

IBM Cúram Social Program Management
Version 7.0.10

IBM Cúram Identity Intelligence Guide



Note

Before using this information and the product it supports, read the information in [“Notices” on page 23](#)

Edition

This edition applies to IBM® Cúram Social Program Management v7.0.10 and to all subsequent releases unless otherwise indicated in new editions.

Licensed Materials - Property of IBM.

© **Copyright International Business Machines Corporation 2016, 2020.**

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

Contents

Figures..... iv

Tables..... v

Chapter 1. IBM Cúram Identity Intelligence..... 1

- IBM Cúram Identity Intelligence Business Guide.....1
- Identity Intelligence Key Terminology..... 2
- Identity Intelligence within Case Types..... 3
- IBM Cúram Identity Intelligence Developer Guide.....6
- Integration..... 6
- Defining System Architecture..... 8
- Configuring Identity Insight for Cúram..... 10
- Identity Intelligence Data Set..... 11
- Extract and Transform Batch Program..... 15
- Configuring Cúram with web services..... 18
- Integrating the Web Services..... 21
- Configuring Logging..... 22

Notices..... 23

- Privacy Policy considerations..... 24
- Trademarks..... 24

Figures

- 1. IBM Cúram Identity Intelligence system overview diagram.....2
- 2. IBM Cúram Identity Intelligence System Overview Diagram..... 7
- 3. Deployment example..... 8

Tables

1. Cúram Settings from Within Identity Insight.....	10
2. Program Integrity (Identity Intelligence) Batch Program System Application Properties.....	15
3. System Administration Properties.....	18

Chapter 1. IBM Cúram Identity Intelligence

Fraud, waste, and abuse drains billions from social program funds each year. Social program clients might benefit from tracking citizens, their identities, and interactions with other programs. The IBM Cúram Identity Intelligence product aims to give caseworkers the confidence that an applicant is who they say they are and are not duplicated within the system, which might result in duplicate benefits. The product solves this problem by applying existing IBM algorithms and analytics to client data and verifies information with limited worker involvement and reduces improper payments for social programs.

To assist caseworkers in this important task, an IBM Cúram Identity Intelligence product is available with the IBM Cúram SPM system to provide a clearer indication of the benefit applicant's integrity. The caseworker can delve into the history of clients who are highlighted as having potential duplicate identities.

A caseworker can see whether potential duplicate identities exist for people who are already registered in the system, newly registered people, and new applicants (including new case members) without leaving IBM Cúram SPM. As a result, they can accurately determine whether the client is legitimately entitled to benefits or services before payments are made. The benefit might be the prevention of billions lost to fraud, waste, and abuse each year.

IBM Cúram Identity Intelligence Business Guide

IBM Cúram Identity Intelligence is used to identify and address the client's needs to verify the true identity of someone ("who is who").

The IBM Cúram Identity Intelligence product contains the product IBM InfoSphere Identity Insight bundled as part of the software. The following two systems are integrated to provide a working IBM Cúram Identity Intelligence system.

IBM Cúram Social Program Management

The IBM Cúram Social Program Management supports the end-to-end social program delivery process. Using IBM Cúram Social Program Management, organizations can collaborate around citizen's needs. This collaboration makes governmental services more effective in achieving their social goals, and makes it easier to access services for citizens easier.

IBM InfoSphere Identity Insight

IBM InfoSphere Identity Insight helps organizations solve business problems that are related to recognizing the true identity of someone among client records. IBM InfoSphere Identity Insight provides immediate and actionable information to help clients prevent fraud waste and abuse.

The IBM InfoSphere Identity Insight product analyzes participant data that is collected from the IBM Cúram SPM system. The product checks if similar or suspicious identities exist in the participant data. An analysis takes place to indicate a risk of fraud, waste, or abuse when a caseworker enters or works with one candidate. The IBM InfoSphere Identity Insight tool checks existing data, based on a series of predefined rules. If a predefined level of concern is reached, an entity is created outlining matching identity records. This process is known as *Entity Resolution*. This entity resolution can be communicated back to IBM Cúram SPM and is made visible in the caseworker's workflow.

