6 February 2015

Partner Beta Demo Guide

Table of Contents

Overview 3

Purpose 3

Definition of Terms 3

Covisint Identity Service (CIS) 3

AppCloud Developer 3

Company 3

Solution 3

Solution Instance 4

Top-Level Package 4

Sub-Package 4

Service 4

Getting Started 4

1. Add a New Security Administrator 5

1.1 Invite a New User 5

1.2 User Accepts the Invitation 6

1.3 Add Security Administrator Role 7

1.4 Grant Portal Package 8

2. Add a New Developer 9

3. Create a New Solution Instance 10

4. Add a New Security Administrator 14

5. Grant Portal Package 14

6. Assign Portal Administrator Role 14

7. Site Content Management 15

7.1 Create a site 16

7.2 Create Site Pages 17

7.3 Change Permissions 19

7.4 Add Content to a Page 20

8. Upload Site Content 22

8.1 Upload Web Content 22

8.2 Upload Documents and Media 24

8.3 Upload Entire Site 27

9. Upload a Portlet 29

10. Secure the Portlet 31

10.1 Create a sub-package 31
10.2 Confirm the User Group in Portal 34
10.3 Create a Role in Portal 35
10.4 Assign the User Group to the Invoice Manage Role 36
10.5 Assign Permissions to Invoice Manager Role 37
11. Access Control for Invoice Portlet 38
11.1 Invite a new user 38
11.2 User Accepts the Invitation 40
11.3 Grant Portal Package 41
11.4 Access the Invoice Portlet 43

Overview

The Covisint B2B cloud platform is designed to allow companies to develop and run custom applications based on Covisint APIs. As part of the platform solution, the customer will be provided with a portal application called AppCloud Developer that will provide administrative control over the platform. It has self-service administrative functions for all of the concepts mentioned in this document.

Purpose

The purpose of this document is to provide general information and step-by-step instructions to Partners on the following items:

- How to create and manage a solution using the AppCloud Developer?
- How to create and manage the site?
- How to upload and secure the Invoice Portlet?

Definition of Terms

Covisint Identity Service (CIS)

Integrates complex systems reaching cloud applications, manage multiple IDs, passwords and integrates across a wide network of constituents, perform administration, and reporting.

AppCloud Developer

AppCloud Developer is a portal application that provides administrative control over the platform. The application is used by both Covisint and external companies that are developing on the platform. It has self-service administrative functions for all of the concepts mentioned in this section. The application requires its own dedicated identity realm, which contains the companies and users that are administering the platform.

Company

A company is either a partner or a customer that is using AppCloud Developer to administer their solutions on the platform. A company is represented by a top-level organization in the AppCloud Developer identity realm. Companies must be invited to join the platform, and during registration, their top-level organizations and initial user account are created. There is also a special company, called the owner company, which contains users who administer the overall platform. This company is created automatically during the creation of the identity realm.

Solution

Solutions are a way of logically grouping related development and administrative efforts together under a single concept. A solution is always associated with a contract, which defines the scope of platform services that will be made available to it. Once a solution is available to a company, they can begin creating solution instances, which will contain the applications and other platform resources dedicated to it. A single solution can have any number of solution instances, and is only limited by what is defined in the contract. A solution also has a repository of deployables, and a set of releases, which are associated to it.

Solution Instance

Solution instances, or just instances as they are more commonly referred to, provide a grouping of platform resources that are intended to run together. Many people think of instances as application environments, as they contain everything needed for an instance of the solution to run, and are generally dedicated to a specific purpose such as development, QA, staging or production. Each instance has a portal and identity realm dedicated to it, and an instance type which identifies if that instance will act in a development, pre-production, or production capacity. Instances contain runtime nodes, and are the target of deployments for releases.

Top-Level Package

It is defined as a group of services and packages that can be requested and granted to an Organization or User. A package acts as a gateway which provides secure access to the applications/services associated with the package.

Sub-Package

It is defined as a group of services that is always associated with a parent package.

Service

It is defined as an application which is always linked with a package. By default, a service is automatically created when a top-level package or a sub-package is created. Services appear in the portal or CIS landing page with its own URL and link name.

Getting Started

For Beta release, Covisint will provide the login credentials for your organization, which could then be used to invite other users to create a solution or a solution instance.

SEED ACCOUNT: ____________________

PASSWORD: ____________________

The seed account has the security administrator role, which means that this account has the ability to invite users, modify roles, or add service packages.

By going through the exercise mentioned in this document, partners should be able to build their own applications using the Covisint Platform. Please follow the steps below.

Go to the learn section to read more about our Portal:
https://portal.beta.developer.covisintlabs.com/web/guest/learn

1. Add a New Security Administrator

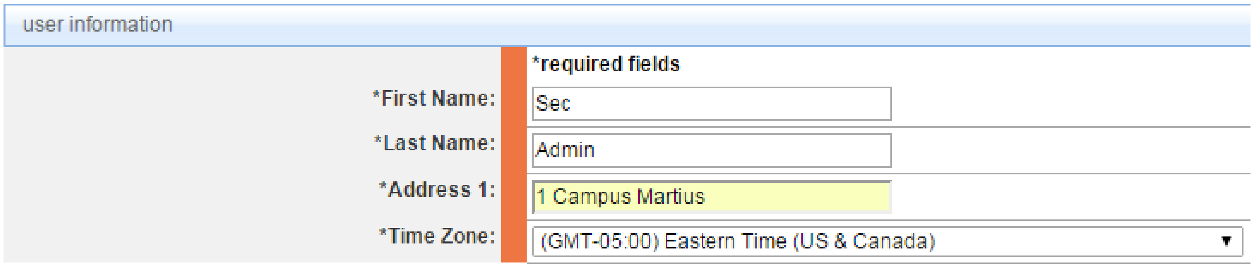
Description: The first step is to create another security administrator within the organization provided by Covisint using the SEED ACCOUNT. The new security administrator will be responsible for creating a new solution.

1.1 Invite a New User

Description: Using the SEED ACCOUNT, invite a new user.

Steps:

1. Log in to Covisint Identity Service (CIS) as a security administrator.
2. Click the **Administration** menu.
3. Click **Invite** and **Invite Users**.
4. Fill in the user information, and click **Next**.



user information

*required fields

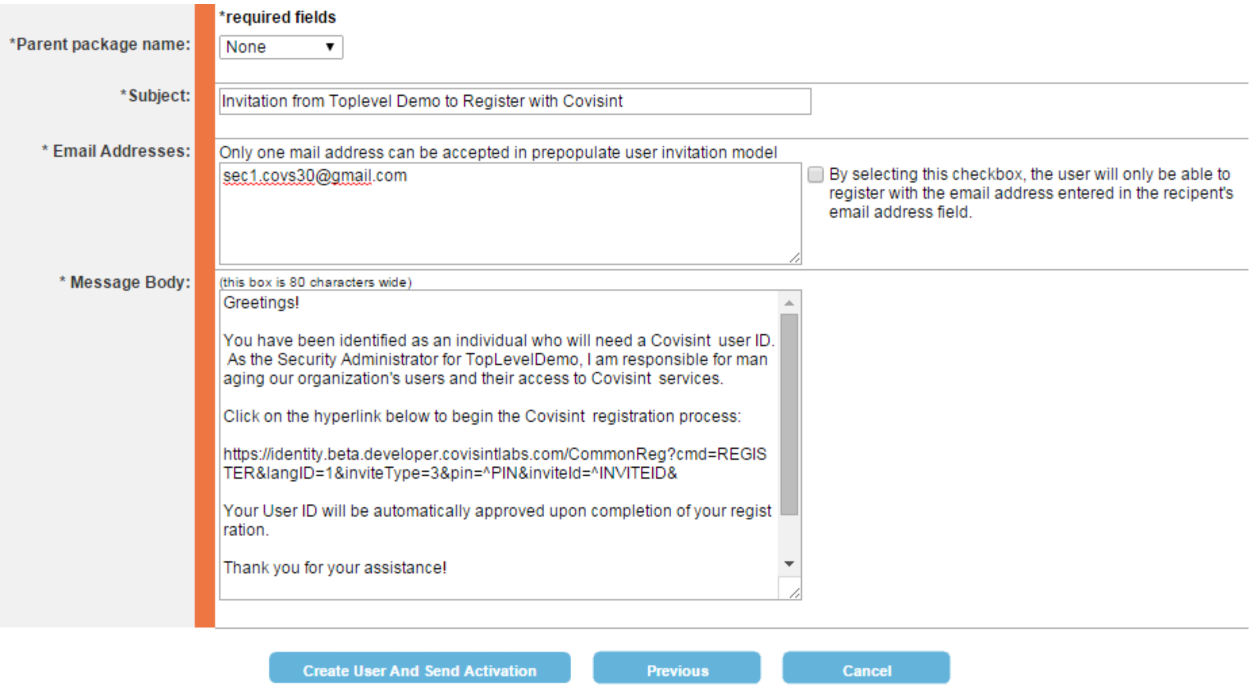
*First Name: Sec

*Last Name: Admin

*Address 1: 1 Campus Martius

*Time Zone: (GMT-05:00) Eastern Time (US & Canada) ▼

5. Key in the user email address and click **Create User** and **Send Activation**.



*required fields

*Parent package name: None ▼

*Subject: Invitation from Toplevel Demo to Register with Covisint

* Email Addresses: Only one mail address can be accepted in prepopulate user invitation model

sec1.covs30@gmail.com

□ By selecting this checkbox, the user will only be able to register with the email address entered in the recipent's email address field.

* Message Body: (this box is 80 characters wide)

Greetings!

You have been identified as an individual who will need a Covisint user ID. As the Security Administrator for TopLevelDemo, I am responsible for man aging our organization's users and their access to Covisint services.

Click on the hyperlink below to begin the Covisint registration process:

https://identity.beta.developer.covisintlabs.com/CommonReg?cmd=REGIS TER&langID=1&inviteType=3&pin=^PIN&inviteId=^INVITEID&

Your User ID will be automatically approved upon completion of your regist ration.

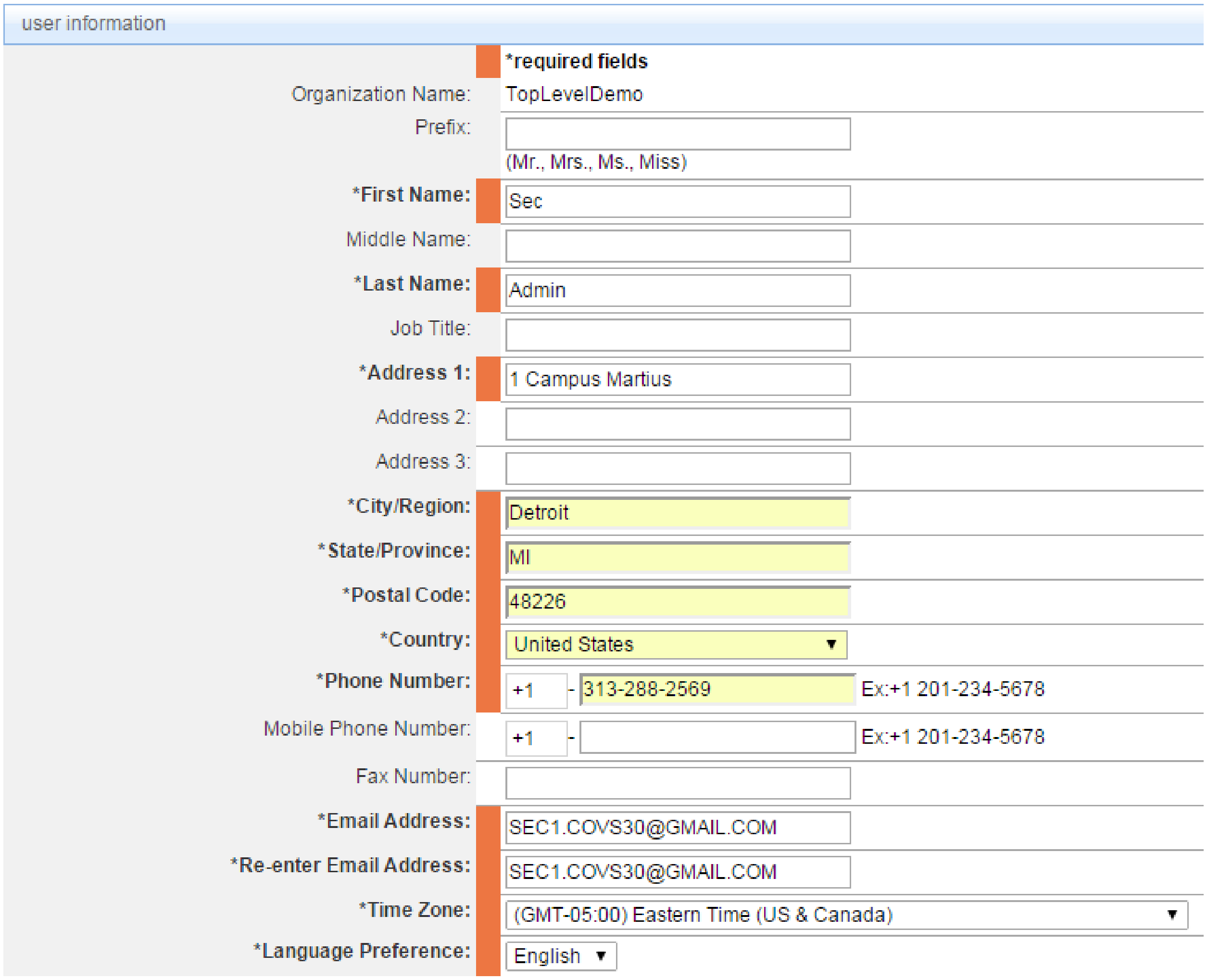
Thank you for your assistance!

1.2 User Accepts the Invitation

Description: Once the invitation is received, the new user should click on the invitation link to complete the user registration process. The registration will be approved by the SEED ADMINISTRATOR, upon which the new user account will be activated in CIS.

Steps:

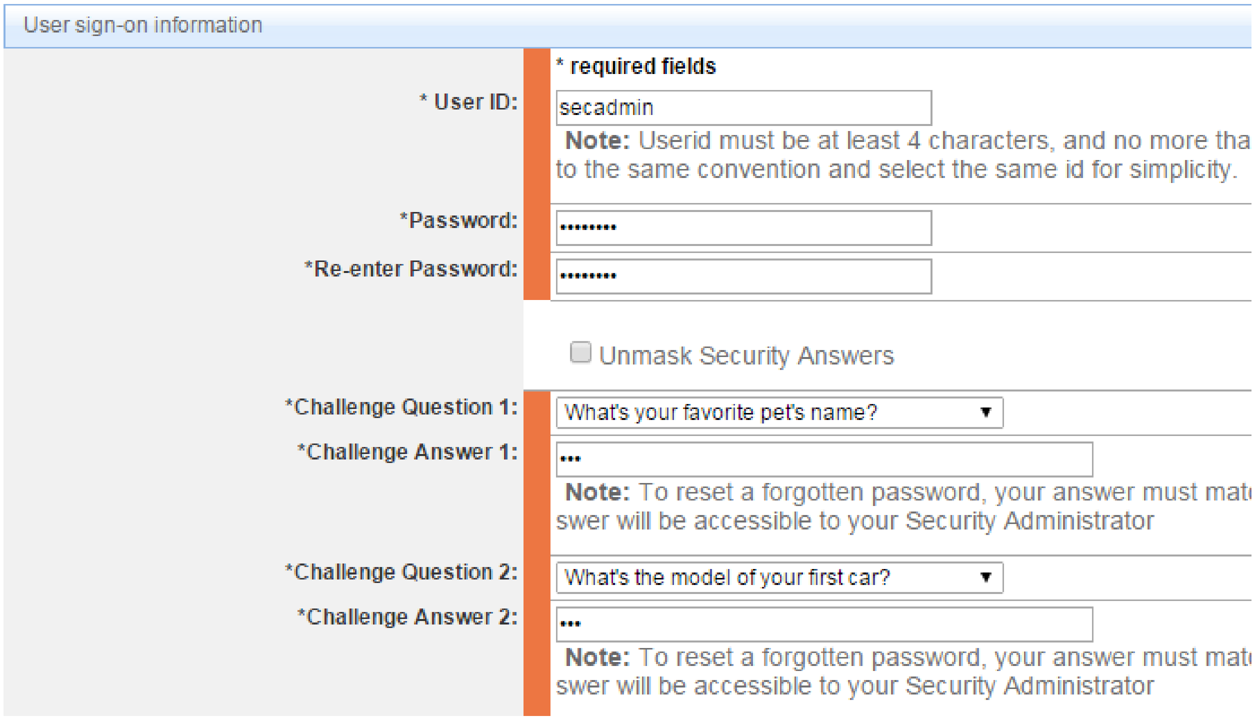
1. The user clicks on the invitation email.
2. Fill in the user information and click **Continue Registration**.



user information

	*required fields
Organization Name:	TopLevelDemo
Prefix:	(Mr., Mrs., Ms., Miss)
*First Name:	Sec
Middle Name:	
*Last Name:	Admin
Job Title:	
*Address 1:	1 Campus Martius
Address 2:	
Address 3:	
*City/Region:	Detroit
*State/Province:	MI
*Postal Code:	48226
*Country:	United States ▼
*Phone Number:	+1 - 313-288-2569 Ex:+1 201-234-5678
Mobile Phone Number:	+1 - Ex:+1 201-234-5678
Fax Number:	
*Email Address:	SEC1.COVS30@GMAIL.COM
*Re-enter Email Address:	SEC1.COVS30@GMAIL.COM
*Time Zone:	(GMT-05:00) Eastern Time (US & Canada) ▼
*Language Preference:	English ▼

3. Fill in the user sign on information and click **Continue Registration**.



User sign-on information

* required fields

* User ID: secadmin

Note: Userid must be at least 4 characters, and no more tha
to the same convention and select the same id for simplicity.

*Password: ••••••••

*Re-enter Password: ••••••••

□ Unmask Security Answers

*Challenge Question 1: What's your favorite pet's name? ▼

*Challenge Answer 1: •••

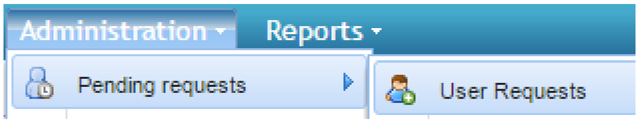
Note: To reset a forgotten password, your answer must mat
swer will be accessible to your Security Administrator

*Challenge Question 2: What's the model of your first car? ▼

*Challenge Answer 2: •••

Note: To reset a forgotten password, your answer must mat
swer will be accessible to your Security Administrator

4. Review the details and click **Submit**.
5. Log in to CIS as a security administrator.
6. Click the **Administration** menu, and then select **Pending requests** and **User Requests**.



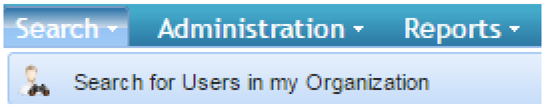
7. Review the request and click **Submit Decision**.

1.3 Add Security Administrator Role

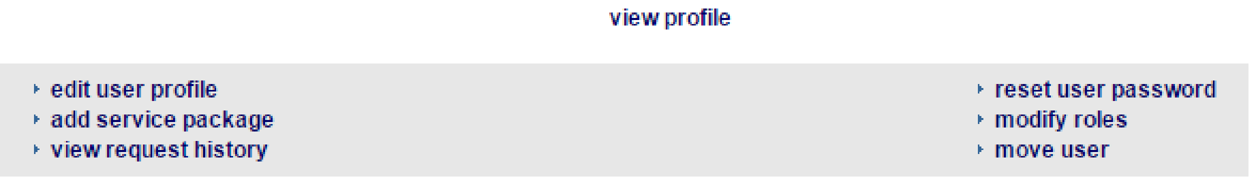
Description: This section illustrates how to add the security administrator role to the new user created in section 1.2.

Steps:

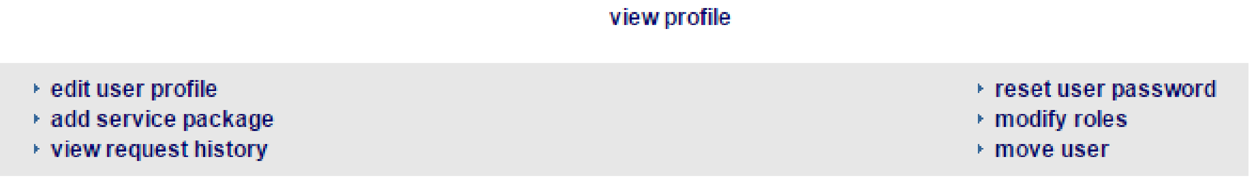
1. Log in to CIS as a Security Administrator.
2. Click the **Search** menu and then **Search for Users in my Organization**.



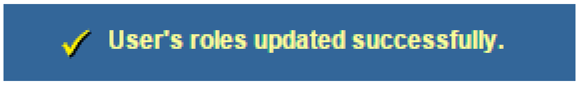
3. Select the desired user and click **modify roles**.



4. Select the **Security Administrator** role and click **Submit**.



5. User’s role has been updated successfully.


User's roles updated successfully.

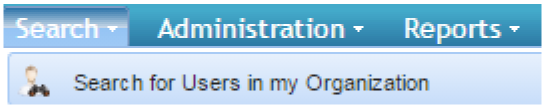
1.4 Grant Portal Package

Description: Grant the portal package to the newly added security administrator so that the administrator can create a new solution instance.

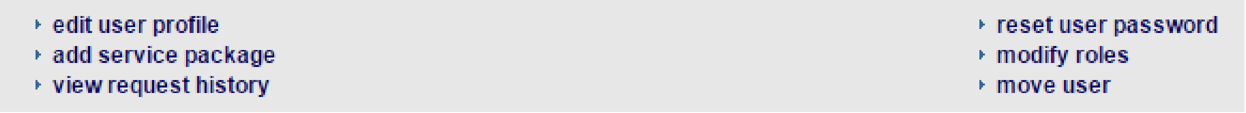
NOTE: The Portal itself is secured by the top-level package called *“DEVELOPE-BETA”*, which is auto-granted to the user at the time of the registration. The solution center on the Portal is secured by the package called *“Develope-Beta portal”*, which should be granted to the desired user by the security administrator.

Steps:

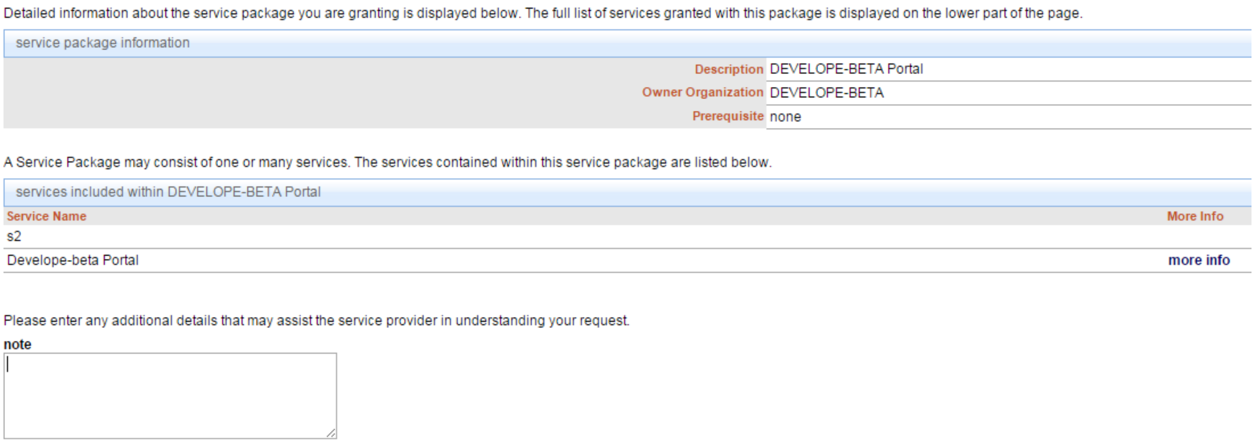
1. Log in to CIS as a security administrator.
2. Click the **Search** menu and then **Search for Users in my Organization**.



3. Click **add service package**.



4. Select **"Develope-Beta portal"** package and click **Add Checked…**
5. Review the service package you’re granting, click **Continue** and then **Submit**.



Detailed information about the service package you are granting is displayed below. The full list of services granted with this package is displayed on the lower part of the page.

service package information

Description	DEVELOPE-BETA Portal
Owner Organization	DEVELOPE-BETA
Prerequisite	none

A Service Package may consist of one or many services. The services contained within this service package are listed below.

services included within DEVELOPE-BETA Portal

Service Name	More Info
s2	
Develope-beta Portal	more info

Please enter any additional details that may assist the service provider in understanding your request.

note

2. Add a New Developer

Description: This section depicts how to add another user in CIS by referring to the steps mentioned in section 1. This user would play the developer role who will be able to access the solution instance created by the security administrator, and execute the development work. In other words, the developer is a regular user in CIS with the portal package grant.

Steps:

1. Invite a new user – Refer to 1.1
2. User accepts the invitation – Refer to 1.2
3. Grant the portal package to this user – Refer to 1.4

3. Create a New Solution Instance

Description: This section illustrates how to create a new solution instance through Covisint Developer Platform using the security administrator account created in section 1. This security administrator is only responsible for creating a new solution instance.

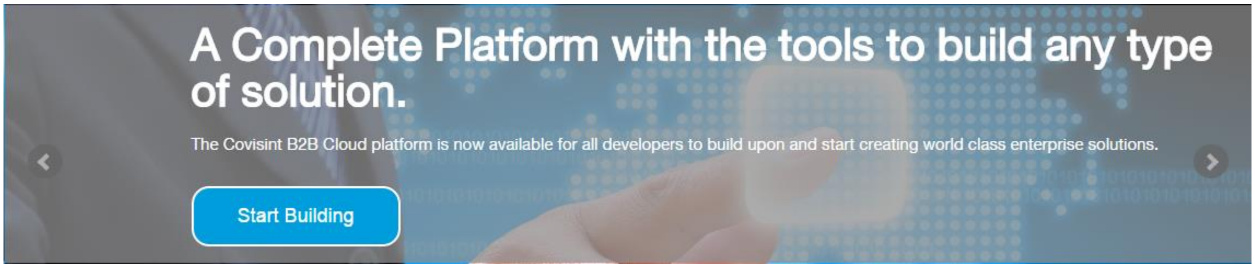
When you build and deploy applications on the platform, you are creating solutions in an environment that includes a rich set of content management and security capabilities that make it easy to create a compelling end-user experience.

NOTE: Do NOT use SEED ACCOUNT to create a solution or a solution instance.

Steps:

1. Log in to https://portal.beta.developer.covisintlabs.com.

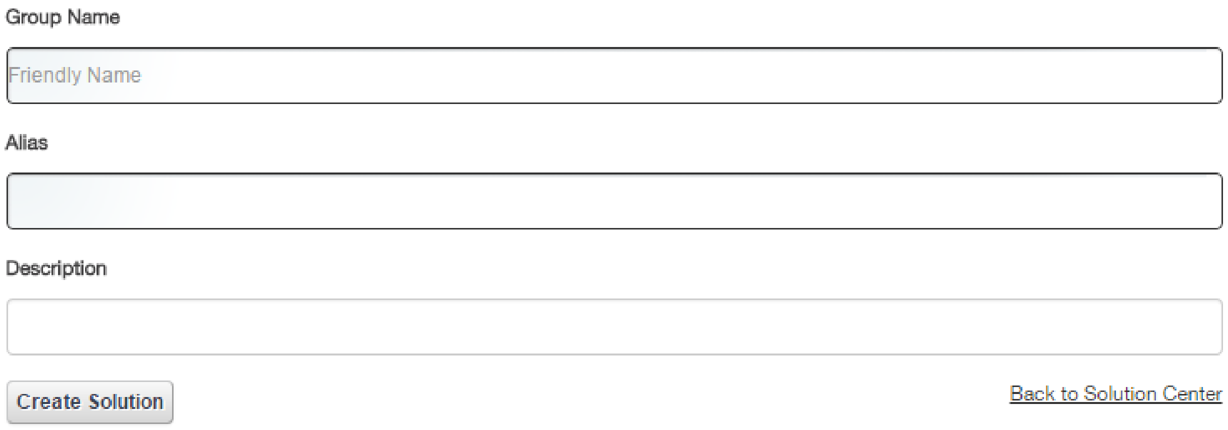
2. Click Start Building. Or go to the **SOLUTION CENTER** tab.



A Complete Platform with the tools to build any type of solution.

The Covisint B2B Cloud platform is now available for all developers to build upon and start creating world class enterprise solutions.

3. Click ⊕ Add new solution
4. Provide a friendly group name in the field "**Group Name**".
5. Provide a solution alias name in the field "**Alias**".
6. Provide a description in the field "**Description**".
7. Click Create Solution



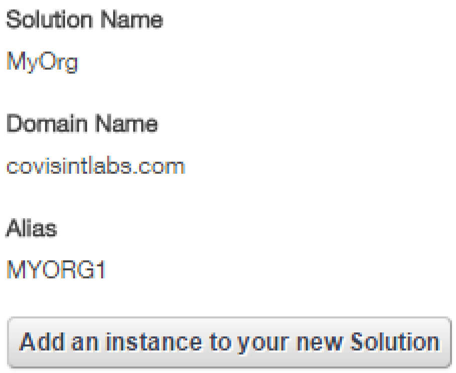
Group Name

Friendly Name

Alias

Description

8. Review the details and click Add an instance to your new Solution.

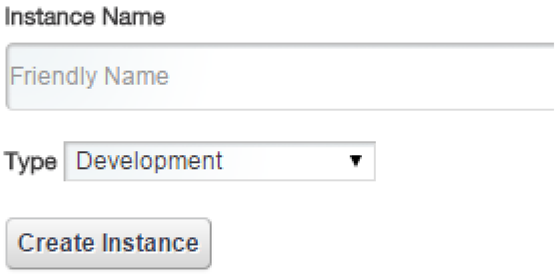


Solution Name
MyOrg

Domain Name
covisintlabs.com

Alias
MYORG1

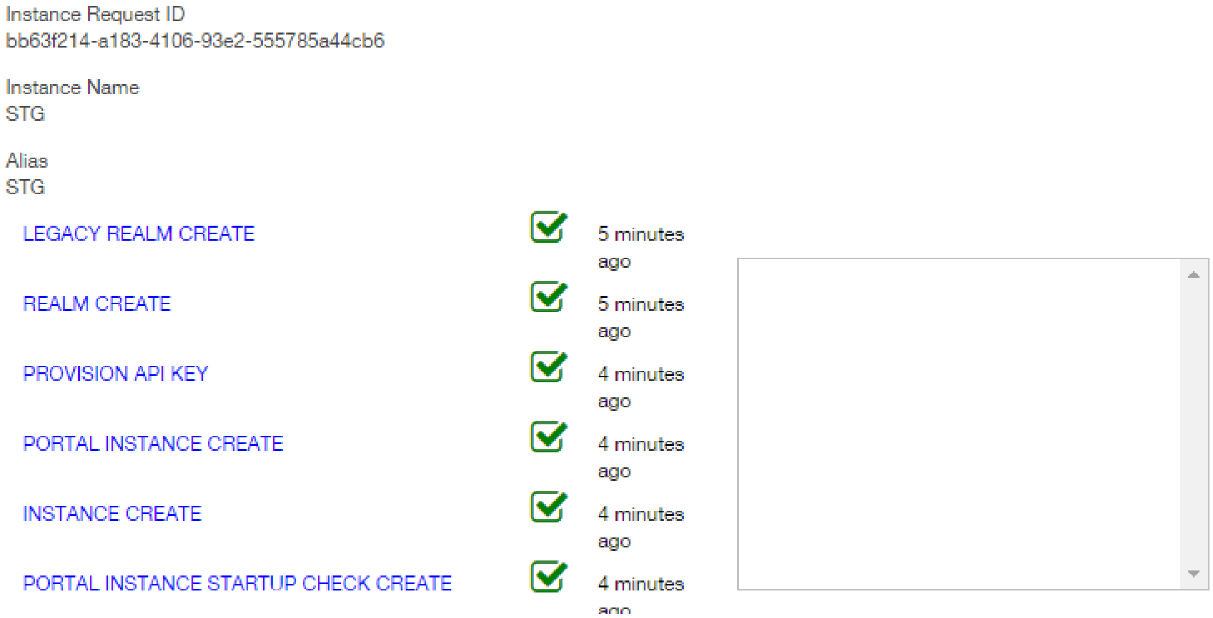
9. Enter the **Instance Name**, select the environment type from the drop-down menu next to **Type**, and click Create Instance.



Instance Name
Friendly Name

Type Development ▼

10. The instance creation does the following background work to set up the instance:
    a. Create Realm
    b. Create Portal



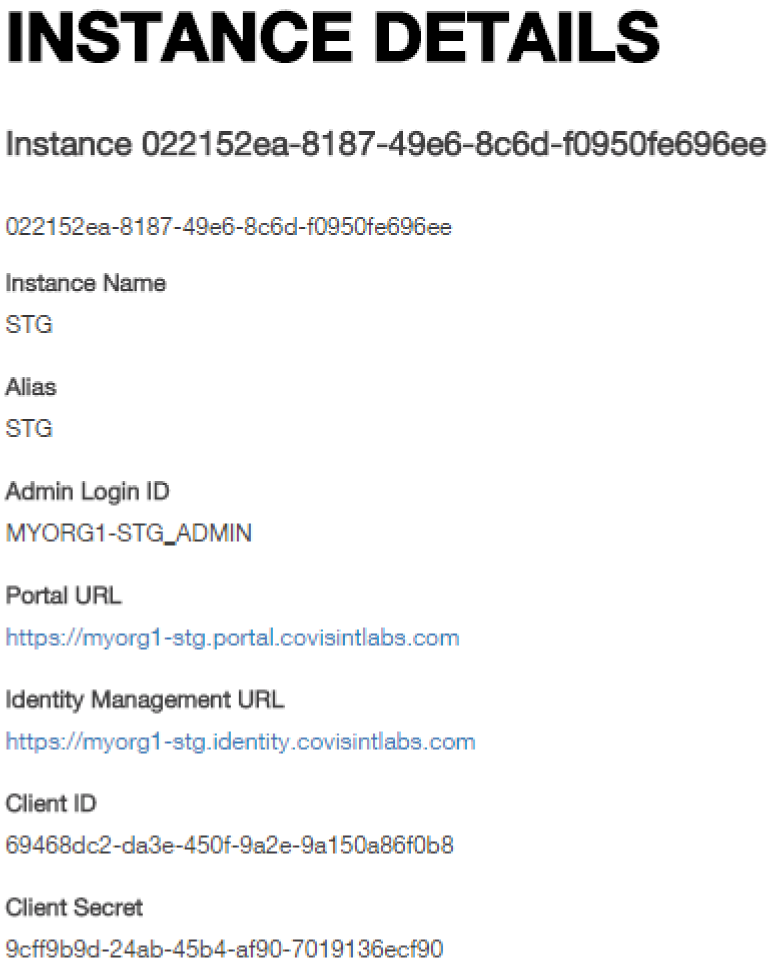
Instance Request ID
bb63f214-a183-4106-93e2-555785a44cb6

Instance Name
STG

Alias
STG

LEGACY REALM CREATE	☑	5 minutes ago
REALM CREATE	☑	5 minutes ago
PROVISION API KEY	☑	4 minutes ago
PORTAL INSTANCE CREATE	☑	4 minutes ago
INSTANCE CREATE	☑	4 minutes ago
PORTAL INSTANCE STARTUP CHECK CREATE	☑	4 minutes ago

11. Your solution has been created successfully. Note down the solution details for your reference. The admin login Id is always “SOLUTION ALIAS-INSTANCE ALIAS_ADMIN”, and the default password is “Covisint$2015”. This is the SEED ACCOUNT for this solution instance.



INSTANCE DETAILS

Instance 022152ea-8187-49e6-8c6d-f0950fe696ee

022152ea-8187-49e6-8c6d-f0950fe696ee

Instance Name
STG

Alias
STG

Admin Login ID
MYORG1-STG_ADMIN

Portal URL
https://myorg1-stg.portal.covisintlabs.com

Identity Management URL
https://myorg1-stg.identity.covisintlabs.com

Client ID
69468dc2-da3e-450f-9a2e-9a150a86f0b8

Client Secret
9cff9b9d-24ab-45b4-af90-7019136ecf90

4. Add a New Security Administrator

Description: Once the solution instance is created, use the admin login Id (created in section 3, step# 11) to add a new security administrator in this instance who will be responsible for the development work on this particular instance. Please refer to the steps mentioned in section 1 to create this user.

NOTE: Do NOT use the admin account that was created in section 3 to perform the following steps.

Steps:

1. Invite a new user – Refer to 1.1
2. User accepts the invitation – Refer to 1.2
3. Add the security administrator role – Refer to 1.3
4. Grant the portal package to this user – Refer to 1.4

5. Grant Portal Package

NOTE: By default, the top-level package name for a new solution instance that secures your Portal is "SOLUTION ALIAS-INSTANCE ALIAS", and the package that secures your Solution Center is "SOLUTION ALIAS-INSTANCE ALIAS Portal".

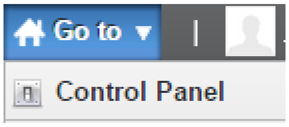
In order to access the solution center, grant the "SOLUTION ALIAS-INSTANCE ALIAS Portal" package to the newly created security administrator in section 4. Please refer to section 1.4 to perform the steps of granting the portal package.

6. Assign Portal Administrator Role

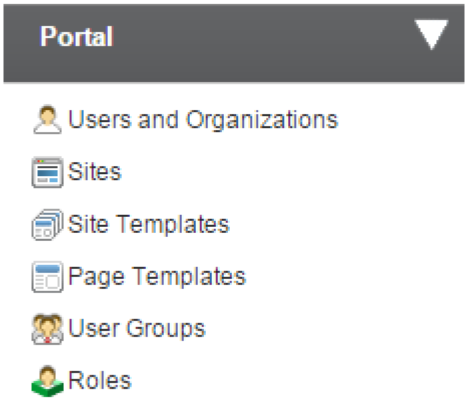
Description: Assign the portal administrator role to the newly created security administrator who will be responsible for site configuration and management in the new solution instance. Use the admin account that was created in section 3 to perform the steps mentioned in this section.

Steps:

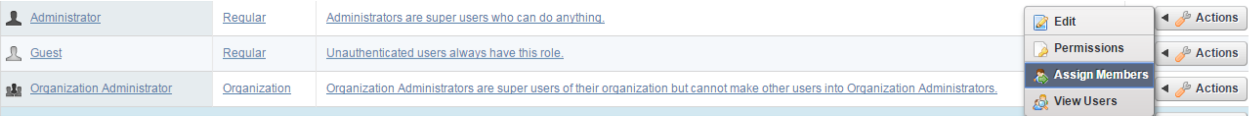
1. Log in to the Portal instance using the admin account.
2. Click the **Go to** menu and select **Control Panel**.



3. On the left side, under Portal section, click **Roles**.

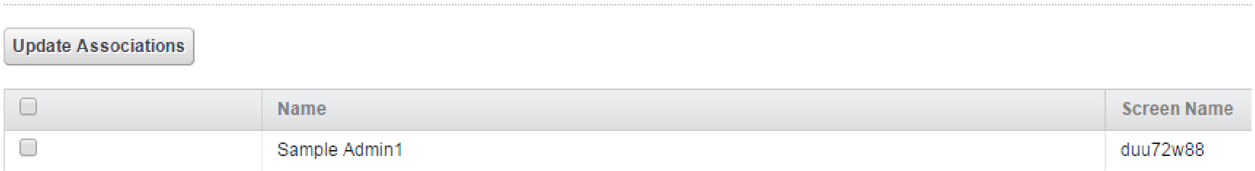


4. Click **Actions** corresponding to Administrator, and select **Assign Members**.



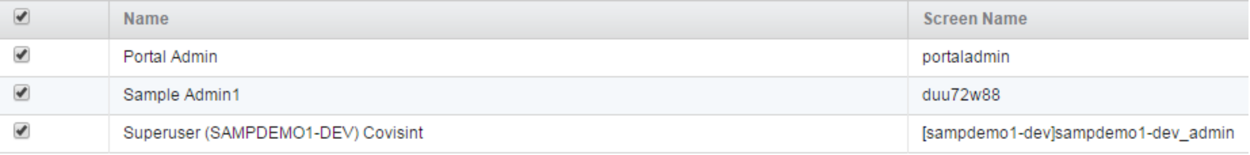
Administrator	Regular	Administrators are super users who can do anything.
Guest	Regular	Unauthenticated users always have this role.
Organization Administrator	Organization	Organization Administrators are super users of their organization but cannot make other users into Organization Administrators.

5. Search for the desired user, click the **Available** tab, check the box beside the desired name, and click **Update Associations**.



☐	Name	Screen Name
☐	Sample Admin1	duu72w88

6. You have successfully added the portal administrator role to the user.



☑	Name	Screen Name
☑	Portal Admin	portaladmin
☑	Sample Admin1	duu72w88
☑	Superuser (SAMPDEMO1-DEV) Covisint	[sampdemo1-dev]sampdemo1-dev_admin

7. Site Content Management

Description: This section illustrates how to quickly create and manage rich web content using the Portal Administrator role.

An unlimited number of web pages can be created in the portal.

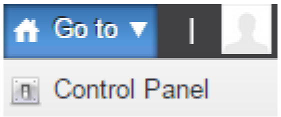
Page Types:

- Public Pages – Public pages can be exposed to unauthenticated users (Guest) or authenticated users; Public pages can be secured by role/service package if required.
- Private Pages – Private pages can only be seen by users with at least one Site role.
- User Pages – Users can enable private pages and public pages as part of their profile that can include all of the Social Network portlets

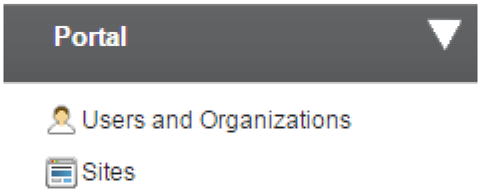
7.1 Create a site

Steps:

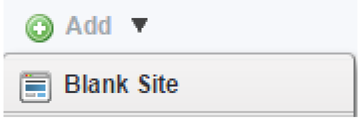
1. Click the **Go to** menu and select **Control Panel**.



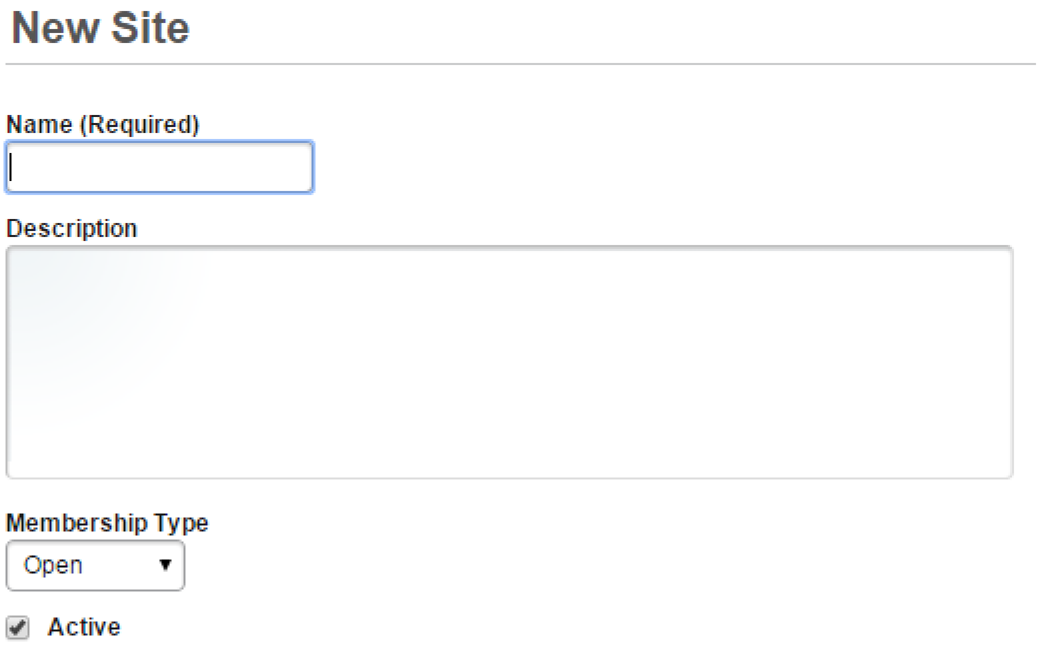
2. On the left side, under Portal section, click **Sites**.



3. Click the **Add** menu and select **Blank Site**.



4. Enter the site name, description, select **Open**, and check **Active**. Then, click **Save** to save the site.



New Site

Name (Required)

Description

Membership Type
Open

☑ Active

5. You have successfully created a new site.

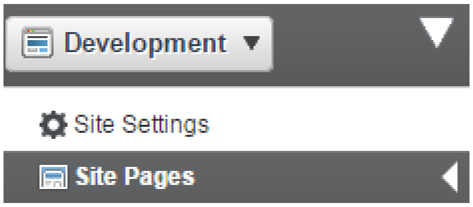
7.2 Create Site Pages

Each Site has its own set of pages, public and private. Pages can be individually styled with one of the available page layouts, a unique theme, CSS, and JavaScript.

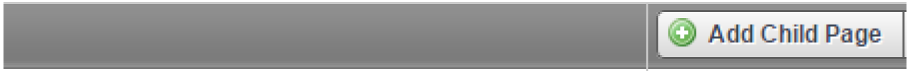
For purposes of this Beta release, public pages are used for all of the content. Pages may all share a common look and feel or can be independently styled. When using the dynamic theme, only one dynamic theme can be paired with a user, and only set of dynamic theme settings can be used in a particular site. Manual CSS and JavaScript can be applied to a site.

Steps:

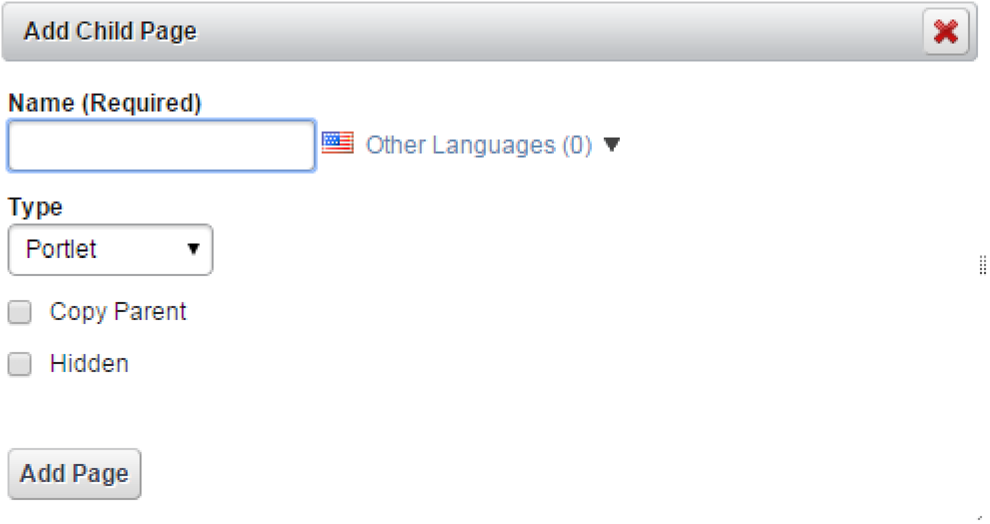
1. Select the desired site and click **Site Pages**.



2. Click **Add Child Page**.



3. Enter the **Name**, select **Portlet** from the drop down menu, and click **Add Page**.


Add Child Page

Name (Required)

Other Languages (0) ▼

Type

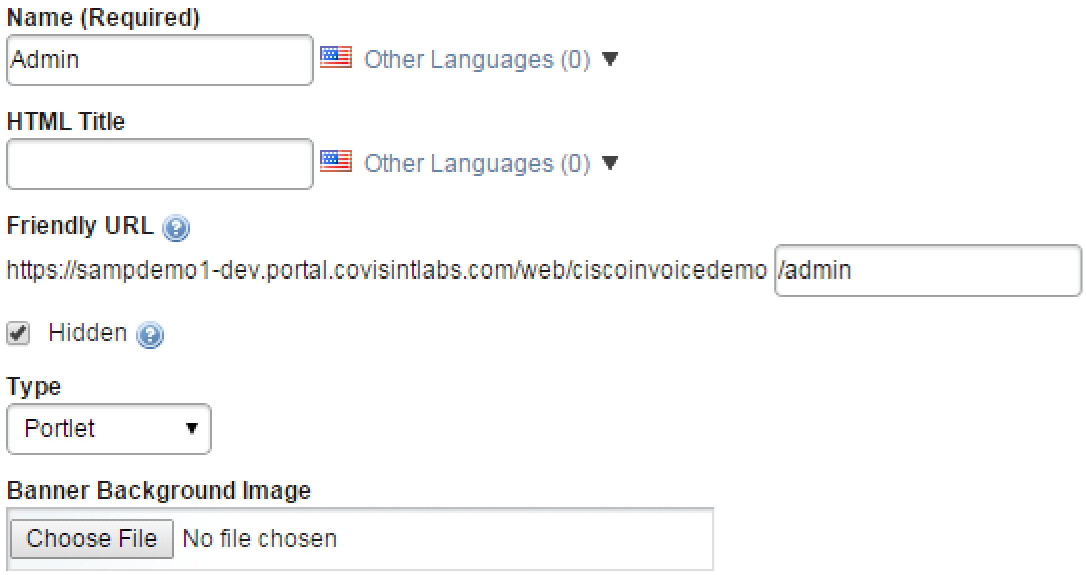
Portlet ▼

☐ Copy Parent

☐ Hidden

4. You have successfully created a child page.
5. Create child pages for **Welcome**, **Invoice**, **Contact**, **Admin.**

6. For the **Admin** child page, check the **Hidden** checkbox. This page will usually contain portlets for administration content.



Name (Required)

Admin

HTML Title

Friendly URL

https://sampdemo1-dev.portal.covisintlabs.com/web/ciscoinvoicedemo /admin

☑ Hidden

Type

Portlet

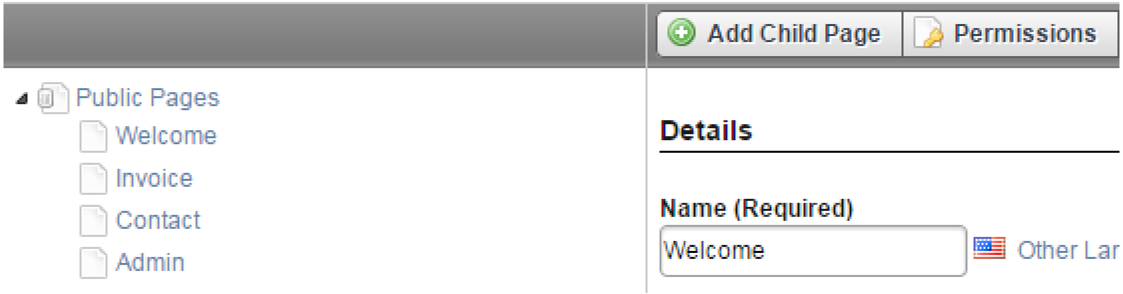
Banner Background Image

No file chosen

7.3 Change Permissions

Description: Set the appropriate permissions based on the available roles. You can improve the access to and sharing of information stored within your organization with the help of permissions.

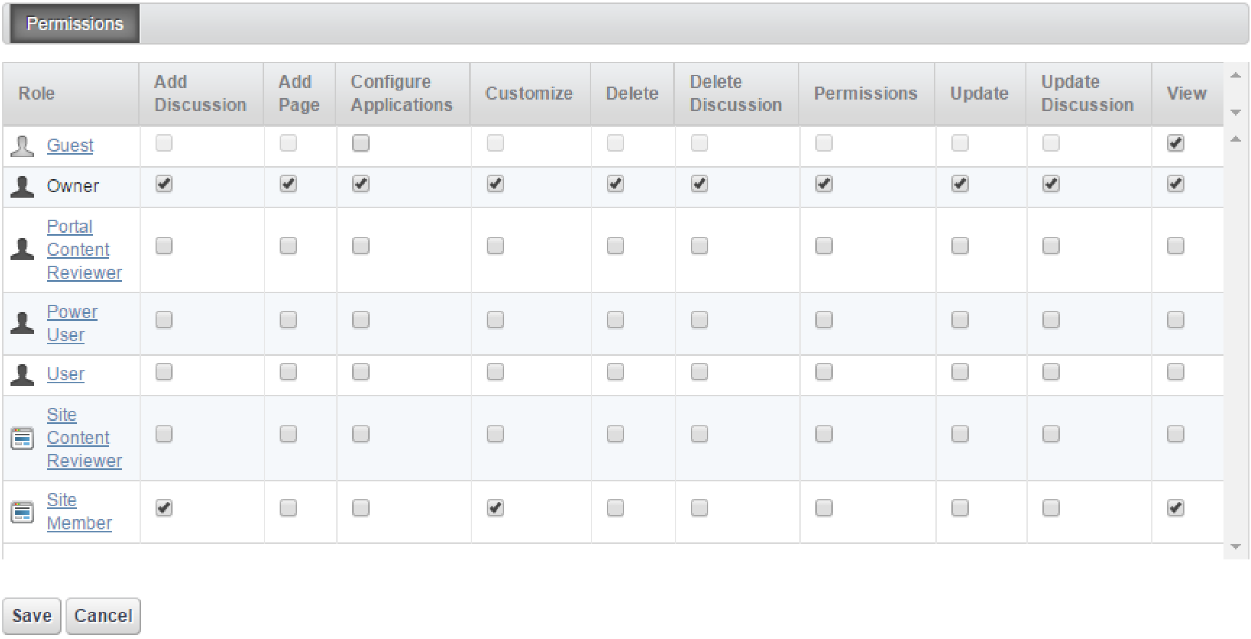
Steps: Click the **Permissions** tab.



Details

Name (Required): Welcome

1. Verify the permissions as shown in the screenshot below and click **Save**.

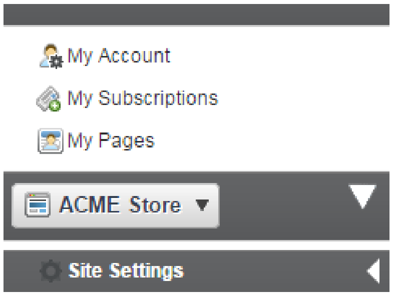


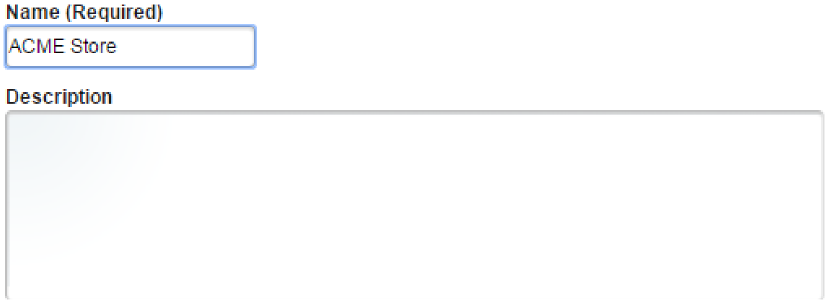
Role	Add Discussion	Add Page	Configure Applications	Customize	Delete	Delete Discussion	Permissions	Update	Update Discussion	View
Guest	□	□	□	□	□	□	□	□	□	☑
Owner	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Portal Content Reviewer	□	□	□	□	□	□	□	□	□	□
Power User	□	□	□	□	□	□	□	□	□	□
User	□	□	□	□	□	□	□	□	□	□
Site Content Reviewer	□	□	□	□	□	□	□	□	□	□
Site Member	☑	□	□	☑	□	□	□	□	□	☑

7.4 Add Content to a Page

Steps:

1. Go to the site URL. To get the site URL, go to **Site Settings**, and note down the site name from the **Name** field.



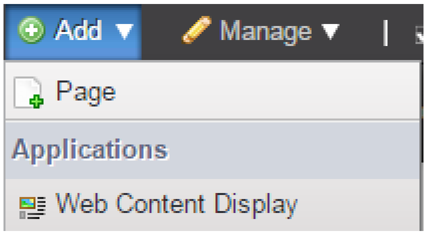


Name (Required)

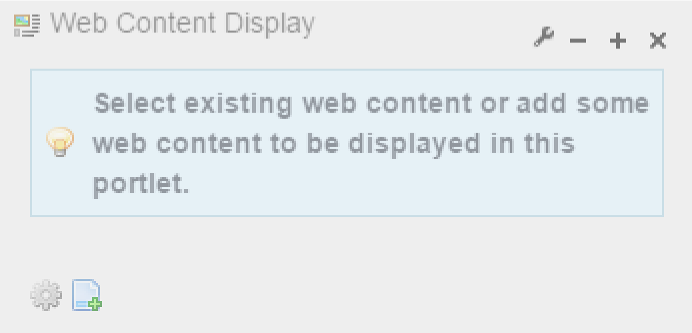
ACME Store

Description

2. Go to https://sampdemo1-dev.portal.covisintlabs.com/web/<siteName>.
3. Click the **Add** menu and select **Web Content Display**.

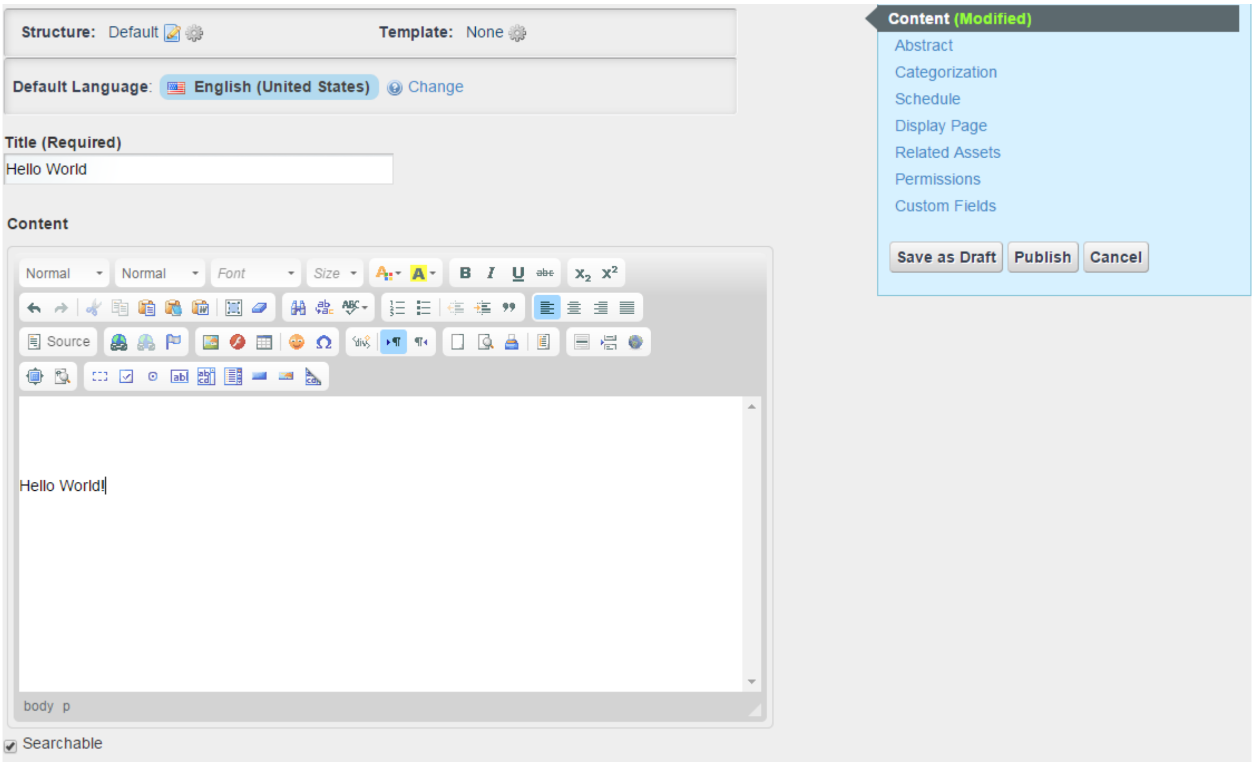


4. Click to add the content.



Select existing web content or add some web content to be displayed in this portlet.

5. Enter the **Title** and the **Content.** Click **Publish**.

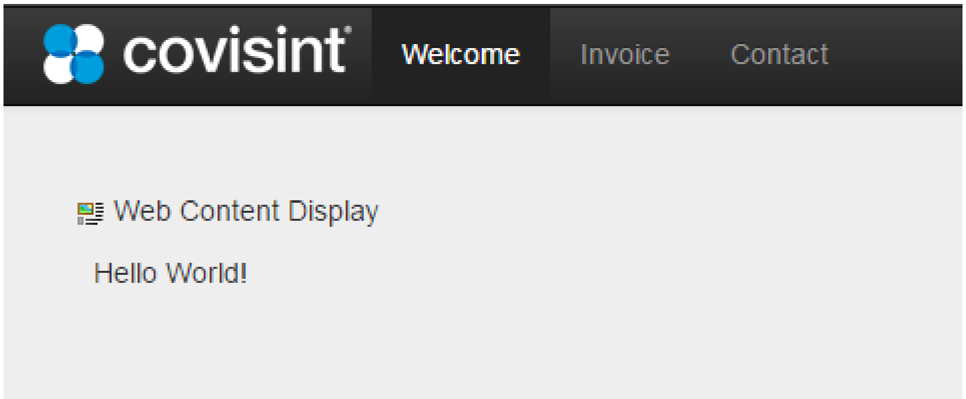


Title (Required)
Hello World

Content

Hello World!

6. You have successfully added the content to the **Welcome** page.



Hello World!

8. Upload Site Content

Description: You can upload three types of contents via a LAR file 1) Web Content 2) Documents and Media, and 3) Entire Site. Be careful not to confuse portlet-specific .lar files with site-specific .lar files. This section depicts how to upload these contents.

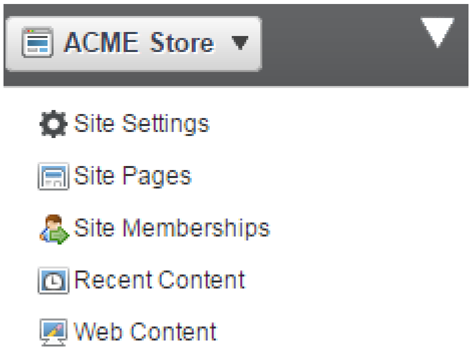
NOTE: To use our sample pre-configured theme, click here https://github.com/Covisint/developer-demo

8.1 Upload Web Content

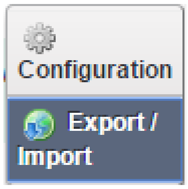
Description: You can upload the web content via a LAR file.

Steps:

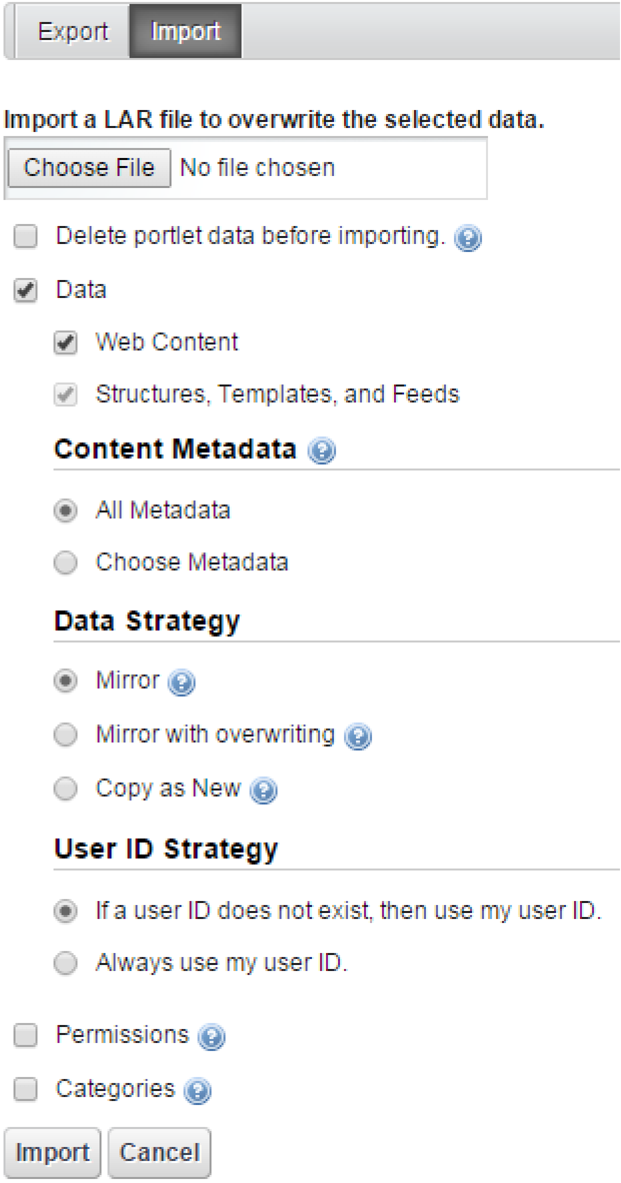
1. Log in to your site as a Portal Administrator.
2. Under your site section, click **Web Content**.



3. On the right corner, click 🔧 and select **Export/Import**.



4. Click the **Import** tab, select Choose File to select the desired LAR file. Then, click **Import**.



Import a LAR file to overwrite the selected data.

Choose File No file chosen

□ Delete portlet data before importing.

☑ Data

☑ Web Content

☑ Structures, Templates, and Feeds

Content Metadata

● All Metadata

○ Choose Metadata

Data Strategy

● Mirror

○ Mirror with overwriting

○ Copy as New

User ID Strategy

● If a user ID does not exist, then use my user ID.

○ Always use my user ID.

□ Permissions

□ Categories

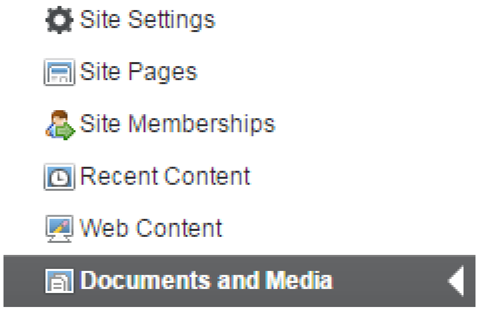
5. You have successfully imported the Web Content.

8.2 Upload Documents and Media

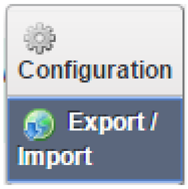
Description: You can upload documents and media via a LAR file.

Steps:

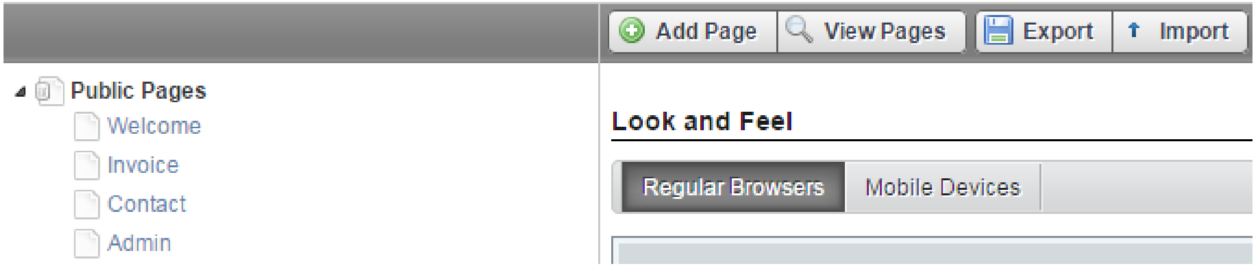
1. Log in to your site as a Portal Administrator.
2. Under your site section, click **Documents and Media**.



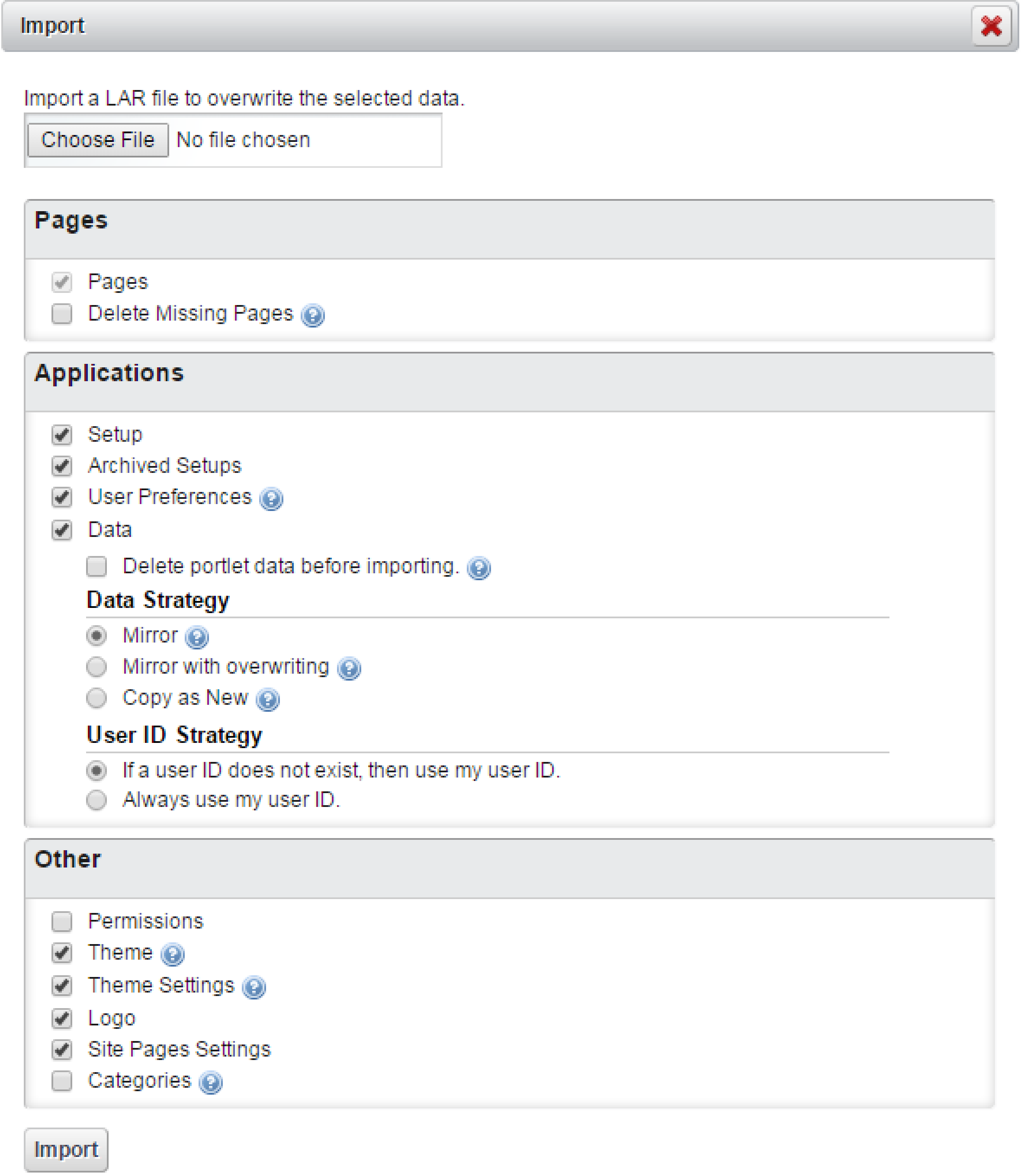
3. On the right corner, click 🔧 and select **Export/Import**.



4. Click **Public Pages** and then click **Import**.



5. Choose the LAR file and then click **Import**.



Import

Import a LAR file to overwrite the selected data.

Choose File No file chosen

Pages

☑ Pages
□ Delete Missing Pages

Applications

☑ Setup
☑ Archived Setups
☑ User Preferences
☑ Data
□ Delete portlet data before importing.

Data Strategy

● Mirror
○ Mirror with overwriting
○ Copy as New

User ID Strategy

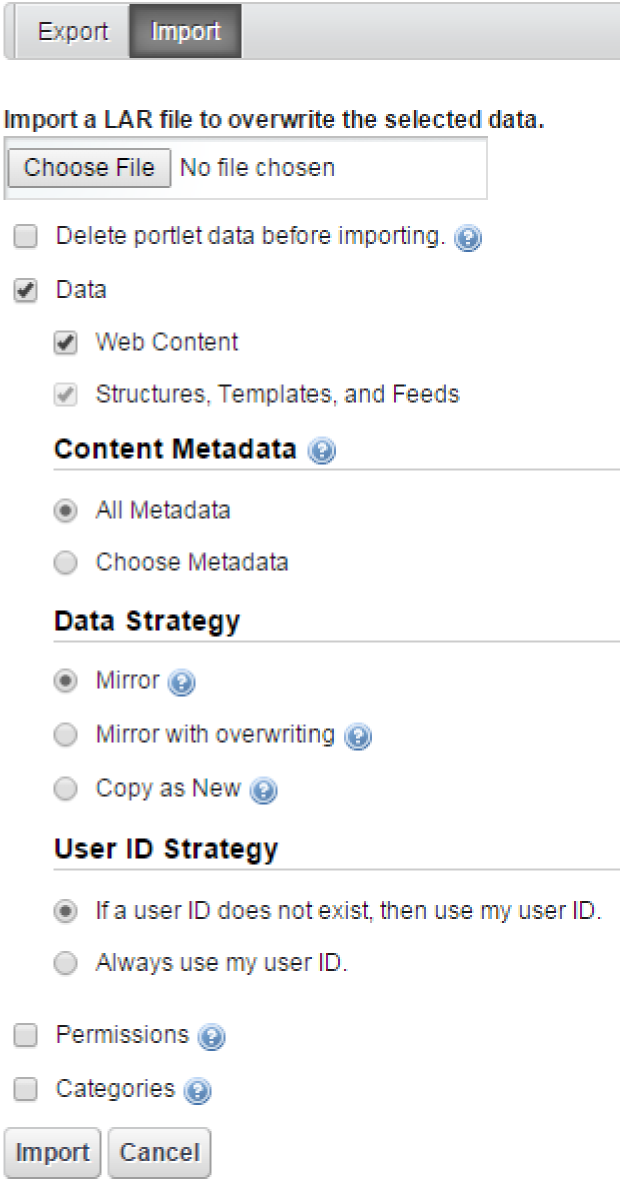
● If a user ID does not exist, then use my user ID.
○ Always use my user ID.

Other

□ Permissions
☑ Theme
☑ Theme Settings
☑ Logo
☑ Site Pages Settings
□ Categories

Import

6. Click the **Import** tab, select Choose File to select the desired LAR file. Then, click **Import**.



Import a LAR file to overwrite the selected data.

Choose File No file chosen

□ Delete portlet data before importing.

☑ Data

- ☑ Web Content
- ☑ Structures, Templates, and Feeds

Content Metadata

- ● All Metadata
- ○ Choose Metadata

Data Strategy

- ● Mirror
- ○ Mirror with overwriting
- ○ Copy as New

User ID Strategy

- ● If a user ID does not exist, then use my user ID.
- ○ Always use my user ID.

□ Permissions

□ Categories

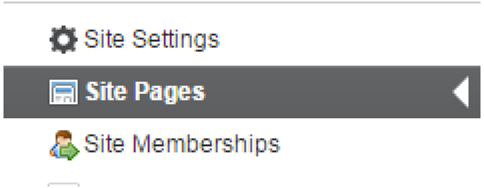
7. You have successfully imported documents and media.

8.3 Upload Entire Site

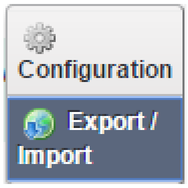
Description: You can upload the entire site via a LAR file.

Steps:

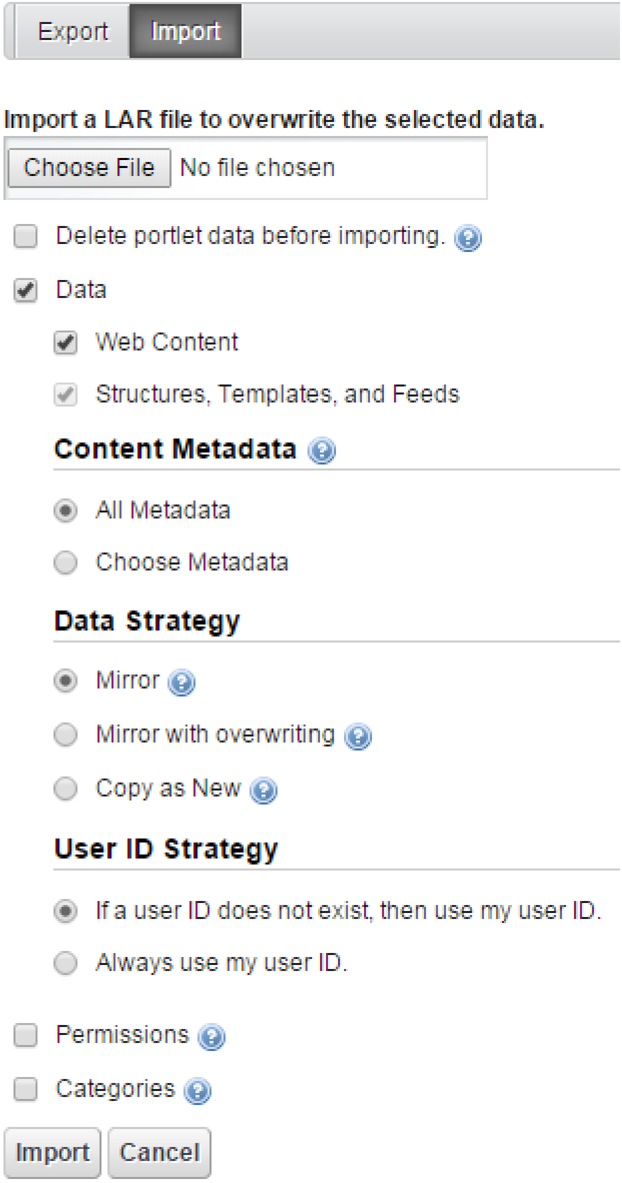
1. Log in to your site as a Portal Administrator.
2. Under your site section, click **Web Content**.



3. On the right corner, click 🔧 and select **Export/Import**.



4. Click the **Import** tab, select Choose File to select the desired LAR file. Then, click **Import**.



Import a LAR file to overwrite the selected data.

Choose File No file chosen

□ Delete portlet data before importing.

☑ Data

☑ Web Content

☑ Structures, Templates, and Feeds

Content Metadata

● All Metadata

○ Choose Metadata

Data Strategy

● Mirror

○ Mirror with overwriting

○ Copy as New

User ID Strategy

● If a user ID does not exist, then use my user ID.

○ Always use my user ID.

□ Permissions

□ Categories

5. You have successfully imported the Web Content.

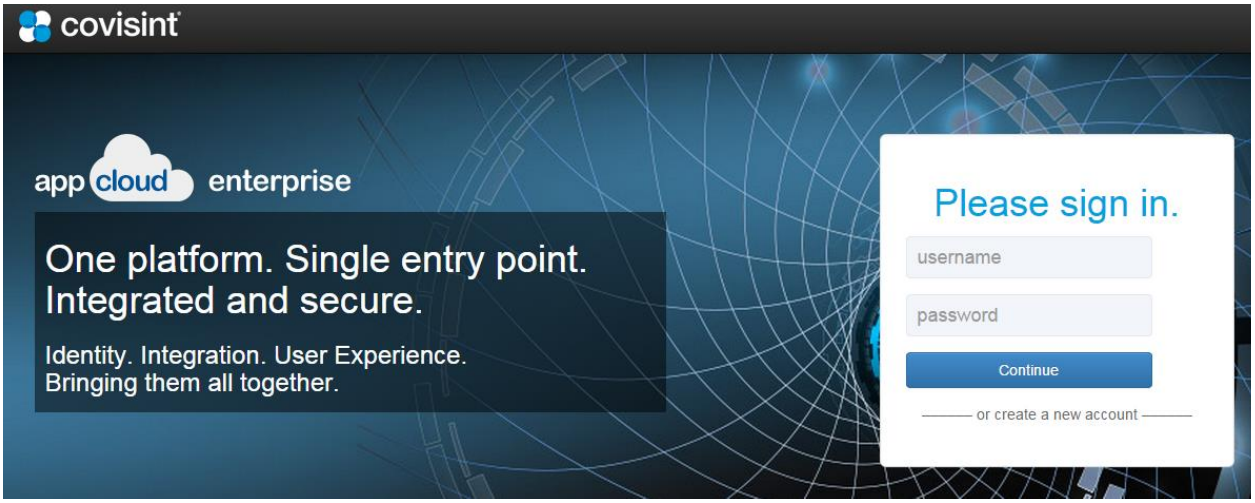
9. Upload a Portlet

Description: This section illustrates how you can import a portlet using the portlet-specific LAR file.

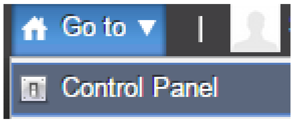
NOTE: To use the sample portlet, click here https://github.com/Covisint/developer-demo

Steps:

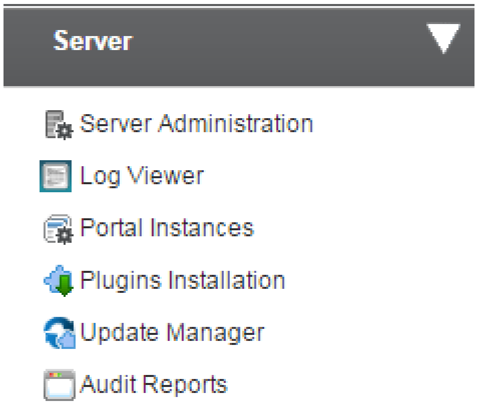
1. Log into Covisint Portal App Cloud.



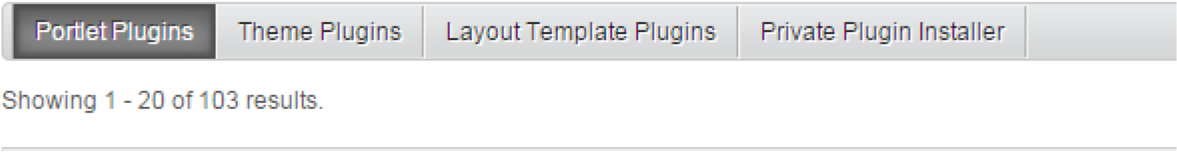
2. Click **Go to** and **Control Panel**.



3. Click **Plugins Installation**.

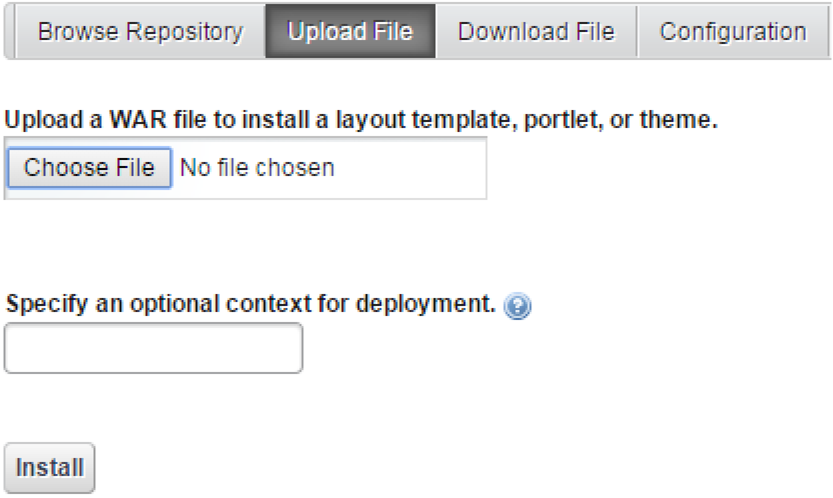


4. Click **Private Plugin Installer**.



Showing 1 - 20 of 103 results.

5. Click **Upload File**, and then choose a WAR file to install a layout template, and click **Install**.



Upload a WAR file to install a layout template, portlet, or theme.

No file chosen

Specify an optional context for deployment.

10. Secure the Portlet

Description: Securing the invoice portlet is a five-step process. The following section describes how to provision your portlet based on service packages.

10.1 Create a sub-package

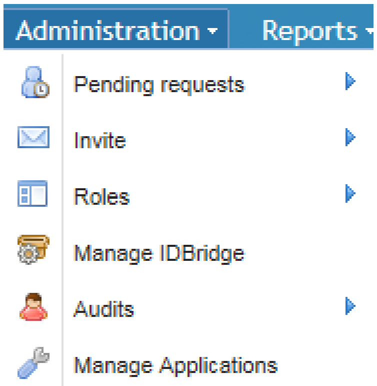
Description: Create a sub-package in CIS to secure your portlet.

NOTES:

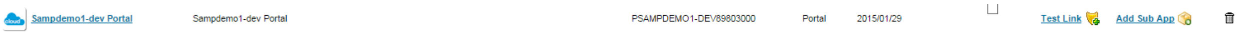
1. Set the **Federation Connection** to **None**.
2. Don't key in any URL.

Steps:

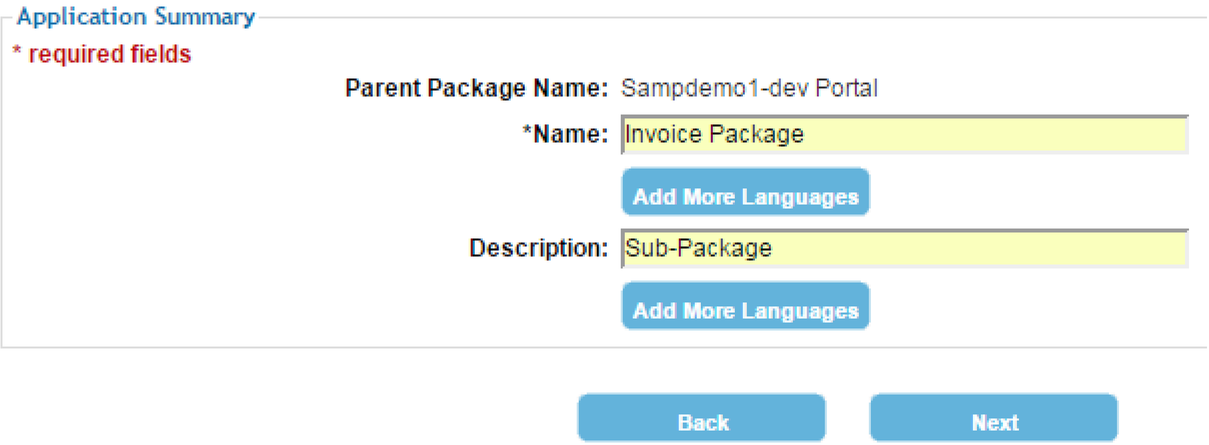
1. Log in to CIS as a Security Administrator.
2. Click the **Administration** menu and select **Manage Applications**.



3. Click Add **Sub App.**


Sampdemo1-dev Portal   Sampdemo1-dev Portal   PSAMPDEMO1-DEV89803000   Portal   2015/01/29   □   Test Link   Add Sub App

4. Enter the Package Name and the Description. Click **Next**.


Application Summary

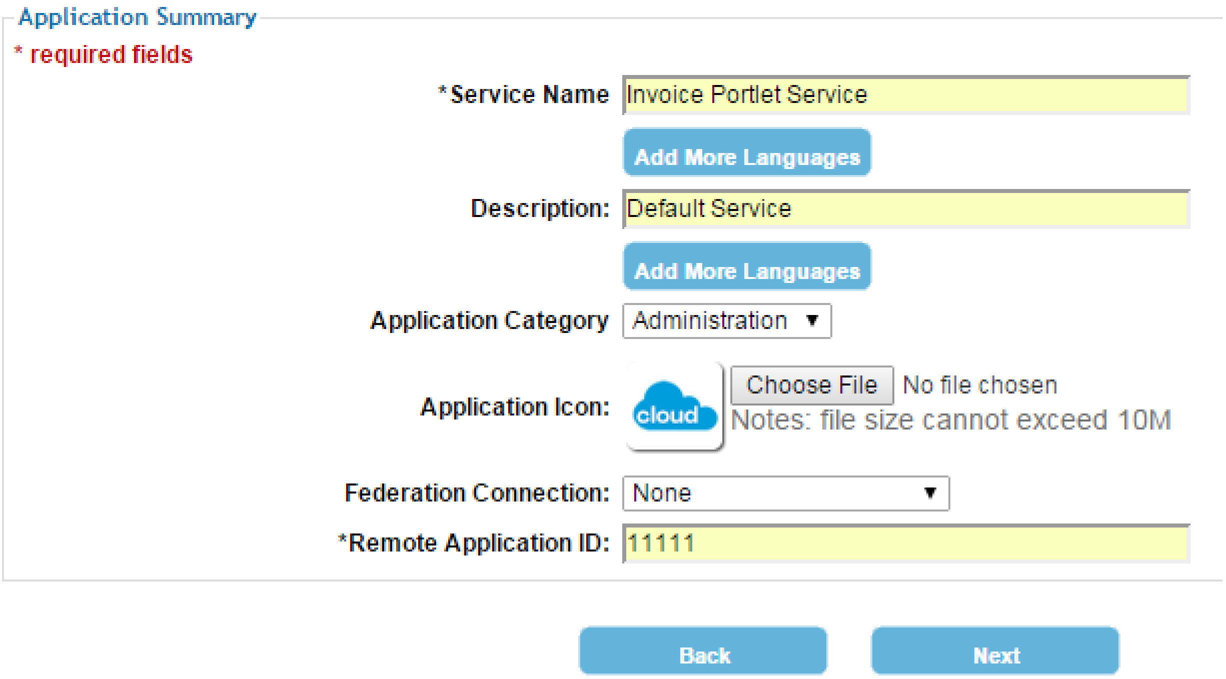
* required fields

Parent Package Name: Sampdemo1-dev Portal

*Name: Invoice Package

Description: Sub-Package

5. Enter the details as shown in the screenshot below and click **Next**.



Application Summary

* required fields

*Service Name: Invoice Portlet Service

Description: Default Service

Application Category: Administration ▼

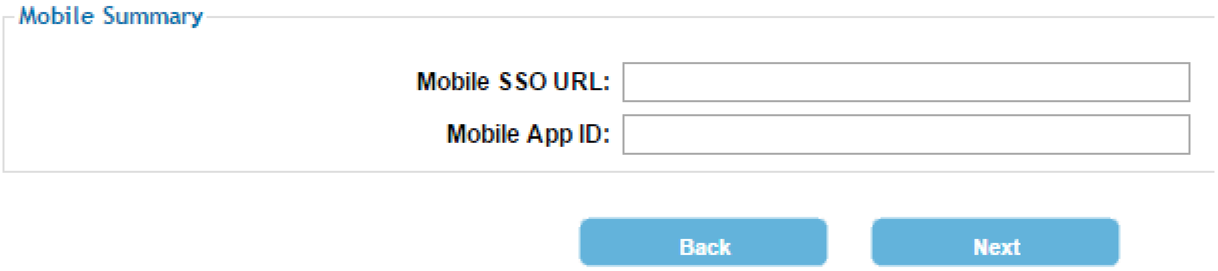
Application Icon:

Notes: file size cannot exceed 10M

Federation Connection: None ▼

*Remote Application ID: 11111

6. Skip the **Mobile Summary** screen. Click **Next**.

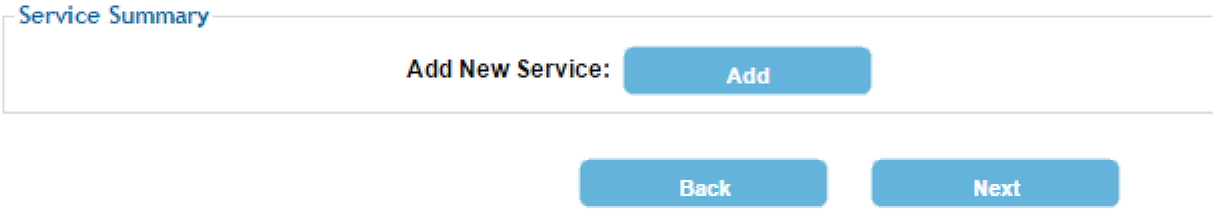


Mobile Summary

Mobile SSO URL:

Mobile App ID:

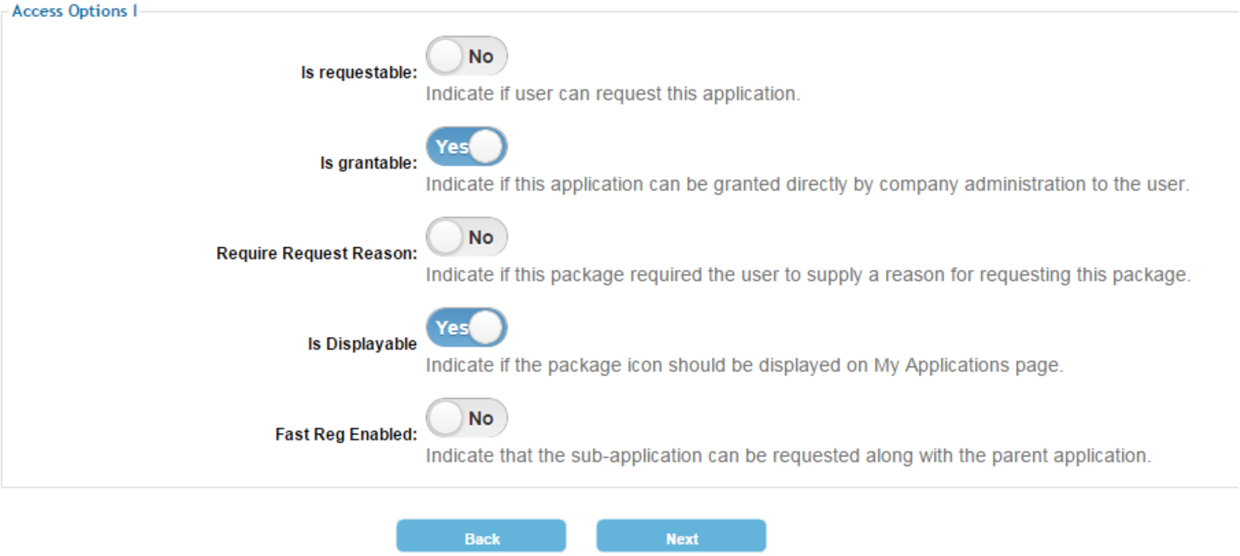
7. Skip the **Service Summary** screen. Click **Next**.



Service Summary

Add New Service:

8. Set the access options I as shown in the screenshot below.



Access Options I

Is requestable: No
Indicate if user can request this application.

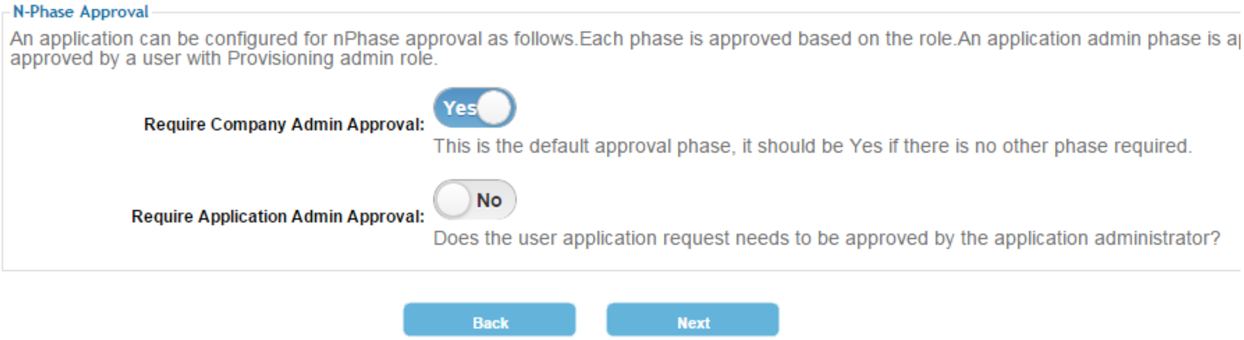
Is grantable: Yes
Indicate if this application can be granted directly by company administration to the user.

Require Request Reason: No
Indicate if this package required the user to supply a reason for requesting this package.

Is Displayable Yes
Indicate if the package icon should be displayed on My Applications page.

Fast Reg Enabled: No
Indicate that the sub-application can be requested along with the parent application.

9. Set the N-Phase approval as shown in the screenshot below. Click **Next**.



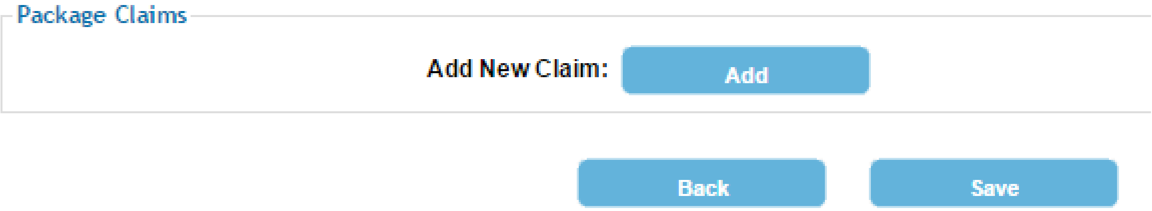
N-Phase Approval

An application can be configured for nPhase approval as follows.Each phase is approved based on the role.An application admin phase is a approved by a user with Provisioning admin role.

Require Company Admin Approval: Yes
This is the default approval phase, it should be Yes if there is no other phase required.

Require Application Admin Approval: No
Does the user application request needs to be approved by the application administrator?

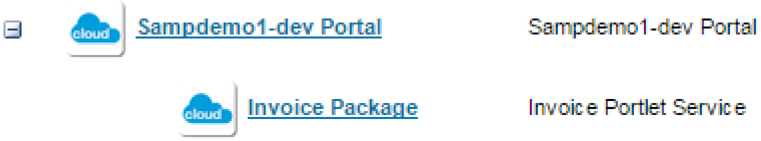
10. Skip the **Package Claims** and click **Save**.



Package Claims

Add New Claim:

11. You have successfully created a sub-package.



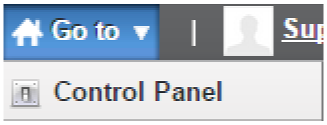
Sampdemo1-dev Portal	Sampdemo1-dev Portal
Invoice Package	Invoice Portlet Service

10.2 Confirm the User Group in Portal

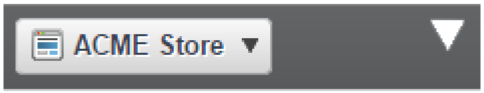
Description: All the services in CIS show as user groups in Portal.

Steps:

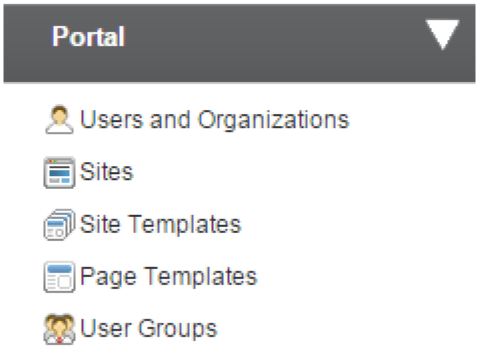
1. Log in to your portal as Portal Administrator.
2. Click the **Go to** menu and select **Control Panel**.



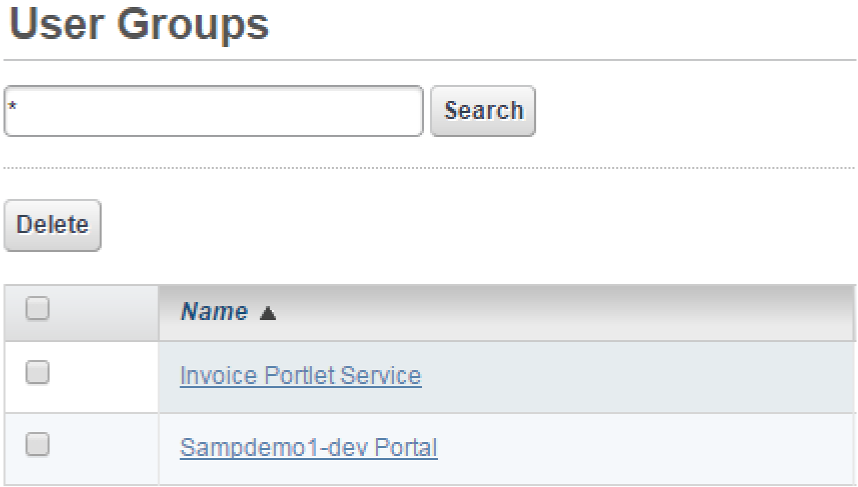
3. Select your site from the drop-down menu.



4. Under Portal section, click **User Groups**.



5. Enter * in the search box and click **Search**. You should see your Invoice Portlet Service now.



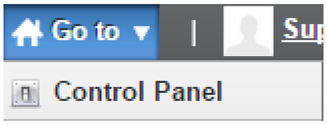
□	Name ▲
□	Invoice Portlet Service
□	Sampdemo1-dev Portal

10.3 Create a Role in Portal

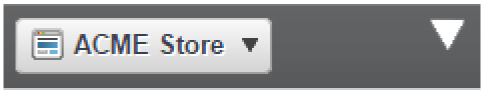
Description: Create a role for this portlet and assign desired members to this role.

Steps:

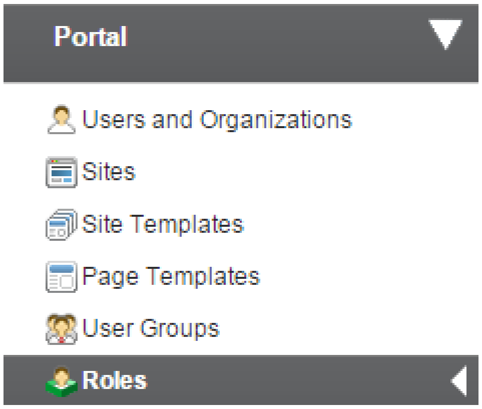
1. Log in to your portal as Portal Administrator.
2. Click the **Go to** menu and select **Control Panel**.



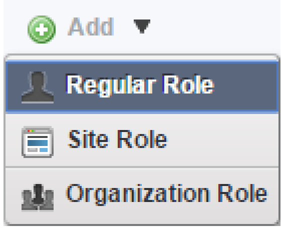
3. Select your site from the drop-down menu.



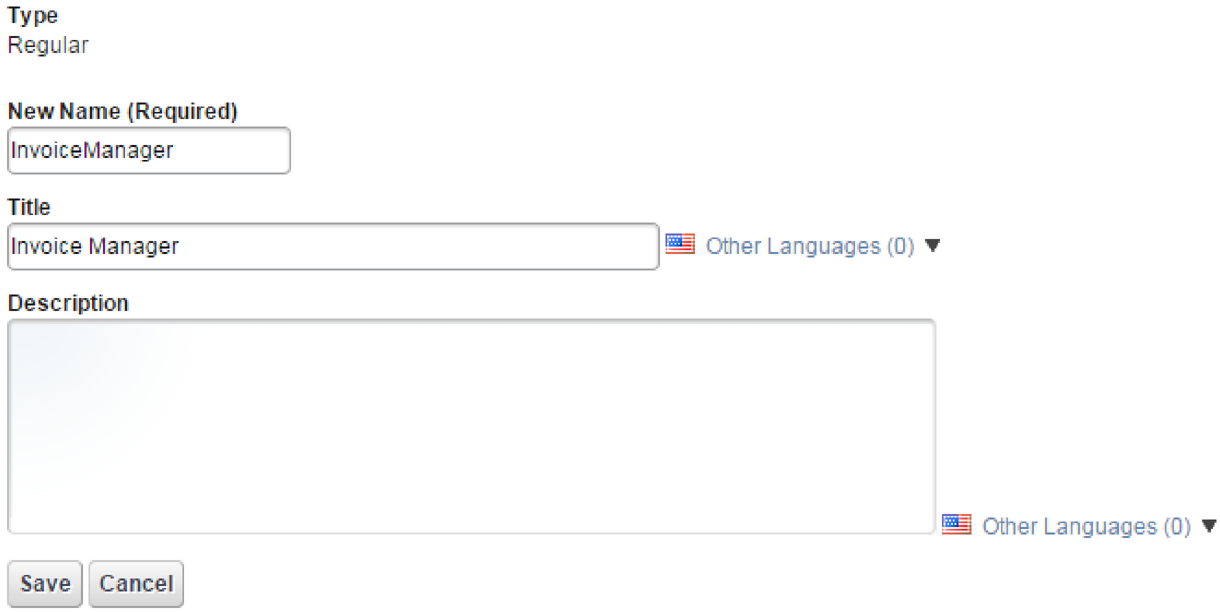
4. Under Portal section, click **Roles**.



5. Click **Add** and select **Regular Role**.



6. Enter a name, title, and a description. Click **Save**.



Type
Regular

New Name (Required)
InvoiceManager

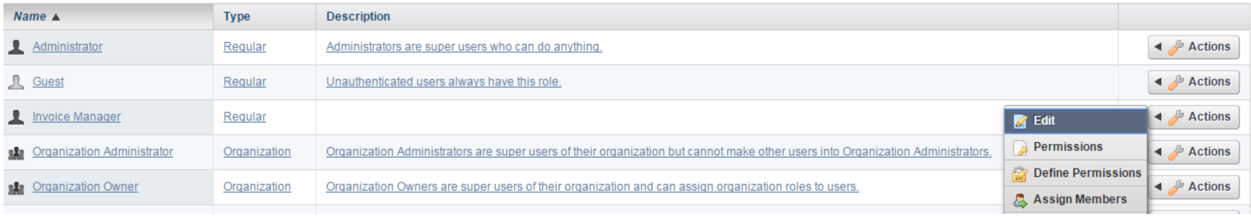
Title
Invoice Manager

Description

10.4 Assign the User Group to the Invoice Manage Role

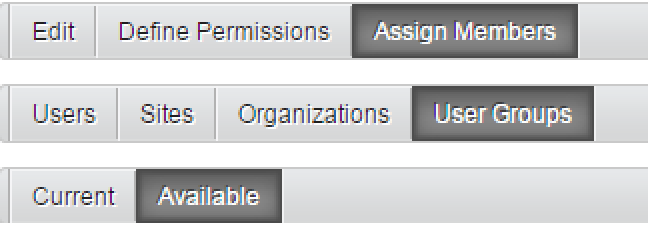
Steps:

1. Go to the **Roles** section, click **Actions** next to **Invoice Manager**, and select **Assign Members**.

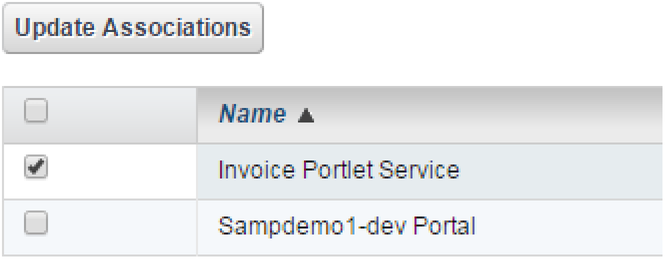


Name ▲	Type	Description	
Administrator	Regular	Administrators are super users who can do anything.	Actions
Guest	Regular	Unauthenticated users always have this role.	Actions
Invoice Manager	Regular		Actions
Organization Administrator	Organization	Organization Administrators are super users of their organization but cannot make other users into Organization Administrators.	Actions
Organization Owner	Organization	Organization Owners are super users of their organization and can assign organization roles to users.	Actions

2. Click the **User Groups** tab and then the **Available** tab.



3. Check the box next to **Invoice Portlet Service** and click **Update Associations**.



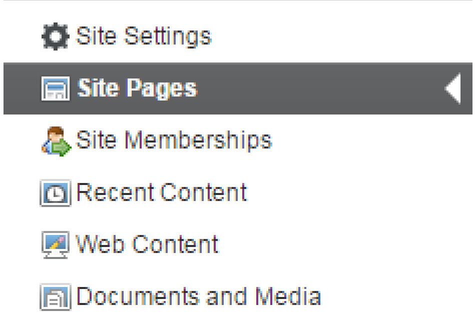
☐	Name ▲
☑	Invoice Portlet Service
☐	Sampdemo1-dev Portal

10.5 Assign Permissions to Invoice Manager Role

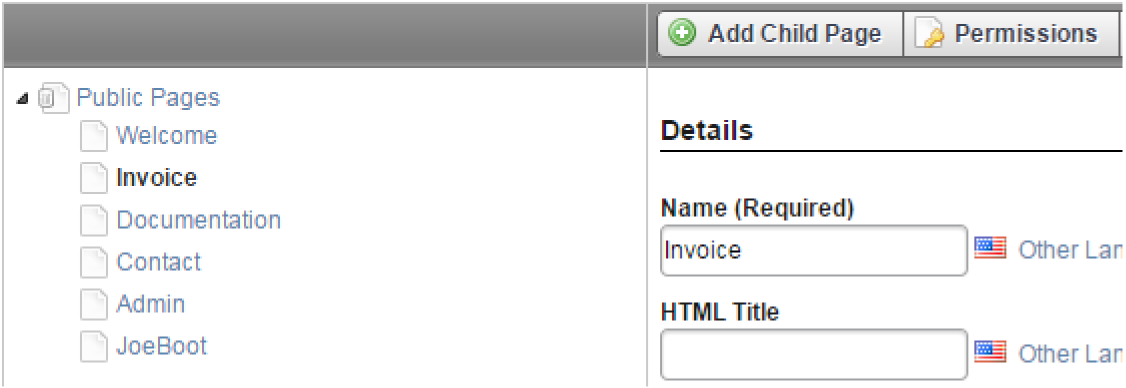
Description: Assign **view** permission to the Invoice Manager role so that any user who has this role would only be able to view the Invoice Portlet.

Steps:

1. Click **Site Pages** under your site.



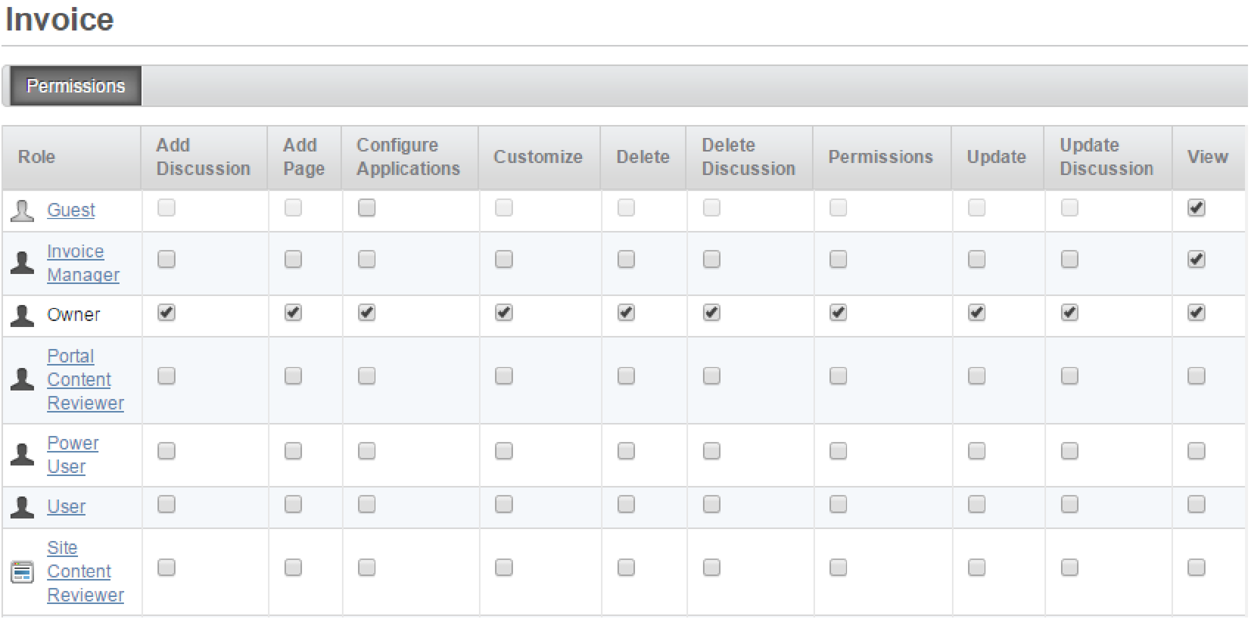
2. Click **Invoice** and select the **Permissions** tab.



Name (Required): Invoice

HTML Title:

3. Check the box for the **View** permission corresponding to the **Invoice Manager** role and click **Save**.



Invoice

Role	Add Discussion	Add Page	Configure Applications	Customize	Delete	Delete Discussion	Permissions	Update	Update Discussion	View
Guest	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑
Invoice Manager	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑
Owner	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Portal Content Reviewer	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Power User	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
User	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Site Content Reviewer	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

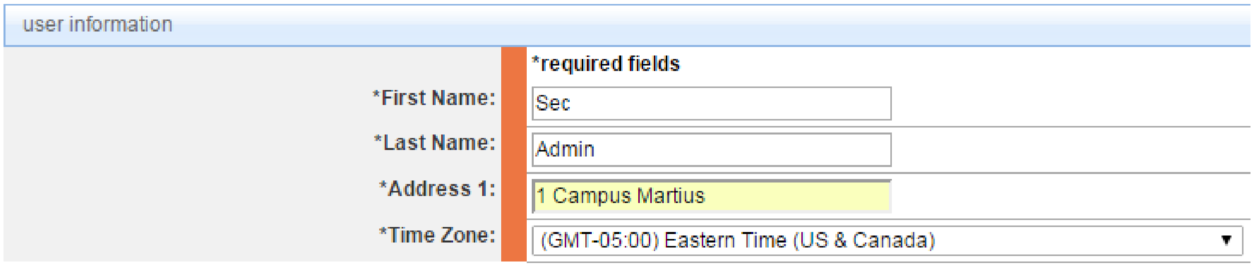
11. Access Control for Invoice Portlet

Description: The goal here is to create a new user in your solution instance, and give access to this user so that they can view the Invoice Portlet. This is a four-step process.

11.1 Invite a new user

Steps:

6. Log in to CIS as a security administrator.
7. Click the **Administration** menu.
8. Click **Invite** and **Invite Users**.
9. Fill in the user information, and click **Next**.

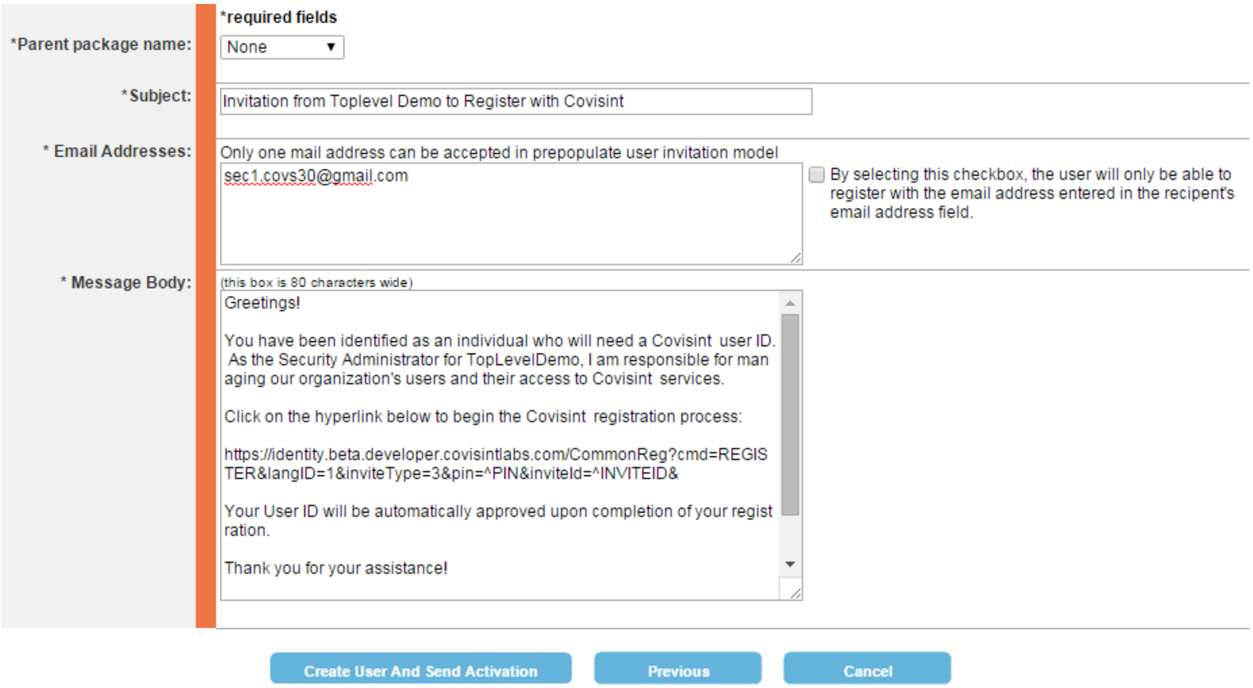


user information

*required fields

*First Name:	Sec
*Last Name:	Admin
*Address 1:	1 Campus Martius
*Time Zone:	(GMT-05:00) Eastern Time (US & Canada) ▼

10. Key in the user email address and click **Create User** and **Send Activation**.



*required fields

*Parent package name: None ▾

*Subject: Invitation from Toplevel Demo to Register with Covisint

* Email Addresses: Only one mail address can be accepted in prepopulate user invitation model

sec1.covs30@gmail.com

□ By selecting this checkbox, the user will only be able to register with the email address entered in the recipent's email address field.

* Message Body: (this box is 80 characters wide)

Greetings!

You have been identified as an individual who will need a Covisint user ID. As the Security Administrator for TopLevelDemo, I am responsible for managing our organization's users and their access to Covisint services.

Click on the hyperlink below to begin the Covisint registration process:

https://identity.beta.developer.covisintlabs.com/CommonReg?cmd=REGISTER&langID=1&inviteType=3&pin=^PIN&inviteId=^INVITEID&

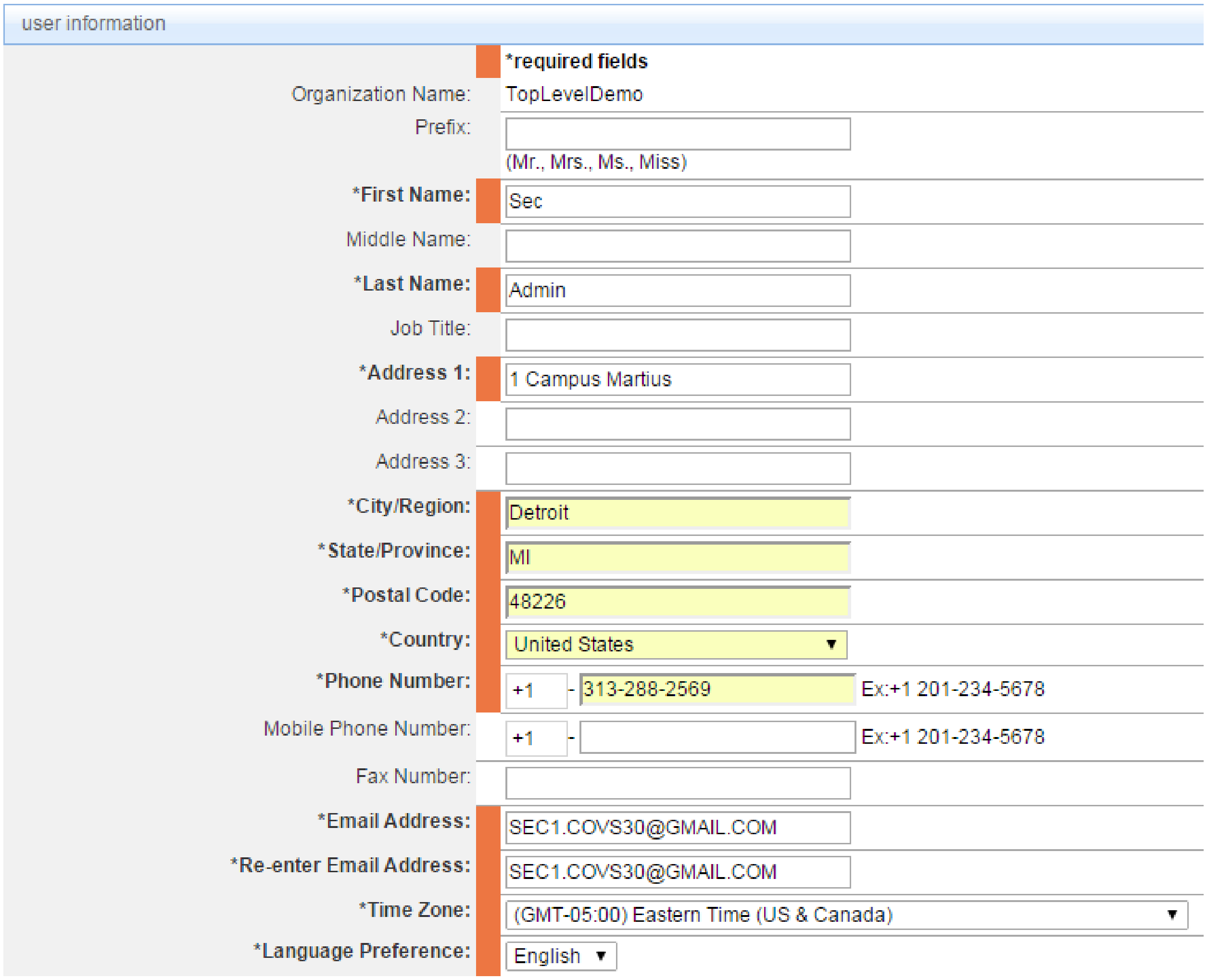
Your User ID will be automatically approved upon completion of your registration.

Thank you for your assistance!

11.2 User Accepts the Invitation

Steps:

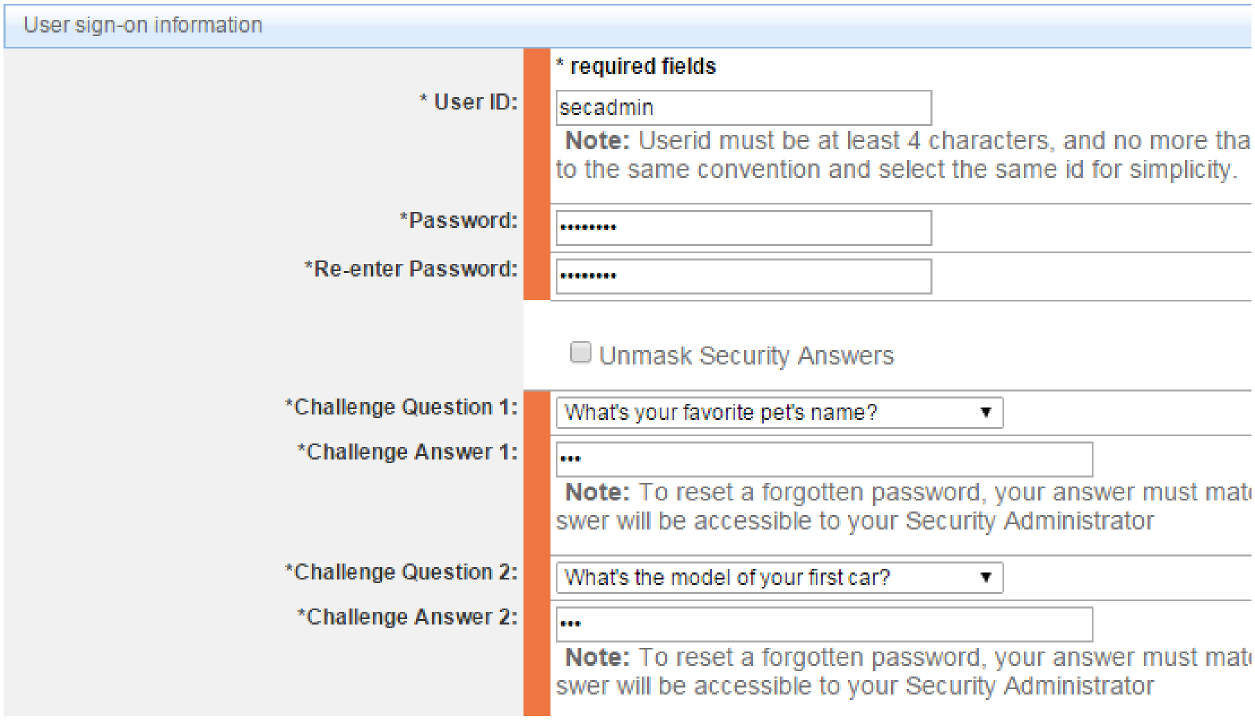
8. The user should click on the invitation email.
9. Fill in the user information and click **Continue Registration**.



user information

	*required fields
Organization Name:	TopLevelDemo
Prefix:	(Mr., Mrs., Ms., Miss)
*First Name:	Sec
Middle Name:	
*Last Name:	Admin
Job Title:	
*Address 1:	1 Campus Martius
Address 2:	
Address 3:	
*City/Region:	Detroit
*State/Province:	MI
*Postal Code:	48226
*Country:	United States ▼
*Phone Number:	+1 - 313-288-2569 Ex:+1 201-234-5678
Mobile Phone Number:	+1 - Ex:+1 201-234-5678
Fax Number:	
*Email Address:	SEC1.COVS30@GMAIL.COM
*Re-enter Email Address:	SEC1.COVS30@GMAIL.COM
*Time Zone:	(GMT-05:00) Eastern Time (US & Canada) ▼
*Language Preference:	English ▼

10. Fill in the user sign on information and click **Continue Registration**.



User sign-on information

* required fields

* User ID: secadmin

Note: Userid must be at least 4 characters, and no more tha
to the same convention and select the same id for simplicity.

*Password: ••••••••

*Re-enter Password: ••••••••

□ Unmask Security Answers

*Challenge Question 1: What's your favorite pet's name? ▼

*Challenge Answer 1: •••

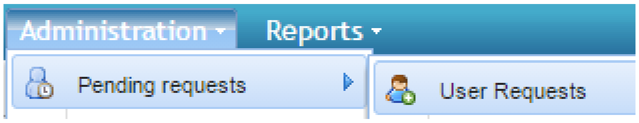
Note: To reset a forgotten password, your answer must mat
swer will be accessible to your Security Administrator

*Challenge Question 2: What's the model of your first car? ▼

*Challenge Answer 2: •••

Note: To reset a forgotten password, your answer must mat
swer will be accessible to your Security Administrator

11. Review the details and click **Submit**.
12. Log in to CIS as a security administrator.
13. Click the **Administration** menu, and then select **Pending requests** and **User Requests**.



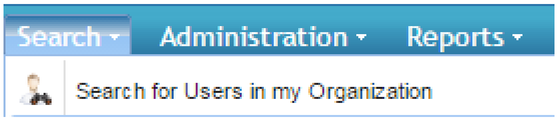
14. Review the request and click **Submit Decision**.

11.3 Grant Portal Package

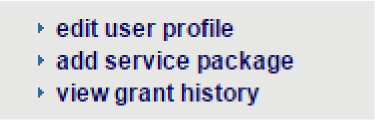
Description: Grant the top-level portal package to the new user.

Steps:

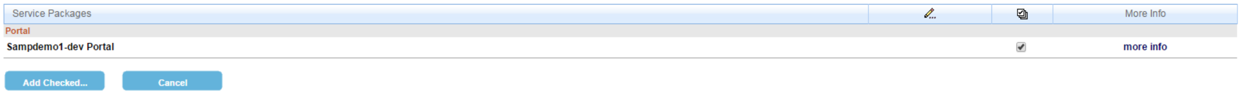
1. Log in to CIS as a security administrator.
2. Click the **Search** menu and select **Search for Users in my Organization**.



3. Select the desired and click **add service package**.

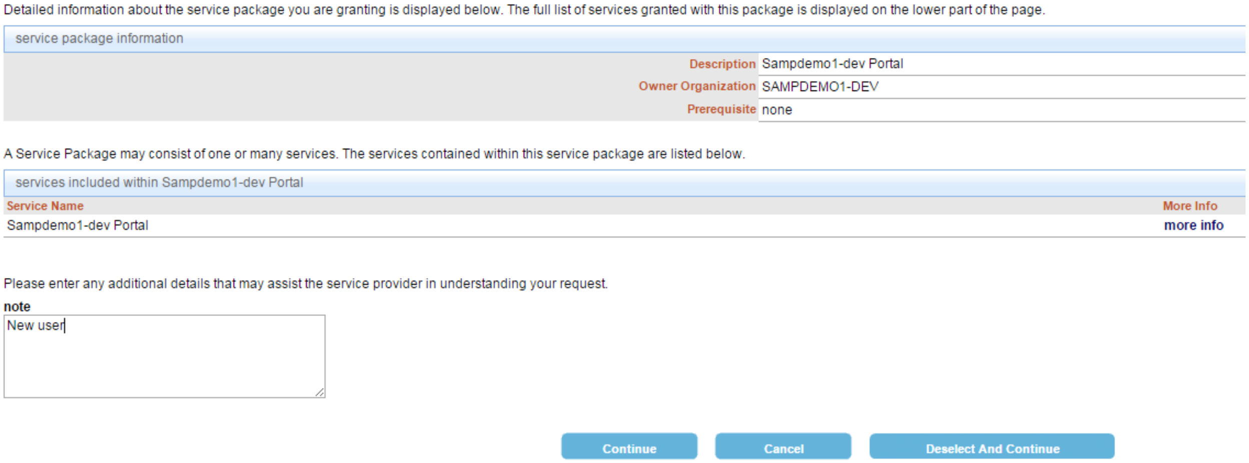


4. Select the top-level package and click **Add Checked…**



Service Packages	✎	☑	More Info
Portal			
Sampdemo1-dev Portal		☑	more info

5. Review the details and click **Continue**.



Detailed information about the service package you are granting is displayed below. The full list of services granted with this package is displayed on the lower part of the page.

service package information

Description	Sampdemo1-dev Portal
Owner Organization	SAMPDEMO1-DEV
Prerequisite	none

A Service Package may consist of one or many services. The services contained within this service package are listed below.

services included within Sampdemo1-dev Portal

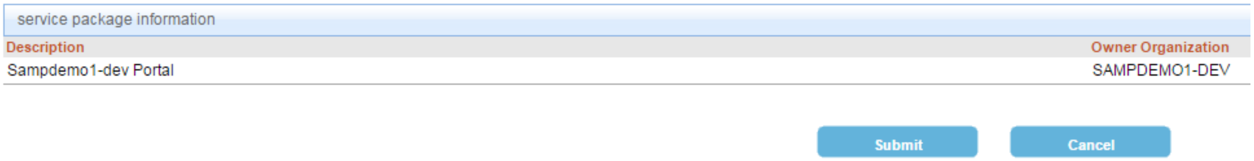
Service Name	More Info
Sampdemo1-dev Portal	more info

Please enter any additional details that may assist the service provider in understanding your request.

note

New user

6. Click **Submit**.



service package information

Description	Owner Organization
Sampdemo1-dev Portal	SAMPDEMO1-DEV

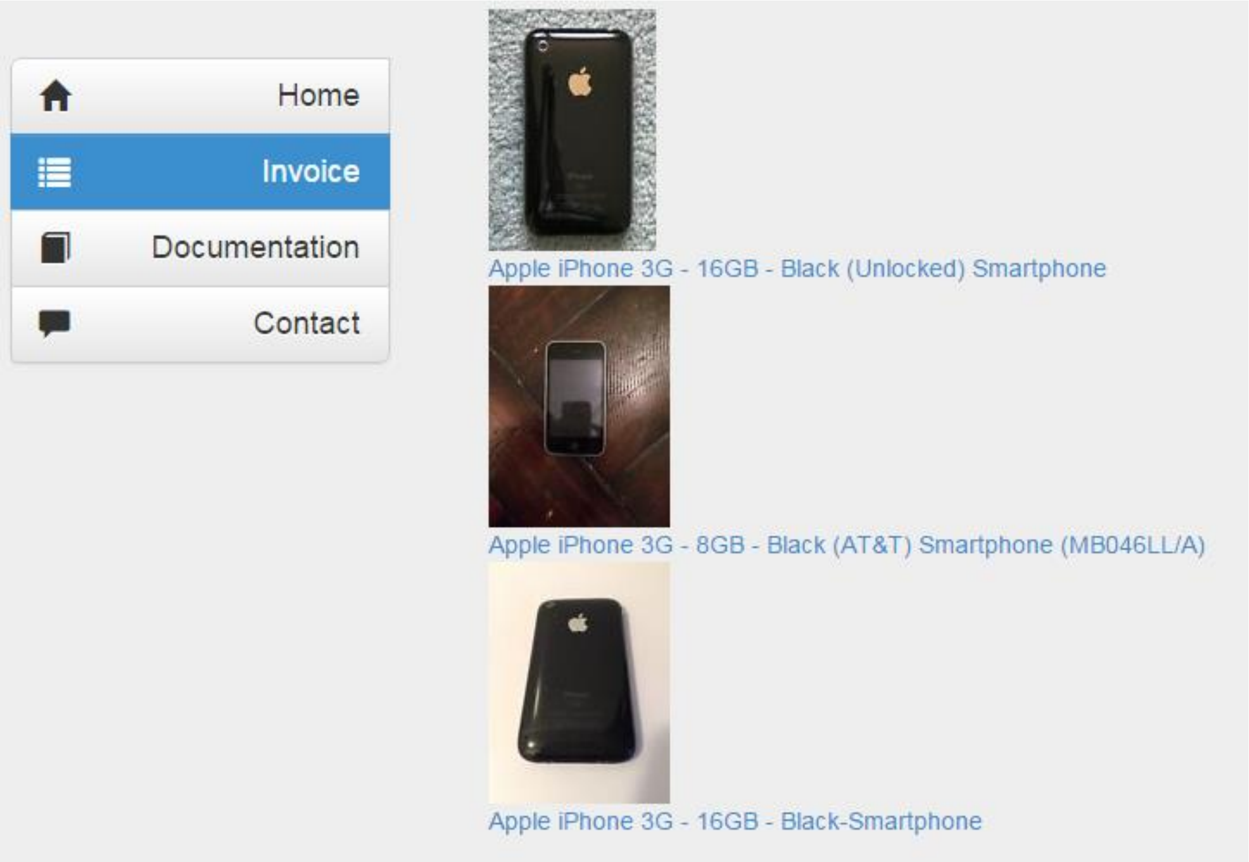
7. You have successfully granted the portal package access to the user.
8. Click **Add Another Service Package** and add the Invoice sub-package. Follow the steps 1 through 7 and granted the Invoice sub-package access to the same user.

11.4 Access the Invoice Portlet

Description: The new user should be able to log in to Portal and access the Invoice portlet.

Steps:

1. Log in to Portal as a user.
2. Click the **Invoice** tab. The Invoice portlet will be displayed.


Home
Invoice
Documentation
Contact
Apple iPhone 3G - 16GB - Black (Unlocked) Smartphone
Apple iPhone 3G - 8GB - Black (AT&T) Smartphone (MB046LL/A)
Apple iPhone 3G - 16GB - Black-Smartphone

3. The new user is successfully able to view the Invoice portlet.