AppCloud^{TM}
Administrator’s Guide

Table Of Contents

APPCLOUDTM OVERVIEW

AppCloudTM provides Application Providers with a single point of integration and management, utilizing self-service features, which allows an Application Provider to make their application or applications available to specific targeted communities.

AppCloud also provides Application Providers with standard integration interfaces that can be utilized to support various types of bi-directional data exchanges between the targeted communities and the Application Provider.

AppCloudTM provides Sponsors of Covisint hosted portal communities with a single location to obtain business relevant third-party applications for their users. With the click of a mouse, users may register or subscribe to a variety of software applications in a highly secure environment at their desktop.

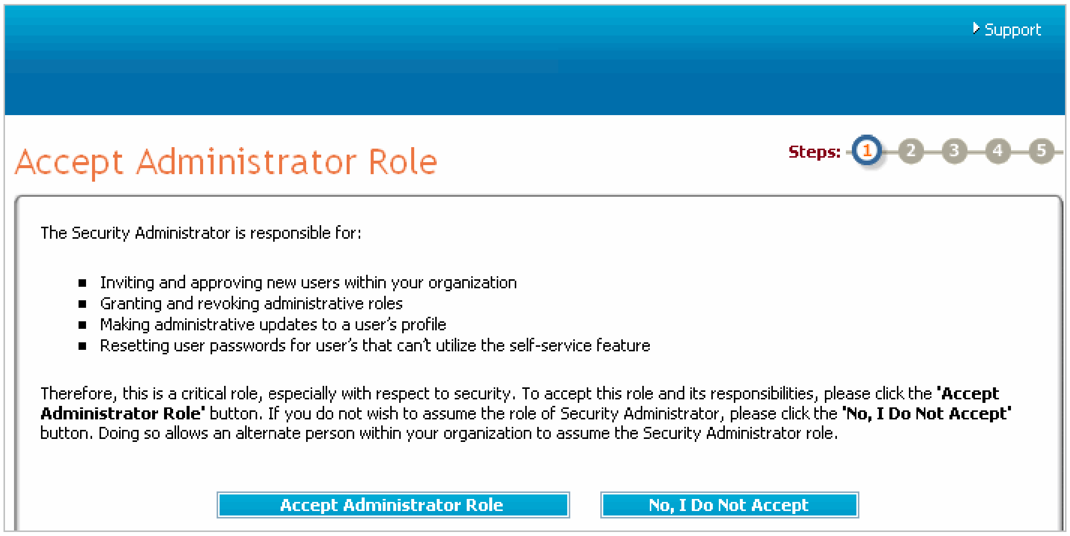
Once approved, the user may access the applications through Single Sign-On (SSO), avoiding the need to recall multiple user names and passwords. Additionally, users are able to utilize data within their portal that was provided by the Application Provider through AppCloud.

AppCloud is an ideal solution for Application Providers that want to offer applications to an established set of targeted business communities within a specific industry and/or across a variety of industries.

REGISTERING MY ORGANIZATION

This feature is used to allow Organizations, which have been invited to AppCloud™ by Covisint, to register their Organizations with AppCloud™. This registration process is also used to specify the Organization's primary ***Security Administrator.*** During registration, the designated Security Administrator provides information which is required by Covisint in order to obtain a User Name and Password that the Security Administrator will use to sign-on to AppCloud™.

1. Retrieve from your email Inbox the invitation to register your organization. This email should have a subject line similar to: "Organization Invitation from AppCloud™"
2. Copy / paste the URL from the email into a web browser. Step One of the Organization Registration wizard is displayed.



Accept Administrator Role

The Security Administrator is responsible for:

- Inviting and approving new users within your organization
- Granting and revoking administrative roles
- Making administrative updates to a user's profile
- Resetting user passwords for user's that can't utilize the self-service feature

Therefore, this is a critical role, especially with respect to security. To accept this role and its responsibilities, please click the **'Accept Administrator Role'** button. If you do not wish to assume the role of Security Administrator, please click the **'No, I Do Not Accept'** button. Doing so allows an alternate person within your organization to assume the Security Administrator role.

3. Click **Accept Administration Role.** You are able to delegate this role to other users in your organization after they have also registered in the system. The Organization Information screen is displayed.
4. Key in all fields as required. (Required fields are identified with an * and a red bar next to the field name).
5. Click **Continue Registration.** The User Information screen is displayed.
6. Key in all fields as required. (Required fields are identified with an * and a red bar next to the field name).
7. Click **Continue Registration.** The User Information screen is displayed.
8. In the User Name field, create the user name you will use each time you log in to the system.
9. Create a password in the Password field. Ensure the password conforms to the ***password rules.***
10. Key in the password again in the Re-enter Password field.
11. Select a ***challenge question*** from the drop down menu.
12. Key in the answer to the question in the Challenge Answer field. There is a 255-character limit in the answer field.
13. Click **Continue Registration.** The Review and Submit screen is displayed.

14. After reviewing the information and verifying accuracy, click **Submit Registration.** The screen refreshes, and your request is submitted to the Community Administrator.

RESULT:
You have successfully submitted a registration request for your organization.

Defining User Roles and Privileges

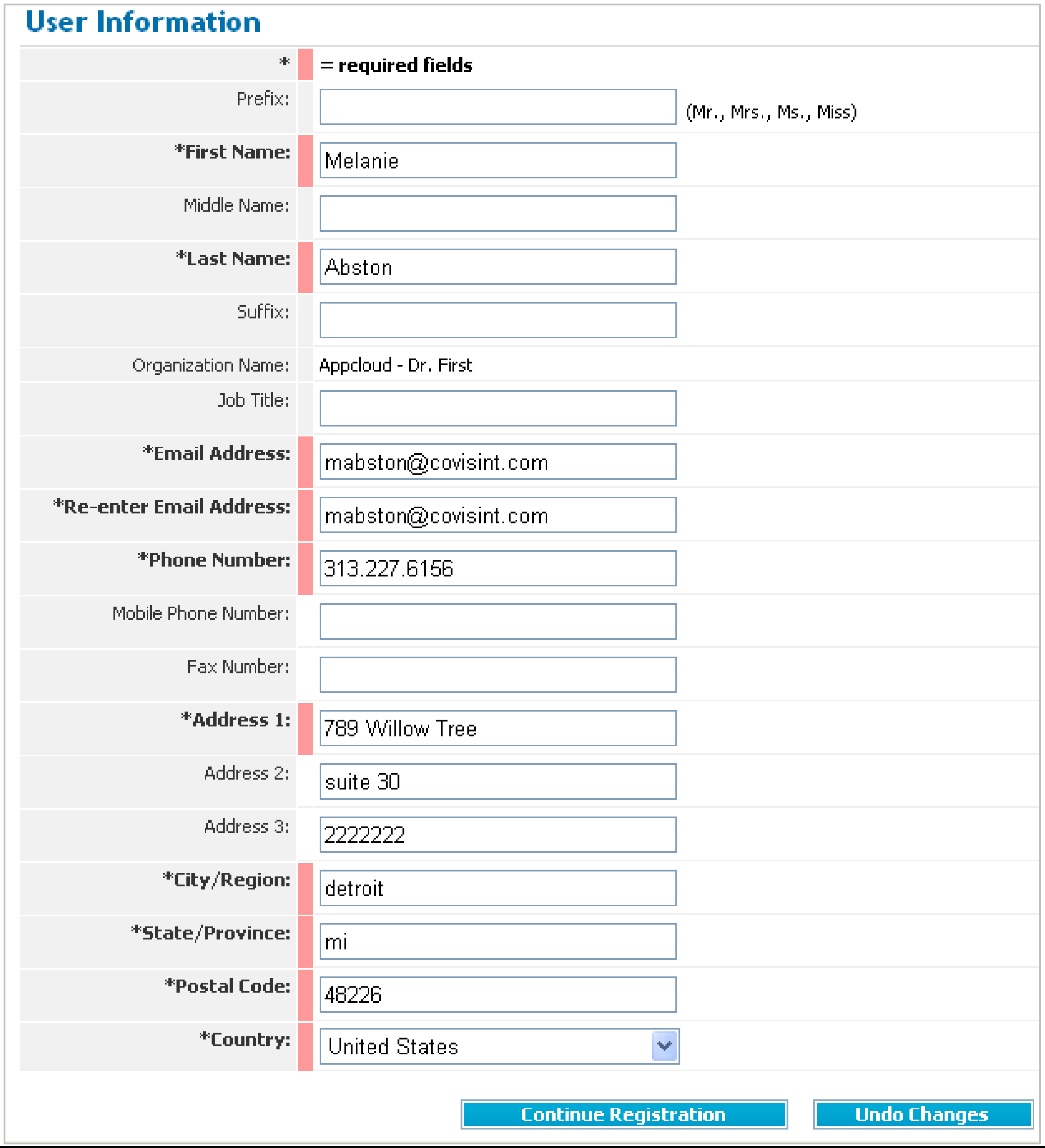
ROLE NAME:	PRIVILEGES:
Security Administrator	• invite a user to register • grant/revoke Admin role to/from a users • modify a user profile • reset a user password • suspend a user account • unsuspend a user account • terminate a user account
Federation Configuration Administrator (referred to as Fed Config Admin)	• create a Federation Connection by using the self-service configuration wizard that is protocol-specific and is used to exchange configuration information between Covisint and the Application Service Provider • test the federation connection • review and update configuration information associated with any of their federation connections (limited to the staging environment only)
Application Configuration Administrator (referred to as App Config Admin)	• add new applications to AppCloud • manage existing applications within AppCloud • delete from AppCloud applications that are no longer in use
Application Access Administrator (referred to as App Access Admin)	• review all the pending application access requests that have originated from one to many sponsors • view details of a request approve or reject a user request for access to the Access Admin's application • view users that have access to the Access Admin's application • revoke access from selected users

COMMON TASKS FOR ALL ROLES

Registering as a New User

1. Click the URL in the **invitation email** you received. The **Registration screen** is displayed.

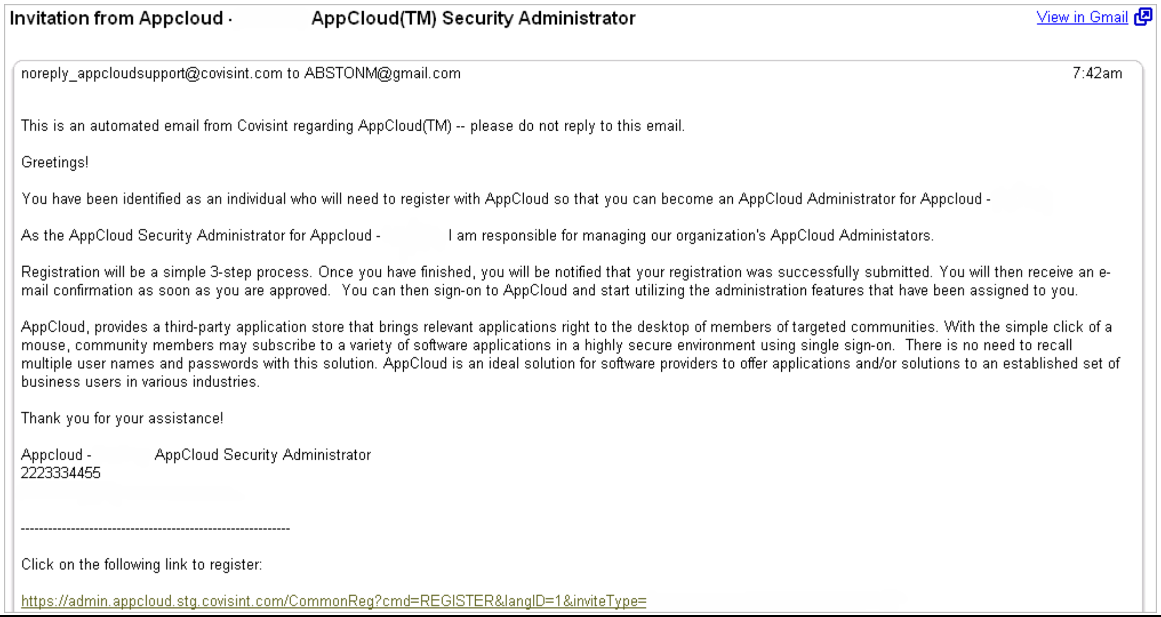
Registration Screen:



User Information

*	= required fields
Prefix:	(Mr., Mrs., Ms., Miss)
*First Name:	Melanie
Middle Name:	
*Last Name:	Abston
Suffix:	
Organization Name:	Appcloud - Dr. First
Job Title:	
*Email Address:	mabston@covisint.com
*Re-enter Email Address:	mabston@covisint.com
*Phone Number:	313.227.6156
Mobile Phone Number:	
Fax Number:	
*Address 1:	789 Willow Tree
Address 2:	suite 30
Address 3:	2222222
*City/Region:	detroit
*State/Province:	mi
*Postal Code:	48226
*Country:	United States

Email Invitation:



Invitation from Appcloud - AppCloud(TM) Security Administrator

noreply_appcloudsupport@covisint.com to ABSTONM@gmail.com 7:42am

This is an automated email from Covisint regarding AppCloud(TM) -- please do not reply to this email.

Greetings!

You have been identified as an individual who will need to register with AppCloud so that you can become an AppCloud Administrator for Appcloud -

As the AppCloud Security Administrator for Appcloud - I am responsible for managing our organization's AppCloud Administators.

Registration will be a simple 3-step process. Once you have finished, you will be notified that your registration was successfully submitted. You will then receive an e-mail confirmation as soon as you are approved. You can then sign-on to AppCloud and start utilizing the administration features that have been assigned to you.

AppCloud, provides a third-party application store that brings relevant applications right to the desktop of members of targeted communities. With the simple click of a mouse, community members may subscribe to a variety of software applications in a highly secure environment using single sign-on. There is no need to recall multiple user names and passwords with this solution. AppCloud is an ideal solution for software providers to offer applications and/or solutions to an established set of business users in various industries.

Thank you for your assistance!

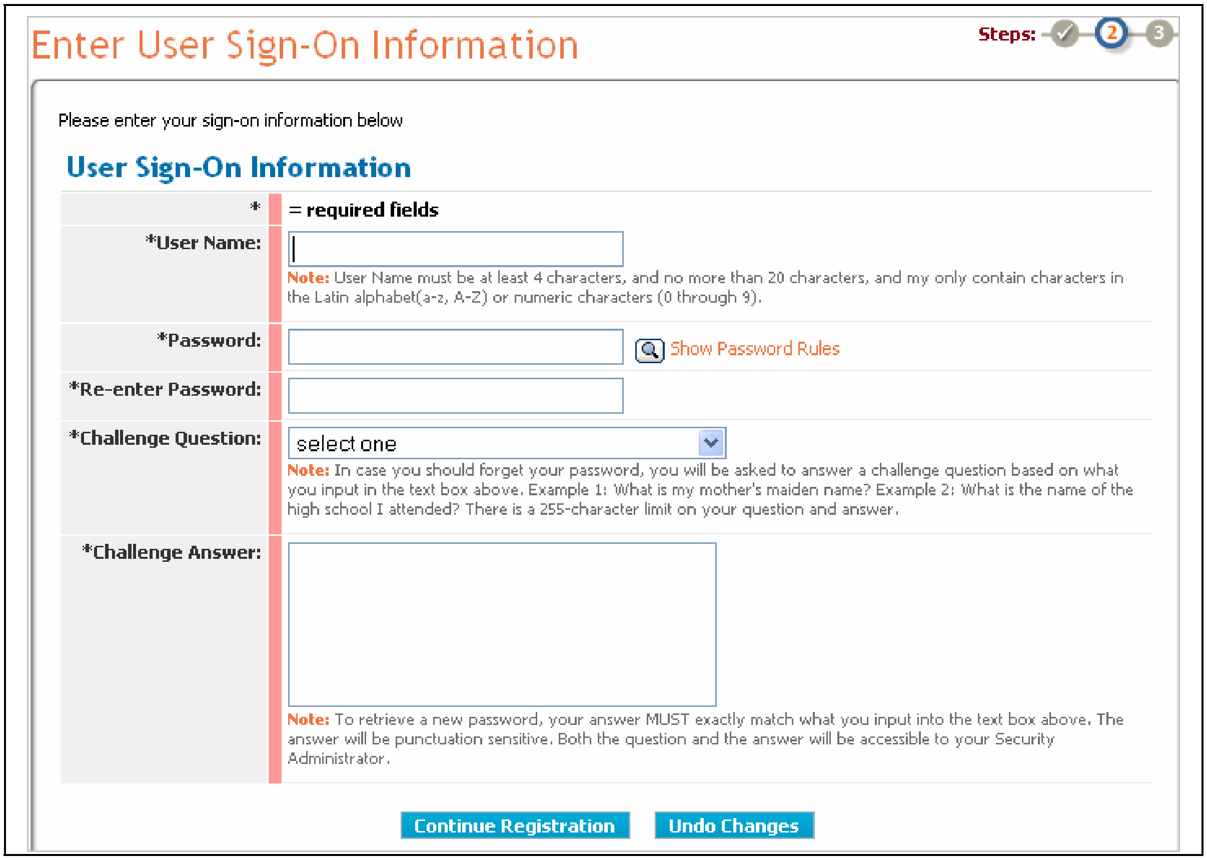
Appcloud - AppCloud Security Administrator
2223334455

Click on the following link to register:

https://admin.appcloud.stg.covisint.com/CommonReg?cmd=REGISTER&langID=1&inviteType=

2. Key in all fields as required. (Required fields are identified with an * and a red bar next to the field name).
3. Click **Continue Registration**. The screen refreshes and the **User Information** screen is displayed.

User Information Screen:



Enter User Sign-On Information

Please enter your sign-on information below

User Sign-On Information

*	= required fields
*User Name:	Note: User Name must be at least 4 characters, and no more than 20 characters, and my only contain characters in the Latin alphabet(a-z, A-Z) or numeric characters (0 through 9).
*Password:	Show Password Rules
*Re-enter Password:	
*Challenge Question:	select one Note: In case you should forget your password, you will be asked to answer a challenge question based on what you input in the text box above. Example 1: What is my mother's maiden name? Example 2: What is the name of the high school I attended? There is a 255-character limit on your question and answer.
*Challenge Answer:	Note: To retrieve a new password, your answer MUST exactly match what you input into the text box above. The answer will be punctuation sensitive. Both the question and the answer will be accessible to your Security Administrator.

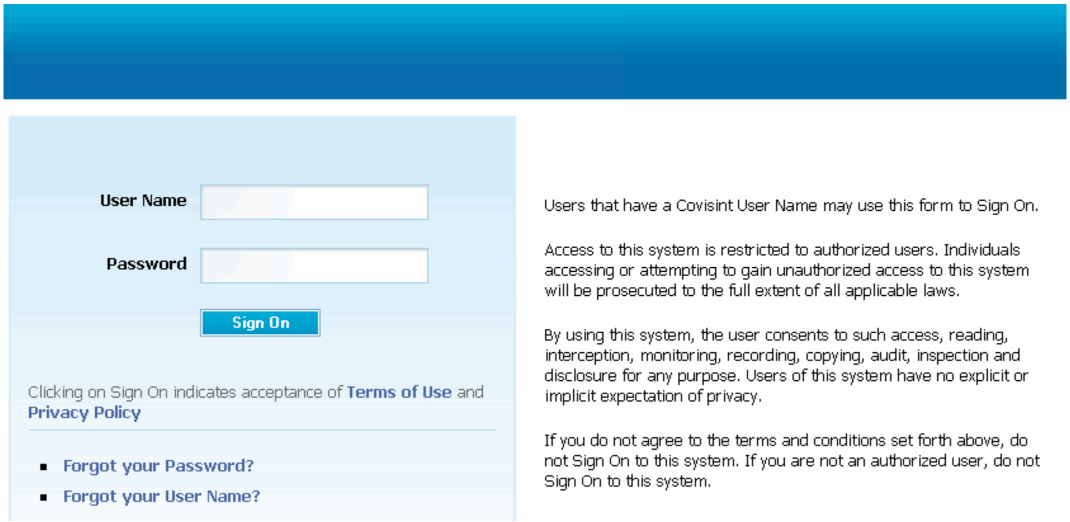
4. In the User Name field, create the user name you will use each time you sign-on to the system.
5. Create a password in the Password field. Ensure the password conforms to the ***password rules.***
6. Key in the password again in the Re-enter Password field.
7. Select a ***challenge question*** from the drop down menu.
8. Key in the answer to the question in the Challenge Answer field. There is a 255-character limit in the answer field.
9. Click **Continue Registration.** The Review and Submit screen is displayed.
10. After reviewing the information and verifying accuracy, click **Submit Registration.** The screen refreshes, and your request is submitted to the Security Administrator.

RESULT:

You have successfully submitted a registration request.

Signing-On to AppCloud

1. Navigate to the AppCloud™ URL.



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

- **Forgot your Password?**
- **Forgot your User Name?**

Users that have a Covisint User Name may use this form to Sign On.

Access to this system is restricted to authorized users. Individuals accessing or attempting to gain unauthorized access to this system will be prosecuted to the full extent of all applicable laws.

By using this system, the user consents to such access, reading, interception, monitoring, recording, copying, audit, inspection and disclosure for any purpose. Users of this system have no explicit or implicit expectation of privacy.

If you do not agree to the terms and conditions set forth above, do not Sign On to this system. If you are not an authorized user, do not Sign On to this system.

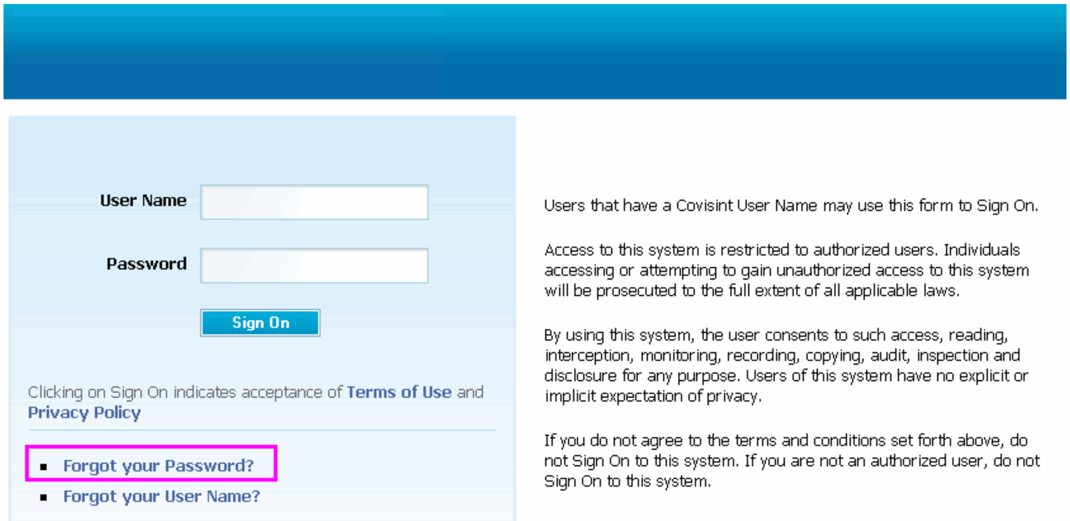
2. Key in your user name in the open text field (this is the name you created during registration).
3. Key in your password in the open text field (this is the password you created during registration).
4. Click **Sign On.** The screen refreshes and you are signed-on to AppCloud™

RESULT:

You have successfully signed-on to AppCloud™

Forgot Your Password?

1. Navigate to the AppCloud^{TM} URL.



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

- **Forgot your Password?**
- **Forgot your User Name?**

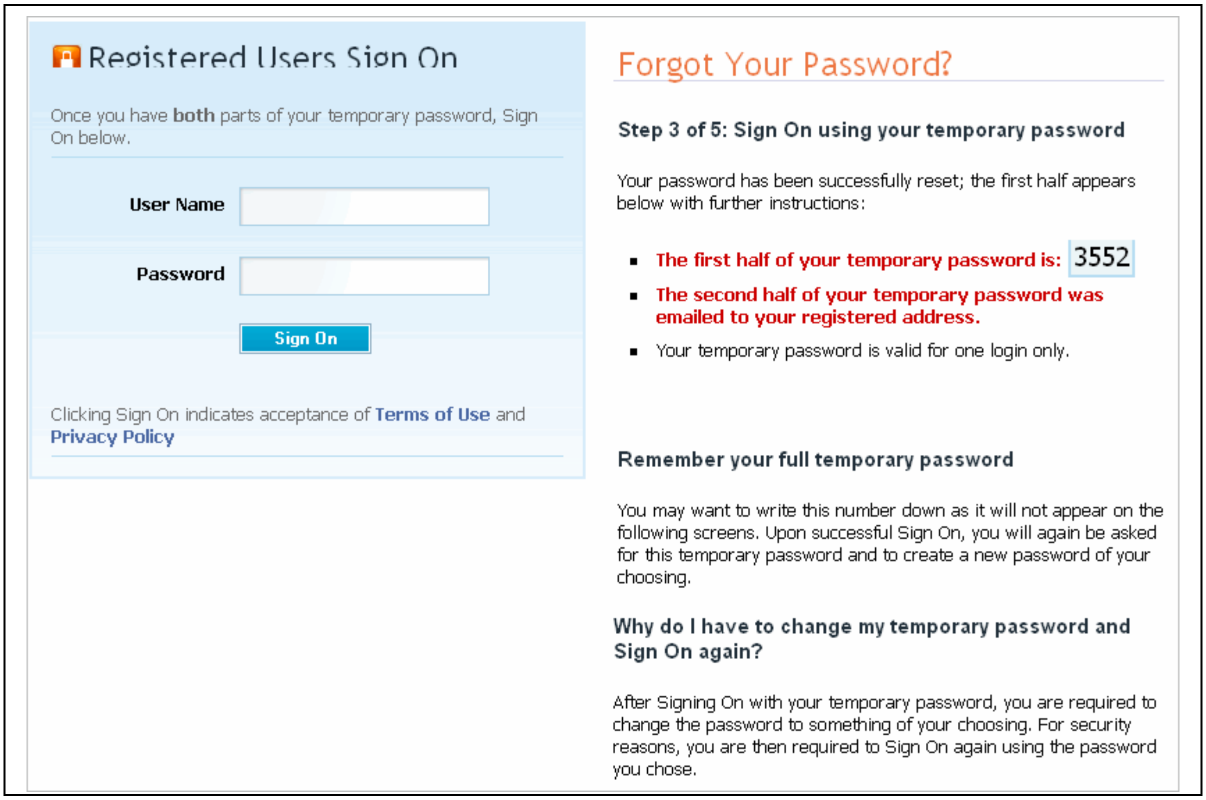
Users that have a Covisint User Name may use this form to Sign On.

Access to this system is restricted to authorized users. Individuals accessing or attempting to gain unauthorized access to this system will be prosecuted to the full extent of all applicable laws.

By using this system, the user consents to such access, reading, interception, monitoring, recording, copying, audit, inspection and disclosure for any purpose. Users of this system have no explicit or implicit expectation of privacy.

If you do not agree to the terms and conditions set forth above, do not Sign On to this system. If you are not an authorized user, do not Sign On to this system.

2. Click **Forgot your Password?** The User Name screen is displayed.
3. Key in your user name in the open text field, then click **Submit**. The challenge question you selected during registration is displayed.
4. Key in the answer to the challenge question. The answer must match exactly the answer you provided during registration, including punctuation and case-sensitivity.
5. Click **Submit**. The screen refreshes, and the **first four digits of your temporary eight digit password is displayed**.



Registered Users Sign On

Once you have **both** parts of your temporary password, Sign On below.

User Name

Password

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

Forgot Your Password?

Step 3 of 5: Sign On using your temporary password

Your password has been successfully reset; the first half appears below with further instructions:

- **The first half of your temporary password is:** 3552
- **The second half of your temporary password was emailed to your registered address.**
- Your temporary password is valid for one login only.

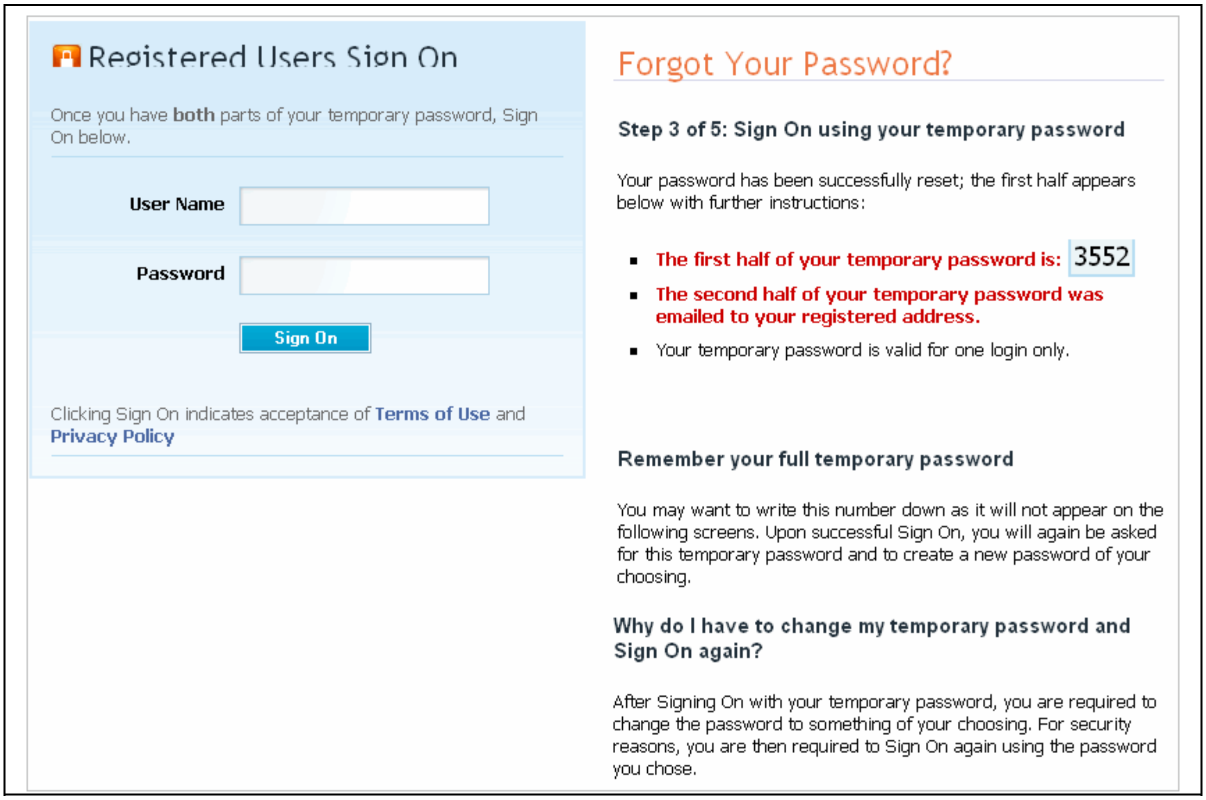
Remember your full temporary password

You may want to write this number down as it will not appear on the following screens. Upon successful Sign On, you will again be asked for this temporary password and to create a new password of your choosing.

Why do I have to change my temporary password and Sign On again?

After Signing On with your temporary password, you are required to change the password to something of your choosing. For security reasons, you are then required to Sign On again using the password you chose.

6. Write down the **four digits that are displayed on your screen**.



Registered Users Sign On

Once you have **both** parts of your temporary password, Sign On below.

User Name

Password

Sign On

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

Forgot Your Password?

Step 3 of 5: Sign On using your temporary password

Your password has been successfully reset; the first half appears below with further instructions:

- **The first half of your temporary password is:** 3552
- **The second half of your temporary password was emailed to your registered address.**
- Your temporary password is valid for one login only.

Remember your full temporary password

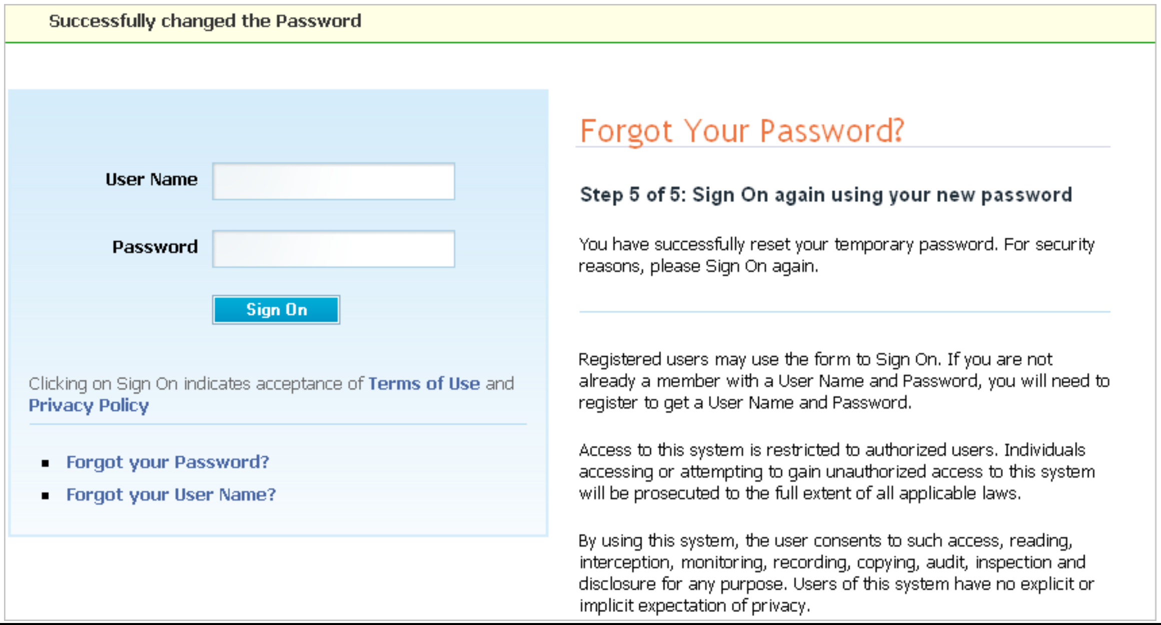
You may want to write this number down as it will not appear on the following screens. Upon successful Sign On, you will again be asked for this temporary password and to create a new password of your choosing.

Why do I have to change my temporary password and Sign On again?

After Signing On with your temporary password, you are required to change the password to something of your choosing. For security reasons, you are then required to Sign On again using the password you chose.

7. Retrieve the remaining four digits of the temporary password from the email inbox of the account that you provided during registration.
8. Navigate back to the sign-on URL.
9. Key in your user name in the open text field.
10. Key in the temporary eight-digit password in the password field.
11. Click **Sign On.** The screen refreshes, and the Create New Password screen is displayed.
12. Key in the eight-digit password in the Old Password field.
13. Key in a new password in the New Password field. Ensure the password conforms to the ***password rules.***
14. Key in the new password again in the Confirm New Password field.
15. Click **Update**. A **message confirming the successful update of the password is displayed**.

Successful Password Change



Successfully changed the Password

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

- Forgot your Password?
- Forgot your User Name?

Forgot Your Password?

Step 5 of 5: Sign On again using your new password

You have successfully reset your temporary password. For security reasons, please Sign On again.

Registered users may use the form to Sign On. If you are not already a member with a User Name and Password, you will need to register to get a User Name and Password.

Access to this system is restricted to authorized users. Individuals accessing or attempting to gain unauthorized access to this system will be prosecuted to the full extent of all applicable laws.

By using this system, the user consents to such access, reading, interception, monitoring, recording, copying, audit, inspection and disclosure for any purpose. Users of this system have no explicit or implicit expectation of privacy.

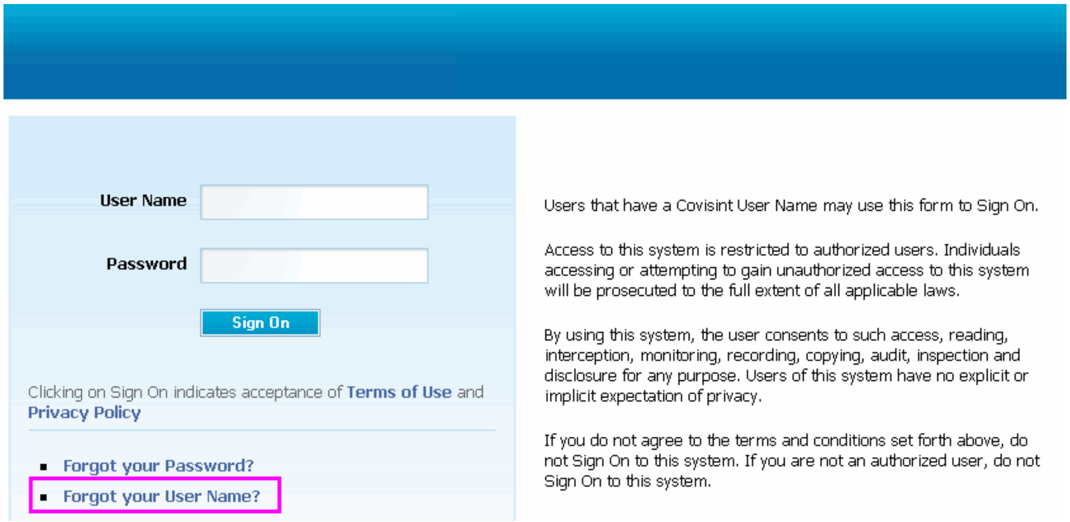
16. Optionally, sign-on to AppCloud™ using your new password.

RESULT:

You have successfully reset your forgotten password.

Forgot Your User Name?

1. Navigate to the AppCloud^{TM} URL.



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

- Forgot your Password?
- Forgot your User Name?

Users that have a Covisint User Name may use this form to Sign On.

Access to this system is restricted to authorized users. Individuals accessing or attempting to gain unauthorized access to this system will be prosecuted to the full extent of all applicable laws.

By using this system, the user consents to such access, reading, interception, monitoring, recording, copying, audit, inspection and disclosure for any purpose. Users of this system have no explicit or implicit expectation of privacy.

If you do not agree to the terms and conditions set forth above, do not Sign On to this system. If you are not an authorized user, do not Sign On to this system.

2. Click **Forgot your User Name?**
3. Key in the email address that you provided during registration in the open text field.
4. Click **Submit**. The screen refreshes, and your User Name is delivered to the inbox of the email address you provided during registration.

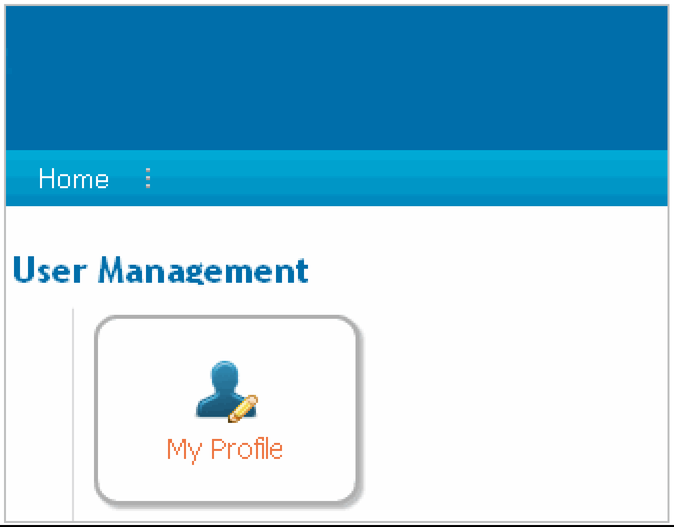
RESULT:

You have successfully retrieved your user name.

Changing My Password

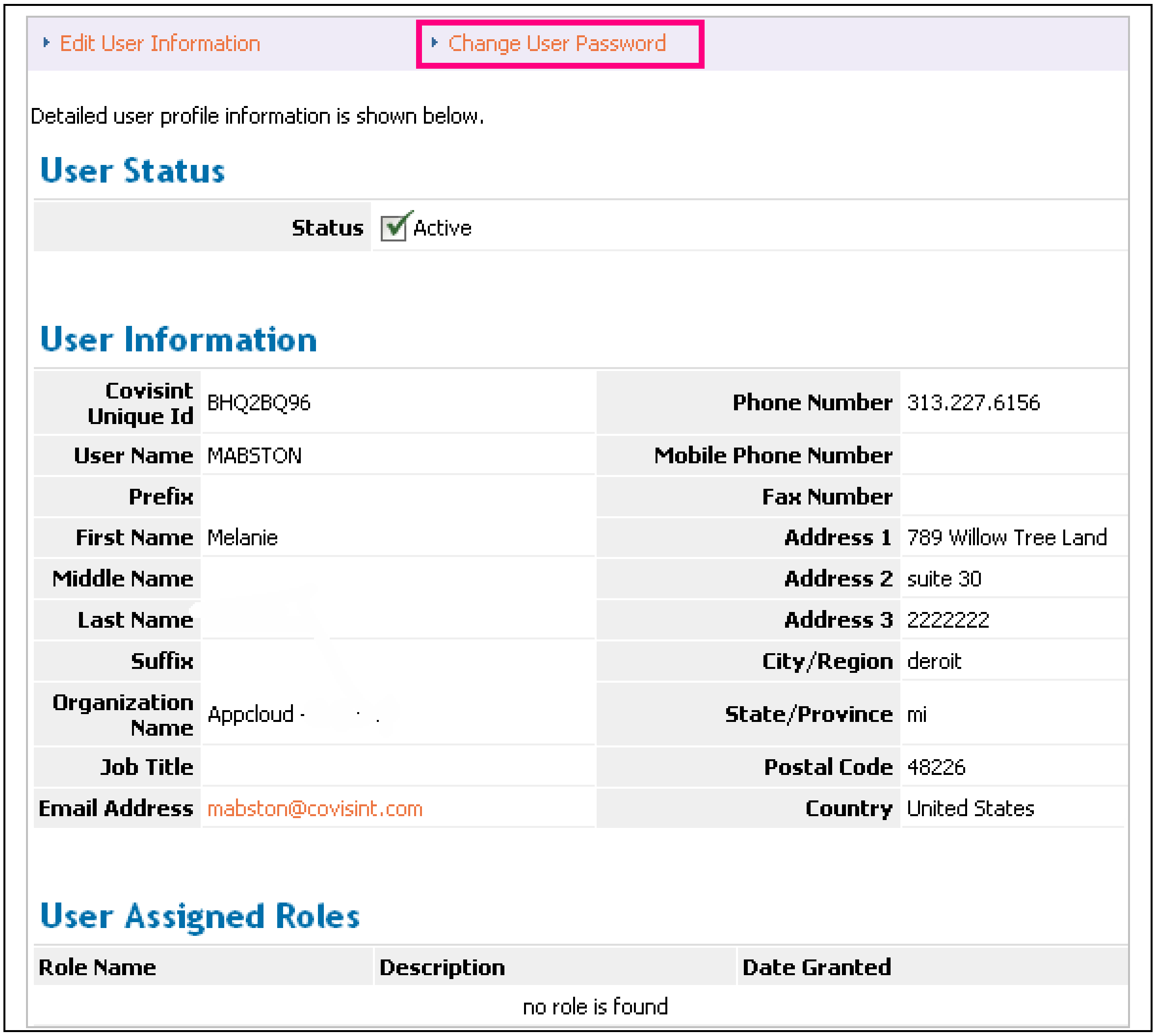
1. Sign-on to AppCloud™.
2. Click **My Profile.** The View User Profile screen is displayed.

User Home Screen:



3. Click **Change User Password.** The Change Your Password screen is displayed.

Change Password Link



Detailed user profile information is shown below.

User Status

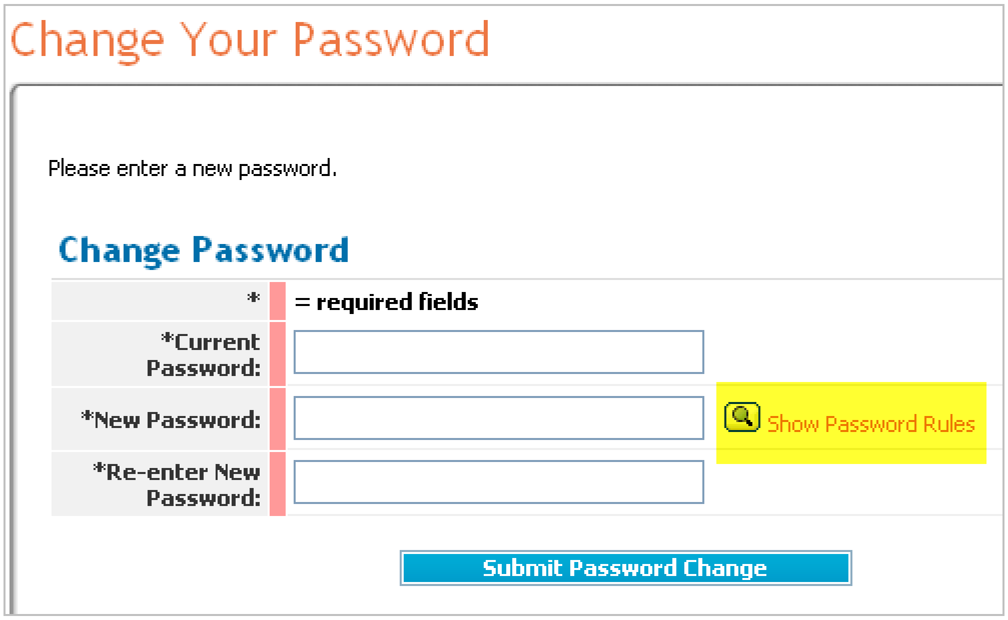
Status	☑ Active

User Information

Covisint Unique Id	BHQ2BQ96	Phone Number	313.227.6156
User Name	MABSTON	Mobile Phone Number	
Prefix		Fax Number	
First Name	Melanie	Address 1	789 Willow Tree Land
Middle Name		Address 2	suite 30
Last Name		Address 3	2222222
Suffix		City/Region	deroit
Organization Name	Appcloud -	State/Province	mi
Job Title		Postal Code	48226
Email Address	mabston@covisint.com	Country	United States

User Assigned Roles

Role Name	Description	Date Granted
	no role is found	



Change Your Password

Please enter a new password.

Change Password

*	= required fields	
*Current Password:		
*New Password:		Show Password Rules
*Re-enter New Password:		

4. Key in your existing password in the Current Password field.
5. Create a new password and key it into the New Password field. Ensure the password conforms to the ***rules.***
6. Key in the password again in the Re-enter New Password field.
7. Click **Submit Password Change.**

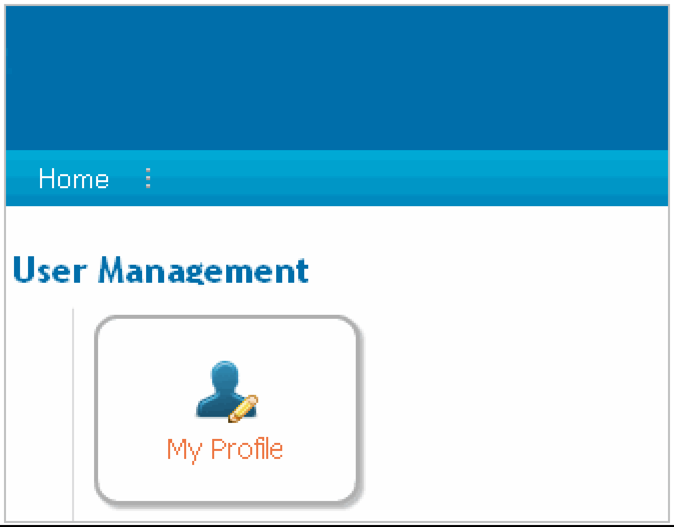
RESULT:

You have successfully changed your password.

Editing My Profile Information

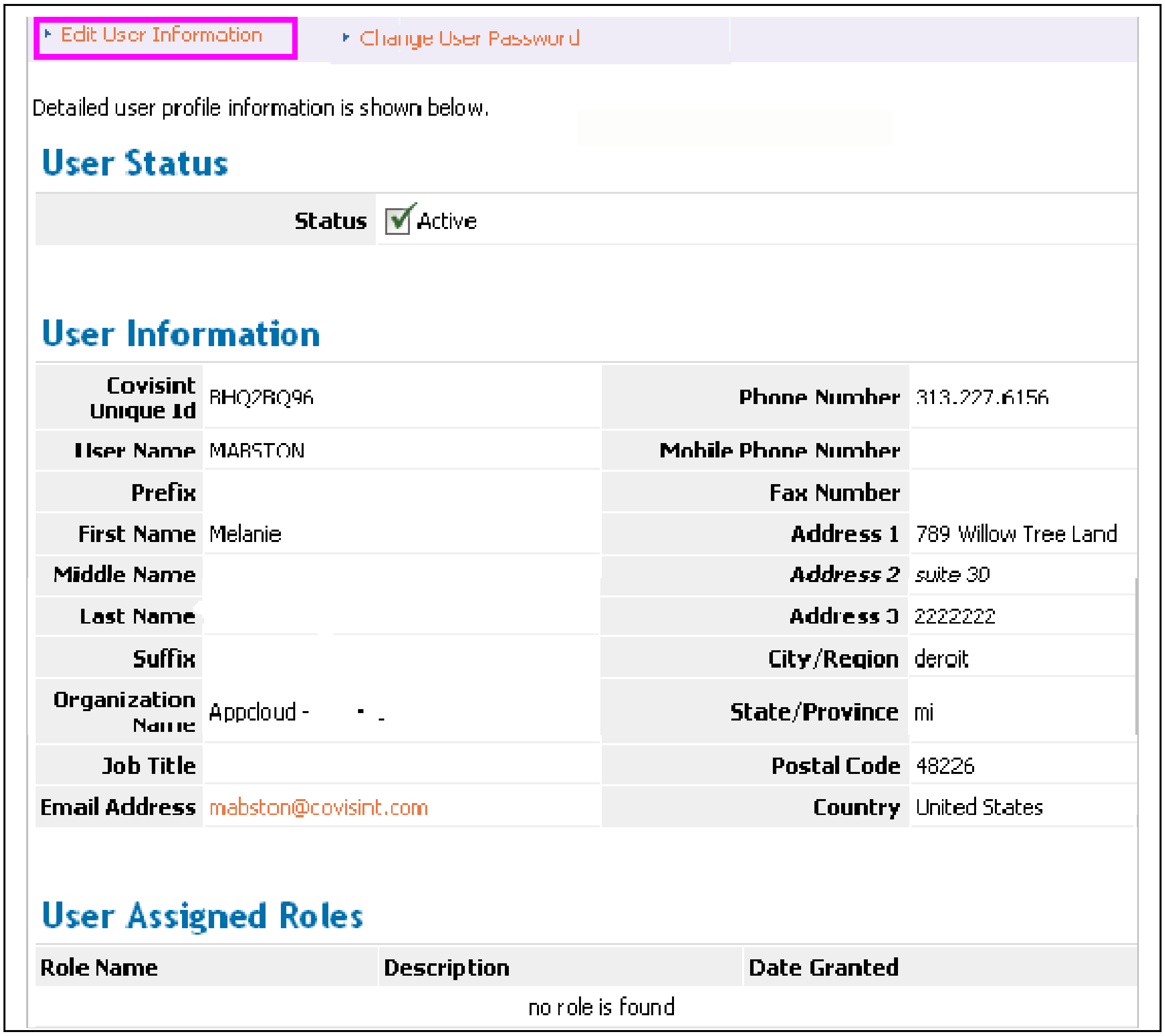
1. Sign-on to AppCloud™.
2. Click **My Profile.** The View User Profile screen is displayed.

User Home Screen:



3. Click **Edit User Information.** The Edit Screen is displayed.

Edit User Information Link



Detailed user profile information is shown below.

User Status

Status	☑ Active

User Information

Covisint Unique Id	RHQ2RQ96	Phone Number	313.227.6156
User Name	MARSTON	Mobile Phone Number	
Prefix		Fax Number	
First Name	Melanie	Address 1	789 Willow Tree Land
Middle Name		Address 2	*suite 30*
Last Name		Address 3	2222222
Suffix		City/Region	deroit
Organization Name	Appcloud - · _	State/Province	mi
Job Title		Postal Code	48226
Email Address	mabston@covisint.com	Country	United States

User Assigned Roles

Role Name	Description	Date Granted
	no role is found	

4. Modify user information as desired.
5. Click **Submit Changes**. The screen refreshes and the changes are saved. The changes are applied to your user profile and will display as such upon next sign-on.

RESULT:

You have successfully edited your user profile information.

SECURITY ADMINISTRATOR TASKS

Working as a Security Administrator

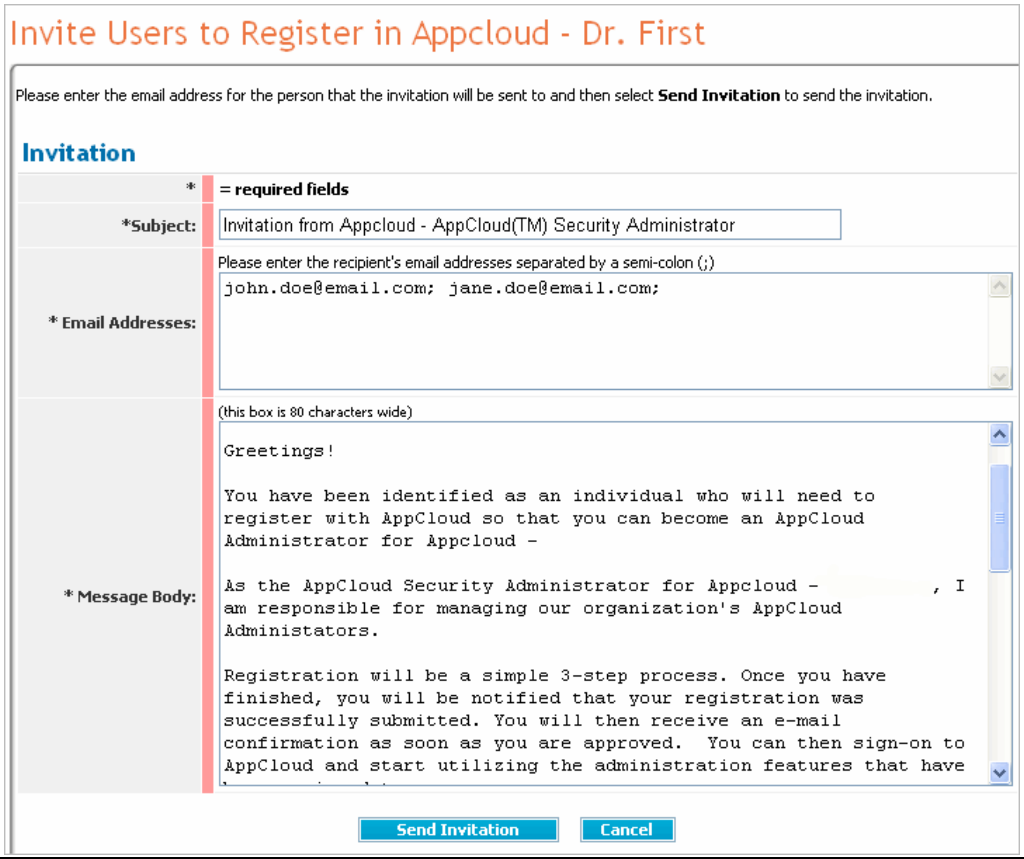
Assumptions:

- The role of Security Administrator is assigned to your user profile
- You are signed-on to AppCloud when performing all Security Administrator tasks
- You have reviewed privileges assigned to the Security Administrator role

Inviting Users to Register for Access

1. From the **User Management screen**, click **Invite User.** The **invitation is displayed**.

Invitation Screen



Invite Users to Register in Appcloud - Dr. First

Please enter the email address for the person that the invitation will be sent to and then select **Send Invitation** to send the invitation.

Invitation

*	= **required fields**
***Subject:**	Invitation from Appcloud - AppCloud(TM) Security Administrator
*** Email Addresses:**	Please enter the recipient's email addresses separated by a semi-colon (;) john.doe@email.com; jane.doe@email.com;
*** Message Body:**	(this box is 80 characters wide)

```
Greetings!

You have been identified as an individual who will need to
register with AppCloud so that you can become an AppCloud
Administrator for Appcloud -

As the AppCloud Security Administrator for Appcloud -           , I
am responsible for managing our organization's AppCloud
Administators.

Registration will be a simple 3-step process. Once you have
finished, you will be notified that your registration was
successfully submitted. You will then receive an e-mail
confirmation as soon as you are approved.  You can then sign-on to
AppCloud and start utilizing the administration features that have
```

2. Key in the email address of each user you wish to invite. Separate email addresses by a semi-colon.

> You may prefer to copy/paste email addresses from a verified list of addresses. Since the users are not yet registered, the system has no record and therefore cannot validate whether you have keyed in the email address correctly. If you mistype an email address, the user will not receive the invitation.

3. Scroll to the bottom of the screen, and click **Send Invitation**. The screen refreshes and a message is displayed confirming that the invitation has been sent.

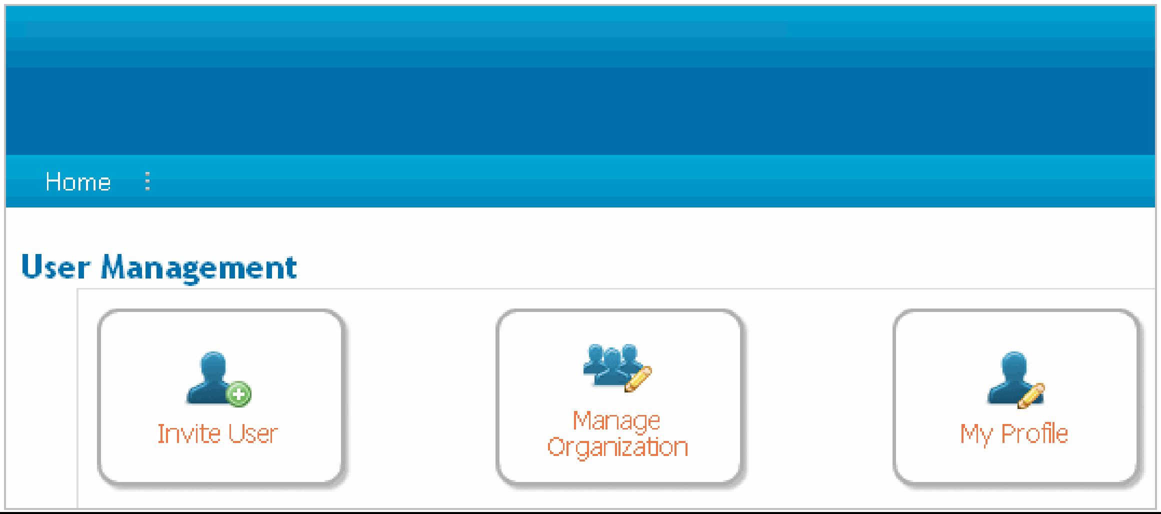
RESULT:

You have successfully invited users to register for access.

Viewing a User's Profile

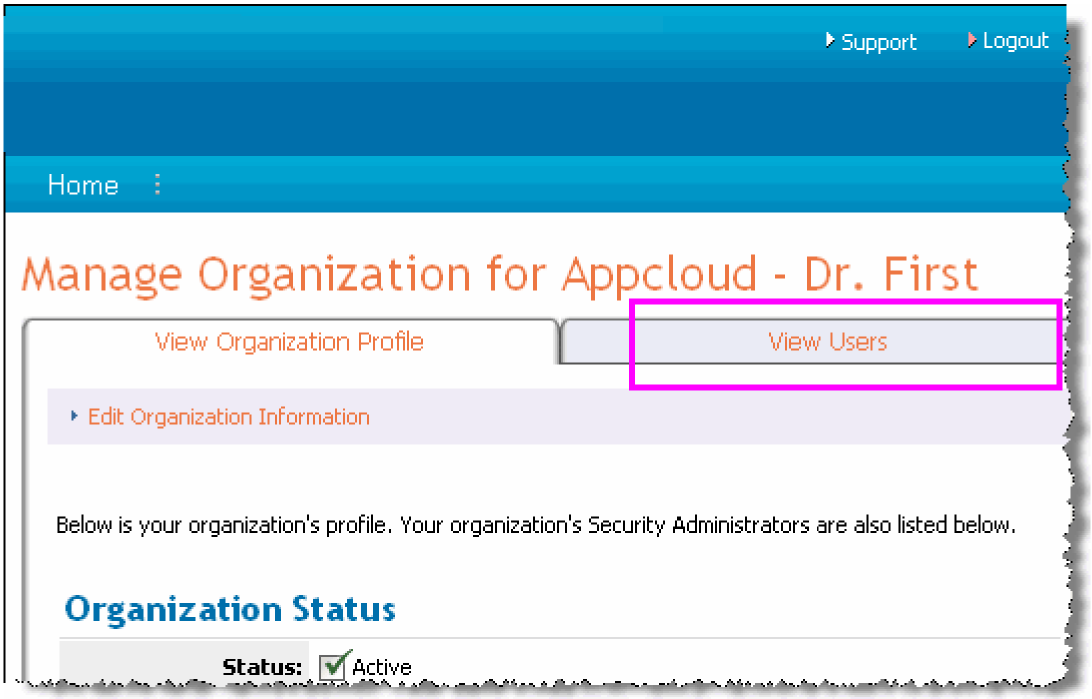
1. From the **User Management screen**, click **Manage Organization.**

User Management Screen



2. Click **View Users.**

View Users Link


Support
Logout
Home
Manage Organization for Appcloud - Dr. First
View Organization Profile
View Users
Edit Organization Information

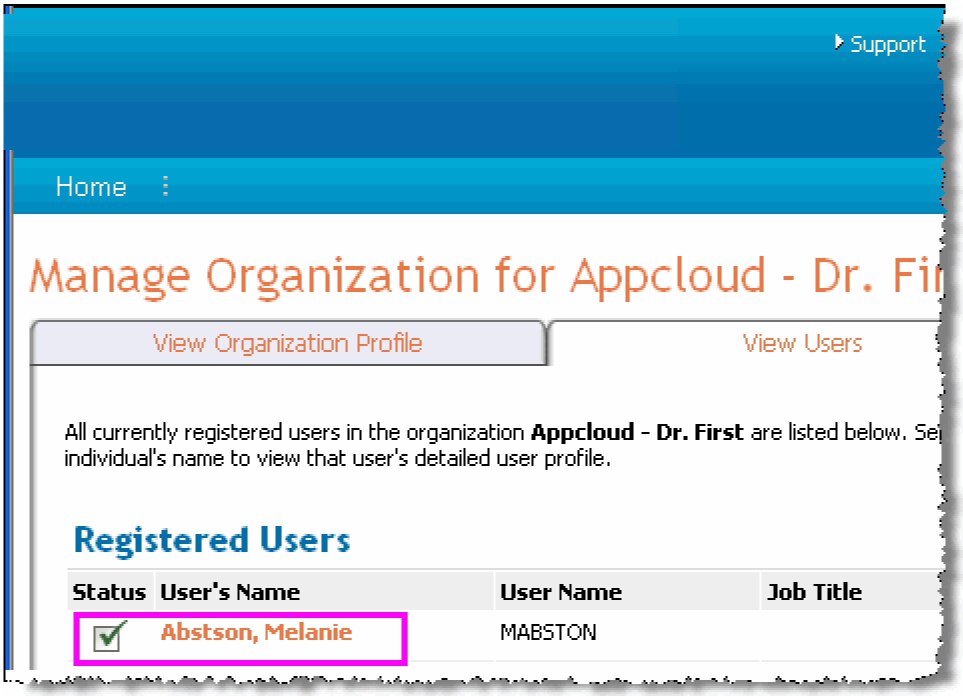
Below is your organization's profile. Your organization's Security Administrators are also listed below.

Organization Status

Status: ☑ Active

3. Click on the **name of the user** for whom you wish to view the profile. The User's Profile is displayed.

View Users Screen

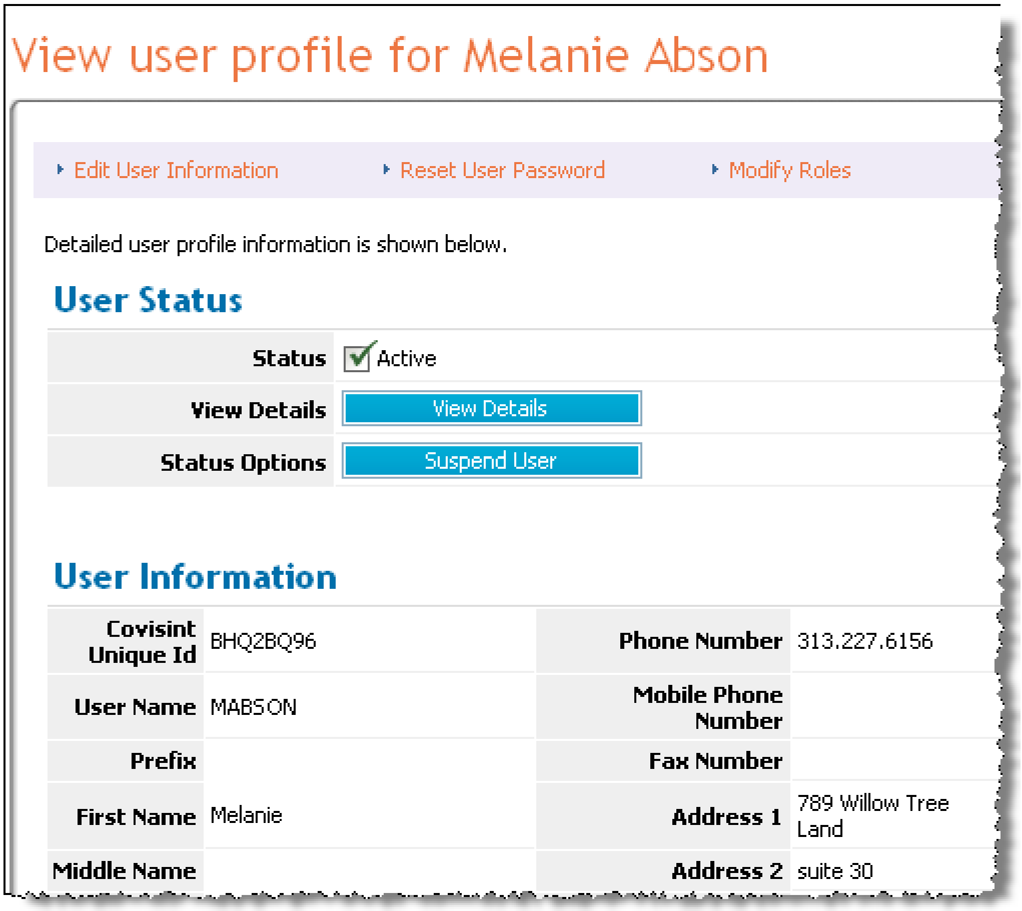


Manage Organization for Appcloud - Dr. Fi

All currently registered users in the organization **Appcloud - Dr. First** are listed below. Se individual's name to view that user's detailed user profile.

Registered Users

Status	User's Name	User Name	Job Title
☑	Abstson, Melanie	MABSTON	



View user profile for Melanie Abson

Detailed user profile information is shown below.

User Status

Status	☑ Active
View Details	View Details
Status Options	Suspend User

User Information

Covisint Unique Id	BHQ2BQ96	Phone Number	313.227.6156
User Name	MABSON	Mobile Phone Number	
Prefix		Fax Number	
First Name	Melanie	Address 1	789 Willow Tree Land
Middle Name		Address 2	suite 30

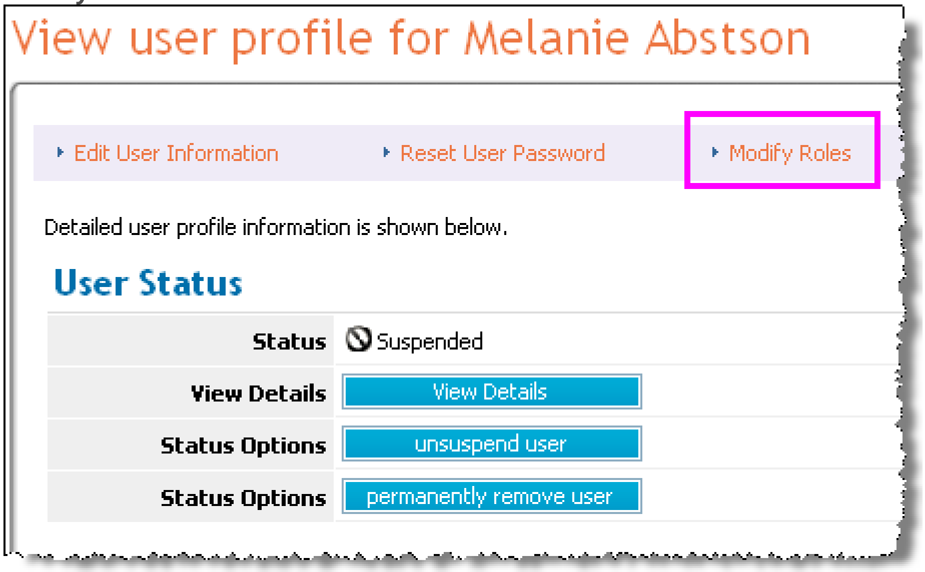
RESULT:

You have successfully viewed a user's profile.

Modifying User Roles

1. Navigate to the Profile of the user for whom you wish to modify roles.
2. Click **Modify Roles**. The Modify User Roles screen is displayed.

Modify Roles Link

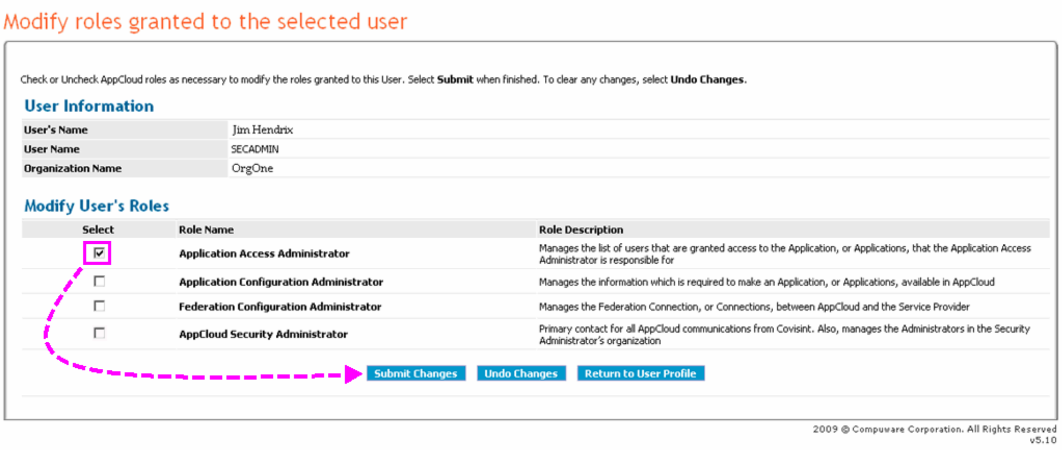


View user profile for Melanie Abstson

Detailed user profile information is shown below.

User Status

Status	Suspended
View Details	View Details
Status Options	unsuspend user
Status Options	permanently remove user



Modify roles granted to the selected user

Check or Uncheck AppCloud roles as necessary to modify the roles granted to this User. Select **Submit** when finished. To clear any changes, select **Undo Changes**.

User Information

User's Name	Jim Hendrix
User Name	SECADMIN
Organization Name	OrgOne

Modify User's Roles

Select	Role Name	Role Description
☑	Application Access Administrator	Manages the list of users that are granted access to the Application, or Applications, that the Application Access Administrator is responsible for
□	Application Configuration Administrator	Manages the information which is required to make an Application, or Applications, available in AppCloud
□	Federation Configuration Administrator	Manages the Federation Connection, or Connections, between AppCloud and the Service Provider
□	AppCloud Security Administrator	Primary contact for all AppCloud communications from Covisint. Also, manages the Administrators in the Security Administrator's organization

2009 © Compuware Corporation. All Rights Reserved
v5.10

3. Enable the checkbox of each role you wish to apply to this user.
4. Disable the checkbox of each role you wish to remove from this user.
5. Click **Submit Changes.** The screen refreshes, and the role change is applied to the user's account. The user must sign-off and back on for the change to take effect.

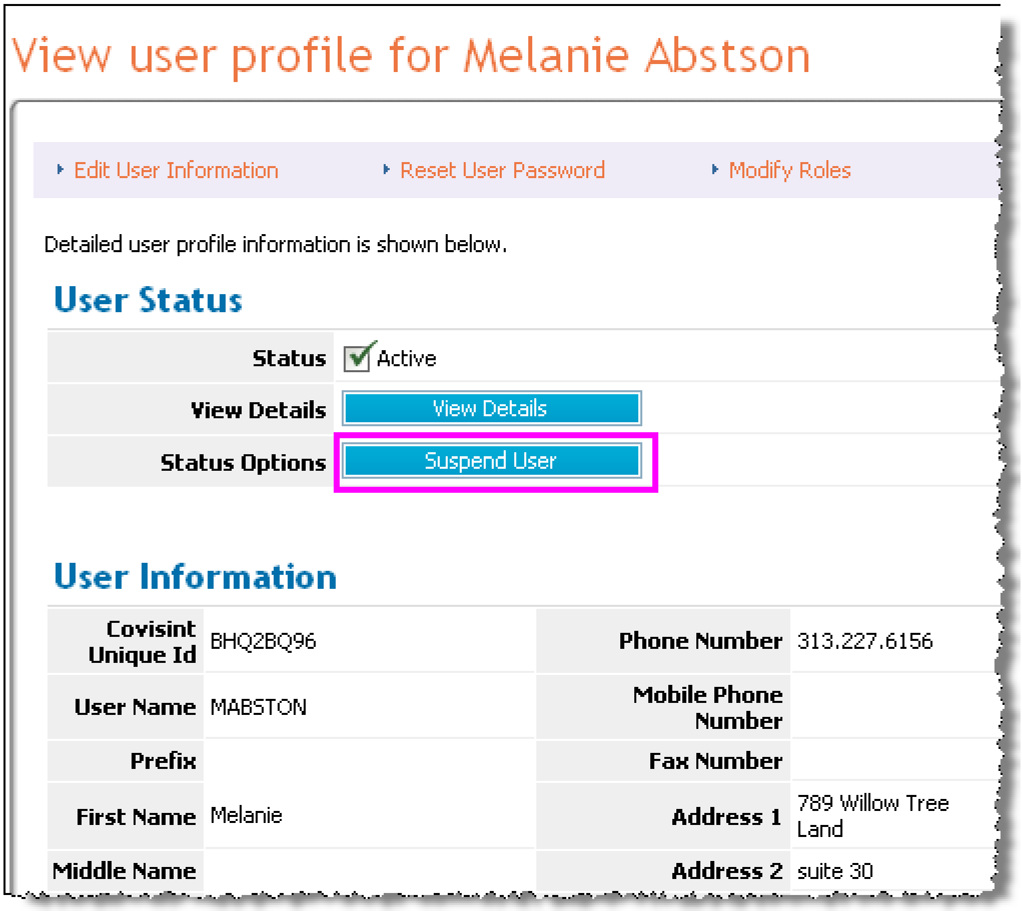
RESULT:

You have successfully modified a user role.

Suspending a User Account

Suspending a user account locks the user's account, preventing the user from being able to sign-on to AppCloud™. The account remains locked until you unsuspend it.

1. Navigate to the User Profile of the account you wish to suspend.



View user profile for Melanie Abstson

Detailed user profile information is shown below.

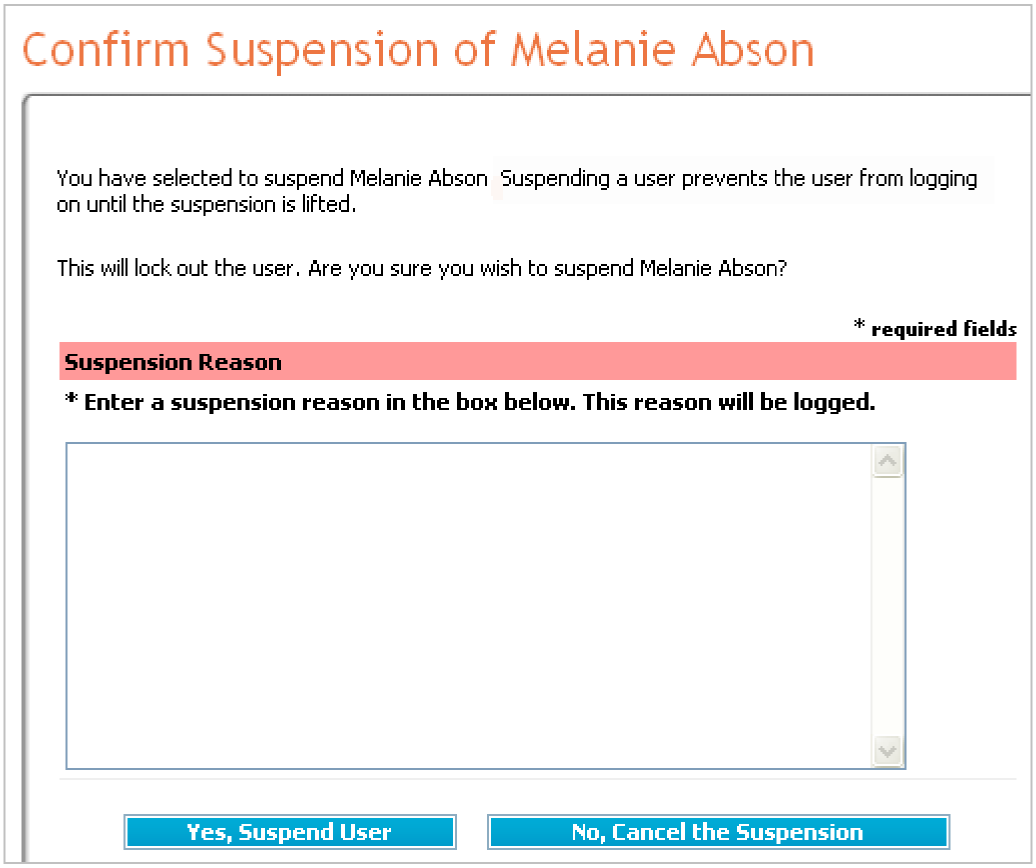
User Status

Status	☑ Active
View Details	View Details
Status Options	Suspend User

User Information

Covisint Unique Id	BHQ2BQ96	**Phone Number**	313.227.6156
User Name	MABSTON	**Mobile Phone Number**	
Prefix		**Fax Number**	
First Name	Melanie	**Address 1**	789 Willow Tree Land
Middle Name		**Address 2**	suite 30

2. Click **Suspend User.**



Confirm Suspension of Melanie Abson

You have selected to suspend Melanie Abson Suspending a user prevents the user from logging on until the suspension is lifted.

This will lock out the user. Are you sure you wish to suspend Melanie Abson?

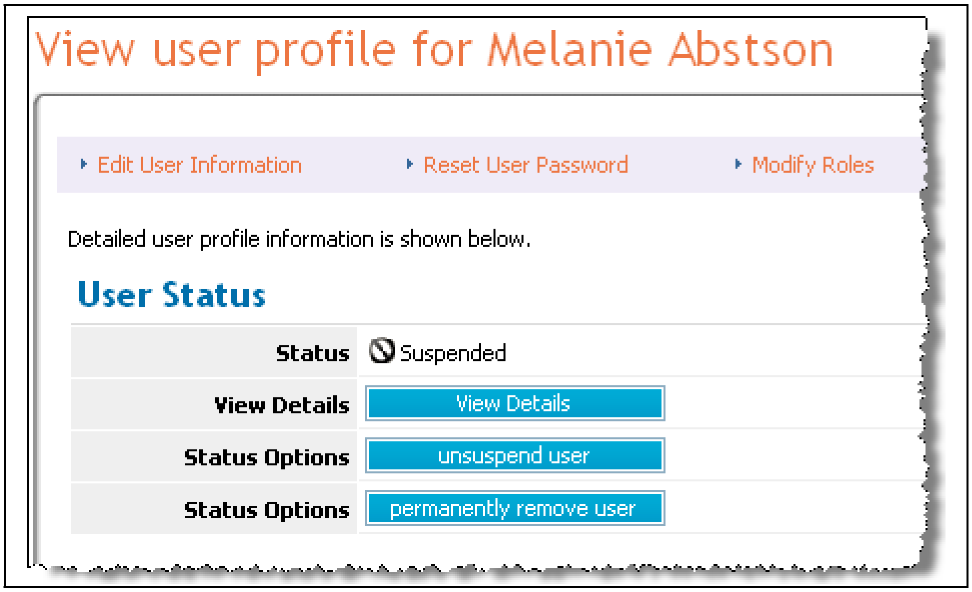
* required fields

Suspension Reason

* Enter a suspension reason in the box below. This reason will be logged.

3. In the open text field, key in the reason for suspension. The information you provide in this field is logged in the user's status history and is viewable by other Security Administrators in your organization
4. Click **Yes, Suspend User.** The screen refreshes, and a message confirming the suspension is displayed.
5. Click **back to user profile.** The **user's status is suspended.**

User Status Screen



View user profile for Melanie Abstson

Detailed user profile information is shown below.

User Status

Status	Suspended
View Details	View Details
Status Options	unsuspend user
Status Options	permanently remove user

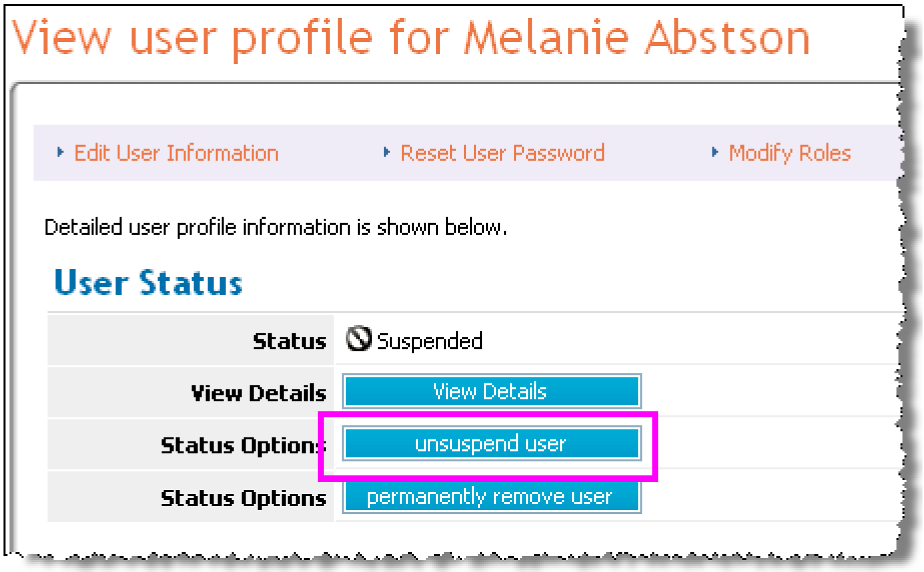
RESULT:

You have successfully suspended a user.

Unsuspending a User Account

Unsuspending unlocks the user's account. The user will be able to sign-on to AppCloud™ once unsuspending is complete and the account is again active.

1. Navigate to the User Profile of the account you wish to unsuspend.



View user profile for Melanie Abstson

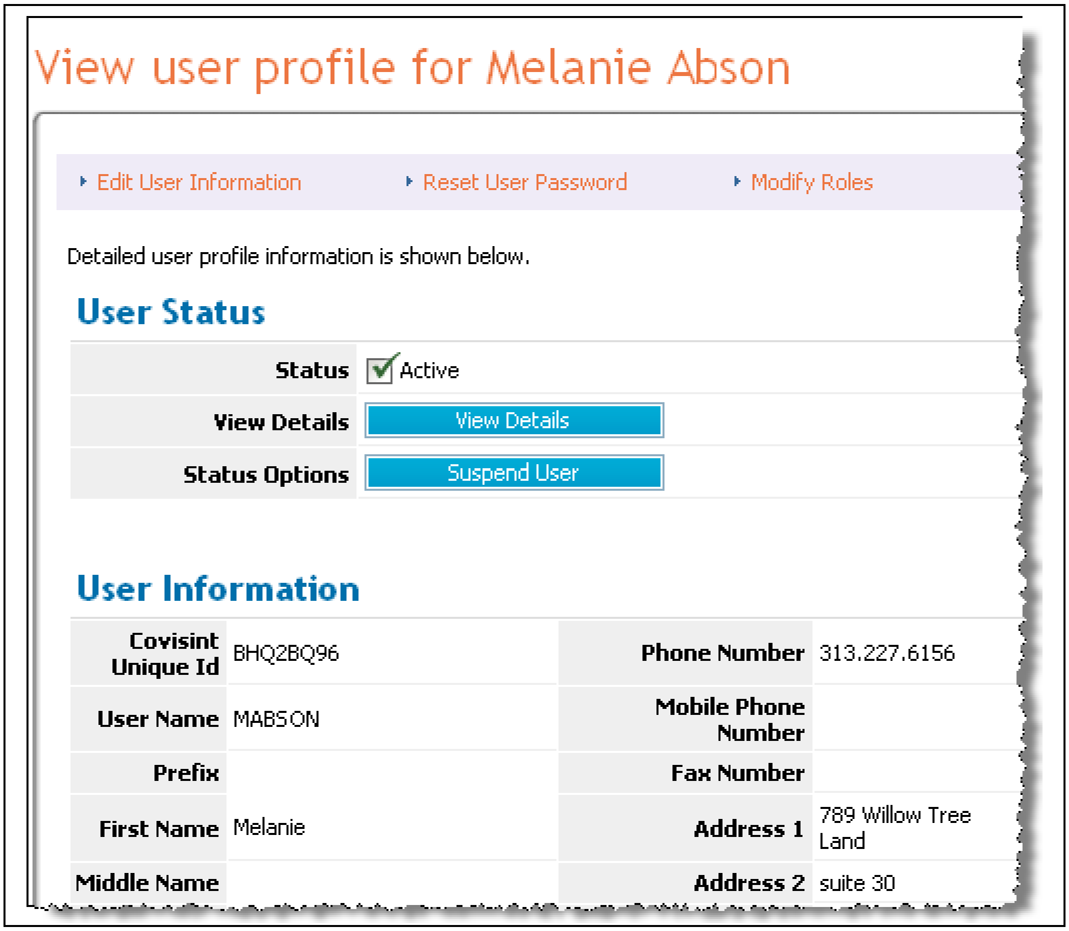
Detailed user profile information is shown below.

User Status

Status	Suspended
View Details	View Details
Status Options	unsuspend user
Status Options	permanently remove user

2. Click **unsuspend user**.
3. In the open text field, key in the reason for unsuspending the user account. The information you provide in this field is logged in the user's status history and is viewable by other Security Administrators in your organization
4. Click **Yes, Unspend User.** The screen refreshes, and a message confirming the unsuspension is displayed.
5. Click **back to user profile.** The **user's status is active.**

User Status Screen



View user profile for Melanie Abson

Detailed user profile information is shown below.

User Status

Status	☑ Active
View Details	View Details
Status Options	Suspend User

User Information

Covisint Unique Id	BHQ2BQ96	Phone Number	313.227.6156
User Name	MABSON	Mobile Phone Number	
Prefix		Fax Number	
First Name	Melanie	Address 1	789 Willow Tree Land
Middle Name		Address 2	suite 30

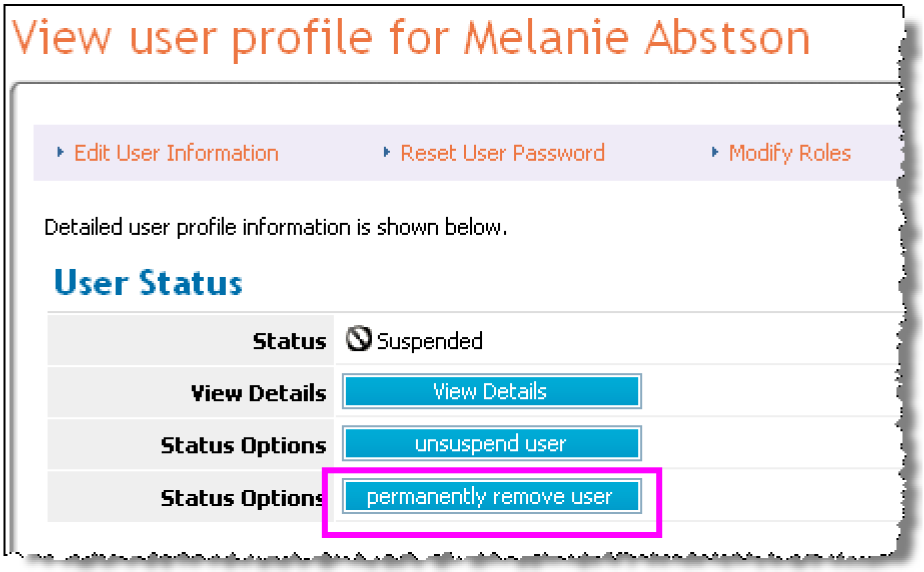
RESULT:

You have successfully unsuspended a user's account.

Removing a User Account

Terminating a user account permanently removes the profile from the system. The user will not be able to sign-on to AppCloud™. Termination cannot be undone.

1. Navigate to the User Profile of the account you wish to terminate. The user's account must be suspended before the 'permanently remove user' option will display.



View user profile for Melanie Abstson

Detailed user profile information is shown below.

User Status

Status	Suspended
View Details	View Details
Status Options	unsuspend user
Status Options	permanently remove user

2. Click **permanently remove user**.
3. In the open text field, key in the reason for permanently removing the user from the system. The information you provide in this field is logged in the user's status history and is viewable by other Security Administrators in your organization
4. Click **Yes, Permanently Remove User.** The screen refreshes, and a message confirming the removal is displayed.

RESULT:

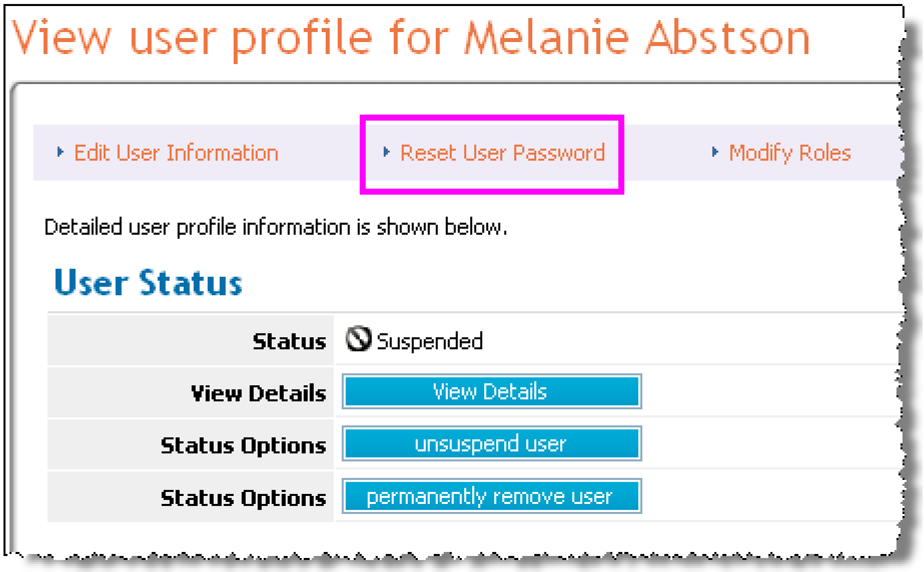
You have successfully removed a user account from the system.

Resetting a User Password

While users are able to reset their own passwords, the Security Administrator is also able to reset a User's Password on behalf of the user.

1. Navigate to the Profile of the user for whom you wish to reset the password.
2. Click **Reset User Password.** The Reset User Password screen is displayed.

Reset User Password Link

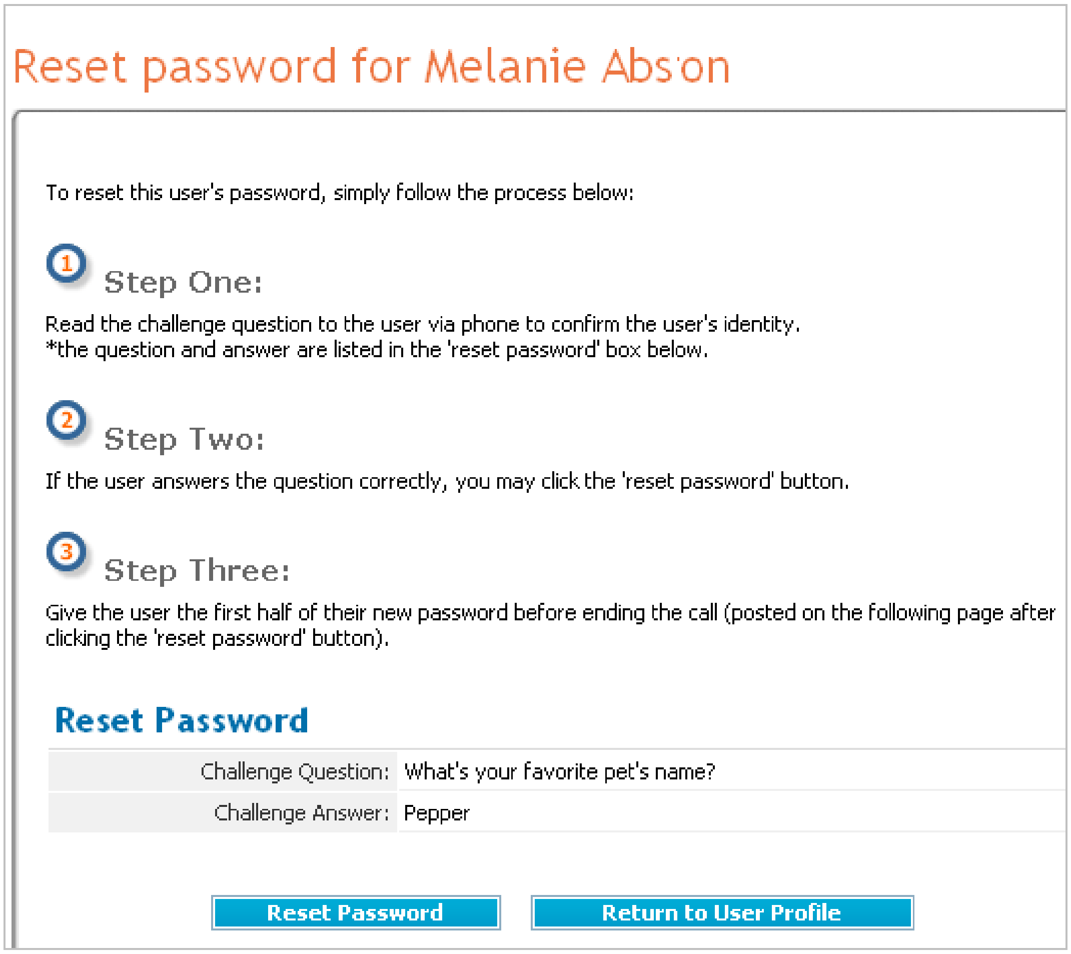


View user profile for Melanie Abstson

Detailed user profile information is shown below.

User Status

Status	Suspended
View Details	View Details
Status Options	unsuspend user
Status Options	permanently remove user



Reset password for Melanie Abs'on

To reset this user's password, simply follow the process below:

1 Step One:

Read the challenge question to the user via phone to confirm the user's identity.
*the question and answer are listed in the 'reset password' box below.

2 Step Two:

If the user answers the question correctly, you may click the 'reset password' button.

3 Step Three:

Give the user the first half of their new password before ending the call (posted on the following page after clicking the 'reset password' button).

Reset Password

Challenge Question:	What's your favorite pet's name?
Challenge Answer:	Pepper

3. Confirm the user's identity by reading the challenge question to the user, or by whatever other means per your organization's business rules regarding the security policy requires.
4. If the user provides the correct answer, click **Reset Password.** The screen refreshes, and the first four digits of the eight digit temporary password is displayed.
5. Read the first for digits to the user.
6. Ask the user to write these numbers down on a piece of paper, as they will not be seen again by any user.
7. Instruct the user to retrieve the remaining four digits of the temporary password from the email account that the user provided during registration.
8. Instruct the user to attempt to sign-on to the system using this temporary eight-digit password, and to follow the remaining prompts on the screen.
9. Click **Return To User Profile.**

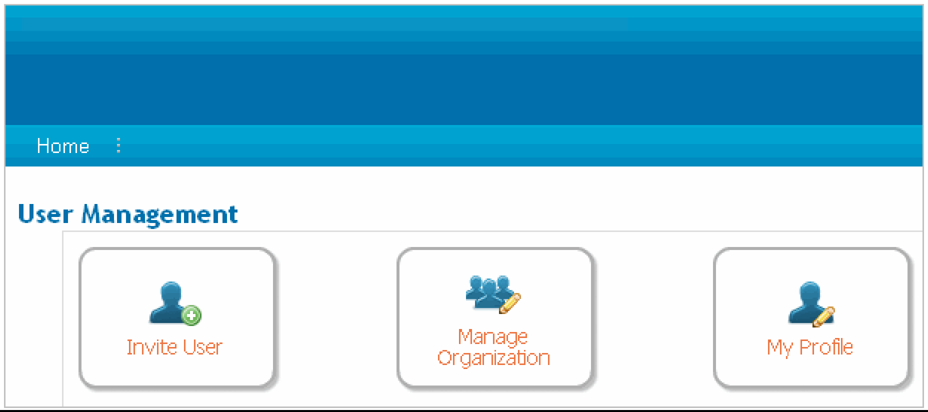
RESULT:

You have successfully reset a user's password.

Viewing Users in My Organization

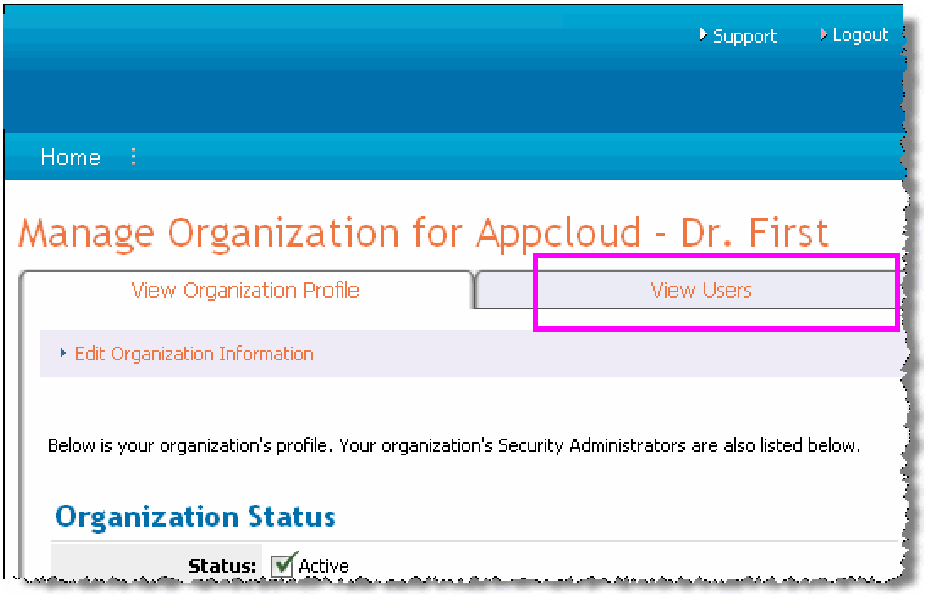
1. From the **User Management screen**, click **Manage Organization.**

User Management Screen



2. Click **View Users.** A list of all users in your organization is displayed.

View Users Link


Support
Logout
Home
Manage Organization for Appcloud - Dr. First
View Organization Profile
View Users
Edit Organization Information

Below is your organization's profile. Your organization's Security Administrators are also listed below.

Organization Status

Status: ☑ Active

RESULT:

You have successfully viewed a list of users in your organization. Next, you may wish to:

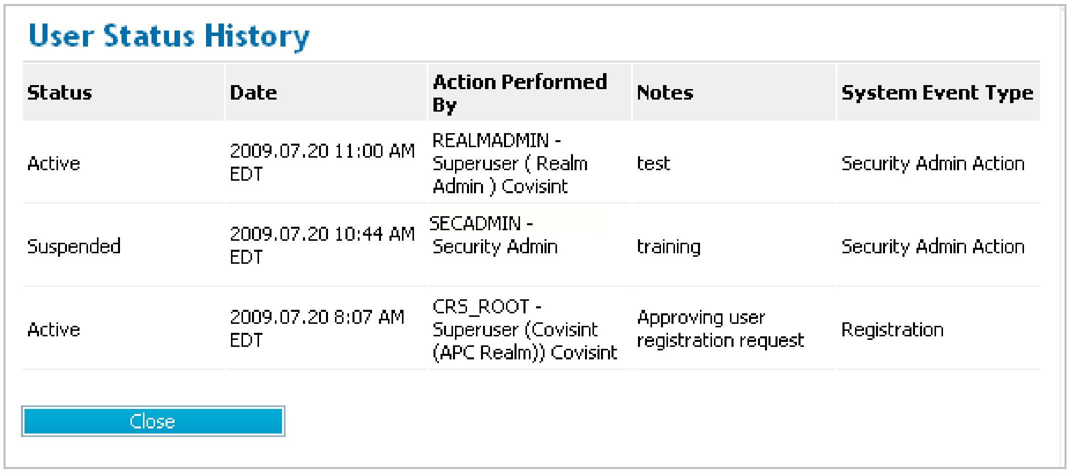
- click on a user's name to view the user's profile
- update the user's information
- perform other user management tasks of the Security Administrator

Viewing a User's Status History

Changes to a user's status are logged in the system and available as history of the account. The User Status History displays the following information each time a change is applied to a user's account:

- type of status change
- date and time stamp of the change
- name of the Administrator that applied the change to the user's status
- the reason (provided by the Administrator) that the change was made

1. Navigate to the User Profile of the account for which you wish to view status details.
2. Click **View Details**. The User Status History is displayed.



User Status History

Status	Date	Action Performed By	Notes	System Event Type
Active	2009.07.20 11:00 AM EDT	REALMADMIN - Superuser (Realm Admin) Covisint	test	Security Admin Action
Suspended	2009.07.20 10:44 AM EDT	SECADMIN - Security Admin	training	Security Admin Action
Active	2009.07.20 8:07 AM EDT	CRS_ROOT - Superuser (Covisint (APC Realm)) Covisint	Approving user registration request	Registration

3. Review information as desired, then click **Close**.

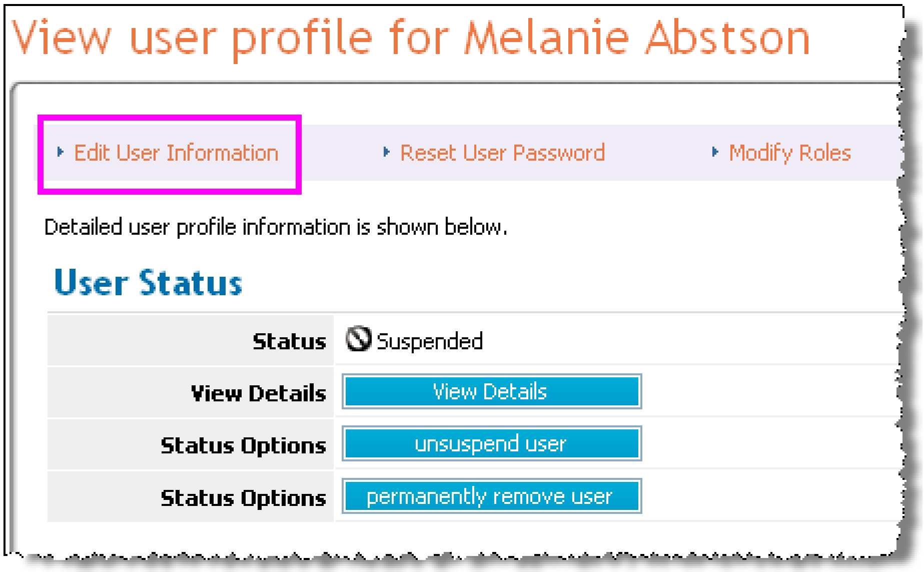
RESULT:

You have successfully viewed a user's status history.

Updating a User's Profile Information

1. Navigate to the Profile of the user for whom you wish to modify profile information.
2. Click **Edit User Information.** The Edit Screen is displayed.

Edit User Information Link



View user profile for Melanie Abstson

Detailed user profile information is shown below.

User Status

Status	Suspended
View Details	View Details
Status Options	unsuspend user
Status Options	permanently remove user

3. Modify user information as desired.
4. Click **Submit Changes**. The screen refreshes and the changes are saved. The changes are applied to the user profile and will display as such the next time the user signs-on to AppCloud™.

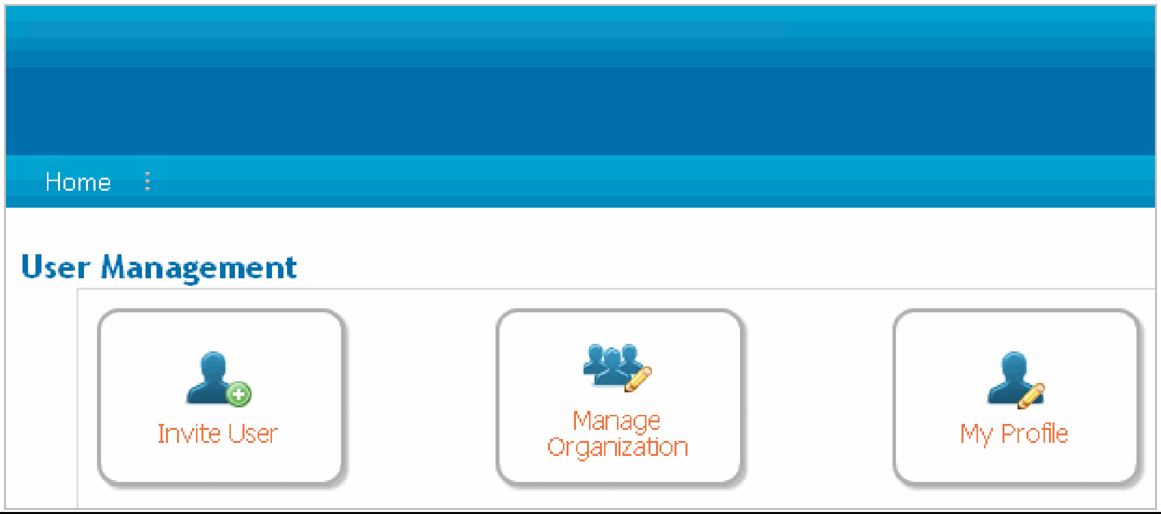
RESULT:

You have successfully updated a user's profile information.

Updating Organization Information

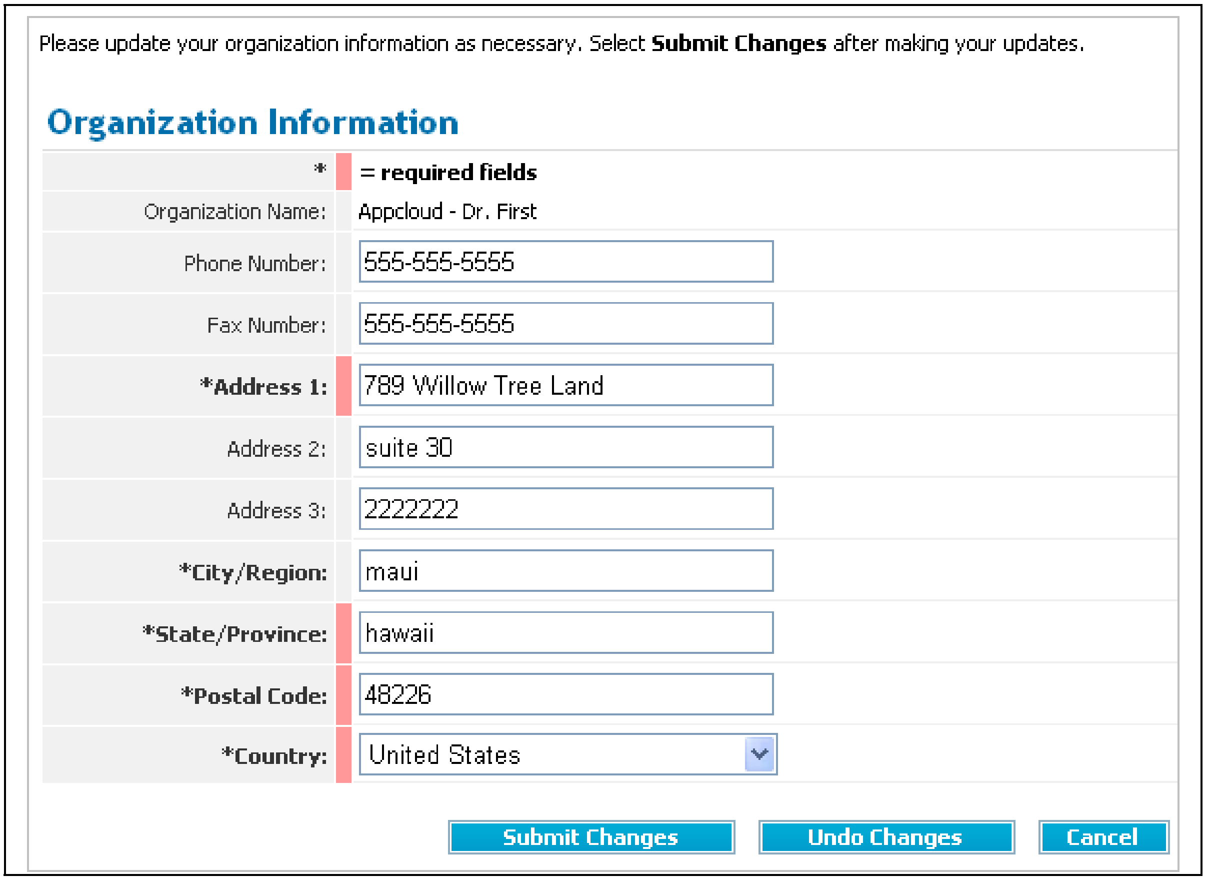
1. From the **User Management screen**, click **Manage Organization.** The Manage Organization Screen is displayed.

User Management Screen



2. Click **Edit Organization Information.** The **Edit Organization Screen** is displayed.

Edit Organization Screen



Please update your organization information as necessary. Select **Submit Changes** after making your updates.

Organization Information

*	**= required fields**
Organization Name:	Appcloud - Dr. First
Phone Number:	555-555-5555
Fax Number:	555-555-5555
***Address 1:**	789 Willow Tree Land
Address 2:	suite 30
Address 3:	2222222
***City/Region:**	maui
***State/Province:**	hawaii
***Postal Code:**	48226
***Country:**	United States

3. Edit information as required, then click **Submit Changes.**
4. Click **OK** to confirm. The screen refreshes, and a message is displayed confirming your updated organization.

RESULT:

You have successfully updated organization information.

FEDERATION CONFIGURATION ADMINISTRATOR TASKS

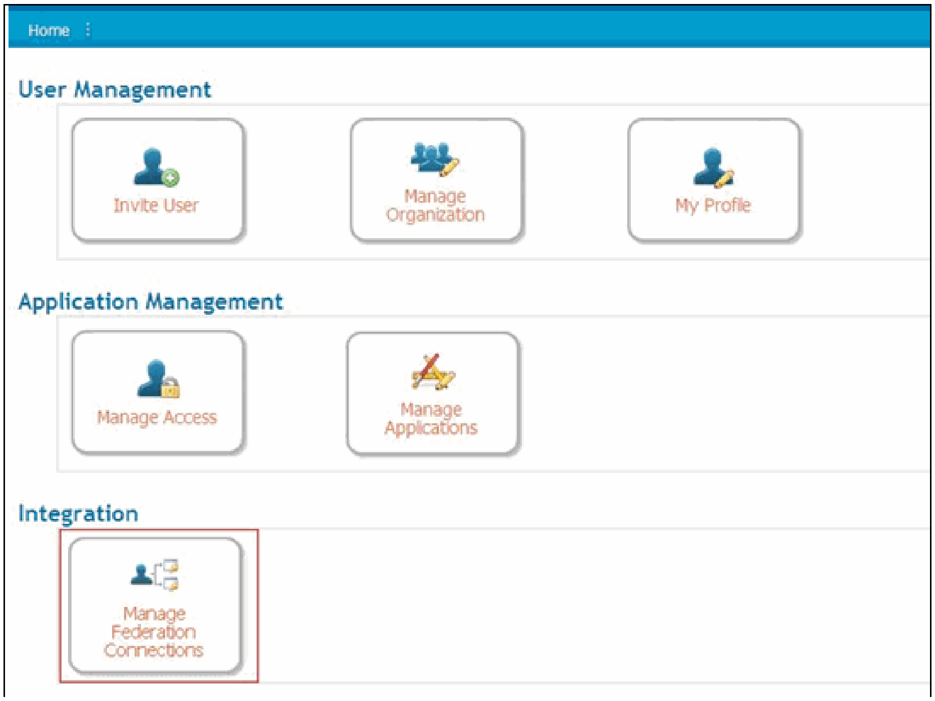
Working as a Federation Configuration Administrator

Assumptions:

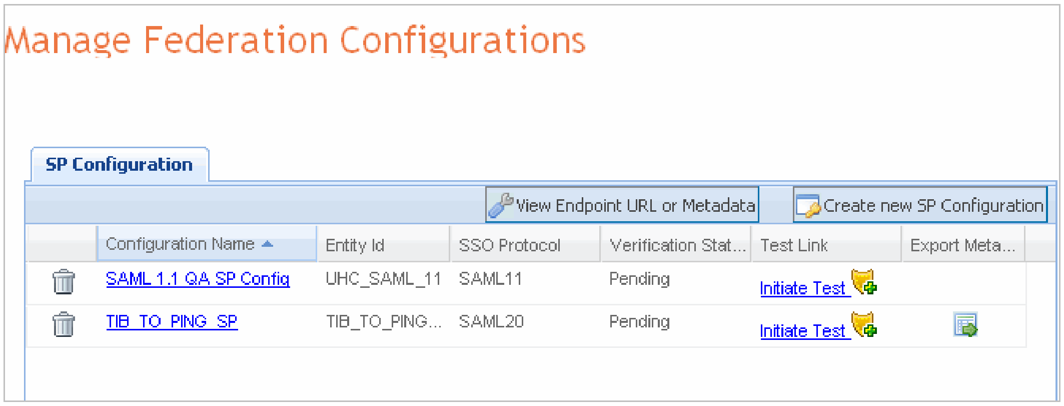
- The role of Federation Configuration Administrator is assigned to your user profile
- You are signed-on to AppCloud when performing all Federation Configuration Administrator tasks
- You have reviewed privileges assigned to the Federation Configuration Administrator role

Viewing Existing SP Federation Connections

1. Sign-on to AppCloud.



2. Click **Manage Federation Connections.** The Manage Federation Configurations screen displays a list of all existing configurations, along with the verification status of each.


Manage Federation Configurations
SP Configuration
View Endpoint URL or Metadata
Create new SP Configuration

	Configuration Name ▲	Entity Id	SSO Protocol	Verification Stat...	Test Link	Export Meta...
🗑	SAML 1.1 QA SP Config	UHC_SAML_11	SAML11	Pending	Initiate Test	
🗑	TIB_TO_PING_SP	TIB_TO_PING...	SAML20	Pending	Initiate Test	

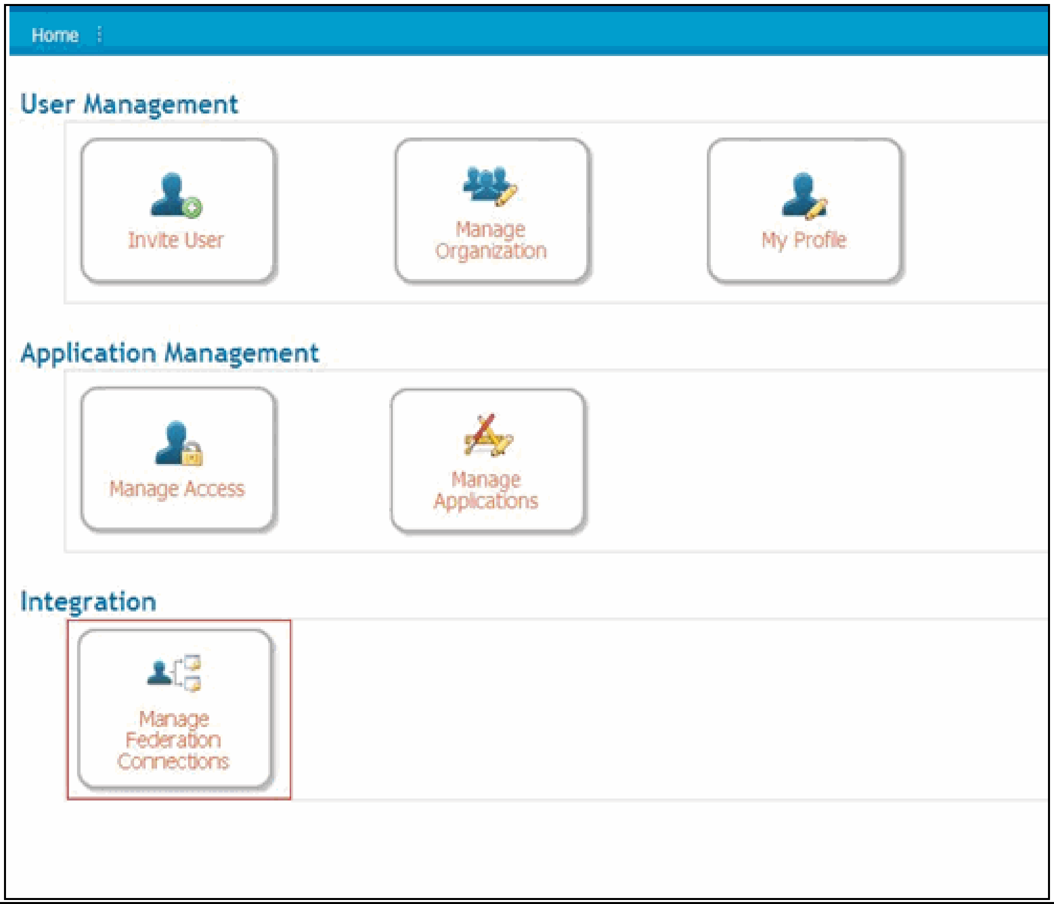
RESULT:

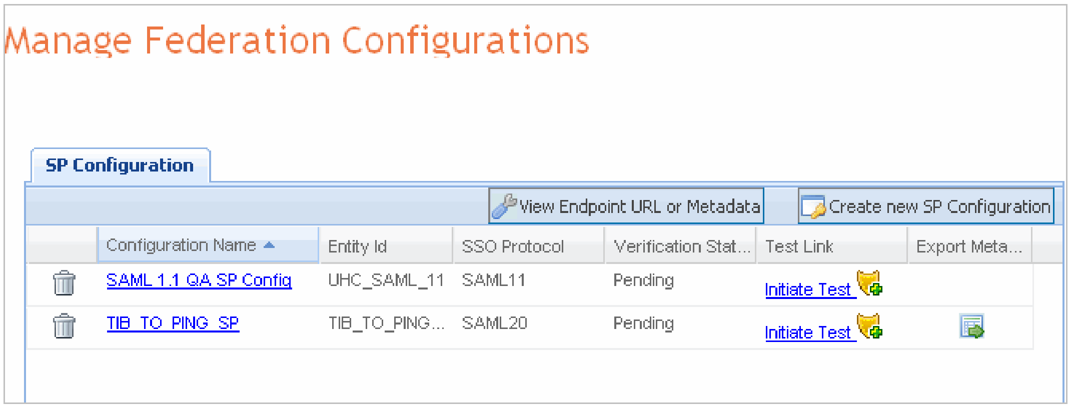
You have successfully viewed existing ***SP*** Federation Configurations.

Creating a Federation Connection

1. Click **Manage Federation Connections.** The Manage Federation Configurations screen displays a list of all existing configurations, along with the verification status of each.

Manage Federation Connections Link

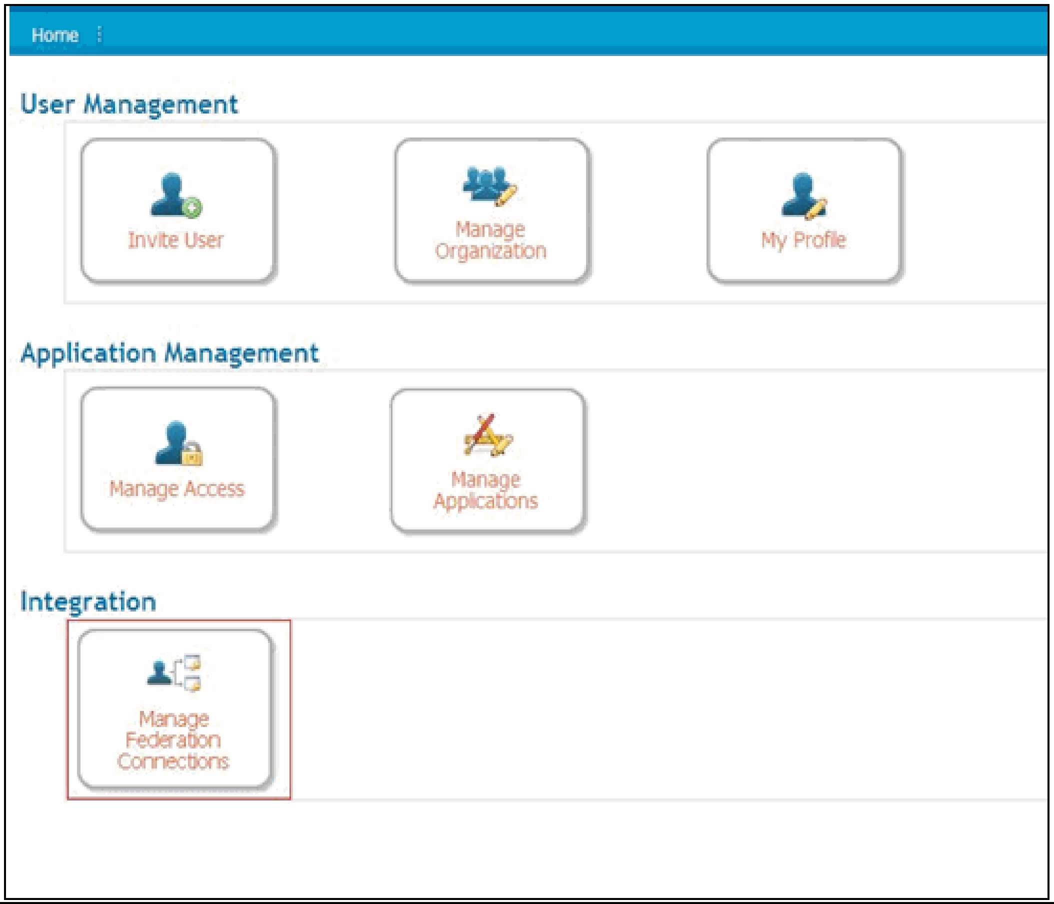



Manage Federation Configurations
SP Configuration
View Endpoint URL or Metadata
Create new SP Configuration

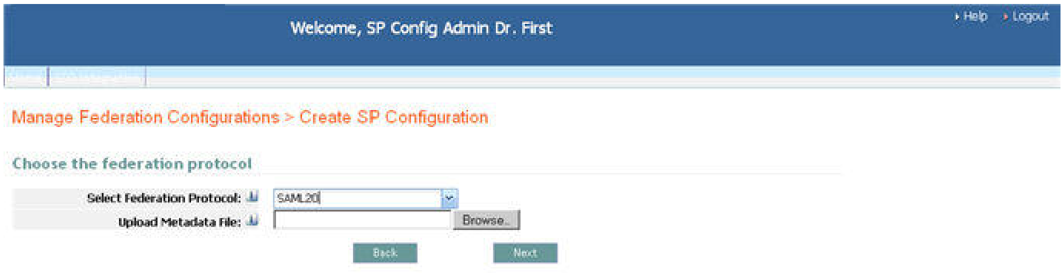
	Configuration Name ▲	Entity Id	SSO Protocol	Verification Stat...	Test Link	Export Meta...
🗑	SAML 1.1 QA SP Config	UHC_SAML_11	SAML11	Pending	Initiate Test	
🗑	TIB_TO_PING_SP	TIB_TO_PING...	SAML20	Pending	Initiate Test	

2. View **EndPoint URLs or Metadata** to obtain the information required to start the configuration process. A list of supported options is displayed.
3. Download the signature verification certificate and use the Endpoints displayed.
    a. Optionally if the federation solution supports metadata, download the Covisint SSO metadata file.
4. After configuring the federation consumer at the Application Provider's site, click **Manage Federation Connections.** The Manage Federation Configurations screen displays a list of all existing configurations, along with the verification status of each.

Manage SSO Link



5. Click **Create new SP Configuration.**



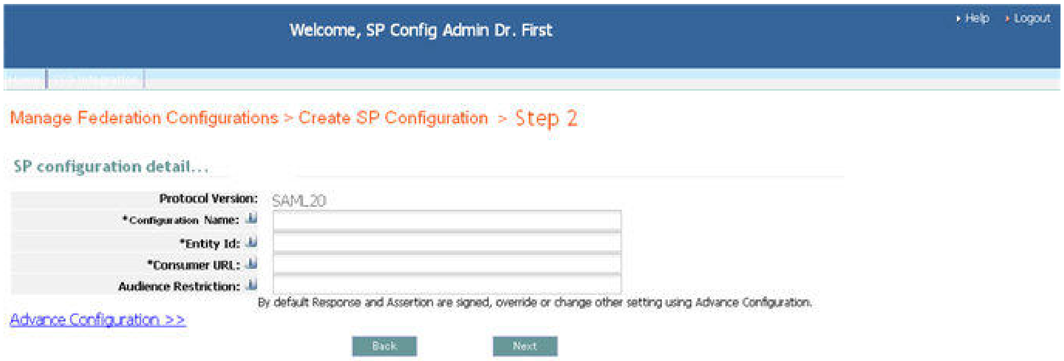
Manage Federation Configurations > Create SP Configuration

Choose the federation protocol

Select Federation Protocol: SAML2.0

Upload Metadata File:

6. Select the Federation Protocol from the drop down menu.
7. Upload the metadata file by clicking **Browse...** and then select the file to upload.
8. Click **Next**. The Step 2 screen is displayed.



Welcome, SP Config Admin Dr. First

Manage Federation Configurations > Create SP Configuration > Step 2

SP configuration detail...

Protocol Version: SAML20
*Configuration Name:
*Entity Id:
*Consumer URL:
Audience Restriction:

By default Response and Assertion are signed, override or change other setting using Advance Configuration.

Advance Configuration >>

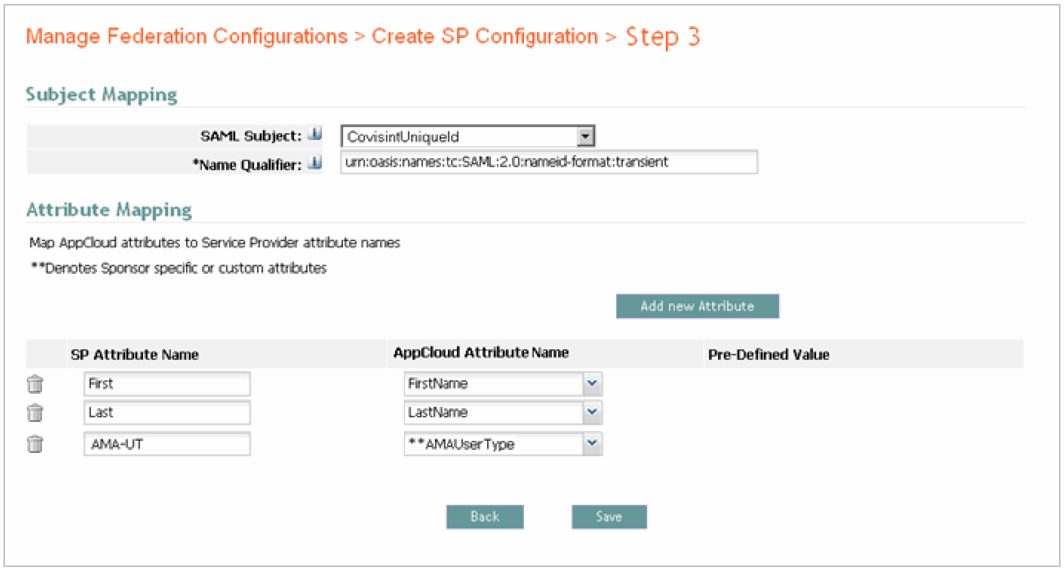
9. Key in the following Basic information as required / desired:

FIELD NAME:	DEFINITION:
Configuration Name	A Service Provider (SP) name that can be easily identified by the end user (this is a “user friendly” name)
Entity ID	The Entity ID is the identifier that uniquely represents every SAML Identity Provider or Service Provider.
Consumer URL	URL that the assertion will be posted to.
Audience Restriction	Used by the SP to limit the scope of which entity should consume the information in the assertion

10. Optionally, key in additional information by clicking **Advance Configuration.**

FIELD NAME:	DEFINITION:
Response Signing Enabled	Integrity of a message between providers is insured by using digital signatures. By enabling response signing, a digital signature is generated for the SAML Response document. Covisint will provide the SP with the Public Key that will be used to verify the Response signature.
Assertion Signing Enabled	Integrity of a message between providers is insured by using digital signatures. By enabling assertion signature signing, the digital signature is generated for the SAML Assertion document. Covisint will provide the SP with the Public Key that will be used to verify the Assertion signature.
Signing Algorithm	Singing algorithm that will be used for signing the SAML Assertions.
Canonical Algorithm	Canonical algorithm that will be used for signing the SAML assertions.

11. Click **Next**. The Step 3 screen is displayed.



Manage Federation Configurations > Create SP Configuration > Step 3

Subject Mapping

SAML Subject: CovisintUniqueId

*Name Qualifier: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Attribute Mapping

Map AppCloud attributes to Service Provider attribute names

**Denotes Sponsor specific or custom attributes

SP Attribute Name	AppCloud Attribute Name	Pre-Defined Value
First	FirstName	
Last	LastName	
AMA-UT	**AMAUserType	

Sponsor-specific attributes and custom attributes are distinguished from the standard attributes by a double asterisk.

12. Key in mapping details as required.
13. Click **Save**. The screen refreshes, and new federation configuration is added to the system and displayed in the list.
14. Test the connection. Refer to the section entitled Testing SP Federation Connection for more details.

RESULT:

You have successfully initiated the process of creating a new Federation Connection. Next, test the Federation Connection.

Updating a Federation Configuration

Complete the steps below to modify an existing federation configuration.

1. Navigate to the SP Configuration screen. A list of all existing federation configurations is displayed.
2. Click on the name of the Configuration you wish to update.
3. Update the information as required on the Step 1 screen.
4. Click **Next**. The mapping information is displayed.
5. Update the mapping information as required on Step 2 screen.
6. Optionally, add additional attributes by clicking **Add new Attribute**. An attribute maps the user attribute to the Service Provider attribute.
    a. Key in the attribute name in the SP Attribute open text field.
    b. Select the associated AppCloud attribute from the drop down menu.
7. Click **Save**.
8. Test the federation connection. Refer to the section entitled Testing Federation Connections for more details.

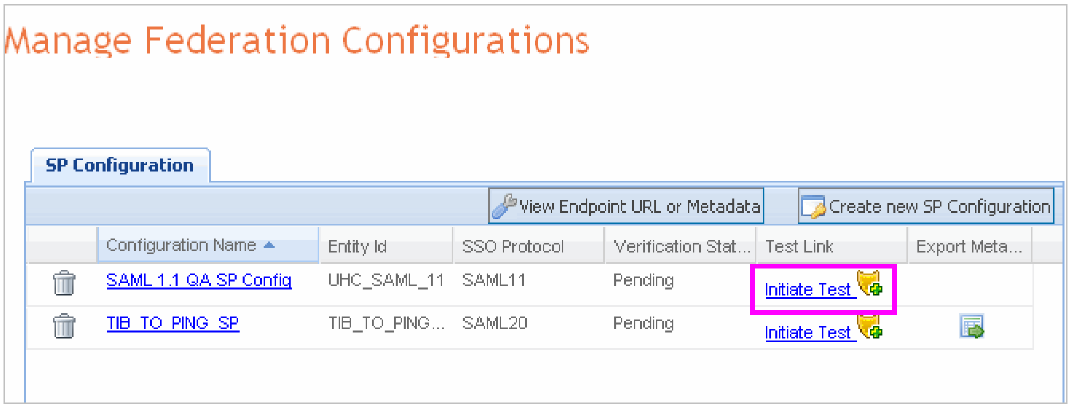
RESULT:

You have successfully updated a federation configuration. Next, test the Federation Connection.

Testing a Federation Connection

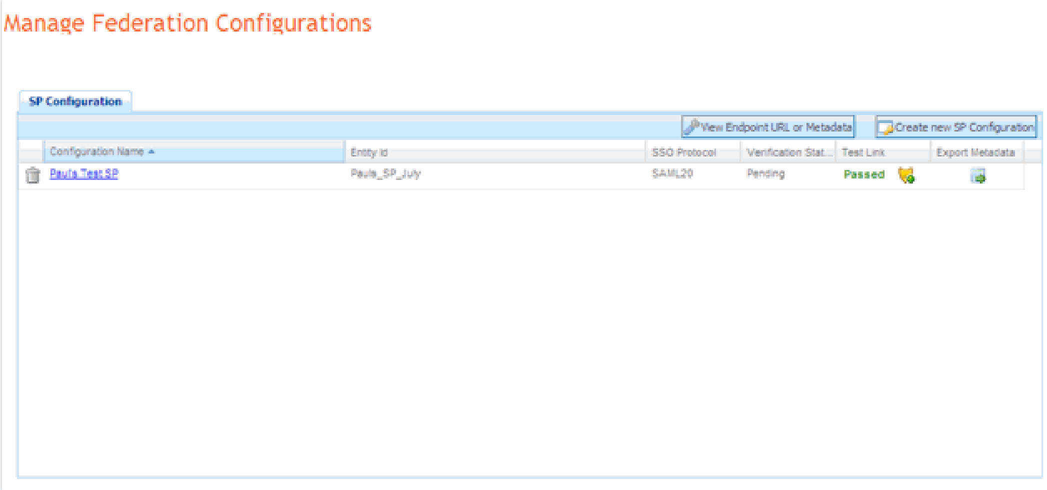
Complete the steps below to test the federation connection after creating or updating a configuration. The purpose of this test is to validate that a federation assertion, for a test user, that is sent from AppCloud can be successfully consumed by the Application Provider's federation consumer.

1. Navigate to the SP Configuration screen. A list of all existing configurations, along with the verification status of each is displayed.


Manage Federation Configurations

	Configuration Name ▲	Entity Id	SSO Protocol	Verification Stat...	Test Link	Export Meta...
	SAML 1.1 QA SP Config	UHC_SAML_11	SAML11	Pending	Initiate Test	
	TIB_TO_PING_SP	TIB_TO_PING...	SAML20	Pending	Initiate Test	

2. Click **Initiate Test** for the pending federation connection you wish to test.
3. Once the test is complete, the verification status is updated to passed if the test passed successfully.


Manage Federation Configurations

	Configuration Name ▲	Entity Id	SSO Protocol	Verification Stat...	Test Link	Export Metadata
	Pauls Test SP	Pauls_SP_July	SAML20	Pending	Passed	

RESULT:

You have successfully tested a federation connection and confirmed the creation or updates of the associated configuration.

Deleting SP Federation Configuration

Complete the steps below to delete an existing federation configuration.

1. Navigate to the SP Configuration screen. A list of all existing federation configurations is displayed.
2. Click 🗑 in the row of the federation configuration you wish to delete from the system.
3. Optionally, key in the reason for deleting the federation configuration from the system in the open text field.
4. Click **Yes.** The screen refreshes, and a list of existing federation configurations is displayed, and the deleted SP Federation Configuration is no longer on the list.

RESULT:

You have successfully deleted a configuration and removed the associated federation connection.

APPLICATION CONFIGURATION ADMINISTRATOR TASKS

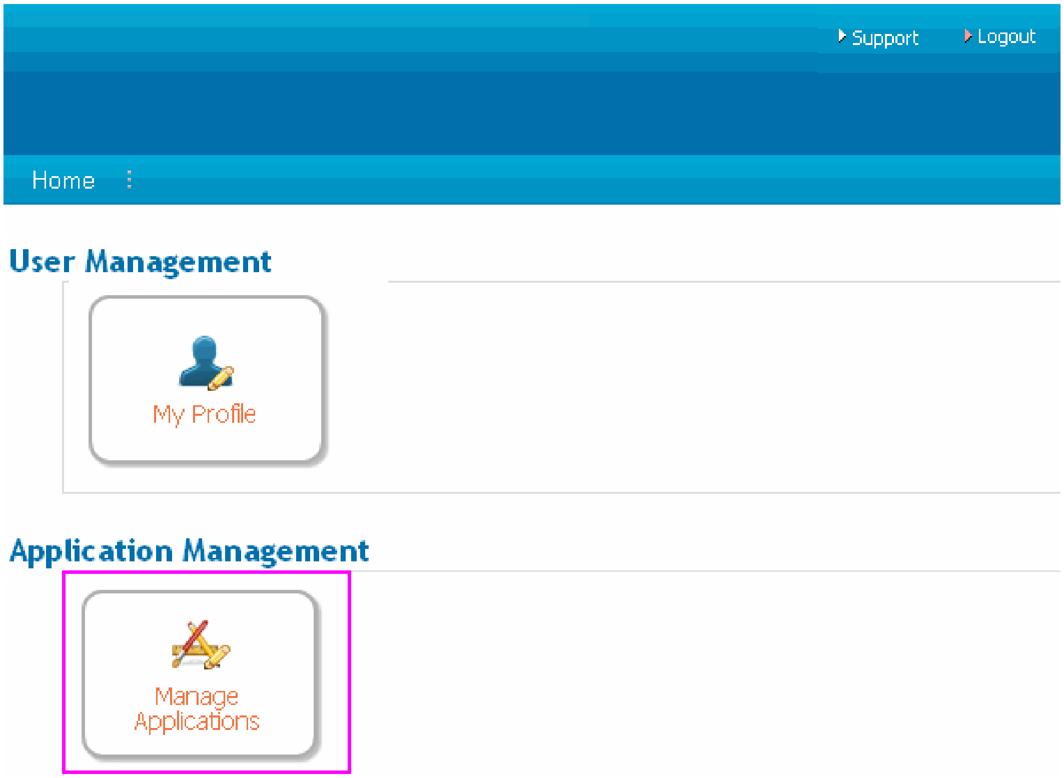
Working as a Application Configuration Administrator

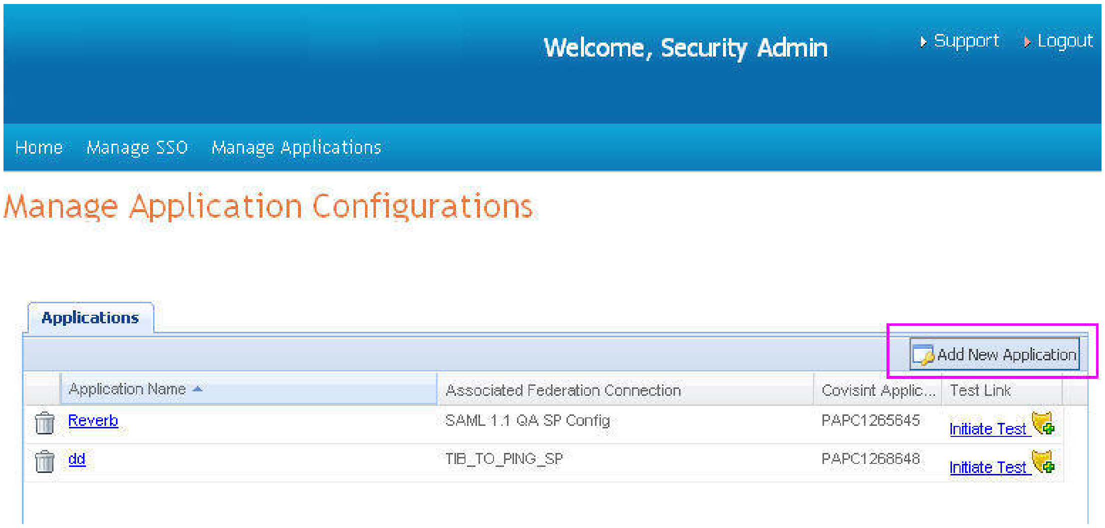
Assumptions:

- The role of Application Configuration Administrator is assigned to your user profile
- You are signed-on to AppCloudTM when performing all Application Configuration Administrator tasks
- You have reviewed privileges assigned to the Application Configuration Administrator role

Adding a New Application to AppCloud

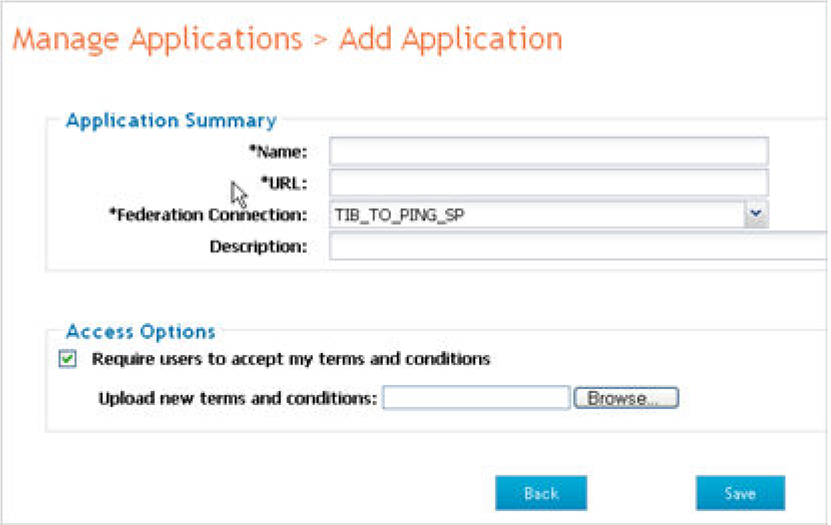
1. After signing-on to AppCloud™ click **Manage Applications**. The Application Management screen is displayed.





	Application Name	Associated Federation Connection	Covisint Applic...	Test Link
	Reverb	SAML 1.1 QA SP Config	PAPC1265645	Initiate Test
	dd	TIB_TO_PING_SP	PAPC1268648	Initiate Test

2. Click **Add New Application.** The Add Application screen is displayed.



Manage Applications > Add Application

Application Summary

*Name:

*URL:

*Federation Connection: TIB_TO_PING_SP

Description:

Access Options

☑ Require users to accept my terms and conditions

Upload new terms and conditions:

3. In the fields provided, key in the following:
    - key in the name of application
    - key in the URL to the application
    - select the Federation Connection from the drop down menu
    - key in a description of the application

4. Perform one of the following:

IF TERMS AND CONDITIONS SHOULD:	THEN:
not be required in order for access to be granted	a. do not enable the Access Options Checkbox. b. proceed to step 6.
be required in order for access to be granted	a. enable the **Access Options Checkbox.** The upload new terms option is displayed. b. upload the terms and conditions by clicking **Browse...** to select them. c. the proceed to step 6.

6. Click **Save**. The screen refreshes, and the new application is added to the list.

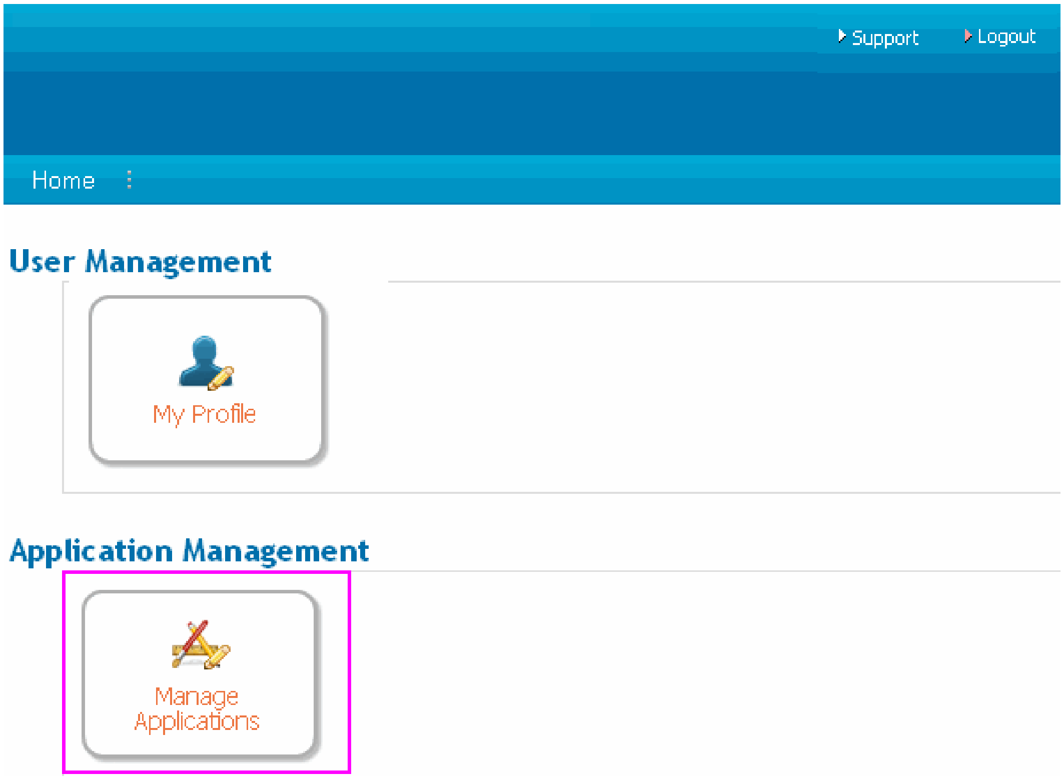
RESULT:

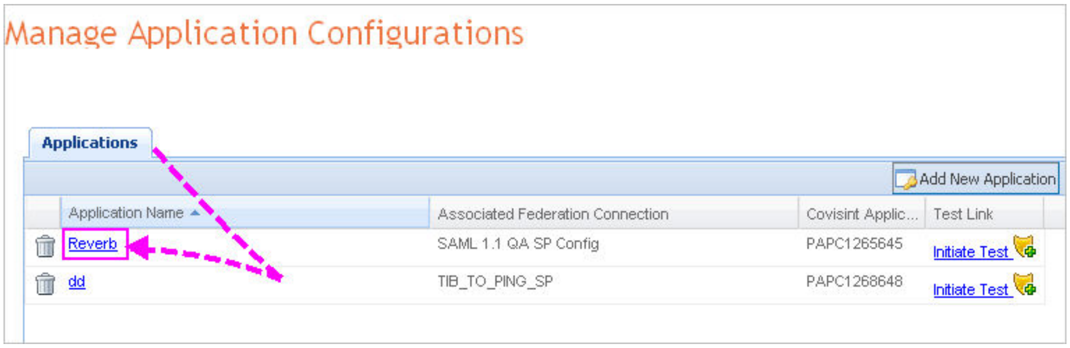
You have successfully added a new application to AppCloud. Next, verify that SSO to the application has been configured correctly by testing SSO to the new application.

Editing an Application Configuration

Complete the steps below to edit an existing application configuration.

1. After signing-on to AppCloud™ click **Manage Applications**. The Application Management screen is displayed.





Application Name ▲	Associated Federation Connection	Covisint Applic...	Test Link
Reverb	SAML 1.1 QA SP Config	PAPC1265645	Initiate Test
dd	TIB_TO_PING_SP	PAPC1268648	Initiate Test

2. Click on the *name of the application configuration* you wish to update.
3. In the fields provided, modify any of the following by:
   - keying in the name of application
   - keying in the URL to the application
   - keying in a description of the application

- selecting the Federation Connection from the drop down menu

4. Optionally, modify terms and condition requirements by performing one of the following:

IF:	THEN:
terms and conditions should not be required in order for access to be granted	a. do not enable the **Access Options Checkbox**. b. proceed to step 6.
terms and conditions should be required in order for access to be granted	a. enable the **Access Options Checkbox.** The upload new terms option is displayed. b. upload the terms and conditions by clicking **Browse...** to select them. c. the proceed to step 6.
you wish to upload a different set of terms and conditions	a. validate that the **Access Options Checkbox** is enabled. b. upload the new terms and conditions by clicking **Browse...** to select them. c. the proceed to step 6.

5. Click **Save**. The screen refreshes, and the application configuration is updated.

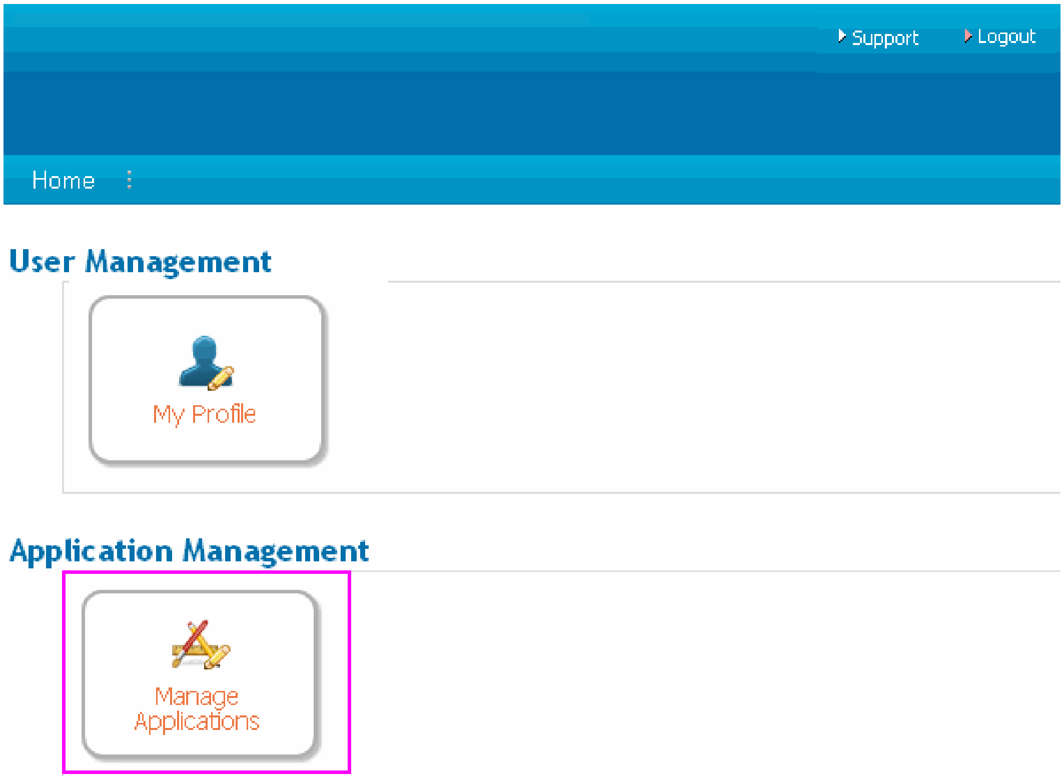
RESULT:

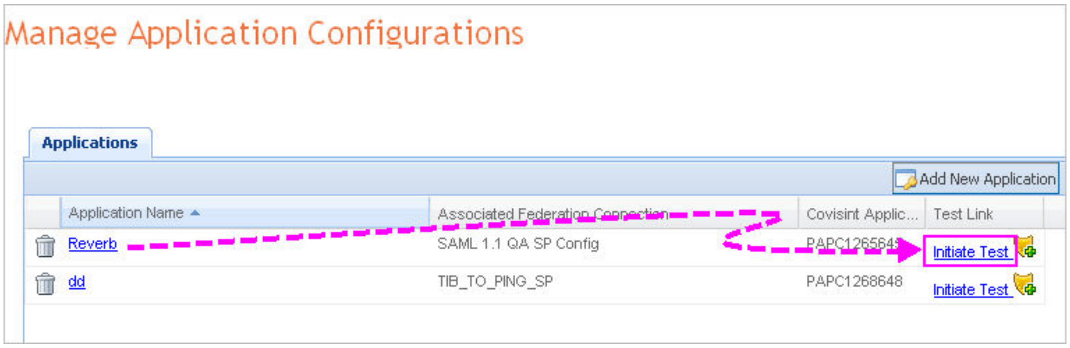
You have successfully updated application configuration. Next, test the sso to application.

Testing SSO to an Application

Complete the steps below to test SSO to an application after creating or updating a configuration. The purpose of the test is to confirm that a test user can SSO to the application that was added or modified.

1. After signing-on to AppCloud™ click **Manage Applications**. The Application Management screen is displayed.

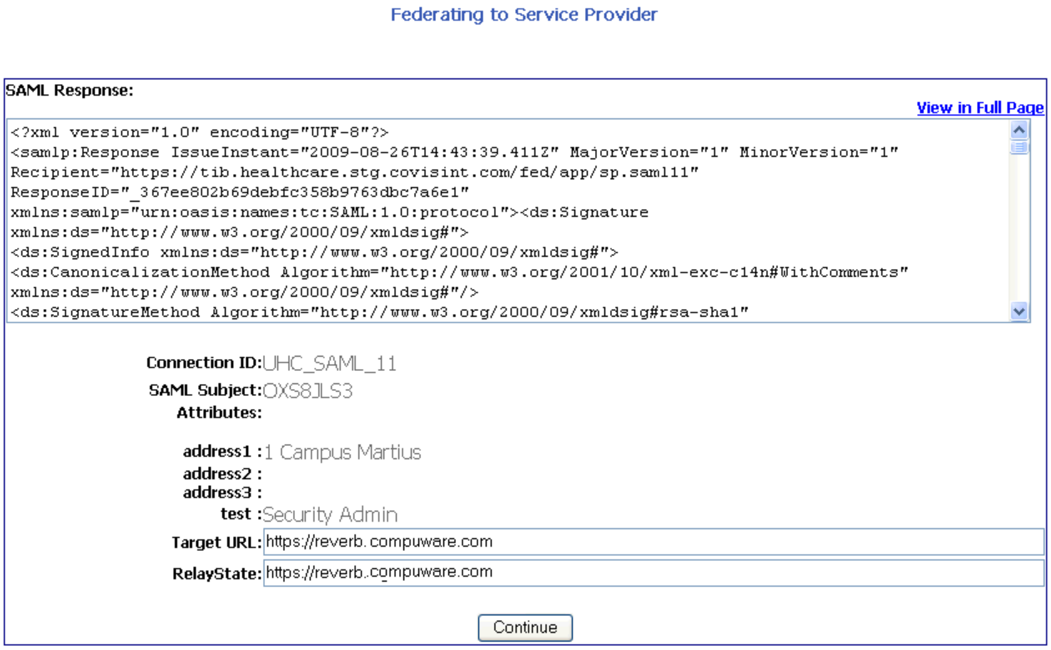




	Application Name ▲	Associated Federation Connection	Covisint Applic...	Test Link
🗑	Reverb	SAML 1.1 QA SP Config	PAPC126564[illegible]	Initiate Test
🗑	dd	TIB_TO_PING_SP	PAPC1268648	Initiate Test

2. Click **Initiate Test** for the application you wish to test. The **SAML response screen is displayed** in a new window and displays the information included in the assertion.

SAML Response Screen



Federating to Service Provider

SAML Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response IssueInstant="2009-08-26T14:43:39.411Z" MajorVersion="1" MinorVersion="1"
Recipient="https://tib.healthcare.stg.covisint.com/fed/app/sp.saml11"
ResponseID="_367ee802b69debfc358b9763dbc7a6e1"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
```

Connection ID: UHC_SAML_11

SAML Subject: OXS8JLS3

Attributes:

address1 : 1 Campus Martius

address2 :

address3 :

test : Security Admin

Target URL: https://reverb.compuware.com

RelayState: https://reverb.compuware.com

3. Click **Continue**. A test assertion is sent to the federation consumer specified in the federation connection's configuration and then redirected by the federation consumer to the URL specified in the application configuration. The test is complete.

RESULT:

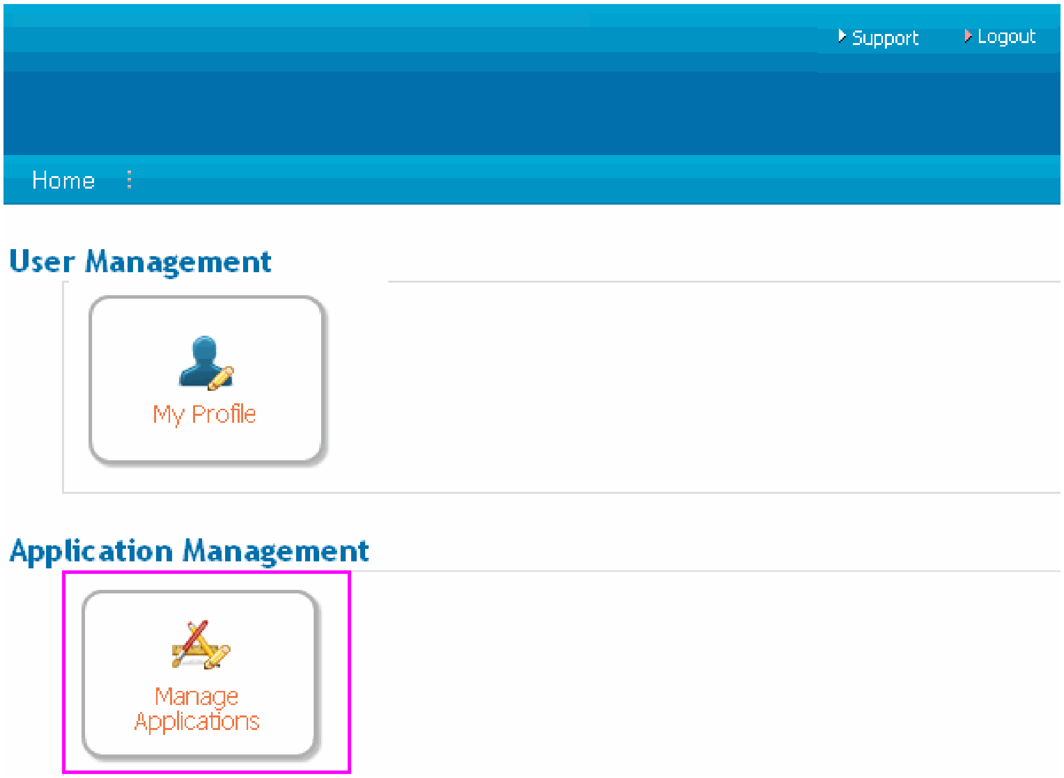
You have successfully tested SSO to the application and confirmed application configuration creation or updates.

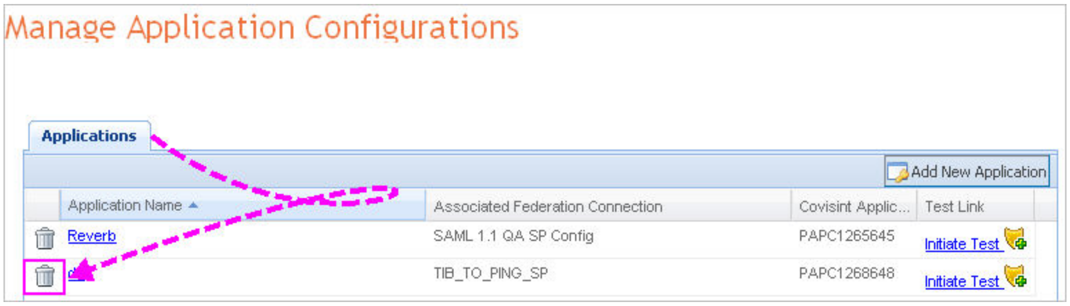
Deleting an Application Configuration

Complete the steps below to delete an application configuration that is no longer required / in use.

> An application can only be deleted when all users no longer have access to the application.

1. After signing-on to AppCloud™ click **Manage Applications**. The Application Management screen is displayed.




Manage Application Configurations

	Application Name ▲	Associated Federation Connection	Covisint Applic...	Test Link
🗑	Reverb	SAML 1.1 QA SP Config	PAPC1265645	Initiate Test
🗑	[illegible]	TIB_TO_PING_SP	PAPC1268648	Initiate Test

1. Click 🗑 in the row of the application configuration you wish to delete from the system. A confirmation box is displayed.

ℹ If access to the application is still granted to users, the confirmation box will not be displayed. Instead, you will receive a message stating "application currently in use", and you will not be able to delete the application configuration. When necessary, work with the Application Access Administrator of your organization to remove user grants.

3. In the Confirm Action pop up box, key in the reason for deleting the configuration in the open text field.

4. Click **Yes.** The screen refreshes, and a list of existing application configurations is displayed, and the deleted application configuration is no longer displayed in the list.

RESULT:

You have successfully deleted an application configuration.

APPLICATION ACCESS ADMINISTRATOR TASKS

Working as a Application Access Administrator

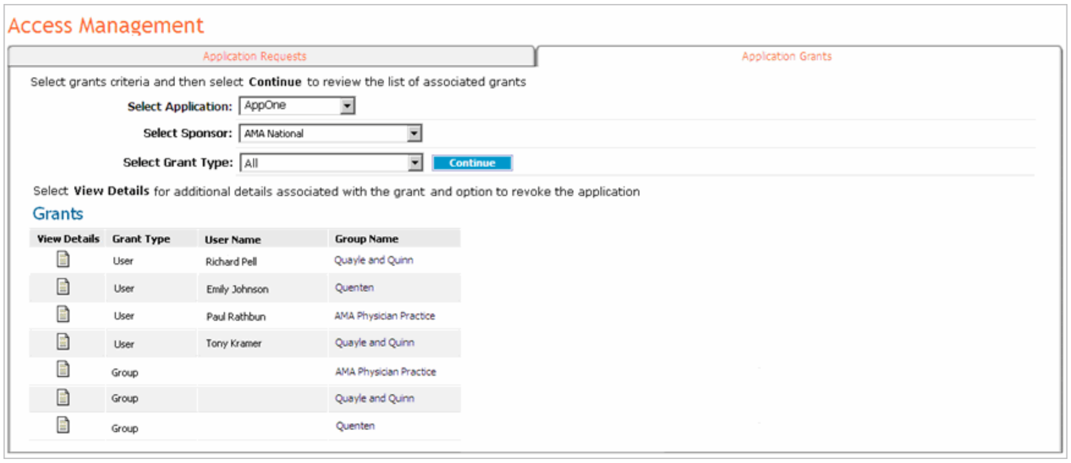
Assumptions:

- The role of Application Access Administrator is assigned to your user profile
- You are signed-on to AppCloud™ when performing all Application Access Administrator tasks
- You have reviewed privileges assigned to the Application Access Administrator role

Viewing Application Access Grants

Application Access Administrators are able to select any of the applications for which they are responsible and view all the users and groups who have requested access to a selected application.

1. After signing on to AppCloud™, click **Manage Access**. The Access Management screen is displayed.



Access Management

Select grants criteria and then select **Continue** to review the list of associated grants

Select Application: AppOne

Select Sponsor: AMA National

Select Grant Type: All

Select **View Details** for additional details associated with the grant and option to revoke the application

Grants

View Details	Grant Type	User Name	Group Name
🗎	User	Richard Pell	Quayle and Quinn
🗎	User	Emily Johnson	Quenten
🗎	User	Paul Rathbun	AMA Physician Practice
🗎	User	Tony Kramer	Quayle and Quinn
🗎	Group		AMA Physician Practice
🗎	Group		Quayle and Quinn
🗎	Group		Quenten

2. Click **Application Grants.**
3. Select the application, sponsor, and grant type for which you wish to view current application grants from the drop down menus.
4. Click **Continue**. The screen refreshes, and a list of all users with access meeting the criteria selected in the drop down menus is displayed.

Grant type is used to distinguish if an application was granted for potential use to a specific 'group' of users, or was granted to a specific 'user'.

RESULT:

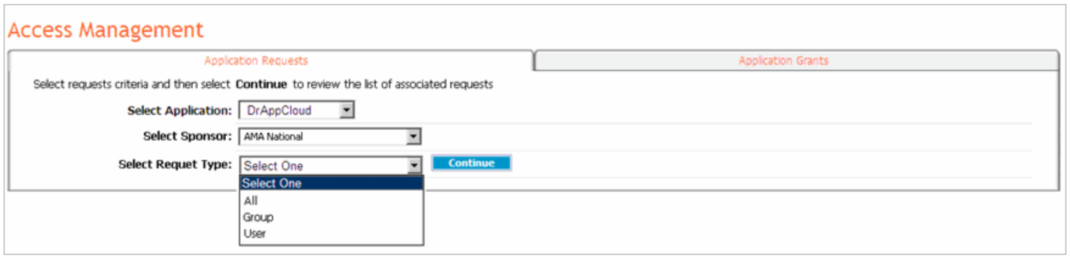
You have successfully viewed application access grants.

Approve or Reject Application Access Requests of Users

Before beginning this task:

You cannot approve a request until a user account has been created in the Application Provider's system for the requestor.

If the requestor does not have an account in the Application Provider's system, use the user information provided on the Request Details screen to create the account using your standard process. (See step 4).



Access Management

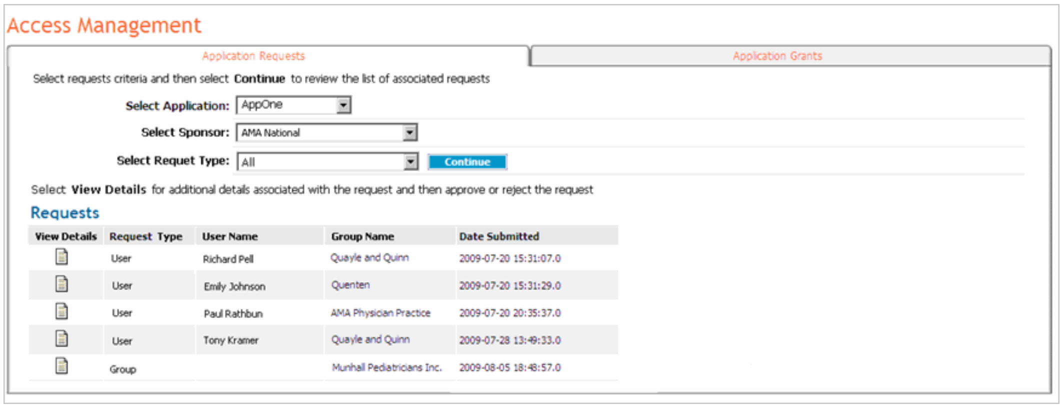
Select requests criteria and then select **Continue** to review the list of associated requests

Select Application: DrAppCloud

Select Sponsor: AMA National

Select Requet Type: Select One

1. From the Access Management screen, click **Application Requests**.
2. Select the application for which you wish to view access requests from the Select Application drop down menu.
3. Select the sponsor for which you wish to view access requests from the Select Sponsor drop down menu.
4. Select the request type for which you wish to view access requests from the Select Request Type drop down menu.
5. Click **Continue**. The screen refreshes, and all requests associated with the criteria selected are displayed.



Access Management

Select requests criteria and then select **Continue** to review the list of associated requests

Select Application: AppOne

Select Sponsor: AMA National

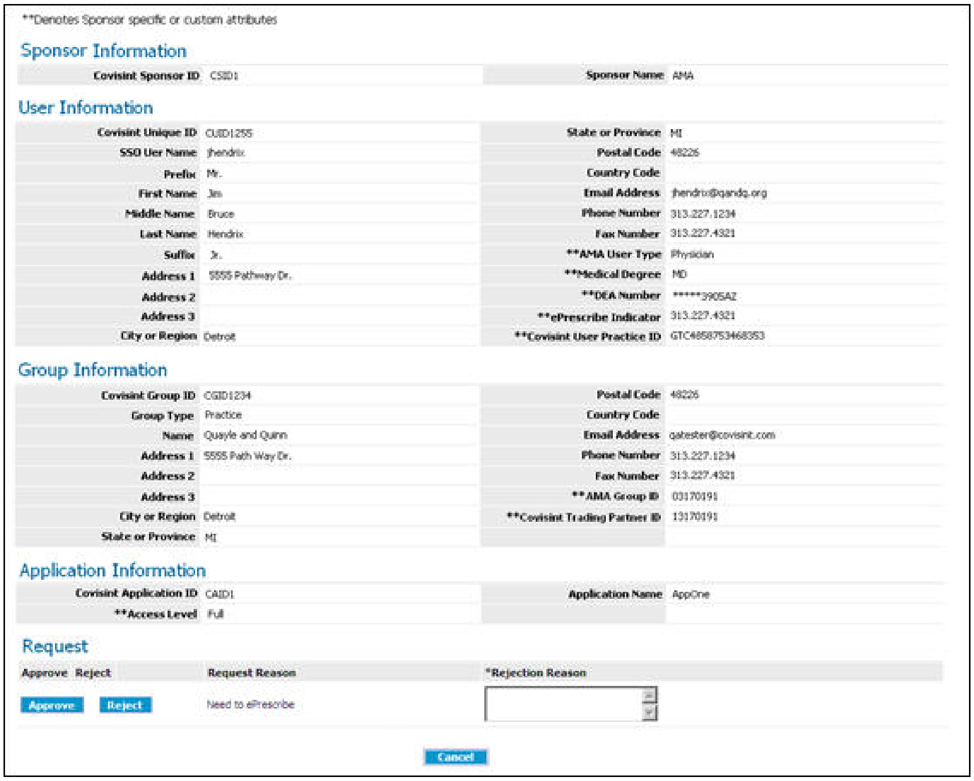
Select Requet Type: All

Select **View Details** for additional details associated with the request and then approve or reject the request

Requests

View Details	Request Type	User Name	Group Name	Date Submitted
🗎	User	Richard Pell	Quayle and Quinn	2009-07-20 15:31:07.0
🗎	User	Emily Johnson	Quenten	2009-07-20 15:31:29.0
🗎	User	Paul Rathbun	AMA Physician Practice	2009-07-20 20:35:37.0
🗎	User	Tony Kramer	Quayle and Quinn	2009-07-28 13:49:33.0
🗎	Group		Munhall Pediatricians Inc.	2009-08-05 18:48:57.0

6. Click 🗎 in the View Request column of the **user** for whom you wish to manage pending access request. The Request Details screen of the user is displayed.



**Denotes Sponsor specific or custom attributes

Sponsor Information

Covisint Sponsor ID	CSID1	Sponsor Name	AMA

User Information

Covisint Unique ID	CUID1255	State or Province	MI
SSO Uer Name	jhendrix	Postal Code	48226
Prefix	Mr.	Country Code	
First Name	Jim	Email Address	jhendrix@qandq.org
Middle Name	Bruce	Phone Number	313.227.1234
Last Name	Hendrix	Fax Number	313.227.4321
Suffix	Jr.	**AMA User Type	Physician
Address 1	5555 Pathway Dr.	**Medical Degree	MD
Address 2		**DEA Number	*****3905AZ
Address 3		**ePrescribe Indicator	313.227.4321
City or Region	Detroit	**Covisint User Practice ID	GTC4858753468353

Group Information

Covisint Group ID	CGID1234	Postal Code	48226
Group Type	Practice	Country Code	
Name	Quayle and Quinn	Email Address	qatester@covisint.com
Address 1	5555 Path Way Dr.	Phone Number	313.227.1234
Address 2		Fax Number	313.227.4321
Address 3		**AMA Group ID	03170191
City or Region	Detroit	**Covisint Trading Partner ID	13170191
State or Province	MI		

Application Information

Covisint Application ID	CAID1	Application Name	AppOne
**Access Level	Full		

Request

Approve	Reject	Request Reason	*Rejection Reason
Approve	Reject	Need to ePrescribe	

Sponsor-specific attributes and custom attributes are distinguished from the standard attributes by a double asterisk.

5. Scroll to the bottom of the screen, and perform one of the following:

IF YOU WISH TO...	THEN:
approve the request	a. Click **Approve**. b. Click **OK** to confirm.
reject the request	a. Key in the reason for rejecting the request in the *Rejection Reason* open text field. **This field becomes a required field when rejecting a request**. b. Click **Reject**. c. Click **OK** to confirm.

RESULT:

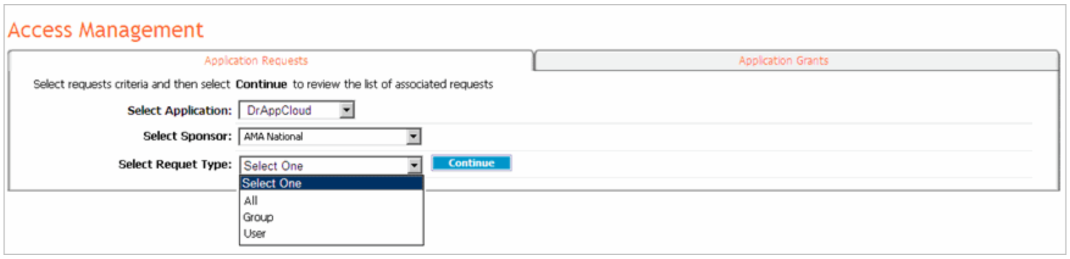
You have successfully managed application access requests for users. A user will receive email notification of your approval decision.

Approve or Reject Application Access Requests of Groups

Before beginning this task:

You cannot approve a group request until a group has been created in the Application Provider's system for the group.

If the group does not have an account in the Application Provider’s system, use the group information provided on the Request Details screen to create the account using your standard process.



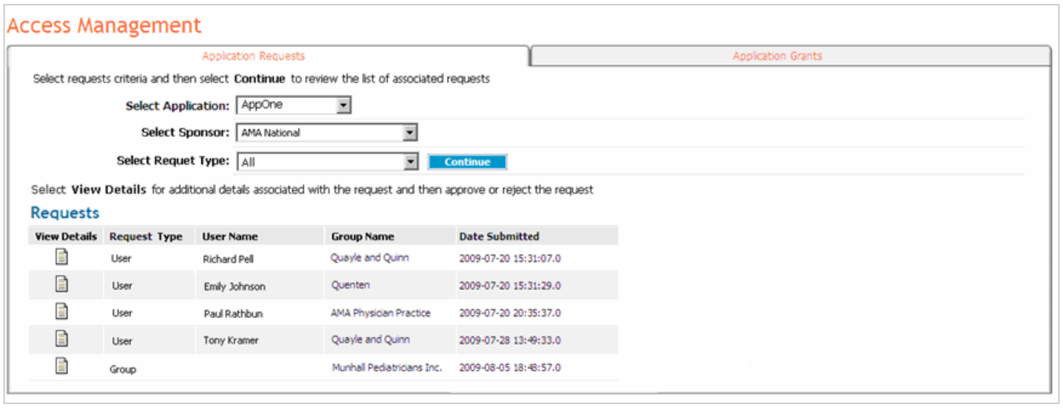
Select requests criteria and then select **Continue** to review the list of associated requests

Select Application: DrAppCloud

Select Sponsor: AMA National

Select Requet Type: Select One

1. From the Access Management screen, click **Application Requests**.
2. Select the application for which you wish to view access requests from the Select Application drop down menu.
3. Select the sponsor for which you wish to view access requests from the Select Sponsor drop down menu.
4. Select the request type for which you wish to view access requests from the Select Request Type drop down menu.
5. Click **Continue**. The screen refreshes, and all requests associated with the criteria selected are displayed.



Select requests criteria and then select **Continue** to review the list of associated requests

Select Application: AppOne

Select Sponsor: AMA National

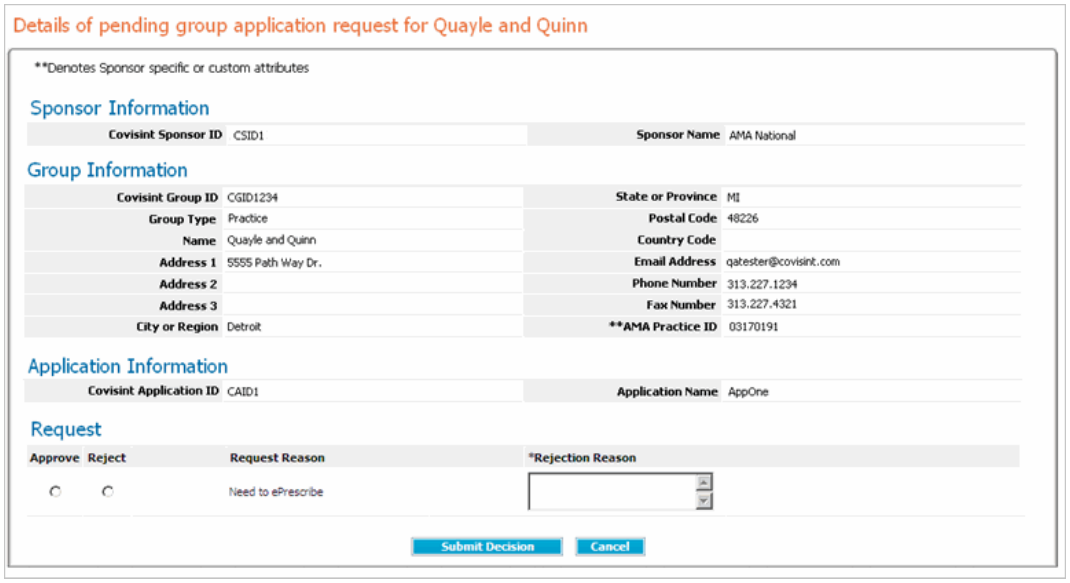
Select Requet Type: All

Select **View Details** for additional details associated with the request and then approve or reject the request

Requests

View Details	Request Type	User Name	Group Name	Date Submitted
🗎	User	Richard Pell	Quayle and Quinn	2009-07-20 15:31:07.0
🗎	User	Emily Johnson	Quenten	2009-07-20 15:31:29.0
🗎	User	Paul Rathbun	AMA Physician Practice	2009-07-20 20:35:37.0
🗎	User	Tony Kramer	Quayle and Quinn	2009-07-28 13:49:33.0
🗎	Group		Munhall Pediatricians Inc.	2009-08-05 18:48:57.0

6. Click 🗎 in the View Request column of the ***group*** for whom you wish to manage pending access request. The Group Request Details screen is displayed.



Details of pending group application request for Quayle and Quinn

**Denotes Sponsor specific or custom attributes

Sponsor Information

Covisint Sponsor ID	CSID1	Sponsor Name	AMA National

Group Information

Covisint Group ID	CGID1234	State or Province	MI
Group Type	Practice	Postal Code	48226
Name	Quayle and Quinn	Country Code	
Address 1	5555 Path Way Dr.	Email Address	qatester@covisint.com
Address 2		Phone Number	313.227.1234
Address 3		Fax Number	313.227.4321
City or Region	Detroit	**AMA Practice ID	03170191

Application Information

Covisint Application ID	CAID1	Application Name	AppOne

Request

Approve	Reject	Request Reason	*Rejection Reason
○	○	Need to ePrescribe	

Sponsor-specific attributes and custom attributes are distinguished from the standard attributes by a double asterisk.

5. Scroll to the bottom of the screen, and perform one of the following:

IF YOU WISH TO...	THEN:
approve the request	a. Click **Approve**. b. Click **OK** to confirm.
reject the request	a. Key in the reason for rejecting the request in the *Rejection Reason* open text field. This field becomes a required field when rejecting a request. b. Click **Reject**. c. Click **OK** to confirm.

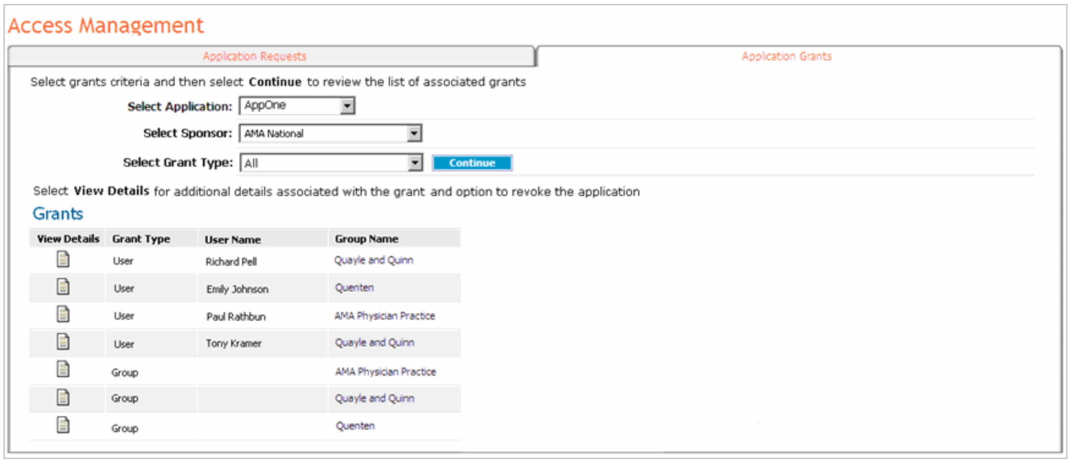
RESULT:

You have successfully managed application access requests. The group administrator will receive email notification of your approval decision. Next, the users belonging to this group may also request access. If approval is required, manage user access request >>>

Revoking Application Access from a Group

When revoking application access from a ***group***, the application is revoked from the group and simultaneously auto-revoked from all users within the group.

1. Navigate to the Application Access Grants screen.
2. From the drop down menus, select the Application, Sponsor, and Grant type of the group from whom you wish to revoke the application.



Access Management

Select grants criteria and then select **Continue** to review the list of associated grants

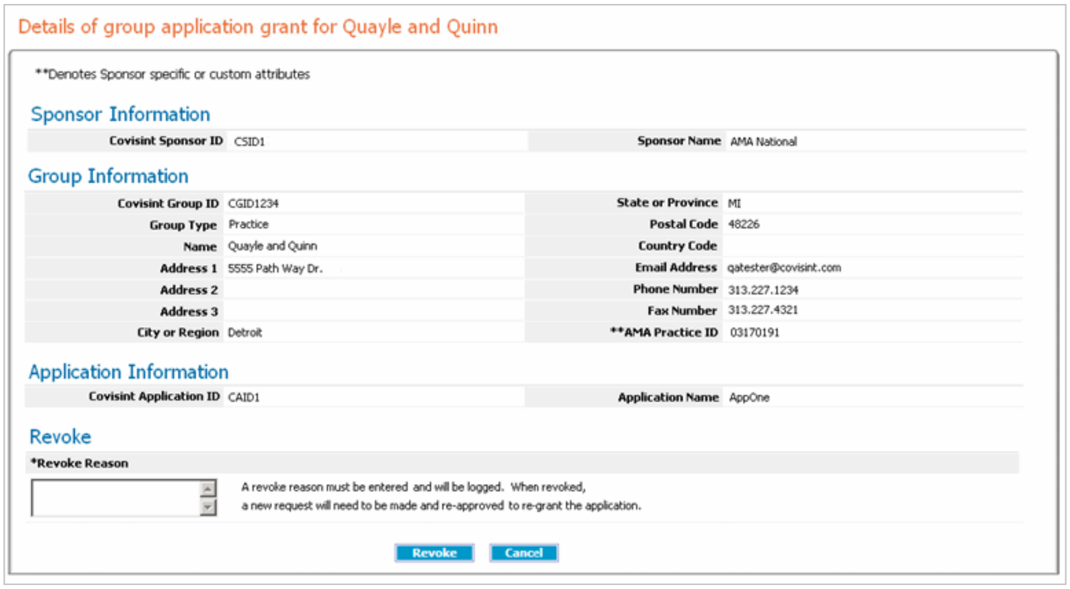
Select Application: AppOne
Select Sponsor: AMA National
Select Grant Type: All

Select **View Details** for additional details associated with the grant and option to revoke the application

Grants

View Details	Grant Type	User Name	Group Name
🗎	User	Richard Pell	Quayle and Quinn
🗎	User	Emily Johnson	Quenten
🗎	User	Paul Rathbun	AMA Physician Practice
🗎	User	Tony Kramer	Quayle and Quinn
🗎	Group		AMA Physician Practice
🗎	Group		Quayle and Quinn
🗎	Group		Quenten

2. Click 🗎 in the details column of the group from whom you wish to revoke access to this application. The Details screen is displayed.



Details of group application grant for Quayle and Quinn

**Denotes Sponsor specific or custom attributes

Sponsor Information

Covisint Sponsor ID	CSID1	**Sponsor Name**	AMA National

Group Information

Covisint Group ID	CGID1234	**State or Province**	MI
Group Type	Practice	**Postal Code**	48226
Name	Quayle and Quinn	**Country Code**	
Address 1	5555 Path Way Dr.	**Email Address**	qatester@covisint.com
Address 2		**Phone Number**	313.227.1234
Address 3		**Fax Number**	313.227.4321
City or Region	Detroit	****AMA Practice ID**	03170191

Application Information

Covisint Application ID	CAID1	**Application Name**	AppOne

Revoke

***Revoke Reason**

A revoke reason must be entered and will be logged. When revoked, a new request will need to be made and re-approved to re-grant the application.

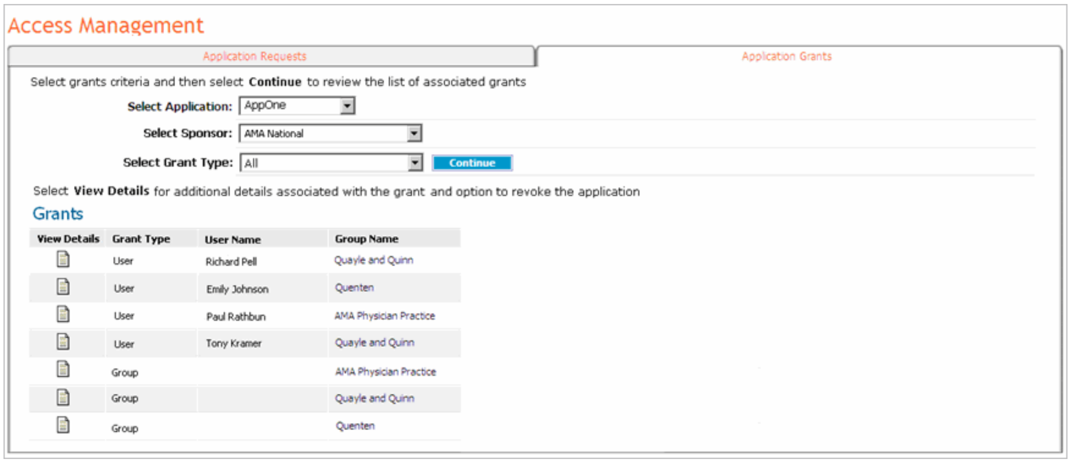
3. In the open text field, key in the reason for revoking the application access. The information you provide in this field is logged in the status history and is viewable by other Security Administrators in your organization.

4. Click **Revoke**. A message is displayed, confirming the application access has been revoked.

RESULT:
You have successfully revoked application access from a group and all of its users.

Revoking Application Access from a User

1. Navigate to the Application Access Grants screen.
2. From the drop down menus, select the Application, Sponsor, and Grant type of the user from whom you wish to revoke the application.



Access Management

Select grants criteria and then select **Continue** to review the list of associated grants

Select Application: AppOne

Select Sponsor: AMA National

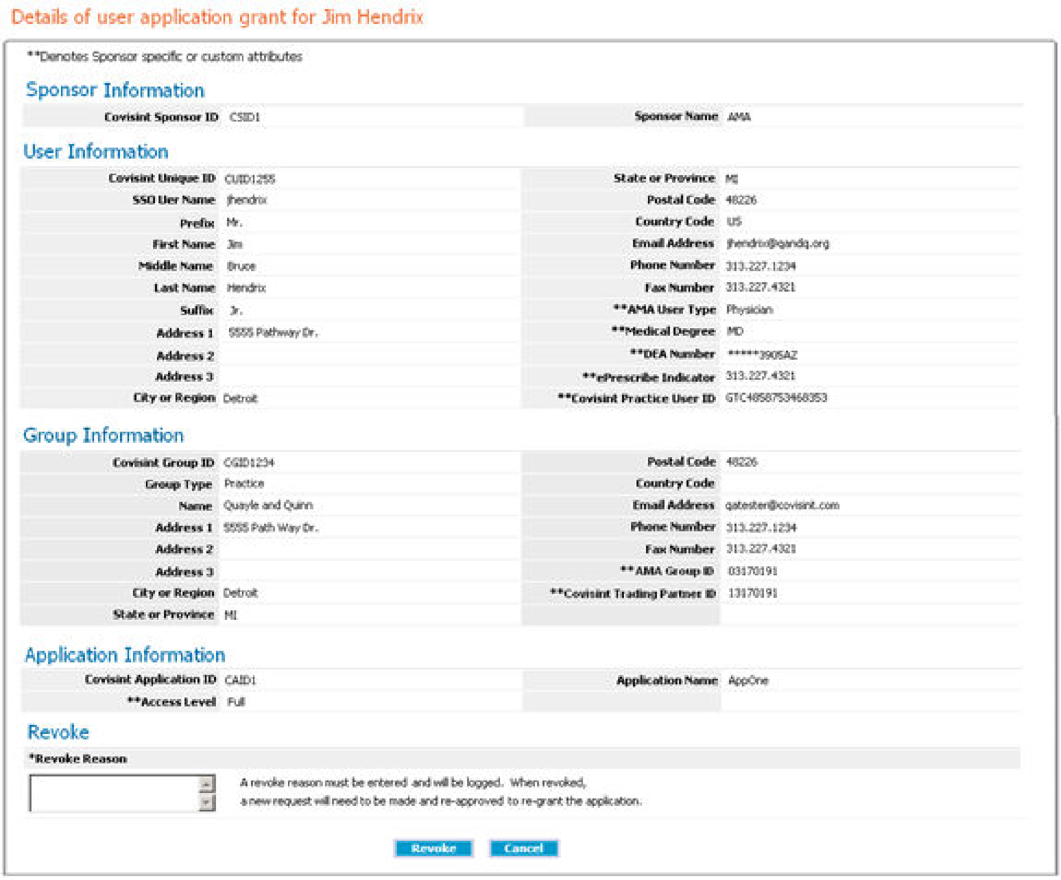
Select Grant Type: All

Select **View Details** for additional details associated with the grant and option to revoke the application

Grants

View Details	Grant Type	User Name	Group Name
🗎	User	Richard Pell	Quayle and Quinn
🗎	User	Emily Johnson	Quenten
🗎	User	Paul Rathbun	AMA Physician Practice
🗎	User	Tony Kramer	Quayle and Quinn
🗎	Group		AMA Physician Practice
🗎	Group		Quayle and Quinn
🗎	Group		Quenten

2. Click 🗎 in the details column of the user from whom you wish to revoke access to this application. The Details screen is displayed.



Details of user application grant for Jim Hendrix

**Denotes Sponsor specific or custom attributes

Sponsor Information

Covisint Sponsor ID	CSID1	Sponsor Name	AMA

User Information

Covisint Unique ID	CUID1255	State or Province	MI
SSO Uer Name	jhendrix	Postal Code	48226
Prefix	Mr.	Country Code	US
First Name	Jim	Email Address	jhendrix@qandq.org
Middle Name	Bruce	Phone Number	313.227.1234
Last Name	Hendrix	Fax Number	313.227.4321
Suffix	Jr.	**AMA User Type	Physician
Address 1	5555 Pathway Dr.	**Medical Degree	MD
Address 2		**DEA Number	*****3905AZ
Address 3		**ePrescribe Indicator	313.227.4321
City or Region	Detroit	**Covisint Practice User ID	GTC4858753468353

Group Information

Covisint Group ID	CGID1234	Postal Code	48226
Group Type	Practice	Country Code	
Name	Quayle and Quinn	Email Address	qatester@covisint.com
Address 1	5555 Path Way Dr.	Phone Number	313.227.1234
Address 2		Fax Number	313.227.4321
Address 3		**AMA Group ID	03170191
City or Region	Detroit	**Covisint Trading Partner ID	13170191
State or Province	MI		

Application Information

Covisint Application ID	CAID1	Application Name	AppOne
**Access Level	Full		

Revoke

*Revoke Reason

A revoke reason must be entered and will be logged. When revoked,
a new request will need to be made and re-approved to re-grant the application.

3. In the open text field, key in the reason for revoking the application access. The information you provide in this field is logged in the status history and is viewable by other Security Administrators in your organization.

4. Click **Revoke**. A message is displayed, confirming the application access has been revoked.

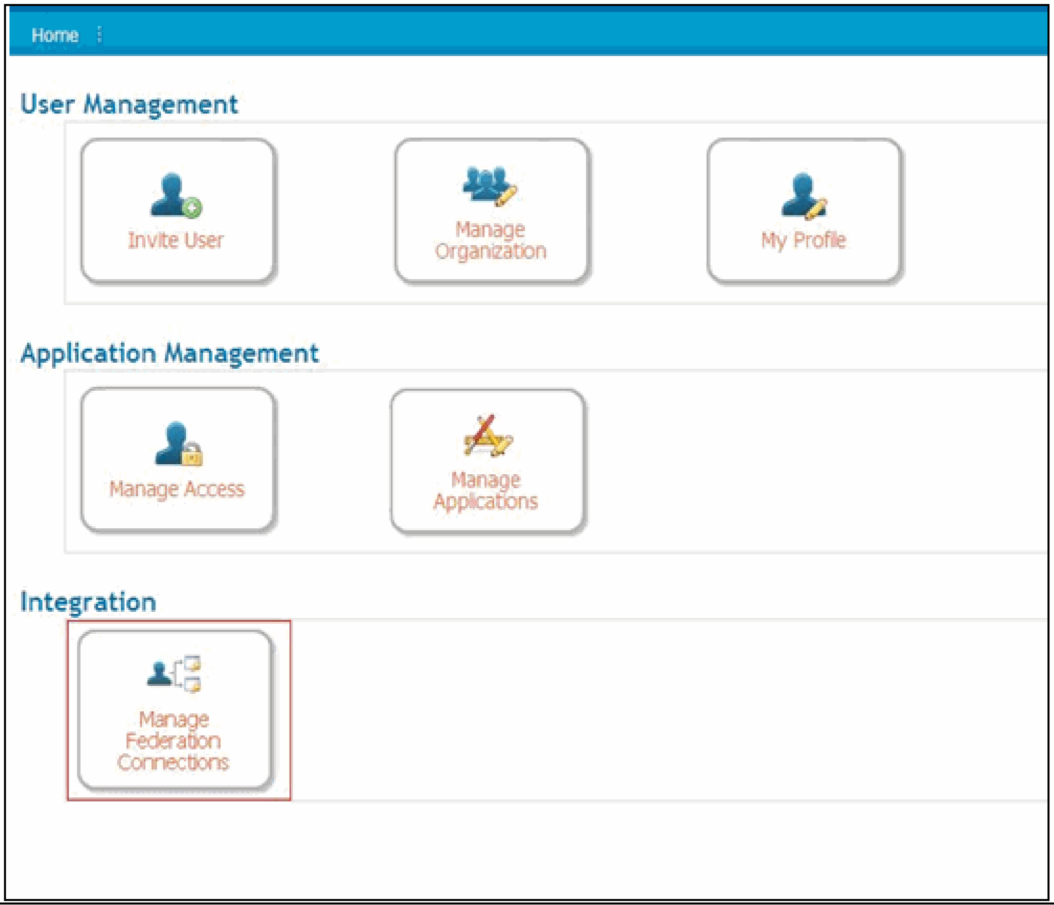
RESULT:

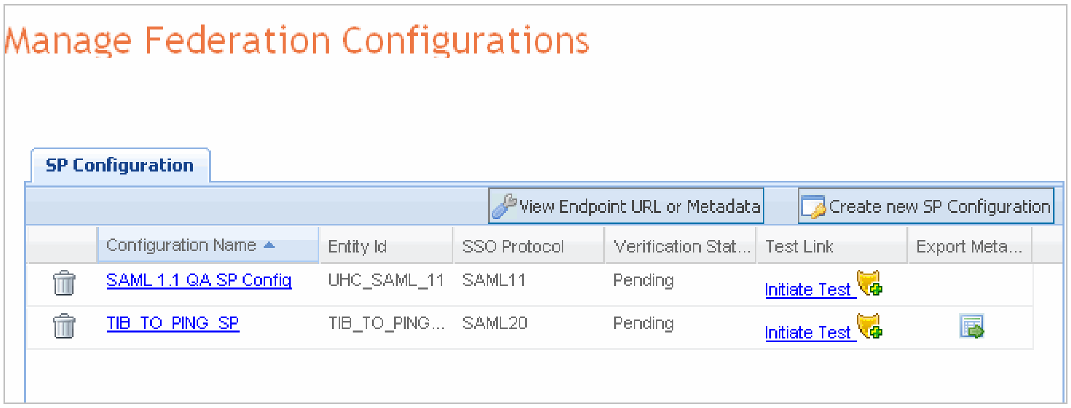
You have successfully revoked application access from a user.

Creating a Federation Connection

1. Click **Manage Federation Connections.** The Manage Federation Configurations screen displays a list of all existing configurations, along with the verification status of each.

Manage Federation Connections Link



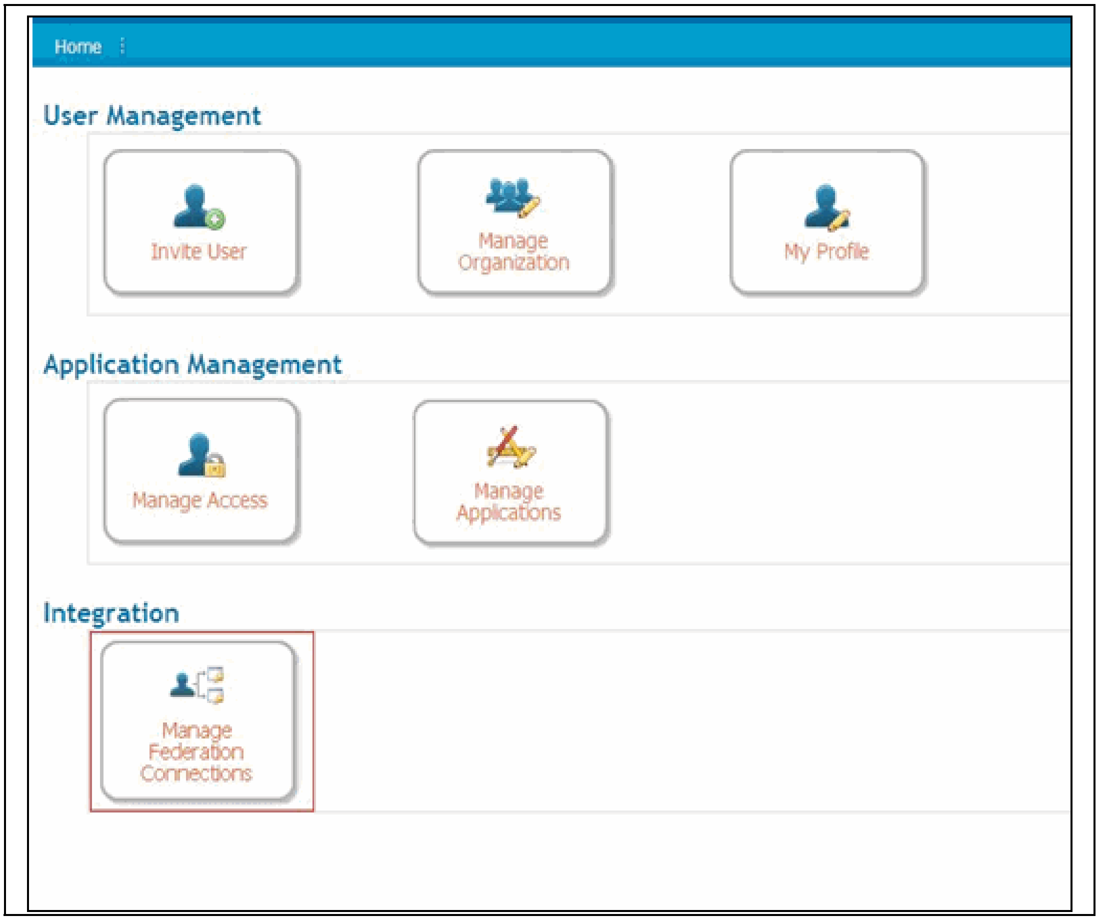


Manage Federation Configurations

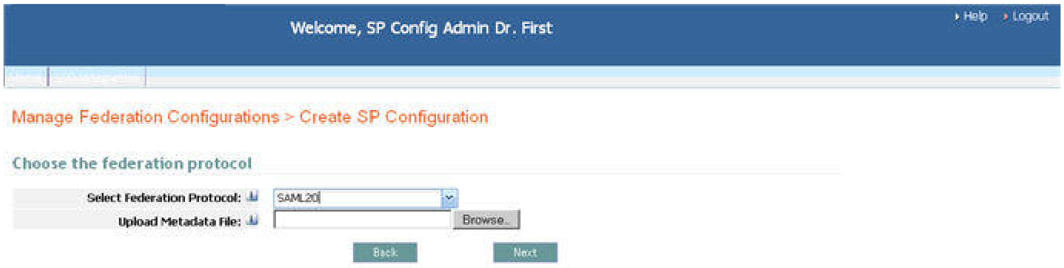
	Configuration Name ▲	Entity Id	SSO Protocol	Verification Stat...	Test Link	Export Meta...
🗑	SAML 1.1 QA SP Config	UHC_SAML_11	SAML11	Pending	Initiate Test	
🗑	TIB_TO_PING_SP	TIB_TO_PING...	SAML20	Pending	Initiate Test	▤

2. View **EndPoint URLs or Metadata** to obtain the information required to start the configuration process. A list of supported options is displayed.
3. Download the signature verification certificate and use the Endpoints displayed.
    a. Optionally if the federation solution supports metadata, download the Covisint SSO metadata file.
4. After configuring the federation consumer at the Application Provider's site, click **Manage Federation Connections.** The Manage Federation Configurations screen displays a list of all existing configurations, along with the verification status of each.

Manage SSO Link



5. Click **Create new SP Configuration.**



Welcome, SP Config Admin Dr. First

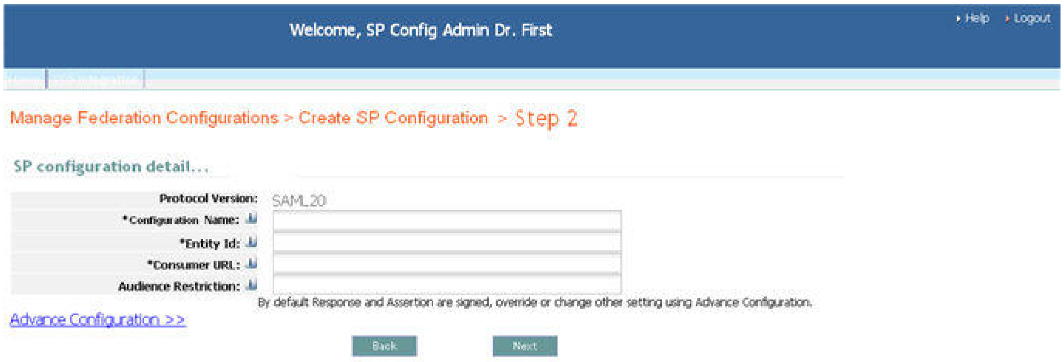
Manage Federation Configurations > Create SP Configuration

Choose the federation protocol

Select Federation Protocol: SAML20

Upload Metadata File:

6. Select the Federation Protocol from the drop down menu.
7. Upload the metadata file by clicking **Browse...** and then select the file to upload.
8. Click **Next**. The Step 2 screen is displayed.



Welcome, SP Config Admin Dr. First

Manage Federation Configurations > Create SP Configuration > Step 2

SP configuration detail...

Protocol Version:	SAML20
*Configuration Name:	
*Entity Id:	
*Consumer URL:	
Audience Restriction:	

By default Response and Assertion are signed, override or change other setting using Advance Configuration.

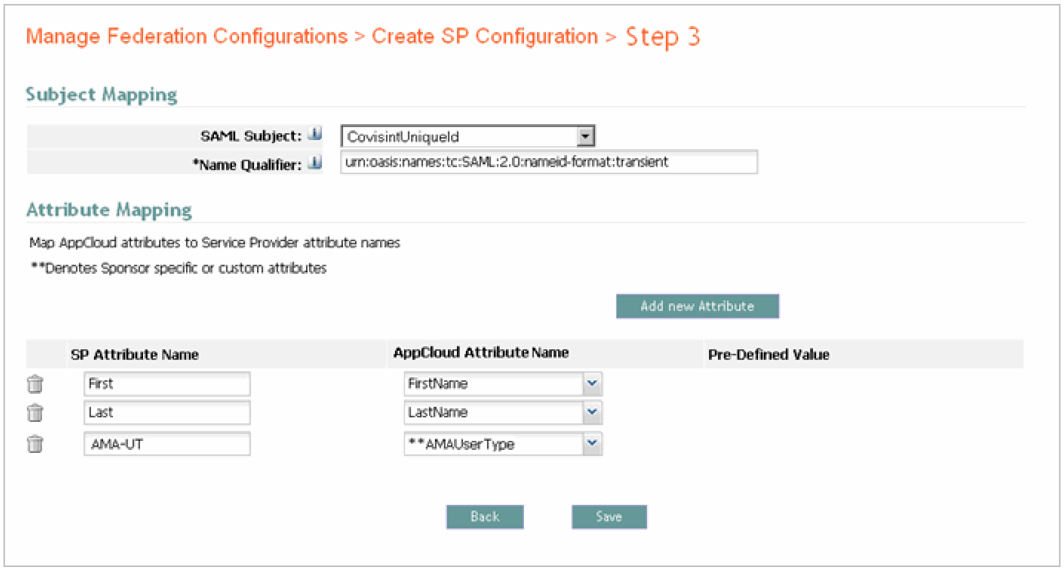
9. Key in the following Basic information as required / desired:

FIELD NAME:	DEFINITION:
Configuration Name	A Service Provider (SP) name that can be easily identified by the end user (this is a “user friendly” name)
Entity ID	The Entity ID is the identifier that uniquely represents every SAML Identity Provider or Service Provider.
Consumer URL	URL that the assertion will be posted to.
Audience Restriction	Used by the SP to limit the scope of which entity should consume the information in the assertion

10. Optionally, key in additional information by clicking **Advance Configuration.**

FIELD NAME:	DEFINITION:
Response Signing Enabled	Integrity of a message between providers is insured by using digital signatures. By enabling response signing, a digital signature is generated for the SAML Response document. Covisint will provide the SP with the Public Key that will be used to verify the Response signature.
Assertion Signing Enabled	Integrity of a message between providers is insured by using digital signatures. By enabling assertion signature signing, the digital signature is generated for the SAML Assertion document. Covisint will provide the SP with the Public Key that will be used to verify the Assertion signature.
Signing Algorithm	Singing algorithm that will be used for signing the SAML Assertions.
Canonical Algorithm	Canonical algorithm that will be used for signing the SAML assertions.

11. Click **Next**. The Step 3 screen is displayed.



Manage Federation Configurations > Create SP Configuration > Step 3

Subject Mapping

SAML Subject:	CovisintUniqueId
*Name Qualifier:	urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Attribute Mapping

Map AppCloud attributes to Service Provider attribute names

**Denotes Sponsor specific or custom attributes

SP Attribute Name	AppCloud Attribute Name	Pre-Defined Value
First	FirstName	
Last	LastName	
AMA-UT	**AMAUserType	

Sponsor-specific attributes and custom attributes are distinguished from the standard attributes by a double asterisk.

12. Key in mapping details as required.
13. Click **Save**. The screen refreshes, and new federation configuration is added to the system and displayed in the list.
14. Test the connection. Refer to the section entitled Testing SP Federation Connection for more details.

RESULT:

You have successfully initiated the process of creating a new Federation Connection. Next, test the Federation Connection.

GLOSSARY

A

Application Access Administrator: reviews all the pending application access requests that have originated from one to many sponsor communities; views details of a request; approves or rejects a user request for access to an application; views users that have access to the Access Admin's application; revokes access from selected users.

Application Configuration Administrator: Manages the information associated with an Application(s) that is required to make it available within AppCloud. Adds new applications to AppCloud, edits existing application configuration, and deletes applications no longer in use.

Assertion Signing: Integrity of a message between providers is insured by using digital signatures. By enabling assertion signature signing, the digital signature is generated forthe SAML Assertion document. Covisint will provide the SP with the Public Key thatwill be used to verify the Assertion signature.

Audience Restriction: Used by the SP to limit the scope of which entity should consume the information in the assertion.

C

Canonical Algorithm: An algorithm that will be used for signing the SAML assertions.

Challenge Answer: The answer to the challenge question, used for security purposes by the system and/or Administrators to validate user identity. This answer is punctuation and case-sensitive.

Challenge Question: The challenge question is a security question, used to validate your identity by the system and/or administration. This question is used in the case where you forget your password, you will be asked to provide the answer to this challenge question. Note, you must provide the answer exactly as you keyed it into this field during registration, including punctuation and case-sensitivity.

Covisint Unique ID: Uniquely identifies a user in Covisint systems.

E

Entity ID: The Entity ID is the identifier that uniquely represents every SAML Identity Provideror Service Provider.

F

Federation: The ability to utilize identities from one security domain within another using a pre-established trust relationship between the participating entities. The IdP is responsible for making an identity assertion and the SP is responsible for providing the appropriate service(s) to the identity's principal.

Federation Configuration Administrator: Creates the Service Provider's federation configuration by using the self-service registration wizard that is protocol-specific and is used to exchange federation configuration information between Covisint and the SP; tests the federation connection; reviews and updates information associated with any of the federation configurations (limited to the staging environment only)

G

Group: Group is the generic name used to reference a group of users. There is an attribute associated with a group called GroupType that is used to distinguish if the group is an Organization, Practice, Plant, HQ, etc.

I

Identity Broker (IdB): Provides support for protocol translation allowing an IdP and SP to use different federation protocols. Provides support for attribute mapping allowing an IdP and SP to use different attribute names to reference the same identity information. An IdB receives incoming assertions from IdPs using formats and protocols which are specific to each individual IdP and subsequently translates and routes the assertions for consumption by authorized SPs using the formats and protocols required by each individual SP.

Identity Provider (IdP): Is responsible for the creation and management of a principal's identity, the authentication of the principal, and the federation of the principal's identity to an SP or an IdB when providing support for federation.

P

Password Rules: - 8 characters minimum, 20 character maximum - Must contain characters in the Latin alphabet (a-z, A-Z) and at least one non-alpha character (number or special character*) - Cannot be the same as the User Name - Cannot be repeated for a cycle of 8 password changes - Should be difficult to guess. Allowable special characters: (numbers 0-9) , ? < > ! @ # $ % ^ & * - ( ) _ / | \ [ ] + = : ; ' "

R

Response Signing: Integrity of a message between providers is insured by using digital signatures. By enabling response signing, a digital signature is generated for the SAML Responsedocument. Covisint will provide the SP with the Public Key that will be used toverify the Response signature.

S

SAML (Security Assertion Markup Language): An OASIS XML-based framework for securely exchanging authentication and authorization data between security domains, that is, between and identity provider (a producer of assertions) and a service provider (a consumer of assertions).

Security Administrator: invites a user to register; grants or revokes the Security Administrator, Federation Configuration Administrator, Application Configuration Administrator, or Application Access Administrator role to a user; modifies a user profile; resets a user password; suspends a user account; unsuspends a user account; terminates a user account

Service Package: A grouping of one or more services that must be requested and granted as a group. Service packages also contain additional information about the services (i.e. User must accept Terms & Conditions to gain access). Service packages, not services, are requested and granted.

Service Provider (SP): Consumes an identity for the purpose of providing a service(s) to the identity's principal. The Identity is provided to the SP through an inbound federation from an Identity Provider (IdP).

Signing Algorithm: Signed algorithm that will be used to sign the SAML assertions.

SP Configuration Name: A Service Provider name that can be easily identified by the end user (this is a“user friendly” name)

SP Consumer URL: URL that the assertion will be posted to.

SPML (Service Provisioning Markup Language): An OASIS XML-based framework for exchanging user, resource and service provisioning information between cooperating organizations.