Project co-funded by the
CIVIL JUSTICE PROGRAMME
Of the EUROPEAN UNION

iSupport

cross-border recovery
of maintenance obligations
pour le recouvrement transfrontière
des obligations alimentaires

D2.4 Security and data protection report

Project Name:	iSupport		
Date:	May 2018	**Release:**	1.0
Authors:	Marie Vautravers, Jean-Marc Pellet		
Owner:	Philippe Lortie		
Document Name:	Security and data protection report		

Revision History

Revision Date	**Version**	**Author**	**Reviewed by**	**Remarks**
2 November 2016	0.2	Marie Vautravers	Office of child support enforcement, USA	Additional questions to Me-CODEX
5 May 2017	0.3	JM Pellet		Clarifications received from Hiba Salma, state of California Additions related to GDPR
11 June 2018	1.0	JM Pellet	Charlotte Darbas	Version for submission

Contents

Annexes

List of figures

Introduction

iSupport is an electronic case management and secure communication system for the cross-border recovery of maintenance obligations under the 2009 EU Maintenance Regulation and the 2007 Hague Child Support Convention.

To help develop iSupport, the European Commission awarded a significant grant and nine Hague Conference Member States and three organisations contributed to an initial project. It lasted from 2014 to 2016 and resulted in the delivery of the iSupport software. The iSupport software also uses the e-CODEX electronic communication technology to connect Central Authorities. Both iSupport and e-CODEX are released as open-source software under the European Union Public Licence, which helps with their sustainability, and provided free of charge (with the exception of maintenance costs for iSupport). In addition, following a 2016 decision, iSupport is developed to function with an open-source database, MySQL. Legislative steps are also being taken at European Union level to ensure the long-term sustainability of e-CODEX.

In 2016 a second EU-funded project, iSupport 2.0, started. It involves 13 States and one organisation: Austria, Belgium, Brazil, Estonia, Finland, France, Germany, Italy, the Netherlands, Norway, Portugal, Switzerland, the United States of America and the Italian Institute of Legal Information Theory and Techniques (ITTIG). The two main aspects of this project, which will last until 2018, are the extension of iSupport to other countries and its consolidation, with the addition of new functionalities that had to be postponed. With built-in security, the intention is to provide a complete package that can be readily installed by countries with little IT infrastructure. October 2016 also witnessed the successful implementation of iSupport by Portugal and the State of California.

In December 2017, a new version, including several bug fixes and improvements, was made available to participants.

From the inception, the Permanent Bureau of the HCCH has developed the iSupport software using a "privacy by design" approach which promotes privacy and data protection compliance from the start. These issues are often bolted on as an after-thought or ignored altogether. Although this approach was not a requirement of the 1995 EU Directive, it will help participating States comply with their obligations under their local legislation. It also anticipated on the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as GDPR - General Data Protection Regulation). The Regulation also states that this privacy by design must be implemented "*taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*".

The GDPR applies from 25 May 2018.

The HCCH has made his best efforts to ensure that privacy and data protection was a key consideration in the early stages of any project (Data protection working group), and then throughout its lifecycle. The use of e-CODEX is testament to this willingness, as is the planned implementation of encryption of data at rest in the application.

Prior to the start of the project, both the 2009 Regulation and the 2007 Convention have established a strong legal and practical framework in relation to data protection. The 2007 Convention provides a greater protection in the event of domestic violence issues. Specific provisions on the collection of personal data, the conditions of use and the duration of retention are set out in Article 61 and 62 of the 2009 Regulation. More generally, data shared between Central Authorities were strictly defined by the mandatory and recommended forms adopted under both instruments.

To avoid any misunderstanding, the reader is reminded that data processing and data control will be the sole responsibility of the States/authorities/bodies that implement the system, under their national applicable law and for EU Sates the EU data protection legislation. In this respect, there is an element of extra-territoriality of EU law that is introduced by Article 4 of the GDPR: "*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union*". However, the Regulation restricts this situation to "*the offerings of goods or services*" or "*monitoring of the behaviour* [of European data subjects]". In view of EU legislation and case law, international recovery of child support cannot be construed as a "service", in so far as it is an activity of governments that remains essentially funded by public funds and results of international obligations.

1 Scope

iSupport may only be used for specific purposes in relation with maintenance recovery applications made under the 2007 Hague Child Support Convention and the EU 2009 Maintenance Regulation, as well as other international agreements (such as the NY 1956 Convention) or bilateral agreements.

The 2007 Convention applies to:

- maintenance obligations arising from a parent-child relationship towards a person under the age of 21 years,
- recognition and enforcement or enforcement of a decision for spousal support when the application is made with a claim within the scope of the previous paragraph.

The EU, Albania, Turkey and Norway have extended the scope of the Convention to spousal support.

The 2009 EU Regulation applies to:

- maintenance obligations arising from a family relationship, parentage, marriage or affinity.

Non-binding instruments: States agreeing to process between themselves child / spousal support applications on the basis of reciprocity (outside a Convention or bilateral agreement) will sign an agreement or proceed to an exchange of letters. It is recommended this agreement or letters include a specific scope and all data protection requirements.

2 Type of collected data and responsibilities of participants

iSupport involves the collection of information about individuals. Those individuals are the persons involved in a maintenance recovery case: persons for whom maintenance is sought (children or spouse), representatives of the persons for whom maintenance is sought and debtors. Other information related to the assets and financial status of each party may also be collected (employers, individuals sharing assets with the debtor). This information is mandated by European and international law (content of the 2009 Regulation and 2007 Convention forms), which ensures the collection is necessary and proportionate.

Applicants are required to provide information to complete the application forms. The defendant may also be compelled to provide information on their financial/marital/personal situation.

iSupport will greatly facilitate the recovery of maintenance and will have an important impact on individuals (mainly increase the welfare of families and children around the world).

The information collected and shared through iSupport does not contain prohibited data according to Art. 9 of the GDPR or Art. 6 of Convention 108[1]. However, iSupport contains data that is potentially of interest for ill-intentioned persons: addresses of former spouses, information on income and financial situation. The address information is specifically protected under the 2007 Convention (Art. 40) and the 2009 Regulation (Art. 57) and this mechanism has been implemented in iSupport: a box indicating "non-disclosure" can be

[1] http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

ticked and the corresponding forms will be generated without disclosing the personal address of the party concerned.

The information collected either through the individual himself or through competent authorities may be shared with the State where the other party resides or where assets are located.

All participants to iSupport (Central Authority, Service Provider and HCCH coordinator) are jointly responsible for the security of the system and its activities, including if any functions are subcontracted.

The HCCH makes sure that iSupport complies with the standard software security requirements. It means that a risk analysis has been performed (please see below 3), and relevant technical security measures have been implemented in the software.

Central Authorities will be the data controller (please see 5.5.1) and therefore responsible for personal data security. Central Authorities will thus be responsible for implementing organisational security measures under their national law. Those security measures are identical to any security measures implemented for IT software used by the Central Authority. They will imply for instance keeping password and user ID in a safe place not for public view, and maintaining the iSupport user list in a timely and efficient manner.

The Service Provider will provide maintenance also in relation with security matters as directed by the HCCH, and will provide its staff members with a restricted access to iSupport information only in accordance with the terms and conditions of the Maintenance Contract (See 5.5.2). Any production issues should be replicated in the test environment reducing the need for access to production data.

3 Risk analysis – methodology

Prior to the development of the system, the Permanent Bureau has set up a Data Protection Working Group in order to identify and address data protection and security issues such as access rights and user profiles, external access, logging of changes and views, database encryption, European Data Protection Regulation etc.

This Working Group was comprised of several data protection experts and has met twice by videoconference on 15 January and 12 February 2015. Meeting reports[2] are available on the iSupport webpage.

All-important findings and recommendations of the Working Group have been incorporated as “Must Have” requirements into the Deliverables Documents aimed at potential tenderers that was released on 2 April 2015 under the call for tender.

According to the decision of the Data Protection Working group, a security and data protection working group met twice during the development of the system to undertake a security scan and ultimately draft this report.
Further to the recommendation of the Data Protection Working Group, Data Protection experts have been consulted by the Council of Bars and Law societies of Europe (CCBE) who

[2] https://assets.hcch.net/docs/9ec19157-272c-45c3-bb38-4703f5d2cbe3.zip

has produced a questionnaire on Data Protection listing all existing concerns and possible issues. This questionnaire and the answers provided by the Permanent Bureau have been reviewed by all stakeholders and are included in this report.

4 Information flows

4.1 iSupport servers

iSupport related servers are all located in the environment of the State installing iSupport. Those servers will store all functional and technical data required to run the system.

4.2 External and internal data exchange in iSupport

Data transferred **from a country to another** will be of two different types:

- Data contained in the forms (most common cases): 2009 European Regulation forms as well as 2007 Convention mandatory and recommended forms have been agreed upon by Member States of the European Union and State parties to the Convention respectively. For other international or bilateral instruments, or even reciprocity based exchanges, neutral forms have been developed on the model of Convention forms. The use of neutral forms will guarantee that only data required for maintenance recovery is transferred. Data contained in the forms is solely related to the purpose of maintenance recovery.

- Information exchanged via letters or emails (less frequent): These data cannot be subject to a specific control and are not stored per se in the system.

Data **provided by national competent authorities** to Central Authority is exchanged/processed by EU Central Authorities under articles 61 and 62 of the 2009 Regulation.

Domestic law will apply to internal data flows outside of the EU (see introduction).

Within Central Authorities, staff members can be provided with different access rights depending on their role (manager, caseworker, accountant, registrar and any specific role created by a Central Authority). Those staff members will be granted with “view”, “update”, “add” and “delete” rights that will vary depending on the iSupport screens. The iSupport “Role Screen Access Entry” screen allows the creation and modification of roles and access rights on an extremely flexible basis.

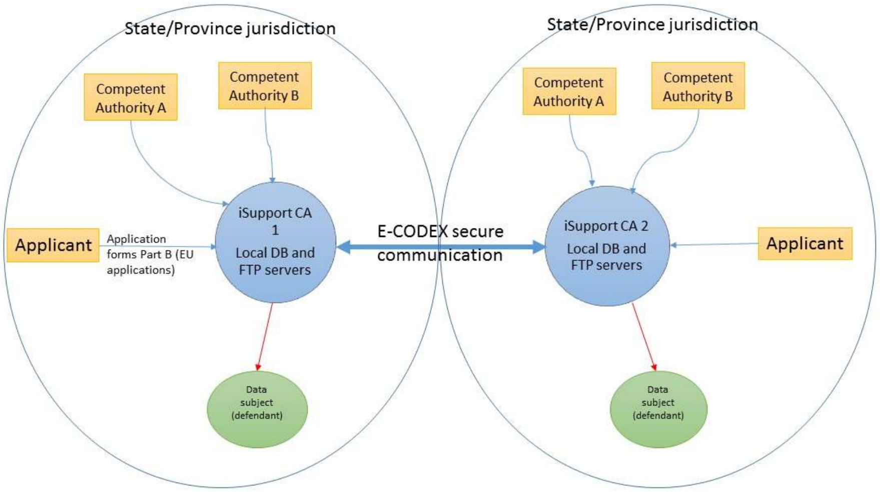


Figure 1 iSupport simplified data flow outline

5 Privacy and related risks and solutions

5.1 Risks to individuals

5.1.1 Proper and timely information of data subject

- Will the data subject be informed that their personal data are being processed, for which purpose and how?

Each Central Authority will inform the data subject under the applicable data protection legislation. Different legal requirements may apply. As a minimum best practice, the Central authority should provide the data subject with the following information:

- The fact that their personal data may be processed in iSupport
- The identity and contact details of the controller (i.e. those of the Central Authority)
- The categories of recipients to whom the data may be disclosed (i.e. competent authorities in the requested and requesting States)
- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject.

Templates letter to the applicant/defendant can be associated to one particular task in the activity list/edited to display specific appropriate notification.

The 2009 Regulation provides specific provisions about the processing of the defendant's personal data.

"*Article 63 Notification of the data subject*
1.Notification of the data subject of the communication of all or part of the information collected on him shall take place in accordance with the national law of the requested Member State.
2.Where there is a risk that it may prejudice the effective recovery of the maintenance claim, such notification may be deferred for a period which shall not exceed 90 days from the date on which the information was provided to the requested Central Authority."

This maximum deadline of 90 days has been implemented in iSupport Regulation cases as a reminder to inform the data subject when information is provided by a competent authority.

- Will the data subject be informed of their right of access (recital 34 Regulation 2009) and duly notified in conformity with Article 63 Regulation 2009?

Please refer to the answer to the question above. (It is for each CA to determine the content of the data subject notification)

- Will the data subject be informed about the people or organisations their data may be passed onto?

CF Answer to the question above.

- Does iSupport enable authorities to comply with the non-disclosure and confidentiality requirements set out in Articles 39 and 40 of the Convention, and Article 61 Regulation?

When the health, safety or liberty of a person is at risk, the case-worker ticks the non-disclosure box, and sensitive information will not be transmitted, in compliance with Articles 39 and 40 of the Convention and 57 of the 2009 Regulation. The generation of the adequate form is automatic when sending out the application.
A "Non-disclosure" notice is displayed in the case summary ribbon, as well as in the case management screen and in the debtor and creditor demo screens.
Pursuant to Article 61(2) of the 2009 Regulation, caseworkers will have the ability to only disclose the information which is adequate, relevant and not excessive. Mandatory EU forms have been designed for this purpose.

- Is the prior consent of the data subject needed before processing their information?

Personal data are processed in iSupport on the basis of specific provisions of the 2009 Regulation and 2007 Convention, therefore it is not necessary to ask for the data subject's consent in order to justify the processing. This is in line with Article 6 GDPR ("*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*").

Moreover, in Regulation cases, the applicant's personal data is only contained in Part B which is filled by the applicant.

As for Convention cases, Article 12 (2) provides that the Central Authority transmits the application "*on behalf and with the consent of the applicant".* In that view, recommended forms include a tick box indicating that "*This application is forwarded by the Central Authority on behalf of and with the consent of the applicant*".

- If the data collection includes sensitive data, will explicit consent to process such data be required from the data subject?

The GDPR prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. According to this definition, applications made under the Convention and / or the Regulation do not include sensitive data.

iSupport does not contain fields related to such data.

Specific provisions have been set out for family violence cases (please see above).

- Will it be made clear to the data subject what the data will be used for?

Applicants are aware of the purpose of their own application, and the range of possible use of the data is extremely restricted.

More generally, States and Central authorities are responsible for the actual notification of the data subject, which will be documented by the attestations found in the forms transmitted.

- Will any "non-obvious" uses of the data be made clear to the data subject *i.e.*, things that the data subject cannot realise iSupport will do from a general description of the processing?

Applications are exclusively made for maintenance recovery purposes. iSupport processes are extremely straightforward and clear. In that respect, there are no "non-obvious use" of data. Data will only be sent out to other Central Authorities.

States will be responsible for ensuring that these data are not used for any other purpose unless the data subject is informed and can give his prior consent.

2009 EU Regulation, Article 62: *Any authority or court to which information has been transmitted pursuant to Article 61 may use this only to facilitate the recovery of maintenance claims.*
Templates of letters sent to competent authorities and courts can refer to Article 61 2), 3) and 4).

2007 Convention, Article 38: *Personal data gathered or transmitted under the Convention shall be used only for the purposes for which they were gathered or transmitted*.

5.1.2 Risk in relation to the accuracy of data

- What steps will be taken to ensure the accuracy of the data?

Change logs will be kept in the system, which will ensure data integrity. All actor information can be updated in the dedicated screens (demographics and addresses).

- Is there a system of rolling reviews of data to keep the data up to date?

Periodical review of cases will be the responsibility of States. An automatic reminder for caseworkers to review the case has been implemented in iSupport after six months of inactivity in a case. This time period can be modified.

5.1.3 Risk in relation to the retention of data

- Are data being kept for no longer than is necessary to comply with relevant laws and regulations that define minimum periods of retention?

iSupport prompts caseworkers to review periodically cases that are no longer active (by default every six months). Cases can be closed (in that case they are no longer editable) or archived (in that case, data is moved from iSupport to a separate database: only basic information will be kept such as the iSupport and internal numbers, the full names and dates of birth of the debtor and persons for whom maintenance is sought). Data management, including case review, closure and archiving procedure will depend on domestic legal requirements.

- Can it be confirmed that data are not being kept on a “just in case” basis?

On the condition that relevant processes have been implemented in iSupport, and that periodical reviews are performed, cases should be archived on time, according to national law.

5.2 Applicable law

- How is iSupport "future proofed" to ensure compliance with the General Data Protection Regulation?

The iSupport solution complies with the 2009 Regulation data protection requirements and more generally with the data protection EU Directive 95/46/EC.

The GDPR will apply from 25 May 2018. It promotes a risk-based approach, with security measures in proportion to those risks. Most of its innovations centre on commercial activities, therefore outside of iSupport’s scope.

Consent of the data subject is not necessary as “*processing is necessary for compliance with a legal obligation to which the controller is subject*” and “*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*”.

iSupport does not handle any prohibited data according to Art. 9 GDPR.

In terms of additional responsibilities for data controllers in the iSupport participating States, Art.13 lists the information that should be provided where personal data are collected from the data subject (addition from the Directive in italics):

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- The contact details of the data protection officer, where applicable;
- The purposes of the processing for which the personal data are intended as well as the *legal basis* for the processing;
- The recipients or categories of recipients of the personal data, if any;
- Where applicable, the fact that the controller *intends to transfer personal data to a third country or international organisation* and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
- *The period for which the personal data will be stored*, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from the controller access to and rectification or *erasure of personal data or restriction of processing concerning the data subject*;
- The right to lodge a complaint with a supervisory authority.

Slightly more information must be provided where personal data have not been obtained from the data subject, as listed in Art. 14 (this was already present in the Directive): the categories of data concerned; from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

Right of access can be obtained at reasonable intervals and free of charge. It should also be noted that the controller should implement reasonable measures to verify the identity of a data subject who requests access.

Rectification can be obtained from the controller without undue delay.

The right of erasure and to be forgotten shall be granted without undue delay when the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; when the data subject withdraws consent and there is no other legal ground for the processing of the data; when the data have to be erased for compliance with a legal obligation to which the controller is subject.

The right of erasure is balanced with the right of freedom of expression and information and the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

There is also a right to restriction of processing where the accuracy of the data is contested by the data subject; where the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.

Provisions on the transfer of data to third countries and international organisations are also very much in the continuity of the Directive. The basis for the transfer can either be an adequacy decision of the European Commission or a legally binding and enforceable instrument between public authorities or bodies.

- Under which national law(s) are data stored?

Each iSupport instance database is located in the State that will be responsible for ensuring compliance with the applicable domestic law.

- Which jurisdiction's data protection law(s) do apply and is the solution be compliant with each of these laws?

Data management within Central Authorities as well as data import from other national competent authorities are the responsibility of the State, in compliance with its national law and jurisdiction rules.

2007 Convention, Article 39 Confidentiality: "*Any authority processing information shall ensure its confidentiality in accordance with the law of its State*".

2009 EU Regulation, Article 62.4: "*Any authority processing information communicated to it pursuant to Article 61 shall ensure the confidentiality of such information, in accordance with its national law.*"

In that respect, iSupport is extremely flexible and allows any adjustment locally required. For instance, iSupport does not allow the permanent deletion of data except for archiving purpose and therefore ensures appropriate access right of the data subject to his personal data.

In addition, as already indicated, access rights and archiving procedure are customizable depending on each State's domestic data protection rules.