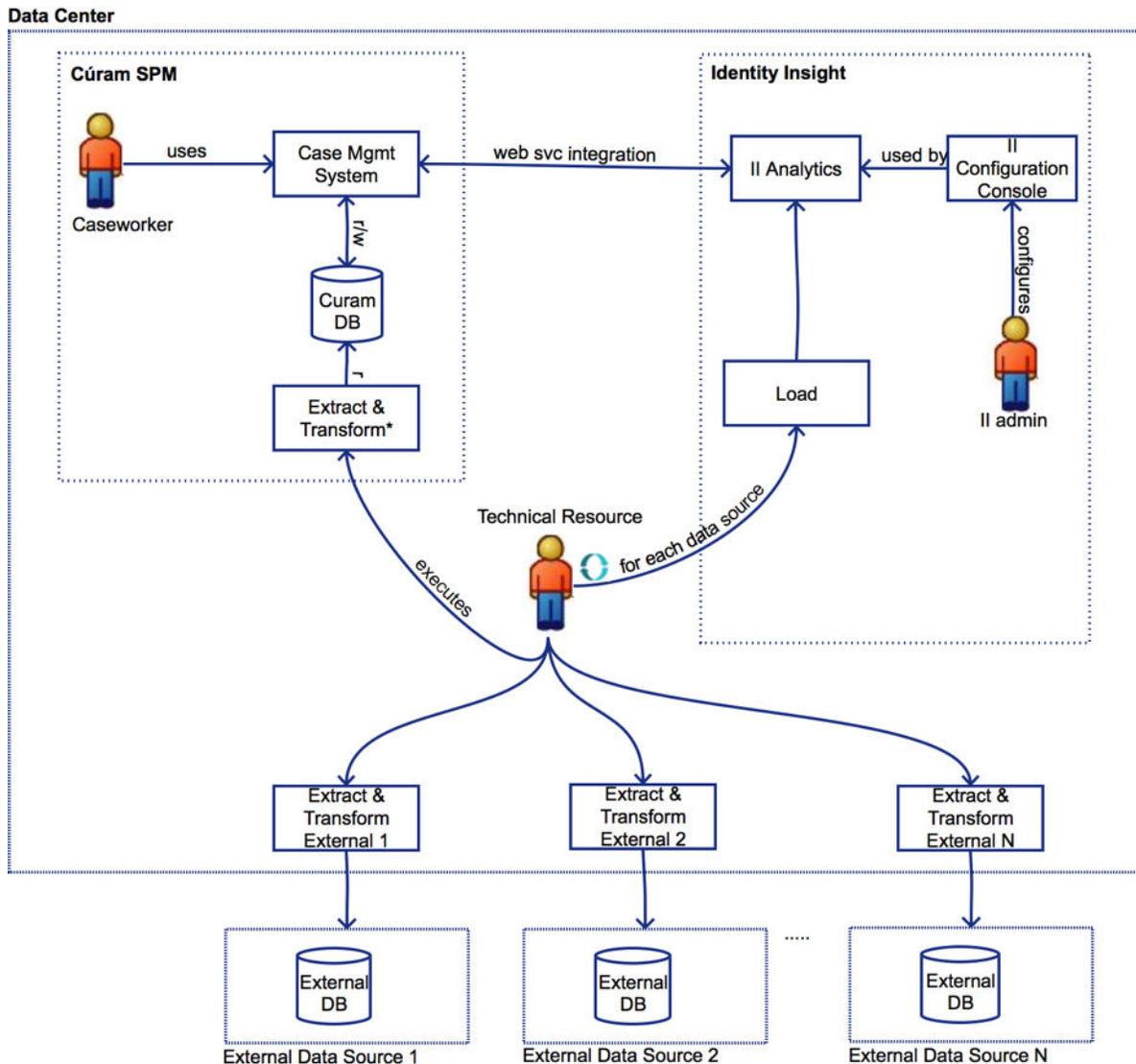


Figure 1. IBM Cúram Identity Intelligence system overview diagram

Identity Intelligence Key Terminology

Entity resolution is the key mechanism that is provided by IBM InfoSphere Identity Insight to reconcile identities within the IBM Cúram SPM database records. Entity resolution is carried out automatically by Identity Insight.

- **Sending Data to Identity Insight** - IBM InfoSphere Identity Insight receives data in real time through web services that are sourced from IBM Cúram SPM. IBM InfoSphere Identity Insight then analyses the data set sent by Cúram SPM. Data is then returned in real time to the Cúram SPM user.
- **Data Used to Check Identities** - An agreed data set between IBM Cúram SPM and IBM InfoSphere Identity Insight exists that is used to compare identities. The data is taken from the IBM Cúram SPM Participant Data Case (PDC) evidence and this data can also be transferred as part of an Application Case. Note prospect persons are out of scope for this release.
- **Identities and Entities under Identity Insight** - Single and multiple identity records are handled by Identity Insight. An IBM InfoSphere Identity Insight entity contains single or multiple identity records that are transferred from an external system and processed by the entity resolution process.
- **Entity Resolution Process** - The process of entity resolution uses sophisticated algorithms to compare the data values of an incoming identity record against existing identities in the database to determine whether they are the same entity. The results of an entity resolution are presented to the caseworker as

potential duplicates and can be viewed by the caseworker if they press the Insights tab on a person or on an application case record in IBM Cúram SPM. As new data is loaded into the system, IBM InfoSphere Identity Insight updates and manages the information in context for the entities in the entity database. It can completely comprehend the meaning of new or changed data as it is loaded. It can make the most of each transaction and enhancing the comprehensive view of each entity in the entity database.

Related information

[Cúram Participant Guide](#)

Identity Intelligence within Case Types

A caseworker manages cases and performs tasks that relate to participants on a case.

The caseworker follows a case work flow when they work within the IBM Cúram SPM caseworker screens.

- Register a person.
- Complete an Application Case for a new entrant or a Participant Data Case to add evidence details.
- Check identities by using the Insights tab available with the IBM Cúram Identity Intelligence product.
- Data is exchanged automatically between the two systems (IBM InfoSphere Identity Insight and IBM Cúram SPM elements).
- Review the data available with the Insights tab that displays in IBM Cúram SPM or check the Insights if prompted on case authorization.
- Check if a duplication of identity data exists on the system.
- Review this data and proceed with authorizations as required.

Participant Data Case

A Participant Data Case can be described as a record for one person. A number of Evidence Types are maintained for a Participant Data Case record of a person or participant on the system.

Note prospect persons are out of scope for this release.

The Evidence Types are typically:

- Names
- Birth and Death Details
- Relationships
- Addresses
- Identifications
- Phone Numbers
- Email Address
- Gender

This data forms a key data set for all persons. IBM Cúram Identity Intelligence can then establish the accuracy of the personal information that is given and whether the person exists already on the system.

Viewing Insights on Participant Data Case

As a caseworker you view the most up-to-date insights within the Participant Data Case by selecting the **Insights** tab.

About this task

You can be searching for an existing citizen or you are registering a new person and have recorded evidence data when you are working in IBM Cúram SPM.

Procedure

1. Select the **Cases and Outcomes Applications** tab.

2. Select the **Shortcuts** panel.
3. Select **Person...** under the **Searches Page Group Navigation** bar.
4. Use the **First Name** and **Last Name** fields of the **Person Search** tab to enter the name of an individual you are recording a case for on the Search person form.
5. Select the link for the participant that is returned to view their data.
6. Select the **Insights** tab. The following outcomes are possible:

Possible Outcomes	Description
Potential Duplicates are displayed	For any identity that is returned by IBM InfoSphere Identity Insight, review the details. Each attribute is displayed line-by-line across the screen. Continue to Step 7.
No duplicates are available	An error message is displayed. No further action is possible.
Communication Error	An error message is displayed. No further action is possible.

7. Click the **Potential Duplicate** twistie to see a list of attribute data for the two identities.
When the user opens a potential duplicate identity, a side-by-side comparison of the person and potential duplicate identity is shown.
8. Click the person name link field in the **Potential Duplicate Identity** column to display the person record for that identity and the related evidence details.

Application Case

An Application Case captures the client's initial application for benefits or services.

An Application Case normally contains the Participant Data Case details for one or more persons and other application case details as well. In addition, there can be more than one person for an Application Case, meaning data might be sent for several persons and their relevant Application Case details. The Participant Data Case data for each case member is sent to IBM Cúram Identity Intelligence when the caseworker views the **Insights** tab or upon Authorization.

Viewing Insights on Application Case

View Insights to determine if potential duplicate identities exist for any member of an Application Case.

About this task

When you are working in IBM Cúram SPM, go to an Application Case.

Procedure

1. Select the **Cases and Outcomes Applications** tab.
2. Select the **Shortcuts** panel.
3. Select the **Searches** option.
4. Select the **Case...** option under the **Search** navigation bar.
5. Enter an application case reference number.
6. Press the **Search** button.
A case is displayed.
7. Select the case.
The details for the case are displayed and relevant persons shown.
8. Select the **Insights** tab.
The following outcomes are possible:

Possible Outcome	Description
Potential Duplicates are displayed	For any identity that is returned by IBM InfoSphere Identity Insight, review the details. Each attribute is displayed line-by-line across the screen. Continue to Step 9.
No duplicates are available	An error message is displayed. No further action is possible.
Communication Error	An error message is displayed. No further action is possible.

- Click the **Potential Duplicate** twistie to see a list of attribute data for the two identities.
When the user opens a potential duplicate identity, a side-by-side comparison of the person and potential duplicate identity is shown.
- Click the person name link field in the **Potential Duplicate Identity** column to display the person record for that identity.

