

IBM Cúram Social Program Management



# Cúram Security Guide

*Version 6.0.5*



IBM Cúram Social Program Management



# Cúram Security Guide

*Version 6.0.5*

**Note**

Before using this information and the product it supports, read the information in "Notices" on page 59

**Revised: May 2013**

This edition applies to IBM Cúram Social Program Management v6.0.5 and to all subsequent releases unless otherwise indicated in new editions.

Licensed Materials - Property of IBM.

© **Copyright IBM Corporation 2012, 2013.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© Cúram Software Limited. 2011. All rights reserved.

---

# Contents

**Figures . . . . . v**

**Tables . . . . . vii**

**Chapter 1. Cúram Security . . . . . 1**

1.1 Purpose . . . . . 1  
1.2 Audience . . . . . 1  
1.3 Overview . . . . . 1  
1.4 Chapters in this Guide . . . . . 1

**Chapter 2. Authentication . . . . . 3**

2.1 Overview . . . . . 3  
2.2 Authentication . . . . . 3  
2.3 Authentication Architecture . . . . . 4  
2.4 Default Authentication . . . . . 4  
2.5 Alternate Login IDs . . . . . 5  
2.6 The Login Page . . . . . 6  
2.7 Customization of the Login Page . . . . . 6  
2.8 Cúram JAAS Login Module . . . . . 7  
2.9 Password Management . . . . . 7  
2.10 Default Configuration for WebLogic Server . . . . . 8  
2.11 Default Configuration for WebSphere . . . . . 8  
2.12 Customization of the JAAS Login Module . . . . . 10  
2.13 Verification Process for Authentication . . . . . 11  
2.14 Default Authentication . . . . . 11  
2.15 Default Verification Process . . . . . 11  
2.16 Authentication Attempts . . . . . 11  
2.17 Customization of Default Authentication . . . . . 11  
2.18 Identity Only Authentication . . . . . 11  
2.19 Customization of Identity Only Authentication . . . . . 13  
2.20 External Access Security Authentication . . . . . 13  
2.21 Custom Verifications . . . . . 13

**Chapter 3. Authorization . . . . . 15**

3.1 Overview . . . . . 15  
3.2 Users, Roles and Groups . . . . . 15  
3.3 Security Identifiers (SIDs) . . . . . 16  
3.4 Function Identifiers (FIDs) . . . . . 16  
3.5 Field Level Security Identifiers . . . . . 16  
3.6 User Defined SIDs . . . . . 16  
3.7 Runtime Authorization . . . . . 17  
3.8 Client Authorization Checks . . . . . 17  
3.9 Server Authorization Checks . . . . . 17

**Chapter 4. Cryptography in Cúram . . . . . 19**

4.1 Overview . . . . . 19  
4.2 Cipherng . . . . . 19  
4.3 Digesting . . . . . 19  
4.4 Cryptography Properties . . . . . 19  
4.5 Cúram Cipher Settings . . . . . 20  
4.6 Cúram Digest Settings . . . . . 21  
4.7 Cipher-Encrypted Passwords . . . . . 21

**Chapter 5. Security Data Caching . . . . . 23**

5.1 Overview . . . . . 23  
5.2 Cúram Security Cache . . . . . 23  
5.3 Cache Refresh . . . . . 23  
5.4 Cache Refresh Failure . . . . . 23  
5.5 WebSphere Caching Behavior . . . . . 23

**Chapter 6. Security for Alternative Clients . . . . . 25**

6.1 Overview . . . . . 25  
6.2 Mandatory Cúram Users . . . . . 25  
6.3 Web Services . . . . . 25  
6.4 Batch Processing . . . . . 26  
6.5 JMS Messaging . . . . . 26  
6.6 Deferred Processing . . . . . 26

**Chapter 7. External User Applications . . . . . 27**

7.1 Overview . . . . . 27  
7.2 External User Applications . . . . . 27  
7.3 User Scope . . . . . 27  
7.4 Deployment of an External Application . . . . . 28

**Chapter 8. Using Single Sign On . . . . . 31**

8.1 Overview . . . . . 31  
8.2 Single Sign On with WebSphere . . . . . 31  
8.3 Single Sign On for WebLogic Server . . . . . 32

**Chapter 9. Other Security Considerations . . . . . 33**

9.1 Overview . . . . . 33  
9.2 SSL Settings for the Application . . . . . 33  
9.3 Using Cúram in a Secure Environment . . . . . 33

**Chapter 10. Customizing Authentication . . . . . 35**

10.1 Customizing the Login Page . . . . . 35  
10.2 Applying Styling to the Login Page . . . . . 35  
10.3 Enabling Usernames With Extended Characters for WebLogic Server . . . . . 35  
10.4 Changing the Case-Sensitivity of the Username . . . . . 35  
10.5 Adding Custom Verifications to the Authentication Process . . . . . 35  
10.6 Configuring the Custom Authenticator . . . . . 36  
10.7 Configuring Identity Only Authentication . . . . . 36  
10.8 Adding the Cache Refresh Failure Callback Interface . . . . . 36  
10.9 Turning Off SSL Settings for the Application . . . . . 36  
10.10 Modifying the web.xml File for the Client Application . . . . . 36  
10.11 Modifying the Application Server Configuration . . . . . 37  
10.12 Analyzing the AuthenticationLog Database Table . . . . . 37

## **Chapter 11. Customizing Authorization 39**

|   |    |
|---|----|
| 11.1 Overview . . . . .   | 39 |
| 11.2 Creating Authorization Data Mapping . . . . .                                  | 39 |
| 11.3 Creating a New Security Role . . . . .   | 39 |
| 11.4 Creating a New Security Group . . . . .  | 39 |
| 11.5 Linking the Security Group to the Security Role                                | 39 |
| 11.6 Creating the Security Identifier (SID) . . . . .                               | 39 |
| 11.7 Linking the Security Group to the SID . . . . .                                | 40 |
| 11.8 Linking the Security Role to the User . . . . .                                | 40 |
| 11.9 Loading Security Information onto the Database                                 | 40 |
| 11.10 Creating Function Identifiers (FIDs) . . . . .                                | 40 |
| 11.11 Switching Security off for a Process Method . . . . .                         | 40 |
| 11.12 Security Considerations During Development                                    | 41 |
| 11.13 Controlling the Logging of Authorization<br>Failures for the Client . . . . . | 41 |
| 11.14 Authorizing New SID Types . . . . .   | 41 |
| 11.15 Analyzing the AuthorisationLog Database<br>Table . . . . .                    | 42 |

## **Chapter 12. Customizing Cryptography 43**

|   |    |
|---|----|
| 12.1 Overview . . . . .   | 43 |
| 12.2 Cipher Customization . . . . .   | 43 |
| 12.3 Key Management . . . . .   | 43 |
| 12.4 How to Create a New Keystore . . . . .   | 44 |
| 12.5 Digest Customization . . . . .   | 45 |
| 12.6 How to Specify a Digest Salt . . . . .   | 45 |
| 12.7 How to Utilize the Superseded Digest Settings<br>for a Period of Migration . . . . . | 45 |
| 12.8 Modifying Your Crypto Configuration for a<br>Production System . . . . .             | 47 |

## **Chapter 13. Customizing External User Applications 49**

|  |    |
|--|----|
| 13.1 Overview . . . . .  | 49 |
| 13.2 Creating an External User Application . . . . .   | 49 |
| 13.3 Creating an External User Client Login Page. . . . .                                      | 49 |
| 13.4 Creating an External User Client Automatic<br>Login Page . . . . .                        | 49 |
| 13.5 Extending the Public Access User Class . . . . .  | 51 |
| 13.6 Authenticating an External User . . . . .   | 51 |
| 13.7 Determine External User Details . . . . .   | 53 |
| 13.8 Authorizing an External User . . . . .  | 53 |
| 13.9 Determining the User Type . . . . .   | 54 |
| 13.10 Preventing the Deletion of a Security Role:<br>Role Usage Count . . . . .                | 54 |
| 13.11 Retrieving a Registered Username . . . . .   | 55 |
| 13.12 Reading User Preferences . . . . .   | 55 |
| 13.13 Modifying User Preferences . . . . .   | 56 |
| 13.14 Configuring External Access Security . . . . .   | 56 |
| 13.15 Determining if a User is Internal or External<br>using the UserScope Interface . . . . . | 56 |
| 13.16 User Type Determination . . . . .  | 57 |

## **Notices 59**

|   |    |
|---|----|
| Programming Interface Information . . . . . | 61 |
| Trademarks . . . . .                        | 61 |

---

## Figures

|  |    |   |    |
|--|----|---|----|
| 1. Authentication Architecture . . . . .               | 4  | 6. WebLogic Server Support for Logins With      |    |
| 2. Default Authentication . . . . .                    | 5  | Extended Characters . . . . .                   | 35 |
| 3. Default Authentication Flow for WebSphere . . . . . | 9  | 7. Example Usage of isSIDAuthorised() . . . . . | 42 |
| 4. Authentication Flow for WebSphere with User         |    | 8. Automatic Login JSP . . . . .                | 50 |
| Registry Enabled. . . . .                              | 10 | 9. Automatic Logout JSP . . . . .               | 51 |
| 5. Identity Only Authentication. . . . .               | 12 |   |    |





---

## Tables

- |    |  |    |    |   |    |
|----|--|----|----|---|----|
| 1. | Contents of the Authentication Log . . . . . | 37 | 3. | Relationship of keytool Command Arguments<br>to Cúram Crypto Properties . . . . . | 44 |
| 2. | Contents of the Authorization Log . . . . .  | 42 |    |   |    |



---

# Chapter 1. Cúram Security

---

## 1.1 Purpose

The purpose of this guide is to describe the aspects of security that must be considered when developing and deploying a IBM Cúram Social Program Managemententerprise application. The term security is used to describe many different areas. For the purpose of this document, the following areas will be covered: authentication and authorization. This guide also describes the securable elements of IBM Cúram Social Program Managementapplications.

This guide is divided into two parts. The first part contains an overview of the security areas and should be read by all interested parties, both technical architects and developers. The second part provides development "how to" information and examples for application security.

---

## 1.2 Audience

There are two main audiences for this document:

- Technical Architects who need to consider integration with other systems at deployment time, e.g., LDAP.
- Developers who must consider the type of application that will developed, i.e., is the application for internal users, external users, or both.

**Note:** Internal users are users that exist on the Cúram Users database table. They are part of the organisation and typically are there to manage claims for participants. External users are all other types of users. External users are not part of the organisation. Their access is limited. An example of an external user would be a provider that provides a service to the organisation.

---

## 1.3 Overview

Security is built into the infrastructure that underpins the development of the IBM Cúram Social Program Managementapplication. It supports the authentication of a user at login time as well as providing support for the authorization process. The design of an application is not complete without first considering the implications of securing the application against unauthorized access to sensitive data or functionality. Security is therefore one of the key priorities during application development.

The following are the main concepts of IBM Cúram Social Program Managementsecurity:

- Authentication
- Authorization

There is also the concept of location based security. At the organization level, location security limits a user's access to client and case information. Location data security can also be configured to allow a user to access locations other than their own. This guide does not detail location based security. The *Cúram Location Administration Guide* should be consulted for further details on location based security.

---

## 1.4 Chapters in this Guide

This guide is in two parts. Part 1 consists of the following chapters, which provide a high-level overview of the IBM Cúram Social Program Management security architecture for the application and deployment to application servers:

**Chapter 2 Authentication**

This chapter describes the authentication architecture for IBM Cúram Social Program Management, giving a detailed description of each area and any customizable points available.

**Chapter 3 Authorization**

This chapter describes how authorization works and how this can be configured for users.

**Chapter 4 Cryptography in Cúram**

This chapter describes how IBM Cúram Social Program Management uses cryptography to secure passwords.

**Chapter 5 Security Data Caching**

This chapter describes the in-built Cúram Security Cache and also describes the IBM® WebSphere® Application Server cache and how it affects user authentication.

**Chapter 6 Security for Alternative Clients**

This chapter describes the usernames that must exist on the Cúram Users database table to ensure processes like Workflow can run successfully.

**Chapter 7 External User Applications**

This chapter describes why an external user application would be needed and what should be considered for this.

**Chapter 8 Using Single Sign On**

This chapter describes the application server properties that must be considered when IBM Cúram Social Program Management will be used in a Single Sign On solution.

**Chapter 9 Other Security Considerations**

This chapter gives a brief overview of some external security practices and considerations.

Part 2 consists of the following chapters, which provide several how-to's on development activities for coding and customizing security:

**Chapter 10 Customizing Authentication**

This chapter describes customization points and development artefacts relevant to authentication.

**Chapter 11 Customizing Authorization**

This chapter describes how to implement authorization for IBM Cúram Social Program Management.

**Chapter 12 Customizing Cryptography**

This chapter describes how to customize Cúram's use of cryptography.

**Chapter 13 Customizing External User Applications**

This chapter describes how to develop an external user application.

---

## Chapter 2. Authentication

---

### 2.1 Overview

This chapter covers authentication for IBM Cúram Social Program Management. Authentication is the process of determining if a user is who they say they are. Authentication is needed where a user must be verified in order to access a secure resource on a system.

Form-based authentication is where a user is presented with a form allowing them to enter username and password credentials. These credentials are compared against the credentials stored on the system for this username, if they match the user is considered an authenticated user for the system. For security reasons the password for authenticating a user is stored on the system in a digested form.

The IBM Cúram Social Program Management web client is configured to support form-based authentication, which means that before a user can access any of the web client content, they will be redirected to a login form to authenticate.

The authentication process involves the verification of the username and password, and this is performed by default by a JAAS (Java™ Authentication and Authorization Service) login module. HTTPS/SSL is turned on by default in the web client ensuring the form-based login authentication mode is secure.

---

### 2.2 Authentication

Different authentication modes can be configured (depending on authentication requirements) via the Cúram JAAS login module.

The following are the authentication modes supported:

- Default Authentication;
- Identity Only Authentication;
- External Access Security Authentication.

Each of these modes are described in detail in the sections below.

## 2.3 Authentication Architecture

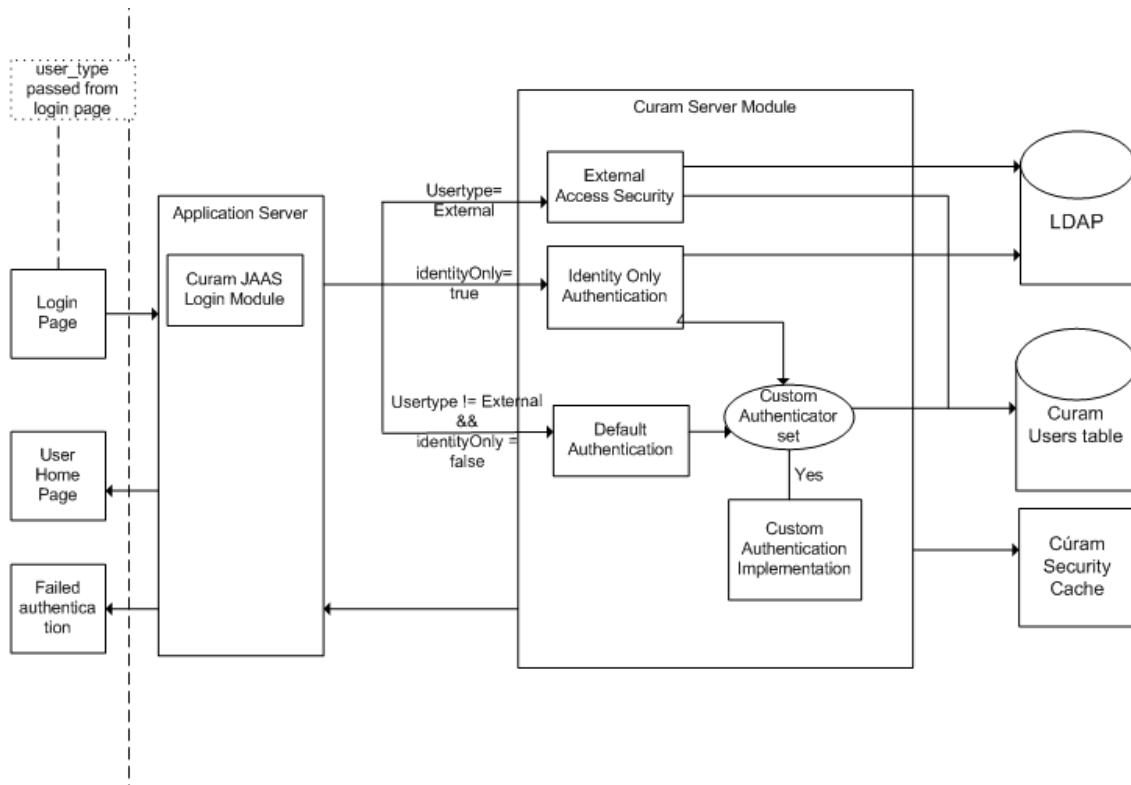


Figure 1. Authentication Architecture

2.3, “Authentication Architecture”, above, outlines the architecture for the authentication process of a user. Out-of-the-box, default authentication is performed for a user. This behavior can be customized for both internal and external users, depending on the authentication requirements. The following sections in this chapter describe in detail each of the functional areas that make up the authentication architecture, indicating where customizations are possible.

## 2.4 Default Authentication

Default out-of-the-box authentication for IBM Cúram Social Program Management involves the user logging in via the login screen, where the user is prompted for a username and password as credentials. These credentials are then passed to the Cúram JAAS login module configured in the application server.

The default authentication is invoked and the username and password entered are checked against the username and password stored on the Cúram Users database table. The Cúram username is immutable, but you have the option of configuring your system to use a Cúram login ID instead, which is changeable. The login ID is a logical extension of the Cúram user and the same verifications checked for the username are also checked for the login ID. See 2.5, “Alternate Login IDs,” on page 5 for more information about alternate login IDs.

Authentication performs a number of verifications against the login credentials, 2.14, “Default Authentication,” on page 11 should be consulted for details on the verifications.

Provided all verifications are successful, the user is considered to be authenticated by the application.

Once the user is authenticated, the user is then added to the Cúram Security Cache. The Cúram Security Cache stores the username and all related authorization data for that user in order to optimize the authorization data retrieval for a user. Chapter 5, “Security Data Caching,” on page 23 should be consulted for further details on the Cúram Security Cache. Figure 2.3 below highlights the path taken for default authentication.

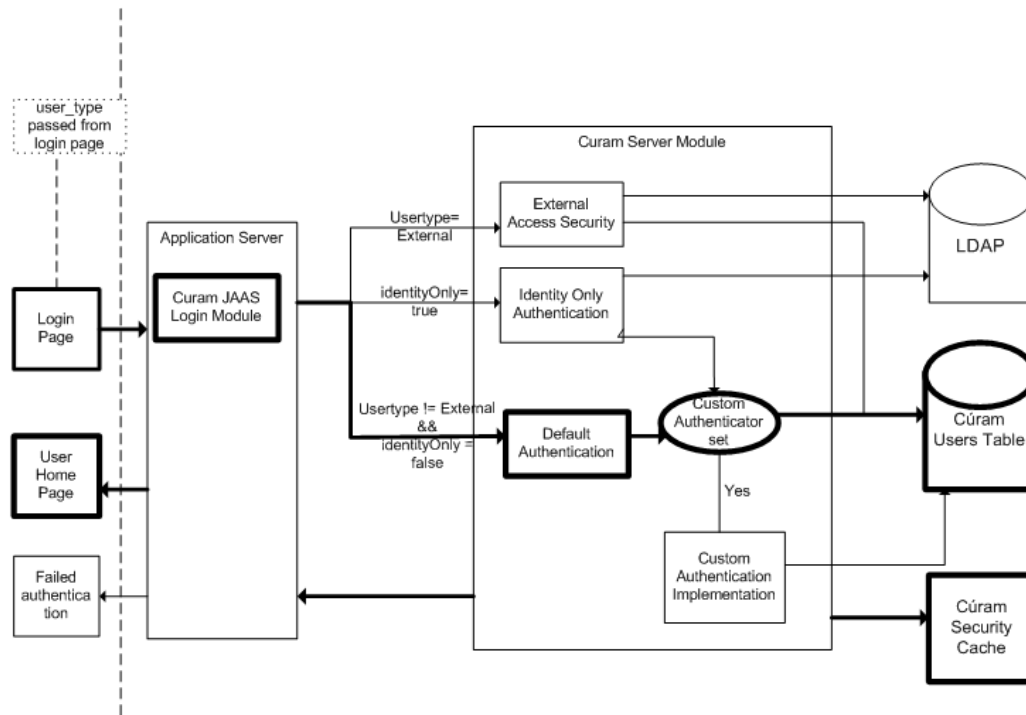


Figure 2. Default Authentication

## 2.5 Alternate Login IDs

By default, Cúram utilizes the username and digested password stored in the Users table for authentication. This username is immutable, once created it cannot be changed. This lack of flexibility may not meet requirements for some installations. However, you have the option of using a login ID, which can be updated, instead of the immutable username. The login ID functions as a logical extension of the Cúram Users table. When the alternate login ID is used the username still exists and is used internally by Cúram, but the user logs into Cúram using the login ID.

Things to note when using the alternate login ID:

- The use of the alternate login ID is mutually exclusive with the username. That is, you cannot have a mix of Cúram users logging in with usernames and login IDs.
- The Cúram ExtendedUsersInfo table, where the login ID is stored, must be populated before turning on the alternate login ID feature, which is explained in more detail below.
- When using login IDs authentication results are stored in the AuthenticationLog table and the AltLogin column indicates whether the UserName column represents a username (false) or login ID (true).
- Login IDs are only applicable to internal Cúram users; i.e., users stored on the Cúram Users table. However, if you are using identity-only with alternate Login IDs then wherever those IDs are stored (e.g. WebSphere registry, LDAP, etc.) must match the login IDs stored in the Cúram ExtendedUsersInfo table.

- When assigning login IDs you need to take care with IDs that are used internally and/or have dependencies (e.g. with property values) outside of the *Cúram Users* table. These are the usernames that would cause issues if its login ID differed from the username without a corresponding change as indicated:
  - *SYSTEM* - In WebSphere this username is associated with JMS processing and is made part of the WebSphere configuration at application deployment time. See 6.2, “Mandatory *Cúram Users*,” on page 25 and the appropriate WebSphere *Cúram Deployment Guide* for information on changing this ID.
  - *DBTOJMS* - this is the default DBtoJMS username used by batch processing and is referenced by property `curam.security.credentials.dbtojms.username`. See 6.2, “Mandatory *Cúram Users*,” on page 25, 6.5, “JMS Messaging,” on page 26, 6.6, “Deferred Processing,” on page 26 and the *Cúram Batch Processing Guide* for more information.
  - *WEBSVCS* - this is the default web services username and is referenced by property `curam.security.credentials.ws.username`. See 6.2, “Mandatory *Cúram Users*,” on page 25, 6.3, “Web Services,” on page 25, and the *Cúram Web Services Guide* for more information.
  - *unauthenticated* - is the principal WebSphere uses for unauthenticated users and this login ID should not be changed.

To enable the use of the alternate login ID, once you've populated the *ExtendedUsersInfo* table, set the `curam.security.altlogin.enabled` property to true (see the *Cúram Server Developer's Guide* for more information on *Cúram* properties). This is a static property and *Cúram* must be restarted for it to take effect.

To populate the *ExtendedUsersInfo* table before activating the feature you have a number of options; for instance:

- With a simple SQL statement you can populate the table using the username in the *Users* table; so, there is no immediate user impact: `INSERT INTO EXTENDEDUSERSINFO (USERNAME, LOGINID, UPPERLOGINID, VERSIONNO) (SELECT USERNAME, USERNAME, UPPER(USERNAME), 1 FROM USERS)`; You can then roll-out your modifications to the login IDs in a controlled manner.
- You can implement an SQL application that implements your username and login ID mapping (e.g. LDAP common names).

**Note:** You must maintain the username foreign key relationship between the *Users* and *ExtendedUsersInfo* tables.

---

## 2.6 The Login Page

The default out-of-box login page is represented by the `logon.jsp` file. This `logon.jsp` represents the login page for the user to complete form-based login authentication. By default, the `logon.jsp` file contains the username and password fields. However, the `logon.jsp` file can be customized to pass an additional parameter by adding the `user_type` field. This field determines the type of user logging in, i.e., internal or external user. The username, password and `user_type` (if present) are all passed to the *Cúram JAAS* login module as part of the authentication process.

The default out-of-the-box `logon.jsp` file does not have the `user_type` property set. If this property is omitted, the user is assumed to be internal. When this property is set, it indicates that an external user is logging in. This property can be set to any value other than 'INTERNAL'.

---

## 2.7 Customization of the Login Page

The `logon.jsp` file can be customized, i.e. the `logon.jsp` file can be completely replaced by a custom `logon.jsp` file, for a number of reasons including the following:

### **An external user client application is being developed;**

If an external user client application is being developed, a new `logon.jsp` file must be created, as



the user type must be set to indicate an external user is logging in. 13.3, “Creating an External User Client Login Page,” on page 49 should be referenced for further details.

**Automatic login is needed;**

Some external user client applications require no user authentication and hence a username and password should not be requested, i.e. in the case of a external public access application. It is not possible to disable authentication, so the best way to achieve this requirement is to write an automatic login script. This is done by customizing the `logon.jsp` file for the external public access application. 13.4, “Creating an External User Client Automatic Login Page,” on page 49 should be referenced for further details.

**Different styling is required;**

The section on Login Pages in the *Cúram Web Client Reference Manual* should be referenced for further details on styling for the `logon.jsp` file.

**A requirement exists for usernames to contain extended characters (valid only for Oracle WebLogic Server).**

WebLogic Server provides a proprietary attribute, `j_character_encoding`, which must be added to the `logon.jsp` file. 10.3, “Enabling Usernames With Extended Characters for WebLogic Server,” on page 35 should be consulted for further details.

---

## 2.8 Cúram JAAS Login Module

Authentication is performed by a JAAS login module. It is configured in the application server and is invoked automatically by the application server as part of the authentication process for any access to the IBM Cúram Social Program Management application. The advantage to this approach is that the default authentication mechanism can be used with, or replaced by, a custom approach, without affecting the IBM Cúram Social Program Management application.

As mentioned earlier, the Cúram JAAS login module can be configured to operate in three modes. For more information on the configuration of the login modules and any application server specific behavior, the section on Application Server Configuration within the *Cúram Server Deployment Guide* for the application server being used should be consulted for further details.

Project specific requirements may mean that more than one login module is needed, e.g., a user may be required to enter more than the username and password for verification purposes. It is possible to configure multiple login modules in the application server. Each login module will be executed in the order as determined by the settings in the application server. For more information on these settings, the WebSphere or WebLogic Server documentation should be consulted.

Once the user is successfully authenticated by all login modules that require successful authentication of the user (this is configurable in the application server), the user is considered authenticated by the application.

---

## 2.9 Password Management

The passwords for all Cúram internal and external users are stored in their digest format on the Cúram Users and ExternalUsers database tables. When the Cúram JAAS login module receives the password it is digested before being sent to the login bean for comparison. Digesting is a one-way process to ensure the security of the password. The password stored for the user on the database uses the same digest algorithm, subject to your crypto settings, thereby ensuring the encrypted passwords can be successfully compared to each other, but remain secure.

Users managed externally, e.g. via LDAP with Cúram identity-only configured, are not subject to the above process. When authenticating against a third-party system (e.g., LDAP or a SSO Server), where there is a need for the Cúram application to pass the user-entered credentials to the third-party

system, the custom implementation of `curam.util.security.PublicAccessUser` can be used, as it will allow access to the credentials with plain-text password.

---

## 2.10 Default Configuration for WebLogic Server

The Cúram JAAS login module is configured as an authentication provider in WebLogic Server . The Cúram authentication provider is the only provider configured by the configuration scripts provided for WebLogic Server . As it is the only configured authentication provider, the Cúram authentication provider is responsible for authenticating and verifying the user. As mentioned previously, it is possible there may be more than one authentication provider configured in WebLogic Server , in this case the Cúram authentication provider may not be responsible for authenticating and verifying the user. 8.3, “Single Sign On for WebLogic Server,” on page 32 should be referenced for further details.

---

## 2.11 Default Configuration for WebSphere

The Cúram JAAS login module is configured as a system login module in WebSphere . The default, scripted security configuration within WebSphere involves the default file-based user registry and the Cúram system login module. The user registry in WebSphere is the default authentication mechanism and can be configured to be:

- A custom user registry;
- An LDAP directory server;
- The Local OS or;
- The WebSphere file-based repository.

There are multiple system login configurations for WebSphere . The Cúram system login module is configured for the `DEFAULT` , `WEB_INBOUND` and `RMI_INBOUND` configurations. The same login module is used for all three configurations. WebSphere automatically invokes the login modules configured as system login modules under certain circumstances:

- `DEFAULT`

The login modules specified for the `DEFAULT` configuration are invoked for authentication of web services and JMS invocations. They are also invoked during the startup phase of WebSphere ;

- `WEB_INBOUND`

The login modules specified for the `WEB_INBOUND` configuration are used for authentication of web requests;

- `RMI_INBOUND`

The login modules specified for the `RMI_INBOUND` configuration are used for authentication of Java clients.

The Cúram JAAS login module exists as a login module within a chain of login modules set up in WebSphere . It is expected that at least one of these login modules be responsible for adding credentials for the user. By default, the Cúram login module adds credentials for an authenticated user. As a result of this, the configured WebSphere user registry handled by a subsequent login module does not add credentials. Therefore, it is not necessary to define Cúram users within the WebSphere user registry. This behavior is configurable through the use of the `curam.security.user.registry.enabled` property set in the `AppServer.properties` file. The *Cúram Deployment Guide for WebSphere Application Server* or *Cúram Deployment Guide for WebSphere Application Server on z/OS* should be consulted for further details on setting this property. 2.11, “Default Configuration for WebSphere” below illustrates the default authentication flow for WebSphere . 2.11, “Default Configuration for WebSphere” below illustrates the authentication flow for WebSphere where its user registry is also queried, i.e. where the `curam.security.user.registry.enabled` property is set to true.

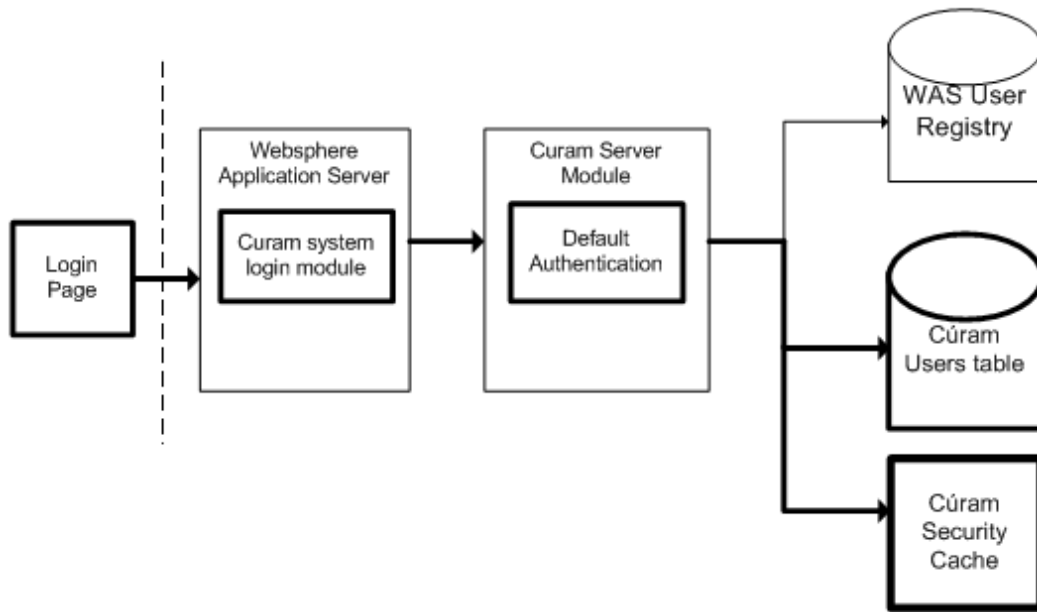


Figure 3. Default Authentication Flow for WebSphere

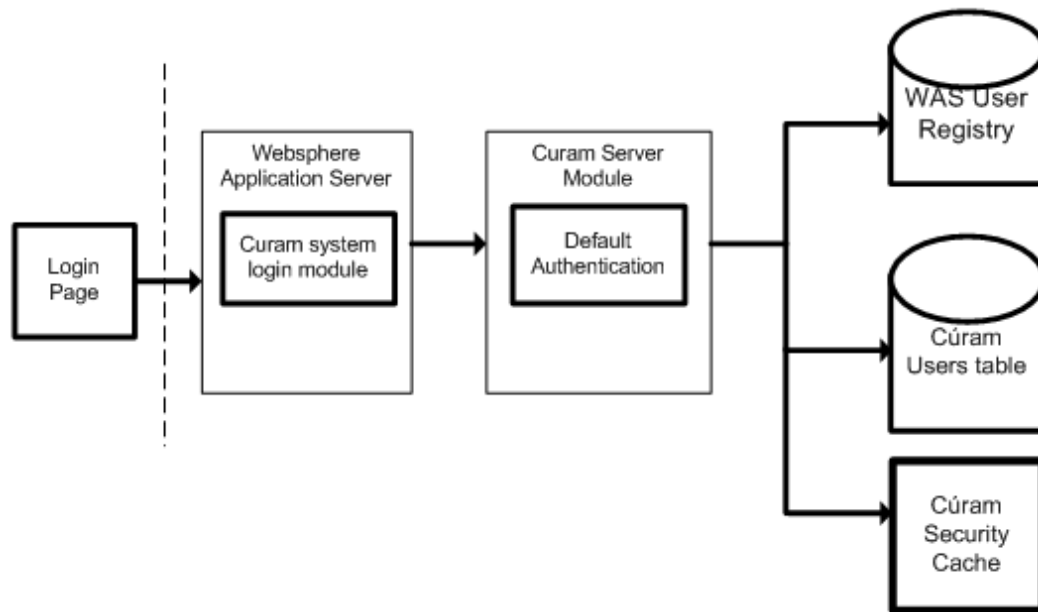


Figure 4. Authentication Flow for WebSphere with User Registry Enabled

As part of the security configuration there are certain users that are excluded from authentication and for these users the configured user registry *will* be queried. This list of users is configured automatically to be the WebSphere security user, as specified by the `security.username` property in `AppServer.properties` and the database user, as specified by the `curam.db.username` property in `Bootstrap.properties`. These two users are classified administrative users and not application users. It is possible to extend this list of excluded users manually, see the *Cúram Deployment Guide for WebSphere Application Server* and *Cúram Deployment Guide for WebSphere Application Server on z/OS* for more information.

**Warning:** The `security.username` and `curam.db.username` users are automatically added to the WebSphere file-based user repository by the provided configuration scripts. If the configured WebSphere user registry is not the default, these users must exist in the alternate WebSphere user registry.

## 2.12 Customization of the JAAS Login Module

It is possible that the Cúram JAAS login module may not support the authentication requirements for a particular custom solution. We strongly recommend that when developing a custom login module, that the Cúram JAAS login module be left in place and used with identity only authentication enabled. However, if deemed necessary, the Cúram JAAS login module can be removed and replaced by a custom solution. If this is the case Support must be consulted.

**Warning:** While it is possible to remove the Cúram JAAS login module completely, it should be noted that users must still exist in the Cúram Users database table for authorization reasons.

The Cúram JAAS login module adds new users to the Cúram Security Cache automatically, and when this Cúram JAAS login module is replaced by a custom JAAS login module, this functionality is no longer present. If a custom JAAS login module is completely replacing the Cúram JAAS login module, it is the responsibility of the custom JAAS login module to ensure an update of the Security Cache is triggered when a new user is added to the database.

---

## 2.13 Verification Process for Authentication

The type of verifications performed is dependent on the authentication mode being used. Below is a list of the authentication modes/configurations and full details on the verifications completed for each authentication mode.

---

## 2.14 Default Authentication

Default authentication is part of the out-of-the-box configuration and this mode of authentication involves verifying the username and password specified during login against the Cúram Users database table. All login information in this case is maintained by the IBM Cúram Social Program Management application.

---

## 2.15 Default Verification Process

The verifications performed by the Cúram login module during default authentication are:

- username and password.
- account and/or password expiry.
- username synchronization with security cache.
- break-in detection, e.g. upper limit on password entry attempts, incorrect usernames, password change failures.
- day and time access restrictions - day of the week and time range within the day.

The authentication and authorization of usernames is case sensitive by default, however it is possible to disable case sensitive authentication. If duplicate case insensitive usernames exist (e.g. caseworker, CaseWorker), authentication will fail due to an ambiguous username. 10.4, “Changing the Case-Sensitivity of the Username,” on page 35 should be referenced for further details on this.

---

## 2.16 Authentication Attempts

Authentication failures are not reported directly to a client as this would provide extra information to an intruder attempting to break into the system. For example, reporting an incorrect password would indicate that the username is valid. All authentication attempts (both success and failure) are instead logged in a database table called the AuthenticationLog . 11.15, “Analyzing the AuthorisationLog Database Table,” on page 42 should be consulted for further details.

---

## 2.17 Customization of Default Authentication

The default implementation can be customized to use a mutable login ID instead of the Curam username and the ability to add extra verifications is available by implementing the custom authenticator (2.21, “Custom Verifications,” on page 13 should be referenced for further details).

---

## 2.18 Identity Only Authentication

Authentication can be configured to perform identity-only verification, in place of the default verifications listed in 2.15, “Default Verification Process” above.

Identity only verification means that the authentication mechanism only ensures that the username for the user logging in exists on the Cúram Users database table. Full authentication must be completed by an alternative mechanism, to be configured in the application server.

An example of an alternative mechanism is an LDAP directory server, which is supported as an authentication mechanism by both the WebSphere and WebLogic Server application servers. Another alternative is to use a Single Sign-On Solution for authentication, or to implement a custom login module. For custom application server solutions the IBM or Oracle documentation should be consulted.

With identity-only authentication (as for default authentication), entries are added to the AuthenticationLog database table at the end of the authentication process.

For a successful login the following status is used:

- AUTHONLY

For a failure scenario, the following status is used:

- BADUSER

This is the only possible failure scenario where a user does not exist.

The loginFailures and lastLogin fields of the AuthenticationLog are not set. This is true even if customized verifications are implemented.

When the password expiry information for a user is set (on the Cúram Users database table), the password expiry warning will be displayed if it is about to expire. With identity-only authentication this warning is misleading. It is recommended that any fields relating to the authentication verifications, such as password expiry or account enabled, are not used if identity-only authentication is enabled.

When identity-only authentication is enabled, security is not used for authentication but is still used for authorization purposes. As a result of this, all users requiring access to the application must still exist in the Cúram Users database table, as well as in the alternative authentication mechanism, e.g., LDAP. It is important to note that there are two users that must exist in both locations, i.e. the SYSTEM user and the DBTOJMS user. Chapter 6, “Security for Alternative Clients,” on page 25 should be consulted for further details on these users.

10.7, “Configuring Identity Only Authentication,” on page 36 should be consulted for details on how to configure identity only for an application server.

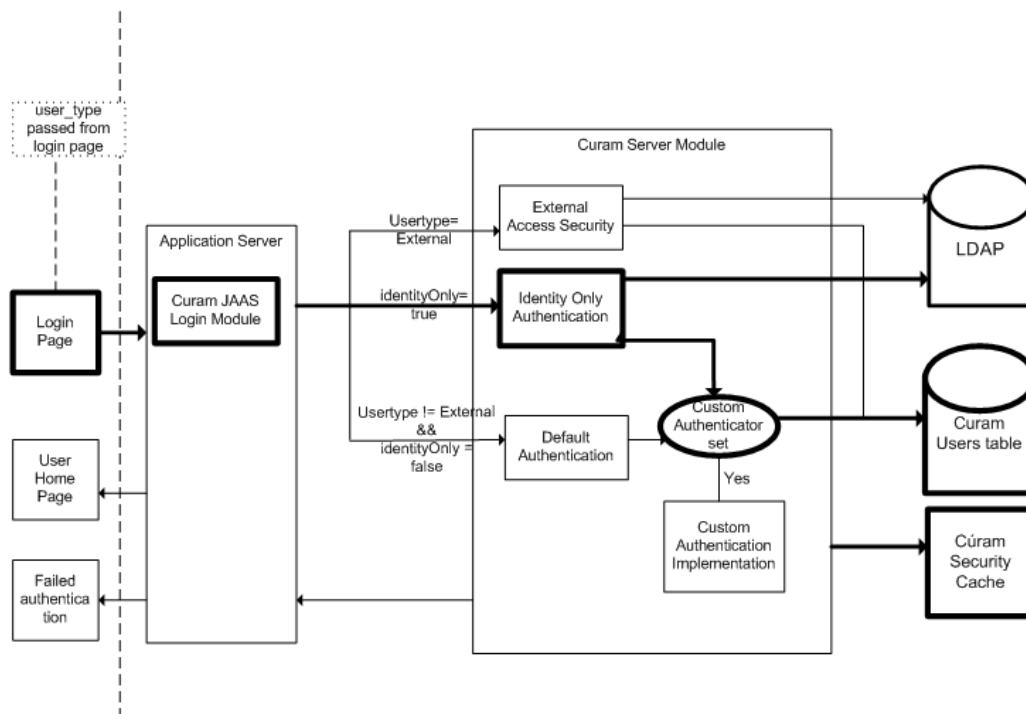


Figure 5. Identity Only Authentication

---

## 2.19 Customization of Identity Only Authentication

The identity-only implementation cannot be customized, but extra verifications can be added by implementing the custom authenticator. 2.21, “Custom Verifications” should be consulted for further details.

---

## 2.20 External Access Security Authentication

The architecture allows a developer to implement their own custom authentication solution for external users by providing a “hook” into the existing authentication and authorization infrastructure of the SDEJ.

To “hook” the custom solution into the application the `curam.util.security.PublicAccessUser` class must be extended, which requires implementing the `curam.util.security.ExternalAccessSecurity` interface. This class is used during the authentication and authorization process to determine required information relating to the External User. Chapter 13, “Customizing External User Applications,” on page 49 should be consulted for further details.

---

## 2.21 Custom Verifications

Support is provided for adding custom verifications to the authentication process e.g., a user may be required to answer a security question that must then be verified. The custom code, if implemented, is invoked after the relevant IBM Cúram Social Program Management verifications or identity assertion, and only if they have been successful.

After the custom verifications are invoked, the authentication process will update the relevant fields on the Users database table.

10.5, “Adding Custom Verifications to the Authentication Process,” on page 35 should be consulted for further details.





---

## Chapter 3. Authorization

---

### 3.1 Overview

In IBM Cúram Social Program Management the process of granting or refusing a user access to functional elements of an application is called authorization. The functional element can be anything to which a unique identifier can be attached, such as:

- a server process call,
- an element of the application that requires security checking, e.g. a series of registered welfare products.

Access to the functional element is controlled by a Security Identifier (SID) that forms part of the IBM Cúram Social Program Management authorization data. This data is linked to a user and can be configured through the Cúram Administration screens or through the Data Manager. The *Cúram Server Developer's Guide* should be consulted for further details.

The security data created for authorization is central to the processing performed during every client-server call, and it is important that access be optimized for performance reasons. The Cúram Security Cache is responsible for caching authorization data for a user. 5.2, "Cúram Security Cache," on page 23 should be consulted for further details.

The following sections describe the relationship for these authorization concepts and how this works within IBM Cúram Social Program Management.

---

### 3.2 Users, Roles and Groups

The security information associated with an application must first be organized into security profiles before it can be utilized in a runtime environment. A security profile consists of a security role, one or more security groups and the associations between security identifiers (SIDs) and securable elements of an application.

Every authorized user is assigned a security role during security configuration and these roles are associated with a number of security groups. Each security group is associated with a number of security identifiers. The security identifier represents the securable elements of IBM Cúram Social Program Management, e.g., a method or a field. The role, groups and identifier information is stored on the database in a number of tables and is configured using the application Data Manager or the Cúram Administration screens.

This data structure makes it possible to authorize every user against any secured element of an application. This is a powerful and flexible method of providing authorization to Cúram users.

There is a minimum set of SIDs required for a user to operate the Social Program Management Platform application. These SIDs are associated to the out-of-the-box BASESECURITYGROUP group. The `EJBServer/components/core/data/initial/handcraftedscripts/Supergroup.sql` file should be consulted to identify the list of these SIDs. This file is responsible for linking the SIDs to the BASESECURITYGROUP out-of-the-box.

A simple way to ensure that all users have the privileges from this set of SIDs is to create a single security group for them and then associate that security group with every security role in the system.

---

### 3.3 Security Identifiers (SIDs)

Every secured element in IBM Cúram Social Program Management is given a security identifier (SID) that is unique across the entire application.

The authorization process is built into the infrastructure and once the securable elements have been identified, the rest is handled by code generators, scripts and the Cúram Administration screens. The analysis of what elements must be securable is a manual process that must be done by the developer or security administrator. This section outlines the infrastructure available to set up authorization.

The first type of authorization to consider is that of the process method (facade) also known as *function-level security*. In the Cúram model, a developer may choose if security is switched on or off at the process method level. The option applies only to Business Process Objects (BPOs) since they encapsulate the calls exposed to the client. Entity object methods are not included in the authorization process.

There are a number of types of SIDs and these include:

- Function Identifiers (FIDs)
- Field Level Security Identifiers
- User defined SID types.

---

### 3.4 Function Identifiers (FIDs)

Function identifiers (FIDs) are a specialized type of security identifier (SID) where the type is set to FUNCTION. When a method is made publicly accessible (by setting the stereotype as facade in the model), a FID is generated for that method and security is automatically switched on.

It is possible to switch security off for a process method at design time. 11.11, “Switching Security off for a Process Method,” on page 40 should be referenced for further details on this.

---

### 3.5 Field Level Security Identifiers

The Field Level SID allows authorization to be applied to specific fields on a publicly accessible method. At runtime, if a user does not have access rights to view the field to be displayed, the contents of the field are displayed as a number of asterisks (\*\*). For more information on Field Level SIDs, the *Cúram Modeling Reference Guide* should be consulted.

---

### 3.6 User Defined SIDs

In the previous sections, we have described

**FIDs;** An automatically generated SID of type function.

**Field Level SID;**

Security applied to specific fields on a method.

There is also the concept of a user defined SID. The authorization process is sufficiently flexible to accommodate any securable element of an IBM Cúram Social Program Management application. The developer can effectively customize the authorization process by defining new *types* of SIDs. The new types represent a conceptual element requiring security. The following server interface method enables authorization to be invoked directly on these new user defined SID types.

```
curam.util.security.Authorisation.isSIDAuthorised()
```

Out-of-the-box, the LOCATION and PRODUCT SIDs are SIDs of this type. Using the above method there is effectively no limit to the SID types that can be defined. 11.14, “Authorizing New SID Types,” on page 41 should be consulted for further details.

---

### 3.7 Runtime Authorization

The IBM Cúram Social Program Management infrastructure performs authorization checks from both the web client and server side.

---

### 3.8 Client Authorization Checks

Before a user can access a method or field, the web client performs authorization checks before the page is initially loaded. If the user does not have access, the client authorization check fails, and the server is not invoked. This check is configurable in the `curam-config.xml` by setting the `SECURITY_CHECK_ON_PAGE_LOAD` property. Section 3.12.13 General Configuration in the *Cúram Web Client Reference Manual* should be consulted for further details on this.

By default any such web client authorization failures are not recorded. This behavior is configurable. 11.13, “Controlling the Logging of Authorization Failures for the Client,” on page 41 should be consulted for further details.

---

### 3.9 Server Authorization Checks

To cater for other access to IBM Cúram Social Program Management, and where the web client authorization check is disabled, there is a second level authorization check made by the server. This server side check will always log authorization failures, and the client property does not affect this logging.

The log of all authorization failures is stored on the database to allow these failures to be audited at a later stage. The `AuthorisationLog` table contains the User Name and Security Identifier for the failed authorization, as well as a timestamp indicating when the failure occurred. 11.15, “Analyzing the `AuthorisationLog` Database Table,” on page 42 should be consulted for further details on the `AuthorisationLog` table.



---

## Chapter 4. Cryptography in Cúram

---

### 4.1 Overview

In IBM Cúram Social Program Management cryptography refers broadly to two types of functionality related to keeping your Cúram systems safe and secure:

1. ciphers - for two-way encryption of passwords used at various processing points
2. digests - for one-way hashing (or digesting) of passwords; e.g. used at login

The values for configuring cryptographic behavior are user-selectable via a property file (`CryptoConfig.properties`) to provide you with the most control and security possible for your Cúram installation. This flexibility provides the capability to adjust to changing security standards. See Chapter 12, “Customizing Cryptography,” on page 43 for details on how to configure and customize cryptography.

For any IBM Cúram Social Program Management users migrating for the first time to a level of Cúram that has this level of cryptographic support, which was introduced in version 6.0.5.0, it is recommended that you upgrade system (new cipher) and user (new digest) passwords from the existing out-of-the-box (OOTB) defaults to improve your security.

Supported cryptographic configurations are:

1. AES: 128, 192, 256 (FIPS 140-2 and SP800-131a compliant);
2. Two-key Triple DES - DESede: 112 (FIPS 140-2 compliant);
3. Three-key Triple DES - DESede: 168 (FIPS 140-2 and SP800-131a compliant);
4. No cryptography configuration, which is configured by removing the `CryptoConfig.properties` file in which case Cúram will revert to its previous OOTB crypto settings.

In the environment where Cúram runs, the application server, database, and other software (e.g. web server, LDAP, etc.) will have its own cryptographic support and you should refer to the relevant vendor's documentation as is appropriate to you.

---

### 4.2 Cipherng

Cipherng refers to the process of encrypting passwords, which are listed in 4.7, “Cipher-Encrypted Passwords,” on page 21. That is, this is a two-way process representing decrypt-able values. There are about a dozen of these encrypted passwords in various property files in Cúram and encrypting them helps keep them secure and they are decrypted at the necessary points for usage; e.g. connecting to your database system.

---

### 4.3 Digesting

Digesting refers to the one-way process of handling passwords that do not require decrypting, but is used for storing passwords for later comparison; e.g. Cúram user logins. That is, this is a one-way process representing non-decryptable values.

---

### 4.4 Cryptography Properties

The Cúram `CryptoConfig.properties` file contains settings for cipher and digest cryptography. Therefore, this file and all the files it refers to (i.e., keystore and salt) should be considered critical items to the security of your system and should be provided with adequate access controls (e.g., file permissions) and specifically modified and segregated when used for production systems. That is, if the details of these

files were to become widely known, while not necessarily a security risk themselves, would remove a level of protection that might necessitate a disruptive crypto change (see 12.2, “Cipher Customization,” on page 43 and 12.5, “Digest Customization,” on page 45).

Related topics:

- 4.5, “Cúram Cipher Settings”
- 4.6, “Cúram Digest Settings,” on page 21

---

## 4.5 Cúram Cipher Settings

Various passwords within Cúram property files and configurations are stored in an encrypted format out-of-the-box (OOTB).

The Cúram crypto configuration will work for you out-of-the box, but it is recommended you modify these settings with respect to your local security requirements. For instance, the OOTB settings may be adequate in development, but for production environments it is strongly recommended that you modify them (e.g. by changing the cipher secret key).

The cipher settings are stored in the `CryptoConfig.properties` file. The properties and their values are as follows:

- `curam.security.crypto.cipher.algorithm`
  - **Valid values:** In JCE documentation, for example: <http://docs.oracle.com/javase/6/docs/technotes/guides/security/StandardNames.html#Cipher>. The supported ciphers are AES and the various forms of Triple DES.
  - **Default:** AES (FIPS 140-2 and SP800-131a compliant)
- `curam.security.crypto.superseded.cipher.algorithm`
  - **Valid values:** See `curam.security.crypto.cipher.algorithm`
  - **Default:** None
  - **Purpose:** Provides for flexibility to support an upgrade/migration period for Cúram user passwords with custom code (e.g. a batch program) via the `curam.util.security.EncryptionUtil.decryptSupersededPassword()` API. The use of an upgrade/migration period is explained in more detail in 12.7, “How to Utilize the Superseded Digest Settings for a Period of Migration,” on page 45.
- `curam.security.crypto.cipher.keystore.location`
  - **Valid values:** Path to keystore file containing secret key. This can be an absolute path specification or relative to the classpath (e.g. `CuramSample.keystore`).
  - **Default:** None
- `curam.security.crypto.cipher.keystore.storepass`
  - **Valid values:** As per the JDK **keytool** command.
  - **Default:** password
  - **Purpose:** Specify the password used to access the keystore.
- `curam.security.crypto.cipher.provider.class`
  - **Valid values:** Fully-qualified name of a JCE cryptography provider class.
  - **Default:** blank
  - **Purpose:** Optional way to enable the use of an alternate standards-compliant provider.

This ciphering functionality applies to the properties as described in 4.7, “Cipher-Encrypted Passwords,” on page 21.

These Cúram cryptographic settings are enabled by default OOTB and represents changes that existing Cúram installations must address as documented in the *Cúram Upgrade Guide*.

---

## 4.6 Cúram Digest Settings

Cúram users, internal and external, when not invoked with identity-only, are authenticated using form-based login and the password entered in the form is digested and compared to the digest value stored in the database for the user.

**Note:** This processing does not apply to users authenticated in third party systems like LDAP.

The Cúram crypto configuration will work for you out-of-the box, but it is recommended you modify these settings with respect to your local security requirements. For instance, the OOTB settings may be adequate in development, but for production environments it is strongly recommended that you modify them (e.g. digest salt encrypted value).

The digest settings are stored in the `CryptoConfig.properties` file. The properties and their values are as follows:

- `curam.security.crypto.digest.algorithm`
  - **Valid values:** In JCE documentation, for instance: <http://docs.oracle.com/javase/6/docs/technotes/guides/security/StandardNames.html#MessageDigest>. The supported digests are the SHA variants (1, 256, etc.) and MD5.
  - **Default:** SHA-256 (FIPS 140-2 and SP800-131a compliant)
  - **Purpose:** Specification of the digest algorithm.
- `curam.security.crypto.digest.salt.location`
  - **Valid values:** A path identifying the file containing the encrypted secret digest salt.
  - **Default:** None
  - **Purpose:** An optional file to specify the salt (encrypted) for digesting.
- `curam.security.crypto.digest.iterations`
  - **Valid values:** 0 or a positive integer.
  - **Default:** 0
  - **Purpose:** Typically, higher values give better security, but at the cost of processing (e.g. at login time).

There are a set of corresponding "superseded" properties to allow for flexibility when migrating from one set of digest settings or standards to another. The following have a similar function to their counterparts above, but are used by the Cúram encryption functionality to support both old and new settings for a time of migration:

- `curam.security.crypto.superseded.digest.algorithm`
- `curam.security.crypto.superseded.digest.salt.location`
- `curam.security.crypto.superseded.digest.iterations`

The usage and behavior of the superseded properties are controlled by the `curam.security.convertsupersededpassworddigests.enabled` property as managed by the Properties Administration user interface. See 12.7, "How to Utilize the Superseded Digest Settings for a Period of Migration," on page 45 for more information on using the superseded properties.

---

## 4.7 Cipher-Encrypted Passwords

The following passwords are cipher-encrypted in Cúram:

- `Bootstrap.properties`:
  - `curam.db.password` - database password
  - `curam.searchserver.sync.password` - see *Cúram Generic Search Server* for more information

- AppServer.properties: (typically this property file is used for configuring test servers and is not appropriate for production systems)
  - security.password - application server administration console password
  - curam.security.credentials.async.password - replacing the runas.password property
- Application.prx - individual property descriptions are as documented with the properties in the Curam Property Administration user interface:
  - curam.security.credentials.dbtojms.password - (in conjunction with curam.security.credentials.dbtojms.username), which replaces the curam.omega3.DBtoJMSCredentialsIntf interface APIs previously used to provide custom credentials for DB-TO-JMS
  - curam.security.credentials.ws.password (in conjunction with curam.security.credentials.ws.username), which replaces the build-time default web services default credential settings.
  - curam.meeting.request.reply.password - (an SMTP password)
  - curam.ldap.password
  - curam.citizenworkspace.password.protection.key
- BIBootstrap.properties - BIRT users only; see the *Cúram Business Intelligence BIRT Developer Guide*:
  - curamsource.db.password
  - central.db.password
  - centraldm.db.password
- Web Services - See the *Cúram Web Services Guide*:
  - ws\_inbound.xml - <ws\_service\_password>
  - services.xml - <parameter name="jndiPassword">
- CTM - Cúram Transport Manager:
  - The Password column of the TargetSystemService table contains an encrypted password



---

## Chapter 5. Security Data Caching

---

### 5.1 Overview

This chapter describes the Cúram Security Cache, which stores all authorization data for a user. Details on the WebSphere cache and how this affects the authentication of a user at login are also included in this chapter.

---

### 5.2 Cúram Security Cache

Security information from the database tables supporting the profiles mentioned in 3.2, “Users, Roles and Groups,” on page 15 is cached by the infrastructure. This is done to optimize the search and retrieval of data during the authorization process.

To optimize performance, the cache is loaded on demand as security authorization requests come into the application and is a shared resource. For application code, the cache is a protected resource and cannot be accessed directly. It is accessible, for queries only, through the authorization interface ( `curam.util.security.Authorisation` ) which allows a developer to implement a customized authorization procedure. 11.14, “Authorizing New SID Types,” on page 41 should be referenced for further details on this.

When the `curam.security.casesensitive` property is set to false the security cache will store all usernames in upper case and all queries to the cache will automatically change the specified username into the upper case equivalent. It is also worth noting that the existence of duplicate case insensitive usernames will cause a fatal error during the initialization of the security cache. 10.4, “Changing the Case-Sensitivity of the Username,” on page 35 should be consulted for further details on this.

---

### 5.3 Cache Refresh

As security data is so important to the operation of IBM Cúram Social Program Management, the cache must be refreshed whenever any changes have been made to security related database tables. The refreshing of the Cúram Security Cache is an asynchronous process.

---

### 5.4 Cache Refresh Failure

The refreshing of the Cúram Security Cache is triggered by either an application reboot, or by the system administrator (`sysadmin`) via the Cúram Administration screens, therefore, the administrator receives no feedback if the cache reload fails. Having to check the system logs or manually verify the application following a refresh to verify its success can be cumbersome. It is therefore recommended that the optional callback interface for providing feedback in the event of a cache reload failure be implemented. 10.8, “Adding the Cache Refresh Failure Callback Interface,” on page 36 should be consulted for further details.

---

### 5.5 WebSphere Caching Behavior

WebSphere caches user information and credentials in its own security cache. The Cúram login module will not be invoked while a user entry is valid in this cache. The default invalidation time for this security cache is ten minutes, where the user has been inactive for ten minutes.

For example, the first time a user logs into the application from the web client they will be requested for their username and password. The Cúram login module will be invoked, and will authenticate the information specified. If the same user opens a second new web browser and attempts to access the application, they will again be requested for their username and password. When WebSphere receives

this information it will query the security cache to determine if the username and password are already in the cache. If they are, and the password matches, WebSphere will not query the login modules.

The impact of this behavior is that any modifications to a user's account restrictions or password will not take effect until the user has been invalidated from the WebSphere security cache.

For more information see the appropriate *WebSphere Application Server Information Center*.

---

## Chapter 6. Security for Alternative Clients

---

### 6.1 Overview

There are processes that may not be associated with a specific logged in user. These include alternative clients, e.g. non-web processes such as batch processing, web services and deferred processing. As any process that interacts with a IBM Cúram Social Program Management application must be authenticated, a valid user must exist for each of these processes. The following sections provide details on the users that must exist on the Cúram Users table as well as details on the processes that depend on these users.

---

### 6.2 Mandatory Cúram Users

A number of users must always exist in the Cúram Users database table. These users are necessary for application processes such as deferred processing and workflow. If these users do not exist, then authentication will fail and subsequently these processes will fail.

The usernames and passwords for each of the processed below are the default out-of-the-box credentials and it is recommended that these credentials be changed for security reasons.

These users include:

- SYSTEM

The SYSTEM user is the user under which JMS messages are executed. This user must exist and the username is case sensitive. 6.5, “JMS Messaging,” on page 26 should be referenced for further details.

- DBTOJMS

The DBTOJMS user is the default user under which the Database to JMS (DBToJMS) trigger for batch processing is executed. This user must exist and the username is case sensitive. 6.4, “Batch Processing,” on page 26 should be referenced for further details.

- WEBSVCS

The WEBSVCS user is the default user under web services are executed. This user must exist and the username is case sensitive. 6.3, “Web Services” should be referenced for further details.

---

### 6.3 Web Services

For Apache Axis2 (the recommended implementation for web services) there are default credentials for authentication. A user has the ability to change these credentials at a global level or per service if required. To ensure that web services are not vulnerable to a security breach this default user is not authorized to access web services by default. For authorization, a web service must be associated with a security group and in turn a security role that is linked to the user (e.g. WEBSVCS) in order to access it. Ensuring the user is authorized is a manual process. Please see the *Customizing Receiver Runtime Functionality* section in the *Cúram Web Services Guide* for further details on web services and also the chapter on Authorization in this book.

For Apache Axis 1.4, i.e. legacy web services, once a process is modeled as a web service, this web service will automatically be logged into the application using default credentials. This default user is set up for authorization automatically, i.e. the user will have access to the web service created. Therefore caution is advised when making a class visible as a web service. Please see the *Legacy Inbound Web Services* section within the *Cúram Web Services Guide*.

There are a number of other topics related to the security of web services - for example, encrypting data - using Rampart. The *Cúram Web Services Guide* should be consulted for further details on these.

---

## 6.4 Batch Processing

Since the Batch Launcher does not require the application server to be running, it does not perform any application level authentication or authorization. It must only authenticate against the database. The same credentials as used by the application server (located in `%SERVER_DIR%/project/properties/Bootstrap.properties`) are used by the Batch Launcher to connect to the database and run batch programs.

The Batch Launcher or batch programs can optionally trigger the application server to begin a DB-to-JMS transfer. This involves logging in and invoking a method on the server, which in turn requires a valid username and password. By default the DB-to-JMS transfer operation uses default credentials; therefore, the DBTOJMS account must exist on the Cúram Users table and must be enabled and assigned the role 'SYSTEMROLE' to allow authorization. The locale DB-to-JMS transfer is the default locale for this user as specified in field 'defaultLocale' on the Users table.

The Security Considerations section in the *Cúram Batch Processing Guide* guide should be consulted for further details on changing the user for the DB-to-JMS transfer.

The property `batch.username` can be used to specify the user name for the operations run by the Batch Launcher. This is set using the `-D` parameter. For example: `build runbatch -Dbatch.username=admin`

---

## 6.5 JMS Messaging

JMS messages are used for communication purposes by deferred processes and Workflow. Since JMS messages are triggered by the application server and need to interact with the IBM Cúram Social Program Management application, valid Cúram credentials must exist. The SYSTEM user account must exist on the Cúram Users table and must be enabled and assigned the role 'SYSTEMROLE' to ensure authorization. The locale for JMS messages is the default locale for this user as specified in field 'defaultLocale' on the Users table.

It is possible to change the SYSTEM username during or after the deployment of the application. For more information the *Cúram Server Deployment Guide* for the relevant application server should be consulted.

---

## 6.6 Deferred Processing

A deferred process in IBM Cúram Social Program Management is a business method that is invoked asynchronously. As deferred processes interact with the application, valid Cúram credentials must exist. The SYSTEM user account must exist on the Cúram Users table and must be enabled and assigned the role 'SYSTEMROLE' to ensure authorization. The locale for deferred processes is the default locale for this user as specified in field 'defaultLocale' on the Users table. In the case of offline unit-testing of deferred processes, the username is blank and the effective locale is the default locale for the IBM Cúram Social Program Management server.

---

## Chapter 7. External User Applications

---

### 7.1 Overview

The IBM Cúram Social Program Management default, out-of-the-box application is enabled for internal users. Internal users are users that exist on the Cúram Users database table. A typical internal user would be a case worker who creates and manages claims for participants and has full access to the application. The infrastructure provides functionality for authenticating and authorizing these internal users.

There is also the concept of a user that needs to securely access parts of the IBM Cúram Social Program Management application. These users are outside the organisation. Their access is limited. These users are considered external users and authentication for these users is completely customizable through the use of the External Access Security hook point provided. As external users are processed differently to internal users, a specific web application is required for external users.

---

### 7.2 External User Applications

When developing an application for an external user, the following must be implemented:

- An external user client application, i.e., a separate EAR file containing the web client application.
- A custom `logon.jsp`, where the external application must pass in a parameter `user_type` indicating an external user is logging in.
- A custom class that extends `curam.util.security.PublicAccessUser`, which requires implementing the `curam.util.security.ExternalAccessSecurity` interface, must be provided. This abstract class contains methods responsible for the authentication and authorization of an external user.

As well as there being internal and external user types. There can also be different types of external users. For example, there may be an external user of type 'PUBLIC' who could have limited access to an external application. There could be another external user of type 'PROVIDER' who is a registered external user. The ability to have different types of external users provides more flexibility within an external application, allowing finer grained control over authentication of the external user based on the external user type.

---

### 7.3 User Scope

There are two different types, or scopes, of users within the IBM Cúram Social Program Management application: internal and external. The type of a user is determined in one of the following ways:

- By the Cúram Security Cache;  
If the user exists in the Cúram Security Cache, the type is assumed to be internal. If the user does not exist in the cache, the type is assumed to be external. In this case, (which is the default behavior) all usernames, internal and external, must be unique.
- By the UserScope custom interface;  
If the UserScope custom interface is implemented. This custom interface, takes precedence over the check for a user in the Cúram Security Cache to determine the user type. Consult 13.15, "Determining if a User is Internal or External using the UserScope Interface," on page 56 for further details.

When the type of a user is external the implementation of the `curam.util.security.ExternalAccessSecurity.getSecurityRole()` method will be used to determine the user role instead of the internal security roles. 13.8, "Authorizing an External User," on page 53 should be consulted for further details on this method.

To support alternative methods for determining if a user is internal or external the custom interface, `UserScope`, is available. Consult 13.15, “Determining if a User is Internal or External using the `UserScope` Interface,” on page 56 for more details.

---

## 7.4 Deployment of an External Application

When deploying an application to an application server, the security configuration for the application server is applicable to all IBM Cúram Social Program Management applications deployed to that application server instance. Therefore, care must be taken when considering the deployment architecture for more than one application. This is important when deciding if an internal and external application will be deployed to the same application server instance.

An example of some considerations to think about are:

- Is identity only being used for internal users?
- Is an alternative authentication mechanism used, e.g., LDAP?
- Will both internal and external users be authenticated by LDAP?

The answers to the considerations above will affect the setting of the application server properties (i.e. properties specified in the `AppServer.properties` file), that affect the behavior of the Cúram JAAS login module. These considerations will also drive the implementation of the `curam.util.security.PublicAccessUser` class and `curam.util.security.ExternalAccessSecurity` interface for external users.

The application server properties in the Cúram JAAS login module allow for finer grained control over the authentication of user types. External users and internal users can be authenticated differently, as can different types of external users, in a situation where the internal and external applications are deployed to the same application server. These properties include the following:

- `curam.security.user.registry.disabled.types` ;  
Set this property to a comma separated list of user types for which the application server user registry *will not* be queried, i.e. the implementation within the `PublicAccessUser.authenticate()` method is responsible for authenticating the external user of this type. For example, LDAP could be configured to be the user registry.
- `curam.security.user.registry.enabled.types`.  
Set this property to a comma separated list of user types for which the user registry *will* be queried, i.e., the implementation within the `PublicAccessUser.authenticate()` method does not have to fully authenticate the user. The user registry will be responsible for authenticating this type of external user. For example, LDAP could be configured as the user registry, and in this case, LDAP could be responsible for the authentication of these external user types.

These properties are dependent on the implementation of the `curam.util.security.PublicAccessUser` class and `ExternalAccessSecurity` interface.

Consider the following example project requirements:

- An internal user must authenticate with LDAP.
- An external user of type 'EXT\_PUBLIC' must authenticate with IBM Cúram Social Program Management and not LDAP;
- An external user of type, 'EXTERNAL' must authenticate with LDAP only and not IBM Cúram Social Program Management.
- Both the internal and external applications are deployed to the same application server instance.

The following settings could cater for the example above:

- `curam.security.check.identity.only` set to `true` ;
- `curam.security.user.registry.disabled.types=EXT_PUBLIC`.

As well as the properties being set, the `PublicAccessUser` extension (and `curam.util.security.ExternalAccessSecurity` implementation) must have the logic to cater for the different types of external users and how they will be authenticated.





---

## Chapter 8. Using Single Sign On

---

### 8.1 Overview

The number of applications in an enterprise often results in an increase in the number of usernames and passwords in use, resulting in poor user experience and additional cost of maintaining them. Multiple user names and passwords also compromise security as users either choose very simple passwords or write down their passwords in easy to find locations. For the system administrators additional applications result in an increased directory maintenance effort and fielding increased help desk calls to reset passwords. Some of the problems caused by additional applications can be resolved by using single sign-on functionality. Single sign-on (SSO) functionality allows users to access multiple secure applications by authenticating only once.

**Note:** Secure refers to applications that require users to be authenticated before accessing the functionality

Single sign on is supported for the supported application servers, by allowing alternative mechanisms to be used alongside the Cúram login module. The implementation of an SSO solution is the responsibility of the custom implementation. It is recommended that a third party tool be used, e.g. IBM Tivoli®™ or CA SiteMinder.

This chapter describes the application server properties that allows use of an SSO solution.

---

### 8.2 Single Sign On with WebSphere

When SSO is required with WebSphere, it can be achieved using the WebSphere lightweight third-party authentication mechanism (LTPA) and additional custom login modules. The LTPA protocol results in a token being created for an authenticated user. In WebSphere, a token is generated once credentials are added for an authenticated user. This token is then used to retrieve identity information for an authenticated user in an SSO environment.

Security is implemented as a Cúram login module within a chain of login modules set up in WebSphere. It is expected that at least one of these login modules be responsible for adding credentials for the user. By default, the Cúram login module adds credentials for an authenticated user. As a result of this, the configured WebSphere user registry handled by a subsequent login module does not add credentials. The recommended approach to implementing an SSO solution is to add a custom login module somewhere along the chain of login modules.

The ability to disable the addition of credentials for an unauthenticated user is provided, thus enabling an SSO solution to be implemented.

The Cúram JAAS login module for WebSphere checks if an LTPA token exists within WebSphere using the WSCredTokenCallbackImpl callback for WebSphere. If this token exists and is valid, then no authentication is performed by the Cúram login module.

Credentials may be added to the WebSphere user registry. Credentials include authentication information on the user logging in, including the unique identifier for the user. WebSphere checks that credentials exist for a user after all configured system login modules have executed, if the credentials exist, then the WebSphere user registry is not queried. Credentials are not added by the Cúram JAAS login module if the following settings are in place:

- `curam.security.check.identity.only` property is set to true.
- `curam.security.user.registry.enabled` property is set to true.

As mentioned in 7.4, “Deployment of an External Application,” on page 28, there are properties relating to the type of external user that control if credentials are added to WebSphere for a specific external user type. These include:

- `curam.security.user.registry.enabled.types` property.
- `curam.security.user.registry.disabled.types` property.

These properties provide fine grained control over authentication for external user types.

In the case where the Cúram JAAS login module does not add credentials, the WebSphere user registry will be queried to attempt to add credentials for the user.

---

## 8.3 Single Sign On for WebLogic Server

When SSO is required with WebLogic Server , it can be achieved by using the WebLogic Server authentication provider or a custom authentication provider. Consult the WebLogic Server documentation for further information on authentication providers. WebLogic Server expects credentials/principals and the group the user belongs to, to be added by the configured authentication provider. For an SSO solution the Cúram JAAS login module does not add credentials to the JAAS subject to allow for an alternative authentication provider to be responsible for adding credentials.

Credentials are not added if the following settings are in place:

- `curam.security.check.identity.only` is set to true.
- `curam.security.user.registry.enabled` is set to true.

As mentioned in 7.4, “Deployment of an External Application,” on page 28, there are properties relating to the type of external user that control if credentials are added to WebLogic Server for a specific external user type. These include:

- `curam.security.user.registry.enabled.types` property.
- `curam.security.user.registry.disabled.types` property.

These properties provide fine grained control over authentication for external user types.

The responsibility for adding credentials is left to another authentication provider, i.e., the main authentication provider for authenticating the user. In an SSO scenario, only one of the authentication providers needs to add credentials to the JAAS subject during the `commit()` method of the login module for a user

---

## Chapter 9. Other Security Considerations

---

### 9.1 Overview

Another important security concern is protecting content as it is entered, displayed and transferred across the network for the IBM Cúram Social Program Management application. The default configuration uses SSL provided by the application server to secure content as it is transferred.

In addition to this, during the development lifecycle, industry leading products are used to regularly monitor for security vulnerabilities in the application. Examples of such potential vulnerabilities include: cross site scripting, and SQL injection. Such threats are resolved within the infrastructure when discovered.

It is recommended that customers perform similar security monitoring of their application.

---

### 9.2 SSL Settings for the Application

SSL is on by default for access to the web application. This ensures a secure SSL connection between the client and server and also ensures data is encrypted. SSL is turned on for the client through settings in the `web.xml` file for the web client application. SSL is turned on at the application server level by settings in WebLogic Server and WebSphere . These settings for the application servers are done through the IBM Cúram Social Program Management configuration scripts.

**Important:** The configuration scripts ensure SSL is turned on by default, however, this is a default configuration that must be updated and new certificates must be established for the SSL protocol.

It is recommended to leave SSL on for access to the IBM Cúram Social Program Management application, however depending on specific project configurations, there may be a need to turn SSL off for the application.

It is possible, but not recommended to turn off SSL. 10.9, "Turning Off SSL Settings for the Application," on page 36 should be consulted for further details.

---

### 9.3 Using Cúram in a Secure Environment

Cúram can be used in a secure server environment (e.g. FIPS-compliant) and is dependent on the requirements and capabilities of that environment (e.g. Websphere FIPS configuration). However there are a few specific areas where Cúram-specific or related operation or configuration is required:

- When using the DB-to-JMS feature, which is enabled via the `curam.batchlauncher.dbtojms.notification.ssl` property, described in the *Cúram Batch Processing Guide*
- When using the Word Integration Control, used for the FILE\_EDIT widget, documented in the *Cúram Web Client Reference Manual*, which has two aspects to consider:
  - When needing to use it with a browser in a TLS v1.2 environment, which is discussed in the "User Machine Configuration" topic of the *Cúram Web Client Reference Manual*.
  - The SP800-131a-compliant version of the supporting jar file can be used as long as your browser JVM supports SHA2, regardless of whether the server environment supports SP800-131a. To digitally sign the Word Integration jar for SP800-131a compliance you must build your environment using the `enable-sha-2-signed-jars` property (e.g. `-Denable-sha-2-signed-jars=true`) when invoking the Cúram build targets (e.g. `server`, `client`, `websphereEAR`).



---

## Chapter 10. Customizing Authentication

---

### 10.1 Customizing the Login Page

The default out-of-box login screen is represented by the `logon.jsp` file located in the `lib/curam/web/jsp` directory of the Client Development Environment for Java (CDEJ). The `logon.jsp` file can be customized by creating a copy of the out-of-the-box file and placing this in a `webclient/components/<custom>/WebContent` folder, where `<custom>` represents the name of the custom web client component.

The section on Login Pages in the *Cúram Web Client Reference Manual* has guidelines on what needs to remain in place in the `logon.jsp` file and should be referenced for further details.

---

### 10.2 Applying Styling to the Login Page

Styling changes can be applied to the `logon.jsp` in the usual way, i.e., by adding the relevant CSS to any `.css` file in the custom component. The *Cúram Web Client Reference Manual* should be consulted for details on styling.

---

### 10.3 Enabling Usernames With Extended Characters for WebLogic Server

If the WebLogic Server application server is not being used, this section can be ignored.

In the event that you have Cúram user names or passwords with extended characters (e.g. "üßer") WebLogic Server provides a proprietary attribute, `j_character_encoding`, which must be added to the `logon.jsp` form-based login page. The WebLogic Server documentation should be consulted for more information. The attribute must be added to the table element in the `logon.jsp` file, as illustrated below: 10.3, "Enabling Usernames With Extended Characters for WebLogic Server."

```
<input type="hidden" name="j_character_encoding" value="UTF-8"/>
```

*Figure 6. WebLogic Server Support for Logins With Extended Characters*

---

### 10.4 Changing the Case-Sensitivity of the Username

The `curam.security.casesensitive` property controls the case sensitivity of usernames. By default, this is set to `true` in the `Application.prx` file. When set to `false` in the `Application.prx` file, this will result in the authentication and authorization mechanisms ignoring the case of the username.

The *Cúram Configuration Settings* chapter in the *Cúram Server Developer's Guide* should be consulted for further details on the `Application.prx` file.

---

### 10.5 Adding Custom Verifications to the Authentication Process

To add custom verifications, the `curam.util.security.CustomAuthenticator` interface must be implemented. This interface contains one method - `authenticateUser()`. The `authenticateUser()` method is invoked for both default authentication and identity only authentication. The results of this method are expected to be an entry from the `curam.util.codetable.SECURITYSTATUS` codetable. In the case of successful authentication, the result must be `curam.util.codetable.SECURITYSTATUS.LOGIN`

For authentication failures anything, including null, can be returned. It is recommended though that another code from the `curam.util.codetable.SECURITYSTATUS` codetable be used. This codetable can be extended to include custom codes as detailed in the chapter on Code Tables in the *Cúram Server Developer's Guide*.

After the custom verifications are invoked, the authentication process will update the relevant fields on the Users database table. For example, if the result of the customized verifications is not `SECURITYSTATUS.LOGIN` the number of login failures is increased by 1, and if the break-in threshold is reached, the account will be disabled. Alternatively, if the result is `SECURITYSTATUS.LOGIN`, the login failures are reset to 0 and the last successful login field is updated.

**Note:** When identity-only authentication is enabled the fields of the Users database table are not updated, irrespective of the result of the custom verification.

---

## 10.6 Configuring the Custom Authenticator

To configure the application to use this custom extension, the property `curam.custom.authentication.implementation` in the `Application.prx` must be set to the fully qualified name of the class implementing the `CustomAuthenticator` interface.

The *Cúram Configuration Settings* chapter in the *Cúram Server Developer's Guide* should be consulted for further details on the `Application.prx` file.

---

## 10.7 Configuring Identity Only Authentication

To configure identity-only authentication the `curam.security.check.identity.only` property should be set to true in the `AppServer.properties` file before running the **configure** target. It is also possible to set this property once the application is deployed through the application server console. For more information on configuring the application server the *Cúram Server Deployment Guides* for the application server being used should be consulted.

---

## 10.8 Adding the Cache Refresh Failure Callback Interface

The new callback class must implement the interface: `curam.util.security.SecurityCacheFailureCallback` in a class that has a public default constructor. The implementation of the callback is registered by setting the application property `curam.security.cache.failure.callback` to the name of the implementation class. If the property is not set, no attempt is made to invoke a callback handler.

---

## 10.9 Turning Off SSL Settings for the Application

SSL is on by default for access to the IBM Cúram Social Program Management application. This ensures a secure SSL connection between the client and server and also ensures data is encrypted. SSL can be turned on and off for the client through settings in the `web.xml` file for the web client application, and at the application server level by settings in WebLogic Server and WebSphere. These settings for the application servers are configured via the configuration scripts. It is recommended to leave SSL on for access to the application, however depending on specific project configurations, there may be a need to turn SSL off for the application. The following sections detail how to do this.

---

## 10.10 Modifying the web.xml File for the Client Application

This can be modified by changing the `<transport-guarantee>` from `CONFIDENTIAL` to `NONE` in the `web.xml` file. Note, this does not disable access to the web client over HTTPS, but enables additional access via HTTP. For further details on modifying the `web.xml` file, the section on *Customizing the Web Application Descriptor* in the *Cúram Web Client Reference Manual* should be referenced. An example of setting this

property is below:

```
<user-data-constraint>  
  <transport-guarantee>NONE</transport-guarantee>  
</user-data-constraint>
```

---

## 10.11 Modifying the Application Server Configuration

Modifying the configuration for WebSphere can be done in one of two ways. The first approach below being the recommended approach.

- Use the existing non-secure port, setup by default for Web Services (recommended approach). This caters for both SSL and non-SSL connections.
  1. Navigate to Environment -> Virtual Hosts -> client\_host->Host aliases
  2. Click New and enter \* for host name and 9082 for port number, then click OK
  3. On the next page click Save to store your new value to the server configuration. Please note that the port 9082 corresponds to the *CuramWebServicesChain* configured in the default client application and this port is now the port that can be used to access the application using HTTP
- Reuse the current SSL port of 9044 :

The current port can be set up as a non-secure port. The steps to do this are described in the *Cúram Deployment Guide for WebSphere Application Server* - Section A.2.11 Server Configuration - Set up port access. Follow Steps 7 to 11 inclusive. The only difference for Step 11, is that that the Transport Chain Template should be set to 'WebContainer' (and not WebContainer Secure).

---

## 10.12 Analyzing the AuthenticationLog Database Table

All authentication attempts (both successes and failures) are logged in the AuthenticationLog database table. The following are the rows of interest on this table:

Table 1. Contents of the Authentication Log

| Field         | Meaning  |
|---------------|--|
| timeEntered   | The timestamp of the entry in the log.   |
| userName      | The username associated with the login attempt.  |
| altLogin      | Boolean indication of whether the username represents an alternate Login ID. When this column equals '1' (true) the value in the userName column is an alternate login ID as per 2.5, "Alternate Login IDs," on page 5; otherwise, the userName column represents the userName from the Users or ExternalUser table. |
| loginFailures | The number of login failures for this user since their last successful login.  |
| lastLogin     | The date and time of the last successful login.  |

Table 1. Contents of the Authentication Log (continued)

| Field       | Meaning   |
|-------------|---|
| loginStatus | <p>The status of the login attempt. This may be one of:</p> <ul style="list-style-type: none"> <li>• LOGIN: Successful login.</li> <li>• ACCDISABLE: The account has been explicitly disabled.</li> <li>• ACCEXPRED: The password expiry date has been reached.</li> <li>• PWDEXPIRED: The number of days which the user was given to change their password has been exceeded.</li> <li>• BADUSER: The user does not exist.</li> <li>• AUTHONLY: This is used in the case of identity only authentication and indicates that only authorization verifications will be performed.</li> <li>• BADPWD: The specified password was incorrect.</li> <li>• BREAKIN: A specified number of incorrect passwords has been reached. The account is disabled.</li> <li>• RESTRICTED: The user is not allowed access the system at this time.</li> <li>• LOGEXPR: The number of login attempts which the user was given to change their password has been exceeded.</li> <li>• AMBIGUOUS: The specified username is ambiguous as it is a case insensitive duplicate of another username.</li> </ul> |

The LogAdmin API can be used to query the AuthenticationLog database table. The Java documentation for this class should be referenced for further details.



---

## Chapter 11. Customizing Authorization

---

### 11.1 Overview

This chapter details how to set up authorization for users.

---

### 11.2 Creating Authorization Data Mapping

The authorization data for a user can be set up through the use of the Data Manager (DMX files) or through the Cúram Administration screens. The *Cúram System Configuration Guide* should be consulted for details on identifying how to group security from a business perspective.

To create a new security role for a user, the security identifiers (SIDs) that the user must have access to, need to be identified. These SIDs should then be organized into groups of SIDs. The role, groups and SIDs, once identified, need to be set up on the security tables that these represent.

Security data is considered essential for the set up of a IBM Cúram Social Program Management application. As such, the examples below describe adding security data to the data/initial directory within the component.

---

### 11.3 Creating a New Security Role

To create a new security role, a new entry must be added to the SecurityRole database table, setting the rolename attribute.

To do this, create/add to the SecurityRole.dmx file in the %SERVER\_DIR%/components/<custom>/data/initial , where <custom> is any new directory created under components that conforms to the same directory structure as components/core.

---

### 11.4 Creating a New Security Group

To create a new security group, a new entry must be added to the SecurityGroup database table setting the groupname attribute.

To do this, create/add to the SecurityGroup.dmx file in the %SERVER\_DIR%/components/<custom>/data/initial , where <custom> is any new directory created under components that conforms to the same directory structure as components/core.

---

### 11.5 Linking the Security Group to the Security Role

The security role must be linked to the security group. To do this, create a new entry in the SecurityRoleGroup table, setting the rolename and groupname attributes.

To do this, create/add to the SecurityRoleGroup.dmx file in the %SERVER\_DIR%/components/<custom>/data/initial , where <custom> is any new directory created under components that conforms to the same directory structure as components/core.

---

### 11.6 Creating the Security Identifier (SID)

To create a new SID, an entry must be added to the SecurityIdentifier table, setting the sidname and sidtype attributes.

To do this, create/add to the SecurityIdentifier.dmx file in the %SERVER\_DIR%/components/<custom>/data/initial , where <custom> is any new directory created under components that conforms to the same directory structure as components/core.

---

## 11.7 Linking the Security Group to the SID

To link the security group with the SID, an entry must be added to the SecurityGroupSID table, setting the groupname and sidname attributes.

To do this, create/add to the SecurityGroupSID.dmx file in the %SERVER\_DIR%/components/<custom>/data/initial , where <custom> is any new directory created under components that conforms to the same directory structure as components/core.

---

## 11.8 Linking the Security Role to the User

To associate authorization data to a user, the security role must be linked to the user.

To do this, update the entry for the specified user in the Users.dmx file located in the %SERVER\_DIR%/components/<custom>/data/initial , where <custom> is any new directory created under components that conforms to the same directory structure as components/core , setting the rolename attribute to be the rolename as specified on the SecurityRole table.

---

## 11.9 Loading Security Information onto the Database

Once all of the information has been entered in the various DMX files, the Data Manager should be used to load the DMX data onto the database. The *Data Manager* chapter in the *Cúram Server Developer's Guide* should be consulted for further details.

---

## 11.10 Creating Function Identifiers (FIDs)

When a method is made publicly accessible; by setting the stereotype to be <<facade>>, security is automatically switched on. This means a SID is automatically generated for that method and the security enabled flag for the method is set to true . The SID and its fidenabled flag are stored in the database-independent <ProjectName>\_Fids.xml file located in the /build/svr/gen/ddl subdirectory. This file is used to insert the FID information onto the database via the Data Manager.

A FID follows the naming convention of <classname>.<methodname> , and the maximum length of a FID is 100 characters. For example, for a BPO called ProductEligibility , with two methods called insertProduct and testProduct , two FIDs are created: ProductEligibility.insertProduct and ProductEligibility.testProduct.

If security for a process method is switched off at design time in the model, a SID/FID is still generated but the security enabled flag is set to false . Setting the security enabled flag to false means that no authorization check is performed for this method.

---

## 11.11 Switching Security off for a Process Method

Setting the Generate\_Security option on the process method to false in the model switches off security for a process method.

If security for a process method is switched off at design time in the model, a FID is still generated but the security enabled flag is set to false . Setting the security enabled flag to false means that no authorization check is performed for this method.

---

## 11.12 Security Considerations During Development

It is important to consider the effect of these design options when implementing security during the development of a IBM Cúram Social Program Management application. They are the first and last line of defense against unauthorized access to application process functionality. Generally speaking, security will be switched on for almost all process methods. Security may be switched off for a process method that does not need security, e.g., a login method that gets invoked when a user tries to login to an application. As a user has not yet been authenticated or authorized, they need access to this method in order to login, therefore switching off security for this method may be necessary.

During the initial design phase of an application the overhead of keeping the security environment “in sync” with an evolving application can be tedious. It is possible to disable the authorization check by setting the `curam.security.disable.authorisation` property in the `Application.prx` file.

### **warning: Warning**

The `curam.security.disable.authorisation` property should only be turned on at design phase. This should never be set to true in a production environment.

Finally, it should be noted that once the code and scripts have been generated from a working model, the information associated with a FID cannot be changed. To change this information requires modifying the model, re-generating and re-building the database.

---

## 11.13 Controlling the Logging of Authorization Failures for the Client

By default, web client authorization failures are not recorded.

The `curam.enable.logging.client.authcheck` property controls whether the authorization failures encountered by the web client are logged or not. This property is false by default, meaning these failures will not be logged. When set to true a log of these authorization failures is stored on the database table `AuthorisationLog`. The *Cúram Server Developers Guide*, `Application.prx` - Dynamic properties section should be consulted for more information on this property.

---

## 11.14 Authorizing New SID Types

A server interface method is provided to enable authorization to be performed directly. This method may be added to a class that manipulates data on the conceptual element being secured by the new SID type.

```
curam.util.security.Authorisation.isSIDAuthorised()
```

A usage example of this method is below:

```

// The SID associated with the conceptual element
// to be secured.
String someSID = "someSID";

// Get the logged in username
String loggedUser =
    curam.util.transaction.TransactionInfo.getProgramUser();

// Check if the user has access rights
if (curam.util.security.Authorisation.isSIDAuthorised(
    someSID, loggedUser)) {
    // Do something sensitive that this user has rights to do
    ...
} else {
    // Throw an exception indicating the user doesn't have
    // access to perform this action
    ApplicationException exception
        = new ApplicationException(MESSAGE.ERR_USER_NO_ACCESS);
    throw exception;
}

```

Figure 7. Example Usage of `isSIDAuthorised()`

---

## 11.15 Analyzing the AuthorisationLog Database Table

All authorization failures are logged in a database table called the AuthorisationLog. The following are the rows of interest on this table:

Table 2. Contents of the Authorization Log

| Field          | Meaning   |
|----------------|---|
| timeEntered    | The timestamp of the entry in the log.  |
| userName       | The username associated with the authorization attempt.                                   |
| identifierName | The security identifier (SID) or functional identifier (FID) associated with the failure. |

The LogAdmin API can be used to query the AuthorisationLog database table. The Java documentation for this class should be referenced for further details.

---

## Chapter 12. Customizing Cryptography

---

### 12.1 Overview

This chapter details how to configure and customize cryptography for IBM Cúram Social Program Management.

---

### 12.2 Cipher Customization

Modification of the default cipher settings is a relatively straightforward process, but needs to be adequately planned and tested. You will require an application restart for the changes to be implemented and depending on the size and topology of your organization and deployments you need to choose a time when in-progress changes won't be an impact. Also, consider any data (e.g., properties containing encrypted passwords) managed by the Cúram Transport Manager (CTM) that will either need to be updated or managed to prevent systems from being out of sync with one another (see the *Cúram Transport Manager Guide* for more information).

Modification of the default cipher settings involves the following steps:

1. Choosing new settings for the `CryptoConfig.properties` and underlying artifacts - see 4.5, "Cúram Cipher Settings," on page 20
2. Depending on the settings, you may need to perform additional steps (e.g. when modifying the keystore as per 12.4, "How to Create a New Keystore," on page 44).
3. Modify the `CryptoConfig.properties` file; note the default location is `<SERVER_DIR>/project/properties`.
4. Remove any existing `CryptoConfig.jar` files (these contain `CryptoConfig.properties`) that are found in the `<JAVA_HOME>/jre/lib/ext` directory (`$JAVA_HOME/lib/ext` on IBM z/OS®). If any Cúram clients or servers are running these will need to be terminated in order to be able to deploy an updated `CryptoConfig.jar` file with the updated settings.
5. Re-encrypt the passwords in all existing property files as identified in 4.7, "Cipher-Encrypted Passwords," on page 21. The Apache Ant `configtest`, `configure`, and `installapp` targets will place an updated `CryptoConfig.jar` file in the `Java lib/ext` directory.
6. Test and verify your changes.

Testing of your changes should include verifying any functionality that would be impacted; for example:

- Ensure the Ant `configtest` target still works.
- Ensure batch programs still work.
- If you utilize the Ant `configure` target ensure it still works.

Related topics:

- 4.6, "Cúram Digest Settings," on page 21
- 4.7, "Cipher-Encrypted Passwords," on page 21

---

### 12.3 Key Management

The management of the secret key for Cúram encrypted passwords is done via the JDK-provided **keytool** command, or equivalent. You will need to make local decisions about placement and isolation of the secret key for Cúram that are compatible with your local organization and standards.

Keep in mind that some settings passed to the **keytool** command need to be reflected in the `CryptoConfig.properties` settings, which needs to be coordinated for successful deployment as discussed in 12.2, “Cipher Customization,” on page 43. The following table shows the relationship between **keytool** command arguments and the Curam crypto properties.

Table 3. Relationship of keytool Command Arguments to Curam Crypto Properties

| Keytool argument | CryptoConfig.properties property                   |
|------------------|--|
| -keyalg          | curam.security.crypto.cipher.algorithm             |
| -alias           | curam.security.crypto.cipher.keystore.seckey.alias |
| -keystore        | curam.security.crypto.cipher.keystore.location     |
| -storepass       | curam.security.crypto.cipher.keystore.storepass    |

**Note:** The secret key password defaults to the storepass password and should not be changed.

See the JDK documentation for more information on using the **keytool** command.

Related topics:

- 4.5, “Curam Cipher Settings,” on page 20
- 4.4, “Cryptography Properties,” on page 19
- 12.4, “How to Create a New Keystore”

---

## 12.4 How to Create a New Keystore

Creating a new keystore to replace the Curam default requires running the **keytool** command provided with the JDK (or equivalent), modifying the `CryptoConfig.properties` settings to correspond (necessary, only if the keystore name and/or location is changed from the default, but changing the name can make your customizations more obvious), and ensure the Curam Ant targets can find the new keystore (necessary, only if the default location is changed).

For example:

```
keytool -genseckey -v -alias MySecretKey -keyalg AES -keysize 128 -keystore MyOrganization.keystore -storepass secretpw -s
```

The section 12.3, “Key Management,” on page 43 identifies the **keytool** command arguments that relate to the `CryptoConfig.properties` settings.

The default location of the keystore file is the `<SERVER_DIR>/project/properties` directory with a sub-directory structure that reflects the JDK in use: “ibm” for the IBM JDK and “sun” for the Oracle JDK. So, when creating a keystore file the Curam build scripts expect to find it in the case of the IBM JDK in: `<SERVER_DIR>/project/properties/ibm`. If you desire to use a location different from the default you can do one of two things:

1. Use an absolute location for the keystore file as described in 4.4, “Cryptography Properties,” on page 19. In this case the Curam default keystore files in `CryptoConfig.jar` will be ignored in favor of the absolute setting `CryptoConfig.properties`.
2. Use the Ant `crypto.prop.file.location` property when you run any of the targets, described in 12.2, “Cipher Customization,” on page 43, that create and copy the `CryptoConfig.jar` to point to your alternate location. The location specified will have to reflect the structure of your JDK - “ibm” or “sun”. For instance:
  - Place the new keystore file in a location like this on Windows for the IBM JDK:  
C:\Curam\keystore\ibm\MyOrganization.keystore
  - Point to that location when running the build targets: `ant configure -Dcrypto.prop.file.location=C:\Curam\keystore`

**Note:** In the example above the change of keystore file name to `MyOrganization.keystore` will require a corresponding change to `CryptoConfig.properties` as per 4.4, “Cryptography Properties,” on page 19.

**Note:** The only supported keystore type for Cúram cryptography is `jceks`.

Following the keystore creation you need to follow the steps in 12.2, “Cipher Customization,” on page 43.

Related topics:

- 12.3, “Key Management,” on page 43
- 12.2, “Cipher Customization,” on page 43

---

## 12.5 Digest Customization

Modification of the default digest settings is a relatively straightforward process, but needs to be adequately planned and tested. You will require an application restart for the changes to be implemented and depending on the size and topology of your organization and deployments you need to choose a time when in-progress changes won't be an impact. Also, consider any data (e.g., User passwords) managed by the Cúram Transport Manager (CTM) that will either need to be updated or managed to prevent systems from being out of sync with one another (see the *Cúram Transport Manager Guide* for more information).

The process is covered in detail in 12.7, “How to Utilize the Superseded Digest Settings for a Period of Migration.”

Related topics:

- 4.6, “Cúram Digest Settings,” on page 21
- 12.6, “How to Specify a Digest Salt”

---

## 12.6 How to Specify a Digest Salt

While Cúram doesn't specify one out-of-the-box, specifying a salt for digested passwords provides an additional level of protection against brute-force attacks.

To specify a salt for your digested passwords:

1. Choose a sufficiently long and random string.
2. Encrypt this string using the Ant **encrypt** target (as documented in the *Cúram Server Developer's Guide*).
3. Place the encrypted string in a file.
4. Specify the location of the file containing the encrypted salt string using the `curam.security.crypto.digest.salt.location` property in `CryptoConfig.properties` and ensure that any deployed `CryptoConfig.jar` files reflect the updated settings.

For manageability you should make these changes in conjunction with the steps in 12.7, “How to Utilize the Superseded Digest Settings for a Period of Migration.”

---

## 12.7 How to Utilize the Superseded Digest Settings for a Period of Migration

Utilizing the superseded digest settings means you are migrating your existing digested passwords to a new crypto configuration (e.g. new salt) and would like Cúram user passwords automatically migrated for a period of time. This applies to Cúram internal and external users, but does not apply to users managed by third-party security systems such as LDAP.

The process to do this is:

1. Choose a time when your Cúram system can be down and with the Cúram system not running.
2. Copy the existing digest property names and values in `CryptoConfig.properties` and rename the properties to the new superseded property names.
3. Modify the existing digest property names in `CryptoConfig.properties`.
4. Set the `curam.security.convertsupersededpassworddigests.enabled` property to 'true'.
5. Set the `curam.security.crypto.upgrade.start` property to help you track when you introduced the updated configuration. This value can be used below to help manage unmigrated user passwords.
6. Restart the application server, but note the following.

**Note:** The Cúram default web services user (WEBSVCS), or any user not processed via the `CuramLoginModule`, is not available for automatic password migration. You must reset these users before restarting the application server. To do this:

1. Obtain the new digest password value via the Ant digest target (e.g. `ant digest -Dpassword=password`).
2. Update the password value in the database, which is easily done via SQL (e.g. `UPDATE USERS SET PASSWORD='<new digest value>' WHERE USERNAME='WEBSVCS';`).
3. You can now start the application server

After a period of time (e.g. weeks or months) when you consider the migration period to be over set the `curam.security.convertsupersededpassworddigests.enabled` property to 'false' and unset the `curam.security.crypto.upgrade.start` property.

Users who did not login during the migration period will now see their logins fail due to password mismatches. You have two approaches for addressing the passwords not updated during the migration period:

1. Require these users to contact your internal support to have their password reset via the admin user interface.
2. Manually identify the users in the Cúram USERS table who were not updated during the migration period and either manually set new default password either via SQL (see the **digest** target described in the *Cúram Server Developer's Guide* to obtain new digest password values) or via the admin user screens. For example, using the following query: `SELECT username FROM users WHERE lastwritten between timestamp('2013-06-01 15:00:00') AND timestamp('2013-09-01 00:00:00')`

You should not leave `curam.security.convertsupersededpassworddigests.enabled` set to true indefinitely because:

1. It's meaningless to have gone to the trouble of upgrading from configuration 'A' to configuration 'B' and leave the original 'A' configuration active;
2. It leaves potentially weaker crypto settings active in the system; and
3. In order to use this functionality for a future upgrade, say from configuration 'B' to 'C', you would have to have upgraded all the 'A' passwords to at least 'B'.

**Note:** Any files, e.g. DMX, with stored digests need to be considered with respect to your migration strategy so they reflect the correct values.

**Note:** Any use of the Cúram Transport Manager (CTM) during a migration needs to be considered in terms of ensuring compatible settings and expectations between the source and target systems.

Related topics:

- 4.5, "Cúram Cipher Settings," on page 20
- 4.6, "Cúram Digest Settings," on page 21



---

## 12.8 Modifying Your Crypto Configuration for a Production System

While the out-of-the-box (OOTB) crypto settings are adequate for typical development or test environments, they should be modified for production environments to protect and provide isolation between these relatively low-risk environments and high-risk production environments.

Some typical changes to the OOTB crypto configuration, in preparation for production, might include:

- Providing a new secret key.
  - Such a key can be generated using the JDK keytool utility; see 12.4, “How to Create a New Keystore,” on page 44
  - This secret key should be stored in a separate keystore.
  - The properties for these secret key changes would be as described in 12.3, “Key Management,” on page 43.
- Providing new digest settings
  - New digest settings can include a new salt, iteration count, and/or algorithm.
  - The properties for these digest changes would be as described in 4.6, “Cúram Digest Settings,” on page 21 and 12.6, “How to Specify a Digest Salt,” on page 45 and the process described in 12.7, “How to Utilize the Superseded Digest Settings for a Period of Migration,” on page 45.

Remember to keep your configuration files isolated from personnel who do not absolutely have to access; specifically, keeping development, test, and production configuration information isolated.



---

## Chapter 13. Customizing External User Applications

---

### 13.1 Overview

As external users are processed differently to internal users, a separate IBM Cúram Social Program Managementweb application is required specifically for external users.

---

### 13.2 Creating an External User Application

A new web client application must be developed for external users. The *Cúram Web Client Reference Manual* should be consulted for details on creating a new web client application.

---

### 13.3 Creating an External User Client Login Page

A new logon.jsp must be created for an external user application. The Social Program Management Platform ships with a default login page, logon.jsp, located in the lib/curam/web/jsp directory of the CDEJ (Client Development Environment for Java). This file should be copied to a webclient/components/<custom component>/WebContent folder in the web client application and modified as follows:

The table element should be extended to include a hidden input field user\_type:

```
<input type="hidden" name="user_type"
      value="EXTERNAL"/>
```

Where EXTERNAL indicates the type of external user. This can be set to any value, excluding INTERNAL.

---

### 13.4 Creating an External User Client Automatic Login Page

Some external user client applications require no user authentication and hence a username and password should not be requested. It is not possible to disable authentication in IBM Cúram Social Program Management, so the best way to achieve this requirement is to write an automatic login script.

The automatic login script takes a hard coded username and password and provides that as the authentication information when requested. This means that all users for such an application will always execute under the same username. Use of such a script should be limited to true open access applications.

When implementing applications that have a need for an automatic login, the implications for session management must be considered. Session management in IBM Cúram Social Program Management maintains a user's session information to ensure when the user logs back in, the relevant session information, i.e., their tabs and navigation opens to where they left off for them. In the case of a user that has been automatically logged in, this information must not be maintained, therefore session management may need to be turned off in this scenario. The *Cúram Web Client Reference Manual* should be referenced for further details on how to turn this off.

The following are examples of automatic login and logout JSP scripts.

**Note:** Security implementations and configurations differ across application server vendors so these examples may not work in all cases or for all application server versions.

```

<?xml version="1.0" encoding="UTF-8"?>
<jsp:root xmlns:jsp="http://java.sun.com/JSP/Page"
  xmlns:prefix="URI"
  version="2.0">
  <jsp:directive.page buffer="32kb"
    contentType="text/html; charset=UTF-8"
    pageEncoding="UTF-8" />

  <jsp:text>
    <![CDATA[
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
        "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">]]>
  </jsp:text>

  <!-- Automatic redirect to login security check of user
    details specified below -->

  <html>
    <head>
      <script type="text/javascript">
        function autoSubmit() {
          document.getElementById("loginform").submit();
        }
      </script>
      <meta content="text/html; charset=UTF-8"
        http-equiv="Content-Type" />
    </head>
    <body class="logonBody"
      style="visibility: hidden;"
      onload="autoSubmit()">
      <form id="loginform"
        name="loginform"
        action="j_security_check"
        method="post">
        <input type="hidden"
          name="j_username"
          value="generalpublic" />
        <input type="hidden"
          name="j_password"
          value="password" />
        <input type="hidden"
          name="user_type"
          value="EXTERNAL" />
      </form>
    </body>
  </html>
</jsp:root>

```

Figure 8. Automatic Login JSP

```

<?xml version="1.0" encoding="UTF-8"?>
<jsp:root xmlns:jsp="http://java.sun.com/JSP/Page"
  xmlns:prefix="URI"
  version="2.0">
  <jsp:directive.page buffer="32kb"
    contentType="text/html; charset=UTF-8"
    pageEncoding="UTF-8" />

  <jsp:text>
    <![CDATA[
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
        "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">]]>
  </jsp:text>
  <html>
    <head>
      <script type="text/javascript">
        function autoSubmit() {
          document.getElementById("logout").submit();
        }
      </script>
      <meta content="text/html; charset=UTF-8"
        http-equiv="Content-Type" />
    </head>
    <body class="logoutBody"
      style="visibility: hidden;"
      onload="autoSubmit()">
      <form id="logout"
        name="logout"
        action="servlet/ApplicationController"
        method="post">
        <input type="submit"
          name="j_logout"
          value="Log Out" />
        <input type="hidden"
          name="logoutExitPage"
          value="redirect.jsp" />
      </form>
    </body>
  </html>
</jsp:root>

```

Figure 9. Automatic Logout JSP

---

## 13.5 Extending the Public Access User Class

To “hook” the custom solution into the application the `curam.util.security.PublicAccessUser` abstract class must be extended, which requires implementing the `curam.util.security.ExternalAccessSecurity` interface. That concrete class will be used during the authentication and authorization process to determine required information relating to the external user. This class and its methods are described in detail below.

---

## 13.6 Authenticating an External User

The `authenticate()` method is responsible for authenticating an external user. It is invoked during the authentication process if the user is identifier as an external user. In the case of external users this method is invoked in place of the configured authentication.

**Note:** If an alternative authentication mechanism, e.g. LDAP, is configured, the external users must be able to authenticate against this mechanism.

```

/**
 * The implementation of this method should validate the identifier and
 * password and return the result of the validation. If the information is
 * valid, the codetable code SecurityStatus.LOGIN should be returned.
 *
 * @param identifier The identifier of the external user.
 * @param password The password as array of characters.
 * @param userType The type of external user.
 *
 * @return The status of the authentication in the form of a codetable code.
 *
 * @throws ApplicationException Generic Exception Signature.
 * @throws InformationalException Generic Exception Signature.
 */

public abstract String authenticate(String identifier,
    char[] password, String userType)
    throws ApplicationException, InformationalException;

```

The input parameters to the method include an identifier, the digested password as an array of characters, and the type of the external user to be authenticated.

The userType parameter is intended to allow for support of multiple types of external users that require different authentication mechanisms. The use of this parameter depends on the custom implementation.

The expected result of this method will be an entry from the curam.util.codetable.SECURITYSTATUS codetable. In the case of successful authentication the result must be:

```
curam.util.codetable.SECURITYSTATUS.LOGIN
```

For authentication failures this codetable contains a number of entries, including BADUSER , BADPWD and PWDEXPIRED . This codetable can be extended to include custom codes as detailed in the *Cúram Server Developer's Guide*.

The authentication result returned by this method is automatically logged in the AuthenticationLog database table. For more information on this table see the *Cúram Server Developers Guide*.

The abstract class PublicAccessUser also defines the following abstract methods that any concrete subclass must implement:

- Method upgradeSafePasswordValidation() is required to allow for password comparison and is defined as follows:

```

public final boolean upgradeSafePasswordValidation(
    final String userName,
    final String storedPasswordHash,
    final String plaintextPassword)

```

- Method setPassword() is to allow the implementor to persist the password (e.g. a new password) in the case of crypto upgrades. So this method gets called when the upgradeSafePasswordValidation() method is called. Here is the method definition:

```

public abstract void setPassword(String username, String hashedPassword)
    throws ApplicationException, InformationalException;

```

See the associated JavaDoc of the PublicAccessUser class for more details regarding the above methods.

---

## 13.7 Determine External User Details

Details for an external user are retrieved by calling the `getLoginDetails()` method of the `curam.util.security.ExternalAccessSecurity` interface. These details are returned directly after authentication to direct the external user to the correct application homepage.

```
/**
 * The implementation of this method should retrieve the
 * details of the user required to redirect them to the correct
 * application page. This information includes the name of the
 * application home page for the user, the default locale for
 * the user and a list of warnings/messages for the user.
 *
 * @param identifier The identifier of the external user.
 *
 * @return The user details, including the application
 *         home page.
 *
 * @throws ApplicationException Generic Exception Signature.
 * @throws InformationalException Generic Exception Signature.
 */
UserLoginDetails getLoginDetails(String identifier)
    throws ApplicationException, InformationalException;
```

An instance of the `curam.util.security.UserLoginDetails` class must be created and returned from this method. The following information should be returned using this class:

- `UserLoginDetails . setApplicationCode(String code)`  
The code corresponding to the application homepage for the external user.  
This must be a valid entry in the `APPLICATION_CODE` codetable.
- `UserLoginDetails . setDefaultLocale(String defaultLocale)`  
The default locale for the external user.  
This is the locale the application will be displayed in by default for the external user.
- `UserLoginDetails . addInformationals(InformationalManager informationalManager)`  
Any informationals that must be displayed to the external user.  
The `curam.util.exception.InformationalManager` class can be used to create a number of informational or warning messages that will be displayed when the external user logs in. For example, a warning to let the external user know that their password is due to expire.

---

## 13.8 Authorizing an External User

The `getSecurityRole()` method is used during authorization to determine the security role associated with the external user. The security roles used for external users are configured in the same way as the security roles for internal users.

```

/**
 * The implementation of this method should return the security
 * role associated with the external user for authorization
 * purposes. If the user does not exist null should be
 * returned.
 *
 * @param identifier The identifier of the external user.
 *
 * @return The security role for authorization.
 *
 * @throws AppException Generic Exception Signature.
 * @throws InformationalException Generic Exception Signature.
 */
String getSecurityRole(String identifier)
    throws AppException, InformationalException;

```

The SDEJ will invoke an implementation of this method during the authorization process if the user does not exist in the security cache. Only internal users can exist in the security cache. This means that the identifiers used to identify external users must be unique and not conflict with usernames setup for internal users, unless the custom `UserScope` interface as described in 7.3, “User Scope,” on page 27, is implemented. Otherwise, if any usernames conflict the access rights assigned to the internal user will also be used for the external user.

If a role cannot be determined for the external user, null must be returned so that the SDEJ can report the authorization error correctly.

---

## 13.9 Determining the User Type

The `getUserType()` method is used to determine if a user is an external user.

```

/**
 * Return the type of the user. This is to allow support for
 * different types of external user. If there is only one
 * type of external user, simply return "EXTERNAL".
 *
 * @param identifier The identifier of the external user.
 *
 * @return The type of the external user.
 *
 * @throws AppException Generic Exception Signature.
 * @throws InformationalException Generic Exception Signature.
 */
String getUserType(final String identifier)
    throws AppException, InformationalException;

```

The `getProgramUserType()` in `curam.util.transaction.TransactionInfo` will invoke this method to return the type of user if the user is not recognized as an internal user. For internal users “INTERNAL” is always returned.

For external users, there may be multiple types of external users, so this method should return the specific type of external user.

---

## 13.10 Preventing the Deletion of a Security Role: Role Usage Count

The `getRoleUsageCount()` method is used to prevent the deletion of a security role that is currently referenced by an external user.



```

/**
 * Return the number of users using a particular role. This
 * method is used to ensure that a role cannot be deleted when
 * it is in use by an external user.
 *
 * @param role The security role name.
 *
 * @return The number of users currently using the
 *         specified role.
 *
 * @throws AppException Generic Exception Signature.
 * @throws InformationalException Generic Exception Signature.
 */
int getRoleUsageCount(String role)
    throws AppException, InformationalException;

```

Security roles that are referenced by any user, internal or external, cannot be removed. This method should return a number of 1 or more if any external users reference the specified role.

---

## 13.11 Retrieving a Registered Username

The `getRegisteredUserName()` method is used retrieve the correct case username, which may be independent of the username typed during login.

```

/**
 * Gets the correct casing for this user independent of mixed
 * case which may have been typed in by the logged in user.
 *
 * @param identifier The identifier of the external user,
 * whose casing may not match that of the persisted identifier
 * for the user.
 *
 * @return The actual case for this user, before its case has
 * been modified by external factors.
 *
 * @throws AppException Generic Exception Signature.
 * @throws InformationalException Generic Exception Signature.
 */
public String getRegisteredUserName(final String identifier)
    throws AppException, InformationalException;

```

The default implementation for this method should return the username that has been provided. It is only if the `curam.security.casesensitive` has been set to false that this method may need to change the case of the username returned.

**Note:** Where the `curam.security.casesensitive` property has been set to false and is required for external users, it is the responsibility of all methods in this interface to handle any case specific requirements.

---

## 13.12 Reading User Preferences

The `getUserPreferenceSetID()` method is used to retrieve the user preference set ID associated with an external user. If no user preferences exist for an external user, then the default preferences will be used for the external user. The *User Preferences* chapter in the *Cúram Server Developer's Guide* should be referenced for further details on user preferences.

```

/**
 * This method is used to retrieve a set of user preferences
 * associated with an external user. The userPrefSetID is a
 * foreign key to the UserPreferenceInfo table.
 * The UserPreferenceInfo table contains information on
 * the user preferences.
 *
 * @param identifier The identifier of the external user.
 *
 * @return The userPrefSetID for the external user.
 *
 * @throws AppException Generic Exception Signature.
 * @throws InformationalException Generic Exception Signature.
 */
String getUserPreferenceSetID(final String identifier)
    throws AppException, InformationalException;

```

The default implementation for this method should return the user preference set ID for the user preferences associated with an external user.

---

### 13.13 Modifying User Preferences

The `modifyUserPreferenceSetID()` method is used to update the external user details with a new set of user preferences. Please see User Preferences for further details on user preferences.

```

/**
 * This method updates the external user details with new user
 * preferences.
 *
 * @param userPreferenceSetID The ID for the user preferences.
 * @param username The identifier of the external user.
 *
 * @throws AppException Generic Exception Signature.
 * @throws InformationalException Generic Exception Signature.
 */
void modifyUserPreferenceSetID(
    final String userPreferenceSetID, final String username)
    throws AppException, InformationalException;

```

The default implementation for this method should update the user preference set id associated with an external user.

---

### 13.14 Configuring External Access Security

The `curam.custom.externalaccess.implementation` property must be set in the `Application.prx` to indicate the fully qualified name of the class which implements the above interface.

**Note:** The `curam.custom.externalaccess.implementation` property is not dynamic, and if changed the application must be restarted before the change will take effect.

---

### 13.15 Determining if a User is Internal or External using the UserScope Interface

To support alternative methods for determining if a user is internal or external the custom interface `UserScope` is available. For example, even though usernames must be unique across the set of internal and external users, this custom interface can be implemented to allow duplicate usernames across internal and external applications in a limited way.

To provide a custom implementation for determining the type of user, the `curam.util.security.UserScope` interface must be implemented. This interface has one method

`isUserExternal()` that determines the type of user. This method should return true if the user is considered external or false indicating the user is internal.

For example, an installation might have `application1` deployed with `userA`, a Cúram internal user, and `application2` deployed with `userA` being external (e.g. defined to LDAP). The ability for `application1` to use internal `userA` and `application2` to use external `userA` would be controlled by different properties. That is, `Bootstrap.properties` in `properties.jar` in the `application1` EAR would have a different custom property setting from `application2` EAR and the implementation of `curam.util.security.UserScope.isUserExternal()` would interrogate this setting to decide if the user is internal or external.

To specify a custom implementation of the `UserScope` interface the `curam.custom.userscope.implementation` property must be set in `Application.prx`. This should be set to the fully qualified name of the class that implements the `UserScope` interface.

**Note:** The `curam.custom.userscope.implementation` property is not dynamic, and if changed the application must be restarted before the change will take effect.

The `isUserExternal()` method of the `UserScope` interface is detailed in 13.16, “User Type Determination.”

---

## 13.16 User Type Determination

The `isUserExternal()` method is invoked anywhere in the application where the type of user is to be determined. This includes when the user logs into the application and when they attempt authorization to access secured elements of IBM Cúram Social Program Management.

```
/**
 * The implementation of this method should determine the type of
 * User that is logged into the application. There are 2 types of
 * users: INTERNAL and EXTERNAL. If the user is an EXTERNAL user,
 * then this method should return true. If false is returned,
 * then the user is considered INTERNAL.
 *
 * @param username - The username.
 * @return A boolean value of true indicating an EXTERNAL user,
 * false indicates an INTERNAL user.
 *
 * @throws ApplicationException Generic Exception Signature.
 * @throws InformationalException Generic Exception Signature.
 */
boolean isUserExternal(String username)
    throws ApplicationException, InformationalException;
```



---

## Notices

This information was developed for products and services offered in the U.S.A. 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

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte (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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: 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 states 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply 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 Corporation

Dept F6, Bldg 1

294 Route 100

Somers NY 10589-3216

U.S.A.

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All 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 the names and addresses used by an actual business enterprise 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.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. \_enter the year or years\_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

## Programming Interface Information

This publication documents intended programming interfaces that allow the customer to write programs to obtain the services of IBM Cúram Social Program Management.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://www.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/us/en/copytrade.shtml>.

Apache is a trademark of Apache Software Foundation.

Oracle, WebLogic Server, Java and all Java-based trademarks and logos are registered trademarks of Oracle and/or its affiliates.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.









Printed in USA