Cross-border data flows will mainly occur through Regulation and Convention forms. States that implement and use iSupport have agreed to the administrative cooperation and the transfer of data for the purpose of maintenance recovery.

5.3 Appropriate security measures

- Is the level of security adopted appropriate to the risks represented by the processing and the nature of the data to be protected?

It is to each Central Authority to implement measures to guard against theft, malicious damage or corruption (including computer viruses), unlawful access, accidental disclosure, loss and destruction. Particular consideration should be given to the security of sensitive data.

As regards security technical requirements, please see the System Security Documentation provided by Protech (Annex 1).

- What security accreditations (for example, ISO 27001/2) does the service provider hold?

The service provider responsible for the maintenance of the system (Protech) is a CMMI Level 3 organization, which is a certification from Carnegie Mellon University.

- How will the integrity and confidentiality of the data be guaranteed?

The use of e-CODEX ensures that the data are protected against loss, theft or unauthorised access, as they are encrypted when they travel on the internet. Moreover, e-CODEX communication happens between a set of participants that are known to each other through the issuing of processing modes (p-modes) following exchanges of public certificates.
In addition, while participants remain responsible for ensuring the integrity and confidentiality of data once they are stored on their iSupport installation, iSupport is currently implementing the encryption of data at rest in the application, as recommended in Art. 32 GDPR.

5.4 Transferring personal data to non-EEA countries

- Where applicable, will the consent of the data subject be obtained to transfer personal data to countries outside the EEA which are not designated as "adequate" by the European Commission?

(please see 5.2).

The derogation set out in Article 46(1) a of the GDPR applies. No adequacy decision is required as long as the data transfer is legally required on important public interest grounds and for the establishment, exercise of legal claims. Applications made and sent through iSupport under a binding international legal instrument fall under that category.

5.5 Associate organization risk - Contractual arrangements

5.5.1 Data controller and data processor

The Central Authority using iSupport will be the Data processor.
The Data controller is the natural or legal person, public authority, agency or any other body appointed in each State using iSupport. The identity of the controller cannot be predicted and will depend on each State's policy.

The identification of the data controller and possibly data processor may be included in the agreement signed by States implementing iSupport.

As long as Central Authorities do not subcontract the processing of personal data, Data processor and Data controller will be the same. If they subcontract the provision of Servers and other IT services for the purpose of iSupport implementation, it will be their responsibility to sign a contract with the contractor and identify his data protection duties.

5.5.2 Contractual provisions relating to data protection between the data controller(s) and the data processor(s)

The Service provider might have access to personal data. Specific contractual provisions that have been set out to that effect in the iSupport Maintenance Contract:

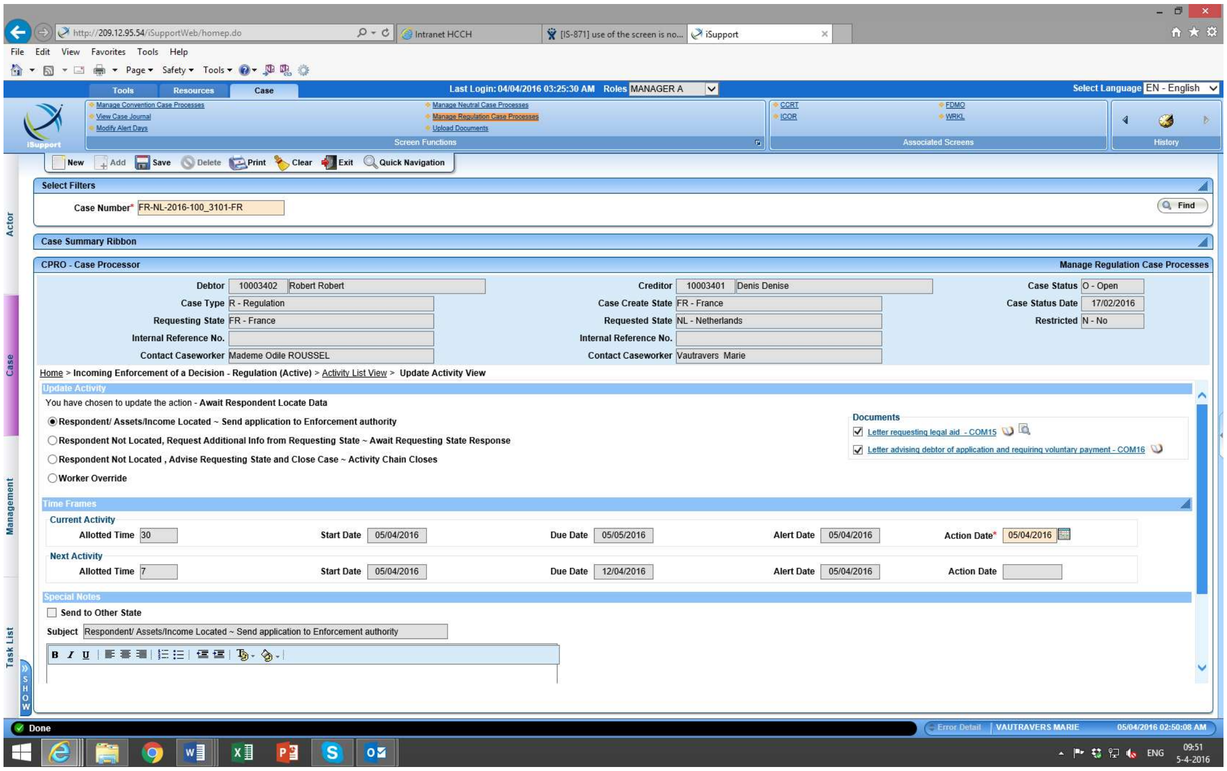
Article 32. Processing of personal data

84. Where the Contract requires the processing of Personal Data by the Contractor, the Contractor may act only under the explicit direction of the Contracting Authority, in particular with regard to the purposes of the processing, the categories of data which may be processed, the recipients of the data and the means by which the data subject may exercise his rights.

85. The Contractor shall grant its Personnel access to the data to the extent necessary for the performance, management and monitoring of the contract.

86. The Contractor undertakes to adopt all technical and organisational security measures that are necessary to protect all Personal Data that are under its direct or indirect control during the course of this Contract and the Contractor agrees and warrants that it will:

a) Ensure the compliance of the Software with the European Legislation on protection of Personal Data and any relevant domestic legislation for any State in which it is providing services or where the Solution is being developed or tested;
b) Ensure all of its personnel are properly screened and adequately trained concerning the legislative and contractual requirements concerning the protection of personal data required by this Contract;
c) Take all required precautions to prevent any unauthorised person from gaining access to any computer systems that is processing personal data;
d) Ensure that authorised users of the Solution during the development and deployment of the Solution can access only the personal data to which their access rights refer;
e) Develop the Solution strictly in compliance with the Deliverables Document requirements concerning personal data; and
f) Ensure that the Solution provides that any personal data being processed on behalf of third parties can be processed only in the manner prescribed by the Contracting Authority.


http://209.12.95.54/iSupportWeb/homep.do
Intranet HCCH
[IS-871] use of the screen is no...
iSupport
File Edit View Favorites Tools Help
Page Safety Tools
Tools Resources Case
Manage Convention Case Processes
View Case Journal
Modify Alert Days
Manage Neutral Case Processes
Manage Regulation Case Processes
Upload Documents
Screen Functions
CCRT
ICOR
FDMO
WRKL
Associated Screens
History
New Add Save Delete Print Clear Exit Quick Navigation
Find
Actor
Case
Management
Task List
» SHOW
Done
Error Detail
ENG

Last Login: 04/04/2016 03:25:30 AM Roles MANAGER A

Select Language EN - English

Select Filters

Case Number* FR-NL-2016-100_3101-FR

Case Summary Ribbon

CPRO - Case Processor — Manage Regulation Case Processes

Debtor	10003402 Robert Robert	Creditor	10003401 Denis Denise	Case Status	O - Open
Case Type	R - Regulation	Case Create State	FR - France	Case Status Date	17/02/2016
Requesting State	FR - France	Requested State	NL - Netherlands	Restricted	N - No
Internal Reference No.		Internal Reference No.			
Contact Caseworker	Mademe Odile ROUSSEL	Contact Caseworker	Vautravers Marie		

Home > Incoming Enforcement of a Decision - Regulation (Active) > Activity List View > Update Activity View

Update Activity

You have chosen to update the action - **Await Respondent Locate Data**

● Respondent/ Assets/Income Located ~ Send application to Enforcement authority
○ Respondent Not Located, Request Additional Info from Requesting State ~ Await Requesting State Response
○ Respondent Not Located , Advise Requesting State and Close Case ~ Activity Chain Closes
○ Worker Override

Documents
☑ Letter requesting legal aid - COM15
☑ Letter advising debtor of application and requiring voluntary payment - COM16

Time Frames

Current Activity									
Allotted Time	30	Start Date	05/04/2016	Due Date	05/05/2016	Alert Date	05/04/2016	Action Date*	05/04/2016
Next Activity									
Allotted Time	7	Start Date	05/04/2016	Due Date	12/04/2016	Alert Date	05/04/2016	Action Date	

Special Notes

□ Send to Other State

Subject Respondent/ Assets/Income Located ~ Send application to Enforcement authority

VAUTRAVERS MARIE 05/04/2016 02:50:08 AM

09:51
5-4-2016

Figure 2 iSupport Screenshot. Notification of the defendant

iSupport

System Documentation
Security and Privacy

Version No. 1.1

Table of Contents

Figures and Tables

Introduction

This document lists the objectives corresponding to the Security and Privacy of the iSupport application.

The narrative documents the iSupport Security and Privacy settings compliance to those requirements as well as the security-related tasks/policies that are expected from each State that implements iSupport.

It is recalled that iSupport will be implemented on each State local environment/servers/databases and will hence be subject to different security policies and procedures. Common requirements are detailed in this document, subject to the approval of the iSupport Governing Body.

System Requirements – Security and Privacy

1. OBJECTIVE 1: The State must have policies and procedures to evaluate the system for risk on a periodic basis.

State Requirements:

Responsibility for conducting periodic risk analysis must be formally assigned.

A specific timetable for conducting a risk analysis must be established. The plan must ensure that special evaluations are performed whenever a significant change to the system's physical security, hardware, or operating system software occurs (cf iSupport maintenance services)

System Requirements

The system must ensure that vulnerability to fraud or theft, loss of data, physical destruction, unauthorized access, intrusion, and harm to agency activities is inexistent or as limited as possible.

a. Responsibility for conducting periodic risk analysis must be formally assigned.

The responsibility for conducting periodic risk analysis for iSupport is assigned to each particular State.

b. A specific timetable for conducting a risk analysis must be established. The plan must ensure that special evaluations are performed whenever a significant change to the system's physical security, hardware, or operating system software occurs.

The responsibility for conducting periodic risk analysis for iSupport should be done by iSupport system administrator in respective states.

c. The risk analysis must measure the system's vulnerability to fraud or theft, loss of data, physical destruction, unauthorized access, intrusion, and harm to agency activities.

The iSupport System is a web-enabled application which is accessible only via a secure intranet to prevent outside intrusion. It is not open to public access.

Access to iSupport is only through https to ensure industry-standard encryption. For OWASP compliance, we recommend the approach of using hardware-based web application firewalls such as Barracuda. To ensure that the application is not vulnerable to additional attacks, we use OpenVas vulnerability scanning.

The technical architecture of the iSupport application is designed to make the application secure against unauthorized access, intrusion, and data fraud. We provide role-based access, and ensure that the TOMCAT and database servers are not accessible from outside the application server, except for maintenance and admin purposes.

States should adopt a methodology to close all Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) ports and allow traffic only on specific ports within each tier, providing restricted security and preventing unwanted intrusion.

Even though the iSupport application is designed to be secure, States should conducts periodic risk analysis to measure the application vulnerability at various levels. This is to ensure the intrusion detection measures are up to date.

2. OBJECTIVE 2: The system must be protected against unauthorized access to computer resources and data in order to reduce erroneous or fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

State System Requirements:

a. The State must have written procedures regarding the safeguarding of data which addresses integrity, completeness, accuracy, use of and access to data in the system. The procedures must include policies regarding agency personnel access to data in the system, sharing of data with other persons, limiting the use of and access to data to the extent necessary to administer the program, and specify the data that may be used for specific program purposes and other authorized purposes and the personnel and other authorized persons who may have access to such data. The system must limit disclosure of personal information or financial institution data match information.

Procedures for system and terminal user identification assignment, maintenance, and cancellation must be in place and include:

Delegation and maintenance of the password system limited to a select number of people, and

A mechanism to quickly notify those responsible when there are personnel changes.

System Requirements:

System, terminal, and password identifications must be controlled, randomly selected, and must uniquely identify the system user.

Password security must extend to the functional screen level and limit the user's capability to view and/or update those screens.

The system must automatically require the system user to change passwords periodically.

The system must provide security levels for access to records and files and utilize automatic sign-off techniques.

The system must detect, record, and lock out unauthorized attempts to gain access to system software and data.

Access to sensitive documents or forms generated by the system must be restricted.

Fiscal data acquired by the system must be protected from unauthorized inquiries and must be kept in a separate data file if necessary to ensure its security.

For security purposes, the system must be capable of maintaining information on all changes to critical records and/or data fields (e.g., Arrearage Balance, Monthly Court-Ordered Support Amounts, SSN, Name, Family Violence Indicator, etc.), including identification of the responsible system user/caseworker and date/time of the change.

The system must be capable of routinely monitoring the access to use of the automated system.

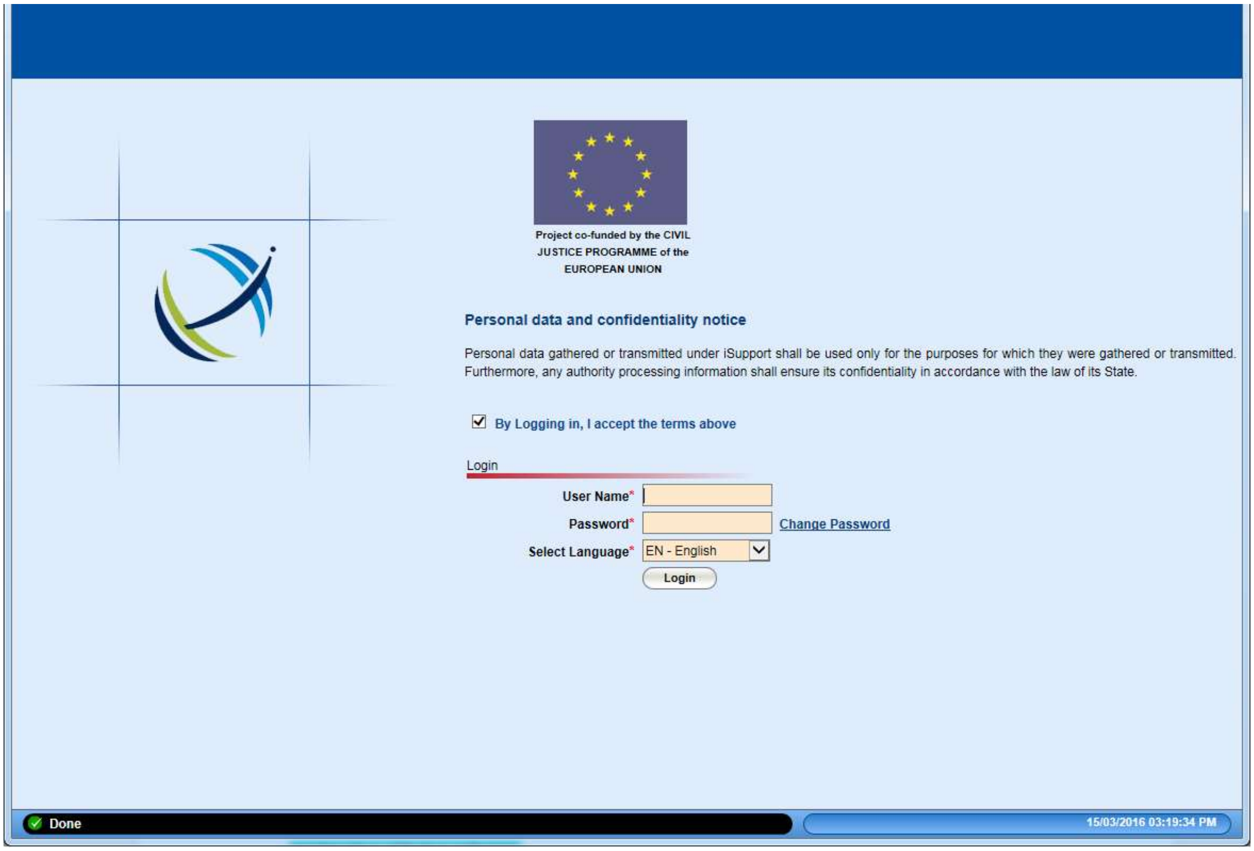
The system document generation function must automatically prevent disclosure of personally identifiable information on persons designated as subject to family violence.

a. **The State must have written procedures regarding the safeguarding of data which addresses integrity, completeness, accuracy, use of and access to data in the system. The procedures must include policies regarding agency personnel access to data in the system, sharing of data with other persons, limiting the use of and access to data to the extent necessary to administer the program, and specify the data that may be used for specific program purposes and other authorized purposes and the personnel and other authorized persons who may have access to such data. The system must limit disclosure of personal information or financial institution data match information**.

Managing data access in iSupport:

iSupport is a web-enabled application accessible only via a secure intranet. It is not open to public access. The iSupport users might initially log on to the State network and or directly to the iSupport application. They will initiate the iSupport application which will display the login page for sign on.

The users must provide the user name (also known as the User ID) and password in the iSupport login page to sign on to the iSupport application. The user name and password are authenticated against the iSupport applications user name and password. On successful authentication, the iSupport application will establish the authorization and enable application access based on the user's role(s).



Project co-funded by the CIVIL JUSTICE PROGRAMME of the EUROPEAN UNION

Personal data and confidentiality notice

Personal data gathered or transmitted under iSupport shall be used only for the purposes for which they were gathered or transmitted. Furthermore, any authority processing information shall ensure its confidentiality in accordance with the law of its State.

☑ By Logging in, I accept the terms above

Login

User Name*

Password*

Select Language* EN - English

Done

15/03/2016 03:19:34 PM

Figure 3 - iSupport login page – requires user name and password to sign on

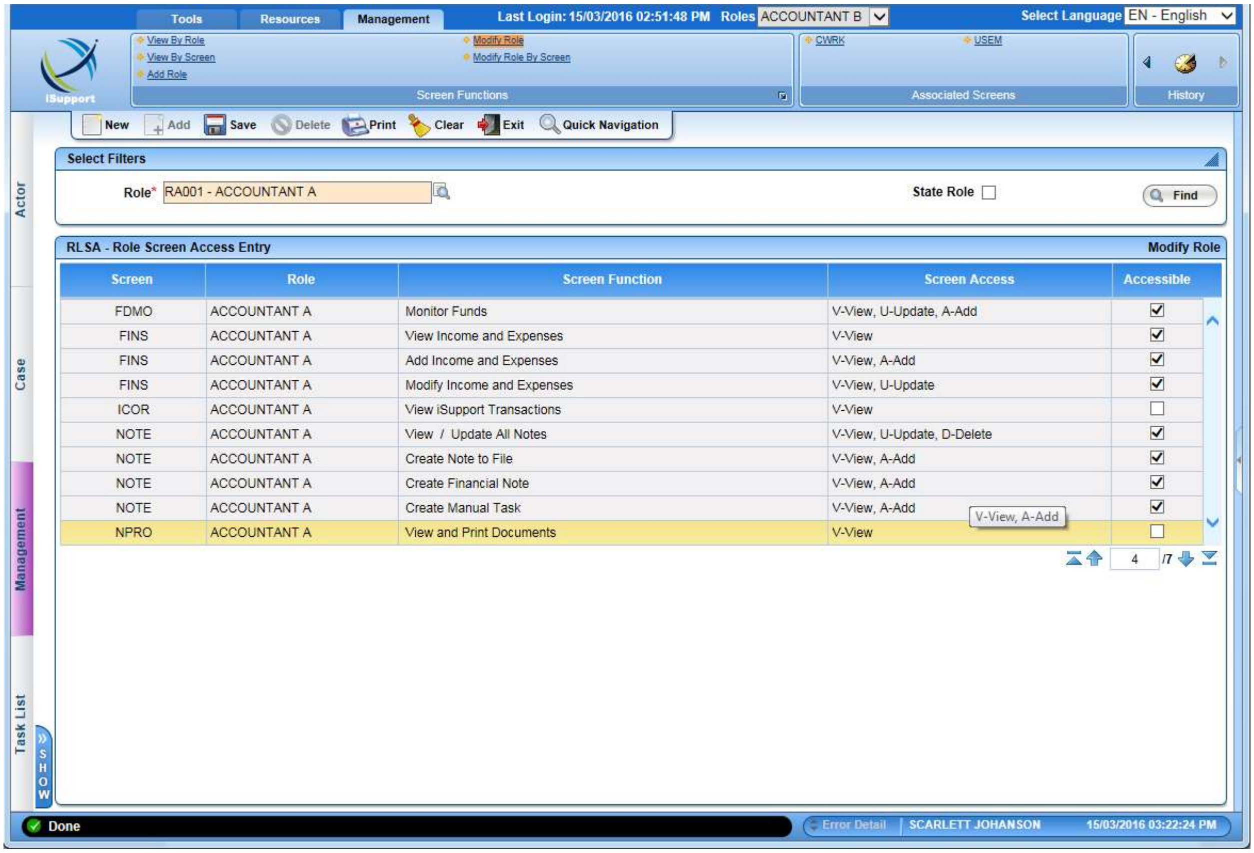
iSupport application password follows ISO standards. It makes the password strong with a combination of below criteria's:

Strong passwords should be used. A strong password will include a combination of:

1. Alphabetic
2. Combination of both upper and lower case: A to Z and a to z
3. Numeric: 0 to 9
4. Special Characters such as: ~!@#$%^*( )+=[ ] { } ?, etc.

    Note: The special characters not allowed are > < ; and &
5. Passwords should be at least 8 positions in length and not more than 15 (i.e. 8 - 15).

The iSupport application controls users' data access via application roles. In iSupport, The Role Screen Access (RLSA) screen is used to create screen access privileges for the various application roles. Access can be restricted to the entire iSupport screen or to a selected function within the specific screen. Also, new roles can be created using the appropriate RLSA screen function.



Last Login: 15/03/2016 02:51:48 PM Roles ACCOUNTANT B

Select Language EN - English

Select Filters

Role* RA001 - ACCOUNTANT A

State Role ☐

RLSA - Role Screen Access Entry

Modify Role

Screen	Role	Screen Function	Screen Access	Accessible
FDMO	ACCOUNTANT A	Monitor Funds	V-View, U-Update, A-Add	☑
FINS	ACCOUNTANT A	View Income and Expenses	V-View	☑
FINS	ACCOUNTANT A	Add Income and Expenses	V-View, A-Add	☑
FINS	ACCOUNTANT A	Modify Income and Expenses	V-View, U-Update	☑
ICOR	ACCOUNTANT A	View iSupport Transactions	V-View	☐
NOTE	ACCOUNTANT A	View / Update All Notes	V-View, U-Update, D-Delete	☑
NOTE	ACCOUNTANT A	Create Note to File	V-View, A-Add	☑
NOTE	ACCOUNTANT A	Create Financial Note	V-View, A-Add	☑
NOTE	ACCOUNTANT A	Create Manual Task	V-View, A-Add	☑
NPRO	ACCOUNTANT A	View and Print Documents	V-View	☐

V-View, A-Add

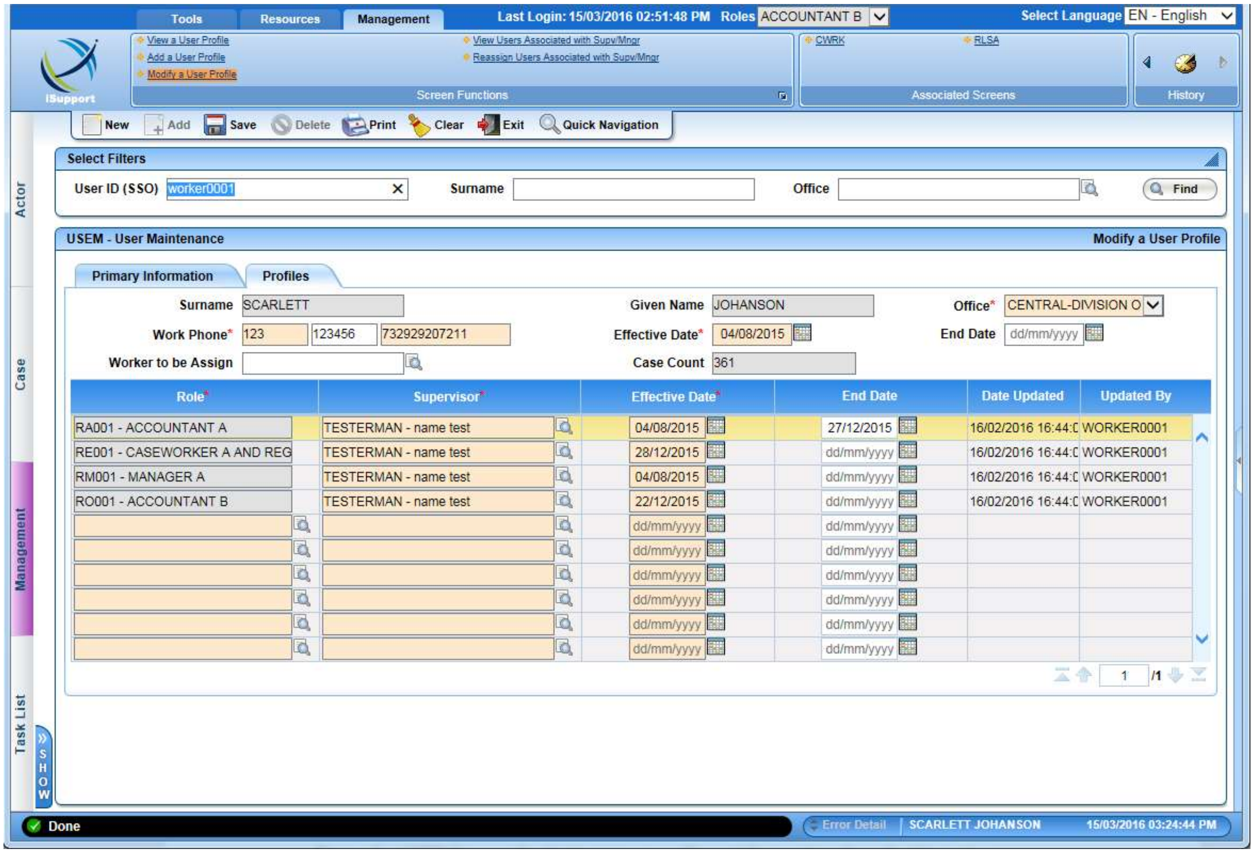
4 /7

Done

SCARLETT JOHANSON 15/03/2016 03:22:24 PM

Figure 4 - RLSA screen displaying screen access permissions for roles

Once the roles and the corresponding screen access permissions are established, the iSupport application security administrators assign the appropriate roles for each user on the User Maintenance (USEM) Screen.



Last Login: 15/03/2016 02:51:48 PM Roles ACCOUNTANT B

Select Language EN - English

Select Filters

User ID (SSO) worker0001 Surname Office

USEM - User Maintenance — Modify a User Profile

Primary Information | Profiles

Surname	SCARLETT	Given Name	JOHANSON	Office*	CENTRAL-DIVISION O
Work Phone*	123 123456 732929207211	Effective Date*	04/08/2015	End Date	dd/mm/yyyy
Worker to be Assign		Case Count	361		

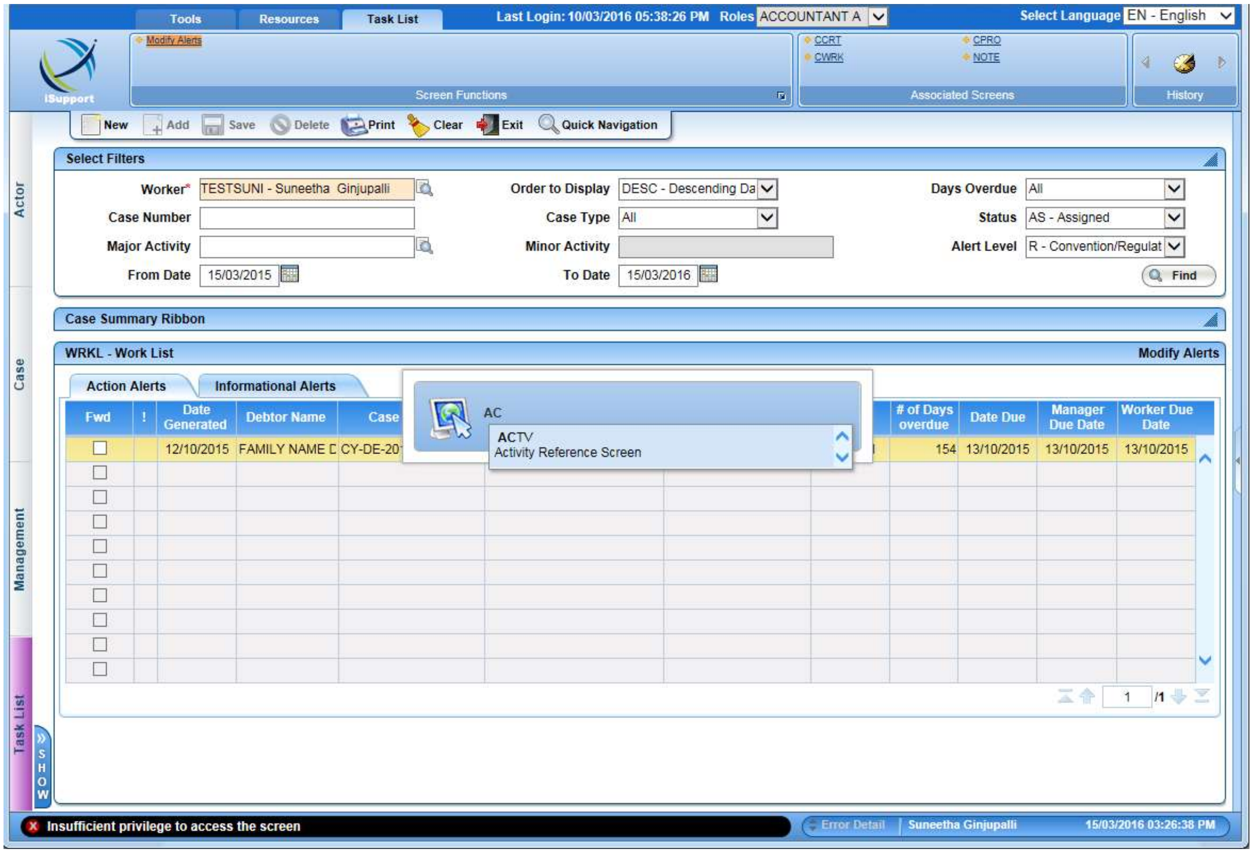
Role*	Supervisor*	Effective Date*	End Date	Date Updated	Updated By
RA001 - ACCOUNTANT A	TESTERMAN - name test	04/08/2015	27/12/2015	16/02/2016 16:44:0	WORKER0001
RE001 - CASEWORKER A AND REG	TESTERMAN - name test	28/12/2015	dd/mm/yyyy	16/02/2016 16:44:0	WORKER0001
RM001 - MANAGER A	TESTERMAN - name test	04/08/2015	dd/mm/yyyy	16/02/2016 16:44:0	WORKER0001
RO001 - ACCOUNTANT B	TESTERMAN - name test	22/12/2015	dd/mm/yyyy	16/02/2016 16:44:0	WORKER0001
		dd/mm/yyyy	dd/mm/yyyy		
		dd/mm/yyyy	dd/mm/yyyy		
		dd/mm/yyyy	dd/mm/yyyy		
		dd/mm/yyyy	dd/mm/yyyy		
		dd/mm/yyyy	dd/mm/yyyy		
		dd/mm/yyyy	dd/mm/yyyy		

1 /1

Done | SCARLETT JOHANSON | 15/03/2016 03:24:44 PM

Figure 5 - USEM Screen displaying a user profile and the assigned application roles

Upon successful login, the application server will validate the User ID against the assigned roles to determine if the user should be granted access to the screen or screen function, when the iSupport user tries to navigate from screen-to-screen. If the user profile is associated with the necessary application role(s), the user will be allowed to navigate and view the screen or use a screen function. If the user does not have the appropriate role to access the screen or screen function(s), iSupport will display a message about insufficient privilege, and the screen function(s) is grayed out and disabled to preclude selection, when security has been restricted at the screen function level.



Last Login: 10/03/2016 05:38:26 PM Roles ACCOUNTANT A

Select Language EN - English

Select Filters

Worker*	TESTSUNI - Suneetha Ginjupalli	Order to Display	DESC - Descending Da	Days Overdue	All
Case Number		Case Type	All	Status	AS - Assigned
Major Activity		Minor Activity		Alert Level	R - Convention/Regulat
From Date	15/03/2015	To Date	15/03/2016		

WRKL - Work List — Modify Alerts

Action Alerts | Informational Alerts

AC

ACTV
Activity Reference Screen

Fwd	!	Date Generated	Debtor Name	Case	# of Days overdue	Date Due	Manager Due Date	Worker Due Date
□		12/10/2015	FAMILY NAME D	CY-DE-20	154	13/10/2015	13/10/2015	13/10/2015
□								
□								
□								
□								
□								
□								
□								
□								
□								

1 /1

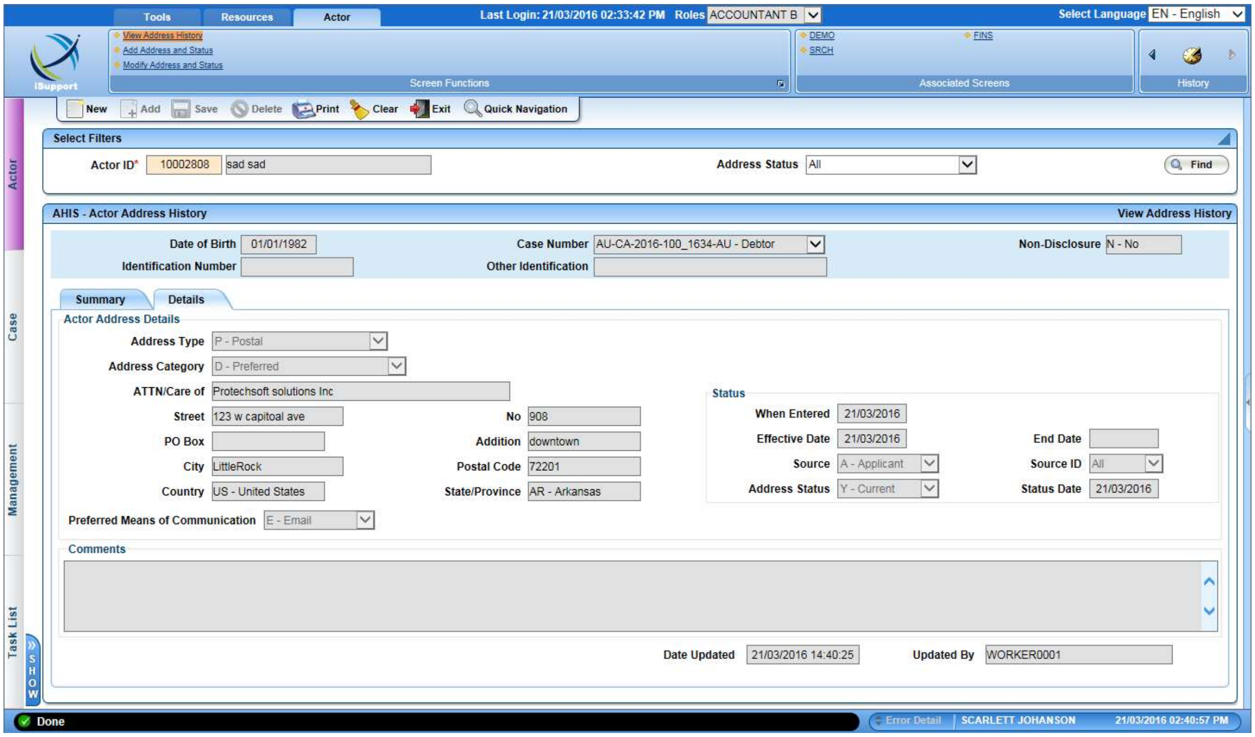
Insufficient privilege to access the screen

Suneetha Ginjupalli 15/03/2016 03:26:38 PM

Figure 4 – iSupport restricting a user with insufficient privilege to access the screen

Limiting disclosure of data to external agencies:

When locate information is received, caseworker will verify the information before updating/modifying in to iSupport.



Last Login: 21/03/2016 02:33:42 PM Roles ACCOUNTANT B

Select Language EN - English

Select Filters

Actor ID* 10002808 sad sad

Address Status All

AHIS - Actor Address History

View Address History

Date of Birth 01/01/1982

Case Number AU-CA-2016-100_1634-AU - Debtor

Non-Disclosure N - No

Identification Number

Other Identification

Actor Address Details

Address Type P - Postal

Address Category D - Preferred

ATTN/Care of Protechsoft solutions Inc

Street 123 w capitoal ave

No 908

PO Box

Addition downtown

City LittleRock

Postal Code 72201

Country US - United States

State/Province AR - Arkansas

Preferred Means of Communication E - Email

Status

When Entered 21/03/2016

Effective Date 21/03/2016

End Date

Source A - Applicant

Source ID All

Address Status Y - Current

Status Date 21/03/2016

Comments

Date Updated 21/03/2016 14:40:25

Updated By WORKER0001

Done

SCARLETT JOHANSON 21/03/2016 02:40:57 PM

Figure 6 - Member Address History (AHIS) displaying locate Source and Address Status

When extracting this locate data to the interface batch files, depending on the locate source or if the locate status is set to Pending Verification, iSupport will not include the information to the file. This is to ensure that the data is not shared with the external agencies without independent verification. The information is included in the outbound interface files only if the status is set to Confirmed Good.

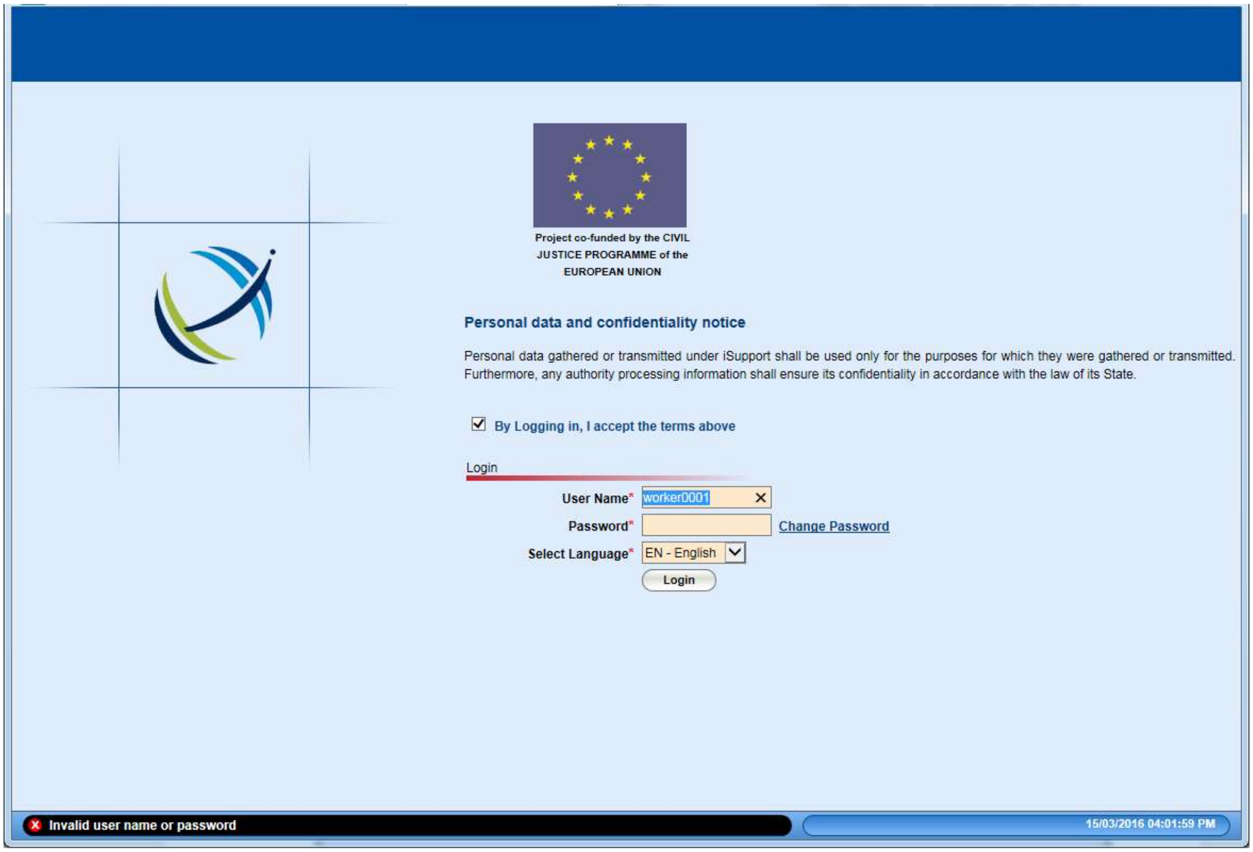
Only the verified address will be transferred to the other State.

b. System, terminal, and password identifications must be controlled, randomly selected, and must uniquely identify the system user.

Through the USEM screen, the manager or the administrator can maintain and manage user ID’s and passwords.

c. Password security must extend to the functional screen level and limit the user's capability to view and/or update those screens.

iSupport will restrict the user from logging into the application, if the password provided by the user is invalid.



Project co-funded by the CIVIL JUSTICE PROGRAMME of the EUROPEAN UNION

Personal data and confidentiality notice

Personal data gathered or transmitted under iSupport shall be used only for the purposes for which they were gathered or transmitted. Furthermore, any authority processing information shall ensure its confidentiality in accordance with the law of its State.

☑ By Logging in, I accept the terms above

Login

User Name* worker0001

Password*

Select Language* EN - English

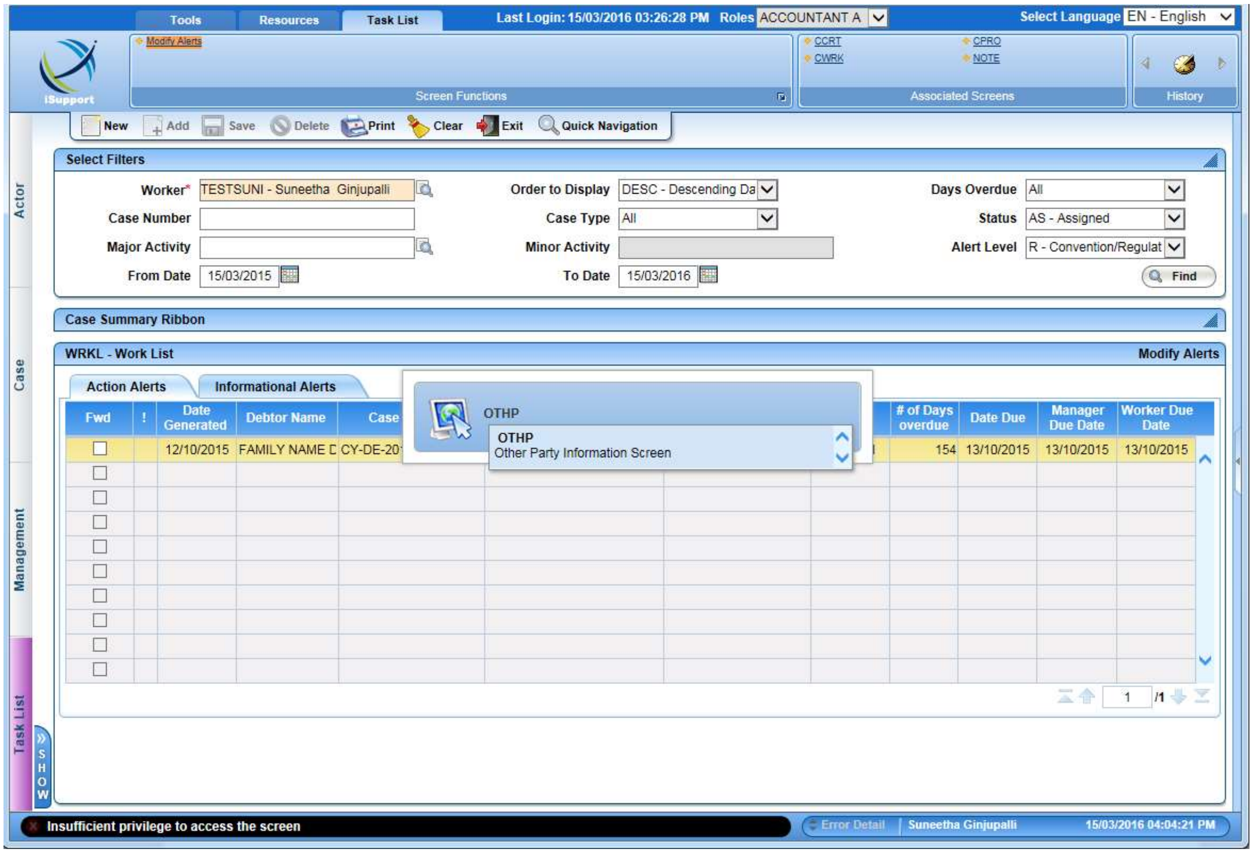
Invalid user name or password

15/03/2016 04:01:59 PM

Figure 7 - iSupport displaying login failure upon providing invalid password

Within the iSupport application, a user’s data access is controlled via application roles. Upon successful login, the application server will validate the User ID against the assigned roles to determine access permissions to the screen or screen function, when the iSupport user tries to navigate from screen-to-screen.

If a user does not have the appropriate role to access the screen, iSupport will display a message about insufficient privilege (Figure 6). If a user does not have the appropriate role to access the screen function(s) will be grayed out and disabled to preclude selection (Figure 7), when security has been restricted at the screen function level.



Last Login: 15/03/2016 03:26:28 PM Roles ACCOUNTANT A

Select Language EN - English

Worker*	TESTSUNI - Suneetha Ginjupalli	Order to Display	DESC - Descending Da	Days Overdue	All
Case Number		Case Type	All	Status	AS - Assigned
Major Activity		Minor Activity		Alert Level	R - Convention/Regulat
From Date	15/03/2015	To Date	15/03/2016		

OTHP

OTHP
Other Party Information Screen

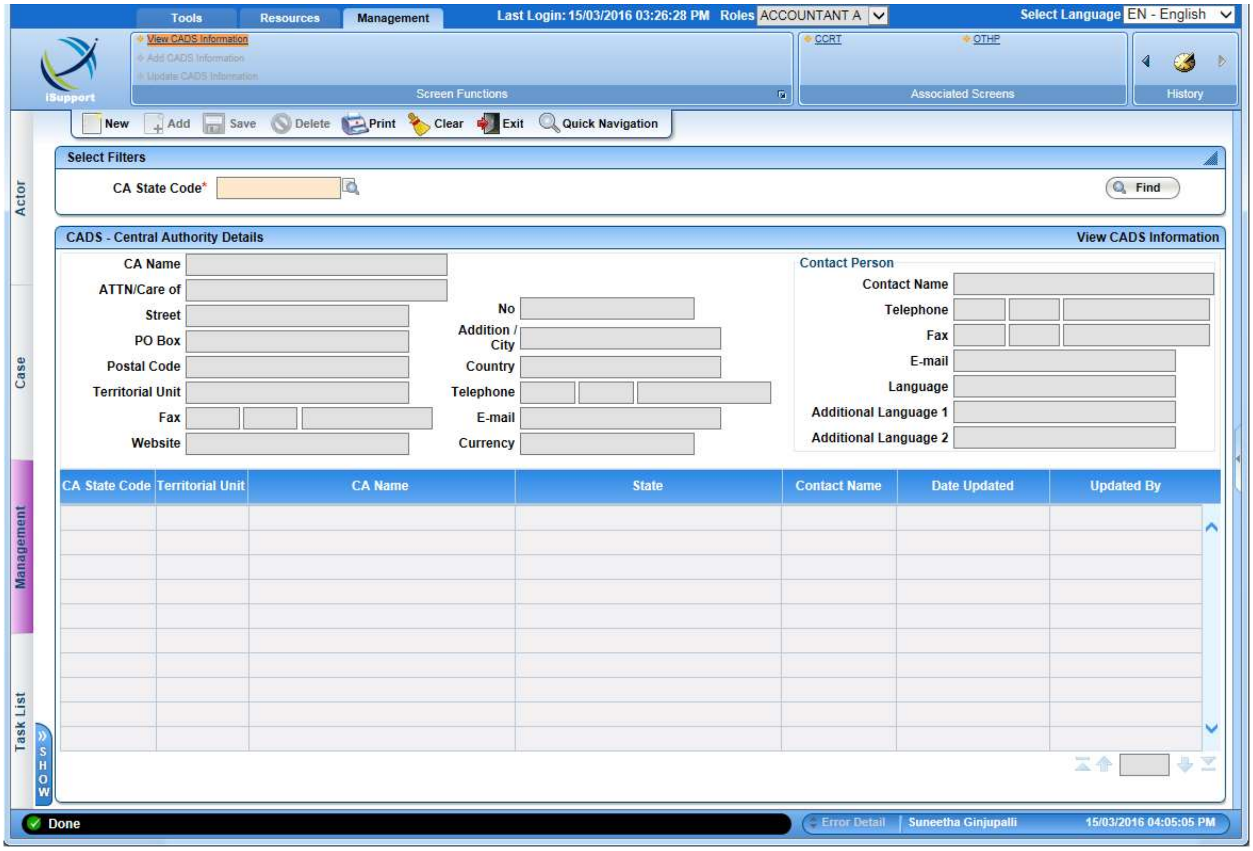
Fwd	!	Date Generated	Debtor Name	Case	# of Days overdue	Date Due	Manager Due Date	Worker Due Date
□		12/10/2015	FAMILY NAME D	CY-DE-20	154	13/10/2015	13/10/2015	13/10/2015
□								
□								
□								
□								
□								
□								
□								
□								
□								

1 /1

Insufficient privilege to access the screen

Suneetha Ginjupalli 15/03/2016 04:04:21 PM

Figure 8 – Work List (WRKL) screen displaying message about insufficient privilege upon trying to navigate to a screen



Last Login: 15/03/2016 03:26:28 PM

Roles: ACCOUNTANT A

Select Language: EN - English

Done

Suneetha Ginjupalli

15/03/2016 04:05:05 PM

Figure 9 - CADS screen displaying disabled screen functions (Add CADS Information and Update CADS Information) based on user's roles

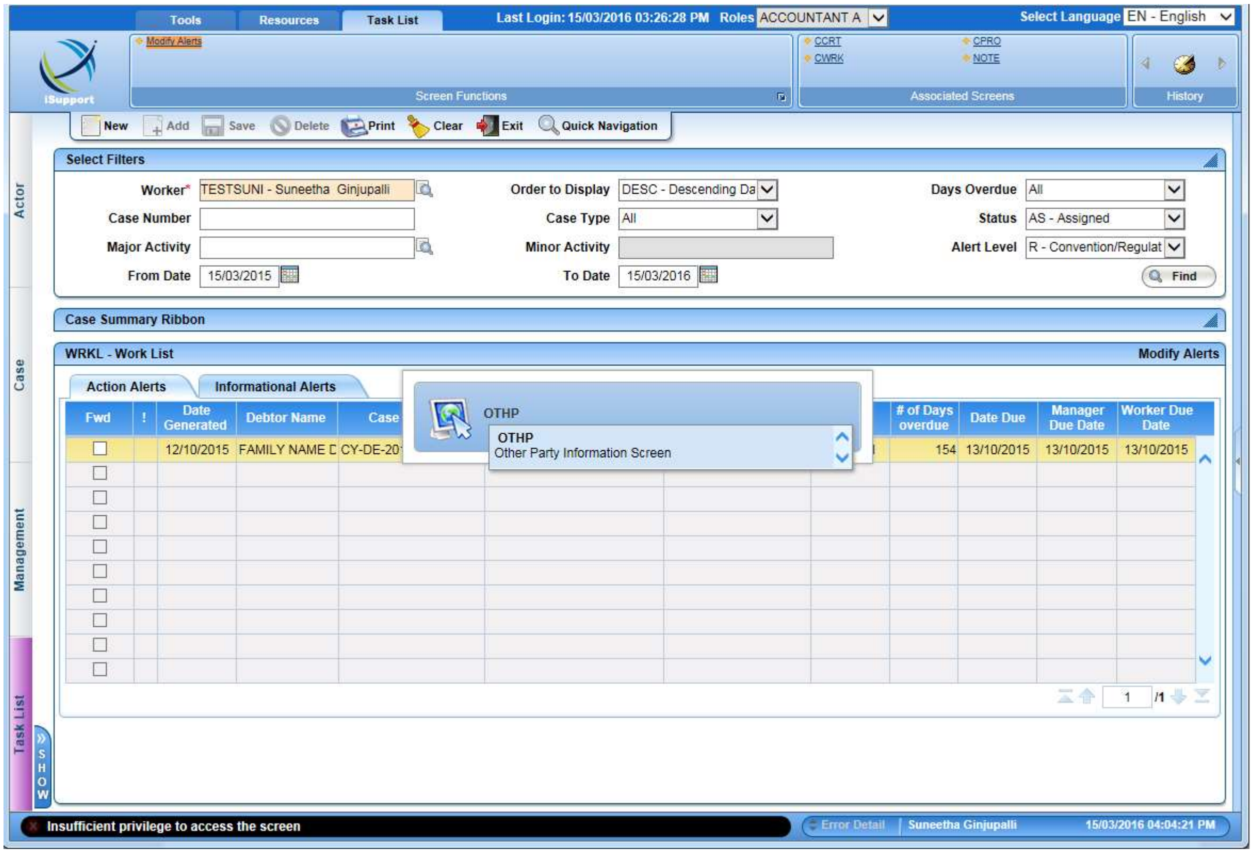
d. The system must automatically require the system user to change passwords periodically.

This functionality is not currently provided by iSupport. However, managers or administrators can reset passwords manually.

e. The system must provide security levels for access to records and files and utilize automatic sign-off techniques.

Within the iSupport application, a user's data access is controlled via application roles. Upon successful login, the application server will validate the User ID against the assigned roles to determine access permissions to the screen or screen function, when the iSupport user tries to navigate from screen-to-screen.

If the user does not have the appropriate role to access the screen (no access to any of the screen function(s)), iSupport will display a message about insufficient privilege (Figure 8). If the user does not have the appropriate role to access any of the screen function(s) are grayed out and disabled to preclude selection (Figure 9), when security has been restricted at the screen function level.



Last Login: 15/03/2016 03:26:28 PM Roles ACCOUNTANT A

Select Language EN - English

Select Filters

Worker* TESTSUNI - Suneetha Ginjupalli

Order to Display DESC - Descending Da

Days Overdue All

Case Number

Case Type All

Status AS - Assigned

Major Activity

Minor Activity

Alert Level R - Convention/Regulat

From Date 15/03/2015

To Date 15/03/2016

Case Summary Ribbon

WRKL - Work List

Modify Alerts

OTHP

OTHP
Other Party Information Screen

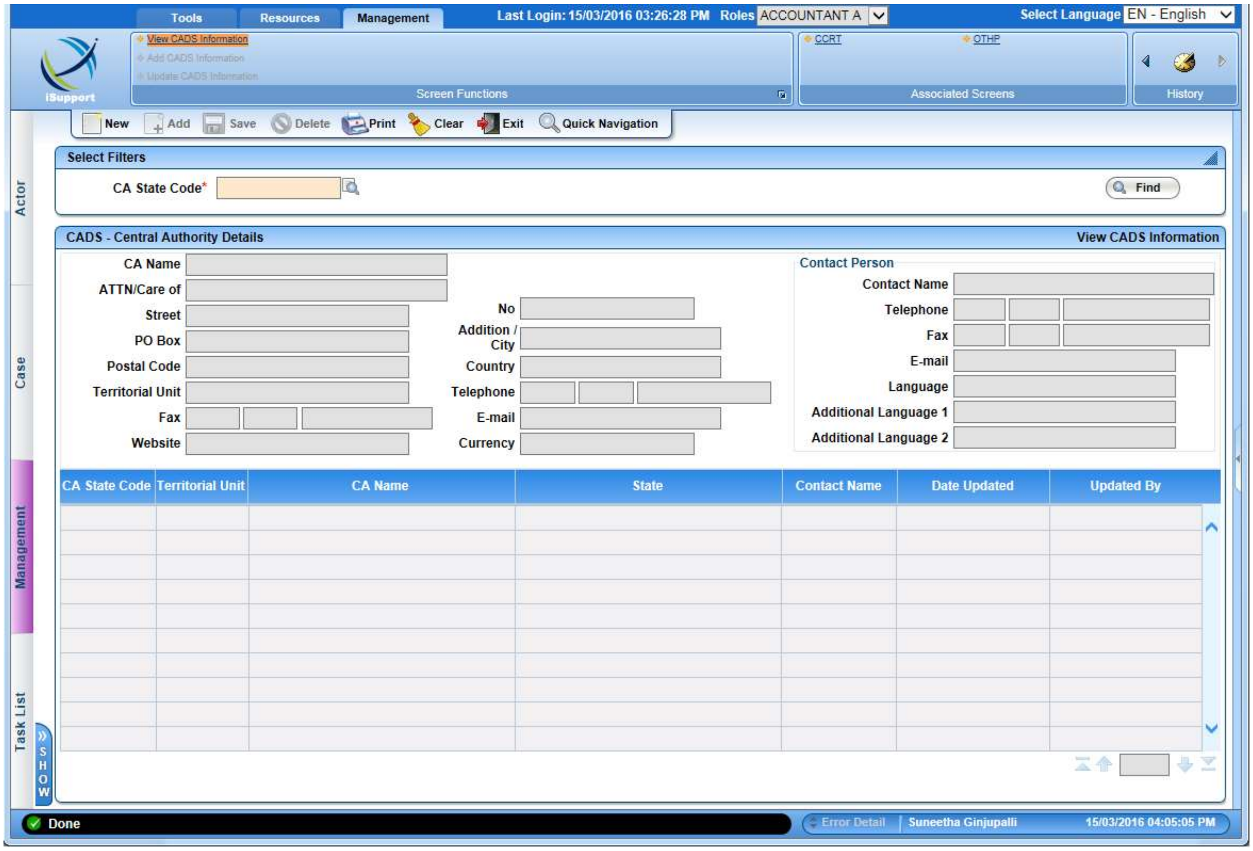
Fwd	!	Date Generated	Debtor Name	Case	# of Days overdue	Date Due	Manager Due Date	Worker Due Date
☐		12/10/2015	FAMILY NAME D	CY-DE-20	154	13/10/2015	13/10/2015	13/10/2015
☐								
☐								
☐								
☐								
☐								
☐								
☐								
☐								
☐								

1 /1

Insufficient privilege to access the screen

Suneetha Ginjupalli 15/03/2016 04:04:21 PM

Figure 10 – Work List (WRKL) screen displaying message about insufficient privilege upon trying to navigate to a screen.



Last Login: 15/03/2016 03:26:28 PM

Roles: ACCOUNTANT A

Select Language: EN - English

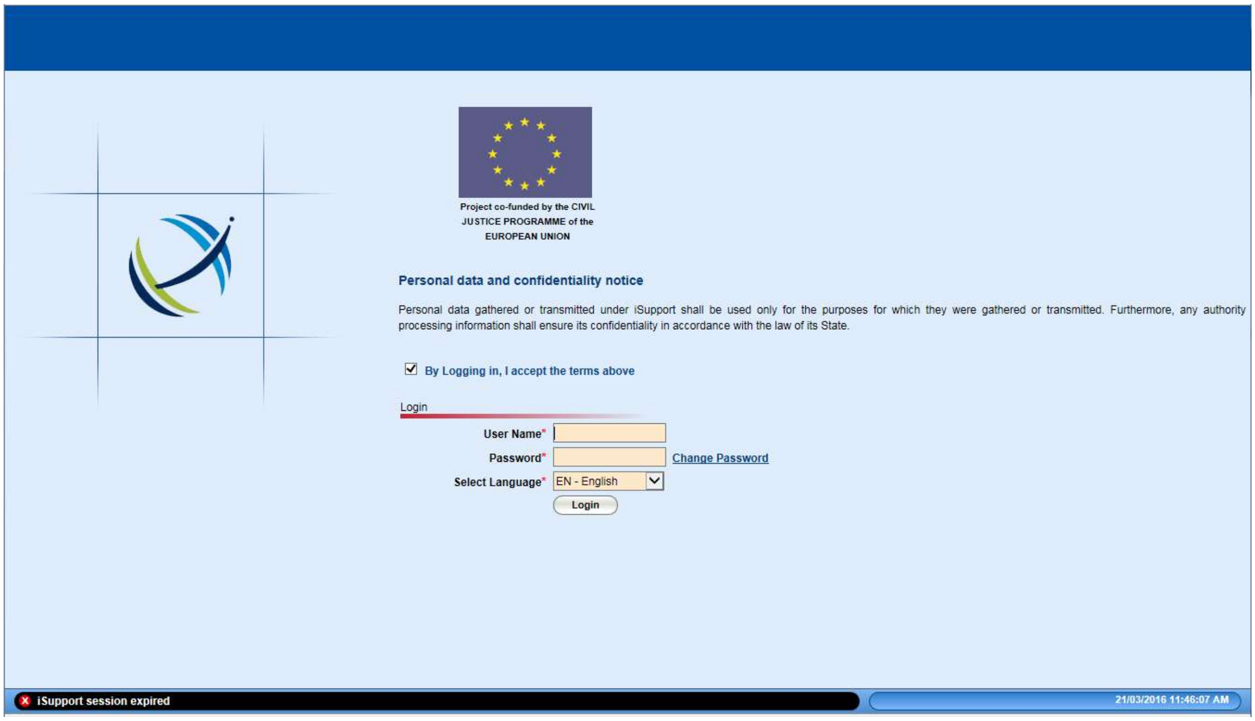
Done

Suneetha Ginjupalli

15/03/2016 04:05:05 PM

Figure 11 - CADS screen displaying a disabled screen function (Add CADS Information and Update CADS Information) based on user's roles

The iSupport application will terminate the user's session, if there is no activity for 30 minutes either via a keyboard entry or mouse movement. At that time, the user will be re-directed to the login screen, when they try to navigate within iSupport. A message will display informing the user that their current session has expired. iSupport will allow access and re-entry only with a valid User ID and password.



Project co-funded by the CIVIL JUSTICE PROGRAMME of the EUROPEAN UNION

Personal data and confidentiality notice

Personal data gathered or transmitted under iSupport shall be used only for the purposes for which they were gathered or transmitted. Furthermore, any authority processing information shall ensure its confidentiality in accordance with the law of its State.

☑ By Logging in, I accept the terms above

Login

User Name*

Password*

Select Language* EN - English

iSupport session expired

21/03/2016 11:46:07 AM

Figure 12 - iSupport re-directed to login page upon user session expiration displaying message about user session expiration

f. Procedures for system and terminal user identification assignment, maintenance, and cancellation must be in place and include:

1. Delegation and maintenance of the password system limited to a select number of people, and
2. A mechanism to quickly notify those responsible when there are personnel changes.

The procedures for system and terminal user identification assignment, maintenance, and cancellation are defined locally.~~.~~

Local policies should provide detailed information about the following:

- Security Clearances
- Authentication and Authorization
- Unique User Access Credentials
- Password Management
- Disabling Inactive Accounts
- Review of System Access
- Terminations and Transfers
- Segregation of Duties
- Security Awareness and Training

g. The system must detect, record, and lock out unauthorized attempts to gain access to system software and data.

Within the Central Authority system, all communication between each tier is sent through the firewalls. These firewalls, routers and switches will require a user authentication in order to perform device configuration changes and control list access configuration. Only authorized personnel (administrators) will be allowed to change firewall devices and/or software configuration. Unused ports will be disabled by administratively shutting them down to prevent unauthorized access.

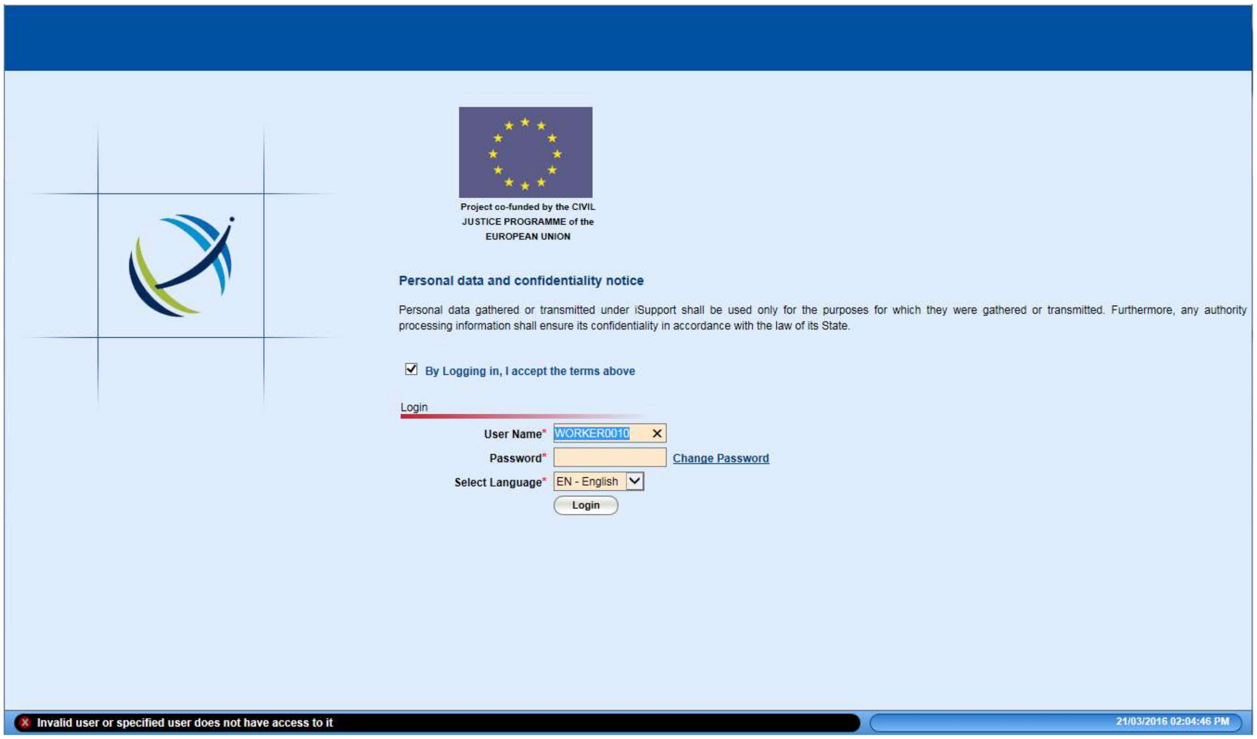
Database Administrators (DBAs), who administer and support the database, are assigned individual password-protected administrative accounts and associated DBA roles. Access to these accounts is restricted to all other users.

Subject to the applicable State regulations, audit logging processes for the operating system, user accounts, and application software should be enabled on all production systems.

Data access via iSupport application:

iSupport is a web-enabled application which is accessible only via a secure intranet to prevent external intrusion. It is not open to public access. Similarly iSupport’s Administration and API utility Applications also follow the same access privileges.

iSupport will restrict the user from logging into the application, if the password provided by the user is invalid.



Project co-funded by the CIVIL JUSTICE PROGRAMME of the EUROPEAN UNION

Personal data and confidentiality notice

Personal data gathered or transmitted under iSupport shall be used only for the purposes for which they were gathered or transmitted. Furthermore, any authority processing information shall ensure its confidentiality in accordance with the law of its State.

☑ By Logging in, I accept the terms above

Login

User Name* WORKER0010

Password*

Select Language* EN - English

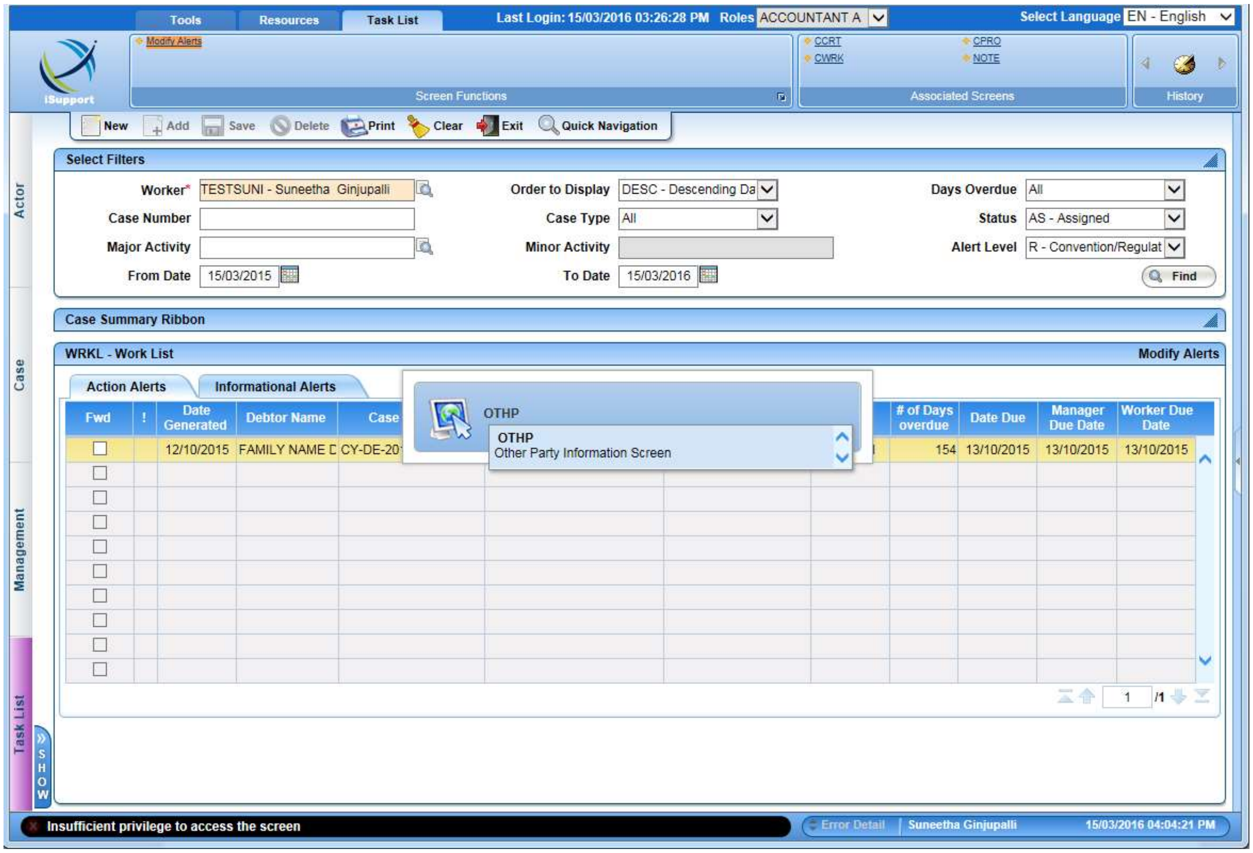
Invalid user or specified user does not have access to it

21/03/2016 02:04:46 PM

Figure 13 - iSupport displaying WARNING about access to unauthorized users

Within the iSupport application, a users' data access is controlled via application roles. Upon successful login, the application server will validate the User ID against the assigned roles to determine access permissions to the screen or screen function, when the iSupport user tries to navigate from screen-to-screen.

If the user does not have the appropriate role to access the screen or screen function, iSupport will display a message about insufficient privilege, and the screen function(s) are grayed out and disabled to preclude selection, when security has been restricted at the screen function level.



Last Login: 15/03/2016 03:26:28 PM Roles ACCOUNTANT A

Select Language EN - English

Worker* TESTSUNI - Suneetha Ginjupalli

Order to Display DESC - Descending Da

Days Overdue All

Case Number

Case Type All

Status AS - Assigned

Major Activity

Minor Activity

Alert Level R - Convention/Regulat

From Date 15/03/2015

To Date 15/03/2016

WRKL - Work List

Fwd	!	Date Generated	Debtor Name	Case	# of Days overdue	Date Due	Manager Due Date	Worker Due Date
□		12/10/2015	FAMILY NAME D	CY-DE-20	154	13/10/2015	13/10/2015	13/10/2015

OTHP

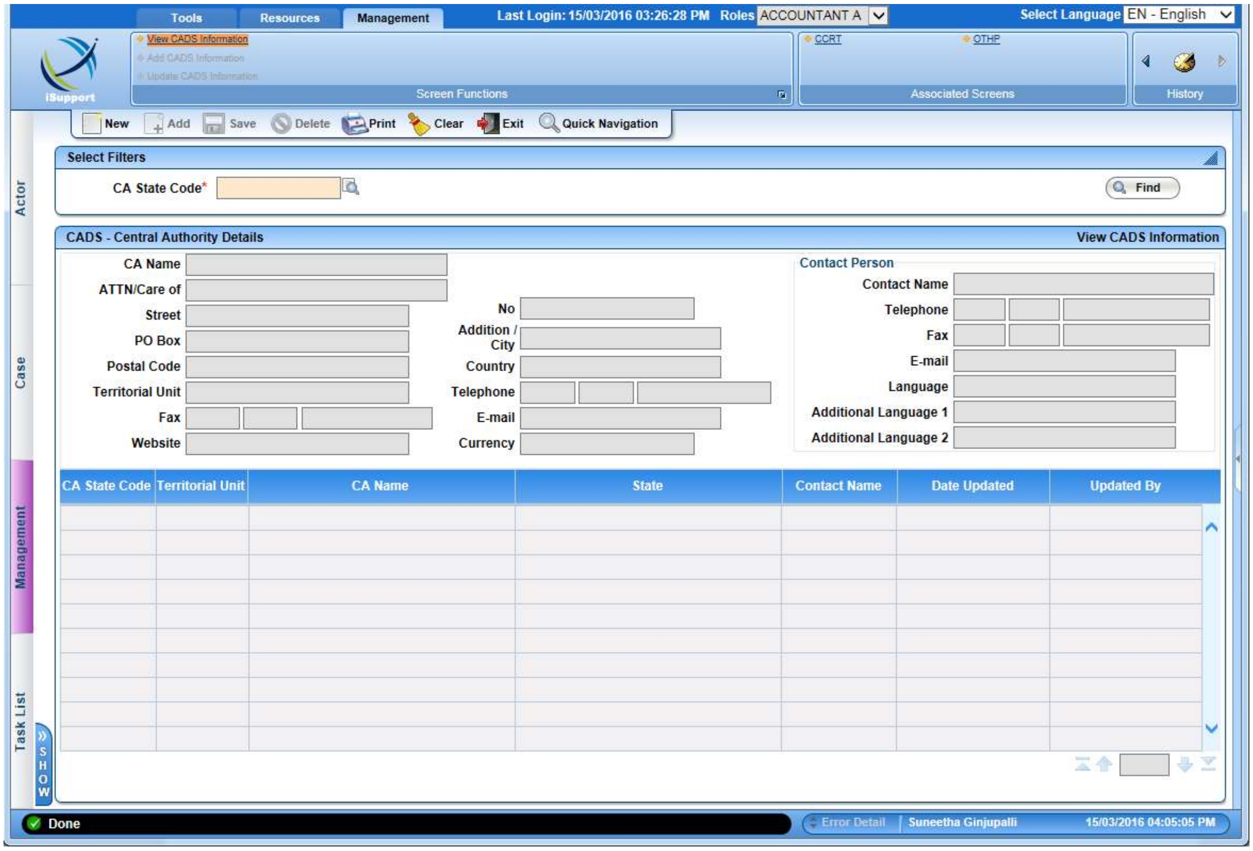
OTHP
Other Party Information Screen

1 /1

Insufficient privilege to access the screen

Suneetha Ginjupalli 15/03/2016 04:04:21 PM

Figure 14 - iSupport displaying message about insufficient access



Last Login: 15/03/2016 03:26:28 PM

Roles: ACCOUNTANT A

Select Language: EN - English

CA State Code	Territorial Unit	CA Name	State	Contact Name	Date Updated	Updated By

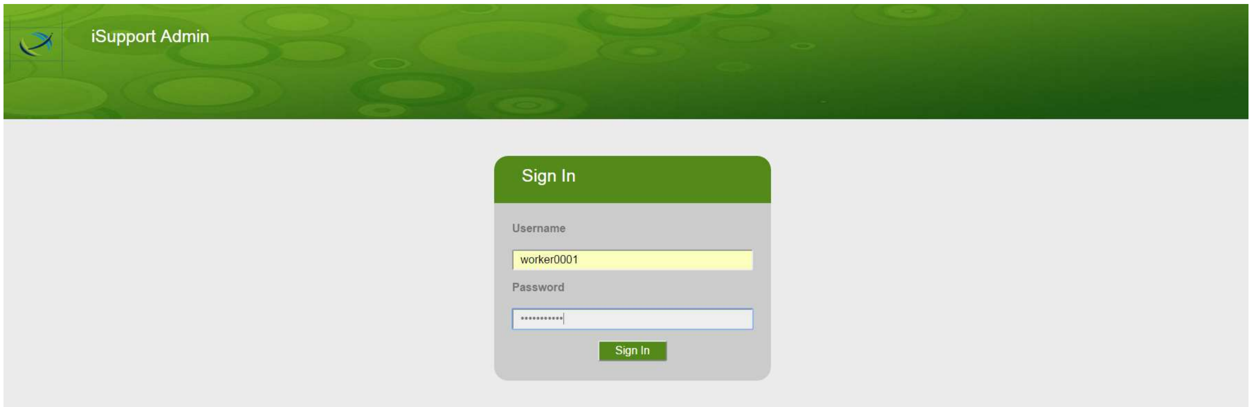
Done

Suneetha Ginjupalli 15/03/2016 04:05:05 PM

Figure 15 - CADS screen displaying disabled screen functions (Add CADS Information and Update CADS Information) based on user's roles

iSupport's Administration and API utility Applications requires user name and password to sign on. The users must provide the user name (also known as the User ID) and password in the iSupport login page to sign on to the iSupportAdmin Utility application. The user name and password are authenticated against the iSupport database. On successful authentication, the iSupport application will establish the authorization and enable admin application access based on the user's role(s). Only user with a Manager Role is permitted to access the iSupport Admin application.

iSupport API Utility application is used by external/internal case management systems to read or update data from iSupport programmatically. Calling application must pass User ID and password with a manager role to use API. Figure 11 demonstrates the requirement to provide User ID and password when API is access from the browser.



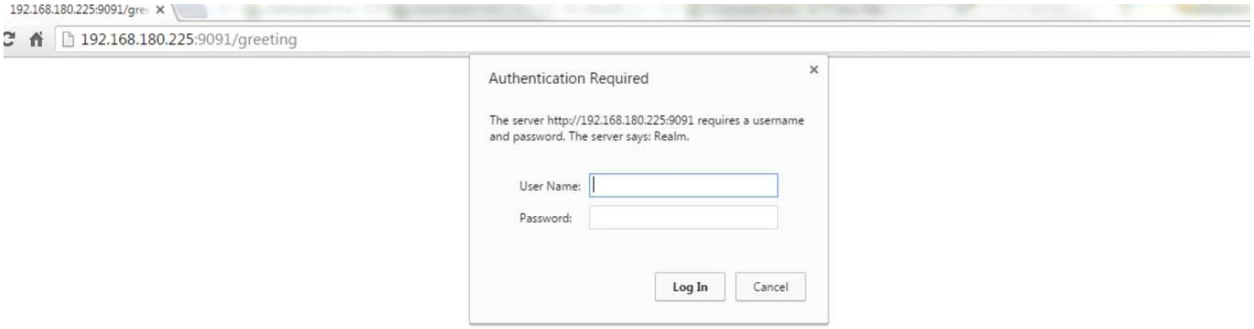
Username

worker0001

Password

•••••••••••

Figure 16 - iSupport Admin Login page – requires user name and password to sign on



192.168.180.225:9091/greeting

Authentication Required

The server http://192.168.180.225:9091 requires a username and password. The server says: Realm.

User Name:

Password:

Figure 17 - iSupport API Login page – requires user name and password to use API

h. Access to sensitive documents or forms generated by the system must be restricted.

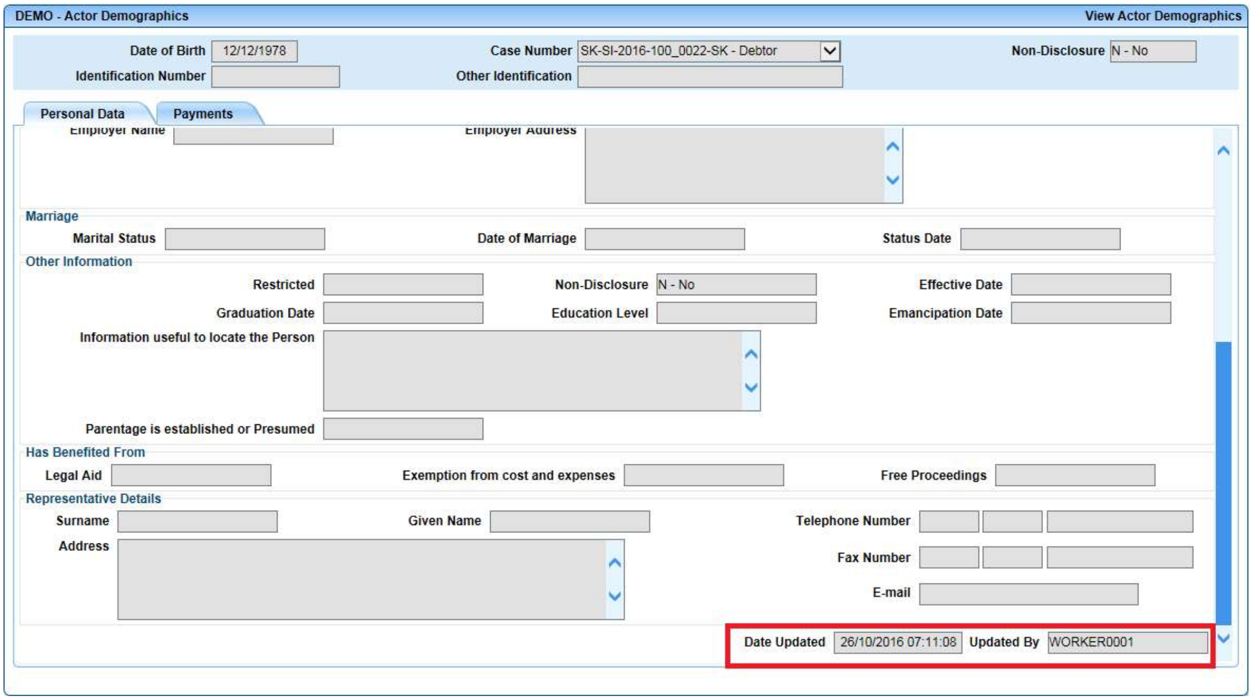
iSupport users have access to sensitive documents or forms only if they have the appropriate application role(s) assigned to their user profile.

i. For security purposes, the system must be capable of maintaining information on all changes to critical records and/or data fields (e.g., Arrearage Balance, Monthly Court-Ordered Support Amounts, SSN, Name, Family Violence Indicator, etc..), including identification of the responsible system user/caseworker and date/time of the change.

As part of data security, a comprehensive audit is provided in the iSupport application. When any business or reference data is modified, a detailed audit is stored on the changed information including:

- **Begin Validity Date** – identifies the date on which the information was created or changed
- **Last Update Date and Time** – identifies the system date on which the information was created or changed
- **Worker** – identifies the unique iSupport user name of the login worker who has affected the change
- **Screen or Function** – identifies the screen name or batch from where the change originated

~~T~~he information is also viewable on iSupport online screens and reports.



DEMO - Actor Demographics

View Actor Demographics

Date of Birth: 12/12/1978

Case Number: SK-SI-2016-100_0022-SK - Debtor

Non-Disclosure: N - No

Identification Number

Other Identification

Marriage

Marital Status

Date of Marriage

Status Date

Other Information

Restricted

Non-Disclosure: N - No

Effective Date

Graduation Date

Education Level

Emancipation Date

Information useful to locate the Person

Parentage is established or Presumed

Has Benefited From

Legal Aid

Exemption from cost and expenses

Free Proceedings

Representative Details

Surname

Given Name

Telephone Number

Address

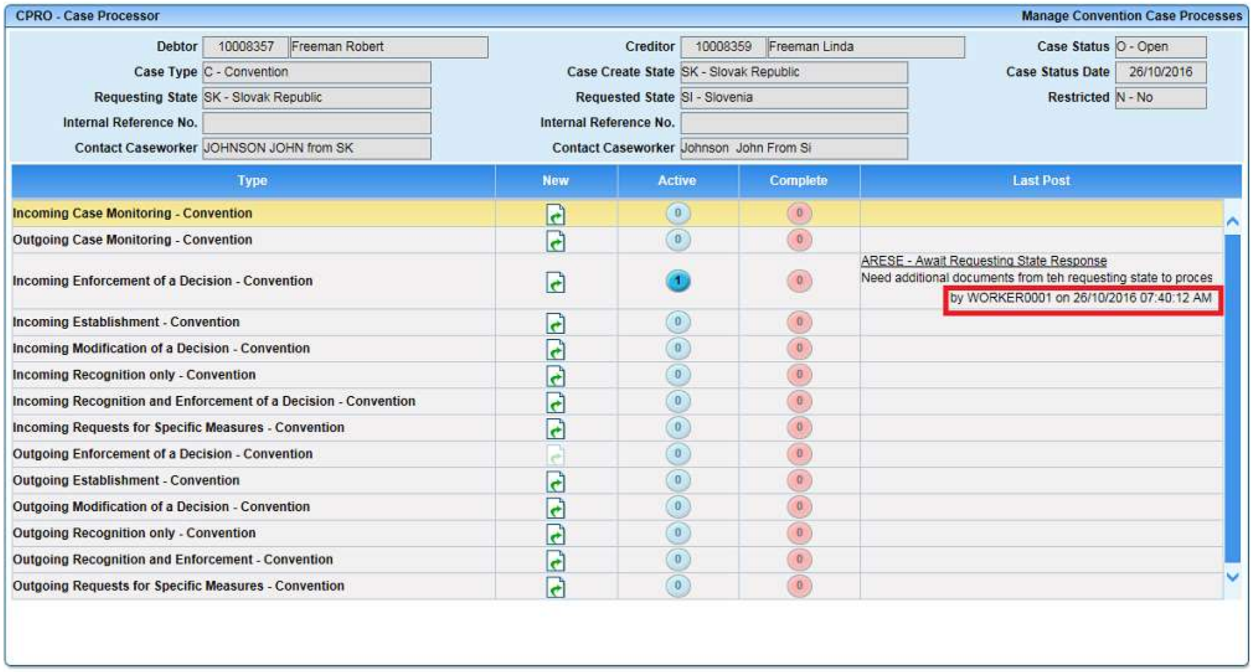
Fax Number

E-mail

Date Updated: 26/10/2016 07:11:08

Updated By: WORKER0001

Figure a- DEMO screen displaying details of Date Updated and Updated by worker for the actor record.

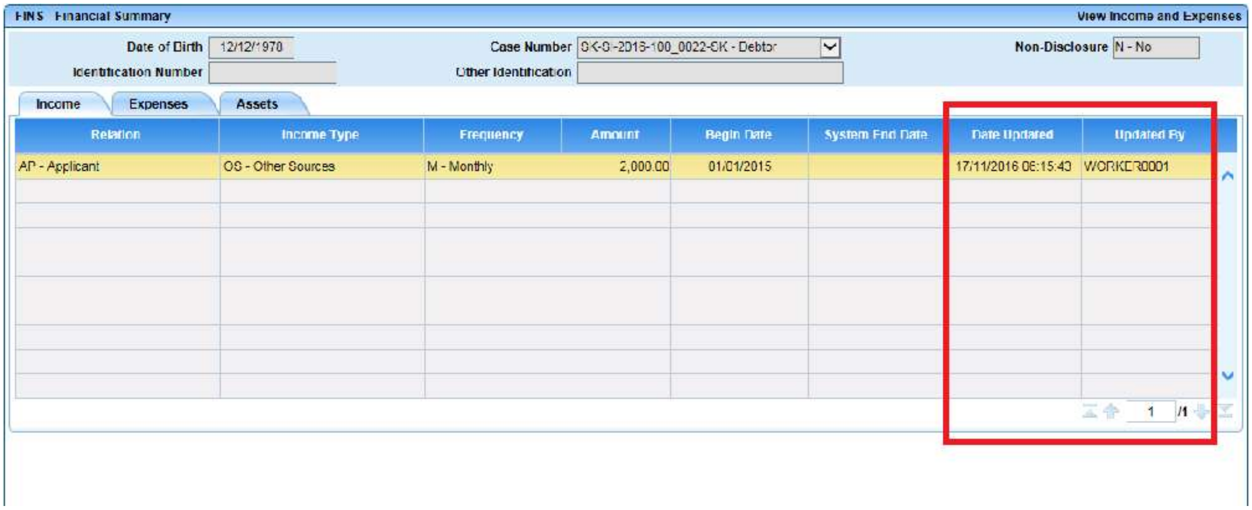


CPRO - Case Processor — Manage Convention Case Processes

Debtor	10008357 Freeman Robert	Creditor	10008359 Freeman Linda	Case Status	O - Open
Case Type	C - Convention	Case Create State	SK - Slovak Republic	Case Status Date	26/10/2016
Requesting State	SK - Slovak Republic	Requested State	SI - Slovenia	Restricted	N - No
Internal Reference No.		Internal Reference No.			
Contact Caseworker	JOHNSON JOHN from SK	Contact Caseworker	Johnson John From Si		

Type	New	Active	Complete	Last Post
Incoming Case Monitoring - Convention		0	0	
Outgoing Case Monitoring - Convention		0	0	
Incoming Enforcement of a Decision - Convention		1	0	ARESE - Await Requesting State Response Need additional documents from teh requesting state to proces by WORKER0001 on 26/10/2016 07:40:12 AM
Incoming Establishment - Convention		0	0	
Incoming Modification of a Decision - Convention		0	0	
Incoming Recognition only - Convention		0	0	
Incoming Recognition and Enforcement of a Decision - Convention		0	0	
Incoming Requests for Specific Measures - Convention		0	0	
Outgoing Enforcement of a Decision - Convention		0	0	
Outgoing Establishment - Convention		0	0	
Outgoing Modification of a Decision - Convention		0	0	
Outgoing Recognition only - Convention		0	0	
Outgoing Recognition and Enforcement - Convention		0	0	
Outgoing Requests for Specific Measures - Convention		0	0	

Figure b- CPRO screen displaying audit details of the record - worker and updated date time.



FINS Financial Summary — View Income and Expenses

Date of Birth	12/12/1970	Case Number	SK-S-2016-100_0022-SK - Debtor	Non-Disclosure	N - No
Identification Number		Other Identification			

Relation	Income Type	Frequency	Amount	Begin Date	System End Date	Date Updated	Updated By
AP - Applicant	OS - Other Sources	M - Monthly	2,000.00	01/01/2015		17/11/2016 06:15:43	WORKER0001

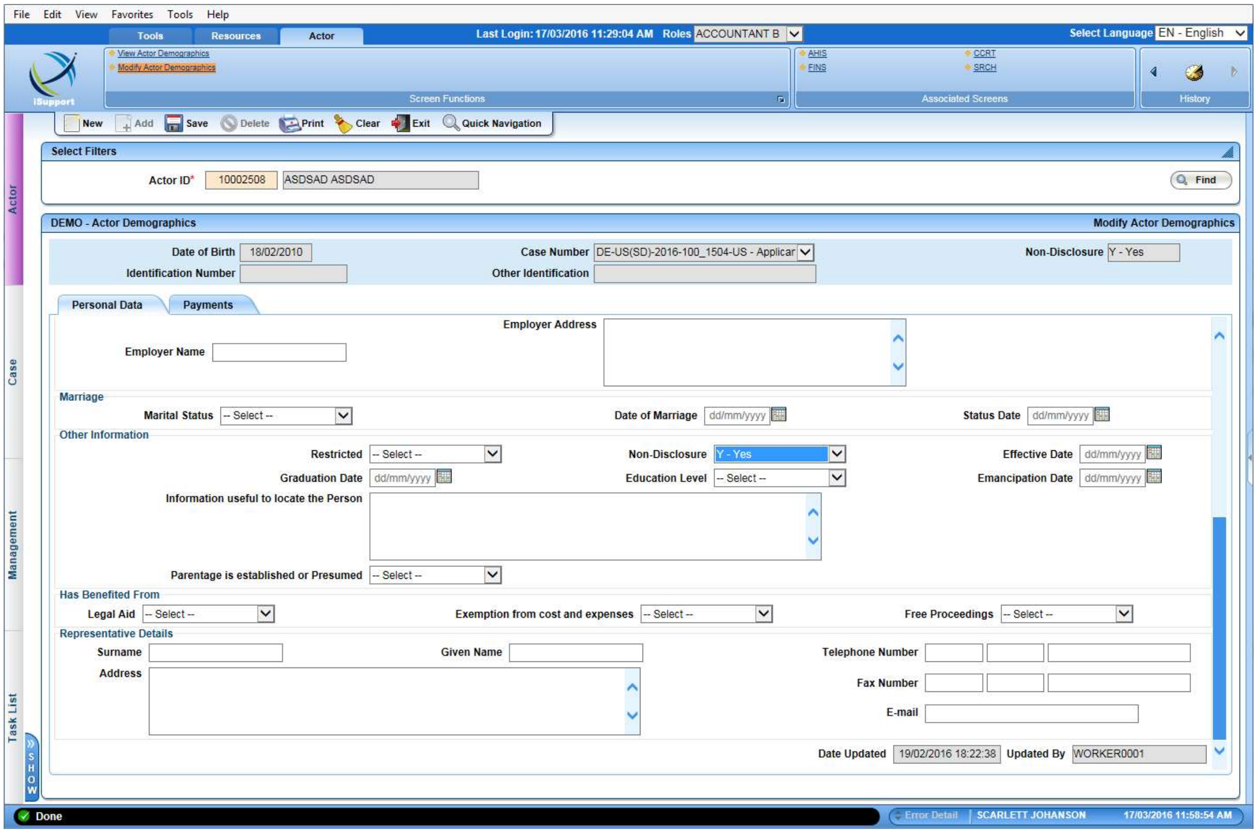
Figure c- CPRO screen displaying audit details of the record - worker and updated date time.

j. The system must be capable of routinely monitoring the access to use of the automated system.

The iSupport application tracks screen access by the login users and records the information in the data tables within the iSupport database. This technical information won't be visible to workers that uses the application. The database administrator will have access to these tables and data. Reports can be generated, as required, from the information that is stored using database queries.

k. The system document generation function must automatically prevent disclosure of personally identifiable information on persons designated as subject to family violence.

The iSupport application suppresses disclosure of personally identifiable information on persons designated as subject to non-disclosure or family violence. Non-disclosure (i.e. Family violence) status is maintained at the actor level in iSupport and is set as ‘Yes’ or ‘No’ for each actor. A value of ‘Yes’ designates an actor as a person subject to non-disclosure.



Last Login: 17/03/2016 11:29:04 AM Roles ACCOUNTANT B

Select Language EN - English

Actor ID* 10002508 ASDSAD ASDSAD

DEMO - Actor Demographics — Modify Actor Demographics

Date of Birth 18/02/2010

Identification Number

Case Number DE-US(SD)-2016-100_1504-US - Applicar

Other Identification

Non-Disclosure Y - Yes

Employer Name

Employer Address

Marital Status -- Select --

Date of Marriage dd/mm/yyyy

Status Date dd/mm/yyyy

Restricted -- Select --

Non-Disclosure Y - Yes

Effective Date dd/mm/yyyy

Graduation Date dd/mm/yyyy

Education Level -- Select --

Emancipation Date dd/mm/yyyy

Information useful to locate the Person

Parentage is established or Presumed -- Select --

Legal Aid -- Select --

Exemption from cost and expenses -- Select --

Free Proceedings -- Select --

Surname

Given Name

Telephone Number

Address

Fax Number

E-mail

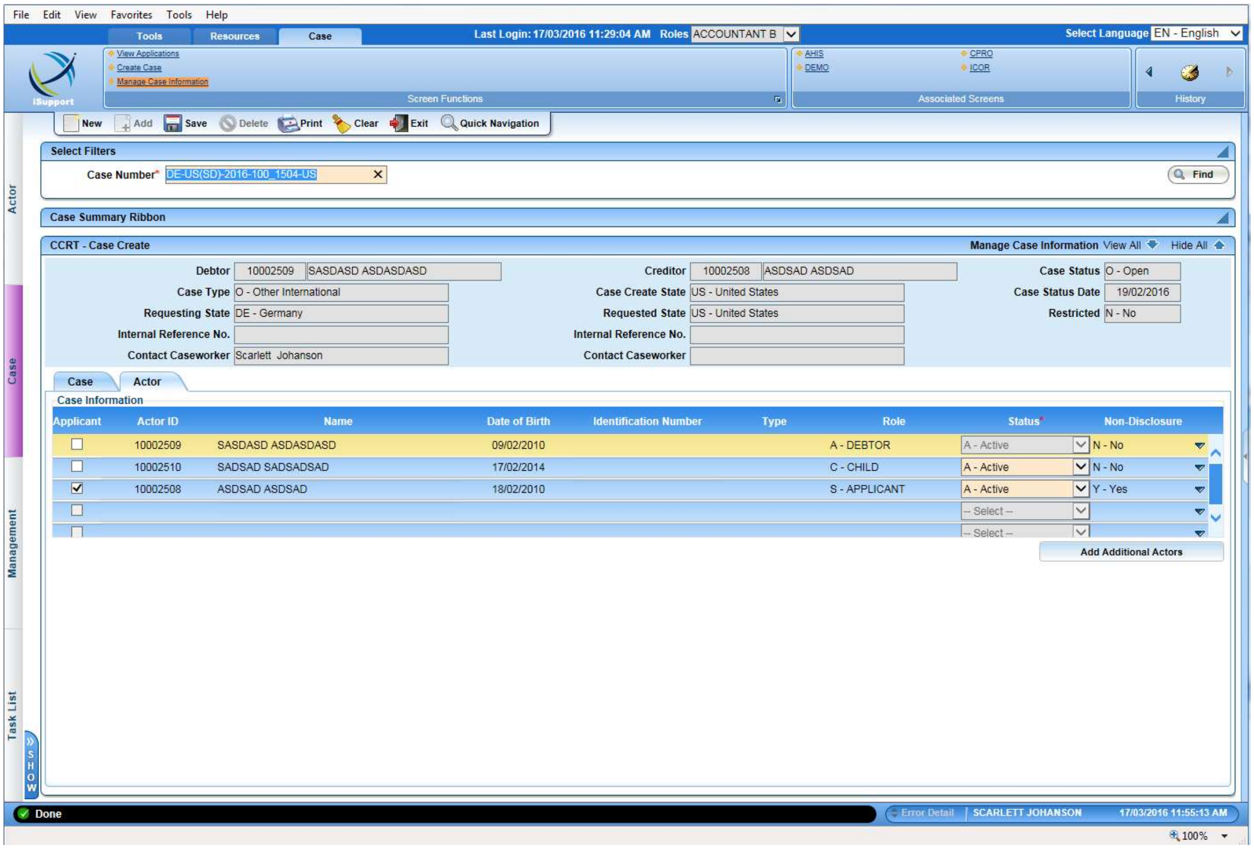
Date Updated 19/02/2016 18:22:38 Updated By WORKER0001

Done

SCARLETT JOHANSON 17/03/2016 11:58:54 AM

Figure 18 - DEMO screen displaying an actor as subject to non-disclosure

If an actor designated as subject to non-disclosure, all of this actors cases will be treated as subject to non-disclosure in iSupport.



Last Login: 17/03/2016 11:29:04 AM Roles ACCOUNTANT B

Select Language EN - English

Select Filters

Case Number* DE-US(SD)-2016-100_1504-US

Case Summary Ribbon

CCRT - Case Create

Manage Case Information View All Hide All

Debtor 10002509 SASDASD ASDASDASD

Case Type O - Other International

Requesting State DE - Germany

Internal Reference No.

Contact Caseworker Scarlett Johanson

Creditor 10002508 ASDSAD ASDSAD

Case Create State US - United States

Requested State US - United States

Internal Reference No.

Contact Caseworker

Case Status O - Open

Case Status Date 19/02/2016

Restricted N - No

Case | Actor

Case Information

Applicant	Actor ID	Name	Date of Birth	Identification Number	Type	Role	Status*	Non-Disclosure
□	10002509	SASDASD ASDASDASD	09/02/2010			A - DEBTOR	A - Active	N - No
□	10002510	SADSAD SADSADSAD	17/02/2014			C - CHILD	A - Active	N - No
☑	10002508	ASDSAD ASDSAD	18/02/2010			S - APPLICANT	A - Active	Y - Yes
□							-- Select --	
□							-- Select --	

Done

SCARLETT JOHANSON 17/03/2016 11:55:13 AM

Figure 19 - CCRT screen displaying applicant as subject to Non-Disclosure

If a case is flagged for family violence, sensitive information will not be displayed and will be printed on separate form (i.e. 'Restricted Information on the Applicant' for convention forms) in generation of iSupport documents, which is sent to the other states on the case. The suppressed data includes the address, and phone numbers for the party who is the subject to family violence or non-disclosure.

Table 1: Summary of screens, notices, and batch processes for H-2				
Screens				
	Screen Name	**Screen Functions**	**Screen Tab(s)**	**Section**
1.	iSupport Login Page			H-2.a H-2.c H-2.e H-2.g H-2.i
2.	Role Screen Access (RLSA)	Modify Role		H-2.a
3.	User Maintenance (USEM)	Modify a User Profile		H-2.a
4.	Member Address History (AHIS)	View Address History	Details	H-2.a
5.	Work List (WRKL)	View Alerts		H-2.c H-2.e H-2.g
6.	Central Authority Details (CADS)	View CADS information		~~H-2.c~~ ~~H-2.e~~ ~~H-2.g~~
7.	Actor Demographics (DEMO)	Modify Actor Demographics		~~H-2.i~~
8.	Case Create (CCRT)	Manage Case Information	Case Member Information	H-2.l

4. OBJECTIVE 3: The State must have procedures in place for the retrieval, maintenance, and control of the application software.

State Requirements (see the Service :

a. Changes to master files and application software must be made under the iSupport Change control procedures.

Under those procedures only authorized changes can be made to the application software and these changes are fully tested, approved, and migrated into production in a controlled manner, and documented to provide an audit trail of all system maintenance.

All testing of programs must be accomplished using test data as opposed to “live (production) data.”

Note: The use of “live (production) data” in a test environment is acceptable, and encouraged.

An audit trail of all operating system actions must be maintained either on the automatic console log or on the computer system's job accounting file.

System Requirements

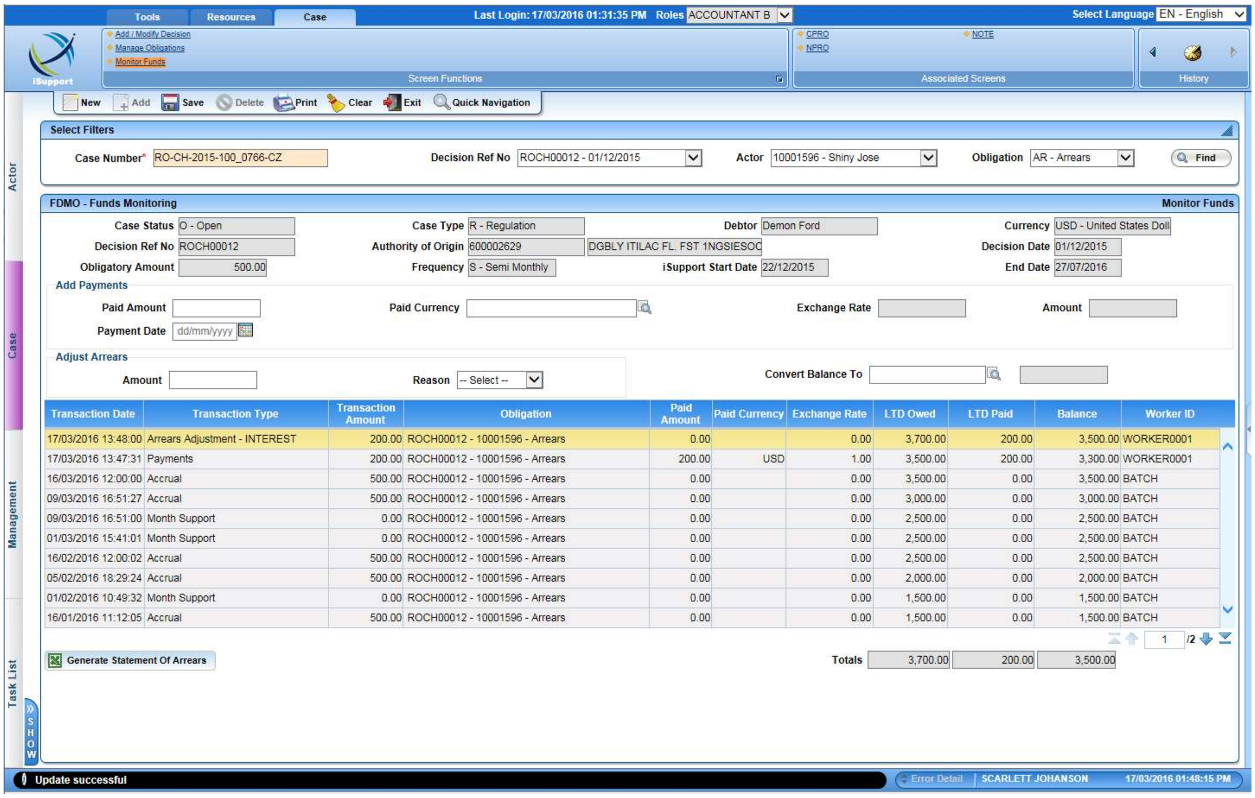
Application software development must also include recovery and restart capabilities for events such as operator errors, data errors and/or hardware/software failures.

The system must provide complete and accurate internal audit trails of all financial management activities, e.g., billing, receipting and distribution, and support order changes.

Access to system utility programs must be limited to necessary individuals with specific designation.

e. The system must provide complete and accurate internal audit trails of all financial management activities, e.g., billing, receipting and distribution, and support order changes.

iSupport provides internal audit trails through transactions like Payments, and adjustments. A complete audit trail is automatically recorded and can be viewed online. The Funds Monitoring (FDMO –Monitor Funds) provides a chronological diary of financial events and transactions for a specific case including Obligation creation, payments and Adjustment changes.



Last Login: 17/03/2016 01:31:35 PM Roles ACCOUNTANT B

Select Language EN - English

Select Filters

Case Number* RO-CH-2015-100_0766-CZ
Decision Ref No ROCH00012 - 01/12/2015
Actor 10001596 - Shiny Jose
Obligation AR - Arrears

FDMO - Funds Monitoring — Monitor Funds

Case Status O - Open
Case Type R - Regulation
Debtor Demon Ford
Currency USD - United States Doll
Decision Ref No ROCH00012
Authority of Origin 600002629 DGBLY ITILAC FL. FST 1NGSIESOC
Decision Date 01/12/2015
Obligatory Amount 500.00
Frequency S - Semi Monthly
iSupport Start Date 22/12/2015
End Date 27/07/2016

Add Payments

Paid Amount
Paid Currency
Exchange Rate
Amount
Payment Date dd/mm/yyyy

Adjust Arrears

Amount
Reason -- Select --
Convert Balance To

Transaction Date	Transaction Type	Transaction Amount	Obligation	Paid Amount	Paid Currency	Exchange Rate	LTD Owed	LTD Paid	Balance	Worker ID
17/03/2016 13:48:00	Arrears Adjustment - INTEREST	200.00	ROCH00012 - 10001596 - Arrears	0.00		0.00	3,700.00	200.00	3,500.00	WORKER0001
17/03/2016 13:47:31	Payments	200.00	ROCH00012 - 10001596 - Arrears	200.00	USD	1.00	3,500.00	200.00	3,300.00	WORKER0001
16/03/2016 12:00:00	Accrual	500.00	ROCH00012 - 10001596 - Arrears	0.00		0.00	3,500.00	0.00	3,500.00	BATCH
09/03/2016 16:51:27	Accrual	500.00	ROCH00012 - 10001596 - Arrears	0.00		0.00	3,000.00	0.00	3,000.00	BATCH
09/03/2016 16:51:00	Month Support	0.00	ROCH00012 - 10001596 - Arrears	0.00		0.00	2,500.00	0.00	2,500.00	BATCH
01/03/2016 15:41:01	Month Support	0.00	ROCH00012 - 10001596 - Arrears	0.00		0.00	2,500.00	0.00	2,500.00	BATCH
16/02/2016 12:00:02	Accrual	500.00	ROCH00012 - 10001596 - Arrears	0.00		0.00	2,500.00	0.00	2,500.00	BATCH
05/02/2016 18:29:24	Accrual	500.00	ROCH00012 - 10001596 - Arrears	0.00		0.00	2,000.00	0.00	2,000.00	BATCH
01/02/2016 10:49:32	Month Support	0.00	ROCH00012 - 10001596 - Arrears	0.00		0.00	1,500.00	0.00	1,500.00	BATCH
16/01/2016 11:12:05	Accrual	500.00	ROCH00012 - 10001596 - Arrears	0.00		0.00	1,500.00	0.00	1,500.00	BATCH

1 /2

Totals 3,700.00 200.00 3,500.00

Update successful

SCARLETT JOHANSON 17/03/2016 01:48:15 PM

Figure 20 - FDMO displaying the financial events logged on an iSupport case

f. Access to system utility programs must be limited to necessary individuals with specific designation.

The following Central Authority Staff members will have restricted and secure access to Enterprise Core servers:

- Network Interfaces
    - Network Administrators
    - Security Administrators
- System Access
    - System Administrators
    - Database Administrators

The administrators who support the servers in troubleshooting and perform maintenance will have the following controls and measures:

- Access to all servers and devices will require an authentication process and will be restricted to personnel based on their job function.
- The Implementation (IMP) Team DBAs and System Administrators will have access to the development environment only.
- Individual unique User IDs will only be used to access the Enterprise Core servers and their components. The User IDs will have limited access rights.
- Authorized users may login to the server using their User ID and then switch to the super user (root) account, to gain administrative access or root privileges.
- Root privileges will allow for changes to the system configuration or day-to-day maintenance activities.
- Appropriate file permissions will be enforced based on the assigned User IDs and the associated access privileges.
- All security patches related to operating system and software will be updated and installed in the servers.
- Unauthorized access to the system will be logged and stored in an access log. The logs will be maintained for all the servers for general audit and security breach discovery.
- Users will be denied direct access to any tier with the exception of the web tier.

g. Application software development must also include recovery and restart capabilities for events such as operator errors, data errors and/or hardware/software failures.

The iSupport application provides optimal availability. An Oracle Database is the principal data store, and it features clustered architecture that provides an active backup for the host server hardware.

iSupport is primarily based on n-tier architecture for a .Java application using Oracle. N tier architectures rely on interconnections of several components, such as TOMCAT Server, databases, user directories, external applications, and custom applications. The iSupport application is designed to allow restarting from any aborts.

The Technical Support Procedures documentation includes the details for the backup, and restart and recovery procedures for the application.

5. OBJECTIVE 4: The State must have procedures in place for the retrieval, maintenance, and control of program data.

State Requirements:

a. All changes to master files must be authorized and initiated by persons independent of the data processing function.

Override capability or bypassing of data validation on editing problems must be restricted to supervisory personnel.

All system-generated overrides must be automatically logged by the application so that actions can be analyzed for appropriateness and correctness.

System Requirements

The system must generate record counts to validate the completeness of data processed.

All rejected data must be automatically written to a suspense file and a record count made.

a. All changes to master files must be authorized and initiated by persons independent of the data processing function.

All changes to iSupport are initiated by the iSupport coordinator subject to the procedure described in the General description of the iSupport services, and follow a formal change control process managed by the Systems Unit Administrator.

b. Override capability or bypassing of data validation on editing problems must be restricted to supervisory personnel.

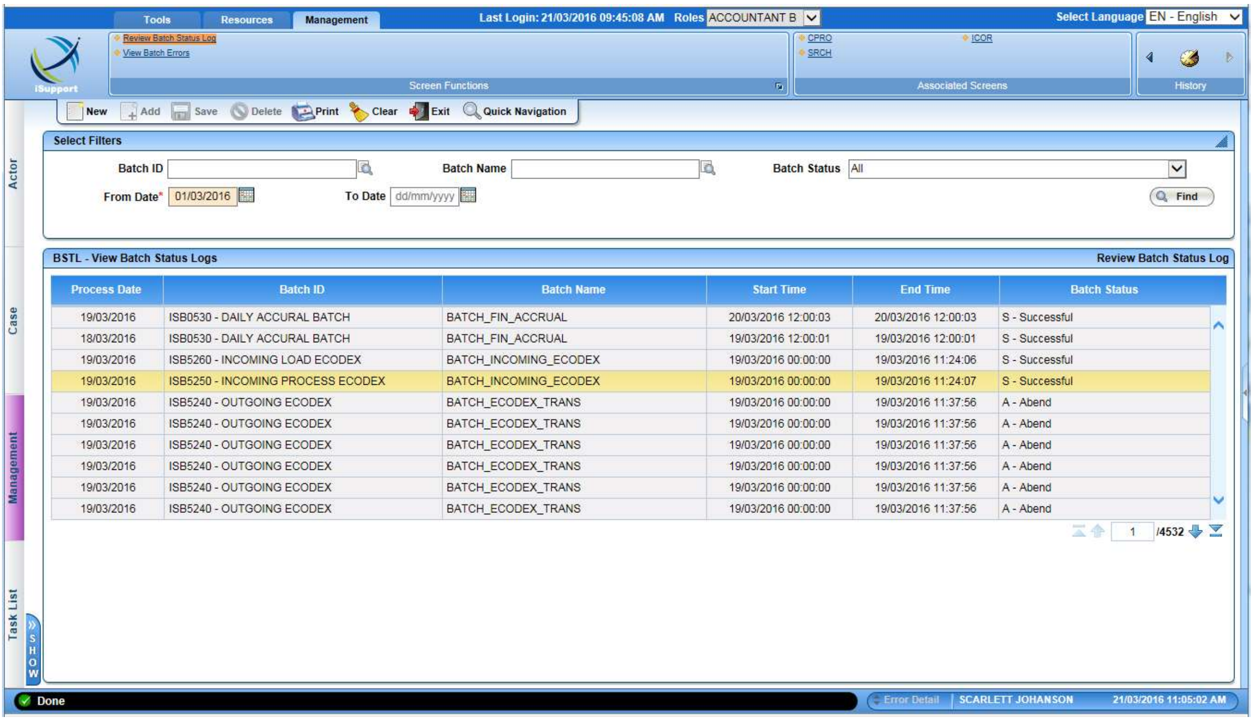
iSupport does not provide for any manual or system-generated overrides or bypassing of data validation.

c. All system-generated overrides must be automatically logged by the application so that actions can be analyzed for appropriateness and correctness.

iSupport does not provide for any manual or system-generated overrides or bypassing of data validation.

d. The system must generate record counts to validate the completeness of data processed.

The online screen status bar generates a message when data is processed successfully in the application. Batch processing completeness records will be loaded in tables when successful. If they fail, they are recorded in the batch error table. The iSupport application tracks and stores the record status for the records that are processed by the batch program. The Batch Status Log (BSTL) screen displays the execution status of the batch program. Batch Status Details popup will provide the total count of the number of records (i.e. Cursor Location) that were processed.



Last Login: 21/03/2016 09:45:08 AM Roles ACCOUNTANT B

Select Language EN - English

Select Filters

Batch ID

Batch Name

Batch Status All

From Date* 01/03/2016

To Date dd/mm/yyyy

BSTL - View Batch Status Logs

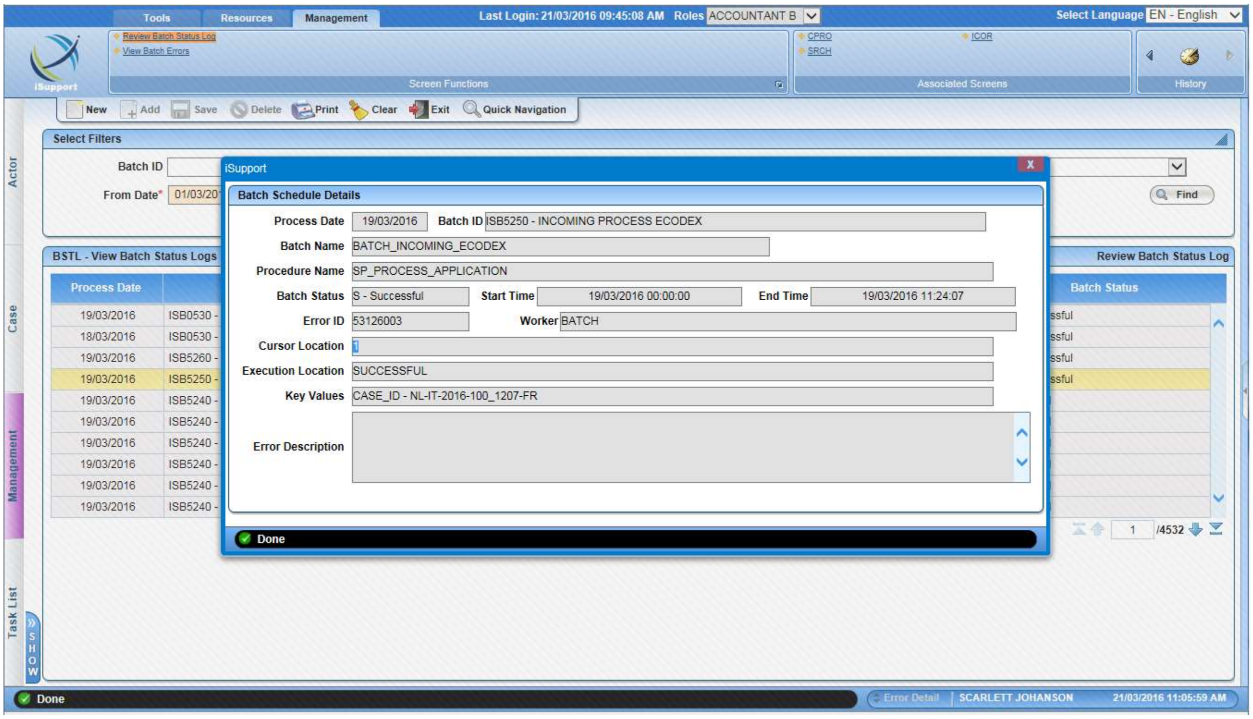
Review Batch Status Log

Process Date	Batch ID	Batch Name	Start Time	End Time	Batch Status
19/03/2016	ISB0530 - DAILY ACCURAL BATCH	BATCH_FIN_ACCRUAL	20/03/2016 12:00:03	20/03/2016 12:00:03	S - Successful
18/03/2016	ISB0530 - DAILY ACCURAL BATCH	BATCH_FIN_ACCRUAL	19/03/2016 12:00:01	19/03/2016 12:00:01	S - Successful
19/03/2016	ISB5260 - INCOMING LOAD ECODEX	BATCH_INCOMING_ECODEX	19/03/2016 00:00:00	19/03/2016 11:24:06	S - Successful
19/03/2016	ISB5250 - INCOMING PROCESS ECODEX	BATCH_INCOMING_ECODEX	19/03/2016 00:00:00	19/03/2016 11:24:07	S - Successful
19/03/2016	ISB5240 - OUTGOING ECODEX	BATCH_ECODEX_TRANS	19/03/2016 00:00:00	19/03/2016 11:37:56	A - Abend
19/03/2016	ISB5240 - OUTGOING ECODEX	BATCH_ECODEX_TRANS	19/03/2016 00:00:00	19/03/2016 11:37:56	A - Abend
19/03/2016	ISB5240 - OUTGOING ECODEX	BATCH_ECODEX_TRANS	19/03/2016 00:00:00	19/03/2016 11:37:56	A - Abend
19/03/2016	ISB5240 - OUTGOING ECODEX	BATCH_ECODEX_TRANS	19/03/2016 00:00:00	19/03/2016 11:37:56	A - Abend
19/03/2016	ISB5240 - OUTGOING ECODEX	BATCH_ECODEX_TRANS	19/03/2016 00:00:00	19/03/2016 11:37:56	A - Abend
19/03/2016	ISB5240 - OUTGOING ECODEX	BATCH_ECODEX_TRANS	19/03/2016 00:00:00	19/03/2016 11:37:56	A - Abend

1 /4532

SCARLETT JOHANSON 21/03/2016 11:05:02 AM

Figure 21 - BSTL displaying the Batch Status



Last Login: 21/03/2016 09:45:08 AM Roles ACCOUNTANT B

Select Language EN - English

iSupport

Batch Schedule Details

Process Date 19/03/2016 Batch ID ISB5250 - INCOMING PROCESS ECODEX

Batch Name BATCH_INCOMING_ECODEX

Procedure Name SP_PROCESS_APPLICATION

Batch Status S - Successful Start Time 19/03/2016 00:00:00 End Time 19/03/2016 11:24:07

Error ID 53126003 Worker BATCH

Cursor Location 1

Execution Location SUCCESSFUL

Key Values CASE_ID - NL-IT-2016-100_1207-FR

Error Description

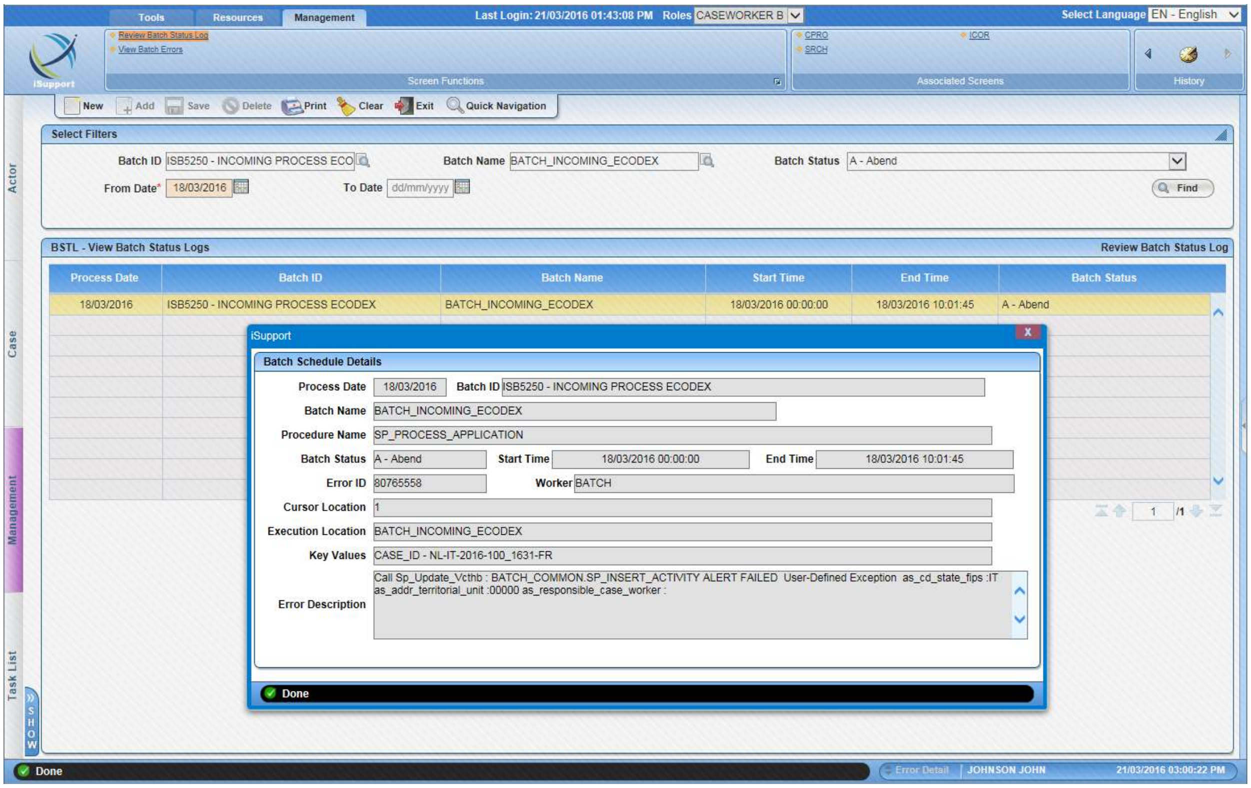
SCARLETT JOHANSON 21/03/2016 11:05:59 AM

Figure 22 - BSTL displaying the Batch Status and the number of records processed

e. All rejected data must be automatically written to a suspense file and a record count made.

In iSupport, data records that were not processed due to an error/discrepancy within a batch process are written into database error tables (BATCH_STATUS_LOG & BATCH_ERROR). The Batch Status Log (BSTL) screen displays this rejected data for further action, as necessary. The screen displays the batch execution status (Figure 21) along with the related rejected records (Figure 22).

The iSupport application tracks and stores the records that are processed by the batch program. The Batch Status Log (BSTL) screen displays the execution status of the batch programs.



Select Filters

Batch ID ISB5250 - INCOMING PROCESS ECO
Batch Name BATCH_INCOMING_ECODEX
Batch Status A - Abend
From Date* 18/03/2016
To Date dd/mm/yyyy
Find

BSTL - View Batch Status Logs — Review Batch Status Log

Process Date	Batch ID	Batch Name	Start Time	End Time	Batch Status
18/03/2016	ISB5250 - INCOMING PROCESS ECODEX	BATCH_INCOMING_ECODEX	18/03/2016 00:00:00	18/03/2016 10:01:45	A - Abend

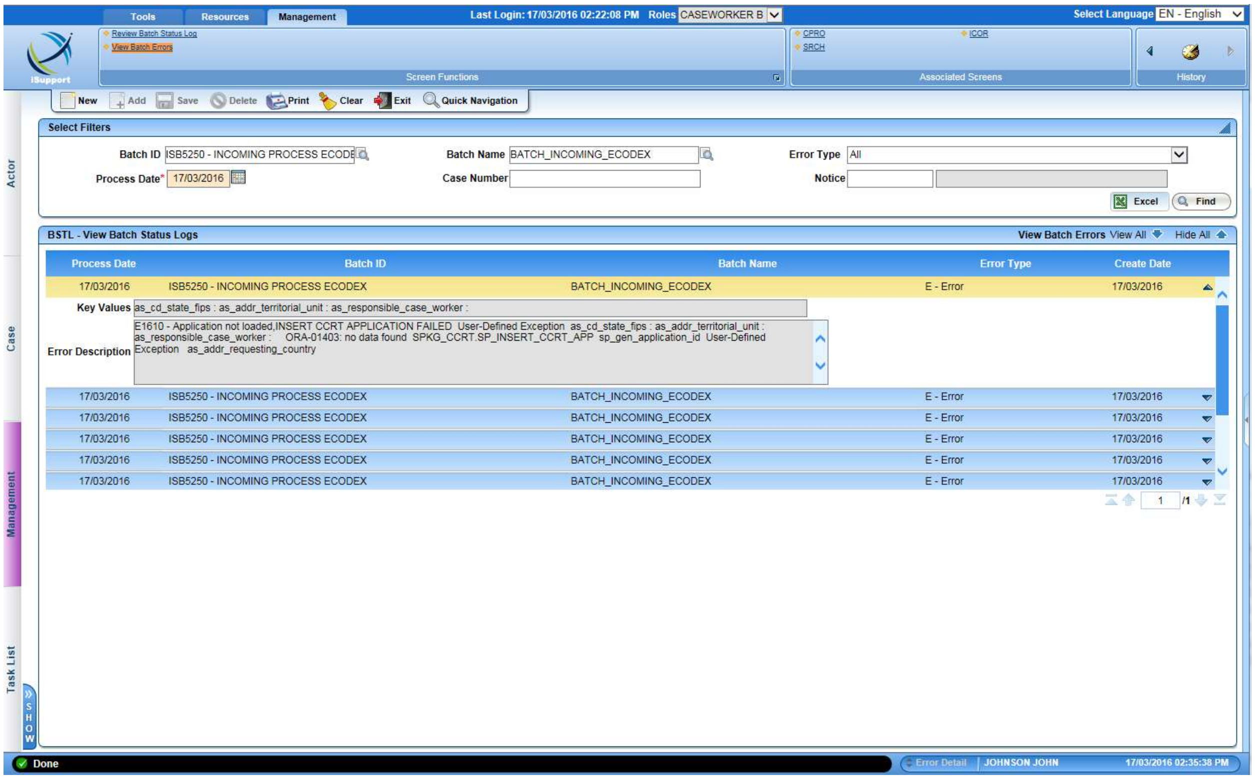
iSupport

Batch Schedule Details

Process Date 18/03/2016
Batch ID ISB5250 - INCOMING PROCESS ECODEX
Batch Name BATCH_INCOMING_ECODEX
Procedure Name SP_PROCESS_APPLICATION
Batch Status A - Abend
Start Time 18/03/2016 00:00:00
End Time 18/03/2016 10:01:45
Error ID 80765558
Worker BATCH
Cursor Location 1
Execution Location BATCH_INCOMING_ECODEX
Key Values CASE_ID - NL-IT-2016-100_1631-FR
Error Description Call Sp_Update_Vcthb : BATCH_COMMON.SP_INSERT_ACTIVITY ALERT FAILED User-Defined Exception as_cd_state_fips :IT as_addr_territorial_unit :00000 as_responsible_case_worker :

Done

Figure 23 - BSTL displaying the Batch Status



Last Login: 17/03/2016 02:22:08 PM Roles CASEWORKER B

Select Language EN - English

Select Filters

Batch ID ISB5250 - INCOMING PROCESS ECODE

Batch Name BATCH_INCOMING_ECODEX

Error Type All

Process Date* 17/03/2016

Case Number

Notice

BSTL - View Batch Status Logs

View Batch Errors

Process Date	Batch ID	Batch Name	Error Type	Create Date
17/03/2016	ISB5250 - INCOMING PROCESS ECODEX	BATCH_INCOMING_ECODEX	E - Error	17/03/2016

Key Values as_cd_state_fips : as_addr_territorial_unit : as_responsible_case_worker :

Error Description E1610 - Application not loaded,INSERT CCRT APPLICATION FAILED User-Defined Exception as_cd_state_fips : as_addr_territorial_unit : as_responsible_case_worker : ORA-01403: no data found SPKG_CCRT.SP_INSERT_CCRT_APP sp_gen_application_id User-Defined Exception as_addr_requesting_country

Process Date	Batch ID	Batch Name	Error Type	Create Date
17/03/2016	ISB5250 - INCOMING PROCESS ECODEX	BATCH_INCOMING_ECODEX	E - Error	17/03/2016
17/03/2016	ISB5250 - INCOMING PROCESS ECODEX	BATCH_INCOMING_ECODEX	E - Error	17/03/2016
17/03/2016	ISB5250 - INCOMING PROCESS ECODEX	BATCH_INCOMING_ECODEX	E - Error	17/03/2016
17/03/2016	ISB5250 - INCOMING PROCESS ECODEX	BATCH_INCOMING_ECODEX	E - Error	17/03/2016
17/03/2016	ISB5250 - INCOMING PROCESS ECODEX	BATCH_INCOMING_ECODEX	E - Error	17/03/2016

1 /1

JOHNSON JOHN 17/03/2016 02:35:38 PM

Figure 24 - BSTL screen displaying rejected records from a specific batch process execution

Table 4: Summary of screens, notices, and batch processes for H-4				
Screens				
	Screen Name	Screen Functions	Screen Tab(s)	Section
1.	Batch Status Log (BSTL)	View Batch Status Logs View Batch Errors		H-4.d H-4.e

7. **OBJECTIVE 5: The system hardware, software, documentation, and communications must be protected and backups must be available.**

State Requirements:

a. The State must have an approved disaster recovery plan which provides detailed actions to be taken in the event of a natural disaster (fire, water damage, etc.) or a disaster resulting from negligence, sabotage, mob action, etc. The disaster recovery plan should at a minimum include:

1. Documentation of approved backup arrangements,

Formal agreement of all parties,

An established processing priority system,

Arrangements for use of a backup facility, and

Periodic testing of the backup procedures/facility.

b. The State must maintain a listing of retention periods for all application and operating system files and program versions.

c. At a minimum the State must retain, in a form retrievable through automated system recovery and restore procedures, a 3-year automated history of the database off-site.

d. The State must conduct routine, periodic backups of all child support system data files, application programs, and documentation.

e. The State must store duplicate sets of files, programs, documentation, etc., off-site in secure waterproof and fireproof facilities.

System Requirements

f. The system must have, or be supported by, an automated recovery and restore capability in case of system malfunction or failure.

a. The State should have an approved disaster recovery plan which provides detailed actions to be taken in the event of a natural disaster (fire, water damage, etc.) or a disaster resulting from negligence, sabotage, mob action, etc. The disaster recovery plan should at a minimum include:

1. Documentation of approved backup arrangements,

Formal agreement of all parties,

An established processing priority system,

Arrangements for use of a backup facility, and

Periodic testing of the backup procedures/facility.

b. The State should maintain a listing of retention periods for all application and operating system files and program versions.

This is the State sole responsibility.

c. At a minimum the State should retain, in a form retrievable through automated system recovery and restore procedures, a 3-year automated history of the database off-site.

This is the State sole responsibility.

d. The State must conduct routine, periodic backups of all child support system data files, application programs, and documentation.

This is the State sole responsibility.

e. The State must store duplicate sets of files, programs, documentation, etc., off-site in secure waterproof and fireproof facilities.

This is the State sole responsibility.

f. The system must have, or be supported by, an automated recovery and restore capability in case of system malfunction or failure.

Restoring data from the tape backup will be performed only if the stand-by production data is determined to be unusable. In order to start using the database in the stand-by production environment, the database will be recovered by applying the last set of redo-logs and attempts will be made to activate the database. During this process the oracle database server will validate any inconsistencies and present error messages. If errors are encountered, attempts will be made to recover using media recovery. If these attempts fail, it will indicate that the stand-by production database is unusable.

The tape backup from offsite storage with the most recent data (typically from the previous date) will be used for the restore. The archive log files from the current production will be applied to do a point-in-time restore.

3. **OBJECTIVE 6: The system must be capable of processing date/time data.**

System Requirements:

All information technology hardware, software, and firmware product utilized by the Statewide automated child support enforcement system shall be able to accurately process date/time data, including, but not limited to, leap year calculations to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.

a. All information technology hardware, software, and firmware product utilized by the Statewide automated child support enforcement system shall be able to accurately process date/time data, including, but not limited to, leap year calculations to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.

iSupport is built on the latest technology that is currently available. This technology enables iSupport to successfully manage all issues related to date and time handling including leap year calculations and time changes. All date and time stamps in iSupport are synchronized with the main server to ensure all data in the system is as accurate as possible with respect to time and date. The application is capable of accurately recording and maintaining dates received from various interfaces.