Authorization

When a caseworker authorizes a case, IBM Cúram Identity Intelligence prompts the user if a potential duplicate identity exists.

A caseworker can authorize an Application Case from different locations:

- The Actions menu
- The Home Tab
- The Programs Tab
- The Authorization Tab

These caseworker screens are available when they are working in IBM Cúram SPM.

If a potential duplicate identity exists, the caseworker has two options:

1. They can choose to view the potential duplicate identities through the **Insights** tab, or
2. They can continue without reviewing the Insights for the persons on the case to be authorized.

If no duplicates are found, the caseworker proceeds to the case authorization program as normal.

Authorization Prompt

View Insights based on potential duplicate identities that are found when case authorization is requested by a caseworker.

About this task

Data is automatically pushed to IBM Cúram Identity Intelligence as a result of requesting authorization.

Procedure

1. Use the **Authorize** option.

The following outcomes are possible:

Possible Outcomes	Description
Potential Duplicate Identity prompt appears	The following prompt and message appears: "Insights exist on the case which can indicate potential duplicates. If you have already reviewed the insights and want to proceed with authorization, select the appropriate action". Go to Step 2.
Authorize Program modal appears	No Insights are available and potential duplicate identities are not found. Go to Step 3.

2. Select one of the functional options displayed.

Functional Options	Description
View Insights	Goes to the Insights tab and you can view potential duplicate identities for this case. Go to Step 4.
Next	Allows you to continue without viewing Insights. Go to Step 3.
Cancel	Cancel dismisses the page.

3. You can continue with the **Authorize Program** modal as usual.
4. View the Insights and act based on the potential duplicate identities that you are shown.

IBM Cúram Identity Intelligence Developer Guide

Use this information to integrate IBM Cúram SPM and IBM InfoSphere Identity Insight.

Integration

The IBM Cúram Identity Intelligence product is an integration of the IBM Cúram SPM and IBM InfoSphere Identity Insight products.

The following tasks need to be completed as part of integration:

1. Installation and Configuration for Product Components

During a typical installation, you need to install:

- IBM Cúram SPM
- IBM Cúram Identity Intelligence using the separate installer that supports the integration with IBM InfoSphere Identity Insight
- IBM InfoSphere Identity Insight

IBM InfoSphere Identity Insight and IBM Cúram SPM components have product installation procedures and can be installed according to their installation procedures as defined in their respective IBM Knowledge Centers. See Related Information.

The following configuration steps are outlined for IBM Cúram Identity Intelligence:

1. Complete Pipeline Management for the IBM InfoSphere Identity Insight configuration. See [“Defining System Architecture”](#) on page 8.
2. The System Source, Data Source, and Role configuration settings are required to complete the customization of IBM InfoSphere Identity Insight connection to IBM Cúram SPM. See [“Configuring Identity Insight for Cúram”](#) on page 10.
3. Within Cúram, you use the system administration properties to tailor the settings for Identity Intelligence and IBM Cúram SPM to communicate with IBM InfoSphere Identity Insight. See [“Configuring Cúram with web services”](#) on page 18.

2. Extract and Transform Batch (ETL) Program

The program is used to facilitate the initial load of data from IBM Cúram SPM to IBM InfoSphere Identity Insight. The process extracts the IBM Cúram Identity Intelligence data set from the IBM Cúram SPM system and converts it into Universal Message Format (UMF).

For more information, see [“Extract and Transform Batch Program”](#) on page 15 and [“Identity Intelligence Data Set”](#) on page 11. When the data is in the UMF format, it can be loaded into IBM InfoSphere Identity Insight by using its pipeline functionality.

Figure 2 on page 7 is a typical system context diagram that might vary from customer to customer based on system architecture. However, integration with external systems and their ETL processes is outside the scope of this release and is the responsibility of the customer.

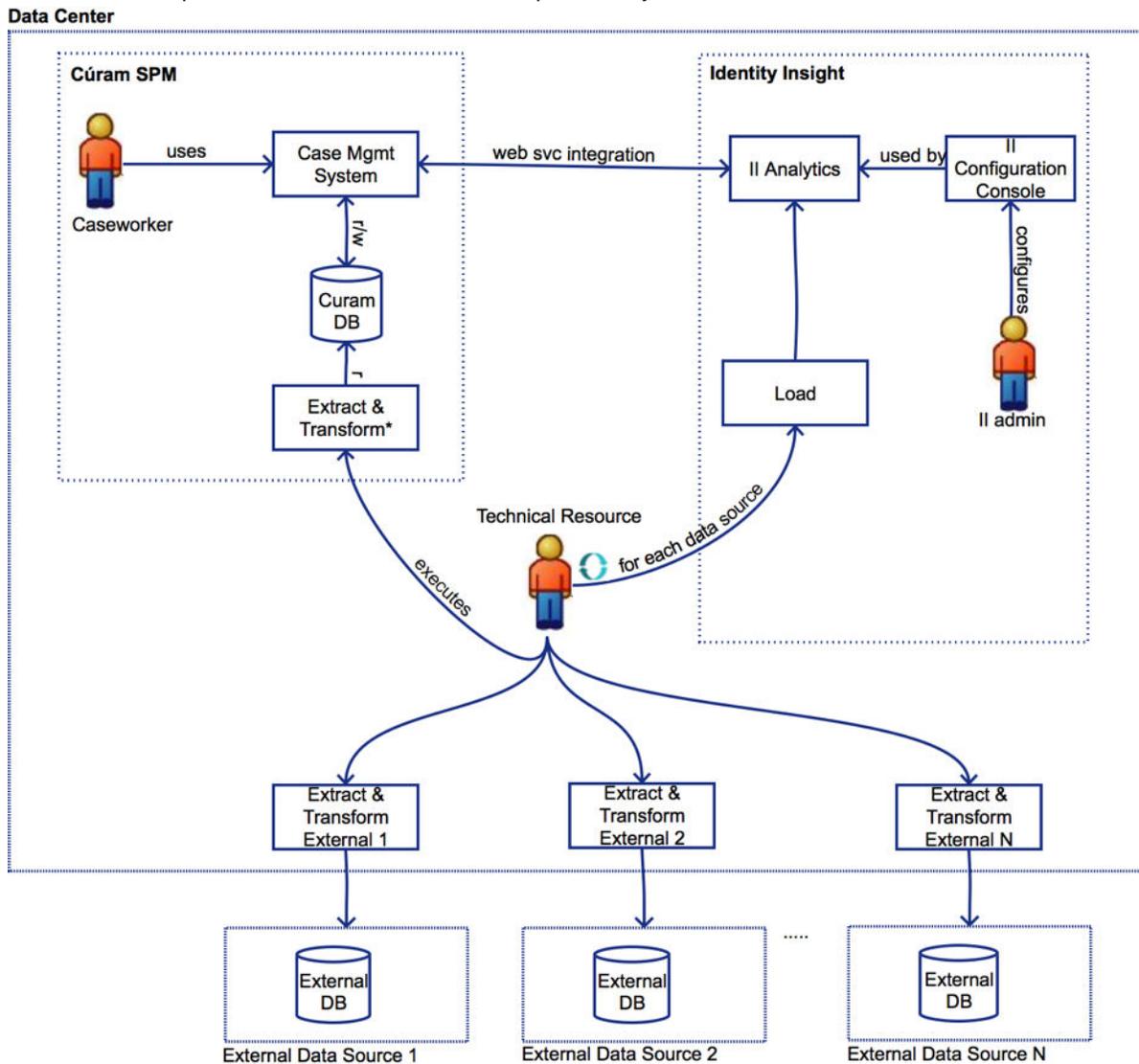


Figure 2. IBM Cúram Identity Intelligence System Overview Diagram

3. Web Service Integration

A web service integration allows IBM Cúram SPM to load new data into IBM InfoSphere Identity Insight after the initial load. And also, it allows IBM Cúram SPM to query IBM InfoSphere Identity Insight for insights about particular identities. For more information, see [“Integrating the Web Services”](#) on page 21.

4. Case Management Screens

The Insights returned by the web service integration are displayed on IBM Cúram SPM caseworker screens for [“Authorization”](#) on page 5 and [“Identity Intelligence within Case Types”](#) on page 3.

5. Pre-requisites

The Participant Data Case (PDC) administration property `curam.evidence.pdc.personenabled` is required and is set to YES. See the property administration procedure as described in [“Configuring Cúram](#)

with web services” on page 18 for an example of how to set the system administration properties for IBM Cúram SPM.

Telephone Number data entry masks might need to be determined for IBM InfoSphere Identity Insight. The format of the telephone number must match in both systems for the exchange of data records with IBM Cúram SPM. See “Updating Telephone Number Settings” on page 11, for more information.

Related information

[Installing \(IBM InfoSphere Identity Insight\)](#)

[Detailed System Requirements \(IBM InfoSphere Identity Insight\)](#)

[Setting up the Databases \(IBM InfoSphere Identity Insight\)](#)

[Pipeline deployments \(IBM InfoSphere Identity Insight\)](#)

[Installing \(IBM Cúram SPM\)](#)

Defining System Architecture

Before deploying IBM Cúram Identity Intelligence, the system architecture must be defined by the organization.

The sections that are listed show some of the areas that might be considered with a focus on IBM InfoSphere Identity Insight product and how it works with IBM Cúram SPM.

Deployment

The organization must define the deployment configuration for the IBM Cúram SPM and IBM InfoSphere Identity Insight products.

Organizations vary and factors such as expected data volumes, number of data sources, performance, and scalability would need to be factored into the decision-making process in this area. For example, a typical deployment would consist of IBM Cúram SPM and IBM InfoSphere Identity Insight running on separate hardware and separate databases.

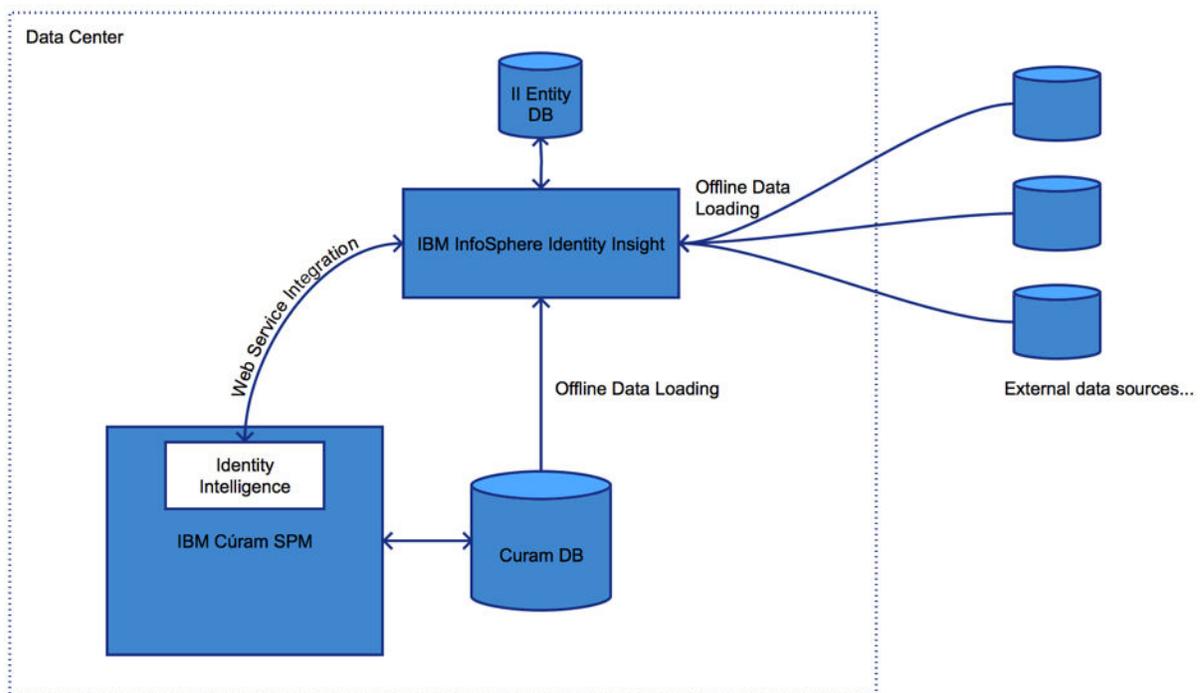


Figure 3. Deployment example

For more information on System Requirements and Planning, see the IBM InfoSphere Identity Insight IBM Knowledge Center.

Related information

[System Requirements and Planning](#)

Performance Management and Scalability

Pipelines are the component that perform name and address hygiene standardization, data quality management, and entity resolution.

The pipelines also perform resolution and generate alerts, based on system configuration.

In terms of performance and scalability, pipelines can be configured for parallel processing to mitigate against hardware and memory constraints. The pipeline configuration model that an organization defines varies depending on individual usage and can be defined by the organization.

For more information about pipelines, see the IBM InfoSphere Identity Insight IBM Knowledge Center.

Related information

[Pipelines](#)

Security and Regulation

The data that is sent to IBM InfoSphere Identity Insight from IBM Cúram SPM consists of Personally Identifiable Information (PII).

Securing this data is the responsibility of the organization. This responsibility includes securing the data at rest and also ensuring adequate controls and protocols are used for the data that employ the web service integration layer.

In addition, it is the responsibility of the organization to ensure that caseworkers are authorized to view any of the data that is presented on the screens within IBM Cúram SPM.

Data Quality Management

Data quality management (DQM) is the process that checks data for required values, valid data types, and valid codes.

You can also confirm DQM to correct the data by providing default values, formatting numbers and dates, and adding new codes. DQM configuration is possible through the IBM InfoSphere Identity Insight Configuration Console.

