IBM Cúram Social Program Management
Version 7.0.3

IBM Cúram Universal Access

Note

Before using this information and the product it supports, read the information in “Notices” on page 119

Edition

This edition applies to IBM® Cúram Social Program Management v7.0.3 and to all subsequent releases unless otherwise indicated in new editions.

Contents

List of Figures v

List of Tables vi

Chapter 1. IBM Cúram Universal Access (New) 1

Getting started 1
Installing IBM Cúram Universal Access 2
Planning the installation 3
Installation prerequisites 3
Installing IBM Cúram Universal Access 4
Installing later versions 5
IBM Cúram Universal Access business overview 5
Citizen account 5
Applying for benefits 10
Developing applications using IBM Cúram Universal Access 16
Development environment 16
Development resources 17
Developing compliantly 18
Developing with routes 18
Developing with the mock server 20
Developing authentication 22
Developing with RESTService 24
Developing with Redux 25
Developing with universal-access modules 27
Developing with headers and footers 28
Customization scenarios 30
Configuring IBM Cúram Universal Access 50
Prerequisites 50
Configuring service areas and PDF forms 50
Configuring programs 51
Configuring applications 56
Configuring online categories 59
Configuring the citizen account 59
Configuring remote systems 69
Securing IBM Cúram Universal Access 69
The security model 70
Authorization roles and groups 71
Configuring user accounts 71
Integrating external security 72
Account Management 72
Data caching 73
External security authentication 74
Configuring single sign-on 78
Customizing IBM Cúram Universal Access 90
Error logging in the citizen account 91
Customizing submitted applications 92
Customizing the Citizen Account 96
Web services 104
Artifacts with limited customization scope 117

Notices 119

Privacy Policy considerations....120
Trademarks....120

List of Figures

1. IdP initiated flow..... 80
2. IdP initiated flow in IBM Cúram Universal Access..... 82
3. Universal Access SSO configuration components..... 84
4. Intake application workflow..... 93

List of Tables

1. 6
2. Information messages for browser preferences..... 50
3. Application acknowledgment..... 61
4. Meeting invite..... 61
5. Meeting cancellation..... 62
6. Meeting update..... 62
7. Payment issued..... 65
8. Payment canceled..... 65
9. Payment due..... 66
10. Case suspended..... 66
11. Case unsuspended..... 67
12. Account events..... 73
13. ACS trust association interceptor custom properties..... 87
14. Application error codes..... 91
15. Message properties files..... 98
16. Payment messages and related properties..... 102
17. Payment message expiry property..... 102
18. Meeting messages..... 103
19. Meeting message display date property..... 103
20. Application acknowledgment message expiry property..... 104

Chapter 1. IBM Cúram Universal Access (New)

7.0.3.0

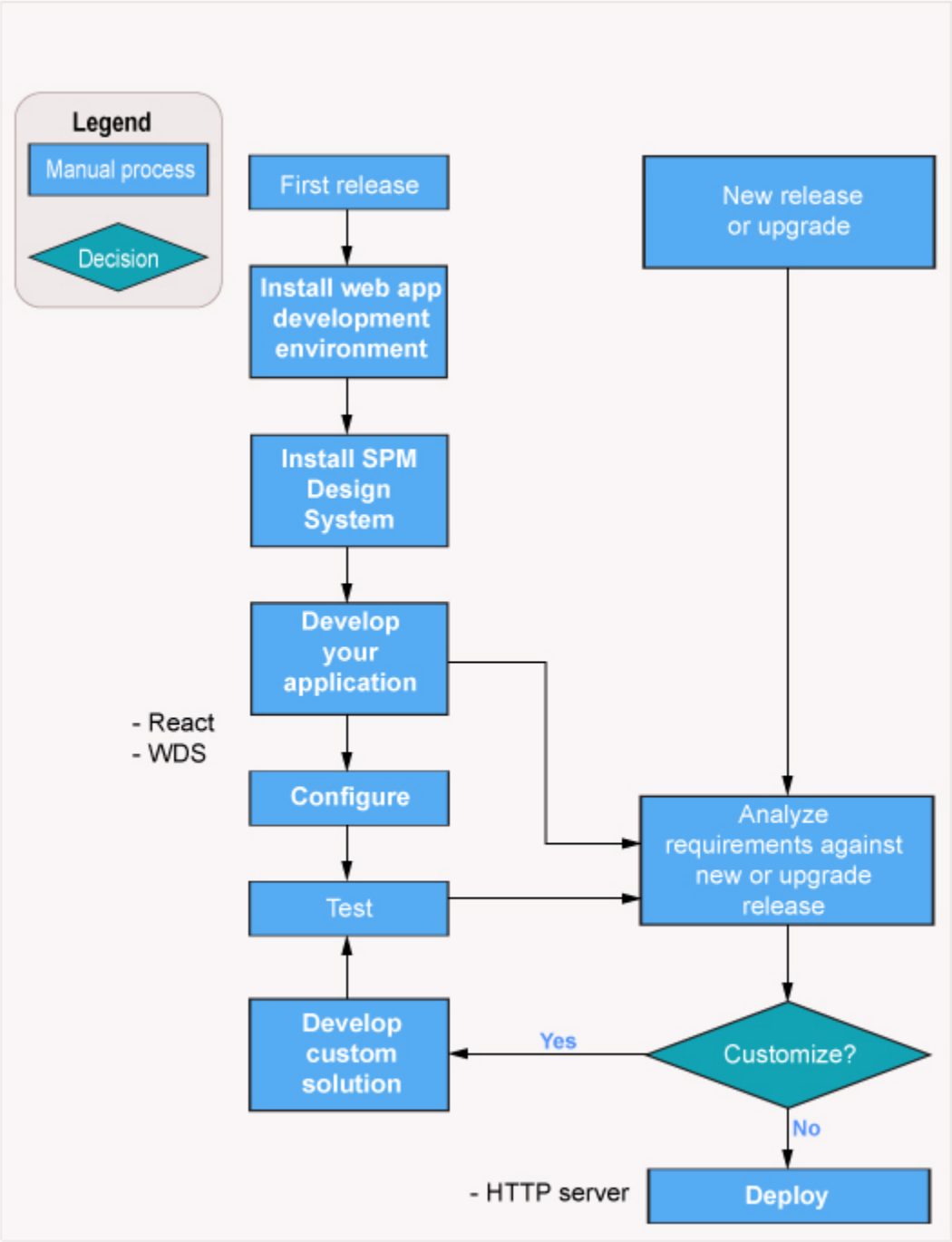
IBM Cúram Universal Access (New) enables citizens to access services in a browser from both desktop and mobile devices. Universal Access uses modern technologies such as React to provide a working reference application that you can customize to provide your own citizen-facing web application. In comparison, Universal Access, delivered with versions 7.0.2 and earlier, use traditional technologies to customize the citizen-facing web application.

Getting started

7.0.3.0

IBM Cúram Universal Access enables governments to provide citizens with a single point of access to all social programs and services for which they are eligible. Universal Access connects citizens to programs, streamlines applications for those programs, and reduces administrative work, allowing caseworker to spend more time interacting with citizens.

You can quickly develop and deploy Universal Access by using the Design System. Hover over some of the process steps in bold text, for example, "Develop your application" to find out more about how to build and deploy your Universal Access:



1. “Installing IBM Cúram Universal Access” on page 2
2. Installing the IBM Social Program Management Design System
3. “Configuring IBM Cúram Universal Access” on page 50
4. Developing applications using the IBM Social Program Management Design System
5. “Developing applications using IBM Cúram Universal Access” on page 16
6. Deploying a built application

Installing IBM Cúram Universal Access

7.0.3.0

Before you install IBM Cúram Universal Access, plan your installation and install the prerequisites.

Planning the installation

7.0.3.0

Review the supported prerequisites, download the required software, install Universal Access, and review the release notes.

The installation steps

When you complete the following installation steps, you are ready to start developing your app:

- Review the supported prerequisites to identify the supported versions of your selected software. For more information, see *Installation prerequisites*.
- Download the software that you need from IBM Passport Advantage® or from another software vendor websites as appropriate.
- Install Universal Access, for more information, see *Installing IBM Cúram Universal Access*.
- Review the IBM Cúram Social Program Management Release Notes® and complete any relevant post-installation steps.

Related tasks

Installing IBM Cúram Universal Access
Installing IBM Cúram Universal Access node packages.

Installation prerequisites

7.0.3.0

The platform, accessibility, and development prerequisites for your installation.

Platforms

There is no dependency on specific hardware platforms, instead the IBM Cúram Universal Access dependency is on the browser. However, the following are minimum requirements:

- Desktop devices that meet Windows 7 specifications.
- Android devices that meet minimum specifications for Android 4.4+ . 4.4+ should function on a two year old Android device or younger.
- Apple devices released in the last 18 months running iOS9 or higher.

Accessibility

Development tools

Choose an Interactive Development Environment (IDE) to develop your app.

There are many IDEs that you can choose, for example Visual Studio Code, Atom, and Sublime. Universal Access does not depend on any specific IDE, you are free to choose your own IDE. However, IBM uses VSCode to develop the your application, it supports many plug ins that make development faster and easier, for example it supports the following tools:

- Linting tools (ESLint)
- Code formatters (Prettier)
- Debugging tools (Debugger for Chrome)
- Documentation tools (JSDoc)

IBM does not own, develop, or support these tools.

Web browsers

The following browsers are supported:

- Desktop: Chrome XX, Firefox XX, MS Edge 40+, IE11, Safari 10+
- Mobile: Chrome XX, Safari 10+

IBM Cúram Social Program Management

IBM Cúram Social Program Management version 7.0.3 is required.

Installing IBM Cúram Universal Access

7.0.3.0

Installing IBM Cúram Universal Access node packages.

Before you begin

IBM Social Program Management Design System should already be installed. For more information, see *Installing the IBM Social Program Management Design System.*

`@spm/universal-access-starter-pack` acts as a starter boiler-plate application, its installation differs from that of other packages.

About this task

Install Universal Access node packages.

- `@spm/mock-server`
- `@spm/universal-access-mocks`
- `@spm/universal-access`
- `@spm/universal-access-ui`
- `@spm/universal-access-starter-pack`

Install the packages into a *React* application, they are not installable on their own. Use any *React* app, however Facebook's *create-react-app* is used as an example in this procedure.

Procedure

1. Unzip `@spm/universal-access-starter-pack`.

   The extracted directory forms the React App, all other packages are installed into this directory.
2. Rename the extracted directory from step 1 to reflect your project, for example `universal-access-custom-app`
3. From the renamed, extracted package directory, install the IBM Social Program Management Design System packages. Enter the following commands, ignore any warnings you might see. `<path>` and `<version>` refer to the download path and package version.

   ```
   npm install <path>/govhhs-govhhs-wds-<version>.tgz
   npm install <path>/govhhs-govhhs-wds-react-<version>.tgz
   npm install <path>/spm-core-<version>.tgz
   npm install <path>/spm-intelligent-evidence-gathering-<version>.tgz
   ```
4. Enter the following commands from the renamed, extracted package directory to install IBM Cúram Universal Access packages. Ignore any warnings you might see. `<path>` and `<version>` refer to the download path and package version.

   ```
   npm install <path>/spm-universal-access-<version>.tgz
   npm install <path>/spm-universal-access-ui-<version>.tgz
   ```

5. Enter the following commands to install the mock-server and mock data as a dev dependency.

```
npm install -D <path>/spm-universal-access-mocks-<version>.tgz
npm install -D <path>/spm-mock-server-<version>.tgz
```

Related information

Installing the IBM Social Program Managememt Design System

Installing later versions

7.0.3.0

You can install later versions of IBM Cúram Universal Access packages.

Procedure

1. Go to IBM Fix Central and search for your product and version to locate the latest version for your installation.
2. Download and extract the new image.
3. Read the latest version of the IBM Cúram Universal Access Release Notes. Take note of any pre-installation steps, requirements, restrictions, installation steps, and post-installation steps that might apply between the new version and your current version.
4. Read the `readme` file that is downloaded with the version. Take note of any pre-installation steps, requirements, restrictions, installation steps, and post-installation steps.
5. Repeat the procedure to install the node_packages. For more information, see *Installing IBM Cúram Universal Access*.

Related tasks

Installing IBM Cúram Universal Access
Installing IBM Cúram Universal Access node packages.

IBM Cúram Universal Access business overview

7.0.3.0

A business overview of the online facilities that are provided by Universal Access enterprise module. Use this information to map existing features and capability to your business requirements during a business analysis.

IBM Cúram Universal Access is a citizen-facing web application that provides citizens with online facilities. Read this business overview of the online facilities that are provided by the Universal Access. Use this information to map existing features and capability to your business requirements during business analysis.

Citizen account

7.0.3.0

When citizens create a secure citizen account, they can access a range of relevant information. Citizens can also use the citizen account to track and manage interactions with the agency.

Creating a citizen account and logging in

7.0.3.0

Citizens can create a citizen account during the application process.

Creating an account

Citizens can select **Sign up** on the organization **Home** page to create an account. Citizens then enter their first and last names, an optional email address and account password. If citizens select **I don't have an email address**, they can specify a user name instead.

For more information about the application process, see *Completing and submitting benefit applications*.

Administration configurations

- Number of login attempts before the account is locked out: 5
- Number of login attempts remaining before a user warning is displayed: 3
- Number of break-in attempts before an account is locked: 3

Logging in

To log in to the citizen account, citizens select **Log in** on the organization **Home** page. Depending on how they created their account, citizens enter either an `Email or username` and `password` and then select **Next**. You can configure the number of login attempts citizens have before their account is locked out. For example, if you set the number of login attempts to three, citizens who make three unsuccessful login attempts have their accounts locked out.

The next page that is displayed depends on whether citizens are linked to a participant and whether second-level authentication is enabled. Second-level authentication means that the citizen is asked to provide more personal information before they are logged in, for example, date of birth or Social Security number (SSN). Administrators can define one or more pieces of data that the citizen must provide.

If second-level authentication is not defined, citizens are brought to the **Citizen account** dashboard. If second-level authentication is defined and citizens must specify a date of birth and SSN before they can log in, then a page is displayed prompting the citizen to enter their details.

If the citizen is not linked to a participant, second-level authentication is not applicable. The citizen is brought to the **account** dashboard if the user name and password passes authentication.

Related concepts

Completing and submitting benefit applications

Browsing the dashboard

7.0.3.0

When the citizen logs in, they see the **Dashboard** and the **Your benefits** tabs.

Dashboard

The **Dashboard** is laid out in a series of panes as outlined in table 1:

Table 1:

User interface pane	Description
System messages	System messages are broadcast to all logged-in citizens. System messages inform citizens about, for example, planned system outages.
In-progress applications	Citizens can decide to either continue or delete in-progress applications.
PAYMENTS	Lists the latest payment made to citizens. Citizens can also view payment details or see their payment history.
TO-DOS	Lists actions that citizens must take to complete an application.
MEETINGS	Outlines details of meetings that citizens have been invited to. A date is included for all meetings. The latest meeting is shown first.

Table 1: (continued)	
User interface pane	**Description**
NOTIFICATIONS	Shows acknowledgments for all the applications that citizens make. A date is included for all notifications. The latest notification is shown first.

For more information on configuring messages, see *Customizing specific message types*.

Related concepts

Customizing specific message types

Browsing the Your benefits page

7.0.3.0

When the citizen logs in, they see the **Dashboard** and the **Your benefits** tabs.

Your benefits

Logged-in citizens who select **Your benefits** on the **Dashboard** are brought to the **Your benefits** page. Citizens who are not logged in are redirected to the **Log in** page, when they log in they are brought to the **Your benefits** page, which displays all types of applications, these are in-progress, pending, withdrawn, denied, and active applications.

If a submitted application is approved by the caseworker and a product delivery case is created for that application, the application also appears on the **Your benefits** page.

The **Your benefits** page displays applications that can be in one of the following states:

- **Application in progress**. The application is in progress but is not yet submitted. Citizens can either continue or delete applications in this category.
- **Pending decision**. The application is awaiting a decision from the case worker. Citizens can either download or withdraw applications in this category.
- **Active**. The caseworker has authorized the application .
- **Denied** The caseworker has rejected the application.
- **Authorization failed**. Citizens can download applications in this state.
- **Withdrawn**. Citizens can withdraw the application if it is **Pending decision** or the caseworker has **Denied** the application.

Viewing payments

7.0.3.0

The **PAYMENTS** pane on the **Dashboard** lists payments that are made to the citizen. The messages associated with these payments can be retrieved from IBM Cúram Social Program Management or another remote system. Canceled or expired payments are also displayed.

A payment can be made by check, electronic funds transfer (EFT), cash, or voucher.

Depending on the payment type, different details are displayed. The following details can be displayed on for each payment:

Check
: Payee address and check number

EFT
: Bank sort code and bank account number

Cash
: Payee address

Voucher
: Payee address and voucher number

Note: Citizens do not see these payment details on the dashboard itself. Instead, citizens must select **All payments** in the **PAYMENTS** panel and then select **>** in a specific payment to see payment details for that payment.

Viewing to-do items

7.0.3.0

The **TO DOs** pane on the **Dashboard** lists verifications and action messages that the caseworker creates for the citizen.

A to-do could be, for example, a request to provide supplementary information to support a benefit application.

Displaying contact information

7.0.3.0

The **Contact us** tab, and **Profile** link display the citizen's contact information and the contact information of the agency caseworker.

Citizen information

Citizens can select **Citizen Name** > **Profile** to display their contact information including address, phone number, and email address. A configuration setting determines whether the citizen's contact information is displayed on the citizen account. For example, an agency can set the `curam.citizenaccount.contactinformation.show.client.details` property to `false` to disable citizen contact information. For more information, see *Configuring contact information*.

Caseworker contact information

The **Contact us** tab displays information for the agency caseworker of each case that the citizen is associated with is displayed. Caseworker contact information from IBM Cúram Social Program Management and remote systems can be displayed. The following information can be displayed for the caseworker:

- Name
- Business phone number
- Mobile phone number
- Pager
- Fax
- Email

Use configuration settings to specify the contact details to display and hide on the contact information page. For example, an agency can display an caseworker's business phone number and email address only. Similarly, an agency can hide contact information. For more information about configuring the display of citizen contact information, see *Configuring contact information*.

Related concepts

Configuring contact information
Configure contact information for citizens and caseworkers.

Citizen account messages

7.0.3.0

The **Payments**, **TO-DO**, **Meetings**, and **Notifications** panes on the **Dashboard** display citizen account messages. Messages can be about meetings the citizen is invited to, or activities that are scheduled for the citizen. By using web services, messages from remote systems can also be displayed.

Displaying a message

Each message has a title and an icon. In addition, the **TO-DO** and **Notifications** messages have an effective date and time that specifies when the message is displayed. Usually the effective date of a

message is set to the current date, but in some circumstances configuration settings can specify the effective date. For example, when a service is scheduled for the citizen, you might not want to display the message immediately if the service is scheduled for two months in the future. In this case, a configuration setting is provided to specify the number of days before the start date of the service that the message must appear in the citizen's account. For example, the system uses these days to populate the effective date. Messages from remote systems are displayed based on the effective date that is specified in the web service.

Prioritization and ordering

You can assign a priority to a message so that it is displayed at the top of the **Messages** listing.

You can also configure the order of messages types in the administration system. For example, you can configure payment messages to be displayed first and meeting messages to be displayed second.

Message duration

The message type determines the length of time that the message is displayed. The message duration can be set either by start and end dates or by replacing one message with another.

Some messages relate to items that have start and end dates that the agency can use to specify the duration for which a message is displayed. For example, service messages are displayed until the start date of the service has passed. In other cases, it might be appropriate for a message to be replaced by another message. The agency can use a configuration setting to determine whether the agency wants to:

- Specify the duration for when a message is replaced.
- Specify the number of days after which the message is removed.

The duration of messages from remote systems is based on the expiry date that is defined in the web service.

System messages

Agencies use system messages to send a message to everyone who has a citizen account. For example, if an agency wants to provide information and help line numbers to clients who were affected by a natural disaster, such as a flood, hurricane, or earthquake. System Messages can be configured in the Administration application by using the **New System Message** page.

The **Title** and **Message** fields define the title of the message and the message body that is displayed to a client in the **My Messages** pane. The message can be defined with a priority by using the **Priority** field, which means that the message appears at the top of the messages listing.

The **Effective Date and Time** field defines an effective date for the message, such as when the message is displayed in the **Citizen Account** page. The **Expiry Date and Time** field define an expiry date for the message, for instance, when the message no longer is to be displayed in the citizen account.

When the message is saved, it has a status of **In-Edit**. Before the message is displayed in the citizen account, it must be published. When it is published, the message is active and is displayed in the citizen account based on the effective and expiry dates defined.

Predictive Response Manager

The Predictive Response Manager (PRM) is the infrastructure that is used to build and then generate and display messages on the Citizen Account home page.

A number of default messages are provided and are described in this information along with their associated configurations

Applying for benefits

7.0.3.0

Citizens can apply for benefits from the organization home page or the **Dashboard**. Citizens must submit an application that includes personal details like income, expenses, employment, education. This information is the evidence of the citizen's case. Agencies can use this information to determine eligibility for benefits. Citizens can also apply offline by downloading the application form, filling it in and sending it to the agency. Citizens can also contact their local agency office.

Before you begin

Citizens can apply for benefits by logging in to their account. Citizens who log in can save an application for a benefit before they submit it and then return later to complete the application. Citizens can also partially apply for benefits without logging in. If the configuration option *submit on completion* is set to **No**, citizens can submit a partial submitted application. Citizens do not have to be logged in to submit the partial application.

Note: The terms "benefit" and "program" are synonymous. An application might consist of one or more benefits. For example, the "Income Support" application might contain the "Food Assistance" and "Cash Assistance" benefits.

Procedure

1. Citizens click **Apply for benefits** on the organization **Home** page, the **Dashboard**, or the **Your benefits** tab.

   Note: Benefits are displayed in alphabetical order by default, but you can override this order.
2. For each benefit type, citizens can take the following actions:
   a) Click **Learn more** to find out more about the benefit. If the *More Info URL* setting is configured for the application, **Learn more** is conditionally displayed.
   b) Click **Print application** to print the application form, complete it by hand and mail it to the agency. If the *PDF Application Form* setting is configured for the application, **Print application** is conditionally displayed.
   c) Click **Apply** to start the application process for the benefit. **Apply** is conditionally displayed if **multiple applications** is set to **Yes** or if **multiple applications** set to **No** and the citizen has no existing, pending decision applications.

Results

If citizens quit the application without saving it, the application displays a warning dialog so that citizens can return to the application if this option is selected in error.

Note: Citizens must click the application name on the page in to see the **Leave this application** dialog. The application name is also conditionally enabled depending on whether the **quit and delete** option is enabled in the IEG script.

Clicking **Leave** brings citizens to the dashboard if they are logged in or the organization home if they are not logged in.

Clicking **Cancel** returns citizens to the point at which they left the application script with the previously entered data available. Citizens can cancel an application without saving at any point before they submit. Citizens can only cancel when the application is in progress, if they **Save** and **Exit** they can only **Delete** the application.

Citizens can also:

- Resume an application by selecting the **Continue** link on the **Your benefits** page, or by selecting **Continue** on any in-progress application alerts in the **Dashboard**.

- **Withdraw** an application. If available, the withdraw option is displayed for the pending decision application on the **Your benefits** page.
- **Delete** an application. Citizens can only delete an *in progress* application that they did not submit to the agency.

Starting and selecting an application

7.0.3.0

Citizens can select the benefits they want to apply for.

Citizen start an application by selecting **Apply for benefits** on the **Organization** home page or selecting the **Benefits** navigation item. Citizens are then brought to the **Apply for benefits** page.

The **Apply for benefits** page describes each of the available applications. To make it easier for administrators to find the required application, they are grouped into categories, for example "unemployment services". The applications, and their categorization, are defined in the Universal Access Administration section of the Administration Application. Citizens can also **Learn more** about each application or can **Print application** to a PDF file.

Citizens can **Apply** for a benefit. Citizens start an application for a benefit they have already applied for, they can resume the application or they can **Start again**.

Citizens might use an application to apply for one or more programs. Typically, the system prompts citizens to select the programs they want to apply for. However, in two situations the system does not prompt the citizen to select programs:

- A single program is defined for the application.
- Each application is configured so that the citizen can select a program or automatically select all of the programs that are associated with the application.

Configuring the application process

You can configure the application process as follows:

- Each configured application is displayed. If an application has more than one associated program, it is displayed in the second column of the **Apply for benefits** page.
- A configuration property **program selection** is available at the application level. If the property is set to **Yes**, an **Include benefits** page is displayed allowing the citizen to select all, or a subset of the configured programs.
- If an application only contains one program and the configuration property program selection is set to **Yes**, the **Include benefits** page is not displayed.
- If the program selection is set to **No** and the application contains multiple programs, all the programs are automatically applied for and the **Include benefits** page is not displayed.
- A configuration property multiple application is available at the program level. If this property is set to **No** there is an existing pending decision for the program, the **Apply** option is visible but disabled.

When citizens select the applications and the programs they want to apply for, the system starts the associated IEG script. Citizens use the script to complete the selected applications.

Managing existing applications

7.0.3.0

When a citizen logs in, any existing applications are listed and the citizen is presented with different options that depend on the state of an application.

The agency can configure the system to specify whether citizens need to be authenticated before they apply for benefits:

- If authentication is enabled, citizens must either create a new user account or log in to an account before they start the application process.
- If authentication is disabled, citizens can proceed with the application without authentication.

The property *curam.citizenworkspace.authenticated.intake* specifies whether citizens must log in to apply for benefits. If the property is set to **NO**, citizens do not have to log in to apply for benefits. If the property is set to **YES**, citizens must create an account or log in to an existing account to apply for benefits.

Depending on how authentication is configured, applications are managed in one of the following ways: Citizens can log in to their account, or they can sign up from the application overview page. Citizens can also be prompted to log in, sign up, or send application without an account at the end of the IEG application script.

If citizens create an account, they are automatically logged in to the system and the intake process starts. The system also checks whether they have any existing applications.

The configuration property **Submit on completion only** is available at the application level. If this property is set to **No**, citizens can submit a partially completed application, if this property is set to **Yes**, citizens cannot submit a partially completed application.

Existing applications are in one of the following categories:

- **Application in progress**. The application is in progress but is not yet submitted. Citizens can either continue or delete applications in this category.
- **Pending decision**. The application is awaiting a decision from the case worker. Citizens can either download or withdraw applications in this category.
- **Active**. The caseworker has authorized the application .
- **Denied** The caseworker has rejected the application.
- **Authorization failed**. Citizens can download applications in this state.
- **Withdrawn**. Citizens can withdraw the application if it is **Pending decision** or the caseworker has **Denied** the application.

The application lists are displayed only if there are items in the list, that is, if there are no saved applications. If applications are listed, the citizen is presented with different options that depend on the state of an application. The citizen might resume or delete an incomplete application, withdraw a submitted application, or start a new application.

Related concepts

Securing the IBM Cúram Universal Access

Saving an application

7.0.3.0

By default, applications are automatically saved for citizens who are logged in. Citizens can also manually save applications, including in-progress applications.

During a timeout or the accidental closure of the browser window, the application is automatically saved each time that citizens click **Next** in the IEG script. When citizens click **Next**, the information on the previous page is saved. Citizens can also use the **Benefits** page to resume or to delete each in-progress screening. Automatic saving works for logged-in citizens only. Applications for citizens who are not logged are not saved.

A system property specifies whether applications are automatically saved. By default, this property is enabled. For more information, see *Configuring applications*.

When citizens quit an application, three options are displayed. The options the system displays depends on how the intake application is configured. Citizens can take one of the following actions:

- **Save the application**
- **Leave the application without saving**
- **Cancel** the application

If citizens save the application and they are not logged in, the save application screen is displayed. Citizens can create an account, log in, or send the application without logging in.

The configuration property **Submit on completion only** is available at the application level. If this property is set to **No**, citizens cannot submit a partially completed application, so the option to **Send**

application without account is displayed when citizens select **Save and exit**. If the property is set to **Yes** citizens cannot submit a partially completed application, so the option to **send application without account** is not displayed when citizens select **Save and exit** .

Related concepts

Configuring applications

The administration system allows an agency to define different types of applications. Once defined, citizens can submit an application for programs to the agency. For each application, you can configure the available programs and an application script and data schema. Configure the remaining applications details, including application withdraw reasons.

Resuming an application

7.0.3.0

Logged-in citizens can resume an application by selecting the **Continue** link on either the **Dashboard** or the **Your benefits** page.

Selecting the **Continue** link in the citizen's **Dashboard** resumes the application from where the application was last saved. When an application is resumed, the data that is entered is automatically saved as citizens moves from page to page through the script.

When citizens resume an application, they are brought to where they left off when the application was saved.

Submitting an application

7.0.3.0

To allow citizens to submit an application to the agency, you must specify a submission script for the application in the administration system. After citizens submit an application, the way the script is processed depends on the configuration of the programs for which the citizen is applying.

The application might be submitted when citizens complete the intake script or when they exit a script before it completes. An intake application can be configured so that an agency can dictate whether an application script can be submitted before it is complete or not.

If citizens send an application to the agency, either by exiting or completing a script, the screen that is displayed depends on:

- Whether citizens are logged in
- Whether citizens must either create or log in to an account before the application is submitted.

If citizens are not logged in, they are prompted to log in or create a new account. If the property is enabled, citizens must log in to an existing account or create a new account before the application can be sent to the agency. For more information, see *Managing existing applications*.

Specifying log in requirements

The system can be configured so that:

- Citizens are not required to identify themselves to the system AND
- Citizens can send the application to the agency without logging in or creating an account.

Alternatively, the system can be configured so that citizens must create an account or log in. For more information, see *Logging in and managing existing applications*.

Managing in-progress and submitted applications

If citizens log in before they send the application to the agency, the system can determine whether:

- There is an in-progress application of the same type OR.
- Citizens previously submitted applications for the same programs that are still pending disposition, that is, awaiting a decision by the agency.

For an in-progress application of the same type, a page is displayed. From here, citizens can send the new application to the agency or keep the saved application, thus discarding the new application. The options available are to **Start again** or **Resume** the in-progress application.

If citizens submit applications for the same programs, the system determines whether they can still submit any of the programs to the agency for processing. Programs can be configured so that multiple applications can be submitted for the program at any time. For example, submitting a new application for cash assistance for a different household unit than a previously submitted application that the agency is processing. This screen indicates that the application cannot be submitted for all of the programs for which the citizen wants to apply. However, the application might still be sent to the agency. There are three options: continue to submit the application for the programs for which the citizen can apply, save the application, or delete the application.

The configuration property **Multiple application** is available at the program level. If this property is set to **No** and there is a pending decision for the program, the **Apply** option is visible but disabled.

Specifying a submission script

To submit an application to the agency, a submission script must be specified for the application in administration. The submission script is required because applications require additional information, which does not form part of the application, to be captured before the applications can be submitted. For example, a Cash Assistance application requires information that relates to the citizen's ability to attend an interview. This information would not be appropriate for another type of application that does not require an interview to be conducted, for example, unemployment insurance. Electronic signatures are another example of the type of information that would typically be captured by using a submission script. This data might not be captured as part of the script, as citizens can submit the application before completing the script.

Processing a submitted script

The processing that happens on completion of the submission script depends upon the configuration of the programs for which citizens are applying. Program eligibility can be configured such that it might be determined by using IBM Cúram Social Program Management or a remote system. If IBM Cúram Social Program Management is specified as the eligibility system, an application case creation process is started. The application case creation process includes a search and match capability, which attempts to match citizens on a new application to registered persons on the system based on configured search criteria. When search and match finishes, one or more application cases are created. If the programs that are applied for are configured for different application case types, multiple application cases are created. If the application was submitted within the business hours of the root location for the organization, the application date on the application case is set to today's date. If the application is submitted outside of the business hours of the organization, the application date is set to the next business date.

Mapping the application data to case evidence tables

The data that is entered for the application might be mapped to case evidence tables. The mappings are configured for a particular program by using the Cúram Data Mapping Editor. For the appropriate evidence entities to be created and populated in response to an online application submission, a mapping configuration must be specified for a program.

Associating requested programs with application cases

When the application case is created, the programs that are requested by the citizen are associated with the relevant application case. Some organizations might impose time limits within which an application for a program must be processed. A number of timer configuration options are available for a particular program. These timers are set when a program is associated with an application case.

If the eligibility is determined by a remote system, configurations are provided to allow a web service to be started on a remote system.

Displaying submission confirmation

The submission confirmation page is displayed upon successful submission of an application to the agency. The submission confirmation page displays the reference number that is associated with the submitted application. Citizens can use this reference number in any further correspondence about application with the agency.

Configuring intake applications for PDFs

The citizen might also open and print a PDF. The configuration of the intake application determines the actual PDF that opens. The application can be configured to use a PDF designed specifically by the agency with the intake application, or, if no PDF form is specified, to use a generated generic PDF. If an agency-designed form is specified, this form is opened when the citizen clicks the **PDF** link. For programs with associated mapping configurations of type **PDF Form Creation**, the data that is entered during the online application is copied to the PDF form. The data is copied for each of the programs for which the citizen is applying with this mapping configuration. If a mapping configuration is not associated with a program, the information that is entered during the online application for that program is not copied to the PDF form. If a PDF form is not specified, a generic generated form opens instead. This form contains a copy of the information that is entered by the citizen when the citizen is completing the online application.

The agency can define additional information to be displayed on the generic generated form. Typically, the information that might be required by the citizen is to help the agency process the application timely and effectively for both the agency and citizen. Proof of identity is an example of this additional information. This additional information is configurable for each type of application.

Submission confirmation

When citizens successfully submit an application, going through the sign and submit screen, they are brought to an updated version of the **Overview**. The stages specific to the application process are now updated with a confirmation message to indicate that the application was successfully submitted:

- A customizable icon
- An application reference number
- Informational message for the citizen
- A **Save submitted application PDF** link that allows citizens to download the information entered as part of the application, in PDF format.

Related concepts

Managing existing applications

When a citizen logs in, any existing applications are listed and the citizen is presented with different options that depend on the state of an application.

Printing an application

7.0.3.0

Citizens can open and print an application form in two ways.

- Citizens are directed to a PDF that they can open, complete, and print.
- Citizens are taken through a script. After citizens complete or exit the script, they can open a PDF containing the information they entered.

PDF forms can be configured to provide versions in all supported languages. The programs that can be applied for using the PDF form can also be configured.

Each PDF form that is defined in the administration system is displayed on the **Apply for Benefits** page. The **Apply for benefits** page is displayed when **Apply For Benefit** is selected from the organization **Home** page.

If **PDF Application Form** is configured for the application, **Print application** is displayed.

To open the PDF form, citizens click **Print application**. Citizens can also identify the address of the local office to which to send the form. A system property sets whether the system uses postal codes or counties for this function.

Withdrawing an application

7.0.3.0

Citizens can withdraw successful applications from the **Your benefits** page. If the application did not successfully submit, the **Withdraw** option is not displayed.

Citizens can withdraw a successfully submitted application or they can also withdraw applications for all or any one of the programs.

Citizens can withdraw each program individually. The reasons for withdrawing the program application can be configured for the intake application in the administration system.

The **Reason** field contains a list of configurable code table values that are defined by the administrator. The list of values is configured at application level.

The **First name**, **Last name**, and **Reason** fields are mandatory.

The submit action on the page withdraws the application. The system automatically updates the status of the programs that are associated with the application case to **Withdrawn** and sends a notification to the application caseworker.

The difference between deleting and withdrawing an application

The **Withdraw** action is different from the **Delete** action in that only a submitted application can be withdrawn and only an in-progress application can be deleted. Also, **Delete** physically deletes the application record, **Withdraw** changes the status of the application to *Withdrawn* after the citizen goes through a workflow.

Related concepts

Citizen account

When citizens create a secure citizen account, they can access a range of relevant information. Citizens can also use the citizen account to track and manage interactions with the agency.

Deleting an application

7.0.3.0

Citizens can delete applications that are not yet submitted to the agency.

Citizens can delete applications from the **Dashboard** or the **Your benefits** pages. When citizens click the **Delete application** link for an in-progress application, a confirmation dialog is displayed.

Developing applications using IBM Cúram Universal Access

7.0.3.0

Build your customized Universal Access application using the development resources supplied.

Development environment

7.0.3.0

Choose an Integrated Development Environment (IDE) to develop your application.

Development Tools

There are many IDEs that you can use to develop your application, for example:

- Visual Studio Code
- Atom

- Sublime
- Vim
- Webstorm

There is no dependency on any specific IDE, so you can choose your own environment. However, IBM uses VSCode, which supports many plug ins that make development faster and easier, for example:

- Linting tools (ESLint)
- Code formatters (Prettier)
- Debugging tools (Debugger for Chrome)
- Documentation tools (JSDoc)

IBM does not own, develop, or support these tools.

Development resources

7.0.3.0

IBM Cúram Universal Access includes the following resources that you can use with the IBM Social Program Management Design System to customize and extend Universal Access.

universal-access-starter-pack

A development environment and a fully functional and deployable reference application. The application uses the IBM Cúram Social Program Management modules (core, web-design-system, universal-access, universal-access-ui) to provide a client that can interact with Universal Access.

You can rename, modify, and extend the starter pack to customize the reference application to suit the needs of your organization. The pack demonstrates how a modern and responsive Universal Access client can be built by using React, Redux and the GovHHS Web Design System.

universal-access

This module connects the client application to the IBM Cúram Social Program Management server. *universal-access* makes HTTP requests to the IBM Cúram Social Program Management server to allow the client to interact with a Universal Access installation. Unlike the *universal-access-ui*, this module does not render content. This module uses Redux as a storage mechanism for requests and responses. For more information, see *Working with Redux*.

universal-access-ui

universal-access-ui contains a set of features that presents the views to the user, it depends on *universal-access* to provide the data it needs for those views.

universal-access-mocks

This module provides mock data specific to Universal Access business scenarios for testing purposes. It is consumed by the mock server to provide mock APIs in the development environment so that developers are not required to host an IBM Cúram Social Program Management server during development.

mock-server

The *mock-server* module is a lightweight server that can serve HTTP requests and return mock data as a response. Use *mock-server* during client development as a substitute for a real server to test features.

Developing compliantly

Follow these guidelines to protect your project from making customization changes that are incompatible with the base product, or have the potential to incur upgrade impacts.

Never use undocumented APIs

JavaScript does not have access modifiers such as public/private/protected. It is possible to call functions in SPM modules that are not intended for public use. Calling these functions is not supported as those APIs can change in a future release and break your code.

The only JavaScript APIs that are intended for public use are documented in the `docs` folder of the SPM `node_modules`. For example, `node_modules/@spm/core/docs/index.html`.

Observe the reducer namespace

If you use Redux, your Reducer names must not infringe on the namespace for universal access reducers. All universal access reducers are prefixed with UA, for example. `UABenefitSelection`. When universal access and custom reducers are combined, clashing names override the universal access reducers. Customizing universal-access reducers is not supported.

Don't modify the starter pack files

While you can modify the starter pack files in place, it is better to copy the files and change the copy. Your upgrades will then be easier as you can compare files between the current and previous version of the product without the added complexity of your customization changes. Where upgrade changes are needed, manually apply the changes to your custom version.

Developing with routes

7.0.3.0

Routes define the valid endpoints for navigation in your application. Your application consists of a network of routes that can be traversed by your users to access the application's pages.

IBM Cúram Universal Access uses the *react-router* and *react-router-dom* packages to manage navigation. React Router defines and works with routes. For more information, see the React Router documentation at https://github.com/ReactTraining/react-router/tree/master/packages.

The UARoutes component

7.0.3.0

The module for Universal Access exports the *UARoutes* component, which exposes the routes defined by the module. The defined routes are the suite of pages that are prebuilt and available for reuse in Universal Access.

UARoutes component

You can import and reuse the UARoutes component in your application. The code example shows how import and reuse the UARoutes component in a sample application.

```
import React from 'react';
import { injectIntl, intlShape } from 'react-intl';
 import { HashRouter } from 'react-router-dom';
import '@spm/web-design-system/js/govhhs-wds.min';
 import { UARoutes } from '@spm/universal-access';

const App = (props) => {
  return (
    {/** You must define your routes controller (Hash vs Browser) */}
     <HashRouter>
      <div className="app">
        <div className="my-header-navigation">
```

```
          <a href="#/">Home</a> | <a href="#/faq">Faq</a>
        </div>
        <UARoutes />
      </div>
    </HashRouter>
  );
};

App.propTypes = {
  intl: intlShape.isRequired,
};

export default injectIntl(App);
```

Note: In the example application, the UARoutes are wrapped in a *HashRouter*. However, the module for Universal Access does not currently support the *BrowserRouter* component. Routes do not resolve if you use *BrowserRouter*. For more information, see https://github.com/ReactTraining/react-router/tree/master/packages.

Adding routes

7.0.3.0

You can add a route by including a new route anywhere inside your Router component.

The following code example adds a route to `MyNewPageComponent` into the router component:

```
import { HashRouter, Route } from 'react-router-dom';
…
<HashRouter>
 <div className="app">
  <div className="my-header-navigation">
   <a href="#/">Home</a> | <a href="#/my-new-page">New Page</a>
  </div>
  <UARoutes />
  <Route path="/my-new-page" component={MyNewPageComponent} />
 </div>
</HashRouter>
```

Replacing routes

7.0.3.0

You can replace existing paths from the Universal Access module's UARoutes component with your preferred component.

Wrap your routes in a *<Switch>* component

You can replace existing paths from the UARoutes component with your preferred component. To achieve this, you must first wrap your routes in a *<Switch>* component from react-router. This action ensures that the first match of the requested path that is found in your application is used to resolve the path. For more information on Switch, see https://github.com/ReactTraining/react-router/tree/master/packages.

Add a route with the same path

When you have wrapped in *Switch*, you add a route with the same path as the page you are overriding.

Note: This route must come before the *<UARoutes/>* component to ensure it is matched first.

The following code example shows a replacement route to *MyHomePageComponent* enclosed in a *<Switch>*:

```
import { HashRouter, Route, Switch } from 'react-router-dom';
…
<HashRouter>
 <div className="app">
  <div className="my-header-navigation">
   <a href="#/">Home</a> | <a href="#/my-new-page">New Page</a>
  </div>
  <Switch>
   <Route path="/" component={MyHomePageComponent} />
   <UARoutes />
   <Route path="/my-new-page" component={MyNewPageComponent} />
  </Switch>
```

```
 </div>
</HashRouter>
```

Redirecting routes

7.0.3.0

You can redirect existing paths by using the react-router Redirect component.

Redirecting a route

The following code example imports the *Redirect* component and redirects the path *'/bring-me-home'* to "/".

```
import { HashRouter, Route, Switch, Redirect } from 'react-router-dom';
…
<HashRouter>
 <div className="app">
  <div className="my-header-navigation">
   <a href="#/">Home</a> | <a href="#/my-new-page">New Page</a>
  </div>
  <Switch>
   <Route path="/" component={MyHomePageComponent} />
   <Redirect path"/bring-me-home" to="/"
   <UARoutes />
   <Route path="/my-new-page" component={MyNewPageComponent} />
  </Switch>
 </div>
</HashRouter>
```

Removing routes

7.0.3.0

You can remove unwanted routes from IBM Cúram Universal Access.

You might want to reuse some but not all of the Universal Access <UARoutes/>. For those routes that you want to remove instead of replacing, use the react-router <Redirect> component to send users to a '404' style page, or some other valid end point.

You must declare the redirect before the <UARoutes/> component. You must also wrap the redirect in a *<Switch>* component. The following code example removes the route to "FAQ" by redirecting to a 404 page:

```
<HashRouter>
 <div className="app">
  <div className="my-header-navigation">
   <a href="#/">Home</a> | <a href="#/faq">FAQ</a>
  </div>
  <Switch>
   <Redirect path="/faq" to="/404page" />
   <UARoutes />
  </Switch>
 </div>
</HashRouter>
```

Developing with the mock server

7.0.3.0

The mock server is a mock API service that is provided to aid rapid development. The mock server serves APIs that simulate calling real web APIs. When you are developing your application, the mock server provides a lightweight environment against which the React components can be tested communicating with the services that provide their data.

Configuring the mock server

Configure the mock server location through the following properties in the `.env.development` file. You can change these values to suit your needs.

- `REACT_APP_REST_URL=http://localhost:3080`

- REACT_APP_BASE_URL=http://localhost:3080
- REACT_APP_API_URL=http://localhost:3080
- MOCK_SERVER_PORT=3080

Deploying the mock server

Deploy the mock server by using the following command from the root directory of your project:

```
npm run start:mock-server
```

However, when you are developing locally, you can use the following command that starts both the mock server and the client.

```
npm run start
```

See the `package.json` file in your project for the full list of commands.

Adding mock APIs

The universal-access project includes a number of mock APIs that simulate calling the SPM Universal Access APIs. These mock APIs support running some basic scenarios in development mode for the existing set of features.

As you develop your application, you typically create new APIs that you also want to mock. When the mock server starts, it looks to import the `/mock/apis/mockapis` file relative to the folder the command was started from. In this file, the mock-server expects to find three objects, GET, POST, and DELETE, that it can query to serve API requests for those HTTP methods.

The format of the mock definition is a relative URL that is assigned a JavaScript object. For example, the following code assigns the object `user` to the URL `/user`, and the object `payments.json`, which is read from a file, to the `/payments` URL.

```
const user = {

  'firstname': 'James',

  'surname': 'Smith',

  'gender': 'male',

   ...

}

const mockAPIsGET = {
  // ADD YOUR GET MOCKS HERE

  // Example of providing mock data in response to an API request in
  // the format uri:mockobject
  '/user': user,

  '/payments': readFile('./payments/payments.json)
};
```

If you use mocking extensively, it is better to use separate files and folders to structure your mocks.

Using universal-access mock APIs

The `mockapis.js` file is preconfigured to import and use mock APIs defined and exported by the universal-access package. This allows your project to reuse and extend the set of universal-access mock APIs.

```
const mockAPIs = require('@spm/universal-access-mocks');

// Extract the existing universal access GET,POST and DELETE mocks for merging.
const UAMockAPIsGET = mockAPIs.GET;
const UAMockAPIsPOST = mockAPIs.POST;
const UAMockAPIsDELETE = mockAPIs.DELETE;

...

//create custom mocks

...

// Merge UA mocks with custom mocks
const GET = Object.assign({}, UAMockAPIsGET, mockAPIsGET);
const POST = Object.assign({}, UAMockAPIsPOST, mockAPIsPOST);
const DELETE = Object.assign({}, UAMockAPIsDELETE, mockAPIsDELETE);

module.exports = { GET, POST, DELETE };
```

Where the same URL is used by a custom mock that was previously assigned to a universal-access package mock, the custom mock replaces the universal access version.

Developing authentication

7.0.3.0

The universal-access package exports the Authentication module, which can be used to log in and out of the application and to inspect the details of the current user. The login service is passed a user name and password, and optionally a callback function that is invoked when the authentication request is completed.

Authentication services

The Authentication API works in three modes:

- Simple Authentication (Development mode)
- SSO Authentication
- JAAS Authentication

Simple Authentication (Development Mode)

During client development, the authentication defaults to use a simple authentication that does not require an SPM server. This simple authentication bypasses proper authentication (JAAS or SSO) and instead accepts the user name `dev` without any password. The login process can be ran and allows access to the 'user account' password protected pages.

This simple authentication is sufficient to do most client development work and avoids the need to configure your client application to communicate with an SPM server. It is triggered by the `REACT_APP_SIMPLE_AUTH_ON=true` property in the `env.development` file.

You can set `REACT_APP_SIMPLE_AUTH_ON=false` if you want to trigger an SSO or JAAS login service.

SSO Authentication

The application supports single sign-on (SSO), which is a typical use case for many enterprises that serve multiple applications with a single user name and password for their clients. The client application can be configured to use SSO through the `REACT_APP_SSO_ENABLED=true` environment property.

For more information about configuring your universal access deployment to use SSO, see "Configuring single sign-on" on page 78.

JAAS Authentication

If not in development mode, and not using single sign-on, then the login process defaults to use the standard JAAS login module.

- `REACT_APP_SIMPLE_AUTH_ON=false`
- `REACT_APP_SSO_ENABLED=false`

The JAAS login module is exposed through the SPM universal access API at the `/j_security_check` end point and authenticates the user against the SPM database of users. For more information about JAAS login, see Authentication Architecture.

User Account Types

The universal access client supports three different user account types, Public, Generated, and Citizen. For more on user accounts and security see User Accounts. If you want to customize the log in and sign up process provided by the universal access starter pack, the Authentication module provides log in functions to support each of these three user account types.

```
Authentication.login

Authentication.loginAsPublicCitizen

Authentication.loginWithGeneratedUser
```

Tracking the logged in user

The universal access client application uses 'session storage' in the browser to store some basic details of the currently logged-in user after they are authenticated with the server. This session storage is typically used to inform the client application what views it should present, for example if no user is logged in, then the login and signup page buttons are presented on the home page.

The Authentication module provides functions that query who the current logged in user is and their account details, according to the session storage in the browser.

```
Authentication.getLoggedInUser

Authentication.getUserAccount
```

Logged in - Client vs Server

It is possible for the user to seem logged in on the client when they are not logged in on the server. This does not compromise the security of the application. The SPM server APIs use session tokens that are stored in cookies to determine whether the current user is authenticated. The cookies are transmitted with each API call, and only a valid token results in a successful response.

For example, if a user's session times out on the server, the next API request to the server results in a 401 unauthorized response, even if the user seems to be logged in to the client application. This behavior

ensures that no matter what the client application says about the currently logged-in user, the server responds only to valid session tokens.

Developing with RESTService

7.0.3.0

The RESTService module is exported from the `@spm/core` package and provides a set of functions that allow SPM APIs to be called from a web application.

The module supports the following HTTP methods:

- GET
- POST
- DELETE

They are supported through the following methods:

- `RESTService.get(url, callback, params)`
- `RESTService.post(url, data, callback)`
- `RESTService.del(url, callback)`

The full API documentation is in the doc folder in the `@spm/core` package.

You don't have to use the RESTService module to communicate with SPM APIs, you can create your own service. However, the RESTService module does provide the following functions during communications.

Authentication

Authentication of the user is handled transparently by the RESTService. Once a user is authenticated, the REST APIs automatically send the required 'credentials', that is, the authentication cookies, with each request. For more on how authentication is handled for REST, see Cúram REST API security.

If a user's session is invalidated before a new request is made to a REST API, then the '401 unauthorised' response is returned by the server. The RESTService relays the response to the callback function passed by the caller.

Handling responses

The RESTService formats the response from the server to ensure that callbacks receive the response in a consistent manner.

Each get, post, and delete method accepts a callback function from the caller. This callback function when invoked by the RESTService will receive a boolean indicating success or failure of the API call and the response. This allows the callback function to deal with the result For example, a failure can be used to trigger your code to throw an error with the response data that can be used to trigger an error boundary. For more information on the callback function parameters, see the API documentation for the RESTService.

User Language

The 'Accept-Langauge' HTTP header is automatically set by the RESTService based on the user's selected language, which the user can select using the language picker in the reference application. This allows the server to respond in the correct locale where locale sensitive information is being handled on the server.

The locale passed in the header is set in the transaction that is initiated by that REST request, and is used for the duration of that transaction. For more on transactions, see Transaction control.

Handling Timeouts

The RESTService can manage unresponsive calls to the server. The following properties are set, and can be modified, in the `.env` files to set thresholds for timeouts.

- `REACT_APP_RESPONSE_TIMEOUT=10000 // Wait 10 seconds for the server to start sending`
- `REACT_APP_RESPONSE_DEADLINE=60000 // but allow 1 minute for the file to finish loading`

Simulating slow responses

During development, it is important to test that your application continues to operate in an acceptable way even when network responses are slow. You can simulate a slow network connection by setting a property in the `.env.development` file in the root of your project.

For example, setting `REACT_APP_DELAY_REST_API=2500` delays the response from all GET requests for 2.5 seconds.

The value can be set to any positive integer to adjust the delay.

Developing with Redux

7.0.3.0

Redux is used as a client-side store to store data that is retrieved by the IBM Cúram Social Program Management APIs and data that is used to present a consistent user experience.

What is Redux?

Redux is a client-side store that provides a mechanism for holding data in the client (browser).

- The store is typically used to manage state in the client application. State can include the following types of data:
  - System data that is returned from an API request.
  - User input data that is collected before it is posted to APIs.
  - Application data that is not sent from, or sent to, the server, but is created and maintained to control how the application works. For example, transient user selections like hiding or showing a side pane.
- Redux uses a unidirectional architecture, which simplifies the process of managing state.
- Redux can be used as a caching mechanism to avoid unnecessary network round-trips, although this usage needs careful consideration to ensure the data that is presented is always current.
- Generally Redux proves to be beneficial as your application grows and becomes more complex. By centralizing state management and offering tools that give a holistic view of the application state, development can scale more easily.

Note: The remainder of this document assumes that you are familiar with Redux and using Redux with React components. If you are not familiar with these technologies and how they work together, it is recommended that you complete tutorials from the official sources for these technologies.

How is Redux used in Universal Access

Universal Access uses Redux to store the data that is retrieved by the IBM Cúram Social Program Management APIs.

Each GET API used by universal access has an associated ‘store slice’ where the response of the API is stored. React components can monitor the store for updates relevant to them and automatically update as data changes. The store is also used for collecting user input, such as user information that is

requested while users sign up. This data can then be retrieved from the store and posted to the SPM server.

Other parts of the store are not tied to IBM Cúram Social Program Management APIs, and track data that is used to present a consistent user experience.

Creating a Redux store

By default, the Universal Access starter pack is configured to use a Redux store. This is necessary to allow it to use the `universal-access` and `universal-access-ui` packages. The store configuration is initiated from the `src/index.js` file in the starter pack.

```
...

import configureStore from './store';

...

// ==================================
// 1. Create the store and initialize the universal-access module.
// ==================================

// Create a Redux store
// This is optional, if you don't want to create your own Redux store you can remove this,
const appStore = configureStore();

// Configure the UA package
// 1. If you are using your own store, you must share it with UA
UAReduxStore.configureStore(appStore);

...
```

Configuring the store

Configure the store in the `src/store.js` file, which exports the `configureStore` function that can be called to create a new Redux store. The configure store function can be modified to:

- Add Redux 'middleware'.
- Provide a custom set of reducers.

  Note: To work with the universal-access packages, the store must use the Universal Access reducers that are exported from the `universal-access` package.

Adding reducers

If you decide to use Redux with your custom React components, you must create custom reducers and add them to the store. All Universal Access reducers are prefixed with UA, for example `UAPaymentsReducer`. Do not use the UA prefix in custom reducers to avoid overriding `universal-access` reducers. Overriding reducers is not supported, see “Developing compliantly” on page 18.

The `src/rootReducer.js` file defines the set of reducers for the store, and combines them into a single *root reducer* that can be passed to the `configureStore` function in the `src/store.js` file.

For convenience, the file defines an `AppReducers` object where you can add custom reducers. The custom reducers that are defined in the `AppReducers` object are combined with the `UAReducers` imported from the `universal-access` package, and the superset of reducers is returned.

The following code excerpt shows the `rootReducer` function that returns the combination of Universal Access reducers and custom reducers.

```
const AppReducers = {
  // Add custom reducers here...
```

```
  // customReducer: (state, action) => state,
};

/**
 * Combines the App reducers with those provided by the universal-access package
 */
const appReducer = combineReducers({
  ...AppReducers,
  ...UAReduxReducers,
});



/**
 * Returns the rootReducer for the Redux store.
 * @param {*} state
 * @param {*} action
 */
const rootReducer = (state, action = { type: 'unknown' }) => {
  ...
  return appReducer(state, action);
};
```

Clearing Redux store data

The Redux store is a JavaScript object that is stored in the global object for the browser window. The content of the store is visible through inspection, either programmatically or by browser plug-in tools, such as the developer tools. It is critical that the store is cleared for the current user when they log out to ensure that no sensitive user data is left on the device for malicious actors. The log out feature that is provided by the starter pack triggers a Redux action that clears the store.

Developing with universal-access modules

7.0.3.0

Universal Access modules provide a connection between React components and the Redux store. This design allows the React components to focus on presentation and reduces the complexity of the code in the presentation layer. The modules also manage the communication between the client application and the IBM Cúram Social Program Management APIs, including authentication, locale management, asynchronous communication, error handling, Redux store management and more.

Modules and APIs

Each universal-access module is responsible for handling the communication between a single API. For example, the Payments module is responsible for communicating with the `/v1/ua/payments` API. For more information about IBM Cúram Social Program Management APIs, see Connecting to a Cúram REST API.

Blackbox

Modules are blackbox so are not open to customization or extension. The modules expose actions and selectors to interact with the module. The actions and selectors are APIs that are documented in the `<your-project-root>/node_modules/@spm/universal-access/docs/index.html` file.

Actions

Module actions are used to modify the Redux store, like inserting, modifying, or deleting data from the store. For example, the `PaymentsActions` action modifies the payments slice of the store.

Some actions include calls to APIs. For example, `PaymentsActions.getData` action calls the `v1/ua/payments` API and dispatches the result to the payments slice of the store, or sets an error if the API call fails.

Selectors

Module selectors are used to query the Redux store. They provide the response to predefined store queries. For example, the `PaymentsSelector.selectData` selector returns the `/payments/data` slice from the store, and the `PaymentsSelector.selectError` selector returns the value of the `/payments/error` slice of the store.

Reusing Universal Access modules in your custom components

You can use the actions and selectors from the universal-access package to connect your custom components to existing IBM Cúram Social Program Management APIs and the Redux store. You can use the `react-redux` module to connect your components. Examples of this technique can be found in the `universal-access-ui` features.

For example, the following code is from the `PaymentsContainer` file in the Payments feature. The code shows how the actions and selectors from the Payments module are connected to the properties of the Payments component.

This pattern is documented extensively in the official Redux documentation.

```
import { connect } from 'react-redux';
import React, { Component } from 'react';

...

/**
 * Retrieves data from the Redux store.
 *
 * @param state  the redux store state
 * @memberof PaymentsContainer
 */
const mapStateToProps = state => ({
  payments: PaymentsSelectors.selectData(state),
  isFetchingPayments: PaymentsSelectors.isProcessing(state),
  paymentsError: PaymentsSelectors.selectError(state),
});
/**
 * Retrieve data from related rest APIs and updates the Redux store.
 *
 * @export
 * @param {*} dispatch the dispatch function
 * @returns {Object} the mappings.
 * @memberof PaymentsContainer
 */
export const mapDispatchToProps = dispatch => ({
  loadPayments: () => PaymentsActions.getData(dispatch),
  resetError: () => PaymentsActions.resetError(dispatch),
});
/**
 * PaymentsContainer initiates the rendering the payments list.
 * This component holds the user's payment details list.
 * @export
 * @namespace
 * @memberof PaymentsContainer
 */
export default connect(
  mapStateToProps,
  mapDispatchToProps
)(PaymentsContainer);
```

Developing with headers and footers

7.0.3.0

IBM Cúram Universal Access contains a predefined header and footer. The header and footer contain content that is found in the header and footer of an application, such as links, **log in**, and **sign up** buttons, and menus for logged in users.

Headers and footers

You can customize your application headers and footers by replacing the sample components with your own custom versions.

The App.js file in the *universal-access-sample-app* module, reuses the sample *ApplicationHeader* and *ApplicationFooter* components that are provided by the universal-access module by placing them above and below the main content of the application:

App.js

```
    <HashRouter>
      <ScrollToTop>
        <div className="app">
          <a className="wds-c-skipnav" href="#main-content">
            {formatMessage(translations.appSkipLink)}
          </a>

          <Route path="/" component={ApplicationHeader} />
          <main id="main-content" className="main-content">
            <Content>{routes}</Content>
          </main>

          <ApplicationFooter />
        </div>
      </ScrollToTop>
    </HashRouter>
```

Header

Typically, an application header has two views. One view has items relevant to users who are not logged in or signed up, for example a **Sign Up** button. The second view shows items that are relevant to users who are signed up and logged in, for example an **Update your profile** button.

To facilitate the separate views, use a react-router-dom *Route* component. The App.js sample demonstrates wrapping the *ApplicationHeader* component in a Route component and passing Route information to the *ApplicationHeader*. This allows the *ApplicationHeader* to query the Route properties and decide what to display based on the current location in the application. For example, you might want to show a different view for the login page route (‘*my-app-domain*/#/login’) from the application home page route (‘*my-app-domain*/#/’).

The following code sample shows how the *ApplicationHeader* queries its location property to find out what page the application is displaying. The sample code then uses this information to decide what to show in the header.

```
 get isOnLoginPage() {
  return this.props.location.pathname === '/login';
}

render() {
 return (
  <Header
    title={this.pageTitle}
    type="scrollable"
    logo={<img src={logo}
    alt="agency"
    id={this.props.loggedInUser} />}>
    <PrimaryNavigation type="scrollable">
      <TabList scrollable>
        <Tab
         id="tab1"
```

```
          href="#/"
          text={
            this.props.intl.formatMessage(translations.headerHomeLabel)}/>
             <Tab
               id="tab2"
               href="#/my-applications"
               text={this.props.intl.formatMessage(
                  translations.headerBenefitsLabel)}/>
           </TabList>
         </PrimaryNavigation>
         <SecondaryNavigation type="Scrollable"/>

          {/* Show signed out menu */}
          {!this.isOnLoginPage &&
           this.props.loggedInUser === null &&
           !this.isUserProfileLoaded &&
           this.signInMenu}

          {/* Show signed in menu */}
          {this.props.loggedInUser &&
           this.isUserProfileLoaded &&
           this.profileMenu}
         </SecondaryNavigation>
       </Header>
    );
  }
```

Login and sign up in the header

If you are building your own customer header, you must identify which page you are currently displaying the Header on, you must also differentiate between logged in and logged out users. Whether a user is logged in or out can be determined by using the authentication API provided by the universal-access module. The Authentication API provides functions to allow you to log in and out of the application, and also allows you to query if a user is logged in and who that user is. For more information, see the Authentication API documentation.

The following code sample shows how the *ApplicationHeader* uses the Authentication API. In this function, a check is made to see whether a user is logged in before it loads that user's profile. The user's profile is needed to display the user's full name in the header.

```
fetchProfile() {
  if (Authentication.isLoggedIn() && !this.isUserProfileLoaded) {
     this.props.loadProfile();
  }
}
```

Footer

You can add a footer to the bottom of the application page in the same way as you add the header to the top of the page. The universal-access module provides a sample application footer that is used in the universal-access-sample-app, see the `App.js` sample. The sample footer is static and does not change based on the location or the authentication state, however the footer can be made dynamic by following the example from the header.

Related tasks

Changing the application header or footer
Build on the styling scenario from *Using the Web Design System to style content* by adding a link to the application header or footer. For more information about the application header and footer, see “Developing with headers and footers” on page 28.

Customization Scenarios

7.0.3.0

Customize the IBM Cúram Universal Access web application.

These scenarios take you through a series of real application customization situations. Each scenario builds on the previous one to build out new content in your Universal Access project.

Changing the application text

7.0.3.0

You can change the default text in the application by providing custom text that overrides the default text for any language. In this example, an English language message is changed.

About this task

Each message or text string that citizens see in the app is provide using the *react-intl* package that supports the globalization of React apps. *react-intl* allows the messages to be extracted and translated to other supported languages, it also adds placeholders for data, for example.

To change the existing text of any of the languages that are provided by IBM, you must provide a custom version of the message that is mapped to the same *message id*.

Procedure

1. Find the ID of the message you want to replace. All product messages are defined in the *universal-access-ui* package. In your project, go to `/node_modules/@spm/universal-access-ui/src/locale`.
   a) The `locale` folder contains message files for each supported locale. For your chosen language, search the appropriate `message_xx.json` for the text string that you want to replace. For example, to change the English text **Apply for a benefit**, search `messages_en.json` for that string as shown in the following example. If there is more than one instance of the string, you must find the correct message ID for the text you want to change. The simplest way to find the correct instance is to try replacing each ID one by one, reloading the page each tine to see if the new string is displayed.

```
"System_Messages_Alert_Description": "System messages alert description",

"Payments_NoPaymentMessages": "No payment messages",

"Payments_ApplyForABenefitLink": " Apply for a benefit ",

"TODO_NoTODOMessages": "No to-dos",

"TODO_CaseworkerMessage": "Your caseworkers can create to-dos for you.",

"Meetings_NoMessages": "No meetings",
```

   b) For the **Apply for a benefit** string, use the associated ID *"Payments_ApplyForABenefitLink"* to override the message in your custom `messages_en.json`.
2. Create a custom message file by creating a `messages_en.json` file in the `src/locale` folder. Custom messages are injected into the application at application start. For more information, see *Localizing the application*. To help you get started, the starter pack provides a locale folder from where custom messages files are automatically loaded. Assuming this process has not been customized for your project, you can add your custom file to this folder: `src/locale`.
3. To replace the message, create a new *id:message* mapping in your custom message file by using the same ID value as shown in the following example.

```
"Payments_ApplyForABenefitLink": " Click here to apply for a benefit ",
```

Related concepts

Providing the application in another language

IBM Cúram Universal Access is globalized, that is it can be translated into different languages. Universal Access also supports regionalization of currencies, calendar and date formats as defined by IBM Cúram Social Program Management on which the application depends, for more information, see *Developing for Regional Support*.

Adding content to the application

7.0.3.0

Build on the text change scenario from *Changing application text* to add a new route and add content that is displayed when that route is loaded.

Before you begin

If you are not familiar with React and React Router, you must take a basic course in building a web application with React and React Router.

The term "feature" refers to the content that is displayed when a route is loaded, this content is what citizens see on the user interface. A feature is an abstraction that includes all the content that comes together to create the end user experience. A feature could be a collection of JavaScript files, json files, and APIs that work together to generate the end user experience. The term "feature" could be referred to as a page, view, or component in other application environments.

This scenario adds a new feature that presents a logged-in person's details in the main content area when a `/person` URL is loaded. This scenario is built on in later scenarios by calling APIs, using client side stores, error handling, or globalization.

About this task

When you extend the IBM Cúram Universal Access reference application you might want to introduce new content that is displayed when citizens click a link.

Procedure

1. Create the content for the feature, take the following steps:
   a) Create a folder called `features` under the `/src` folder in your project
   b) Add a subfolder called `person`, and add a file called `PersonComponent.js` to that folder as shown in the following example.

   ```
   src/features/Person/PersonComponent.js
   ```

   c) Add some HTML to display when the component is loaded. The following example displays some data that is returned by an API:

   ```
   import React from 'react';

   const Person = () => { return (
       <div>
         <h1>James Smith</h1>
         <h2>Gender: Male</h2>
         <h2>Born: April 1st 1996</h2>
       </div>
   )};
   export default Person;
   ```

2. Add a route to link to your feature, take the following steps:
   a) Declare an associated URI for each feature in the application. The URI allows React to present the feature when the URI is requested in the browser. This technique is standard *'React Routing'* for displaying features. For more information on routes in the Universal Access client, see *Customizing navigation in the application*. Add a simple component that displays when the route is loaded:
      1) Open `routes.js` in your project.
      2) Import a *Person* component from the folder `features/person` which you create in the next step.

3) Add a new route "/person" that loads the *Person* component as shown in the following example:

```
import React from 'react';
import { Route, Switch } from 'react-router-dom';
import { Routes as UARoutes } from '@spm/universal-access-ui';
 import Person from './features/PersonComponent'

export default (
  <Switch>
    <Route path="/person" component={Person} />
    <UARoutes />
  </Switch>
);
```

3. Load the new feature by using the route, take the following steps:
   a) Run your application, enter the following command:

```
npm run start
```

   b) Start a browser and enter the full URL for the feature, for example: http://localhost:8888/#/person

Results

When the application loads, the person details are displayed in the main content area.

Related concepts

Developing with routes

Routes define the valid endpoints for navigation in your application. Your application consists of a network of routes that can be traversed by your users to access the application's pages.

Using the Web Design System to style content

7.0.3.0

Build on the person scenario from *Adding content to the application* to style the content of a person's details.

Before you begin

The Web Design System is a design framework that enables developers to build a cohesive and consistent application. By selecting components from a design catalog and applying design principles, design and development is faster and user experience is improved.

About this task

The full catalog of Web Design System components, including descriptions of when and where to use them, is documented in the *govhhs-wds-react* package. You can access these packages through `index.html` file in `/node_modules/@govhhs/govhhs-wds-react/docs`. This scenario uses a number of Web Design System components to improve the person feature.

Procedure

1. Import contents from the Web Design System. Enter the following command to import the *Avatar* and *MediaObject* components from the package `@govhhs/govhhs-wds-react`:

```
import {Avatar, MediaObject} from '@govhhs/govhhs-wds-react'
```

2. Update `PersonComponent.js` to use the Grid, Column, Card, MediaObject, Avatar, and List components to display the person's details. You can also include an address in a separate card.

   Use the following code to replace the previous `PersonComponent.js`:

```
import React from 'react';
import {Grid, Column, Card,CardBody,CardHeader, List, ListItem, Avatar, MediaObject } from
'@govhhs/govhhs-wds-react'
```

```
const avatarMediaJames = <Avatar initials="JS" size="medium" tooltip="profile photo" />;
const Person = () => {
    return (
        <Grid className="wds-u-p--medium">
            <Column width="1/2">
             <Card>
                <MediaObject media={avatarMediaJames} title="James Smith">
                <List>
                    <ListItem>Gender: Male</ListItem>
                    <ListItem>Born: April 1st 1996</ListItem>
                </List>
            </MediaObject>
            </Card>
            </Column>
            <Column width="1/2">
             <Card title="Address">
                 <CardHeader title="Address"/>
                 <CardBody>
                    <List>
                        <ListItem>1074, Park Terrace</ListItem>
                        <ListItem>Fairfield</ListItem>
                        <ListItem>Midway</ListItem>
                        <ListItem>Utah 12345</ListItem>
                    </List>
                </CardBody>
            </Card>
            </Column>
        </Grid>
)};
export default Person;
```

3. Save `PersonComponent.js`.

Results

Reload the application, the application should show the updated styling.

Changing the application header or footer

7.0.3.0

Build on the styling scenario from *Using the Web Design System to style content* by adding a link to the application header or footer. For more information about the application header and footer, see “Developing with headers and footers” on page 28.

Before you begin

To customize the header, you must create your own custom version. To keep this scenario brief, work on the header only and copy the existing header from *universal-access-ui*. Make some small changes to the header to show how it can be customized. Alternatively, completely replace the header or footer with your own version.

About this task

Change the application header to include a new link that to take you to the **My Details** page.

Procedure

1. Copy the Universal Access header by copying the `node_modules/@spm/universal-access-ui/src/features/ApplicationHeader` folder to `src/features`.
2. Fix any broken imports. Take the following steps:
   a) Use ESLint or a similar linting tool to find any errors where imports are not found.

      Note: If you do not use a linting tool, you get build errors.

   b) Errors are generated because the *universal-access-ui* uses relative paths when it imports dependencies from its own project. For imports that are within the *universal-access-ui module*, but outside the `features/ApplicationHeader` folder, you must change the imports to reference the official exported version of those dependencies from the *universal-access-ui* node module.

c) For each import that is not resolved, find the equivalent export in the *universal-access-ui* package. Inspect `node_modules/@spm/universal-access-ui/src/index.js` to find the list of exported artifacts and their exported names.

The *Paths* module is referenced in the *ApplicationHeader* by using the default import from a relative path as shown in the following example: `import PATHS from '../../router/Paths'` Amend module as shown in the following example: `import { Paths } from 'universal-access-ui'`

d) Repeat this procedure for all the files in the `ApplicationHeader` folder, some of the imports of *'Paths'*, and for some other references such as *'ErrorBoundary'* and *'AppSpinner'*.

3. Replace the existing header with your custom version, take the following steps:

a) Open `src/App.js file` and remove the imported *ApplicationHeader* from *universal-access-ui*.

b) Import your cloned version from `./features/ApplicationHeader` as shown in the following example:

```
import ApplicationHeader from './features/ApplicationHeader';
```

Import *ApplicationHeader* as a default import, without curly brackets, rather than a named import. Alternatively, you can add a named export to your *ApplicationHeader* feature.

4. Update the header feature to include a tab that loads the */person* page take the following steps:

a) Open `constants.js` in `src/features/ApplicationHeader/components`. `constants.js` defines an object that represents a navigation item for the header.

b) Add and entry for the new page **My Details** as shown in the following example:

```
/**
 * Application navigation header tabs.
 */
const NAVIGATION_HEADER_TABS = {
    ...

  PROFILE: { NAME: 'PROFILE', ID: 'navigation-profile' },
  CHANGE_PASSWORD: { NAME: 'CHANGE_PASSWORD', ID: 'navigation-change-password' },
  MYDETAILS: { NAME: 'MYDETAILS', ID: 'my-details' },

};
```

c) Open `ApplicationHeaderLogic.js`.. `ApplicationHeaderLogic.js.` contains the logic that tracks which tabs are selected so they can be highlighted as active.

d) Update the *isTabActiveForUrlPathname* function to include the new **My Details** page in the **Your Account** section. For brevity, the value is hardcoded in the following example. However you can replicate the pattern that is used by the *universal-access* code to add it to *Paths*.

```
const isTabActiveForUrlPathname = (urlPathname, navigationTabName) => {

  ...
  switch (navigationTabName) {
    case FIND_HELP.NAME:
      return (
        urlPathname === Paths.HOME ||
        urlPathname === Paths.APPLY ||
        urlPathname === Paths.BENEFIT_SELECTION ||
        urlPathname === Paths.APPLICATION_OVERVIEW
      );
    case YOUR_ACCOUNT.NAME:
      return (
        urlPathname === Paths.ACCOUNT ||
        urlPathname === Paths.BENEFITS ||
        urlPathname === Paths.PAYMENTS.ROOT ||
        urlPathname === Paths.PAYMENTS.DETAILS ||
        urlPathname === '/person'
      );
```

Open `ApplicationHeaderComponent.js` and find the Web Design System *PrimaryNavigation* component. `ApplicationHeaderComponent.js` renders the header.

e) Add a tab called **'My Details'** with a link to the person feature inside `ApplicationHeaderComponent.js`. For brevity, the example is hardcoded values, but you can replace these values with variables. If you want, you can also localize the tab.

```
..
<PrimaryNavigation>
  <Tabs>
    ...

    <Tab
      id={NAVIGATION_HEADER_TABS.YOUR_BENEFITS.ID}
      href={HASH_SYMBOL + LOCATIONS.BENEFITS}
      label={formatMessage(translations.headerYourBenefitsLabel)}
    />
     <Tab
       id="person_tab"
       href="#/person"
       label="My Details"
     />
  </Tabs>
  ...
</PrimaryNavigation>

...
```

5. Save your file and restart the application.
6. You can modify the application footer in the same way by replacing the *universal-access-ui* version in `src/App.js` with your own custom version.

Results

Navigate to the home page. Note the new tab called **My Details** in the primary navigation area. When you select **My Details**, the person feature is loaded in the main content area.

Related reference

Developing with headers and footers
IBM Cúram Universal Access contains a predefined header and footer. The header and footer contain content that is found in the header and footer of an application, such as links, **log in**, and **sign up** buttons, and menus for logged in users.

Creating an IBM Cúram Social Program Management API

7.0.3.0

Build on the scenario from *Changing the application header or footer*, use a web API to get data to your application.

About this task

The most common way to get data to your application is to use a web API to receive the requested data as a JSON string that your application then parses and renders. IBM Cúram Social Program Management provides development tools and the runtime infrastructure that you can use to build and deploying an API with your IBM Cúram Social Program Management server. The API can be called using the standard HTTP verbs such as GET, POST, and DELETE. The API returns data as a JSON string in the response body. For more information, see *Developing Cúram REST APIs*.

Related information

Developing Cúram REST APIs

Calling an API from the application

7.0.3.0

Call the API you created in *Creating an IBM Cúram Social Program Management API*.

About this task

Features in your application rely on passing data to and from the IBM Cúram Social Program Management server or another service. The reference application already consumes a number of Universal Access APIs to support business features.

This scenario updates the person feature to read the data from an API instead of just displaying hardcoded values. The scenario shows you how to create and use the following items:

- Use the *RESTService* module to helps you call APIs.
- Use the mock server to show you how to create a mock API that allows you to rapidly develop your feature without spending time building and deploying the real APIs that it eventually uses.
- Connect your application to a IBM Cúram Social Program Management development environment that hosts the APIs by using Tomcat to enable real integration testing in the development environment.

Procedure

1. Create a mock API, take the following steps:
   a) In your project, open `/mock/apis/mockAPIs.js`.
      The mock server consumes mockAPIs.js, it contains the mappings from APIs to the mock data. The mock server uses this information to provide the correct data when an API call is made in development mode. `mockAPIs.js` also contains an import from the *universal-access-ui* package and assignments for GET, POST and DELETE APIs as shown in the following example:

```
const mockAPIs = require('@spm/universal-access-mocks');

// Extract the existing universal access GET,POST and DELETE mocks for merging.
const UAMockAPIsGET = mockAPIs.GET;
const UAMockAPIsPOST = mockAPIs.POST;
const UAMockAPIsDELETE = mockAPIs.DELETE;
```

      Use these APIs to test the Universal Access application. For more information, see *Working with the mock server*.
   b) To add more mock data, add your mocks to the placeholders provided. This scenario adds the person data for a person 'James Smith' that is returned when the `'/person'` path is loaded.
   c) Add an object in `mockAPIs.js` to represent James Smith. For simplicity, do not normalize the dates, or use code tables, later scenarios show you how to globalize and handle code tables.

```
const user = {
 firstname: 'James',
 surname: 'Smith',
 dob: 'April 1st 1996',
 gender: 'male',
 address: {
   addr1:'1074, Park Terrace',
   addr2:'Fairfield',
   addr3:'Midway',
   addr4:'Utah 12345',
 }
}
```

   d) Include a value for the URI *'/user'* in the *mockAPIsGET* object to return the mock object as shown in the following example:

```
const mockAPIsGET = {
  '/user': user,
}
```

      The new *'/user'* mock API is merged with the mocks from *universal-access-ui* and is deployed by the mock server on port 3080.

e) Test that the new API is working, start the application using `npm start`.

f) Using the browser, load the */person* URL: http://localhost:3080/person. If successful, the browser displays the response.

2. Use the RESTService module from the core package to make an AJAX call to the API.

   There are many agents that can be used to achieve this. The RESTService uses Superagent to make the AJAX call. The RESTService handles the following functions:

   - Authentication credentials are automatically handled for each call, and users are redirect to log in when appropriate.
   - The user's locale is passed to ensure the response is in the correct locale.
   - Timeouts are managed using the settings from the `.env` file.
   - Errors are captured and thrown in a standard fashion so that the error handling infrastructure is invoked.

   For more information on the RESTService module, see *Working with the RESTService*.

3. Open `PersonComponent.js` file. Make the following changes, check that your application is still displaying the page after each step:

   a) To enable lifecycle methods that are required to manage the API calls, convert the old stateless component to a stateful *React.Component* class:

   `Old stateless Person component`

   ```
   const Person = () => {
      return (
       <JSX code here>
      );
   }
   ```

   `Updated stateful Person component`

   ```
   class Person extends Component {
       render(){
         return (
           <JSX code here>
        )};
   }
   ```

   b) Create local state to hold the API data.

   The local state stores the values returned by the API that drive the render function. Whenever the state is updated, the component rerenders to reflect the state change. For this scenario, hardcode the values for the state in your class constructor so that something is displayed on the page. To differentiate between this temporary default data and the API data, change the *firstName* to 'Roger'. Later, when you introduce the API, the data for 'James' is returned from the API and not the default state as shown in the following example:

   ```
   constructor(props) {
     super(props);
       this.state= {
         user : {
           firstName:'Roger',
           surname:'Smith',
           dob:'April 1st 1996',
           gender: 'Male',
           address: {
             addr1:'1074, Park Terrace',
             addr2:'Fairfield',
             addr3:'Midway',
             addr4:'Utah 12345',
           }
       }
     }
   }
   ```

c) Convert all hardcoded references to use the values from the state.

Now that you have a state object, replace all hardcoded values with references to the state. Replace each hardcoded piece of data with a state reference *{this.state.user.X}*. Examples are as follows:

```
...
class Person extends Component {
    render(){
      return (
        ...
            <Card>
               <MediaObject media={avatarMedia} title= {this.state.user.firstName} >
               <List>
                   <ListItem>Gender:  {this.state.user.gender} </ListItem>
                   <ListItem> {this.state.user.gender} </ListItem>
               </List>
           </MediaObject>
    )};
        ...
}
...
```

d) Import the *RESTService* module.

To call an API you must to invoke one of the methods of the *RESTService* module. First you must import it from the core package:`import { RESTService } from '@spm/core'`

e) Create a *componentDidMount* method to invoke the API call.

When your component is mounted by React, the *componentDidMount* function is invoked. In *componentDidMount* the API call can be made to populate the component state. Update your constructor to set the user values to blank when initializing, this setting ensure that your data is being loaded from the API. Then, add the following code to your Person component. The root location of the API is taken from the values set in your `.env.development` file when in development mode. In production mode, it is taken from the `.env` file.

The `.env.development` file specifies the mock server URL as REACT_APP_API_URL, which has the value http://localhost:3080/ where the mock server is deployed. You can use this environment variable to prepend the */user* API.

The RESTService API accepts a URL and a callback function as parameters. In the following code, the callback function is passed as an anonymous function in the second parameter. Here the 'success' is checked, before the state is updated with the response.

Note: Error scenarios are not handled in this code. The scenario *Handling failures in the application* contains details about failure responses, 'Error Boundaries', and failure handling.

```
componentDidMount() {

    const url = `${process.env.REACT_APP_API_URL}/user`;

    const user = RESTService.get(url, (success, response) => {

      if (success) {

        this.setState((user: response));

      }

    });

  }
```

Results

Start your application, log in and select the **My Details** tab. The tab loads using data pulled from the */user* API. The API that you use in development mode is served from the mock server. In production mode, the

'real' API called using the *REACT_APP_API_URL* defined in the `.env` file. Assuming the contract remains the same between your mock and 'real' APIs, that is, the JSON structure matches in both, you can seamlessly switch between development and production, allowing for a much faster development process.

Related reference

Handling failures in the application
You should build fault-tolerant web applications because, for example, web services such as a REST API are never fully reliable. When handling the expected response, the application must also allow for failures, such as network outages, timed out responses, internal server errors, or software bugs.

Developing with IBM Cúram Social Program Management APIs by using Tomcat

7.0.3.0

Build on the scenario from *Calling an API from the application*, perform integration testing with the real IBM Cúram Social Program Management APIs instead of using the mock APIs in your Universal Access client.

Before you begin

You must be familiar with the IBM Cúram Social Program Management development environment, the development of REST APIs, and the IBM Cúram Universal Access development environment.

This scenario uses IP address 192.1.1.1 to represent the development computer for the IBM Cúram Social Program Management server, and 192.9.9.9 for the computer that hosts the Universal Access client. Therefore, however, these could be the same computer, and you could use the same IP address. Replace this address with the IP address of your development computer.

About this task

The mock server is hosted on the same domain as the application during development http://localhost. However, when your APIs are served from a different domain, you might encounter Cross Origin Resource Sharing (CORS) issues. You can use Tomcat to configure your Universal Access client and IBM Cúram Universal Access server to allow Cross Origin requests. To overcome the CORS issues, the REST toolkit uses a filter that provides the required HTTP headers to allow browsers to accept responses from a different domain. In this scenario, the domain is where the REST application is deployed.

Procedure

1. Configure the IBM Cúram Social Program Management server, take the following steps:
   a) In your development environment, add the following properties to *Bootstrap.properties* and set the *hostname/ipaddress* of the computer where the Universal Access client is to be deployed:
      - *curam.rest.refererDomains = 192.9.9.9*
      - *curam.rest.allowedOrigins = 192.9.9.9*

      Note: If you develop the server and client on the same computer, you can use *"localhost"*.

      The property *curam.rest.allowedOrigins* is the *Origin* value in the CORS headers. Both properties can have comma-delimited domain names, for example, `curam.rest.allowedOrigins = 192.9.9.9, 192.9.9.8, mymachine.mycorp.com` to allow multiple domains to access the IBM Cúram Social Program Management application.
   b) Set the *CATALINA_HOME* environment variable to the location of your Tomcat installation. For example, on Windows set the following variable: `'set CATALINA_HOME=C:\DevEnv \7.0.1\tomcat'`
   c) Build IBM Cúram Social Program Management by using the appbuild server, database, client, and other components.
   d) Run an extra target `appbuild rest` to create the REST project in your `EJBServer\build \RestProject\devApp` directory.

e) Copy `Rest.xml` into your Tomcat `conf/localhost` folder. For more information about building Cúram APIs, see *Developing Cúram REST APIs*.

f) Start the server, RMILoginClient, and Tomcat in the normal way for IBM Cúram Social Program Management.

The REST client starts automatically. When the client is running, the APIs are accessible in the `/Rest` base path, for example: `http://192.1.1.1:9080/Rest/<myapi>`.

2. Configure the Universal Access client, take the following steps:

a) Modify the `.env.development` file that is located in *universal-access-starter-pack* to point to the REST URL on `Eclipse/Tomcat` as shown in the following example:

```
REACT_APP_REST_URL=http://192.1.1.1:9080/Rest
REACT_APP_BASE_URL=http://192.1.1.1:9080/Rest/v1
REACT_APP_API_URL=http://192.1.1.1:9080/Rest/v1/ua
```

Note: If you develop the server and client on the same computer, you can use *"localhost"*.

If you do want to connect to an application on WebSphere®, you must change *"http"* to *"https"* and update to the correct port. 9044 is the default port.

b) Build the application, enter the following command: `npm run build`.

c) Start the application, enter the following command: `npm run start`.

Results

Your Universal Access client application now communicates with the REST deployed on Eclipse with Tomcat.

Note: Run the application on in debug mode to allow it to stop at the breakpoints in the application code.

Related information

Developing Cúram REST APIs

Handling failures in the application

You should build fault-tolerant web applications because, for example, web services such as a REST API are never fully reliable. When handling the expected response, the application must also allow for failures, such as network outages, timed out responses, internal server errors, or software bugs.

Universal Access ErrorBoundary component

According to React, "Error boundaries are React components that catch JavaScript errors anywhere in their child component tree, log those errors, and display a fallback UI instead of the component tree that crashed."

An error boundary component is a React component that implements the *componentDidCatch* lifecycle method. For more information about error boundaries, see https://reactjs.org/

The *universal-access-ui* package exports a reusable ErrorBoundary component. The component has a default behavior to handle error scenarios by replacing the failing component with a generic message.

Note: Authentication errors have a specific handler in the ErrorBoundary component. If the error object that is received by the componentDidCatch method contains a status attribute with a value of '401' (Unauthorized error), then the client forces a log-out in the client application. Citizens are automatically redirected to the **Log in** page, so they can re validate and return to the page they were previously on. This situation typically happens if the session times out or has been invalidated on the server. The source code for the ErrorBoundary component is available in the *universal-access-ui* package.

This scenario shows API error handling in the **My Details** page where the API call fails. This scenario also shows how to use the Universal Access ErrorBoundary component to provide a better user experience when failures occur.

Error boundaries in the Universal Access application

The Universal Access starter pack contains the following two error boundaries:

- The first wraps the entire application to capture errors that might occur when loading the header or footer.
- The second wraps the main content to capture errors that are raised from components that are loaded in the main content section.

The error boundaries are shown in the following example:

```
/**
 * App component entry point.
 */
const App = () => (
  <HashRouter>
    <ScrollToTop>
      <ErrorBoundary>
        <ApplicationHeader />
        <ErrorBoundary>
          <Main pushFooter className="wds-u-bg--page">
            {routes}
          </Main>
        </ErrorBoundary>
        <ApplicationFooter />
      </ErrorBoundary>
    </ScrollToTop>
  </HashRouter>
);
```

The error boundary on the main section allows the application context to be retained. That is, the header and footer continue to be displayed when the error is raised from the main section. This continuity provides a better user experience.

You can replace these error boundaries with your own error boundaries.

Faking an API error

This API failure scenario uses a 404 response as the error, you trigger this failure by temporarily changing the API call to a non-existent API.

Take the following steps:

1. Open `PersonComponent.js`
2. Update the API to call in the *componentDidMount* method to the non-existent '/user1' as shown in the following example:

   ```
   componentDidMount() {
      const url = `${process.env.REACT_APP_API_URL}/user1`;
      RESTService.get(url, (success, response) => {
        if (success) {
          this.setState({user: response});
      });
    }
   ```

3. Save your code and wait for the application to reload.

Provided you followed the previous scenarios, when the application reloads it displays the person and address cards but with no details. The values default to be the values that are created in the constructor of the `PersonComponent.js` file. Use the developer tools in your browser to verify the status of the network call that is made for the '/user1' API. You should see that the response status is a 404 indicating that the network call failed.

Catching an API failure

Using the failure scenario from *Faking an API error*, you can modify the code to cater for this failure. The API call is asynchronous, and the callback runs outside the context of the Component tree. This execution mode means that the error that thrown in the call-back function is not caught by the *componentDidCatch* method of the *ErrorBoundary*. Therefore, instead of throwing an error in the callback, you update the state of the component. You can then use the *lifecycle* methods of the React component to react to the updated state when it arrives. Use a state attribute 'apiCallFailed' to hold the response.

In the componentDidMount method, add a branch to the callback passed to the RestService.get method. The failure branch sets the apiCallFailed value to the response value returned by the API as shown in the following example.

```
componentDidMount() {
    const url = `${process.env.REACT_APP_API_URL}/user1`;
    RESTService.get(url, (success, response) => {
      if (success) {
        this.setState({user: response});
      } else {
        this.setState({apiCallFailed: response})
      }
    });
  }
```

When the response is returned it updates the state, and triggers a rerender of the application. You can validate that the state was updated by printing the value in the console from the render method. An example response is as follows:

```
 render() {
    console.log(`state -> ${this.state.apiCallFailed}`);
    return (
      ...
    )
  };
```

The render method should print the following error in the console: `state -> Error: cannot GET http://localhost:3080/user1 (404)`

Throwing an error

Now that you have control of the failure, throw an error with an appropriate value for the ErrorBoundary component to catch. As indicated, the API call is asynchronous, so you cannot throw the error from the componentDidMount. The throw could be placed in the render function which will execute when the state updates, but this pollutes the rendering method with code not dedicated to rendering. Instead, use the componentDidUpdate lifecycle method. This method is called when the state is updated, which happens when the callback updates the 'apiCallFailed' value.

The error object thrown can be anything that you choose so that the error as useful as possible to the citizen. In this instance, throw the string object that is returned by the response because it describes the issue.

Using a loading mask

Response times vary when using REST APIs over a network. In a many cases, the time it takes to receive the response is longer than the time it takes for React to render for the first time. This delay leads to a poor user experience when the page draws the components, but the data is missing.

Before your begin

To avoid poor user experience, use a loading mask that indicates to the user that the application is working on rendering their page.

This scenario uses the *AppSpinner* component from the *universal-access-ui package* to include a loading mask to the **My Details** page to demonstrate how your components can handle slow response times.

API response delay

During development, you must often replicate real world response times for APIs. You can configure the *RestService* to set a delay using the `env.development` file in your environment. By default this value is already set to 2.5 seconds. You should notice this delay when navigating the application in development mode, where you see spinners while components wait for the data to be returned from the mock server by way of the *RestService* module. You can increase or decrease this value to meet your application's needs.

The AppSpinner component

The *universal-access-ui* package includes the *AppSpinner* component, which you can reuse in your project. The *AppSpinner* component wraps the Spinner component from the *govhhs-wds-react* package and includes a label for accessibility purposes. You can also create your own loading mask in the same manner. You can view the source code for AppSpinner in the *universal-access-ui* package.

Waiting for the API

The AppSpinner is displayed while the application waits for the API to respond, so you need a mechanism to notify you when the data is, and is not loaded. Use the state to indicate when data is loaded and when it is not. Take the following steps:

1. Open the `PersonComponent.js` file.
2. In the constructor add an attribute called 'loading' to the state, with a value of true.

```
...
 constructor(props) {
   super(props);
   this.state = {
     user: {
       firstName: "",
       surname: "",
       dob: "",
       gender: "",
       address: {
         addr1: "",
         addr2: "",
         addr3: "",
         addr4: ""
       }
     },
     loading: true,
   };
 }
 ...
```

Display the loading mask

Now you have a value that indicates whether the data is loading. Take the following steps to display the loading mask based on this value:

1. Import the AppSpinner loading mask from *universal-access-ui*:

```
import {AppSpinner} from '@spm/universal-access-ui';
```

2. In the render function, add a check that renders the AppSpinner if the loading value is true:

```
render() {
    if (this.state.loading){
      return <AppSpinner/>
    }
    return (
      <Grid className="wds-u-p--medium">
        <Column width="1/2">
```

```
        ...
    )
}
```

When you save and reload the application, you should see the spinner in the main section area. However, the spinner continues to display after the data is returned.

Remove the loading mask

When the data is returned from the API, remove the mask by updating the state to indicate that loading is finished.

Take the following steps:

1. In the *componentDidMount* function, update the state to set the loading value to false when a successful response is returned.

```
componentDidMount() {
    const url = `${process.env.REACT_APP_API_URL}/user`;
    RESTService.get(url, (success, response) => {
      this.setState({loading: false})
      if (success) {
        this.setState({user: response});
      } else {
        this.setState({apiCallFailed: response})
      }
    });
  }
```

2. Save and reload the application. Now, when the API response is received, the loading mask is removed and the user's data is displayed.

Providing the application in another language

7.0.3.0

IBM Cúram Universal Access is globalized, that is it can be translated into different languages. Universal Access also supports regionalization of currencies, calendar and date formats as defined by IBM Cúram Social Program Management on which the application depends, for more information, see *Developing for Regional Support*.

Related information

Developing for Regional Support

Selecting a language

7.0.3.0

Citizens can select a preferred language from the **language** drop-down in the footer of the application. When citizens select a preferred language, the application is displayed in that language. The application retains the preferred language setting based on a cached value in the browser.

Note: A citizen's language preference is not saved if the browser is configured to block access to its local storage, the application reverts to the default language (English) when the page is reloaded.

Adding or removing languages

7.0.3.0

Add languages to, or remove languages from the application.

About this task

The application includes a number of languages in the user interface. You can customize the application by adding or removing languages.

Procedure

1. Configure the list of languages that are supported by the application by passing an *application configuration* object to the bootstrap function in the custom applications `universal-access-sample-app/src/index.js` file:

```
// Load your custom app configuration from a json file
const appConfig = require('./myAppConfiguration.json');

// Initialize the application by passing app configuration.
bootstrap(appConfig);
```

   Note: If you define a custom *supportedLanguages* property, you are taking control of the full list of supported languages.

   An example of `./myAppConfiguration.json` is as follows:

```
{
  supportedLanguages : ['en', 'fr']
}
```

2. If you add a language, you must add the text to display for that language. For example, if you add **ja** you must add a message `'ja':'Japanese'` for Japanese to appear in the associated *LanguageDropdown*. For more information, see *Translating message text*.
3. Similarly, you can remove a language by removing it from the list of *supportedLanguages* in your configuration file.

Translating your application

7.0.3.0

Use *react-intl* and *babel-plugin-react-intl* to extract text from your application. You can then translate the text into another language and include that translation in the application.

Extracting translatable content

7.0.3.0

During development, IBM used *react-intl* (https://github.com/yahoo/react-intl) and *babel-plugin-react-intl* (https://github.com/yahoo/babel-plugin-react-intl) to globalize IBM Cúram Universal Access.

About this task

Follow the same method as used by IBM during development to add languages to your application.

Note: *react-intl* provides react components and an API to format dates, numbers, and strings, including pluralization and handling translations. *babel-plugin-react-intl* extracts string messages from React components that use *react-intl*.

Procedure

1. Use the *react-intl defineMessages* API to define message string in the application.
2. Use *babel-plugin-react-intl* to extract messages from the application to a JSON format file, for example `messages_en.json`.
3. Translate the English resource file `messages_en.json` into one or more target language files, for example `messages_ja.json` (Japanese) or `messages_de.json` (German).

What to do next

For more information, see *Including translated content in your application*.

Including translated content in your application

7.0.3.0

IBM Cúram Universal Access exposes a *LanguageProvider* component, use this component to seed your application with messages for all the languages you want your application to support.

Procedure

1. Construct a complete set of messages for your app, use the *I18nUtils.getCombinedTranslationMessages* utility to combine your translated messages with the messages from Universal Access. The following code sample shows how to construct the message set:

```
// Provide the app with your translated messages.
const myAppMessages = getMyAppMessages();

// Combine your custom messages with the ones from the product.
// The function will overwrite product messages with your app messages where
// id's match. Which facilitates customization.
const allTranslationMessages = I18nUtils.getCombinedTranslationMessages(myAppMessages);

// Call render with the complete set of messages.
render(allTranslationMessages);


/** Load my messages for each language */
function getMyAppMessages() {
  const messages = [];
  appStore.getState().get('appConfig').
    supportedLanguages.forEach((language) => {
      messages[language] = getMessagesForLanguage(language);
  });
  return messages;
}

/** Load the messages from the json file */
function getMessagesForLanguage(language) {
  let translatedMessages = {};
  try {
    // eslint-disable-next-line
    translatedMessages = require(`./locale/messages_${language}.json`);
  } catch (e) {
    if (!e.message.includes('Cannot find module')) {
      throw e;
    }
    console.warn(
      `No translation files for the configured locale ${language} found @ ./locale/messages_$
{language}.json`,
    );
  }
  return translatedMessages;
}
```

2. Pass the complete set of messages from step 1 into the application by using the *LanguageProvider* component. The following code example shows how to inject the messages:

```
// Render the app, passing messages and the Redux store.
const render = (allTranslationMessages) => {
  ReactDOM.render(
    <Provider store={appStore}>
      <LanguageProvider messages={ allTranslationMessages }>
        <App />
      </LanguageProvider>
    </Provider>,
    document.getElementById('root'),
  );
};
```

Note: If your application does not find messages for the currently selected language at run time, *react-intl* defaults to the text that was used when the message was defined in the source code.

Results

The translated languages are available in the *LanguageDropdown* feature of the application. Users can now change the user interface to display messages in these languages.

Regionalizing your application

7.0.3.0

User interface elements, such as date formats and currency symbols are defined in IBM Cúram Social Program Management, for more information, see *Developing for Regional Support*.

The universal-access module and its components respect the regional settings as defined by the IBM Cúram Social Program Management to ensure your application is synchronized with the configuration of the IBM Cúram Social Program Management instance on which it depends.

Related information

Developing for Regional Support

Advanced: Creating a new feature

The reference application available on install of Universal Access product satisfies a number of general business scenarios such as creating an account, logging in, applying for benefits etc... They are provided both as working software and as examples of how to construct the product. Where small customisations are desired it is possible to reuse the elements of the universal access packages to construct your own version of the feature.

About this task

Features

The `universal-access-ui` package is structured by feature. Each feature is typically mapped to a single route. For example, when the `/profile` route is loaded, the Profile feature is displayed. The feature folder is a collection of files that work together to present that feature. Below is an example from the Profile feature.

```
/universal-access-ui
--/src
----/Feature
------/Profile
--------/components
----------/ContactInformationComponent.js
----------/PersonalInformationComponent.js
----------/ProfileComponent.js
----------/ProfileComponentMessages.js
--------/index.js
--------/ProfileContainer.js
```

The feature uses a commonly used pattern to move the data retrieval and management into a 'container component', and the rendering logic into stateless 'presentation components'. This pattern is widely documented and used extensively when working with React and Redux. The pattern is not covered in detail here, just to note that this is how features are structured.

Modifying how a feature is presented

Features can be cloned and modified. You can copy the entire code base for the feature in to your custom project and replace the route that served that feature with your version. You can then modify the code base to include your customizations.

Procedure

1. Find the feature that you want to replace in the `universal-access-ui` package.
   a) Inspect the URL end point that you want to change.
   For example, `/myapp/universal/#/faqs` uses the `faqs` path.
   b) Open the `/node_modules/@spm/universal-access-ui/src/router/Path.js` file to find the variable referencing the route.

For example, `Paths.FAQS`.

```
const Paths = {
  HOME: '/',

  ...

  FAQS: '/faqs',

  ...
  SIGNUP: '/signup',
};
export default Paths;
```

c) Open the file `/node_modules/@spm/universal-access-ui/src/router/Path.js` to find the variable referencing the route.
For example, `Paths.FAQS`.

```
...
import FAQ from '../features/FAQ';
...
export default () => (
  <Switch>
    ...
    <Route component={FAQ} exact path={PATHS.FAQS} />
    ...
  </Switch>
);
```

2. Copy the feature folder into your custom app.

   Using the location of the feature folder from step 1, copy the entire folder to your custom app. In the example, the contents of `/node_modules/@spm/universal-access-ui/src/features/Profile` would be copied to `/src/features/Profile`.

3. Replace the route with your custom version.

   a) In your project, open the `src/routes.js` file.

   b) Add a new route at any point before the `UARoutes` entry to ensure that your path supersedes the same path in `UARoutes`.

```
import React from 'react';
import { Switch, Route } from 'react-router-dom';
import { Routes as UARoutes } from '@spm/universal-access-ui';
import FAQ from './features/FAQ';

export default (
  <Switch>
    <Route component={FAQ} exact path='/faqs' />
    <UARoutes />
  </Switch>
);
```

4. At this point, you can verify whether your custom version of the feature is being used. Make an obvious change to the feature and reload the application to verify that the change is being picked up and displayed.
5. Customize the feature. Now that you have a exact copy of the feature you can make changes to the code to introduce your customizations.

   Note: You now have full ownership of the feature. On upgrade of the `universal-access-ui` package you will not receive any changes that have been applied to the product version of the feature. Instead, you must manually apply any upgrade features that you wish to retain.

   Note: Most features in the `universal-access-ui` package depend on the modules in the universal-access package to work with the data required by the feature. On upgrade, you must validate that your feature has not been impacted by any changes to modules your feature depends on. See *Working with universal-access modules*.

Configuring IBM Cúram Universal Access

System administrators use the following configuration options to configure and maintain IBM Cúram Universal Access.

Prerequisites

7.0.3.0

You must enable cookies and JavaScript in the browsers to access the application by configuring the appropriate browser preferences.

The following table lists the browser preferences that you must configure for the application to work, and shows the errors that are displayed if the prerequisites are not met.

Table 2: Information messages for browser preferences

Browser preference	Information message
When cookies are disabled	Cookies are currently disabled and are required for the application to work. Please enable cookies and retry.
When JavaScript is disabled	JavaScript is currently disabled and is required for the application to work. Please enable JavaScript and retry.
When cookies and JavaScript are disabled	Cookies and JavaScript are currently disabled and are required for the application to work. Please enable and try again.

Configuring service areas and PDF forms

7.0.3.0

You can define a service area by configuring the counties or ZIP codes that are associated with the service area. You can also specify a PDF form that a citizen can use to apply for programs.

Configuring service areas

Service areas are defined in the **Service Areas** section of the administration application. When defining a service area, you must specify a service area name. You can the associate counties and zip codes with the service area, these represent the areas covered by the service area. Service areas can be associated with a local office which represents the office that services the service areas associated with it. Local offices identify where citizens can apply in person for a particular program or where they can send a particular application. For more information on associating service areas with local offices where a citizen can apply in person for a program, see *Defining local offices for a program*.

Configuring PDF forms

PDF forms are defined in the **PDF Forms** section of the administration application. When defining a PDF form, you must specify a name and language. The agency can add a version of the form for each language that is configured. The forms are accessible from the Universal Access **Print and Mail Form** page.

A local office can be associated with a PDF form. Associating a local office with a PDF form allows an administrator to define the local office and associated service areas where a citizen should send their completed application to.

Enabling citizens to search for a local office

A search page allows citizens to search for their local office. Citizens can either search by county or by zip code. The system property *curam.citizenworkspace.page.location.search.type* determines how the search works. If you set *curam.citizenworkspace.page.location.search.type* to **Zip**, citizens can search for a local

office using a zip code. If you set this property to **County**, citizens can select from a list of counties to get a list of local offices.

Related concepts

Defining local offices for a program

A citizen may be able to apply for a program in person at a local office. A local office must be first defined in the *LocalOffice* code table in system administration.

Configuring programs

7.0.3.0

You can define different types of programs. When you define a program, you can configure display and system processing information, local offices, mappings to PDFs, and evidence types.

Agencies can define different types of programs. When programs have been defined, they can be associated with screenings and applications that allows citizens to screen and apply for these programs. The main aspects to configuring a program are as follows:

- Configuring programs and associated display and system processing information.
- Configuring local offices where an application for a program can be mailed to.
- Configuring mappings that allow information gathered during application intake to be mapped to a PDF form.
- Configuring evidence types that allows for expedited authorization of programs that may need to be processed before other programs within a multi program application.

Configuring a Program

7.0.3.0

Programs are configured on the **New Program** page. Details and specifications of the program are required to be defined when the program is created.

Defining a name and reference

7.0.3.0

The name that is defined is displayed in the administration application. The reference is used to reference the program in code.

A name and reference must be defined when creating a new program. The name that is defined is displayed both to the citizen and in the internal application. The reference is used to reference the program in code.

Defining an intake processing system

7.0.3.0

Specify an intake processing system for each program. If a case processing system is not specified, the system is not able to respond to the submission of an application for that program.

Two options are available: **Cúram** or select from the list of preconfigured remote systems. If intake is managed by IBM Cúram Social Program Management, select **Cúram**. If intake is managed by an external system - the program application is sent to the remote system by using the `ProcessApplicationService` web service, select a remote system.

If **Cúram** is specified as the intake system, an application case type must be selected. An application case of the specified type is created in response to a submission of an application for the program. An indicator is provided which dictates whether a **Reopen** action is enabled on the programs list on an application case for denied and withdrawn programs of a particular type. A workflow can be specified that is initiated when the program is reopened. For more information on configuring application cases, see *Cúram Intake overview*.

When an application case type is selected, the program can be added manually to that type of application case by a worker in the internal application as part of intake processing. A configuration setting specifies whether the program is a coverage type. Coverage types are automatically evaluated by program group rules in the context of healthcare reform applications, such as insurance affordability. Coverage types cannot be applied for directly by a citizen or manually added to an application case by a worker and

authorized. If the program is a coverage type, select **Yes**. The program is filtered out of the list of programs available to be added to online and internal applications in administration and the list of programs available to be manually added to an application case by a worker. If the program is not a coverage type, select **No**. The program will be available to be manually added to online and internal applications in administration and to an application case by a worker.

A remote system must be configured in the administration application before it can be selected as the case processing system. For more information about remote systems, see *Configuring Remote Systems.*

Related concepts

Configuring remote systems

Applications and life events data can be sent through web services for processing by a remote system. To enable remote processing, specify a remote system and the required web services. Remote systems can be configured allowing applications and life event data to be sent to them for processing via associated web services.

Related information

Cúram Intake overview

Defining case processing details

7.0.3.0

A case processing system must be specified for each program.

Two options are available, **Cúram** or select from remote systems. If the program eligibility is determined and managed by using a Cúram-based system, select **Cúram**. If eligibility is determined and managed by an external system, select a remote system.

If **Cúram** is selected as the case processing system, more options are available to allow for program level authorization to be configured. Program level authorization means that if an application case contains multiple programs, each program can be authorized individually, and a separate case is used to manage the citizens on an ongoing basis.

Defining the integrated case strategy

7.0.3.0

Define the integrated case strategy so that the system can identify whether a new or existing integrated case needs to be used when program authorization is successful. The integrated case is used to host any product deliveries created as a result of the authorization.

The integrated case strategy identifies whether a new or existing integrated case should be used when program authorization is successful. The integrated case is used to host any product deliveries created as a result of the authorization. If a new integrated case is created, all of the application case clients are added as case participants to the integrated case. If an existing integrated case is used, any additional clients on the application case are added as case participants to the integrated case. Any evidence captured on the application case that is also required on the integrated case is copied to the integrated case upon successful authorization. The configuration options for the integrated case strategy are as follows:

New
A new integrated case of the specified type is always created when authorization of the program is successful.

Existing (Exact Client Match)
If an integrated case of the specified type exists with the same citizens as those cases present on the application case, the existing case is used automatically. If multiple integrated cases that meet these criteria exist, the worker is presented with a list of the cases and must select one to proceed with the authorization. If no existing cases match the criteria, a new integrated case is created.

Existing (Exact Client Match) or New
If one or more integrated cases of the specified type exist with the same citizens as those cases present on the application case, the user is presented with the option to select an existing case to use as the ongoing case, or to create a new integrated case. If no existing cases match the criteria, a new integrated case is created.

Existing (Any Client Match) or New
If one or more integrated cases of the specified type exist, where any of the clients of the application case are case participants, the user is presented with the option to select one of the existing cases to use as the ongoing case, or to create a new integrated case. If no existing cases match the criteria, a new integrated case is created.

Specifying the Integrated Case Type
The administrator must specify the type of integrated case to be created/used upon successful program authorization as defined by the Integrated Case strategy listed previously.

Specifying a client selection strategy

7.0.3.0

Specify a client selection strategy to define how clients are added from the application case to the product delivery.

The client selection strategy defines how clients are added from the application case to the product delivery created as a result of authorization of a program. If a product delivery type is specified, a client selection strategy must be selected. The configuration options are as follows:

All Clients
All of the application clients are added to the product delivery case. The application case primary client is set as the product delivery primary client. All other clients are added to the product delivery as members of the case members group.

Rules
A rule set determines the clients to be added to the product delivery if a product delivery is configured. At least one client must be determined by the rules for authorization to proceed.

User Selection
The user selects the clients who should be added to the product delivery. The user must select both the primary client and any other clients to be added to the case member group on the product delivery.

Specifying a Client Selection Ruleset
A Client Selection Ruleset must be selected when the Client Selection Strategy is **Rules**.

Specifying a product delivery type

7.0.3.0

Specify a product delivery type.

The **Product Delivery Type** specifies the product delivery that is used to make a payment to citizens in respect of a program. The drop-down displays all active products configured on the system.

Note: This field applies to both program and application authorization processing. That is, program and application authorization can result in the creation of the product delivery type specified.

Submitting a product delivery automatically

The **Submit Product Delivery** indicator specifies if the product delivery created as a result of program authorization should be submitted automatically for approval. If selected, the product delivery created as a result of authorization of this program is submitted automatically for a supervisor for approval.

Note: This field applies to both program and application authorization processing. That is, program and application authorization can result in the automatic submission of a product delivery.

Configuring timers

7.0.3.0

Agencies can impose time limits within which an application for a program must be processed. You can configure application timers for each of these programs.

For example, a government agency might want to specify that food assistance applications are authorized within 30 business days of the date of application.

The following configuration options are available, including the duration of the timer, whether the timer is based on business or calendar days, a warning period, and timer extension and approval.

Duration
The length of the timer in days. This value, along with the fields **Start Date** and **Use Business Days** (and the configured business hours for the organization) are used to calculate the expiry date for the timer. This value is used as a number of business days if **Use Business Days** is set. If **Use Business Days** is not set, this value is used as calendar days.

Start Date
Specifies whether the timer needs to start on the application date or the program addition date. The options available are **Application Date** and **Program Addition Date**.

Note: In most cases, these dates are the same. That is, the programs are added at the same time as the application is made. However, when a program is added later to the application, after initial submission, the dates are not the same.

Warning Days
Allows for the specification of a number of warning days. The warning days are used to warn the user that the timer deadline is approaching. If configured, the Warning Reached workflow also is enacted when the warning date is reached and the timer is still running (for example, the program is not completed).

End Date Extension Allowed
An indicator to dictate whether citizens can extend the timer by a number of days.

Extension Approval Required
An indicator to dictate whether a timer extension requires approval from a supervisor. If approval is required for the extension, the case supervisor must review and either approve or reject the extension. After the extension is approved, or if approval is not required, the timer expiry date is updated to reflect the extension.

Use Business Days
An indicator to dictate that the timer should not decrement on non-working days. If this indicator is set, the system uses the **Working Pattern Hours** for the organization to determine the non-working days when it is calculating the expiry date for the timer.

Resume Timer
An indicator to dictate whether the program timer needs to be resumed when the program is reopened.

Resume From
If a timer is resumed, the **Resume From** field dictates the dates from which a program can be resumed. The values include the date that the program was completed, denied, or withdrawn, and the date that the program was reopened.

Timer Start
Allows for the specification of a workflow that is enacted when the timer starts.

Warning Reached
Allows for the specification of a workflow that is enacted when the warning period is reached.

Deadline Not Achieved
Allows for the specification of a workflow that is enacted if the timer deadline is not achieved; that is, the program is not being withdrawn, denied, or approved by the timer expiry date.

Configuring multiple applications

7.0.3.0

Configure multiple applications so that citizens can apply for a program while they have a previous application pending.

The **Multiple Applications** indicator dictates if citizens can apply for a program while they have a previous application pending. If set to true, citizens can have multiple pending applications for the given program. That is, citizens can submit an application for this program while they already have a pending application in the system. If it is set to false, this program is not offered if logged in citizens have pending applications for this program.

This configuration is not applicable to Health Care Reform Applications.

Defining a PDF form

7.0.3.0

Defining a PDF form for a program enables a citizen to print an application for the specified program and either post it to the agency or bring it, in-person, to a local office.

When a PDF Form is specified for a program, the PDF form will be displayed on the **Print Out and Mail** section of the **Your Next Step** page displayed when a citizen has completed a screening. PDF Forms must be defined before they can be associated with a program. When they are defined, they will be displayed on the **Print and Mail Application Form** page.

Defining a URL

7.0.3.0

If a URL is defined, a **More Info** link is displayed beside the program name allowing a citizen to find out more information about the selected program.

Defining description and summary information

7.0.3.0

When a program is displayed on the **Select Programs** page, a description can be displayed which gives a description of the program. The **Online Program Description** field defines this description.

A description summary of the program can also be defined using the **Online Program Summary** field. The field is a high-level description of the program displayed on the **Your Next Steps** page displayed when citizens complete a screening.

Defining local office application details

7.0.3.0

Citizens can apply for programs at a local office. If this is the case, the **Citizen Can Apply At Local Office** indicator indicates that local office information is displayed for a program.

Additional information can also be defined, for example, citizens might need to bring proof of identity if they want to apply at the local office. An administrator can define this information in the **Local Office Application Information** field.

Defining local offices for a program

7.0.3.0

A citizen may be able to apply for a program in person at a local office. A local office must be first defined in the *LocalOffice* code table in system administration.

Associating a local office with a program allows an administrator to define the local offices and their associated service areas where a particular program can be applied for in person. This information is displayed on the **Your Next Step** page that is displayed to a citizen when they have performed a screening. Service areas must be defined before they can be associated with a local office.

Defining PDF mappings for a program

7.0.3.0

The information entered during an online application can be mapped to a PDF form which can be printed by the citizen.

In order for the application data to be mapped to the PDF Form for all programs a citizen is applying for, a mapping configuration of type PDF Form Creation must exist for each of the programs. The PDF Form is the form specified for the Online Application the program is associated with.

Defining program evidence types

7.0.3.0

Evidence types can be associated with a program.

Evidence types can support applications for multiple programs where a particular program needs to be authorized more quickly than other programs for which citizens might have applied. Using this type of configuration, only the evidence required for the program to be authorized is used and copied to the

ongoing cases. This allows benefits for the authorized program to be delivered to citizens, while the caseworker continues to gather the evidence required for the other programs applied for.

Configuring applications

7.0.3.0

The administration system allows an agency to define different types of applications. Once defined, citizens can submit an application for programs to the agency. For each application, you can configure the available programs and an application script and data schema. Configure the remaining applications details, including application withdraw reasons.

There are five aspects to configuring an application:

- Configuring information about an application and associated display information
- Configuring the script and schema used to collect and store the information specified during the application process.
- Configuring the programs for which an application can be used to apply.
- Configuring reasons that can be selected when a citizen withdraws an application.
- Configuring additional application system properties.

Related concepts

Saving an application

By default, applications are automatically saved for citizens who are logged in. Citizens can also manually save applications, including in-progress applications.

Configuring an application

7.0.3.0

Applications are configured on the **New Application** page using the following application configurations.

Name

The name defined is the name of the application displayed in the online portal.

Program selection

Program Selection indicates whether citizens can select specific programs to apply for or whether they are brought directly into an application script. That is, citizens can apply for all programs associated with the application.

URL

If a URL is defined, a **More Info** link is displayed beside the name of the application so that citizens can find out more information about the selected application.

Summary information

Summary information allows an administrator to define a high-level description of the application to be displayed.

Description information

Allows an administrator to define a description of the application to be displayed.

Configuring an application script

7.0.3.0

Define an IEG for the application to collect the answers to the application questions.

Specify a script name in the **Question Script** field. A data store schema must be specified to store the data entered in the script. A schema name must be specified in the **Schema** field. On saving the application, an empty template for both the script and schema is created by the system based on the question script and schema specified. You can update these templates from the **Application** tab by selecting hyperlinks provided on the page. Clicking the **Question Script** link starts the IEG editor so you can edit the question script. Click the **Schema** link to start the Datastore Editor and edit the schema.

Configuring a submission script

7.0.3.0

A submission script can be defined for an application to submit an application to the agency. This is used to define additional information which does not form part of the application script to be captured, for example, a TANF typically requires information regarding the citizen's ability to attend an interview.

An IEG submission script can be specified in the **Submission Script** field. On saving the application, an empty template for the submission script is created by the system based on the Submission Script specified. You can update this from the **Application** tab by selecting the hyperlink provided on the page. Clicking on the link starts the IEG editor which lets you edit the question script.

Defining a PDF form

7.0.3.0

Define a PDF form for an application identifies the agency-designed form that is displayed when citizens complete and online application.

The data that is collected during the online application is copied by the system into this PDF, which allows citizens to print it. The PDF form can be selected from the **PDF Forms** drop down menu. If a PDF form is not specified for an application, a default generic PDF form can be used. This default template is accessible in the **XSL Templates** section of the system administration application.

The data passed to the XSL template reads directly from the data store. Instead of displaying the datastore labels in the PDF, define a property file to specify user-friendly names for entities and attributes and to hide entities and attributes that you do not want to display in the PDF. Upload the property file to **Application Resources** in the **Intelligent Evidence Gathering** section of the administration application.

Name the property file using the following convention: `<application schema name>PDFProps`. The contents of the property file is as follows:

Name an entity
`<Entity Name=<Name To Be Displayed in the PDF>`, for example, *Application=Intake Application*

Hide an entity
`<Entity Name.hidden=true`, for example, *ScreeningType.hidden=true*

Hide an attribute
`<Entity Name.Attribute Name.hidden=true`, for example, *Application.user Name.hidden=true*

Specify a label for an attribute
`<Entity Name.Attribute Name=PDF Label`, for example, *Submission.dig FirstName=First Name*

Configuring client registration

7.0.3.0

Use the **Client Registration** field to decide whether clients are registered as prospects or persons.

To determine whether to register the client as a prospect or a person, the system checks the client registration configuration in the following two scenarios:

- If **Person Search and Match** is configured, and no match can be found for the client.
- If **Person Search and Match** is not configured, that is, the clients on an application are always registered without the system automatically searching and matching them.

If the **Client Registration** field is not set, the system checks the system property **Register as Prospect Person** to identify whether a client is registered as a prospect or a person.

Configuring submission confirmation page details

7.0.3.0

Additional information can be configured on the **Submission Confirmation** page which is displayed when citizens submit an online application.

The **Title** and **Text** fields can be used to define a title and text to be displayed on the confirmation page.

Associating programs with applications

7.0.3.0

So that citizens can apply for particular programs, you must associate programs with the application.

Any program described in **Configuring Programs** can be associated with an application. When associating programs with an application, you can set the display order of the selected program relative to other programs associated with the application.

Defining mappings for an application

7.0.3.0

Applications can be processed by IBM Cúram Social Program Management or a remote system.

If the application is processed by IBM Cúram Social Program Management the information entered in an application is mapped to the evidence tables associated with the application case defined for the programs associated with the application. The mappings are configured for an application by creating a mapping using the Data Mapping Editor. A mapping configuration must be specified in order for the appropriate evidence entities to be created and populated in response to an online application submission.

For more information about the Data Mapping Editor, see the *Data Mapping Editor Guide*.

Configuring withdrawal reasons

7.0.3.0

Citizens can withdraw the application for all or any one of the programs for which they applied.

When withdrawing an application, a withdrawal reason must be specified. Withdrawal reasons can be defined for a particular application in the **Intake Application** section of the administration application. Before associating a withdrawal reason with an application, withdrawal reasons must be defined in the **WithdrawalRequestReason** code table.

Mandating authentication before applying

7.0.3.0

The agency can configure the system to specify whether, before starting an application, citizens must create an account or log in to make an application.

The system property *curam.citizenworkspace.authenticated.intake* is indicates if authentication is switched on. If this property is switched on, citizens must create an account or log in before starting an application. If *curam.citizenworkspace.authenticated.intake* is switched off, citizens is taken directly to the application selection page.

Optional authenticated application

7.0.3.0

The agency can configure the system to specify whether, before applying, citizens can choose to be authenticated.

The system property *curam.citizenworkspace.intake.allow.login* indicates if authentication is switched on or off. If this property is switched on, citizens will be given the option to log in before starting an application. If *curam.citizenworkspace.intake.allow.login* is switched off, citizens are taken directly to the application selection page.

Displaying a confirmation page on quit

7.0.3.0

The agency might want to display a confirmation page to citizens when they quit the application process.

The system property *curam.citizenworkspace.display.confirm.quit.intake* indicates if a confirmation page is displayed. If this property is switched on, a confirmation page is displayed when quit is selected while making an application. If *curam.citizenworkspace.display.confirm.quit.intake* is switched off, a confirmation page is not displayed when citizens quit an application. This property is only used when the property *curam.citizenworkspace.intake.allow.login* is set to **NO**.

Mandating authentication before submission

7.0.3.0

The agency might want to mandate that citizens log in before submitting an application.

The system property *curam.citizenworkspace.intake.submit.intake.mandatory.login* indicates that citizens must log in before submitting an application. If *curam.citizenworkspace.intake.submit.intake.mandatory.login* is switched on, citizens must create an account or login before they can submit an application. If *curam.citizenworkspace.intake.submit.intake.mandatory.login* is switched off, citizens can submit an application without logging in.

Enabling applications link

7.0.3.0

Use the system property *curam.citizenworkspace.intake.enabled* to indicate whether citizens can start the application process from the **Home** page.

If *curam.citizenworkspace.intake.enabled* is switched on, the **Applications (Apply For Benefits)** link is displayed on the **Home** page. If *curam.citizenworkspace.intake.enabled* is switched off the applications link is not displayed.

Prepopulating the application script

7.0.3.0

When authenticated citizens apply from benefits from their accounts, information already known about the citizen performing the application can be prepopulated.

The system property *curam.citizenaccount.prepopulate.intake* indicates whether the IEG script is prepopulated. The default value of this property is true which means that the script is prepopulated.

The application auto-save property

7.0.3.0

The auto-save Intake property dictates if applications are auto-saved in the citizen account.

By default, this property is set to true. All applications irrespective of type are automatically saved. Each application is auto-saved when citizens click **Next** as they progress through the IEG script. If this property is set to false, applications are not automatically saved in the citizen account.

Configuring online categories

7.0.3.0

Online categories group different types of applications or screenings together to make it easier for citizens to find the ones that they need. You must define online categories for screenings and applications to be displayed. After you define online categories, you must associate each screening and application to a category.

Defining online categories

When defining an online category a name and URL must be defined. If a URL is defined a **More Info** link is displayed beside the name of the online category allowing a citizen to find out more information about the selected category. An order can be assigned to a category which dictates the display order of the selected category relative to other categories.

Associating screenings and applications

Screenings and applications must be associated with an online category in order for them to be displayed in the application. When associating a screening with an online category, an order can be applied which dictates the display order of the screening relative to other screenings within the same category. When associating an application with an online category an order can be applied which dictates the display order of the application relative to other applications within the same category.

Configuring the citizen account

7.0.3.0

Although customization is required to modify some citizen account information, you can configure information on the citizen account and the **Contact Information** tab.

Messages can originate as a result of transactions in IBM Cúram Social Program Management or a remote system. Most of the configuration options apply to all messages but there are a some configuration options that do not apply to messages originating from a remote system.

Configuring the citizen account

7.0.3.0

Configure the citizen account.

Many aspects of the citizen account are configurable:

- The text displayed in the participant messages in the **Messages** panel
- The system messages displayed in the **Messages** panel
- The display order of the messages in the **Messages** panel

Configuring messages

7.0.3.0

The **Messages** panel of the organization **Home** page displays messages to logged-in citizens. For example, a message that informs citizens when their next benefit payment is due or the amount of the last payment.

Messages can be displayed which relate to meetings, activities, and application acknowledgments. Messages can be displayed as a result of transactions in IBM Cúram Social Program Management or they can originate from remote systems by way of a web service.

The links that follow outline the aspects of the **Messages** section, which are configurable.

Account messages

7.0.3.0

Adding a message or changing a dynamic element of an account message requires customization. The text that is defined for existing messages that are provided in the initial application configuration can be updated by using a set of properties for each type of message.

Properties are as follows:

- `CitizenMessageMyPayments` - the messages that relate to payments.
- `CitizenMessageApplicationAcknowledgement` - contains the messages that relate to application acknowledgments.
- `CitizenMessageVerificationMessages` - the messages that relate to verification messages.
- `CitizenMessageMeetingMessages` - the messages that relate to meetings.
- `CitizenMessagesReferral.properties` - the messages that relate to referrals.
- `CitizenMessagesServiceDelivery` - the messages that relate to service deliveries.
- `CitizenAppealRequestMessage` - the messages that relate to appeal requests.

Property files are stored in the **Application Resources** section of the administration application. To update the message, each file needs to be downloaded, updated, and uploaded again. The icons that are displayed in the citizen account for each type of message can be configured in the **Account Messages** section of the **administration** application.

Adding a message that originates from a remote system requires that a code table entry to be added to the `ParticipantMessageType` code table and an associated entry in the **Account Messages** listing in the administration application. Messages then can be sent by way of the `ExternalCitizenMessageWS` web service.

Creating application acknowledgments

7.0.3.0

Create messages to acknowledge an application.

Table 3: Application acknowledgment	
Message Area	**Description**
Title	<Icon> TANF Application Acknowledgment
Message	`We have received your TANF Application form. The status of this application is pending. We will contact you when the application has been processed.`
Effective Date	Current® date
Duration	An administrator can use a configuration setting to define the number of days (from the effective date) that the message is displayed.
Notes	None.

Creating meeting messages

7.0.3.0

Create messages for a meeting invitation, a meeting cancellation, and a meeting update. An administrator can use a configuration setting to set the number of days (from the effective date) that the meeting messages are displayed.

Table 4: Meeting invite	
Message Area	**Description**
Title	<Icon> Meeting Invitation - Meeting with Case Worker
Message 1 (Not an all day meeting and the meeting start and end date are on the same day)	`You are invited to attend a meeting from 9.00AM until 5.00PM on 12/04/2010 in Meeting Room 1, Block C. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.`
Message 2 (All day meeting for one day only)	`You are invited to attend an all day meeting on 12/04/2010 in Meeting Room 1, Block C. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.`
Message 3 (All day meeting for multiple days)	`You are invited to attend an all day meeting each day from 12/04/2010 until 15/04/2010 in Meeting Room 1, Block C. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.`
Message 4 (Non-all day meeting for multiple days)	`You are invited to attend a meeting from 9.00AM until 5.00PM from 12/04/2010 to the 13/04/2010 in Meeting Room 1, Block C. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.`

Table 4: Meeting invite (continued)	
Message Area	**Description**
Notes	When the case worker is setting up a meeting, the location is an optional field. Therefore, if a meeting location is not specified, the preceding messages are displayed without a location. Also, the meeting organizer's contact details are optional. Therefore, if no contact details are found, the preceding message is displayed without the organizer's contact details.

Table 5: Meeting cancellation	
Message Area	**Description**
Title	<Icon> Cancellation - Meeting with Case Worker
Message 1 (Not an all day meeting and the meeting start and end date are on the same day)	The meeting that you were scheduled to attend from 2.00PM until 6.00 PM on 12/04/2010 is canceled. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information.
Message 2 (All day meeting for one day only)	The all day meeting that you were scheduled to attend on 12/04/2010 is canceled. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information.
Message 3 (All day meeting for multiple days)	The all day meeting that you were scheduled to attend from 12/04/2010 until 15/04/2010 is canceled. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information.
Effective Date	Current Date.
Notes	The meeting organizer's contact details link opens a page that shows the organizer's contact details.

Table 6: Meeting update	
Message Area	**Description**
Title	<Icon> Cancellation - Meeting with Case Worker

Table 6: Meeting update (continued)

Message Area	Description
Message 1 (Date and Time change of a non-all-day meeting)	The meeting that you were scheduled to attend from 2.00PM until 6.00 PM on 12/04/2010 is rescheduled to 3.00PM until 7.00 PM on 13/04/2010 in Meeting Room 1, Block C. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 2 (Location change of a non-all-day meeting)	The location of the meeting you are scheduled to attend from 2.00PM until 6.00 PM on 12/04/2010 is changed. This meeting is now scheduled for Meeting Room 1, Block D. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 3 (Date, time, and location change of non-all-day meeting)	The meeting that you were scheduled to attend from 2.00PM until 6.00 PM on 12/04/2010 is rescheduled to 3.00PM until 7.00 PM on 13/04/2010. It is rescheduled for Meeting Room 2, Block C. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 4 (Date change of all day meetings for multiple days)	The all day meeting that you are scheduled to attend from 12/04/2010 until 15/04/2010 is rescheduled. This meeting will now take place from 13/04/2010 until 16/04/2010. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 5 (Location change for all day meeting for multiple days)	The location of the all day meeting you are scheduled to attend from 12/04/2010 until 15/04/2010 is changed. This meeting is rescheduled for Meeting Room 1, Block D. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 6 (Date and location change for all-day meeting for multiple days)	The all day meeting that you are scheduled to attend from 12/04/2010 until 15/04/2010 is rescheduled. This meeting will now take place from 13/04/2010 until 16/04/2010 in Meeting Room 1, Block D. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.

Table 6: Meeting update (continued)

Message Area	Description
Message 7 (Date change for an all-day meeting)	The all day meeting that you are scheduled to attend on 12/04/2010 is rescheduled. This meeting will now take place on 13/04/2010. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 8 (Location change for an all-day meeting)	The location of the all day meeting you are scheduled to attend on 12/04/2010 is changed. This meeting is rescheduled for Meeting Room 1, Block D. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 9 (Date and location change for an all-day meeting)	The all day meeting that you are scheduled to attend on 12/04/2010 is rescheduled. This meeting is rescheduled for 13/04/2010 in Meeting Room 1, Block D. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 10 (Date and time change of a non-all-day meeting for multiple days)	The meeting that you are scheduled to attend from 2.00PM until 6.00 PM on 12/04/2010 until 15/04/2010 is rescheduled. This meeting is rescheduled for 2.00PM until 6.00 PM on 13/04/2010 until 16/04/2010. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 11 (Location change of a non-all-day meeting for multiple days)	The location of the meeting you are scheduled to attend from 2.00PM until 6.00 PM on 12/04/2010 until 15/04/2010 is changed. This meeting is rescheduled for Meeting Room 1, Block D. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.
Message 12 (Date, time, and, location change of non-all-day meeting for multiple days)	The meeting that you are scheduled to attend from 2.00PM until 6.00 PM on 12/04/2010 until 15/04/2010 is rescheduled. This meeting is rescheduled for 2.00PM until 6.00 PM on 13/04/2010 until 16/04/2010 in Meeting Room 1, Block D. Please contact Joe Bloggs at 014567832 or joe@SemAgency.com if you need more information or cannot attend.

Table 6: Meeting update (continued)	
Message Area	**Description**
Notes	When the case worker is setting up a meeting, the location is an optional field. Therefore, if a meeting location is not specified, the preceding messages are displayed without a location. Also, the meeting organizer's contact details are optional. Therefore, if no contact details are found, the preceding message is displayed without the organizer's contact details.

Creating payment messages

7.0.3.0

Create messages for an issued payment, a canceled payment, a due payment, a stopped payment, an unsuspended payment, an issued overpayment, and an issued underpayment. An administrator can use a configuration setting to set the number of days (from the effective date) that the payment messages are displayed.

Table 7: Payment issued	
Message Area	**Description**
Title	<Icon> Latest Payment
Message 1	`Your latest payment of $22.00 was due on 22/07/2009. Click here to view the payment details. Your next payment is due on 29/07/2009. Click My Payments to view your payment history.`
Message 2 (Payment previously canceled)	`Your latest payment of $22.00 was due on 22/07/2009. Click here to view the payment details. This payment was originally canceled on 23/07/2009. Click here to view details of the canceled payment. Your next payment is due on 29/07/2009. Click My Payments to view your payment history.`
Effective Date	Current Date.
Notes	A payment can be issued, then canceled, and then reissued. The **here** hyper link opens a page that shows payment details. The **My Payments** link opens the **My Payments** page in the Citizen Account. **Note:** If no more payments are due, the `Your next payment is due on 29/07/2009` part of the messages is not displayed.

Table 8: Payment canceled	
Message Area	**Description**
Title	<Icon> Payment Canceled

Table 8: Payment canceled (continued)	
Message Area	**Description**
Message	`Your payment of $22.00, due on 22/07/2009, has been canceled. Click here to view the details. Click Contact Information to contact your caseworker if you need more information. Your next payment is due on 29/07/2009. Click My Payments to view your payment history.`
Effective Date	Current Date.
Notes	If no more payments are due, the `Your next payment is due on 29/07/2009` part of the message is not displayed. The **Contact Information** link opens the **Contact Information** tab in the citizen account. The **My Payments** link opens the **My Payments** page in the Citizen Account.

Table 9: Payment due	
Message Area	**Description**
Title	<Icon> Next Payment Due
Message	`Your next Cash Assistance payment is due on 29/07/2011.`
Effective Date	Current Date.
Notes	This message is appropriate when it is the first payment that a citizen receives.

Table 10: Case suspended	
Message Area	**Description**
Title	<Icon> Payments Stopped
Message	`Your Cash Assistance payments have been stopped from 29/07/2009. Click Contact Information to contact your caseworker if you need more information.`
Effective Date	Current Date.
Notes	The **Contact Information** link opens the **Contact Information** tab in the Citizen Account.

Table 11: Case unsuspended	
Message Area	**Description**
Title	<Icon> Payments Unsuspended
Message	`Your Cash Assistance payment suspension has been lifted from 29/07/2009. Your next payment is due on 31/07/2009.`
Effective Date	Current Date.
Notes	None.

System messages

7.0.3.0

Agencies use system messages to send messages to citizens who have a Citizen Account. For example, if an agency wants to provide information and help line numbers to citizens who were affected by a natural disaster. System Messages can be configured in the administration application by using the **New System Message** page.

Use the **Title** and **Message** fields to define the title of the message and the message body that is displayed in the **My Messages** pane. Defined the message as a priority by using the **Priority** field, the message appears at the top of the messages listing.

Note: If multiple priority messages exist, the effective date of the message and the message type is used to dictate the message order. For more information, see *Ordering and Enabling/Disabling Messages*.

Use the **Effective Date and Time** to define an effective date for the message, such as when the message is displayed in the citizen account. Use the **Expiry Date and Time** field to define an expiry date for the message, for instance, when to remove the message from the Citizen Account.

When the message is saved, it has a status of **In-Edit**. Before the message is displayed in the Citizen Account, it must be published. After it is published, the message is active and is displayed in the Citizen Account based on the effective and expiry dates defined.

Configuring message duration

7.0.3.0

System properties set the length of time a type of message is displayed in the citizen account. For example, a payment message can be configured to be displayed for 10 days. These configuration options apply only to messages that originate as a result of transactions on IBM Cúram Social Program Management.

The following system properties are provided:

- `curam.citizenaccount.payment.message.expiry.days` - this property allows an administrator to dictate the number of days from the effective date that a payment message is displayed in the citizen account. A payment message is displayed for this duration unless another payment message is created which replaces it. The default value is 10.
- `curam.citizenaccount.intake.application.acknowledgement.message.expiry.days` - this property allows an administrator to dictate the number of days from the effective date that an application acknowledgment message is displayed in the citizen account. An acknowledgment message is displayed for this duration unless another acknowledgment message is created which replaces it. The default value is 10.
- `curam.citizenaccount.meeting.message.effective.days` - this property allows an administrator to dictate the number of days from the effective date that a meeting message is displayed. A meeting message is displayed for this duration unless another meeting message is created which replaces it. The default value is 10.

Switching off messages

7.0.3.0

An agency might not want to display messages in the Citizen Account. To cater for this choice, the system property `curam.citizenaccount.generate.messages` enables an agency to switch all messages *on* or *off*. The default value is `true`, which means that messages are generated and displayed in the Citizen Account.

Configuring last logged in information

7.0.3.0

The text displayed in the welcome message and last logged on information can be updated using the properties that are stored in the `CitizenAccountHome` properties file stored in the **Application Resource** section of the Administration Application.

The following properties are provided:

- *citizenaccount.welcome.caption* - updates the welcome message.
- *citizenaccount.lastloggedon.caption* - updates the last logged on message.
- *citizenaccount.lastloggedon.date.time.text* - updates the date and time message.

Configuring contact information

7.0.3.0

Configure contact information for citizens and caseworkers.

Contact information displayed in the citizen account displays contact details (phone numbers, addresses and email addresses) stored for the logged in citizen.

Contact information displayed in the citizen account displays contact details (phone numbers, addresses and email addresses) stored for the logged in citizen and also caseworker contact details (business phone number, mobile phone number, pager, fax and email) of the case owners of cases associated with the logged in citizen in IBM Cúram Social Program Management and on remote systems.

Citizen contact information

The following system property is provided that dictates whether contact information is displayed to a citizen.

Note: This property applies only to citizens registered on IBM Cúram Social Program Management.

If the `curam.citizenaccount.contactinformation.show.client.details` property is set to `true`, citizens' address, phone number, and email address is displayed. If this property is set to `false`, contact information is not displayed. The default value for this property is true.

Caseworker

The following system properties are provided to dictate agency worker contact information is displayed to a citizen and if displayed, additional system properties are provided to dictate the type of contact information displayed:

- *curam.citizenaccount.contactinformation.show.caseworker.details* - dictates whether worker contact details are displayed in the citizen account. If this property is set to true, worker contact details of cases associated with the logged in citizen are displayed. If this property is set to false, worker contact information is not displayed. The default value for this property is true.
- *curam.citizenaccount.contactinformation.show.businessphone* - whether worker contact details are displayed, this property dictates if the worker's business phone number is displayed. The default value of this property is true.
- *curam.citizenaccount.contactinformation.show.mobilephone* - whether worker contact details are displayed, this property dictates if the worker's mobile number is displayed. The default value of this property is true.
- *curam.citizenaccount.contactinformation.show.emailaddress* - whether worker contact details are displayed, this property dictates if the worker's email address is displayed. The default value of this property is true.

- *curam.citizenaccount.contactinformation.show.faxnumber* - whether worker contact details are displayed, this property dictates if the worker's fax number is displayed. The default value of this property is true.
- *curam.citizenaccount.contactinformation.show.pagernumber* - whether worker contact details are displayed, this property dictates if the worker's pager is displayed. The default value of this property is true.
- *curam.citizenaccount.contactinformation.show.casemember.cases* - dictates whether worker contact information is displayed for cases where the citizen is a case member. If this property is set to true, cases where the citizen is a case member are displayed. If this property is set to false, then only cases where the citizen is the primary client are displayed. Note: this property only applies to cases originating from IBM Cúram Social Program Management. The types of product deliveries and integrated cases to be displayed can be configured in the Product section of the Administration Application. For more information on administering this see the *Cúram Integrated Case Management Configuration Guide*.

Configuring remote systems

7.0.3.0

Applications and life events data can be sent through web services for processing by a remote system. To enable remote processing, specify a remote system and the required web services. Remote systems can be configured allowing applications and life event data to be sent to them for processing via associated web services.

Specifying a name and root URL

Remote systems are configured in the Administration application. A name and Root URL must be specified. The Root URL represents the root Uniform Resource Locator (URL) of the remote system. It consists of the Protocol (http or https), Host Name (for example, shell) and Port (for example, 9082) . An example for root URL is http://shell:9082/. A Display Name can be configured which is used to display the name of the agency associated with the remote system. This is used in the citizen account when a list of remote systems are displayed to a citizen. It should be used to represent a more meaningful agency name to a citizen rather than using the remote system name. The Source User Name represents the user name that the remote system uses when invoking inbound Cúram web services.

Adding a service to a remote system

A target system can have multiple services associated with it. A URL must be defined for every service associated with a remote system. The URL is used for identifying and interacting with the service in the remote system. The URL is based on the combination of the root URL of the remote system, consisting of the system host name and port, and the extension URL for the associated service. For example, a URL http://shell:9082/ProcessApplicationService for a process application web service on a remote system is the combination of the root URL(http:// shell:9082/) of the remote system and the extension URL(ProcessApplicationService) of the associated process application service. The Invoking User Name and Password define the user name and password required to communicate with the web service on the remote system.

Securing IBM Cúram Universal Access

7.0.3.0

Understand the security model and how to customize securely in line with this model.

The web application is designed to give citizens access to their most sensitive personal data over the Internet. Security must be a primary concern when developing citizen account customizations. All projects built on Universal Access must be focused on delivering security. This requires the project team to think of security from the very beginning rather just testing it at the end. It is recommended that all projects take at least the following steps to ensure the security of their delivery:

- Ensure that the project team are familiar with the principles of secure application development, and common vulnerabilities such as the OWASP Top Ten.

- Develop and apply a Threat Model
- Employ security experts to test everything from requirements to the finished deployment.
- Plan for how the application will be used in public spaces like libraries and kiosks.

The security model

7.0.3.0

IBM Cúram Universal Access has different account types to support both anonymous and registered citizens. As citizens use Universal Access, they transition through the account types.

IBM Cúram Universal Access has the following user types:

Public citizen account

When citizens view the organization **Home** page they are automatically logged in under the *publiccitizen* account. This account only has access to the home page and pages that allow citizens to enter or reset of passwords.

Anonymous account

When the user clicks a link to perform intake, they are logged out as *publiccitizen* and logged back as an *anonymous* account with a random user name. A principle of Universal Access is that users do not have access to the data of other users. If all intakes and screenings are performed using a single user account, *publiccitizen*, for example, one citizen might see data that has been entered by another citizen.

Registered accounts

Standard accounts created by citizens. Citizens can create accounts when they first use the application, or during processes like applying for benefit. These accounts differ from anonymous accounts in that they allow citizens to continue previously saved applications, restart applications that were previously unfinished, and review or withdraw previously submitted applications.

Linked accounts

Linked accounts are accounts that have been linked with an underlying Concern Role ID for a Person entity.

Some typical scenarios for linking are presented. These are examples, the actual processes for linking is unique to each citizen. A citizen requests a Citizen Account. The citizen is asked to present themselves at their local Social Welfare office with drivers license and other personal identification. The caseworker, uses custom developed functions to enter details for the new linked account after verifying the identity of the citizen.

A citizen creates a user account for Universal Access and submits an Intake Application. They are contacted by their caseworker who asks them if they want access to more services. The citizen agrees and presents themselves at the local office with identification such as a passport. The caseworker is able to link the citizen to the account they used to submit the Intake Application.

In both of these cases the caseworker does not have access to the citizen's password. Instead, the linking process triggers a batch job that generates a letter, sent to the citizen's home address. The letter contains the password and a separate letter then contains an electronic code card. All of this functionality is developed by the customer however it is supported by Universal Access APIs that allow a user name to be linked to a Concern Role ID.

Continuing the above scenario, the citizen receives a letter from the Social Enterprise containing their initial password (in the case of the first scenario) and instructing them that a code card will arrive shortly. The code card arrives by post the next day and the citizen is able to log in to their Citizen Account. The login screen contains a username and password as before, however there are also additional authentication factors - The citizen must enter their date of birth, social security number and a code from their electronic code card. This is called Multi-Factor Authentication.

Authorization roles and groups

7.0.3.0

The account types are assigned different authorization roles. The roles limit the methods that can be invoked. No additional permissions should be granted to authorization roles except for Linked Accounts, which use the LINKEDCITIZENROLE. If adding additional custom methods to citizen account, additional permissions will be required.

For more information about adding additional custom methods to citizen account, see *Customizing the citizen account*.

If only a subset of the functionality offered by IBM Cúram Universal Access is being used, permission to invoke the unused methods should be removed from the database. For example, if citizen account is not used, the LINKEDCITIZENROLE and other related authorization artifacts should be removed, as they are not needed. Projects not using citizen account should also consider the deployment implications. For more information, see *Customizing the citizen account*.

Authorization roles should be configured only for the functionality that is being used. It is recommended that unused Security IDentifiers (SIDs) should be removed from the database. For example, if citizen account is not being used, the LINKEDCITIZENROLE and other related authorization artifacts should be removed, as they are not needed. Projects not using citizen account should also consider the deployment implications. For more information, see *Citizen Account Security Considerations*.

Proper use of the authorization roles and groups ensure that no user can access functions for which they have no permission. It will not however, prevent users from using these functions to access data belonging to user users. This is the preserve of Data-based Security. Universal Access provides a framework for Data-based Security and all customizations should use this framework. For more information, see *Citizen Account Security Considerations*.

Related concepts

Customizing the Citizen Account
Users can use the Citizen Account to log in to a secure area where users can screen and apply for programs.

Security and the Citizen Account
Security must be a primary concern when you customize the citizen account customizations. All public-facing applications must be analyzed and tested before they are deployed. Users must contact IBM support to discuss unusual customizations that might have specific security issues.

Configuring user accounts

7.0.3.0

Three user accounts can be configured: a generic public account, a system generated account, and a citizen generated account.

Generic public account
Use a generic public account when citizens first accesses the organization **Home** page.

System generated account
After citizens navigate from the **Home** page, the system generates a temporary user account and automatically logs them on by using the generated credentials. Use this system generated account to secure any data that the citizen enters before the citizen either creates their own user account or logs in to an existing account. After the citizen logs in, ownership of the data is transferred to the citizen's account.

Citizen created account
Citizens can either create a user account or log in to an existing account. After either option is selected, the citizen's data is secured under this account. This account might be linked to a participant on the system of record that provides the citizen with access to all information that is accessible from the Citizen Account. Multifactor authentication also can be activated for extra authentication when the citizen attempts to log in. For more information about creating an account, see the *Creating a Citizen Account* related link. For more information about authentication, see the *Logging in to a Citizen Account* related link.

A number of configuration settings apply to user name and password. The following parameters can be defined:

- User name and password length.
- The number of special characters of which a password must consist.
- The minimum and maximum password length.
- The maximum number of login attempts before an account is locked out.
- The period after which citizens must change their password. This configuration can be specified in days or can use a date.

The terms and conditions URL also can be defined.

Related concepts

Creating a citizen account and logging in
Citizens can create a citizen account during the application process.

Logging in to a Citizen Account

Integrating external security

7.0.3.0

By default, IBM Cúram Universal Access uses its own authentication system that is backed up by a database of registered users. Universal Access can be configured to integrate with external security systems.

As government agencies increasingly provide online services, there is a drive to ensure that citizens can be authenticated for any of these services by using a single set of credentials. This approach provides benefits for the government in streamlining the authentication process and also for the citizen because citizens do not have to remember user names and passwords.

This process, in turn, increases security for the following reasons:

- It makes it less likely that citizens write down their user names and passwords.
- It focuses security efforts on implementing best practice in a single enterprise security system.

Universal Access can be deployed in *Identity Only* mode for registered users so that creating accounts occurs externally and user accounts defer externally for authentication.

When citizens can access government services online, downloading sensitive personal information on a public computer is a security risk as the downloaded files are cached by the browser. To notify citizens of the security risks, a warning message is displayed before citizens download the PDF. The warning message is configurable in system administration.

The system also displays a citizen timeout message when the application is left idle for a specific period. The time after which the timeout message is displayed is configurable. The citizen can either continue to use the application or quit the application by responding to the timeout message. If the citizen does not respond, the system automatically logs the citizen out of the session.

Account Management

7.0.3.0

You can customize account creation and management.

Account management events

7.0.3.0

Events are raised at key points during account processing. The events can be used to add custom validations to the account management process.

For more information about adding custom validations to the account management process, see the *Cúram Server Developer* section. The following table shows the events that are in the `curam.citizenworkspace.security.impl.CitizenWorkspaceAccountEvents` class:

Table 12: Account events	
Event Interface	**Description**
`CitizenWorkspaceCreateAccountEvents`	Events raised around account creation. For more information, see the related Javadoc information in the WorkspaceServices component.
`CitizenWorkspacePasswordChangedEvent`	Event raised when a user is changing their password. For more information, see the related Javadoc information in the WorkspaceServices component.
`CitizenWorkspaceAccountAssociations`	Events raised when a user is linked or unlinked from an associated Person Participant. For more information, see the related Javadoc information in the WorkspaceServices component.

Related information

Cúram Server Developer

PasswordReuseStrategy API

7.0.3.0

Use the `curam.citizenworkspace.security.impl.PasswordReuseStrategy` API to add your own password change validations.

As part of the password reset function, there is a default validation that prevents a user from entering a new password that is the same as the user's current password. Using the `PasswordReuseStrategy` API, custom validations can be added to restrict users from changing their passwords to current or previous values if required. For example, a customer might want to implement a password reuse strategy that prevents users from reusing a previous password until after six password changes.

For further details, see the API Javadoc.

CitizenWorkspaceAccountManager API

7.0.3.0

Use the `curam.citizenworkspace.security.impl.CitizenWorkspaceAccountManager` API to create and link citizen accounts. Use the API to build out custom functionality to support caseworkers who want to link accounts and create accounts on behalf of the citizen.

The API offers the following methods:

- Creating standard accounts
- Creating linked accounts
- Removing links between participants and accounts.
- Retrieving account information

For more information, see the API Javadoc.

Data caching

7.0.3.0

Minimize the risk of citizens accessing each others' data from browser and server data caches. Cached data can be accessed when citizens use the browser back button or browser history to retrieve data entered by other users, or when PDF files are cached locally on the computer that was used to make the application.

Server caching

HTTP servers like Apache can set cache-control response headers to not store a cache. Use this approach to prevent access to data using the browser back button or history.

Browser caching

Browsers can be configured not to cache content. If citizens can access the web portal in a "kiosk", then the browser should be configured never to cache content.

Advise citizens to clear their cache and close all browser windows they have used when they are finished using the web portal. Also tell citizens to remove PDF documents that they download from the browser's temporary internet files.

External security authentication

7.0.3.0

Ensure that citizens can be authenticated for any of your services by using a single set of credentials. This provides benefits for the government in streamlining the authentication process and also for citizens because they do not have to remember lists of user names and passwords. This, in turn, improves security by making it less likely that citizens write down their user names and passwords and by focusing security efforts on implementing best practice in a single Enterprise Security System.

Universal Access uses its own authentication system which is backed up by a database of registered users. It can also be configured to integrate with external security systems.

Analysis

7.0.3.0

Consider an example analysis to integrate with an external security system.

Any analysis of requirements for external security integration should consider the following questions at a minimum:

1. Does your deployment support anonymous screening and/or intake?
2. Is Account Management supported in IBM Cúram Universal Access or in the External Security System?
3. Is Single Sign On Required (SSO)?

Example customization requirements

7.0.3.0

An example is described for a team that is deploying Universal Access.

In the following example, the team that is deploying Universal Access has the following requirements. The example will be used for reference when describing the configuration and development tasks.

1. Users can access Universal Access and perform anonymous Screening or Intake.
2. Users who want to access their saved screening or intake information must first create an account on a system called CentralID.
3. Users logging in to Universal Access can use their CentralID username and password to authenticate.
4. Users perform all of their account management using an external system we're calling CentralID (for example, resetting password, creating a new account, changing account details).
5. CentralID stores all user records in a secure LDAP server.
6. Because all account management is now performed in CentralID, the account creation screens and password reset screens are to be removed from Universal Access.
7. Users should be able to log in as soon as they have registered with CentralID, there should be no delay waiting for id to propagate to Universal Access.

Configuring the sample requirements

7.0.3.0

Configure the sample requirements for the analysis example.

Taking the analysis example, carry out the following configuration tasks:

1. Configure the Application Server to use LDAP for authentication.
2. Deploy the Universal Access in **Identity Only** mode for registered users.
3. Configure the Universal Access so that **Create account** pages are not displayed.
4. Configure the Universal Access so that users are directed to register with the External System.

Configuring an alternate login ID

7.0.3.0

By default, user names cannot be changed after they are created. However, you can configure an alternate login ID that can be updated.

For information about configuring alternate login IDs, see the related links. If you configure an alternate login ID for a user name that is case-sensitive, then the alternative login ID is also case-sensitive.

It is necessary to complete the LDAP setup task that is listed in “Configuring the sample requirements” on page 74 only if the user is in `Identity-Only` mode. In `Identity-Only` mode, it is necessary to match the login IDs that are stored in LDAP with the login IDs that are stored in the `ExtendedUsersInfo` table.

Related information

Cúram Regionalization Guide
Alternate Login IDs
Configuration of the Apache log4j Java-based logging utility

Configure the application server to use LDAP for authentication

7.0.3.0

Refer to the relevant application server documentation for information about how to configure your application server to use LDAP for authentication.

Deploying in identity-only mode for registered users

7.0.3.0

Configure the necessary properties to deploy in identity-only mode for registered users.

Add the following properties to *AppServer.properties*.

```
curam.security.check.identity.only=true
curam.security.user.registry.disabled.types=EXT_AUTO,EXT_GEN
curam.citizenworkspace.enable.usertypes.for.temporary.users=true
public.user.type=EXT_AUTO
```

To re-configure the application server run:

```
appbuild configure
```

The `curam.security.check.identity.only` property ensures that application security is set to work in Identity Only mode. For more information about Identity Only authentication mode, see *Deployment Guide for WebSpher* or *Deployment Guide for WLS* as appropriate. In Identity Only mode authentication only uses the internal user table to check for the existence of the user. The validation of the password is left to a subsequent module, either a JAAS module (Oracle WebLogic) or the User Registry (IBM WebSphere).

Take the example of a user, "johnsmith", who has been registered with the CentralID LDAP server. In order for John Smith to be able to use Universal Access, there must also be a "johnsmith" entry in the ExternalUser table. When John Smith logs in, his authentication request is passed to the Cúram JAAS Login Module. This checks that the user "johnsmith" exists in the Cúram ExternalUser table but does not check the password. The authentication then proceeds to the User Registry (WebSphere) or LDAP JAAS Module (WebLogic) where the username and password are checked against the contents of the CentralID LDAP server. For this to work correctly it is necessary to configure the application server with the connection details for the secure LDAP server.

The Identity Only configuration allows the application to defer to an external security system such as an LDAP-based directory service for the authentication of user credentials. This does not work for anonymous users however. When a user accesses the organization **Home** page for the first time, they are automatically logged in as a "publiccitizen" user. If they subsequently choose to screen themselves or perform an intake, Universal Access creates a new "generated" anonymous user. Each generated user is unique and this ensures that the data belonging to that user is kept confidential. Neither the publiccitizen nor the generated users are inserted into the LDAP directory so they cannot be authenticated using the Identity Only mechanism. This is the purpose of the following line of configuration:

```
curam.security.user.registry.disabled.types=EXT_AUTO,EXT_GEN
```

This line ensures that users with the user type EXT_AUTO (the publiccitizen) and EXT_GEN (generated users) are authenticated against the External User table. Once the server has been configured with the above configuration and started, perform the following configuration steps:

1. Log in as sysadmin.
2. **Select Application Data** > **Property Administration**.
3. Select category **Citizen Account - Configuration**.
4. Set the property **curam.citizenaccount.public.included.user** to EXT_AUTO.
5. Set the property **curam.citizenaccount.anonymous.included.user** to EXT_GEN.
6. Set the property **curam.citizenworkspace.enable.usertypes.for.temporary.users** to TRUE.
7. **Publish** the property changes.

   You need another configuration entry so that Universal Access operates correctly with respect to authentication as follows.
8. Log in as sysadmin.
9. Select **Select Application Data** > **Property Administration**.
10. Select category **Infrastructure – Security parameters**.
11. Set **curam.custom.externalaccess.implementation** to **curam.citizenworkspace.security.impl.CitizenWorkspacePublicAccessSecurity**.
12. **Publish** the property changes.
13. Log out and restart the server.

Disabling the Create Account screens

7.0.3.0

Configure the necessary properties to disable the screens for creating an account.

In the example, requirement 4 in *Example customization requirements* indicates that all Account Management functions are handled by the external system, CentralID. These include creation of a new account and performing a password reset. By default, Universal Access provides screens for these functions. These screens must be configured out to meet requirement 4 above:

1. Log in as sysadmin.
2. Select **Application Data** > **Property Administration**.
3. Select Category **Citizen Portal - Configuration**.
4. Set the property *curam.citizenworkspace.enable.account.creation* to **NO**.
5. **Publish** the property changes.

The above steps remove references to **Account Creation** pages from Universal Access. The Login screen still contains a link to a page for changing passwords. In this example the team implementing want to retain this link but change it to launch a new browser window on the CentralID password reset page. This can be achieved as follows:

1. Log in as sysadmin.
2. Select **Application Data** > **Property Administration**.
3. Select Category **Citizen Portal - Configuration**.
4. Set the property *curam.citizenworkspace.forgot.password.url* to , for example **http:// www.centralid.gov/resetpassword**
5. **Publish** the property changes.

To remove the reset password link altogether use the following steps:

1. Log in as sysadmin.
2. Select **Application Data** > **Property Administration**.
3. Select Category **Citizen Portal - Configuration**.

4. Set the property *curam.citizenworkspace.display.forgot.password.link* to **NO**.
5. **Publish** the property changes.

Redirecting users to register with an external system

7.0.3.0

Configure the message that is displayed in the log-on screen.

Universal Access invites users to log in with the message: **Please enter your User Name and Password and click the Next button to continue.** Replace this message to directing the non-registered user towards the CentralID screen for registration. For example the message on the Logon screen could read something like:

```
"<p>If you are registered with CentralID enter your username
   and password to log in. To register go to
   <a href="http://www.centralid.gov/register"> The CentralID
   registration page.</a></p>"
```

The properties for controlling the login page message are in `<CURAM_DIR>/EJBServer/components/Data_Manager/Initial_Data/blob/prop/Logon.properties`

To customize the message displayed, follow the procedure in *Customizable IBM Cúram Universal Access* Page Content.

Related concepts

Example customization requirements
An example is described for a team that is deploying Universal Access.

Development tasks

7.0.3.0

Complete the configuration required to implement the external security authentication requirements.

The configuration tasks allow customers to fulfill the requirements listed in the example with the exception of requirement:

```
"7 - Users should be able to log in to Universal Access as soon as they have registered with
    CentralID, there should be no delay waiting for id to propagate to other systems".
```

To function correctly, each user must have an entry in the ExternalUser table. The customer could build a batch process to import users from the LDAP directory into the ExternalUser table but this would not satisfy requirement 7 since the user must be able to register with CentralID and then immediately use Universal Access. Another option would be to build a web service or similar mechanism that would be invoked when a new user registers with CentralID. The implementation of the web service would create the appropriate entry in the ExternalUser table.

This document however, now describes a simpler option which is to override the default login behavior to create new accounts on-the-fly, after checking that the relevant entry exists in the LDAP server.

Overriding the default login behavior in Universal Access can be done by extending the curam.citizenworkspace.security.impl.AuthenticateWithPasswordStrategy class and overriding the authenticate() method. The code below outlines how to use the AuthenticateWithPasswordStrategy and other security APIs to meet the requirements described above:

```
public class CustomSecurityStrategy extends AuthenticateWithPasswordStrategy {
  @Inject
  private CitizenWorkspaceAccountManager cwAccountManager;
  ...
  @Override
  public String authenticate(final String username,
      final String password)
      throws AppException, InformationalException {
    final String retval = null;
    if (username.equals(PUBLIC_CITIZEN)) {
      return super.authenticate(username, password);
    }
    // Authenticate generated accounts as normal
    if (cwAccountManager.isGeneratedAccount(username)) {
      return super.authenticate(username, password);
    }
    // Check that the user exists in LDAP
    // This prevents hackers from registering a lot of bogus
```

```
    // accounts that exist in Curam but not in LDAP
    if (!isUserInLDAP(username)) {
      return SECURITYSTATUS.BADUSER;
    }
    // If there's no account for this user
    if (!cwAccountManager.hasAccount(username)) {
      createUserAccount(username);
    }
    return SECURITYSTATUS.LOGIN;
  }
  private void createUserAccount(final String username)
      throws AppException, InformationalException {
    final CreateAccountDetails newAcctDetails;
    ...
    cwAccountManager.createStandardAccount(newAcctDetails);
  }
}
```

The code above checks to see if the user logging in is the publiccitizen user or a generated account. In both of these cases, authentication logic is delegated to the default AuthenticateWithPasswordStrategy. In the case of a registered user, the Strategy checks the LDAP directory to ensure that the user exists there. If the user exists in the LDAP directory and does not exist yet in Universal Access, then a new user account is created. Note, the custom code does not need to authenticate the user against LDAP since the authentication is handled by the User Registry in WebSphere or the LDAP JAAS Module in WebSphere. It is important to note that the password parameter of the authenticate() method is passed in clear text.

In order to install the CustomSecurityStrategy it must be bound in place of the Default Security Strategy. This can be done by using a Guice Module to bind the implementation:

```
public class CustomModule extends AbstractModule {
  @Override
  protected void configure() {
    binder().bind(SecurityStrategy.class).to(
      CustomSecurityStrategy.class);
  }
}
```

The CustomModule must be configured at startup. This can be achieved by adding a DMX file to the custom component as follows:

```
<CURAM_DIR>/EJBServer/custom/data/initial/MODULECLASSNAME.dmx

<?xml version="1.0" encoding="UTF-8"?>
<table name="MODULECLASSNAME">
    <column name="moduleClassName" type="text" />
    <row>
      <attribute name="moduleClassName">
        <value>gov.myorg.CustomModule</value>
      </attribute>
    </row>
</table>
```

Configuring single sign-on

7.0.3.0

Single sign-on (SSO) authentication enables users to access multiple secure applications by authenticating only once by using a single user name and password. Federated single sign-on that uses a SAML 2.0 IdP-initiated POST binding can be implemented through the Citizen Engagement app.

If a user authenticates to an SSO system, the user is no longer prompted for credentials when the user accesses multiple applications that are configured to work with the SSO system.

SSO systems usually maintain the user accounts on an LDAP (lightweight directory application protocol) server. If user accounts are stored at one location, it is easier for system administrators to safeguard the accounts. Also, when necessary, it is easier for users to reset their account passwords at one location instead of at multiple applications.

The following topics discuss the scenario where IBM Cúram Social Program Management is deployed on WebSphere. However, a similar process applies if IBM Cúram Social Program Management is deployed on another supported application server, such as Oracle Weblogic.

Related information

Oracle: Configuring SAML 2.0 Services

SAML web single sign-on profile initiation

7.0.3.0

An unauthenticated user can initiate a SAML web single sign-on (SSO) profile either through a service provider (SDP), or through an identity provider (IdP).

SP initiation

When an unauthenticated user first accesses an application through an SP, the SP directs the user's browser to the IdP to authenticate. To be SAML specification compliant, the flow requires the generation of a SAML `AuthnRequest` from the SP to the IdP. The IdP receives the `AuthnRequest`, validates that the request has come from a registered SP, and then authenticates the user. After the user has been authenticated, the IdP directs the browser to the Assertion Consumer Service (ACS) application that is specified in the `AuthnRequest` that was received from the SP.

IdP initiation

The IdP can send the assertion request to the service provider ACS in one of two ways:

- The IdP sends a URL link in a response to a successful authentication request. The user must click on the URL link to post the SAML response to the service provider ACS.
- The IdP sends an auto-submit form to the browser that automatically posts the SAML response to the service provider ACS.

The ACS validates the assertion and creates a JAAS subject, and then redirects the user to the SP resource, as shown in the following figure.

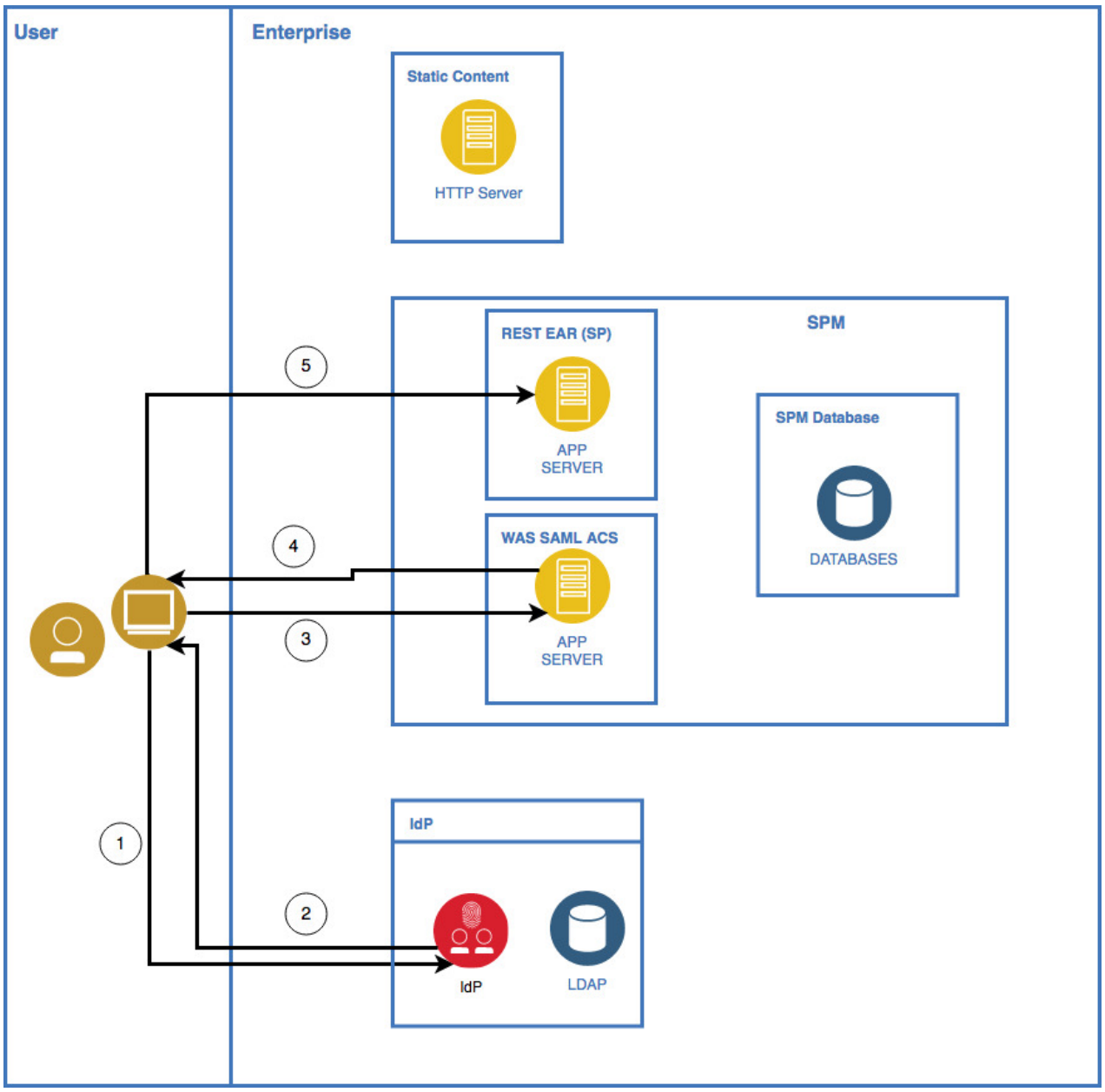


Figure 1: IdP initiated flow

Assertions and the SAML Response document

In all SAML web SSO profile flows, the binding defines the mechanism that is used to send information through assertions between the IdP and the SP. WebSphere supports HTTP POST binding for sending web SSO profiles. The browser sends an HTTP POST request, whose POST body contains a SAML response document document. The SAML Response document is an XML document that contains information that includes the following items:

- – The logged in user's identity, which includes the user name, password, address and role, and how the user authenticated, and so on
  - – The time period for which the assertion is valid
  - – The identify provider that sent the assertion
  - – What audiences the assertion is meant to be valid for

- Group and role information about the user
- Other application-specific assertions and attributes that are related to the user

A simple assertion typically includes only the first three items from the previous list. To prove the authenticity of the information, the assertion is almost always digitally signed. To protect the confidentiality of parts of the assertion, the payload can be digitally encrypted.

The inclusion of extra attributes and assertions is limitless, which can cause the inclusion of a large amount of raw data in the document. The use of the XML format increases the size of the XML document through the inclusion of XML element tags, attribute names, and namespaces. When an assertion is digitally signed, the XML document includes the key information that is necessary for the receiver to validate the signature. If an assertion is encrypted, the XML document includes the public certificate that is used to encrypt the data.

The SAML Response XML document is then deflated and Base64 encoded, which further increases the size of the data. A typical SAML Response contains information that can be sent only through a login by a POST parameter. After login, an alternative mechanism is typically used to maintain the logged-in security context. Most systems use some cookie-based, server-specific mechanism, such as a specific security cookie, or the server's cookie tied to the user's HTTP session.

Related information

Oasis: SAML 2.0 Technical Overview

Oracle: JAAS Authorization Tutorial

The SAML 2.0 single sign-on flow in IBM Cúram Universal Access

7.0.3.0

To implement a more seamless SAML SSO flow,Universal Access only supports an identity provider (IdP) initiated web SSO flow. The SAML POSTs are controlled through the logic in Universal Access.

Browser-based single sign-on (SSO) through SAML v2.0 works well with many web applications where the SAML flow is controlled by HTTP redirects between the identity provider (IDP) and the service provider (SP). The user is guided seamlessly from login screens to SP landing pages by HTTP redirects and hidden forms that use the browser to POST received information to either the IdP or the SP.

In a single page application, all the screens are contained within the application and dynamic content is expected to be passed only in JSON messages through XMLHttpRequests. Therefore, the rendering of HTML content for login pages and the automatic posting of hidden forms in HTML content is more difficult. If the SP processes the content in the same way, it would be necessary to leave the application and hand back control to either the user agent or the browser, in which case the application state would be lost.

Therefore, Universal Access supports only an IdP initiated web SSO flow. Any attempt to connect to a protected resource without first authenticating through IdP results in a 403 HTTP response from IBM Cúram Social Program Management web API. Therefore, an authentication request that is initiated through SP will results in a 403 HTTP response, and the application will then redirect the user to the login page that is contained in Universal Access.

The following figure illustrates the IdP initiated flow that is supported by Universal Access in a default installation.

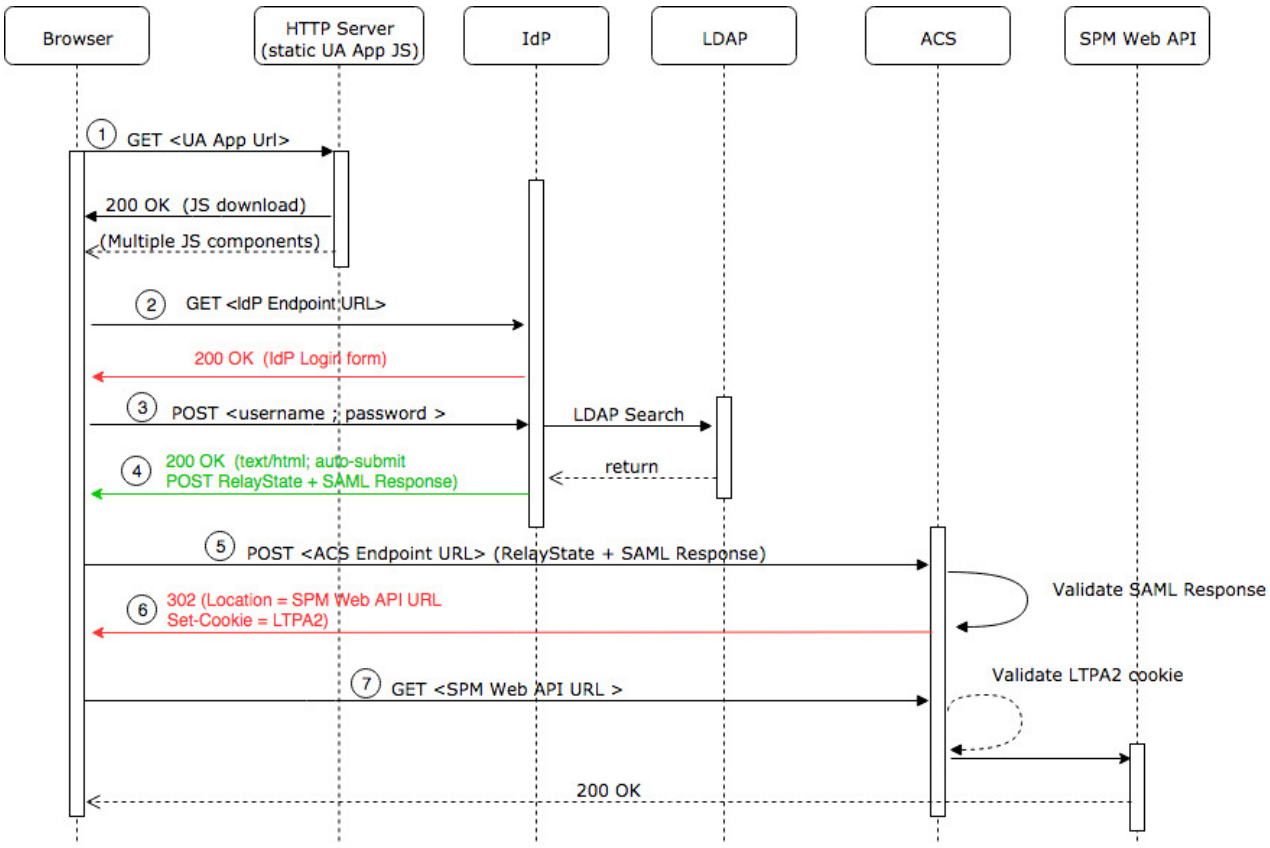


Figure 2: IdP initiated flow in IBM Cúram Universal Access

The following list references the numbered items in the image and provides a description of each step in the flow.

1. A user browses to the HTTP server that contains Universal Access.
2. The user can browse as normal by interacting with IBM Cúram Social Program Management as either a public or a generated user (which is not shown in the diagram). The user then opens the login page to access protected content, which triggers an initial request to the IdP endpoint. In most IdP configurations, an HTML login form responds to the request. Universal Access ignores the response.
3. To authenticate, the user completes the login form and clicks **Submit**. The form submission triggers an HTTP POST request that contains login credentials to the IdP.
4. After successful validation of the user credentials at the IdP, the IdP populates the SAML Response and returns it in an HTML form that contains hidden input fields. Several redirects might occur before the 200 OK HTTP response that contains the SAML information is received. Universal Access does not respond to the redirects.
5. Universal Access extracts the `RelayState` and `SAMLResponse` values, and inserts them in a new POST request to the application server Assertion Consumer Service (ACS).
6. The application server ACS validates the signature that is contained in the SAML Response. WebSphere Application Server also ensures that the originator is a Trusted Authentication Realm. If the validation is successful, the ACS sends an HTTP redirect that points to the configured IBM Cúram Social Program Management target landing page, along with an LTPA2 Cookie that will be used in any subsequent communication. The browser automatically sends a new request to the target URL, but Universal Access does not respond to the request.
7. Universal Access begins its standard user setup by requesting account and profile information from the relevant web API endpoints.

Configuring single sign-on properties

7.0.3.0

To enable IBM Cúram Universal Access to work with SAML single sign-on (SSO), configure the appropriate properties in the `.env` environment variable file that is in the root of the starter pack. Then, rebuild Universal Access.

Procedure

- Edit the following properties:

  REACT_APP_SSO_ENABLED
  This property takes a Boolean value. To enable SO authentication in Universal Access, set the value to `true`. If the value is false, SSO is disabled.

  REACT_APP_IDP_LOGIN_URL
  This property value specifies the identity provider (IdP) login page URL, for example:

  ```
  https://192.168.0.1:12443/pkmslogin.form
  ```

  REACT_APP_ACS_URL
  This property value specifies the Assertion Consumer Service (ACS) application server URL, for example:

  ```
  https:// 192.168.0.2:9443/samlsps/acs
  ```

  REACT_APP_SAML_INITIAL
  This property value specifies the SSO SAML initial request URL as defined by the IdP, for example:

  ```
  REACT_APP_SAML_INITIAL=https://192.168.0.1:12443/isam/sps/saml20idp/saml20/logininitial?
    RequestBinding=HTTPPost&PartnerId=https://192.168.0.2:9443/samlsps/
  acs&NameIdFormat=Email)
  ```

Related information

Cúram REST configuration properties

Configuring cross-origin resource sharing

7.0.3.0

For security reasons, browsers restrict cross-origin HTTP requests, including XMLHttpRequest HTTP requests, that are initiated inside IBM Cúram Universal Access. When the Universal Access application and the Universal Access web API are deployed on different hosts, extra configuration is required.

About this task

Universal Access can request HTTP resources only from the same domain that the application was loaded from, which is the domain that contains the static JavaScript. To enable Universal Access to support cross-origin resource sharing (CORS), enable the use of CORS headers.

Procedure

1. Log on to the IBM Cúram Social Program Management application as a system administrator, and click **System Configurations**.
2. In the Shortcuts panel, click **Application Data** > **Property Administration**.
3. Configure the curam.rest.allowedOrigins property with the values of either the host names or the IP addresses of the IdP server and the web server on which Universal Access is deployed.

Single sign-on configuration example

7.0.3.0

The example outlines a single sign-on (SSO) configuration for IBM Cúram Universal Access that uses IBM Security Access Manager to implement federated single sign-on by using the SAML 2.0 Browser POST profile.

Universal Access SSO configuration components

The following figure shows the components that are included in a Universal Access SSO configuration.

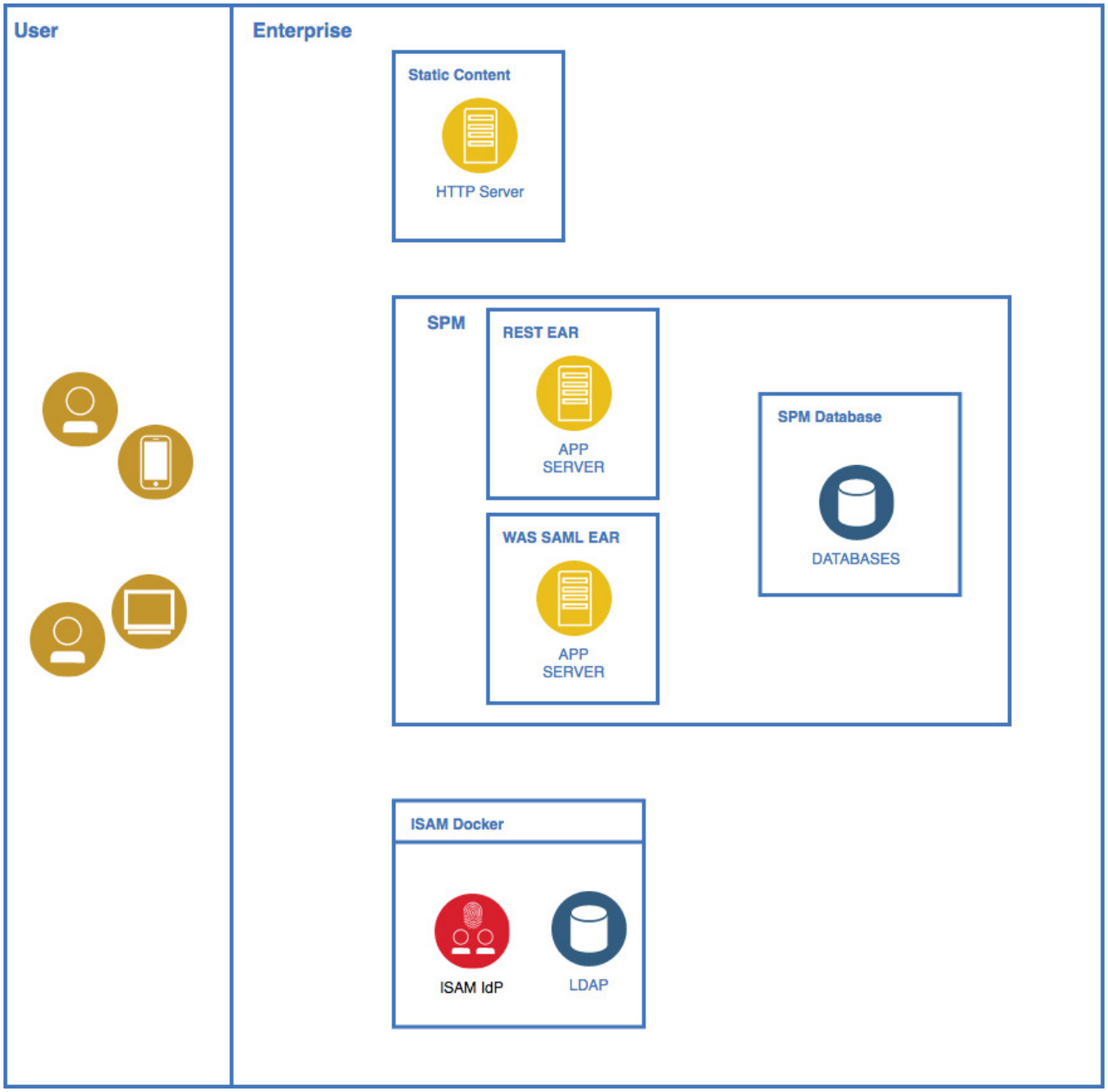


Figure 3: Universal Access SSO configuration components

Web browser
A user sends requests from the web browser for applications in the SSO environment.

Web server
Universal Access ReactJS static content that is deployed on a web server, for example, IBM HTTP Server, Apache.

IBM Security Access Manager server
The IBM Security Access Manager server includes the identity provider (IdP).

OpenLDAP server (user directory)
Among other items, OpenLDAP server contains the user name and password of all the valid users in the SSO environment.

IBM WebSphere Application Server
Among other applications, WebSphere Application Server contains deployed IBM Cúram Social Program Management, Citizen WorkSpace, and REST enterprise applications.

WebSphere SAML EAR
WebSphere package that contains the packages to run the SAML Assertion Consumer Service (ACS).

Database
Storage for the IBM Cúram Social Program Management, Citizen WorkSpace, and REST enterprise applications.

Configuring single sign-on through IBM Security Access Manager

7.0.3.0

Use the IBM Security Access Manager management console to configure single sign-on (SSO) in IBM Cúram Universal Access.

Before you begin

1. Start IBM Security Access Manager.
2. In the management console, log on as an administrator.
3. Accept the services agreement.
4. If required, change the administrative password.

About this task

In the IBM Security Access Manager management console, complete the steps that are outlined in the following procedure:

Procedure

1. Configure the IBM Security Access Manager database:
   a) In the top menu, click **Home Appliance Dashboard** > **Database Configuration**.
   b) Enter the database configuration details, such as **Database Type**, **Address**, **Port**, and so on, and click **Save**.
   c) When the **Deploy Pending Changes** window opens, click **Deploy**.
2. To install all the required product licenses, repeat the following steps for each activation code, where each activation code corresponds to a product license:
   a) In the IBM Security Access Manager management console, click **Manage System Settings** > **Licensing and Activation**.
   b) To import the licenses for IBM Security Access Manager and the federation add-on, click **Import**.
3. Configure the LDAP SSL database:
   a) In the IBM Security Access Manager management console, click **Manage System Settings** > **SSL Certificates**.
   b) Click **New** and create an `Ex: ldap` entry.
   c) Select the new **Ex: ldap** entry in the list.
   d) Click **Manage** > **Edit SSL Certificate Database**.
   e) In the **Edit SSL Certificate Database** window, click **Manage** > **Load**.
   f) In the window that opens, enter the LDAP server host name or IP address, the port number, and a name.
   g) Click load to retrieve the signer certificate from the LDAP server.
   The retrieved signed certificate is displayed in the list.
   h) Close the window.
   i) Select the option to deploy the pending changes.

4. Configure the runtime component:
   a) In the IBM Security Access Manager management console, click **Secure Web Settings** > **Runtime Component**.
   b) Click **Configure to display Runtime Environment Configuration popup**.
   c) Click the **Main** tab, then select **LDAP Remote for remote LDAP registry** and click **Next**.
   d) For **Management Domain**, select the default value, and enter the relevant data in the remaining fields.

      In IBM Security Access Manager Policy Server, you can retain the default value for `Management Domain`.
   e) In the **LDAP** tab, enter the following values:

      Hostname
      `LDAP server host name or IP address`

      Port
      `LDAP server host name or IP address`

      DN
      `cn=root,secAuthority=Default`

      Password
      `LDAP password`

      Enable SSL check box
      Select the **Enable SSL** check box.

      Certificate Database
      From the list, select the LDAP SSL database that you created previously, `Ex: ldap`.
   f) Click **Finish**.

Configuring IBM Security Access Manager as an IdP

7.0.3.0

To configure IBM Security Access Manager as an identity provider (IdP), see the IBM Security Access Manager 9.0 Federation Cookbook that is available from IBM Developer Works.

Before you begin

Download the IBM Security Access Manager 9.0 Federation Cookbook from IBM Developer Works, as shown in the related link. Also download the mapping files that are provided with the cookbook.

About this task

To set up the example environment are, complete the specified sections in the IBM Security Access Manager 9.0 Federation Cookbook in order.

Procedure

1. Complete *Section 5, Create Reverse Proxy instance*.
2. Complete *Section 6, Create SAML 2.0 Identity Provider federation*.

   In Section 6.1, if you are using the ISAM docker deployment, it is possible to re-use the existing keystore that is included in the container instead of creating a new keystore. It is important to reflect this change in subsequent sections where the myidpkeys certificate database is referenced.
3. Complete *Section 8.1, ISAM Configuration for the IdP*.

   In Section 8.1, use the host name of the IdP federation.
4. Optional: After completing Section 8.1.1, if you require ACLs to be defined to allow and restrict access to the IdP junction, then follow the instructions in *Section 25.1.3, Configure ACL policy for IdP*.
5. Complete *Section 9.1, Configuring Partner for the IdP*.

The export from Websphere does not contain all the relevant data. Therefore, in Section 9.1, after you complete configuring partner for the IdP, you must click **Edit configuration** and complete the remaining advanced configuration.

Related information

IBM Security Access Manager 9.0 Federation Cookbook

Configuring WebSphere Application Server

7.0.3.0

The procedure outlines the high-level steps that are required to configure IBM WebSphere Application Server as a SAML service provider.

About this task

For more information, see the related link to the WebSphere Application Server documentation.

Procedure

1. Deploy the `WebSphereSamlSP.ear` file.

   The `WebSphereSamlSP.ear` file is available as an installable package. Choose one of the following methods:

   - Log on to the WebSphere Application Server administrative console, and install the `app_server_root/installableApps/WebSphereSamlSP.ear` file to your application server or cluster.
   - Install the SAML Assertion Consumer Service (ACS) application by using a Python script. In the `app_server_root/bin` directory, enter the following command to run the `installSamlACS.py` script:

     ```
     wsadmin -f installSamlACS.py install nodeName serverName
     ```

     In the previous command, *nodeName* is the node name of the target application server, and *serverName* is the server name of the target application server.
2. Configure the ACS trust association interceptor:
   a) In the WebSphere Application Server administrative console, click **Global security** > **Trust association** > **Interceptors** > **New**.
   b) For **Interceptor class name**, enter `com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor`.
   c) Under custom properties, enter the values that are shown in the following table:

   In a standard WebSphere Application Server configuration, you would also define a value for the `login.error.page` custom property. However, the preferred method is to log onto the IdP first. Therefore, if you do not define a value for `login.error.page`, WebSphere Application Server returns a 403 error if a user logs on without first logging onto the identity provider (IdP).

Table 13: ACS trust association interceptor custom properties

Custom property name	**Value**
sso_1.sp.acsUrl	https://*WAS_host_name:ssl port*//samlsps/acs
sso_1.idp_1.EntityID	https://*isam_hostname:isam_port*//*URL of ISAM/ISAM Junction/IdP endpoint/federation name*/saml20
sso_1.idp_1.SingleSignOnUrl	https:// *isam_hostname:isam_port*//*URL of ISAM/ISAM Junction/IdP endpoint/federation name*/saml20/login
sso_1.sp.targetUrl	https://*WAS_host_name*:*WAS_port*/Rest

Table 13: ACS trust association interceptor custom properties (continued)	
Custom property name	**Value**
sso_1.idp_1.certAlias	isam-conf
sso_1.sp.filter	request-url^=/Rest;request-url!=/Rest/j_security_check
sso_1.sp.enforceTaiCookie	false

3. Add the IdP federation partner data. The following substeps describe how to add the IdP data by using the WebSphere Application Server administrative console.
   a) To add the IdP host name or IP address as a trusted realm, click **Global security** > **Trusted authentication realms - inbound** > **Add External Realm**.
   b) Enter either the IBM Security Access Manager host name or IP address.
   c) To load the IdP certificate from IBM Security Access Manager, click **Security** > **SSL certificate and key management** > **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates** > **Retrieve from port**
   d) Enter the IBM Security Access Manager IP address and listener port, for example, `12443, alias = isam-conf`.

      Note: When the browser first attempts to connect to the IBM Cúram Social Program Management web API, an LTPA2 cookie is sent as part of the request. If the WebSphere Application Server com.ibm.ws.security.web.logoutOnHTTPSessionExpire property is set to true, which is the default configuration in IBM Cúram Social Program Management, then authentication fails because an HTTP session does not exist on the application server. By setting the property to `false`, the check for a valid HTTP session is not completed and when the LTPA2 token is valid, authentication succeeds.

      To configure the property in the WebSphere Application Serveradministrative console, click **Security** > **Global security** > **Custom properties**, and set the value of com.ibm.ws.security.web.logoutOnHTTPSessionExpire to `false`.
4. Implement cross-origin resource sharing (CORS) from the HTTP server to the WebSphere Application Server SAML ACS.
   a) To add a CORS header, configure a servlet filter for the `WebSphereSamlSP.ear` file that is deployed by a Trust Association Interceptor (TAI). The servlet filter adds a CORS HTTP header to HTTP responses. You can archive the implemented servlet filter as a `jar` file, and then store it in the `WebSphereSamlSP.ear\WebSphereSamlSPWeb.war\WEB-INF\lib` directory that is in the `installedApps` directory of your project in WebSphere Application Server.
   See the following example of how to implement a servlet filter:

```
public class SampleFilter implements Filter {

       @Override
       public void doFilter(ServletRequest arg0, ServletResponse servletResponse,
            FilterChain arg2) throws IOException, ServletException {

HttpServletResponse response = (HttpServletResponse) servletResponse;
HttpServletRequest request = (HttpServletRequest) arg0;


response.setHeader("Access-Control-Allow-Origin",
     "http://dubxpcvm156.mul.ie.ibm.com:9880");     <hostname or IP address of IBM UA
server>
response.setHeader("Access-Control-Allow-Credentials", "true");
response.setHeader("Access-Control-Allow-Headers", "x-requested-with, Content-Type,
origin, authorization, accept, client-security-token");
response.setHeader("Access-Control-Expose-Headers", "content-length");
       arg2.doFilter(request, response);
     }
}
```

b) Configure the `web.xml` file for the deployed TAI EAR file to use the servlet filter for all the requests. Add the filter element that is shown in the following sample to the `web.xml` file, with the actual fully qualified name of the filter.

You can add the filter element as a sibling to any existing element n the `web.xml` file, such as `<servlet>`. The `web.xml` file is in the `WebSphereSamlSP.ear\WebSphereSamlSPWeb.war \WEB-INF\lib` directory, which is in the `installed`Apps directory of your project in WebSphere Application Server.

```
<filter>
    <filter-name> SampleFilter </filter-name>
    <filter-class> SampleFilter</filter-class>
  </filter>
  <filter-mapping>
    <filter-name> SampleFilter</filter-name>
    <url-pattern>/*</url-pattern>
 </filter-mapping>
```

Related information

Enabling WebSphere Application Server to use the SAML web SSO feature

Configuring CORS for IBM Security Access Manager

7.0.3.0

To permit cross-origin requests from the HTTP server to the IBM Security Access Manager domain, configure the IBM Security Access Manager runtime environment.

Procedure

1. To create LDAP and IBM Security Access Manager runtime users, create an `ldif` file that can be used to populate OpenLdap, as shown in the following sample:

```
# cat UA_usersCreate_ISAM.ldif
dn: dc=watson-health,secAuthority=Default
objectclass: top
objectclass: domain
dc: watson-health

dn: c=ie,dc=watson-health,secAuthority=Default
objectclass: top
objectclass: country
c: ie

dn: o=curam,c=ie,dc=watson-health,secAuthority=Default
objectclass: top
objectclass: organization
o: curam

dn: ou=curamint,o=curam,c=ie,dc=watson-health,secAuthority=Default
objectclass: top
objectclass: organizationalUnit
ou: curamint

dn: cn=caseworker,ou=curamint,o=curam,c=ie,dc=watson-health,secAuthority=Default
objectclass: person
objectclass: inetOrgPerson
objectclass: top
objectclass: organizationalPerson
objectclass: ePerson
cn: caseworker
sn: caseworkersurname
uid: caseworker
mail: caseworker@curam.com
userpassword: Passw0rd

dn: ou=curamext,o=curam,c=ie,dc=watson-health,secAuthority=Default
objectclass: top
objectclass: organizationalUnit
ou: curamext

dn: cn=jamessmith,ou=curamext,o=curam,c=ie,dc=watson-health,secAuthority=Default
objectclass: person
objectclass: inetOrgPerson
objectclass: top
objectclass: organizationalPerson
```

```
objectclass: ePerson
cn: jamessmith
sn: Smith
uid: jamessmith
mail: jamessmith@curamexternal.com
userpassword: Passw0rd
```

2. Add users to the OpenLDAP database:
   a) On the host server that is running the docker containers, enter the following command:

   ```
   docker cp UA_usersCreate_ISAM.ldif idpisam9040_isam-ldap_1:/tmp
   ```

   b) To log on to the OpenLDAP container, enter the following command:

   ```
   docker exec –ti idpisam9040_isam-ldap_1 bash
   ```

   c) To add the users to OpenLDAP, enter the following command:

   ```
   ldapadd -H ldaps://127.0.0.1:636 -D cn=root,secAuthority=default -f /tmp/
   Curam_usersCreate_ISAM.ldif
   ```

3. Import the users into IBM Security Access Manager:
   a) To log on to the IBM Security Access Manager command line interface, enter the following commands:

   ```
   docker exec -ti idpisam9040_isam-webseal_1 isam_cli
   isam_cli> isam admin
   pdadmin> login -a sec_master -p <password>
   ```

   b) To import the users into IBM Security Access Manager, enter the following commands:

   ```
   pdadmin sec_master> user import caseworker
   cn=caseworker,ou=curamint,o=curam,c=ie,dc=watson-health,secAuthority=Default
   pdadmin sec_master> user modify caseworker account-valid yes
   pdadmin sec_master> user import jamessmith
   cn=jamessmith,ou=curamext,o=curam,c=ie,dc=watson-health,secAuthority=Default
   pdadmin sec_master> user modify jamessmith account-valid yes
   ```

4. To test the identity provider (IdP) flow, enter the following URL in a browser:

   ```
   https://ISAM login initial URL?RequestBinding=HTTPPost
   &PartnerId=webspherehostname:9443/samlsps/acs&NameIdFormat=Email
   &Target=WAS hostname:WAS port/Rest/v1
   ```

   Replace the following values in the URL with the appropriate values for your configuration:

   - *IBM Security Access Manager login initial URL*
   - *WebSphere host name*
   - *WebSphere Application Server host name*
   - *WebSphere Application Server port*; inIBM Cúram Social Program Management the default value is 9044

   When the IBM Security Access Manager docker container starts, the IdP endpoints are initialized only when the first connection request is received. However, if the first connection request is triggered by IBM Cúram Universal Access, an XHR timeout occurs before the initialization finishes. Therefore, this test step is required to ensure that the initialization of the IdP endpoints is completed.

5. In a browser, go to the home page and log in.

Customizing IBM Cúram Universal Access

7.0.3.0

Use this information to customize Universal Access. Typical customizable features are security and the citizen account.

Error logging in the citizen account

7.0.3.0

When a citizen submits an application, when a citizen clicks **Submit** a deferred process starts. If a mapping failure occurs, an error is logged.

Application property

The application property *curam.workspaceservices.application.processing.logging.on* increases the level of detail of error messages.

When *curam.workspaceservices.application.processing.logging.on* is set to *true*, detailed error messages are written to the application log files if the submission process fails.

Error codes

Each error message is prepended with an error code. These error codes help to automatically scan application logs so that unexpected failures can be identified. The error codes that are returned by the application is defined in the code table file `CT_ApplicationProcessingError.ctx`.

The range of codes that are reserved for internal processing is **APROCER001 – APROCER500**. Customers can use the range **APROCER501 – APROCER999** to log errors in custom processing, for example error codes for extension-mapping handler class.

The list of error codes that are returned by the application, and a brief description of the problem, is listed in Table 1.

Table 14: Application error codes

Code	Description
APROCER001	An error occurred creating a person.
APROCER002	An error occurred creating a prospect person.
APROCER003	A relationship error occurred creating a person.
APROCER004	An error occurred creating a case.
APROCER005	An error occurred while performing a "map-attribute" mapping.
APROCER006	An error occurred while performing a "set-attribute" mapping.
APROCER007	An error occurred while performing a "map-address" mapping.
APROCER008	General mapping failure.
APROCER009	Error creating evidence.
APROCER010	More than one PDF form is registered against the program type.
APROCER011	Error setting the alternate id type for a Prospect Person.
APROCER012	Invalid alternate ID value.
APROCER013	Error the Evidence Application Builder has not been correctly configured.
APROCER014	Evidence type not listed in the Mapping Configuration.
APROCER015	No parent evidence entity found.
APROCER016	An error occurred when trying to unmarshal the application XML.
APROCER017	An error occurred when trying to set a field value.

Table 14: Application error codes (continued)	
Code	**Description**
APROCER018	An error occurred when trying to create the PDF document.
APROCER019	An error occurred when trying to create the PDF document. A form code could not be mapped to a codetable description.
APROCER020	An error occurred when trying a WorkspaceServices mapping extension handler.
APROCER021	Missing source attribute in datastore entity.
APROCER022	An attribute in an expression is not valid.
APROCER023	Application builder configuration error.
APROCER024	Failed creating *DataStoreMappingConfig*, no name specified.
APROCER025	Failed creating *DataStoreMappingConfig*, the name is not unique.
APROCER026	The mapping to datastore had to be abandoned because the schema is not registered.
APROCER027	There was a problem parsing the Mapping Specification.
APROCER028	General mapping error. Mapping XML included.
APROCER029	Cannot have multiple primary participants.
APROCER030	No programs have been applied for.
APROCER031	An error occurred while attempting to map to Person data.
APROCER032	An error occurred while attempting to map to Relationship data.
APROCER033	An error occurred while creating Cases.
APROCER034	An error occurred while creating evidence.
APROCER035	No programs have been applied for.
APROCER036	An error occurred reading data from the datastore.
APROCER037	Specified integrated case type does not exist.
APROCER038	Specified case type does not exist
APROCER039	Duplicate SSN entered for prospect person.
APROCER040	Duplicate SSN entered.
APROCER041	There was a problem with the workflow process.
APROCER042	No primary participant has been identified as part of the intake process.

Customizing submitted applications

7.0.3.0

Use customization points, for example, customizing the generic PDF for processed applications, to customize the application intake process when an intake application is submitted.

Customizing the intake application workflow

7.0.3.0

View a summary of the intake application workflow in a flowchart.

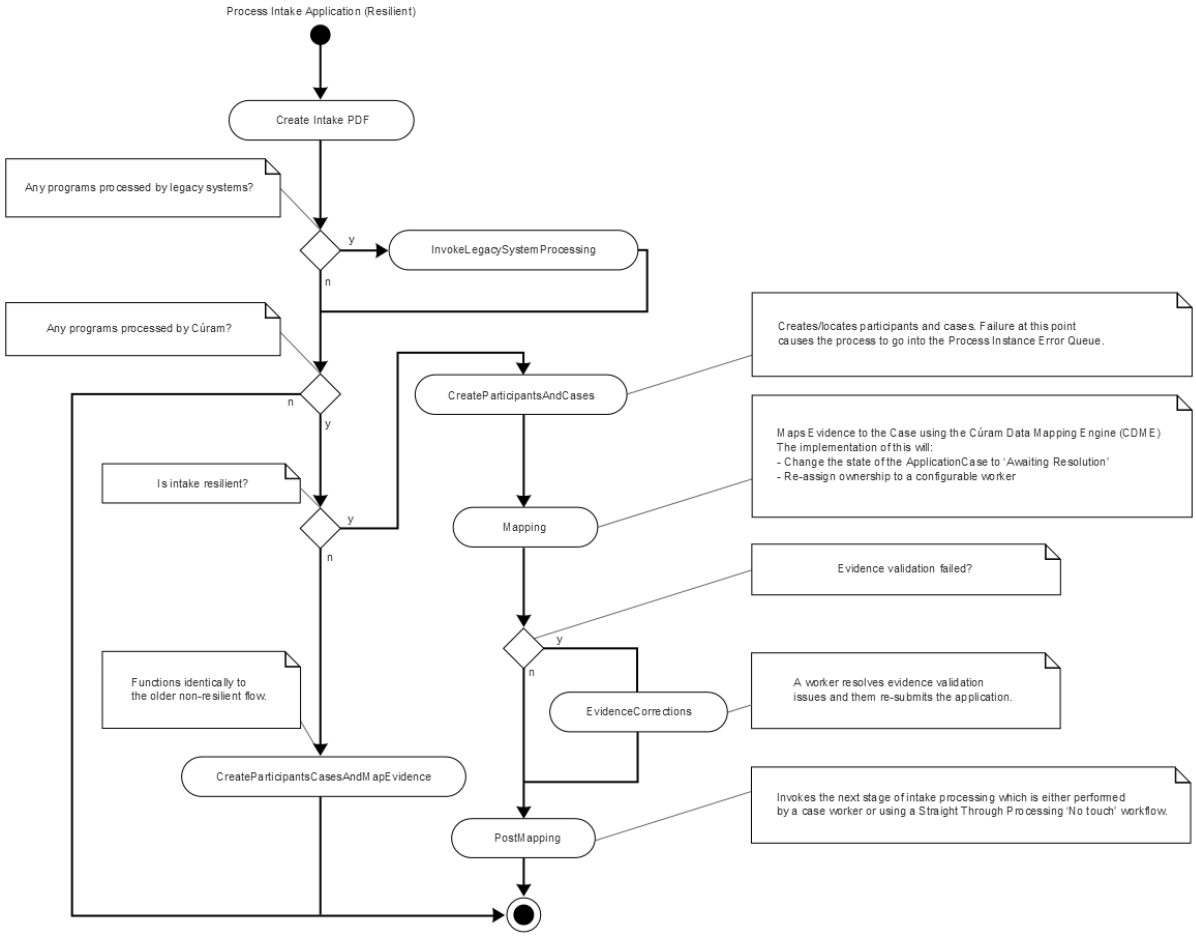


Figure 4: Intake application workflow

Create intake PDF

This automatic activity creates a PDF document based on the content of the application. For more information, see *Customizing the generic PDF for processed applications*.

InvokeLegacySystemProcessing

This automatic activity sends applications to legacy systems via Web Services. This path is taken only if there are legacy systems associated with at least one of the programs on the application.

CreateParticipantsAndCases

This automatic activity creates participants for the submitted application and then creates a case or cases for the various programs associated with the application. In most cases, an Application Case or Cases are created. This path is taken if the value of the configuration property `curam.intake.use.resilience` is set to true. For reasons of backward compatibility, this property is set to false by default, however it is strongly recommended that all production systems set this value to true. For more information on the implications of setting this value to true, see *Using events to extend intake application processing*.

Mapping

This automatic activity uses the Cúram Data Mapping Engine (CDME) to map data collected in the application script into Case Evidence. Under most circumstances this will proceed smoothly. In the event that a validation issue occurs with the mapped evidence, this activity will be automatically re-tried. During the re-try, if there is a single Application Case, the validations will be disabled and a WDO flag `IntakeCaseDetails.mappingValidInd` set to false.

EvidenceCorrections
This manual task is invoked if the Mapping activity failed due to a validation error (`IntakeCaseDetails.mappingValidInd` set to false). The assignment of this task is configurable. For more information, see *Evidence issues intake strategy*. The caseworker or operator will resolve the evidence validation issues and then re-submit the application.

PostMapping
This automatic activity kicks off the next stage of application processing by invoking the event `IntakeApplication.IntakeApplicationEvents.postMapDataToCuram()`.

CreateParticipantsCasesAndMapEvidence
This path is followed when the configuration property `curam.intake.use.resilience` is set to false. This automatic activity behaves identically to the old, non-resilient workflow. It creates cases and participants and performs all evidence mapping in a single transaction. This makes the process less resilient in the event of a failure.

Customers can customize the workflow in the usual recommended manner as described in the `Cúram Development Compliance Guide` and `Cúram Workflow Management System Guide`. Note that customers should not make any changes to the enactment structs used by these workflows.

Related concepts

Customizing the generic PDF for processed applications
Use IBM Cúram Universal Access to map all intake applications to a generic PDF that records the values of all the information that the user enters.

Using events to extend intake application processing
The interface `IntakeApplication.IntakeApplicationEvents` contains events that are invoked when citizens submit an intake application for processing.

Related information

Evidence Issues Ownership Strategy

Customizing the generic PDF for processed applications

7.0.3.0

Use IBM Cúram Universal Access to map all intake applications to a generic PDF that records the values of all the information that the user enters.

This PDF is rendered by the XML Server. Customers can override the default formatting of the generic PDF as follows:

1. Copy `CURAM_DIR/EJBServer/components/Workspaceservices/Data_Manager/InitialData/XSLTEMPLATEINST.dmx` to `CURAM_DIR/EJBServer/components/custom/Data_Manager/InitialData`.
2. Edit `project\config\datamanager_config.xml`, replace the entry for:`CURAM_DIR/EJBServer/components/Workspaceservices/Data_Manager/InitialData/XSLTEMPLATEINST.dmx` with an entry for: `CURAM_DIR/EJBServer/components/custom/Data_Manager/InitialData/ XSLTEMPLATEINST.dmx`
3. Copy `CURAM_DIR/EJBServer/components/Workspaceservices/Data_Manager/InitialData/blob/WSXSLTEMPLATEINST001` to: `CURAM_DIR/EJBServer/components/custom/Data_Manager/InitialData/blob.`
4. Edit `WSXSLTEMPLATEINST001` to suit the needs of the project.

Using events to extend intake application processing

7.0.3.0

The interface `IntakeApplication.IntakeApplicationEvents` contains events that are invoked when citizens submit an intake application for processing.

Use these events to change the way that intake applications are handled, for example supplement or replace the standard CDME mapping or perform an action after an application has been sent to a remote system using web services. For more information, see the API Javadoc information for `IntakeApplication.IntakeApplicationEvents` in `<CURAM_DIR>/EJBServer/components/WorkspaceServices/doc`.

The interface `IntakeProgramApplication.IntakeProgramApplicationEvents` contains events that are invoked at key stages during the processing of an application for a particular program. For information, see the API Javadoc information for `IntakeProgramApplication.IntakeProgramApplicationEvents` in `<CURAM_DIR>/EJBServer/components/WorkspaceServices/doc`.

Note: As of release 6.0.5.5, there is a change to the ordering of the `IntakeApplication.IntakeApplicationEvents.preMapDataToCuram()` and `postMapDataToCuram()` events within the Intake Application Workflow when the configuration property `curam.intake.use.resilience` is set to true. When this property is set to true, `IntakeApplication.IntakeApplicationEvents.preMapDataToCuram()` is called in the Mapping activity prior to Evidence mapping. This means that the `IntakeApplication.IntakeApplicationEvents.preMapDataToCuram()` event is called after the cases and participants have been created by the CreateParticipantsAndCases activity. Previous versions of the intake process invoked this event prior to participant and case creation. When the configuration property `curam.intake.use.resilience` is set to true, the `IntakeApplication.IntakeApplicationEvents.postMapDataToCuram()` event is fired in the PostMapping activity.

Customizing the concern role mapping process

7.0.3.0

The `curam.workspaceservices.applicationprocessing.impl` package contains a ConcernRoleMappingStrategy API that provides a customization point into the online application process.

Use the ConcernRoleMappingStrategy API to implement custom behavior following the creation of each new concern role that is added to an application. For example, customers who have customized the prospect person entity might want to store information on that entity that cannot be mapped using the default CDME processing.

Enable the ConcernRoleMappingStrategy API

7.0.3.0

In the administration application, enable the ConcernRoleMappingStrategy API by setting the Enable Custom Concern Role Mapping property to true.

Procedure

1. Log in to the System Administration application as a user with system administration permissions.
2. Click **System Configurations** > **Application Data** > **Property Administration**.
3. In the **Application - Intake Settings** category.
4. Search for the property *curam.intake.enableCustomConcernRoleMapping*.
5. Edit the property to set its value to true.
6. Save the property.
7. Select **Publish**.

Use the ConcernRoleMappingStrategy API

7.0.3.0

When enabled, use the ConcernRoleMappingStrategy API to implement a strategy for mapping information to a custom concern role.

About this task

The `curam.workspaceservices.applicationprocessing.impl` package contains the ConcernRoleMappingStrategy API.

Procedure

1. Provide an implementation of the customization point.

2. Bind your custom implementation by creating or extending your custom mapping module as follows:

```
package com.myorg.custom;
class MyModule extends AbstractModule {
  @Override
  protected void configure() {

      bind(ConcernRoleMappingStrategy.class).to(
          MyCustomConcernRoleMapping.class);
```

3. If you did not already add your MyModule class to the ModuleClassName table by using an appropriate DMX file, add your MyModule class.

How to send applications to remote systems for processing

7.0.3.0

Use the Citizen Workspace to send applications to remote systems that use web services for processing.

An event `ReceiveApplicationEvents.receiveApplication` is raised before the application is sent to the remote system. The event can be used to edit the contents of the data store that is used to gather application data before transmission. For more information, refer to the API Javadoc for `ReceiveApplicationEvents`, which is in `<CURAM_DIR>/EJBServer/components/WorkspaceServices/doc`.

Customizing the Citizen Account

7.0.3.0

Users can use the Citizen Account to log in to a secure area where users can screen and apply for programs.

Users also use the Citizen Account to view information relevant to them, including individually tailored messages, system-wide announcements, updates on their payments, contact information for agency staff and outreach campaigns that might be relevant to them. The Citizen Account also provides a framework for customers to build their own pages or override the existing pages.

A technical overview of the Citizen Account

7.0.3.0

The Citizen Account framework is defined in the User Interface Metadata (UIM). By using the UIM, customers can override existing pages, add their own pages, and customize the navigation of the framework as users can customize the caseworker application.

The Citizen Account is built on the user interface infrastructure. It uses only a subset of the user interface and navigation components that are offered by the infrastructure to achieve a simple, usable application that citizens can understand and use without any specific training.

Linked users perform the online application by using their account. The Citizen Account includes UIM pages that are a view onto the online application functions. These pages are not configurable or customizable: the functions that they offer are configurable by using administration as specified in the documentation for these areas. The UIM pages that are related to triage, screening, and the online application are not to be modified or overridden.

Security and the Citizen Account

7.0.3.0

Security must be a primary concern when you customize the citizen account customizations. All public-facing applications must be analyzed and tested before they are deployed. Users must contact IBM support to discuss unusual customizations that might have specific security issues.

Permission to call the server facade methods that serve data to citizen account pages is managed by the standard authorization model. For more information, see the *Server Developer* documentation. In addition to the standard authorization checks, each facade method that is called by a **Citizen Account** page must complete the following security checks to ensure the user who is associated with the transaction (the currently logged in user) has permission to access the data they are requesting:

- Ensure that the currently logged in user is of the correct type. They must be an external user with an `applicationCode` of `CITWSAPP`, and have an account of type `Linked`.
- Ensure that the currently logged in user has permission to access the specific records that they are reading. For instance, validate any page parameters that are passed in to ensure that the records requested are related to the currently logged in user in some way.

Ensure that the currently logged in user is the correct type

7.0.3.0

The `curam.citizenaccount.security.impl.CitizenAccountSecurity` API offers a method `performDefaultSecurityChecks` that ensures that the user is the correct type. This method checks the user type, and if not acceptable, writes a message to the logs and fails the transaction.

Note: This API needs to be called in the first line of every custom facade method before any processing or further validation takes place:

```
public CitizenPaymentInstDetailsList listCitizenPayments()
    throws AppException, InformationalException {

    // perform security checks
    citizenAccountSecurity.performDefaultSecurityChecks();

    // validate any page parameters (none in this case)

    // invoke business logic
    return citizenPayments.listPayments();
  }
```

Ensure that the logged in user has access to the requested records

7.0.3.0

A malicious user who is logged in to a valid linked account might send requests to the system to request other users' data. To prevent this intrusion from happening, all page parameters must be validated to ensure that they are somehow traceable back to the currently logged in user. How this conclusion is determined is different for each type of record.

For example, a **Payment** can be traced back to the **Participant** by way of the **Case** on which it was entered.

The `curam.citizenaccount.security.impl.CitizenAccountSecurity` application programming interface (API) offers methods to complete these checks for the types of records that are served to citizens by the initially configured pages. For specific information, review the Javadoc of this API. For custom pages that serve different types of data, additional checks must be implemented to validate the page parameters.

This process needs to be added to a custom security API and called by the facade methods in question. The methods need to check to see whether the record requested can be traced back to the currently logged in user, and if not, it needs to log the user name, method name, and other data. If these conditions are not met, the transaction needs to be failed immediately (as opposed to adding the issue to the validation helper and allowing the transaction to proceed):

```
if (paymentInstrument.getConcernRole().getID()
   != citizenWorkspaceAccountManager
     .getLoggedInUserConcernRoleID().getID()) {

 /**
 * the payment instrument passed in is not related
 * to the logged in user log the user name of the
 * current user, the method invoked and any other
 * pertinent data
 */

 // throw a generic message
 throw PUBLICUSERSECURITYExceptionCreator
   .ERR_CITIZEN_WORKSPACE_UNAUTHORISED_METHOD_INVOKATION();
 }
```

While as much information as possible regarding the infraction needs to be logged, it is important to ensure that the exceptions thrown do not display any information that might be useful to malicious users.

A generic exception needs to be thrown that does not contain any information that relates to what went wrong. The `curam.citizenaccount.security.impl.CitizenAccountSecurity` API throws a generic message that states `You are not privileged to access this page`.

Messages

7.0.3.0

When a linked citizen logs in, messages are gathered from the system and from remote systems for display.

The `curam.citizenmessages.impl.CitizenMessageController` API gathers and displays messages. The API reads persisted messages by participant from the `ParticipantMessage` database table, and also raises the `CitizenMessagesEvent.userRequestsMessages` event, inviting listeners to add messages to a list it passes as part of the event parameter. The messages that are gathered from each source are sorted, turned into XML and returned to the citizen for display.

Configuring citizen messages

7.0.3.0

Global configurations are included that can be specified for **Citizen Messages**, such as enabling certain types and configuring their display order. The different types of messages also include their own configuration points. Specific information about how to customize the various message types is provided later.

The textual content of a message type also can be configured. Each message type has a related properties file that includes the localizable text entries for the various messages displayed for that type. These properties also include placeholders that are substituted for real values related to the citizen at run time.

The wording of this text can be customized, by inserting a different version of the properties file into the resource store. The following table defines which properties file need to be changed for each type of message:

Table 15: Message properties files

Message type	Property file name
Payments	`CitizenMessageMyPayments.properties`
Application Acknowledgment	`CitizenMessageApplicationAcknowledgement.properties`
Verifications	`CitizenMessageVerificationMessages.properties`
Meetings	`CitizenMessageMeetingMessages.properties`
Referral	`CitizenMessagesReferral.properties`
Service Delivery	`CitizenMessagesServiceDelivery.properties`

You can also remove placeholders (which are populated with live data at run time) from the properties. However, there is currently no means to add further placeholders to existing messages. A custom type of message must be implemented in this situation.

Adding a new type of citizen message

7.0.3.0

Messages are gathered by the controller in two ways: the controller reads messages that were persisted to the database by using the `curam.citizenmessages.persistence.impl.ParticipantMessage` API, and also gathers them by raising the `curam.participantmessages.events.impl.CitizenMessagesEvent`

A decision needs to be made regarding whether to 'push' the messages to the database, or else have them generated dynamically by a listener that listens for the event that is raised when the citizen logs in. The specific requirements of the message type need to be considered, along with the benefits and drawbacks of each option.

Persisted messages

In this scenario, when something takes place in the system that might be of interest to the citizen, a message is persisted to the database. For example, when a meeting invitation is created, an event is fired. The initially configured meeting messages function listens for this event. If the meeting invitee is a participant with a linked account, a message is written to the `ParticipantMessage` table that informs the citizen that they are invited to the meeting.

One benefit of this approach is that little processing is done when the citizen logs in to see this message: the message is read from the database and displayed, as opposed to calculation that takes place that would determine whether the message was required. However, the implementation also needs to handle any changes to the underlying data that might invalidate or change the message, and take appropriate action.

For example, the meeting message function also listens for changes to meetings to ensure the meeting time, location, and similar, are up to date, and to send a new message to the citizen to inform the citizen that the location or time was changed.

Dynamic messages

These messages are generated when the citizen logs in, by event listeners that listen for the `curam.participantmessages.events.impl.CitizenMessagesEvent.userRequestsMessages` event.

Because the message is generated at runtime, code is not required to manage change over time. The message is generated based on the data within the system each time the citizen logs in. If some underlying data changes, the next time the citizen logs in, they will get the correct message.

A drawback to this approach is that significant processing might be required at run time to generate the message. Care must be taken to ensure that this processing does not adversely affect the load time of the **Citizen Account** dashboard.

Performance considerations must be evaluated against the requirements of the specific message type and the effort that is required to manage change to the data that the message is related to over time. For example, the initially configured verification message is dynamic. When a citizen logs in, it checks to see whether any outstanding verifications exist for that citizen. This process is a relatively simple database read, whereas it would be complicated to listen for various events in the Verification Engine and ensure that an up-to-date message was stored in the database related to the participants' outstanding verifications. Alternatively, the meeting messages need to inform the citizen of changes to their meetings, so functionality had to be written to manage changes to the meeting record and its related message over time.

Implementing a new message type

7.0.3.0

To implement a new message type, regardless of whether the message will be persisted or generated dynamically, take the following steps:

Common Tasks

- Add a new entry to the `CT_ParticipantMessageType` codetable to represent the new message type. This will be used in administration to configure the new message type.
- Add a DMX entry for the ParticipantMessageConfig database table. This will store the type and sort order of the new message type and is used for administration. For example:

```
<row>
   <attribute name="PARTICIPANTMESSAGECONFIGID">
     <value>2110</value>
   </attribute>
   <attribute name="PARTICIPANTMESSAGETYPE">
     <value>PMT2001</value>
   </attribute>
   <attribute name="ENABLEDIND">
     <value>1</value>
   </attribute>
```

```
    <attribute name="SORTORDER">
      <value>5</value>
    </attribute>
    <attribute name="VERSIONNO">
      <value>1</value>
    </attribute>
  </row>
```

- Add a properties file to the App Resource store that contains the text properties and image reference for the message.
- Add an image for this message type to the resource store.

Implementing a dynamic message

In order to implement a dynamic style message, an event listener needs to be implemented, to listen for the `CitzenMessagesEvent.userRequestsMessages` event. This event argument contains a reference to the Participant and a list, to which the listener will add `curam.participantmessages.impl.ParticipantMessage` Java™ objects. For further details please consult the Javadoc API for `CitzenMessagesEvent`. This can be found in `<CURAM_DIR>/EJBServer/components/core/doc`

Developers should also refer to the Javadoc API for `curam.participantmessages.impl.ParticipantMessage` and `curam.participantmessages.impl.ParticipantMessages` for a full explanation.

The message text is stored in a properties file in the resource store. A dynamic listener will retrieve the relevant properties from the resource store, and create the ParticipantMessage object accordingly. The message text for a given message can include placeholders. Values for placeholders are added to ParticipantMessage objects as parameters. The CitizenMessagesController will resolve these placeholders, replacing them with the real values related to the participant in question that have been added as parameters to the message object.

Take for example this entry from the CitizenMessageMyPayment.properties file:

```
Message.First.Payment=
  Your next payment is due on {Payment.Due.Date}
```

The actual payment due date of the payment in question will be added to the ParticipantMessage object as a parameter (see example code below). The CitizenMessagesController then resolves the placeholders, populating the text with real values, and then turns the message into XML that is rendered on the citizen account (there is also a public CitizenMessageController method that will return all messages for a citizen as a list, please see the Javadoc information).

`From curam.participantmessages.impl.ParticipantMessage API:`

```
/**
 * Adds a parameter to the map. The paramReference
 * should be present in the message title or body so
 * it can be replaced by the paramValue before the message
 * is displayed.
 *
 * @param paramReference
 * a string place holder that is present in either the
 * message title or body. Used to indicate where the value
 * parameter should be positioned in a message.

 * @param paramValue
 * the value to be substituted in place of the place holder
 */
 public void addParameter(final String paramReference,
   final String paramValue) {

   parameters.put(paramReference, paramValue);
 }
```

The call to the method would look like this:

```
participantMessage.addParameter("Payment.Due.Date", "1/1/2011");
```

Messages can also include links. Similarly to placeholders, links are resolved at runtime. Links can use placeholder values as the text to be displayed for that link. A link is defined in a properties file as such:

```
Click {link:here:paymentDetails} to view the payment details.
```

In this example, "here" is the text to display, and "paymentDetails" refers to the name of the link that is to be inserted at that point in the text. Please see the Advisor Developer's Guide for more information. In order for a dynamic listener to populate this link with a target, it would create a curam.participantmessages.impl.ParticipantMessageLink object, specifying a target and a name for the link. The code would look like this:

```
ParicipantMessageLink participantMessageLink =
     new ParticipantMessageLink(false,
       "CitizenAccount_listPayments", "paymentDetails");

   participantMessage.addLink(participantMessageLink);
```

Before composing the message, the dynamic listener must check to ensure that the message type in question is currently enabled. The curam.participantmessages.configuration.impl.ParticipantMessageConfiguration record for that message type should be read, and the isEnabled method used to determine if this message type is enabled. If not, no further processing should occur.

* It is recommended to separate the code that listens for the event and the code that composes a specific message, in order to adhere to the philosophy of "doing one thing and doing it well".

Implementing a persisted message

In order to have a persisted message displayed to the citizen, it must be written to the database via the curam.citizenmessages.persistence.impl.ParticipantMessage API. Message arguments are handled by persisting a curam.advisor.impl.Parameter record and associating it with the ParticipantMessage record, and links by the curam.advisor.impl.Link API. Parameter names should map to placeholders contained within the message text. Link names should relate to the names of links specified in the message text. Please refer to the Javadoc information of curam.citizenmessages.persistence.impl.ParticipantMessage, curam.advisor.impl.Parameter and curam.advisor.impl.Link for more.

An expiry date time must be specified for each ParticipantMessage. After this date time, the message will no longer be displayed.

Messages can be removed from the database. If a message needs to be replaced with a modified version, or removed for another reason, this can be done via the curam.citizenmessages.persistence.impl.ParticipantMessage API.

Each message has a related ID and type. This is used to track the record that the message is related to. For example, meeting messages will store the Activity ID and a type of "Meeting". Messages can be read by participant, related ID and type via the ParticipantMessageDA0.

Before persisting the message, the dynamic listener must check to ensure that the message type in question is currently enabled. The curam.participantmessages.configuration.impl.ParticipantMessageConfiguration record for that message type should be read, and the isEnabled method used to determine if this message type is enabled. If not, no further processing should occur.

Customizing specific message types

7.0.3.0

You can customize the default message types in various ways.

Referral message

This message type creates messages related to referrals. This is a dynamic message. When the citizen logs in, a message will be created for each referral that exists for the citizen in the system, provided that referral has a referral date of today or in the future, and provided that a related Service Offering has been specified for this referral. The properties file EJBServer\components\CitizenWorkspace\data\initial\blob\prop\CitizenMessageReferral.properties contains the properties for the referral message text, message parameters, links and images. This properties file is stored in the resource

store. This resource is registered under the resource name `CitizenMessageReferral`. To change the message text of the message, or to remove placeholders or change links, a new version of this file must be uploaded into the resource store.

Service delivery message

This message type creates messages related to service deliveries. This is a dynamic message. When the citizen logs in, a message will be created for each service delivery that exists for the citizen in the system, provided that service delivery has a status of 'In Progress' or 'Not Started'. The properties file `EJBServer\components\CitizenWorkspace\data\initial\blob\prop\CitizenMessageServiceDelivery.properties` contains the properties for the service delivery message text, message parameters, links and images. This properties file is stored in the resource store. This resource is registered under the resource name `CitizenMessageServiceDelivery`. To change the message text of the message, or to remove placeholders or change links, a new version of this file must be uploaded into the resource store.

Payment messages

7.0.3.0

This message type creates messages based on the payments issued, canceled, an so on, for a citizen. These messages are persisted to the database. They replace each other, for example, if a payment is issued and then canceled, the payment issued message will be replaced with a payment canceled message. The properties file `EJBServer\components\CitizenWorkspace\data\initial\blob\prop\CitizenMessageMyPayments.properties` contains the properties for financial message text, message parameters, links and images. This properties file is stored in the resource store. This resource is registered under the resource name `CitizenMessageMyPayments`. To change the message text of financial messages, or to remove placeholders or change links, a new version of this file must be uploaded into the resource store. The table below describes the messages created when various events related to payments occur in the system, and the property in `CitizenMessageMyPayments.properties` that relates to each message created.

Table 16: Payment messages and related properties

Payment event	Message Property
First payment issued on a case	Message.First.Payment
Latest payment issued	Message.Payment.Latest
Last payment issued	Message.Last.Payment
Payment canceled	Message.Cancelled.Payment
Payment reissued	Message.Reissue.Payment
Payment stopped (case suspended)	Message.Stopped.Payment
Payment / Case unsuspended	Message.Unsuspended.Payment

Customization of the payment messages expiry date

The number of days the payment for which the message will be displayed to the citizen can be configured using a system property. By default the property value is set to 10 days, however, this can be overridden from property administration.

Table 17: Payment message expiry property

Name	Description
curam.citizenaccount.payment.message.expiry.days	The number of days the payment message will be displayed to the participant.

Meeting messages

7.0.3.0

This message type creates messages based on meetings that the citizen is invited to, provided that they are created via the `curam.meetings.sl.impl.Meeting` API. This API raises events that the meeting messages functionality consumes. There are other ways of creating Activity records without this API, but meetings created in these ways will not have related messages created as the events will not be raised. These messages are persisted to the database. They replace each other, for example, if a meeting is scheduled and then the location is changed, the initial invitation message will be replaced with one informing the citizen of the location change. The properties file `EJBServer\components\CitizenWorkspace\data\initial\blob\prop\CitizenMessageMeetingMessages.properties` contains the properties for the meeting messages text, message parameters, links and images. This properties file is stored in the resource store. This resource is registered under the resource name `CitizenMessageMeetingMessages`. To change the message text of meeting messages, or to remove placeholders or change links, a new version of this file must be uploaded into the resource store. The table below describes the messages created when various events related to meetings occur in the system, and the properties in `CitizenMessageMeetingMessages.properties` that relates to each message created. Different versions of the message text are displayed depending on whether the meeting is an all day meeting, whether a location has been specified, and whether the meeting organizer has contact details registered in the system. Accordingly, the property values in this table are approximations that relate to a range of properties within the properties file. Please refer to the properties file for a full list of the message properties.

Table 18: Meeting messages

Meeting event	Message Properties
Meeting invitation	Non.Allday.Meeting.Invitation.*, Allday.Meeting.Invitation.*
Meeting update	Non.Allday.Meeting.Update.*, Allday.Meeting.Update.*
Meeting canceled	Allday.Meeting.Update.*, Allday.Meeting.Cancellation.*

Customization of the meeting messages display date

The number of days before the meeting start date that the message should be displayed to the citizen can be configured using a system property. By default the property value is set to 10 days, however, this can be overridden from property administration.

The meeting message expires (i.e. it is no longer displayed to the citizen) at the end of the meeting, i.e. the date time at which the meeting is scheduled to end.

Table 19: Meeting message display date property

Name	Description
curam.citizenaccount.meeting.message.effective.days	The number of days before the meeting start date that the message should be displayed to the citizen.

Application acknowledgment message

7.0.3.0

This message type creates a message when an application is submitted by a citizen. This message is persisted to the database. The properties file `EJBServer\components\CitizenWorkspace\data\initial\blob\prop\CitizenMessageApplicationAcknowledgment.properties` contains the properties for the messages text, message parameters, links and images. This properties file is stored in the resource store. This resource is registered under the resource name `CitizenMessageApplicationAcknowledgment`. To change the message text of the message, or to remove placeholders or change links, a new version of this file must be uploaded into the resource store.

Customization of application acknowledgment message expiry date

The number of days the Application Acknowledgment message will be displayed to the citizen can be configured using a system property. By default the property value is set to 10 days, however, this can be overridden from property administration.

Table 20: Application acknowledgment message expiry property

Name	Description
curam.citizenaccount. intake.application.acknowledgement.message.expiry.days	The number of days the application acknowledgment message will be displayed to the participant.

Web services

7.0.3.0

In some scenarios, agencies handle interactions with citizens over the Internet, but use an existing legacy system for case processing. To cater for these scenarios, Universal Access can be configured to communicate with various remote systems using web services.

Inbound and outbound web services

7.0.3.0

The following outbound web services are supported:

- Send an application for benefits.
- Withdraw an application for benefits.
- Send a life event.

The following inbound web services are supported:

- Create a citizen account on Universal Access.
- Link a user to a remote system (gives them the right to send information to those systems and receive information from them in turn).
- Unlink a user from a remote system.
- Receive an update to the status of a submitted application.
- Receive an update to the status of a request to withdraw an application.
- Receive a citizen message (for display on a citizen account).
- Receive payment information.
- Receive case contact information.

Web services security

7.0.3.0

Connections to remote systems can be configured through the remote systems configuration page in the administrator application.

Remote systems can invoke web services on Universal Access and must supply user name and password credentials as part of the SOAP header, details of how to do this are described using sample web service requests. It is strongly recommended that a different username and password be assigned to each remote system. The username associated with a remote system is set in the Source User Name field of the remote system configuration page. Having a different user name for each remote system allows Universal Access to perform proper data-based security checks on the incoming service requests. This prevents one remote system sending requests to update data that is properly the concern of a different remote system.

Process application service

7.0.3.0

The process application service web services.

Receive application

7.0.3.0

When the *Receive application* outbound web service is started on remote systems, it communicates an application for benefits for one or more social programs. The Web Service Description Language (WSDL) describing this service can be found in <CURAM_DIR>\EJBServer\components\WorkspaceServices\axis\ProcessApplicationService\ProcessApplicationService.wsdl.

A web service request of this type contains the following information:

- intakeApplicationType - An ID that uniquely identifies an Intake Application Type.
- applicationReference – A unique reference for a particular application. This reference is a human-readable ID that is displayed to citizens after they complete an application; for example, 512 or 756. The application reference is used as an argument to other web services and needs to be stored by the receiver.
- applicationLocale – Denotes the preferred locale of the user who entered the application, for example en_US. This information needs to be stored by the receiver. Remote systems can send various information back to the citizen's account. Some of this information must be localized by the sender to the preferred locale of the citizen.
- submittedDateTime – The date and time at which the application was submitted. This information is in XML schema dateTime format, for example, 2012-05-29T15:34:49.000+01:00.
- programsAppliedFor – This field contains a list of the programs that were applied for as part of this application. Each program is referred to by a unique reference. This information corresponds to the value of the Reference field configured in the Programs section of Universal Access configuration. For example:

```
<ns1:programsAppliedFor>
    <ns1:programTypeReference>CashAssistance</ns1:programTypeReference>
    <ns1:programTypeReference>SNAP</ns1:programTypeReference>
</ns1:programsAppliedFor>
```

- applicationData – Contains a base64 encoded representation of the intake data. This intake data is the XML representation of the XML data store associated with an application.
- applicationSchemaName – The name of the schema that is used to create the data store for the application.
- senderIdentification – Identifies the sender of the request. The sender identification contains two parts, 1) the identifier of the system from which the request originates, 2) The Citizen Workspace Account ID of the user that created the request. The second part is optional, applications submitted anonymously do not contain part two but applications that are submitted by a logged in user do.
- supplementaryInformation – optional, reserved for future use.

The receiver of this information is expected to record the details of the application keyed against sender identification and intake application reference.

On success, the implementation of this web service must return the Boolean value true to indicate that the request was processed successfully. In the case that a problem occurs in processing the request, a fault must be returned containing a string to indicate the nature of the problem. The String needs to be localized to the locale of Universal Access server since it appears in the server log files.

Note: The receiver can receive multiple applications with the same Intake Application reference but the intake application reference is always unique for a particular sender. For example, Systems A and B send a receiveApplication() request to system X. Both requests have the applicationReference 256.

Note: The receiver never should receive two applications from A with an application reference of 256.

Receive withdrawal request

7.0.3.0

IBM Cúram Universal Access invokes this outbound web service on remote systems. It is used by citizens to withdraw an application that they have previously submitted using the Receive Application Service. WSDL describing this service can be found in <CURAM_DIR>\EJBServer\components

\WorkspaceServices\axis\ProcessApplicationService \ProcessApplicationService.wsdl. A web service request of this type contains the following information:

- applicationReference – A unique reference for the application to be withdrawn. This refers to the id transmitted with the Receive Application service request.
- programTypeReference – A reference that identifies the program being withdrawn. Each program type is referred to by a unique reference. This corresponds to the value of the Reference field configured in the Programs section of IBM Cúram Universal Access configuration. For example "CashAssistance".
- requestSubmittedDateTime – A timestamp indicating when the request was submitted in XML Schema dateTime format. For example, 2012-05-29T15:34:49.000+01:00
- withdrawalRequestReason – The value is taken from the code table WithdrawalRequestReason. Values for this code table are
  - WRES1001 – Attained employment
  - WRES1002 – Change of circumstances
  - WRES1003 – Filed in error
- withdrawalRequestID – An id that uniquely identifies this withdrawal request from the sending instance of Universal Access.
- senderIdentification – Identifies the sender of the request. The sender identification contains two parts, 1) the identifier of the system from which the request originates, 2) The Citizen Workspace Account ID of the user that created the request.
- supplementaryInformation – optional, reserved for future use.

The expected result following successful processing is a receiveWithdrawalRequestResponse as follows:

```
<receiveWithdrawalRequestResponse>
  <result>true</result>
</receiveWithdrawalRequestResponse>
```

The service implementation should return a fault if there is an error processing the request. The fault string should be globalized to the locale of the IBM Cúram Universal Access server since it will appear in the server log files. Some problems that may arise include:

- A withdrawal request with the given ID has already been sent by the given instance of Universal Access.
- The application reference referred to is not recognized as an application previously transmitted in a Receive Application service invocation from the same Universal Access instance.

The withdrawal request application is processed by the receiving agency after which a response should be sent in the form of a withdrawal request update. See the sample SOAP request for this web service.

Update Application Service

7.0.3.0

The Update Application Service web services.

Intake program application update

7.0.3.0

An inbound web service invoked by remote systems on IBM Cúram Universal Access. It is used to inform Universal Access of changes to the status of an application for benefits that was previously received via the Receive Application web service. The status of an application can transition to Approved, Denied or Withdrawn. Where an application is denied a reason can be included in the web service message. The schema for the payload of web service requests of this type can be found in <CURAM_DIR>\EJBServer \components\WorkspaceServices\webservices\UpdateApplication.xsd. See the sample SOAP request for this web service.

A web service request of this type contains the following information:

- curamReferenceID – This must match the applicationReference element for the corresponding Receive Application request.

- programApplicationStatus – This can take the following values:
  - IPAS1002 – Withdrawn
  - IPAS1003 – Approved
  - IPAS1004 – Denied
- programApplicationDisposedDateTime – This is a formatted date time string in the standard IBM Cúram ISO8601 format – "YYYYMMDD HH:MM:SS".
- programApplicationDenialReason – Optional, if the status sent is IPAS1004, this contains free text describing the reason for denial. The denial reason should be taken from the code table IBM Cúram IntakeProgApplDenyReason.

The web service request needs to be sent with a Cúram security credential (see a sample SOAP message for details). The user name placed within the credential must match the Source User Name entered into the Remote System entry corresponding to the peer system sending the request.

Withdrawal Request Update

7.0.3.0

An inbound web service invoked by remote systems on IBM Cúram Universal Access. It is used to inform Universal Access of changes to the status of a Withdrawal Request that was previously submitted using the Receive Withdrawal Request web service. You can find the schema for the payload of web service requests of this type in <CURAM_DIR>\EJBServer\components\WorkspaceServices\webservices\UpdateApplication.xsd. See the sample SOAP request for this web service.

A web service request of this type contains the following information:

- curamReferenceID – This must match the withdrawalRequestID in the corresponding Receive Withdrawal Request message.
- withdrawalRequestStatus – This an enumeration taking the following values:
  - WREQ1002 – Approved
  - WREQ1003 – Denied
- resolvedDateTime – A time stamp in the standard IBM Cúram ISO8601 format – "YYYYMMDD HH:MM:SS".
- withdrawalRequestDenialReason – Optional. In the case there the withdrawal request was denied, a textual explanation for the denial. The sender must localize this to the locale of the citizen who originally submitted the application.

See the sample SOAP request for the Withdrawal Request Update operation.

On success this operation returns a document indicating that the request has succeeded. On failure, a fault is raised. Reasons for failure include:

- The withdrawal request id does not match a known withdrawal request id.
- The withdrawal request state transition is invalid.

Life event service

7.0.3.0

This outbound web service is invoked by IBM Cúram Universal Access on remote systems. WSDL describing this service can be found in <CURAM_DIR>\EJBServer\components\WorkspaceServices\axis\LifeEventService\LifeEvent.wsdl.

A request for this web service contains the following fields:

- lifeEventReference – Describes the type of the Life Event, for example "Change of Address"
- senderIdentification – Identifies the sender of the request. The sender identification contains two parts, 1) the identifier of the system from which the request originates, 2) The Citizen Workspace Account ID of the user that created the request.

- lifeEventData - Contains a base64 encoded representation of the Life Event data. This Life Event data is the XML representation of the XML datastore associated with an Life Event.
- lifeEventSchemaName – The name of the schema used to create the data store for the Life Event.
- submittedDateTime – The date and time when the Life Event was submitted. An XML Schema dateTime. For example, 2012-05-29T15:34:49.000+01:00
- supplementaryInformation – optional, reserved for future use.

The implementation should return a response of type lifeEventResponse with the content "true" when the Life Event is successfully processed. If there is an error processing the Life Event then the system should return a fault in accordance with the WSDL specification.

Create account service

7.0.3.0

An inbound web service invoked by remote systems on IBM Cúram Universal Access. The service creates a Citizen Workspace Account for users who previously submitted an Intake Application anonymously. The service performs two functions:

- Create an account for a previously anonymous user.
- Link that account to the remote system that is invoking the Create Account Web Service.

If a Citizen Workspace user is "linked" to a remote system, it means that user is registered on the remote system and the remote system will recognize requests from that Citizen Workspace user as relating to a particular case, cases or an individual on the remote system. This has serious security implications on the remote system – The remote system sending a request to link a user or create an account for a user must be convinced of the identity of the individual who owns the account. The schema for the payload of web service requests of this type can be found in `<CURAM_DIR>\EJBServer\components\WorkspaceServices\webservices\ExternalAccountCreate.xsd`. See the sample SOAP request for this web service.

A create account request contains the following information:

- firstName – The first name.
- middleName – The middle name. Optional.
- surname – The last name.
- username – The username for the newly created account.
- password – The password for the newly created account.
- confirmPassword – Confirmation of the password. Must match password.
- secretQuestionType – The type of secret question selected to unlock the user's account. Values should correspond to entries from the SecretQuestionType code table. For example, SQT1 – Mother's maiden name.
- answer – An answer to the secret question. Non empty.
- termsAndConditionsAccepted – Boolean indication that the citizen has accepted the terms and conditions on which the account is created.
- intakeApplicationReference – Refers to the unique applicationReference passed in as part of the receive application request. If this is specified, a link will be created between the application and the newly created account.
- clientIDOnRemoteSystem – This is a unique identifier that can be used to identify the user of this account on the remote system. There is no prescribed form for this id, it could be a Social Security Number for example. It must be capable of uniquely identifying the citizen on the remote system.
- sourceSystem – Identifies the remote system that sent this request. This must match the name of a remote system configured in the administration application. For more information about configuring remote systems, see *Configuring remote systems*.

If successful this returns the id of the created citizen workspace account. Problems that occur during the processing of the request are flagged by a fault response. Possible issues include:

- An account has already been associated with the intake application reference.
- The username already exists.
- The user name or password do not meet minimum mandatory criteria such as password strength, user name length.

Related concepts

Configuring remote systems

Applications and life events data can be sent through web services for processing by a remote system. To enable remote processing, specify a remote system and the required web services. Remote systems can be configured allowing applications and life event data to be sent to them for processing via associated web services.

Link service

7.0.3.0

This is an inbound web service invoked by remote systems on IBM Cúram Universal Access. It is used to link a Citizen Workspace account to a remote system. See the section on Create Account Service for a general discussion of the implications of linking a user. The schema for the payload of web service requests of this type can be found in `<CURAM_DIR>\EJBServer\components\WorkspaceServices\webservices\ExternalAccountLink.xsd`. See the sample SOAP request for this web service.

This web service request contains the following information:

- sourceSystem – The name of the remote system sending the request. Must match the name of a remote system configured in the system.
- citizenWorkspaceAccountID – The unique citizen workspace account id.
- clientIDOnRemoteSystem - This is a unique identifier that can be used to identify the user of this account on the remote system. There is no prescribed form for this id, it could be a Social Security Number for example. It must be capable of uniquely identifying the client on the remote system.
- createdByUsername – The username on the remote system responsible for this request.

On success this operation returns a document indicating that the request has succeeded. On failure, a fault is raised. Reasons for failure include:

- The citizen workspace account id is invalid, does not exist or is associated with a de-activated account.
- The citizen workspace account in question is already linked to this remote system.

Unlink service

7.0.3.0

An inbound web service invoked by remote systems on IBM Cúram Universal Access. It is used to unlink a Citizen Workspace Account from a remote system. After executing this service it will not be possible for the user of the unlinked account to submit Life Events to this remote system, for example. The schema for the payload of web service requests of this type can be found in `<CURAM_DIR>\EJBServer\components\WorkspaceServices\webservices\ExternalAccountUnlink.xsd`. See the sample SOAP request for this web service.

This web service request contains the following information:

- sourceSystem – The name of the remote system sending the request.
- citizenWorkspaceAccountID – The unique ID of the Citizen Workspace Account being unlinked.

On success this operation returns a document indicating that the request has succeeded. On failure, a fault is raised. Reasons for failure include:

- The indicated account does not exist or is not active.
- The indicated account is not linked to the remote system sending the request.

Citizen message

7.0.3.0

An inbound web service invoked by remote systems on IBM Cúram Universal Access. It is used to send Citizen Messages that are displayed on a user's Home Page when they log in to the Citizen Account. The schema for the payload of web service requests of this type can be found in <CURAM_DIR>\EJBServer\components\WorkspaceServices\webservices\ExternalCitizenMessage.xsd. See the sample SOAP request for this web service.

This web service request contains the following information:

- sourceSystem – The name of the remote system sending the request.
- citizenWorkspaceAccountID – The unique citizen workspace account id.
- cityIndustryType – Denotes the type of industry associated with the message. The values for this element must match codes from the CityIndustry code table.
- relatedID – Refers to the id of an underlying entity in the remote system to which the message refers. For example, if the message concerns a payment then the related ID identifies the ID of the payment within the remote system.
- externalCitizenMessageType – The external citizen message type, taken from the ExternalCitizenMessageType codetable.
- messageTitle – The title of the message. It is the responsibility of the remote system to localize this to the locale of the end user.
- messageBody – The body of the message. It is the responsibility of the remote system to localize this to the locale of the end user.
- effectiveDate – Optional. The date from which the message is effective. It will only be displayed from this date onwards. The date must be in the format – "YYYY-MM-DD". If an effective date is not provided then the current date is taken as the effective date.
- expiryDate – The date that the message is set to expire. Following this date, the message will not be displayed to the user. The date must be in the format – "YYYY-MM-DD".
- priority – A boolean value to indicate whether this message is a high priority.

Some messages are designed such that a newer message can replace an older one. For example, a message is sent concerning a meeting. The time of the meeting changes and a new message is sent with the updated time for the meeting. The citizen does not see both messages, rather the second message replaces the first and only the second message is seen. One external message will automatically replace another external message if the following fields match those of an existing message: sourceSystem, externalCitizenMessageType and relatedID.

Payment service

7.0.3.0

This is an inbound web service invoked by remote systems on IBM Cúram Universal Access. This service is used to transmit information about one or more payments. The schema for the payload of web service requests of this type can be found in <CURAM_DIR>\EJBServer\components\WorkspaceServices\webservices\ExternalPayment.xsd. See the sample SOAP request for this web service.

This web service request can contain one or more Payments. This allows the remote system to batch up payments and send them as a single request for performance reasons. Each payment can relate to an entirely separate citizen account. A single payment may contain a payment breakdown. A payment breakdown may contain one or more payment line items.

A single payment contains the following information:

- paymentID – Together with the source system, this uniquely identifies a payment.
- sourceSystem – The name of the remote system sending the request. Must match the name of a remote system configured in the system.
- citizenWorkspaceAccountID – The unique citizen workspace account id.
- cityIndustryType – Denotes the type of industry associated with the payment. The values for this element must match codes from the CityIndustry code table. Optional.

- paymentAmount – The headline value for the payment as a whole. This payment may optionally be further broken into a number of line items.
- currency – The currency in which the payment was made, contains values from the Currency code table. Optional.
- paymentMethod – The method by which the payment was made, contains values from the MethodOfDelivery code table.
- paymentStatus – The status of the payment, for example cancelled, processed, suspended etc. Contains values from PmtReconciliationStatus code table.
- effectiveDate – The effective date of the payment in the format "YYYY-MM-DD".
- coverPeriodFrom – The start date of the period covered by this payment. In the format "YYYY-MM-DD".
- coverPeriodTo – The end date of the period covered by this payment. In the format "YYYY-MM-DD".
- dueDate – The date that the payment was due to be paid. In the format "YYYY-MM-DD".
- payeeName – The name of the payee for this payment.
- payeeAddress – The address that the payment was sent to (in the case of a cheque). Optional.
- paymentReferenceNo – Uniquely identifies a payment within a given remote system.
- bankSortCode - The sort code of the bank account to which this payment is delivered.
- bankAccountNo – The bank account number to which payment is made.
- A payment may contain a Payment Breakdown (optional).

A Payment Breakdown contains one or more Payment Line Items. A Payment Line Item contains the following information:

- caseName – The human readable name of the case on the remote system with which this payment is associated.
- The case name must be localised to the locale of the citizen. This case name must match the case name displayed on the Contact Information page.
- caseReference – This uniquely identifies the case on a given remote system.
- componentType – This contains a code from the FinComponentType code table.
- debitAmount – The amount debited if this payment was a debit.
- creditAmount – The amount credited if this payment was a credit.
- coverPeriodFrom - The start date of the period covered by this payment. In the format "YYYY-MM-DD".
- coverPeriodTo – The end date of the period covered by this payment. In the format "YYYY-MM-DD".

It is important to note that payments can supersede previously submitted payments. For example, a payment is submitted from TestSystem with paymentID 1234. Subsequently another payment arrives from TestSystem with the same paymentID, 1234. This payment replaces the previous payment. The previous payment is physically removed along with all its related payment line items. A typical example of where this might occur is when a previously issued payment is cancelled.

Contact service

7.0.3.0

An inbound web service invoked by remote systems on IBM Cúram Universal Access. This service is used to update a register of caseworker contact details relating to a remote system. The schema for the payload of web service requests of this type can be found in `<CURAM_DIR>\EJBServer\components\WorkspaceServices\webservices\ExternalContact.xsd`. See the sample SOAP request for this web service.

A contact web service request contains the following information:

- sourceSystem – The name of the remote system sending the request. Must match the name of a remote system configured in the system.
- contactReference – A reference for the contact, unique within the source remote system.

- fullName – The full name of the caseworker.
- phoneNumber – The phone number of the caseworker. Optional.
- mobilePhoneNumber – The mobile/cell phone number of the caseworker. Optional.
- faxNumber – The fax number for the caseworker. Optional.
- email – The email address of the caseworker. Optional.

If a request is received with the same source system and contact reference as a preexisting entry then the information in the newer request supersedes the preexisting information.

Case service

7.0.3.0

An inbound web service invoked by remote systems on IBM Cúram Universal Access. This service is used to update details of cases associated with a particular Citizen Account. The schema for the payload of web service requests of this type can be found in `<CURAM_DIR>\EJBServer\components\WorkspaceServices\webservices\ExternalCase.xsd`. See the sample SOAP request for this web service.

A web service request of this type contains the following information:

- sourceSystem – The name of the remote system sending the request. Must match the name of a remote system configured in the system.
- contactReference – A reference for the contact, unique within the source remote system, this must match a contact reference previously transmitted via a Contact Service request.
- caseReference – This is a case reference and must be unique within the remote system that is the source of this request.
- caseName - The human readable name of the case on the remote system. The case name must be localized to the locale of the client. Case names used in the Payment web service should match case names provided in this request.
- citizenWorkspaceAccountID – The unique citizen workspace account id.

If a request is received with the same source system and case reference as a preexisting entry then the information in the newer request supersedes the preexisting information.

Sample SOAP requests

7.0.3.0

A list of sample SOAP requests to help with development.

Intake program application update

7.0.3.0

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/" xmlns:rem="http://remote.externalservices.workspaceservices
.curam" xmlns:xsd="http://dom.w3c.org/xsd">
   <soapenv:Header>
     <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>userforpeersystem</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:updateIntakeProgramApplication>
      <rem:xmlMessage>
      <intakeProgramApplicationUpdate>
        <applicationReference>256</applicationReference>
        <applicationProgramReference>joannesprogram
</applicationProgramReference>
        <programApplicationStatus>IPAS1004</programApplicationStatus>
        <programApplicationDisposedDateTime>
          20120528 17:19:47
        </programApplicationDisposedDateTime>
        <programApplicationDenialReason>IPADR1001
</programApplicationDenialReason>
      </intakeProgramApplicationUpdate>
         </rem:xmlMessage>
```

```
      </rem:updateIntakeProgramApplication>
   </soapenv:Body>
</soapenv:Envelope>
```

Withdrawal request update

7.0.3.0

```
      <?xml version="1.0" encoding="UTF-8"?>
<table name="SEARCHSERVICEFIELD">

  <column name="
      searchServiceFieldId
      " type="text" />
  <column name="
      searchServiceId
      " type="text" />
  <column name="
      name
      " type="text" />
  <column name="
      indexed
      " type="bool" />
  <column name="
      type
      " type="text" />
  <column name="
      stored
      " type="bool" />
  <column name="
      entityName
      " type="text" />
  <column name="
      analyzerName
      " type="text" />
  <column name="
      untokenized
      " type="bool" />

  <row>
    <attribute name="searchServiceFieldId">
      <value>
      field0
      </value>
    </attribute>
    <attribute name="searchServiceId">
      <value>
      PersonSearch
      </value>
    </attribute><attribute name="name">
      <value>
      primaryAlternateID
      </value>
    </attribute><attribute name="indexed"> <soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:rem="http://remote.externalservices.workspaceservices.curam"
xmlns:xsd="http://dom.w3c.org/xsd">
   <soapenv:Header>
     <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>userforpeersystem</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:updateWithdrawalRequest>
         <rem:xmlMessage>
    <withdrawalRequestUpdate>
      <curamReferenceID>-6897262829317914624</curamReferenceID>
      <withdrawalRequestStatus>WREQ1002</withdrawalRequestStatus>
      <resolvedDateTime>20120525 11:30:50</resolvedDateTime>
    </withdrawalRequestUpdate>
         </rem:xmlMessage>
      </rem:updateWithdrawalRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Create account

7.0.3.0

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/" xmlns:rem="http://remote.externalservices.workspaceservices.
curam" xmlns:xsd="http://dom.w3c.org/xsd">
   <soapenv:Header>
     <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>admin</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:createAccount>
         <!--Optional:-->
         <rem:xmlMessage>
            <!--Optional:-->
     <cre:AccountCreate xmlns:cre="http://www.curamsoftware.com/
WorkspaceServices/ExternalAccountCreate">
        <firstName>John</firstName>
        <middleName>M</middleName>
        <surname>Doe</surname>
        <username>johnmdoe</username>
        <password>password1</password>
        <confirmPassword>password1</confirmPassword>
        <secretQuestionType>SQT1</secretQuestionType>
        <answer>mypassword1</answer>
        <termsAndConditionsAccepted>true</termsAndConditionsAccepted>
        <intakeApplicationReference>256</intakeApplicationReference>
        <clientIDOnRemoteSystem>112233445566</clientIDOnRemoteSystem>
        <sourceSystem>TestSystem</sourceSystem>
    </cre:AccountCreate>
         </rem:xmlMessage>
      </rem:createAccount>
   </soapenv:Body>
</soapenv:Envelope>
```

Account link

7.0.3.0

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/" xmlns:rem="http://remote.externalservices.workspaceservices.
curam" xmlns:xsd="http://dom.w3c.org/xsd">
   <soapenv:Header>
     <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>admin</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:linkTargetSystemToAccount>
         <rem:xmlMessage>
          <lnk:AccountLink xmlns:lnk="http://www.curamsoftware.com/
WorkspaceServices/ExternalAccountLink">
           <sourceSystem>TestSystem</sourceSystem>
           <citizenWorkspaceAccountID>7081910414040104960
</citizenWorkspaceAccountID>
           <clientIDOnRemoteSystem>112233445566</clientIDOnRemoteSystem>
          <createdByUsername>testuser</createdByUsername>
         </lnk:AccountLink>
         </rem:xmlMessage>
      </rem:linkTargetSystemToAccount>
   </soapenv:Body>
</soapenv:Envelope>
```

Account unlink

7.0.3.0

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/" xmlns:rem="http://remote.externalservices.workspaceservices.
curam" xmlns:xsd="http://dom.w3c.org/xsd">
   <soapenv:Header>
     <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>admin</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:unlinkTargetSystemFromAccount>
         <!--Optional:-->
         <rem:xmlMessage>
         <unl:AccountUnlink xmlns:unl="http://www.curamsoftware.com/
WorkspaceServices/ExternalAccountUnlink">
```

```
            <sourceSystem>TestSystem</sourceSystem>
            <citizenWorkspaceAccountID>7081910414040104960
</citizenWorkspaceAccountID>
         </unl:AccountUnlink>
         </rem:xmlMessage>
      </rem:unlinkTargetSystemFromAccount>
   </soapenv:Body>
</soapenv:Envelope>
```

Citizen message

7.0.3.0

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/" xmlns:rem="http://remote.externalservices.workspaceservices.
curam" xmlns:xsd="http://dom.w3c.org/xsd">
    <soapenv:Header>
  <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>admin</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:createMessage>
         <rem:xmlMessage>
<cm:CitizenMessage xmlns:cm="http://www.curamsoftware.com/
WorkspaceServices/ExternalCitizenMessage">
  <sourceSystem>TestSystem</sourceSystem>
  <cityIndustryType>CMI9001</cityIndustryType>
  <citizenWorkspaceAccountID>7081910414040104960
</citizenWorkspaceAccountID>
  <relatedID>6060</relatedID>
  <externalCitizenMessageType>PMT2004</externalCitizenMessageType>
  <messageTitle>Hello, World!</messageTitle>
  <messageBody>This is the body of the message.</messageBody>
  <effectiveDate>2000-01-01</effectiveDate>
  <expiryDate>2020-01-01</expiryDate>
  <priority>false</priority>

</cm:CitizenMessage>
         </rem:xmlMessage>
      </rem:createMessage>
   </soapenv:Body>
</soapenv:Envelope>
```

Payment (simple)

7.0.3.0

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/" xmlns:rem="http://remote.externalservices.workspaceservices.
curam" xmlns:xsd="http://dom.w3c.org/xsd">
   <soapenv:Header>
     <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>admin</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:create>
         <rem:xmlMessage>
     <tns:Payment xmlns:tns="http://www.curamsoftware.com/
WorkspaceServices/ExternalPayment">
        <paymentID>1554</paymentID>
        <sourceSystem>TestSystem</sourceSystem>
        <cityIndustryType>CMI9001</cityIndustryType>
        <citizenWorkspaceAccountID>7081910414040104960
</citizenWorkspaceAccountID>
        <paymentAmount>50.00</paymentAmount>
        <currency>EUR</currency>
        <paymentMethod>CHQ</paymentMethod>
        <paymentStatus>PRO</paymentStatus>
        <effectiveDate>2012-01-01</effectiveDate>
        <coverPeriodFrom>2012-01-01</coverPeriodFrom>
        <coverPeriodTo>2012-01-01</coverPeriodTo>
        <dueDate>2012-01-01</dueDate>
        <payeeName>Dorothy</payeeName>
        <payeeAddress>12 Gloster St., WA 6008</payeeAddress>
        <paymentReferenceNo>F</paymentReferenceNo>
        <bankSortCode>933384</bankSortCode>
        <bankAccountNo>88776655</bankAccountNo>
        <PaymentBreakdown>
```

```
            <PaymentLineItem>
                 <caseName>I</caseName>
                 <caseReferenceNo>J</caseReferenceNo>
                 <componentType>C10</componentType>
                 <debitAmount>22.45</debitAmount>
                 <creditAmount>50.76</creditAmount>
                 <coverPeriodFrom>2012-01-01</coverPeriodFrom>
                 <coverPeriodTo>2012-01-01</coverPeriodTo>
              </PaymentLineItem>
         </PaymentBreakdown>
     </tns:Payment>
  </rem:xmlMessage>
</rem:create>
</soapenv:Body>
</soapenv:Envelope>
```

Payment (batched)

7.0.3.0

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/" xmlns:rem="http://remote.externalservices.workspaceservices.
curam" xmlns:xsd="http://dom.w3c.org/xsd">
   <soapenv:Header>
     <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>admin</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:create>
         <rem:xmlMessage>
     <tns:Payments xmlns:tns="http://www.curamsoftware.com/
WorkspaceServices/ExternalPayment">
        <Payment>
            <paymentID>2346</paymentID>
            <sourceSystem>TestSystem</sourceSystem>
            <cityIndustryType>CMI9001</cityIndustryType>
            <citizenWorkspaceAccountID>8306889512684879872
</citizenWorkspaceAccountID>
            <paymentAmount>48.00</paymentAmount>
            <currency>EUR</currency>
            <paymentMethod>CHQ</paymentMethod>
            <paymentStatus>PRO</paymentStatus>
            <effectiveDate>2012-01-01</effectiveDate>
            <coverPeriodFrom>2012-01-01</coverPeriodFrom>
            <coverPeriodTo>2012-01-01</coverPeriodTo>
            <dueDate>2012-01-01</dueDate>
            <payeeName>D</payeeName>
            <payeeAddress>E</payeeAddress>
            <paymentReferenceNo>F</paymentReferenceNo>
            <bankSortCode>G</bankSortCode>
            <bankAccountNo>H</bankAccountNo>
            <PaymentBreakdown>
                <PaymentLineItem>
                    <caseName>I</caseName>
                    <caseReferenceNo>J</caseReferenceNo>
                    <componentType>C24000</componentType>
                    <debitAmount>22.45</debitAmount>
                    <creditAmount>49.76</creditAmount>
                    <coverPeriodFrom>2012-01-01</coverPeriodFrom>
                    <coverPeriodTo>2012-01-01</coverPeriodTo>
                </PaymentLineItem>
                <PaymentLineItem>
                    <caseName>I</caseName>
                    <caseReferenceNo>J</caseReferenceNo>
                    <componentType>C24000</componentType>
                    <debitAmount>22.45</debitAmount>
                    <creditAmount>49.76</creditAmount>
                    <coverPeriodFrom>2012-01-01</coverPeriodFrom>
                    <coverPeriodTo>2012-01-01</coverPeriodTo>
                </PaymentLineItem>
            </PaymentBreakdown>
        </Payment>
    </tns:Payments>
         </rem:xmlMessage>
      </rem:create>
   </soapenv:Body>
</soapenv:Envelope>
```

Contact

7.0.3.0

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/" xmlns:rem="http://remote.externalservices.workspaceservices.
curam" xmlns:xsd="http://dom.w3c.org/xsd">
   <soapenv:Header>
  <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>admin</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:updateExternalContact>
         <rem:xmlMessage>
     <con:ContactInfo xmlns:con="http://www.curamsoftware.com/
WorkspaceServices/ExternalContact">
        <sourceSystem>TestSystem</sourceSystem>
        <contactReference>CON_100</contactReference>
         <fullName>Harry Neilan</fullName>
        <phoneNumber>1-800-CALL-ME</phoneNumber>
        <mobilePhoneNumber>1-800-CALL-MOB</mobilePhoneNumber>
        <faxNumber>1-800-CALL-FAX</faxNumber>
        <email>harry@x.org</email>
    </con:ContactInfo>
         </rem:xmlMessage>
      </rem:updateExternalContact>
   </soapenv:Body>
</soapenv:Envelope>
```

Cases

7.0.3.0

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/" xmlns:rem="http://remote.externalservices.workspaceservices.
curam" xmlns:xsd="http://dom.w3c.org/xsd">
<soapenv:Header>
     <curam:Credentials xmlns:curam="http://www.curamsoftware.com">
     <Username>admin</Username>
     <Password>password</Password>
   </curam:Credentials>
   </soapenv:Header>
   <soapenv:Body>
      <rem:updateExternalCase>
         <rem:xmlMessage>
    <cas:CaseInfo xmlns:cas="http://www.curamsoftware.com/
WorkspaceServices/ExternalCase">
        <sourceSystem>TestSystem</sourceSystem>
        <contactReference>CON_100</contactReference>
        <caseReference>CAS_109</caseReference>
        <caseName>My Benefit Case - 103</caseName>
        <citizenWorkspaceAccountID>8306889512684879872
</citizenWorkspaceAccountID>
    </cas:CaseInfo>
         </rem:xmlMessage>
      </rem:updateExternalCase>
   </soapenv:Body>
</soapenv:Envelope>
```

Artifacts with limited customization scope

7.0.3.0

A description of IBM Cúram Universal Access artifacts that have restrictions on their use. Customers that want to change these artifacts should consider alternatives or request an enhancement to Universal Access.

Model

Customers are not supported in making changes to any part of the Universal Access model. Changes in the model such as changing the data types of domains can cause failure of the Universal Access system and upgrade issues. This applies to the model files in the following packages:

- WorkspaceServices
- CitizenWorkspace

- CitizenWorkspaceAdmin

Code tables

See the *IBM Cúram Development Compliancy Guide* for a list of restricted code tables.

Related information

Developing Compliantly with Cúram Business Intelligence

Notices

This information was developed for products and services offered in the United States.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd. 19-21, Nihonbashi-Hakozakicho, Chuo-ku Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Privacy Policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies or other similar technologies that collect each user’s name, user name, password, and/or other personally identifiable information for purposes of session management, authentication, enhanced user usability, single sign-on configuration and/or other usage tracking and/or functional purposes. These cookies or other similar technologies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “ Copyright and trademark information ” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.

Part Number:

(1P) P/N: