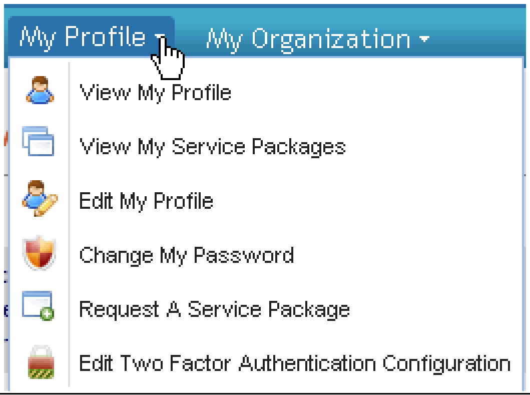
You have successfully viewed a history of your requests.

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.

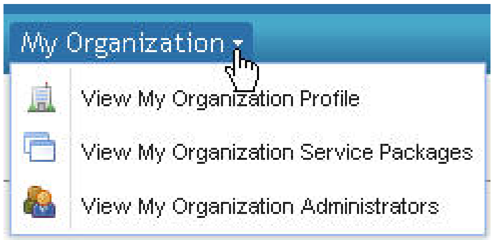
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Administrators

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

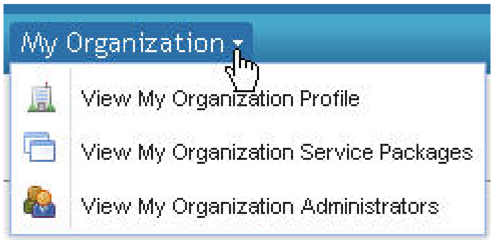
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Administrators

2.

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

RESULT:

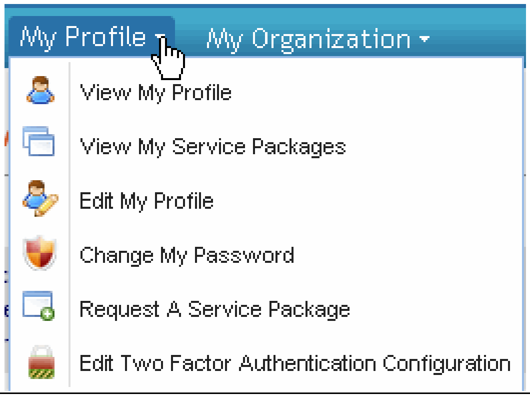
You have successfully viewed your organization services.

View Your 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:

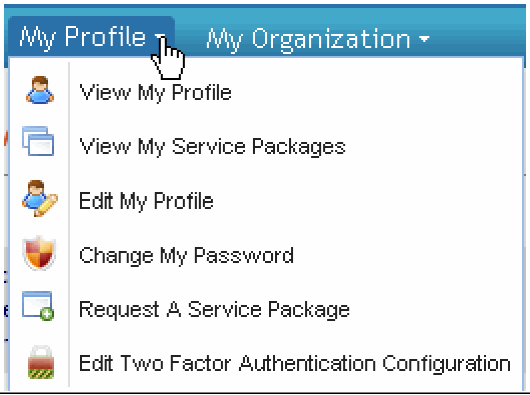
You have successfully viewed your user roles, if any are applicable.

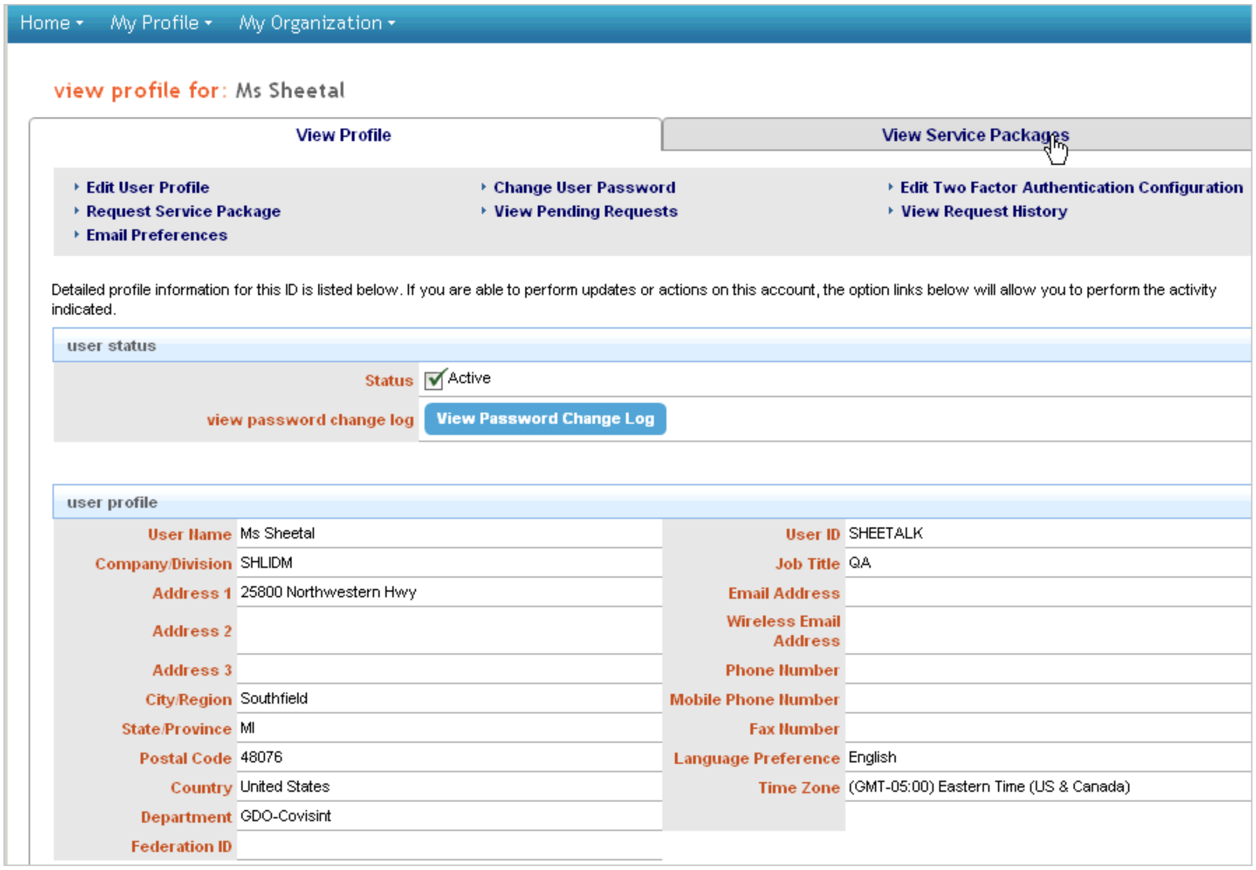
Where Can I Find My Federation ID?

From the *My Profile drop-down menu*, click **View my profile**. Your Federation ID is displayed on the User Profile Page.

Where is the My Profile Drop-down Menu?

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





Detailed profile information for this ID is listed below. If you are able to perform updates or actions on this account, the option links below will allow you to perform the activity indicated.

user status

Status	☑ Active
view password change log	View Password Change Log

user profile

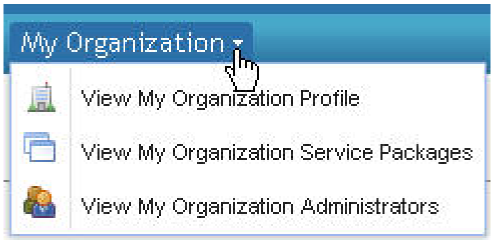
User Name	Ms Sheetal	User ID	SHEETALK
Company/Division	SHLIDM	Job Title	QA
Address 1	25800 Northwestern Hwy	Email Address	
Address 2		Wireless Email Address	
Address 3		Phone Number	
City/Region	Southfield	Mobile Phone Number	
State/Province	MI	Fax Number	
Postal Code	48076	Language Preference	English
Country	United States	Time Zone	(GMT-05:00) Eastern Time (US & Canada)
Department	GDO-Covisint		
Federation ID			

Who are my Organization Security Administrators

Your organization Security Administrators are responsible for approving / rejecting your requests 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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Administrators

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:

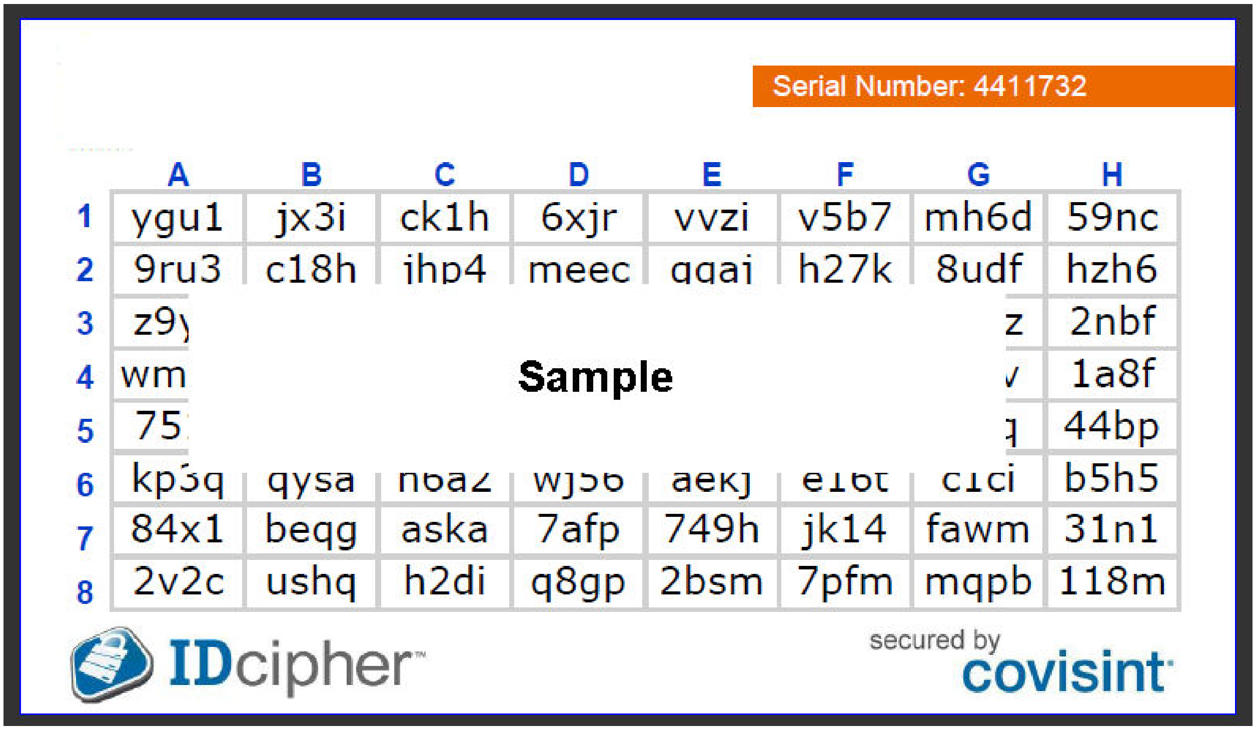
You have successfully viewed your Security Administrators.

IDcipher Card

About the IDcipherTM Card

The IDcipher™ Card is a premium service, available for purchase by your organization.

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 two-factor 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.



Serial Number: 4411732

	A	B	C	D	E	F	G	H
1	ygu1	jx3i	ck1h	6xjr	vvzi	v5b7	mh6d	59nc
2	9ru3	c18h	jhp4	meec	qgai	h27k	8udf	hzh6
3	z9y						z	2nbf
4	wm						v	1a8f
5	75						q	44bp
6	kp3q	qysa	n6a2	wj56	aekj	e16t	c1ci	b5h5
7	84x1	beqg	aska	7afp	749h	jk14	fawm	31n1
8	2v2c	ushq	h2di	q8gp	2bsm	7pfm	mqpb	118m

Sample

IDcipher™

secured by covisint

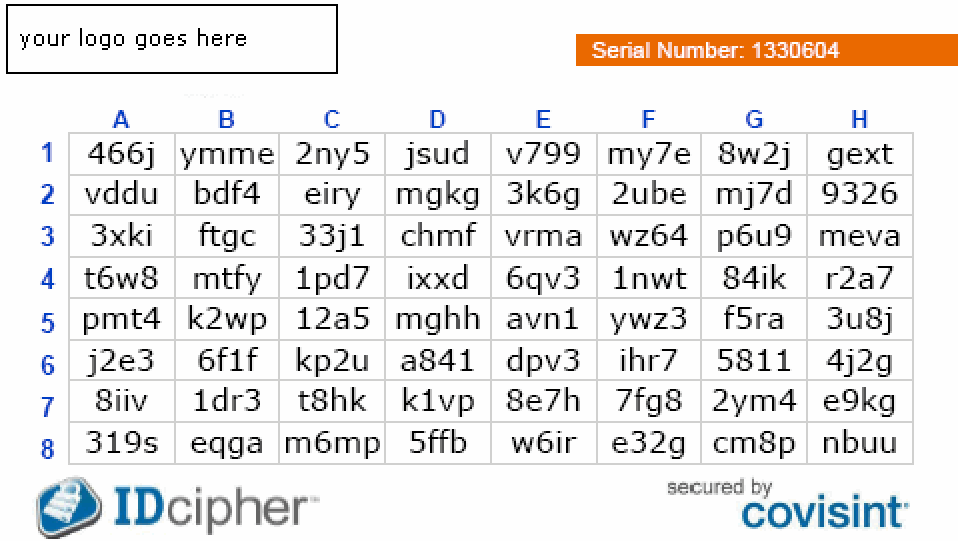
Covisint has trademarked the IDcipher™ Card.

(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 a 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

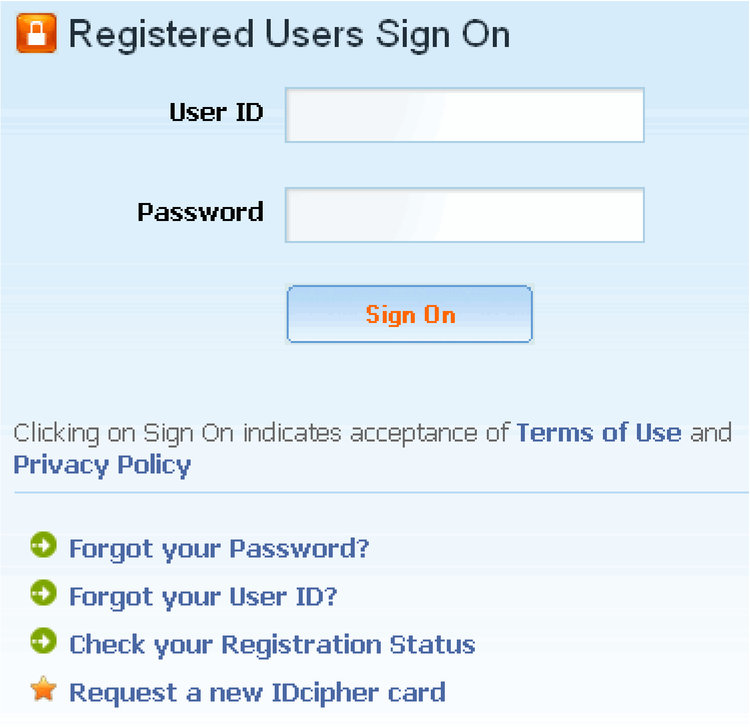
- The card is emailed to the user in PDF format.
- The user prints out a hard copy of the card.
- When a user attempts to sign on to the portal, after keying in the correct User Name and Password, the system may prompt the user for an IDcipherTM card value of a randomly picked cell (for example: column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

(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

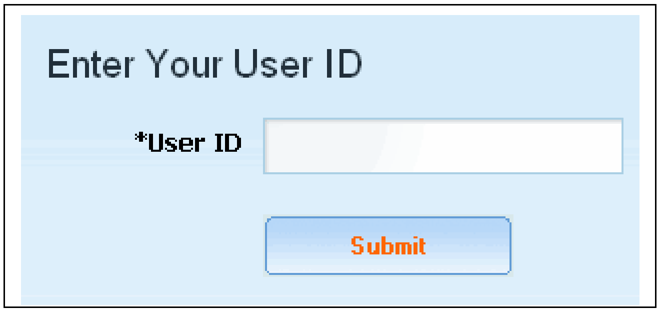
If you are not in possession of your IDcipher™ card, you are able to generate a new card. Complete the following steps to generate a new card that will be emailed to the email address you provided during registration as part of your user profile. (The IDcipher™ Card will be sent to the email address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

1. Navigate to the portal sign on screen.

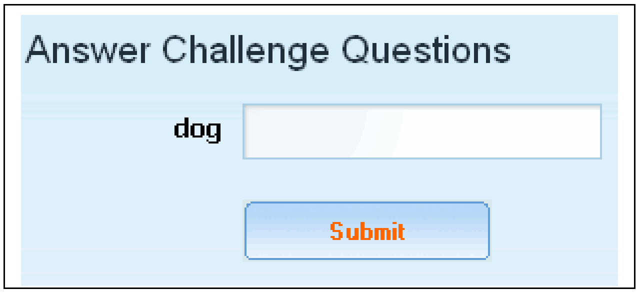


Clicking on Sign On indicates acceptance of Terms of Use and Privacy Policy

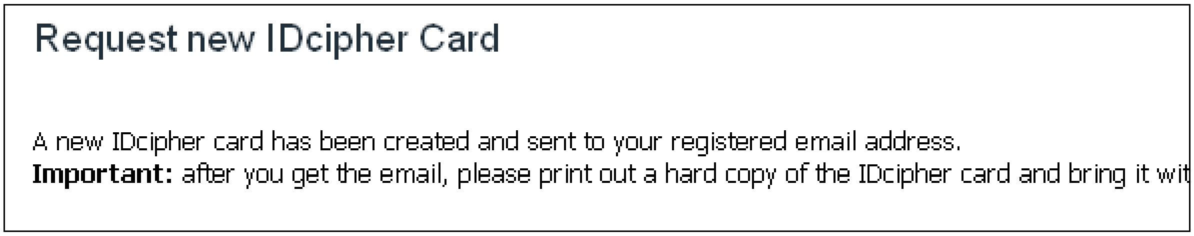
2. Click **Request a new IDcipher**™ **card.** The *enter User ID screen* is displayed.



3.
4. Key in your User ID in the open text field.
5. Click **Submit**. The *challenge question screen* is displayed. **A Challenge Question and Answer combination is used as a security measure if you ever forget your password and need to reset it, or to obtain a replacement IDCipher Card. You will be asked to provide the answer to the challenge question as you created in your account profile.**



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


Request new IDcipher Card

A new IDcipher card has been created and sent to your registered email address.
Important: after you get the email, please print out a hard copy of the IDcipher card and bring it wit

RESULT:

You have successfully obtained a new IDcipherTM Card.

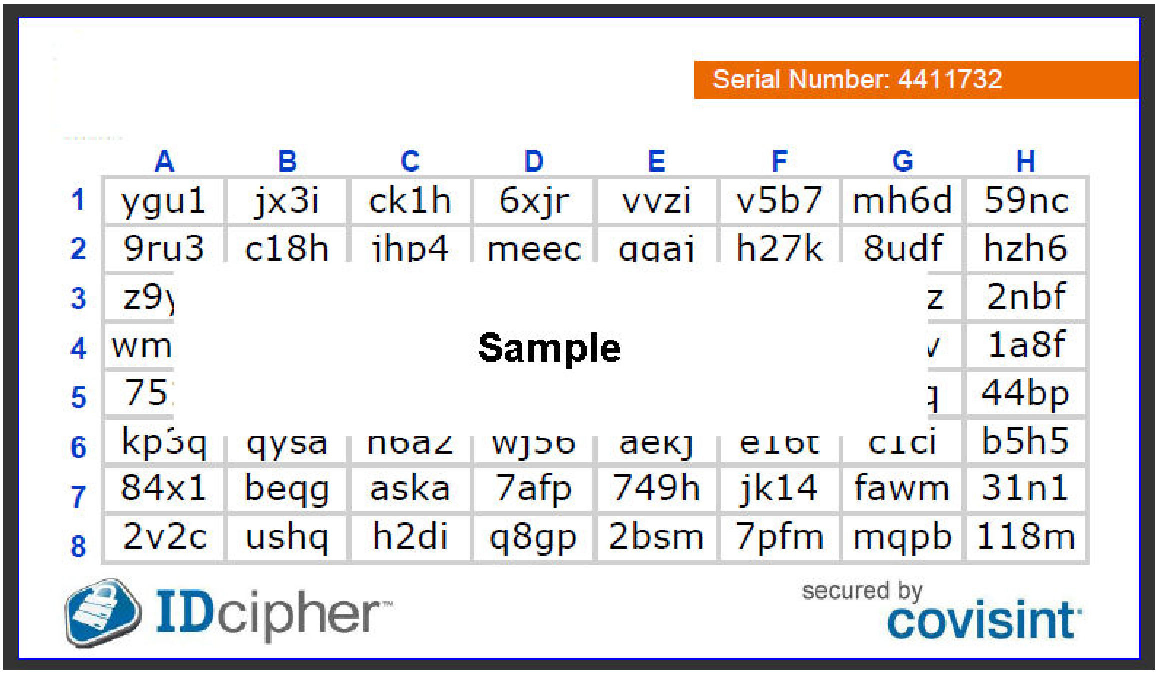
(IDcipher™ card is a premium service available for purchase by portal customers. Please contact your Covisint sales representative for details)

Two-Factor Authentication

Two-factor 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 or how frequently the user signs on).

Covisint provides two-factor authentication (something the user knows and something the user has) for your organization by any of the following methods:

- *IDCipher Card* - User is prompted to key in the code on his/her IDCipher Card Grid at time of login.



Serial Number: 4411732

	A	B	C	D	E	F	G	H
1	ygu1	jx3i	ck1h	6xjr	vvzi	v5b7	mh6d	59nc
2	9ru3	c18h	jhp4	meec	qgai	h27k	8udf	hzh6
3	z9y						z	2nbf
4	wm						v	1a8f
5	75						q	44bp
6	kp3q	qysa	n6a2	wj56	aekj	e16t	c1ci	b5h5
7	84x1	beqg	aska	7afp	749h	jk14	fawm	31n1
8	2v2c	ushq	h2di	q8gp	2bsm	7pfm	mqpb	118m

Sample
IDcipher
secured by
covisint

- SMS Text Messages - User is prompted to key in the code that the system sends to his/her mobile phone at time of login.

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

Application Administrators

Application Administrators

Important Notes:

- **Some organizations do not allow users to request service packages. When that is the case, you will not see the role of Application Administrator.**
- Before proceeding with the help steps in this section for Application Administrators, be sure you have reviewed all of the help steps for **All Users.**
- Some organizations do not allow users to request service packages. When that is the case, you will not see the "view pending requests" option.
- The screenshots in this support material may display links to more tasks then you see when you are logged in, depending on your role/privileges/organization configuration.

Application Administrators are responsible for managing user access to specific applications. The division or organization in which the user belongs must have access to the application before the Application Administrator can grant access to a user.

Division / Organization access is managed by the Organization's Security Administrator (not an Application Administrator).

Approve User's Pending Service Package Request

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

RESULT:

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

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.

Reject User's Pending Service Package Request

1. Click **User Requests** from the Administration -> Pending requests drop-down menu.
2. Click the **User Service Package** tab.
3. Click 📄 to view details of request.
4. Key in the *rejection reason* in the open text box.
5. Enable the 'reject' radio button.
6. Click **submit decision.**
7. 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.

Search for Users in My Organization

1. From the *Search drop-down menu*, click **Search for Users in my Organization.**
2. Select search criteria.
3. Click **Search**. Search results are displayed.
4. Optionally, click on the *name of the user* to view the user's profile.

RESULT:

You have successfully searched for users in your organization

Search for Users across MyAccess

Search for all users across MyAccess who have access to a particular service package that you administer.

1. From the *Search drop-down menu*, click **Search for Users across MyAccess**.
2. Select the *service package* on which you wish to view users from the select a service
3. package drop-down menu.
4. Click **Search**. Search results are displayed.
5. Optionally, click on the name of the user to view the user's profile.

RESULT:

You have successfully searched for users who have access to a particular service package that you administer.

Search for Users by Service Package

Refer to the topic titled Search for Users across MyAccess.

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.

Security Administrators

Getting Started - Managing Users

Important Notes:

- Before proceeding with the help steps in this section for Security Administrators, be sure you have reviewed all of the help steps for **All Users**.
- Some organizations do not allow users to request service packages. When that is the case, you will not see the "view pending requests" option.
- The screenshots in this support material may display links to more tasks then you see when you are logged in, depending on your role/privileges/organization configuration.

Security administrators 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.

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

□ Search for users in your Organization

□ Modify a user's role

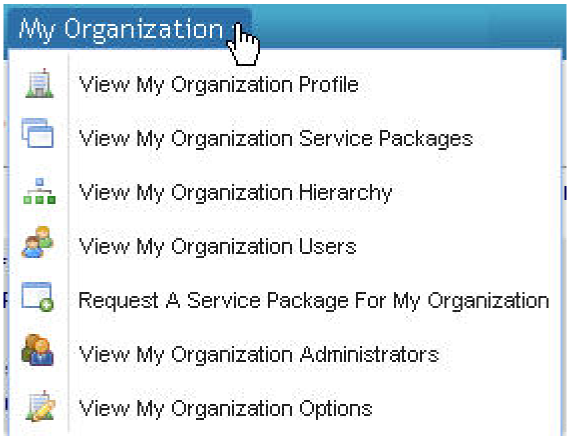
□ Specify a user's password

Managing Your Organization's Users

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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.

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^{TM} card in addition to a user name and password for authentication, then the system will automatically generate and email an IDcipher^{TM} 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^{TM} card, if applicable.

Create a New IDcipherTM Card for User

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

1. Perform a user search.
2. From the search results, click on the *name of the user.*
3. Click **Create a New IDcipher^{TM} 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^{TM} card is sent to the user.

RESULT:

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

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.**

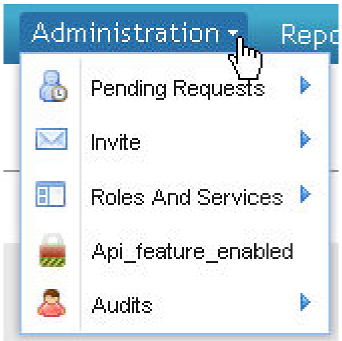
RESULT:

You have successfully edited a user's profile.

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

Getting Started - Managing Users

Important Notes:

- Before proceeding with the help steps in this section for Security Administrators, be sure you have reviewed all of the help steps for **All Users**.
- Some organizations do not allow users to request service packages. When that is the case, you will not see the "view pending requests" option.
- The screenshots in this support material may display links to more tasks then you see when you are logged in, depending on your role/privileges/organization configuration.

Security administrators 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.

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
- □ Search for users in your Organization
- □ Modify a user's role
- □ Specify a user's password

Modify a User’s 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 / divisions 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.

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.

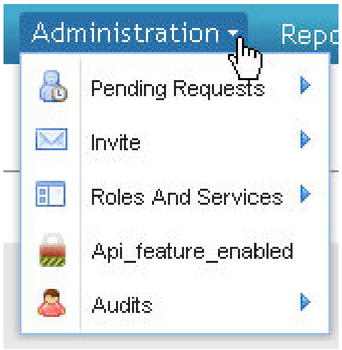
RESULT:

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

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 across MyAccess

Search for all users across MyAccess who have access to a particular service package that you administer.

6. From the *Search drop-down menu*, click **Search for Users across MyAccess**.
7. Select the *service package* on which you wish to view users from the select a service
8. package drop-down menu.
9. Click **Search**. Search results are displayed.
10. Optionally, click on the name of the user to view the user's profile.

RESULT:

You have successfully searched for users who have access to a particular service package that you administer.

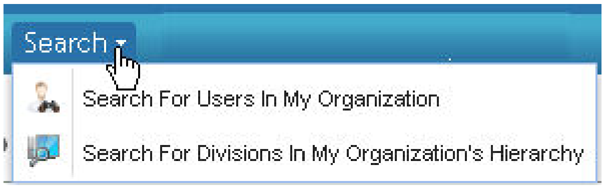
Search for Users by Service Package

Refer to the topic titled Search for Users across MyAccess.

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?


Search
Search For Users In My Organization
Search For Divisions In My Organization's Hierarchy

2. Select search criteria.
3. Click **Search**. Search results are displayed.
4. Optionally, click on the *name of the user* to view the user's profile.

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.**

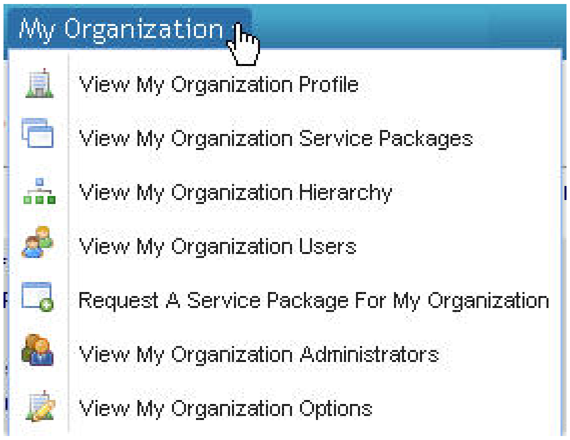
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

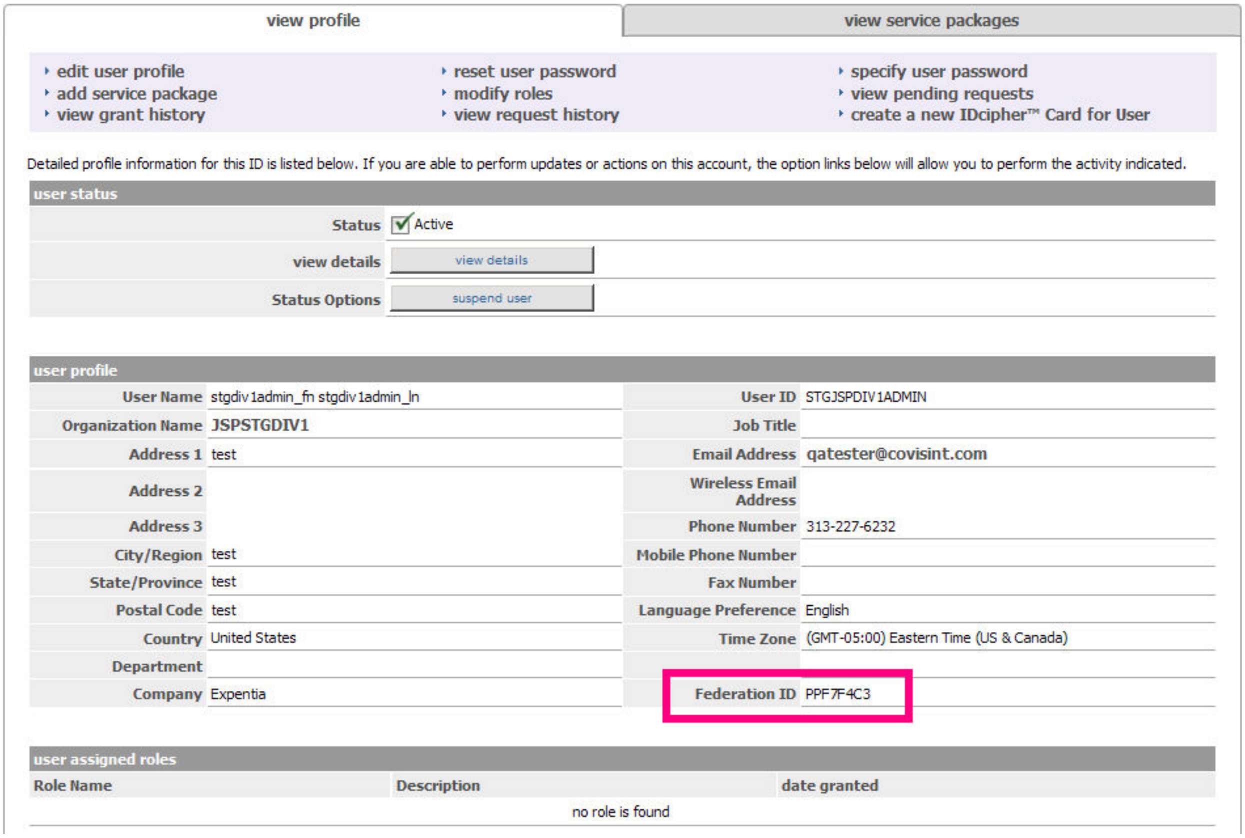
2. Optionally, click on a *User Name* to view details of that user profile.

RESULT:

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

Where Can I Find My User's Federation ID?

Your User's Federation ID is displayed on the View Profile page for that user. As Security Administrator, you may access that page by performing a User Search.



Detailed profile information for this ID is listed below. If you are able to perform updates or actions on this account, the option links below will allow you to perform the activity indicated.

user status

Status	☑ Active
view details	view details
Status Options	suspend user

user profile

User Name	stgdiv1admin_fn stgdiv1admin_ln	User ID	STGJSPDIV1ADMIN
Organization Name	JSPSTGDIV1	Job Title	
Address 1	test	Email Address	qatester@covisint.com
Address 2		Wireless Email Address	
Address 3		Phone Number	313-227-6232
City/Region	test	Mobile Phone Number	
State/Province	test	Fax Number	
Postal Code	test	Language Preference	English
Country	United States	Time Zone	(GMT-05:00) Eastern Time (US & Canada)
Department			
Company	Expentia	Federation ID	PPF7F4C3

user assigned roles

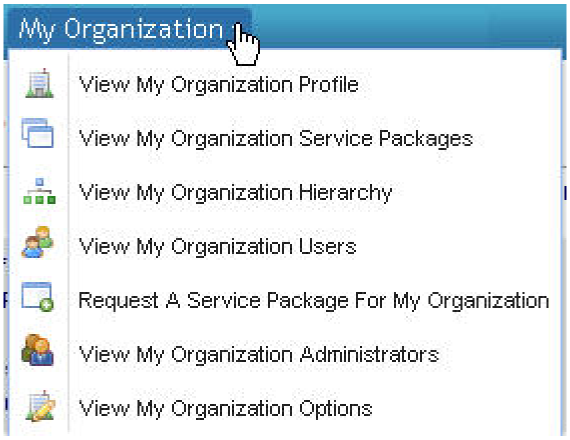
Role Name	Description	date granted
	no role is found	

Managing Your Organization

View Organization Administrators

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

Where is the My Organization drop-down menu?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

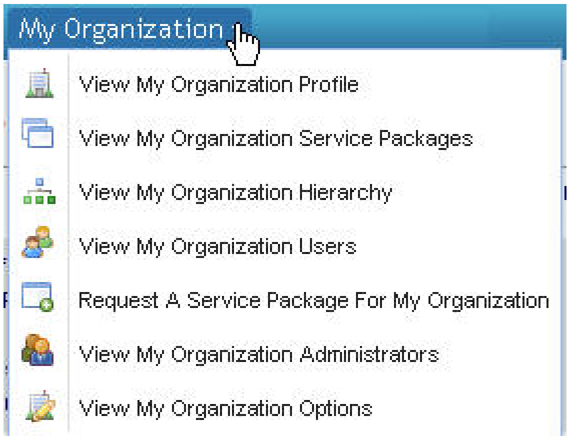
RESULT:

You have successfully viewed all administrators in 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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

RESULT:

You have successfully edited your organizational profile.

Invite Division 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.
2. Key in the *email address for each division's 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 division to register for portal access.

Getting Started - Managing Your Organization

Security Administrators are responsible for the establishment and management of your organization and its divisions, and serve as the main point of contact for the organization.

The checklist below is provided to help you get started managing your **organization** as a Security Administrator, and is applicable for the Top Level Organization as well as at the Division Level Security Administrator.. (Also view the checklist for managing your users.)

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 THE ORGANIZATION

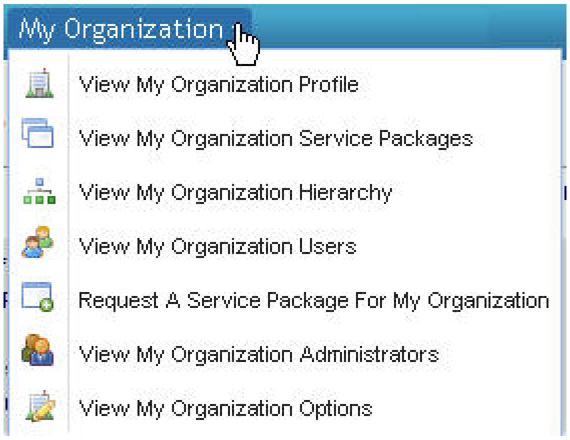
- □ Invite divisions to register for access to the portal
- □ View your organizational hierarchy within this system (and see all divisions belonging to your organization)
- □ Approve pending division access requests
- □ Approve pending service package requests from divisions
- □ Request a sub/service package for your organization
- □ Grant a service package to a division
- □ View your organization's administrators
- □ Edit the organization's profile
- □ Manage your organization's users

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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.**

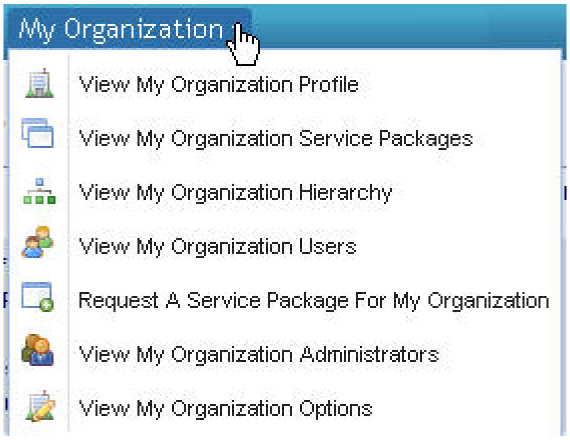
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

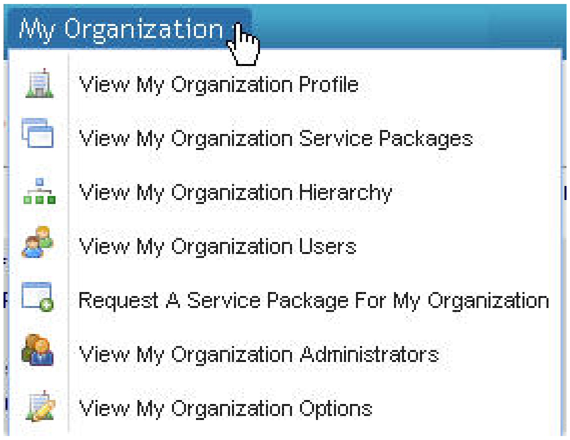
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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:

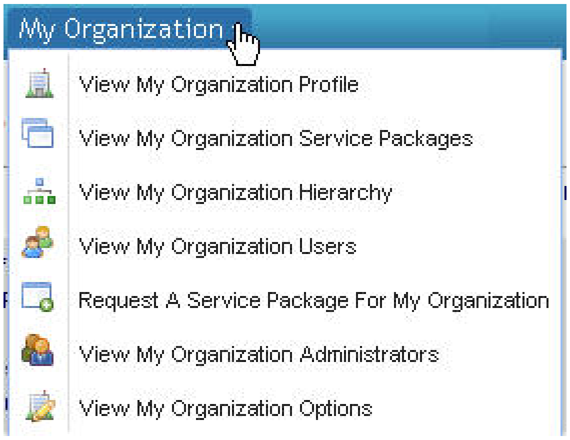
You have successfully requested a service package for your organization.

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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.

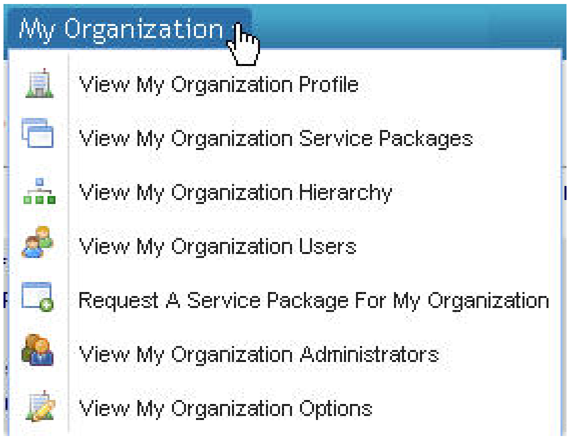
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

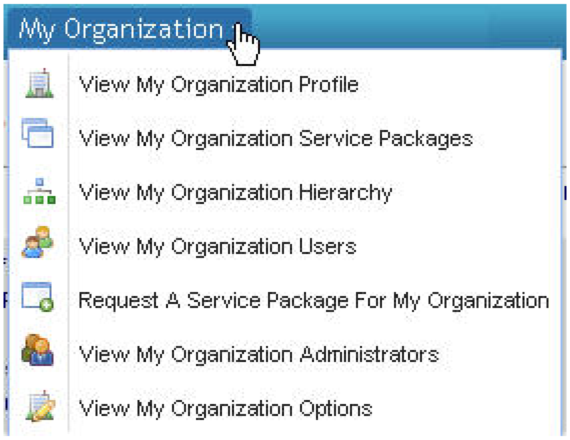
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

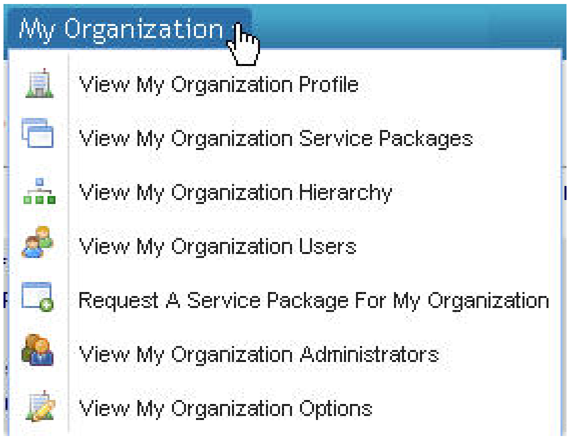
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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.

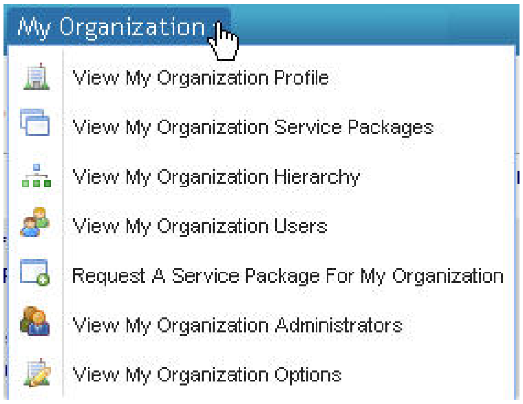
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

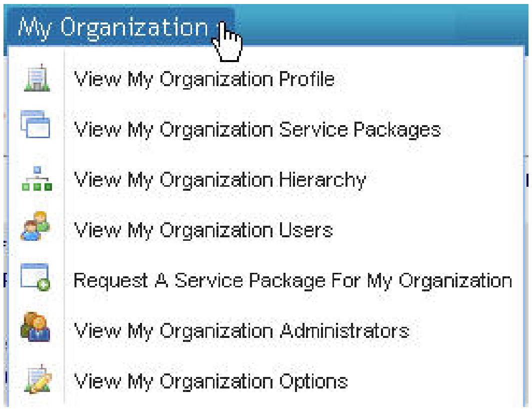
RESULT:

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?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

2. Click **view pending requests.**

RESULT:

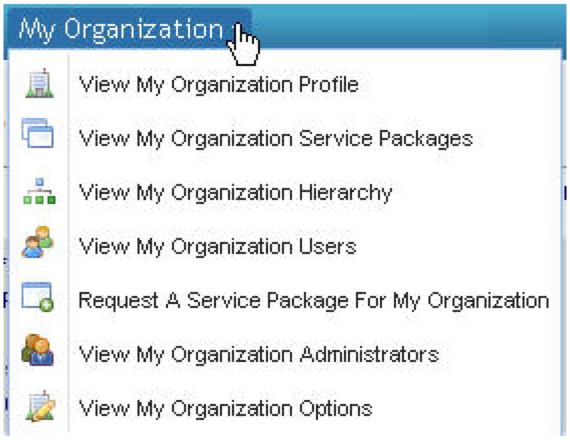
You have successfully viewed your organization's pending requests.

Managing Divisions in Your Organization

View Division Hierarchy

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

Where is the My Organization drop-down menu?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

RESULT:

You have successfully viewed the hierarchy of a division.

Approve Division's Service Package Request

1. Click **Organization Requests** from the **Administration -> Pending requests** drop-down menu.
2. Click 📄 next to the division name.
3. Enable the ‘approve’ radio button next to the selected service package.
4. Click **submit decision**.
5. Click **OK**.

RESULT:

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

Invite Division 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.
2. Key in the *email address for each division's 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.

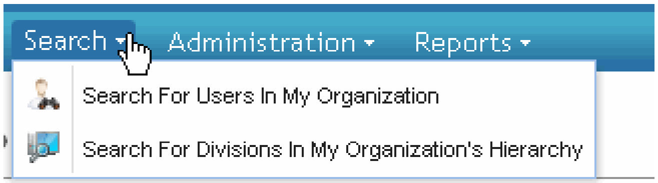
RESULT:

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

Edit Division Profile

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

Where is the Search drop-down menu?


Search
Administration
Reports
Search For Users In My Organization
Search For Divisions In My Organization's Hierarchy

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

RESULT:

You have successfully edited the profile of a division.

Permanently Remove Service Package from a Division

1. Click **View my organization hierarchy** from the Administration -> Pending requests drop-down menu.
2. From the search results, click on the *division name*.
3. Click **view service packages** tab.
4. Click on the *name of the service package* you wish to remove.
5. Click **permanently remove organization's grant for service package.**
6. Key in the *reason for removal* in the open text box.
7. Click **yes, proceed with removal.**

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

RESULT:

You have successfully removed a service package from a division.

Reject Division's Service Package Request

1. Click **Organization Requests** from the Administration -> Pending requests drop-down menu.
2. Click 📄 next to the division name.
3. Enable the ‘reject’ radio button next to the selected service package.
4. Key in the *rejection reason* in the open text box.
5. Click **submit decision.**
6. Click **OK.**

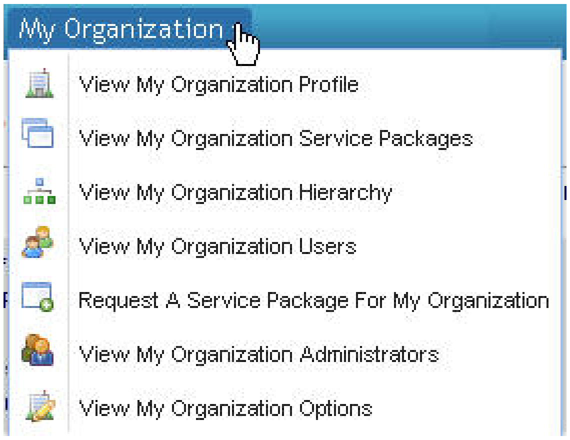
RESULT:

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

Suspend a Service Package from a Division

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

Where is the My Organization drop-down menu?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

2. From the search results, click on the *division name*.
3. Click **view service packages** tab.
4. Click on the *name of the service package* you wish to suspend.
5. Click suspend.
6. Key in the reason for suspension in the open text box.
7. Click **yes, proceed with suspension.**

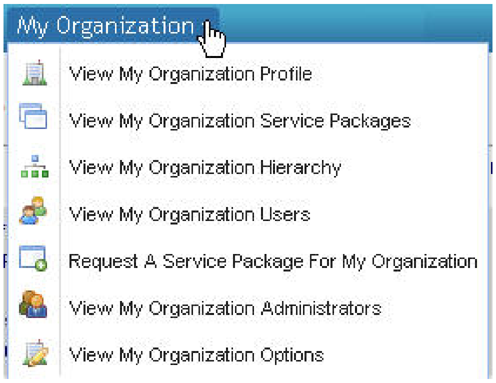
RESULT:

You have successfully suspended a service package from a division.

View Division Administrators

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

Where is the My Organization drop-down menu?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

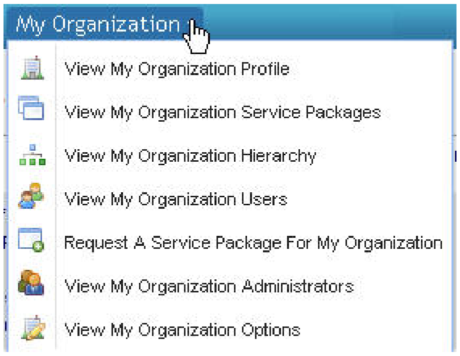
RESULT:

You have successfully viewed division administrators.

View Division Grant History

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

Where is the My Organization drop-down menu?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

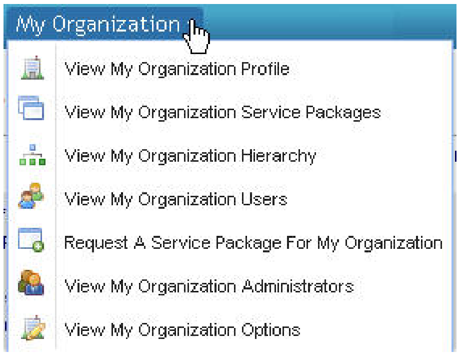
RESULT:

You have successfully viewed the grant history of a division.

View Division Hierarchy

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

Where is the My Organization drop-down menu?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

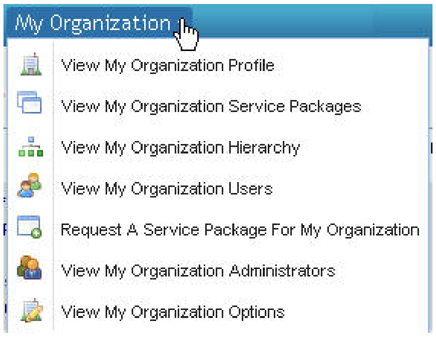
RESULT:

You have successfully viewed the hierarchy of a division.

View Division Request History

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

Where is the My Organization drop-down menu?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

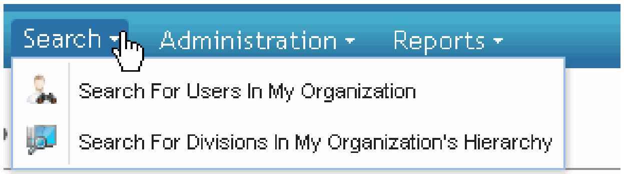
RESULT:

You have successfully viewed the request history of a division.

View Division Service Packages

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

Where is the Search drop-down menu?


Search
Administration
Reports
Search For Users In My Organization
Search For Divisions In My Organization's Hierarchy

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

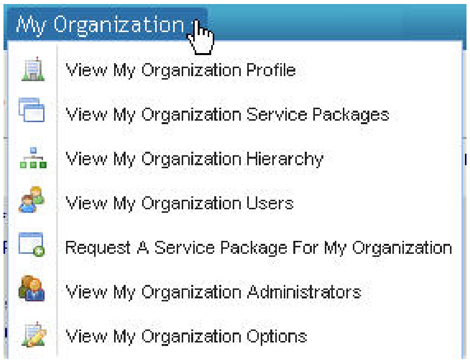
RESULT:

You have successfully viewed service packages of a division.

View Users in a Division

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

Where is the My Organization drop-down menu?


My Organization
View My Organization Profile
View My Organization Service Packages
View My Organization Hierarchy
View My Organization Users
Request A Service Package For My Organization
View My Organization Administrators
View My Organization Options

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

RESULT:

You have successfully viewed all users in a division.

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 Summary Report

1. Click Service Owner Reports from 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 organization count, and total unique parent supplier code count (if applicable) for a given service package.

RESULT:

You have successfully generated a Summary report.

Generate a Service Summary Report

1. Click **Service Summary** from the **Reports** drop down menu. The Service Summary screen is displayed.
2. View the *number of users* by service package type.
3. If desired, click on the number in the column of the Service Package to view additional details. 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.
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.

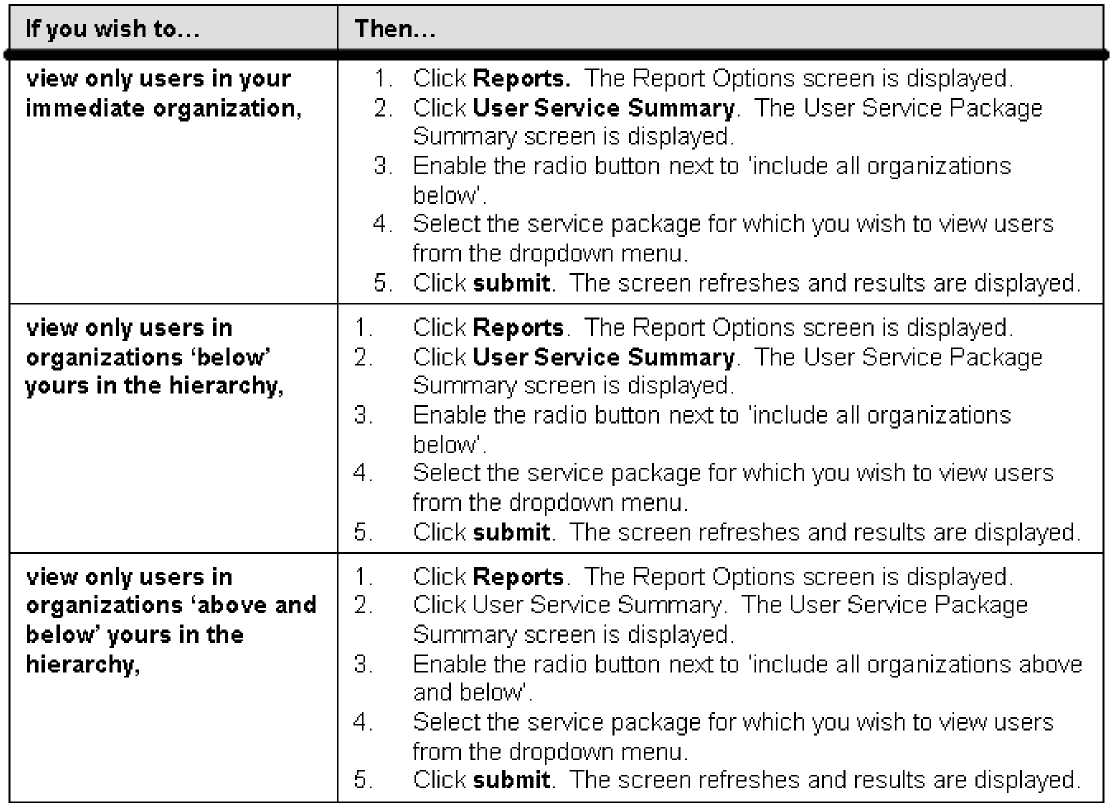
Generate a User Service Package Grant Report

1. Click **Security Administrator Reports** from the **Reports** drop-down menu.
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.
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**.
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**.
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 i*nclude 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 being '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.

Reports - Service Admin

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

Service Administrator Reports

> ℹ 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.
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 organization count, and total unique parent supplier code count (if applicable) 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.
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.
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.