Note: After the application of these settings, the IBM InfoSphere Identity Insight pipelines need to be restarted.

For more information about Data Quality Management, see the IBM InfoSphere Identity Insight IBM Knowledge Center.

Related information

[Data Quality Management](#)

Data Refreshes

Periodically, it might be required to load new and updated data from IBM Cúram SPM to IBM InfoSphere Identity Insight.

You need to ensure that IBM InfoSphere Identity Insight is running against the most up-to-date information. This approach also addresses any connection issues that might occur during web service loads from IBM Cúram SPM to IBM InfoSphere Identity Insight.

While the IBM Cúram Identity Intelligence offering does not contain a data refresh function, the Extract and Transform Batch Program can be customized to meet this requirement.

External Data Sources

An organization can choose to load data from any number of external data sources into IBM InfoSphere Identity Insight.

The Extract, Load, and Transform processes for these external sources are the responsibility of the organization and are outside of the scope of IBM Cúram SPM.

Configuring Identity Insight for Cúram

The configuration requirements for IBM InfoSphere Identity Insight and its integration with IBM Cúram SPM software.

Identity Insight settings for integration with IBM Cúram SPM

Use the **Setup - Source/General** options from IBM InfoSphere Identity Insight.

Setting	Entry
System Source	CURAM
Data Source	CURAM
Role	CURAMROLE

Adding Cúram as a Data Source

Add Cúram as the data source.

About this task

Through the IBM InfoSphere Identity Insight Configuration Console, the following settings need to be applied.

Procedure

1. In the Configuration Console, select **Setup > General > Source Systems**. Use **New** to add a System Source record.
2. Add CURAM as a system source.
This entry must match the *curam.programIntegrity.II.datasource* setting value that is given in the System Administration settings for IBM Cúram SPM.
3. In the Configuration Console, select **Setup > Sources > Data Sources**. Use **New** to add a Datasource record.
4. Add CURAM as a data source.
This entry must match the *curam.programIntegrity.II.datasource* setting value that is given in the System Administration settings for IBM Cúram SPM. Complete the General, Entity Resolution, and Relationship tabs as appropriate.
5. In the Configuration Console, select **Setup > Relationships > Roles**. Use **New** to add a relationship role.
6. Add CURAMROLE as a role.
7. Restart all IBM InfoSphere Identity Insight pipelines after the application of these settings.

Updating Telephone Number Settings

The phone number settings in IBM InfoSphere Identity Insight need to align with those settings that are captured in IBM Cúram SPM to allow for the successful transfer of phone information.

About this task

Through the IBM InfoSphere Identity Insight Configuration Console, the phone number format, length, and mask settings can be updated so that they are aligned with the IBM Cúram SPM system format.

Procedure

1. In the Configuration Console, select **Setup > Sources > Numbers**.
2. Select the **PH - Phone** link.
3. Select the **Format** tab.
4. Enter the telephone numbers to be consistent with the numbers in the IBM Cúram SPM system. The **Mask** field reflects the number of digits that can be exchanged for the telephone number in a Cúram identity record.
5. Restart all IBM InfoSphere Identity Insight pipelines after the application of these settings.

Identity Intelligence Data Set

Data from the following evidence types is sent from the IBM Cúram SPM system to the IBM InfoSphere Identity Insight system.

- PDC Name Details
- PDC Address Details
- PDC Birth and Death Details
- PDC Relationship Details
- PDC Gender Details
- PDC Identifications Details
- PDC Email Address
- PDC Telephone Number

The data that is sent to IBM InfoSphere Identity Insight is either added as a new identity or is added as additional context to an existing identity. Existing data within IBM InfoSphere Identity Insight is not deleted or replaced.

PDC Name Evidence to UMF

Evidence Field	Mapped UMF Example
firstName	<pre><NAME> <FIRST_NAME>Thomas</FIRST_NAME> <...> </NAME></pre>
lastName	<pre><NAME> <...> <LAST_NAME>Jones</LAST_NAME> </NAME></pre>
middleName	<pre><NAME> <...> <MID_NAME>J</MID_NAME> <...> </NAME></pre>

PDC Address Evidence to UMF

Evidence Field	Mapped UMF Example
address	<pre><ADDRESS> <ADDR_TYPE>H</ADDR_TYPE> <ADDR1>12</ADDR1> <ADDR2>street1</ADDR2> <ADDR3>street2</ADDR3> <CITY>city</CITY> <STATE>UT</STATE> <POSTAL_CODE>10002</POSTAL_CODE> </ADDRESS></pre>
addressType <ul style="list-style-type: none"> • PRIVATE maps to "H" • BUSINESS maps to "B" • Everything else maps to "O" 	<pre><ADDR_TYPE>H</ADDR_TYPE></pre>

PDC Birth and Death Evidence to UMF

Evidence Field	Mapped UMF Example
dateOfBirth	<pre><ATTRIBUTE> <ATTR_TYPE>DOB</ATTR_TYPE> <ATTR_VALUE>1992-01-01</ATTR_VALUE> </ATTRIBUTE></pre>

PDC Email Address Evidence to UMF

Evidence Field	Mapped UMF Example
emailAddress	<pre><EMAIL_ADDR> ... <EMAIL_ADDR>tjones@email.com</EMAIL_ADDR> </EMAIL_ADDR></pre>
emailAddressType <ul style="list-style-type: none"> • PERSONAL maps to "H" • BUSINESS maps to "B" 	<pre><EMAIL_ADDR> <ADDR_TYPE>H</ADDR_TYPE> ... </EMAIL_ADDR></pre>

PDC Gender Evidence to UMF

Evidence Field	Mapped UMF Example
gender	<pre><ATTRIBUTE> <ATTR_TYPE>GENDER</ATTR_TYPE> <ATTR_VALUE>Male</ATTR_VALUE> </ATTRIBUTE></pre>

PDC Identifications Evidence to UMF

Evidence Field	Mapped UMF Example
alternateID	<pre><NUMBER> ... <NUM_VALUE>666333111</NUM_VALUE> </NUMBER></pre>
altIDType <ul style="list-style-type: none"> INSURANCENUMBER maps to SSN DRIVERSLICENCE maps to DL PASSPORTNUMBER maps to PP 	<pre><NUMBER> <NUM_TYPE>SSN</NUM_TYPE> </NUMBER></pre>

PDC Relationship

Evidence Field	Mapped UMF Example
relationshipType relatedParticipant	<pre><RELATED_ENTITY> <DSCR_CODE>Curam</DSCR_CODE> <DSCR_ACCT>107</DSCR_ACCT> <DSCR_REF>107</DSCR_REF> <DESCRIPTION>SIBLING</DESCRIPTION> <NAME> <FIRST_NAME>Doroathy</FIRST_NAME> <LAST_NAME>WILLIAMS</LAST_NAME> </NAME> </RELATED_ENTITY></pre>

PDC Telephone Number

Evidence Field	Mapped UMF Example
phoneNumber phoneExtension phoneCountryCode phoneAreaCode (these fields are concatenated together and sent to II as one phone number string)	<pre><NUMBER> <NUM_TYPE>PH</NUM_TYPE> <NUM_VALUE>1510900-0980</NUM_VALUE> </NUMBER></pre>

Example of Complete UMF Record

```
<UMF_ENTITY>
  <DSCR_CODE>Curam</DSCR_CODE>
  <DSCR_ACTION>A</DSCR_ACTION>
  <DSCR_REF>12345</DSCR_REF>
  <DSCR_ACCT>12345</DSCR_ACCT>
  <ADDRESS>
    <ADDR_TYPE>H</ADDR_TYPE>
    <ADDR1>12</ADDR1>
    <ADDR2>street1</ADDR2>
    <ADDR3>street2</ADDR3>
    <CITY>city</CITY>
    <STATE>UT</STATE>
    <POSTAL_CODE>10002</POSTAL_CODE>
  </ADDRESS>
  <ADDRESS>
    <ADDR_TYPE>O</ADDR_TYPE>
    <ADDR1>14</ADDR1>
    <ADDR2>mailing street</ADDR2>
    <ADDR3>mailing street2</ADDR3>
    <CITY>city</CITY>
```

```

    <STATE>UT</STATE>
    <POSTAL_CODE>10003</POSTAL_CODE>
  </ADDRESS>
  <ATTRIBUTE>
    <ATTR_TYPE>DOB</ATTR_TYPE>
    <ATTR_VALUE>1992-01-01</ATTR_VALUE>
  </ATTRIBUTE>
  <EMAIL_ADDR>
    <ADDR_TYPE>H</ADDR_TYPE>
    <EMAIL_ADDR>tjones@email.com</EMAIL_ADDR>
  </EMAIL_ADDR>
  <ATTRIBUTE>
    <ATTR_TYPE>GENDER</ATTR_TYPE>
    <ATTR_VALUE>Male</ATTR_VALUE>
  </ATTRIBUTE>
  <NUMBER>
    <NUM_TYPE>SSN</NUM_TYPE>
    <NUM_VALUE>666333111</NUM_VALUE>
  </NUMBER>
  <NAME>
    <FIRST_NAME>Thomas</FIRST_NAME>
    <LAST_NAME>Jones</LAST_NAME>
  </NAME>
  <NUMBER>
    <NUM_TYPE>PH</NUM_TYPE>
    <NUM_VALUE>1111111111</NUM_VALUE>
  </NUMBER>
</UMF_ENTITY>

```

Customization of the data set

It is possible to customize the data set that is converted to UMF format and sent to IBM InfoSphere Identity Insight.

The interface `curam.programintegrity.impl.ProgramIntegrityEvidenceMapper` can be implemented for any evidence types that might be mapped to IBM InfoSphere Identity Insight. The method

`curam.programintegrity.impl.ProgramIntegrityEvidenceMapper.mapEvidence(ReadEvidenceDetails)` extracts the dynamic evidence attributes from the `ReadEvidenceDetails` and maps them into a UMF String format to be returned.

Any implementations need to be bound to an evidence type through a Map Binder.

Example

```

final MapBinder<String, ProgramIntegrityEvidenceMapper> mapperStrategy =
    MapBinder.newMapBinder(binder(), String.class,
        ProgramIntegrityEvidenceMapper.class);

mapperStrategy.addBinding(PDCConst.PDCIDENTIFICATION )
    .to(PDCIdentificationsMapper.class);

```

To modify any of the existing mappers, a new class can be created that extends the original evidence mapper and overrides the `mapEvidence` method.

Example

```

public class CustomPDCNameMapper extends PDCNameMapper {

    @Override
    public String mapEvidence(final ReadEvidenceDetails readEvidenceDetails)
        throws ApplicationException, InformationException {

```

This new class then needs to be bound to the old one:

```

binder().bind(PDCNameMapper.class).to(CustomPDCNameMapper.class);

```

Extract and Transform Batch Program

The IBM Cúram Identity Intelligence Extract and Transform Batch Program can be used to perform the initial load of person data from the IBM Cúram SPM system to the IBM InfoSphere Identity Insight system.

The batch program reads evidence from a set of Participant Data Cases from the IBM Cúram SPM system. The program converts the data to Universal Message Format (UMF) so that it can then be loaded into the IBM InfoSphere Identity Insight system.

Running the Batch Program

The batch program can be executed from the command line.

Configuring the Batch Program

It is recommended to execute the batch program during off peak hours to avoid adverse effects on the IBM Cúram SPM system. The following system application properties are related to the batch program and are configured by a system administrator before running:

<i>Table 2. Program Integrity (Identity Intelligence) Batch Program System Application Properties. Note OOTB indicates Out-of-the-Box setting</i>	
Application Property ID	Description
curam.batch.ProgramIntegrityExtractAndTransform.dontrunstream	This property determines if the batch program can sleep while it waits for the processing to be completed by the streams (rather than run a stream in itself). This property is set to 'YES' OOTB meaning that it sleeps.
curam.batch.ProgramIntegrityExtractAndTransform.chunkkeywaitinterval	The interval (in milliseconds) for which the batch program waits before retrying when it reads the chunk key table. This property is set to 1000 OOTB.
curam.batch.ProgramIntegrityExtractAndTransform.chunksize	The number of people in each chunk that is processed by batch program. This property is set to 5 OOTB.
curam.batch.ProgramIntegrityExtractAndTransform.processunprocessedchunk	Does the batch program process any unprocessed chunks that are found after all the streams have been completed. This property is set to 'NO' OOTB.
curam.batch.ProgramIntegrityExtractAndTransform.unprocessedchunkwaitinterval	The interval (in milliseconds) for which the program waits before retrying when it reads the chunk table. This property is set to 1000 OOTB.
curam.batch.ProgramIntegrity.stream.database.transport	This option supports database transports for Identity Insight. The UMF records are inserted into the database. This property is set to 'YES' OOTB.

Table 2. Program Integrity (Identity Intelligence) Batch Program System Application Properties. Note OOTB indicates Out-of-the-Box setting (continued)

Application Property ID	Description
curam.batch.ProgramIntegrity.stream.file.transport	This option supports file-based transports for Identity Insight. The UMF records are output to be a file per batch stream. This property is set to 'NO' OOTB.
curam.batch.ProgramIntegrity.stream.file	The location where the streams can output the results to. This property needs to be set if curam.batch.ProgramIntegrity.stream.file.transport is set to 'YES'.

Set these properties in Property Administration as is described in “Configuring Web Service Endpoints” on page 18 or “Configuring Logging” on page 22 and use category Applications - Program Integrity and the property IDs. Or use a bootstrap properties file for these settings with the batch program. When these settings have been configured, the batch program can be executed from the command line. It is recommended that multiple streams can be set up to process the records in parallel. It is the responsibility of the customer to determine how many streams are required for the batch program, chunk size, and any other tuning settings. These settings are based on the number of records to process and the time frame in which they need to be processed and loaded into IBM InfoSphere Identity Insight.

When the streams are running, they wait for records to process. To start the main batch program, the following command is run from the EJBServer directory of the Cúram installation:

```
build runbatch -
  Dbatch.program="curam.programintegrity.sl intf.ProgramIntegrityExtractAndTransform.process" -
  Dbatch.username="<username>" -Dbatch.parameters="instanceID=<instanceID>"
```

This command sends the data to be processed to the streams and provide a report when finished. The report contains details of the number of records that are successfully processed. The report also contains the number of records skipped due to errors, the start time of the batch job and the time it took to complete. This report can be found in the buildlogs folder in the EJBServer directory of the Cúram installation.

To set up a stream, the following command is run from the EJBServer directory of the Cúram installation:

```
build runbatch -
  Dbatch.program="curam.programintegrity.sl intf.ProgramIntegrityExtractAndTransformStream.process" -
  Dbatch.username="<username>" -Dbatch.parameters="instanceID=<instanceID>"
```

Note <username> and <instanceID> are supplied by the system administrator for these commands.

Customizing the Batch Program

The batch program can be customized in the following ways.

Note: It is important to note that this table is part of the Cúram database. The organization might consider the data volume and data access requests and how that would affect the performance of the Cúram system. To mitigate against such performance concerns, the organization might consider a custom database table outside of the Cúram database.

Person selector customization

By default, the batch program iterates over all persons on the IBM Cúram SPM system. The abstract class `curam.programintegrity.sl.impl.AbstractProgramIntegrityPersonSelector` can be

extended to provide a custom person selection strategy. Any extensions of this class are responsible for implementing the following methods:

- `curam.programintegrity.sl.impl.ProgramIntegrityPersonSelector.extractPersons()` - This method can add the concern role IDs of the people to be processed to a `BatchProcessingIDList`.

The extending class can be injected for `curam.programintegrity.sl.impl.ProgramIntegrityPersonSelector`.

Database transport customization

By default, the UMF output is loaded into the `UMFData` IBM Cúram SPM database table. This customization is enabled by default through the `curam.batch.ProgramIntegrity.stream.database.transport` system application property. The abstract class

`curam.programintegrity.sl.impl.AbstractProgramIntegrityDatabaseStrategy` can be extended to provide a custom database insertion strategy. Any extensions of this class are responsible for implementing the following methods:

- `curam.programintegrity.sl.impl.ProgramIntegrityDatabaseStrategy.insertUMF(string)` - This method can insert the UMF string into a database table.

The extending class can be injected for `curam.programintegrity.sl.impl.ProgramIntegrityDatabaseStrategy`.

File-based transport customization

It is possible to output the UMF output to a file. This customization is turned off by default and can be enabled through the `curam.batch.ProgramIntegrity.stream.file.transport` system application property.

The abstract class `curam.programintegrity.sl.impl.AbstractUMFFileOutStrategy` can be extended to provide a custom file output strategy. Any extensions of this class are responsible for implementing the following methods:

- `curam.programintegrity.sl.impl.UMFFileOutStrategy.setUpFile()` - can set up the file that is written to.
- `curam.programintegrity.sl.impl.UMFFileOutStrategy.closeFile()` - can close the file output stream used.
- `curam.programintegrity.sl.impl.UMFFileOutStrategy.writeChunkResult(StringBuffer)` - can write the UMF to the file.

The extending class can be injected for `curam.programintegrity.sl.impl.UMFFileOutStrategy`.

Loading the Output into IBM InfoSphere Identity Insight

After the batch program has executed, the output can then be loaded into the IBM InfoSphere Identity Insight system by using pipelines.

The UMF can be transported into IBM InfoSphere Identity Insight in a few different ways, for example, database transport, file based transport or by using message queues. For more information on Transports, see the IBM InfoSphere Identity Insight IBM Knowledge Center.

Related information

[Transports](#)

Performance and Scalability Considerations

The batch program is a streamed batch program, which means that multiple instances can be executed in parallel to mitigate against hardware and memory constraints.

Note: It is the responsibility of the organization to ensure that the extract and transform batch process is performant for the specific data volumes present on their environments and that these volumes can be extracted, transformed, and loaded within an acceptable time frame for the organization.

Security and Regulation Considerations

The output from the batch program can be customized to be placed in a number of locations, for example, a database table, a file or a set of files.

This UMF output contains Personally Identifiable Information (PII) and it is the responsibility of the organization to ensure that the information is protected and secured in line with any regulations on the data.

Configuring Cúram with web services

You must set system administration properties for IBM Cúram SPM to integrate and communicate with IBM InfoSphere Identity Insight through web services.

System Administration Properties for Cúram and Identity Insight

These properties can be set by a system administrator user of Cúram. Use the **Properties Administration** page to enter these settings.

Property	Description
curam.programIntegrity.II.WSEndpoint	Sets the Web Service Endpoint for Identity Insight installation.
curam.programIntegrity.II.datasource	Sets the name of the data source that is sending information to the Identity Insight installation.
curam.programIntegrity.II.username	Sets the user name to be used for authentication with InfoSphere Identity Insight before any web service calls can be made. For more information, see <i>Configuring the user name and password</i> .
curam.programIntegrity.II.password	Sets the password to be used for authentication with InfoSphere Identity Insight before any web service calls can be made. For more information, see <i>Configuring the user name and password</i> .

Configuring Web Service Endpoints

In order for IBM Cúram SPM to direct the web service calls to the correct location, the IBM InfoSphere Identity Insight web service end point must be configured. The setting can specify the protocol, IP address, and port number of the web service end point. For example, `http://127.0.0.1:13510`

About this task

Log on to Cúram as a system administrator. Use **Property Administration** to administer settings that define the IBM InfoSphere Identity Insight server location from the Cúram environment.

Procedure

1. Select the **System Configurations** tab.
2. Select the **Shortcuts** panel.

3. Select **Property Administration** under the **Application Data** page navigation bar.
4. Select **Application - Program Integrity** as a category.
5. Press **Search** to display property variables.
6. Select **curam.programIntegrity.II.WSEndpoint** from the list of available properties.
7. Use the ... Actions menu to display options for handling a specific property. The following menu options are available:

Menu option	Description
Edit Value	A field appears that permits the amendment of the field.
Reset to Default	If required.
Delete	If required.

8. Select the appropriate menu option and make an amendment or selection.
9. Click the **Publish** button to complete the changes.

Configuring the Data Source

If you send UMF data to IBM InfoSphere Identity Insight, the name of the data source is added to the XML payload.

About this task

Note: The data source value must match the value added to the IBM InfoSphere Identity Insight Configuration Console as described in [“Configuring Identity Insight for Cúram”](#) on page 10, for example “CURAM”.

Log on to Cúram as a system administrator. Use **Property Administration** to administer settings that define the Identity Insight server location from the Cúram environment.

Procedure

1. Select the **System Configurations** tab.
2. Select the **Shortcuts** panel.
3. Select **Property Administration** under the **Application Data** page navigation bar.
4. Select **Application - Program Integrity** as a category.
5. Press **Search** to display property variables.
6. Select **curam.programIntegrity.II.datasource** from the list of available properties.
7. Use the ... Actions menu to display options for handling a specific property. The following menu options are available:

Choice	Description
Edit Value	A field appears that permits the amendment of the field.
Reset to Default	If required.
Delete	If required.

8. Select the appropriate menu option and make an amendment or selection.
9. Click the **Publish** button to complete the changes.

Configuring the user name and password

Configure the user name and password to allow basic web service authentication so that IBM Cúram SPM can direct the web service calls to the correct location.

About this task

Log on to Cúram as a system administrator. Use **Property Administration** to administer settings for the user name and password to allow basic IBM InfoSphere Identity Insight web service authentication.

Procedure

1. Select the **System Configurations** tab.
2. Select the **Shortcuts** panel.
3. Select **Property Administration** under the **Application Data** page navigation bar.
4. Select **Application - Program Integrity** as a category.
5. Press **Search** to display property variables.
6. Select **curam.programIntegrity.II.username** from the list of available properties.
7. Use the ... Actions menu to display options for handling a specific property. The following menu options are available:

Option	Description
Edit Value	A field appears that allows the amendment of the field.
Reset to Default	If required.
Delete	If required.

8. Select the appropriate menu option and make an amendment or selection.
9. Click **Publish** to complete the changes.
10. Repeat steps 4 - 9 to set **curam.programIntegrity.II.password**

Results

The following code snippet shows how the username and password are retrieved from the application properties.

```
@Override
public SRDWebServiceEndpointStub setIISRDSAAuthentication(
    final SRDWebServiceEndpointStub srdWebServiceSoapBindingStub)
    throws ApplicationException, InformationalException {

    final HttpTransportProperties.Authenticator basicAuthentication =
        new HttpTransportProperties.Authenticator();

    final String userName =
        Configuration.getProperty(EnvVars.ENV_PROGRAM_INTEGRITY_II_USERNAME);

    final String encryptedPassword =
        Configuration.getProperty(EnvVars.ENV_PROGRAM_INTEGRITY_II_PASSWORD);

    basicAuthentication.setUsername(userName);
    basicAuthentication.setPassword(getPlainTextPassword(encryptedPassword));
    basicAuthentication.setPreemptiveAuthentication(true);

    srdWebServiceSoapBindingStub._getServiceClient().getOptions().setProperty(
        org.apache.axis2.transport.http.HTTPConstants.AUTHENTICATE,
        basicAuthentication);

    return srdWebServiceSoapBindingStub;
}
```

Integrating the Web Services

The IBM Cúram SPM system integrates with the IBM InfoSphere Identity Insight system through web services.

Web Service APIs

IBM Cúram SPM calls the following web services that are owned by IBM InfoSphere Identity Insight:

- loadRecord
- getEntityDetail

For information on these web services, refer to the related IBM InfoSphere Identity Insight IBM Knowledge Center links:

Related information

[SRDWebService methods](#)

[getEntityDetail\(\) SOAP API Method](#)

Web Service Performance Tuning

IBM InfoSphere Identity Insight supports web service load balancing.

Load balancing can be used to mitigate performance concerns based on expected volumes of web service requests. Web service performance and scalability analysis are the responsibility of the organization.

For more information about web service performance tuning, see the IBM InfoSphere Identity Insight IBM Knowledge Center.

Related information

[webservices.properties file parameters](#)

Web Service Authentication

IBM InfoSphere Identity Insight supports basic web service authentication and authorization.

To send authentication credentials from IBM Cúram SPM to IBM InfoSphere Identity Insight, the following customization task must be implemented. A java interface *IIWebServiceAuthentication* can be implemented to include authorization and authentication for web services connections.

Example of an implementation

```
@Override
public SRDWebServiceEndpointStub setIISRDSAuthentication(
    final SRDWebServiceEndpointStub srdWebServiceSoapBindingStub)
    throws ApplicationException, InformationalException {

    final HttpTransportProperties.Authenticator basicAuthentication =
        new HttpTransportProperties.Authenticator();

    final String userName =
        Configuration.getProperty(EnvVars.ENV_PROGRAM_INTEGRITY_II_USERNAME);

    final String encryptedPassword =
        Configuration.getProperty(EnvVars.ENV_PROGRAM_INTEGRITY_II_PASSWORD);

    basicAuthentication.setUsername(userName);
    basicAuthentication.setPassword(getPlainTextPassword(encryptedPassword));
    basicAuthentication.setPreemptiveAuthentication(true);

    srdWebServiceSoapBindingStub._getServiceClient().getOptions().setProperty(
        org.apache.axis2.transport.http.HTTPConstants.AUTHENTICATE,
        basicAuthentication);

    return srdWebServiceSoapBindingStub;
}
```

For more information about web service authentication, see the related IBM InfoSphere Identity Insight IBM Knowledge Center.

Related information

[webservices.policy](#) and [webservices.passwd](#) file parameters

Configuring Logging

To turn on logging information for IBM Cúram Identity Intelligence on the IBM Cúram SPM system, an administration property can be set.

About this task

Log on to Cúram as a system administrator. Use **Property Administration** to administer settings that define the Cúram environment.

Note: When logging is turned on, UMF data that contains personally identifiable information (PII) is output to the logs. Regulatory and data privacy requirements need to be considered by the organization before using this functionality.

Procedure

1. Select the **System Configurations** tab.
2. Select the **Shortcuts** panel.
3. Select **Property Administration** under the **Application Data** page navigation bar.
4. Select **Application - Program Integrity** as a category.
5. Press **Search** to display property variables.
6. Select **curam.programintegrity.trace** from the list of available properties for logging administration.
7. Use the ... Actions menu to display options for handling a specific property. The following menu options are available:

Choice	Description
Edit Value	A field appears that permits the amendment of the field.
Reset to Default	If required.
Delete	If required.

8. Select the appropriate menu option and make an amendment or selection.
The valid values for the trace setting include trace_off, trace_on, trace_verbose and trace_ultra_verbose.
9. Click the **Publish** button to complete the changes.

Notices

This information was developed for products and services offered in the United States.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd. 19-21, Nihonbashi-Hakozakicho, Chuo-ku Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Privacy Policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies or other similar technologies that collect each user's name, user name, password, and/or other personally identifiable information for purposes of session management, authentication, enhanced user usability, single sign-on configuration and/or other usage tracking and/or functional purposes. These cookies or other similar technologies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Trademarks

IBM, the IBM logo, and [ibm.com](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/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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



Part Number:

(1P) P/N: