EUROPEAN COMMISSION

DIRECTORATE-GENERAL INFORMATICS

User guide

User Guide CIPA Administration Console

Date:	19/06/2015
Version:	1.00
Authors:	Gianluca VENTRE
Revised by:	Anamaria BATRINU, Maarten DANIELS
Approved by:	

TABLE OF CONTENTS

1. BASIC DEFINITION AND ACRONYMS

Term	Description
Party	A **Party** is usually an organisation using the platform in the context of a particular Profile to exchange business documents.
Identifier	A **Party** has one or more **Identifier**s that uniquely distinguish a Party in a particular context.
Credentials	The Party **Credentials** entity contains the information used by the system to identify and authenticate a Party.
PartyAgreement	A **PartyAgreement** is the arrangement between two parties, which specifies that a Party can act on behalf of another Party.
Role	Within each Profile, Roles are defined. A **Role** contains the information about the job function or title which is associated with expected behaviour or responsibilities.
Party Role	A Party will be assigned to a Role in the context of a Profile.
Profile	A **Profile** is the entity that captures the aspects of a business collaboration. A profile includes the following key aspects: • **Role**: The role a Party has in the context of the Profile (e.g. Supplier) • **Document**: The document type exchanged in the context of the Profile (e.g. Invoice) • **Transaction**: The combination (Role1, Document1, Role2), which has the following connotation : Role1 sends Document1 to Role2.
Transaction	The **Transaction** describes one possible information exchange scenario. This would include the roles involved in the information exchange and the type of document.
Document	The **Document** entity contains information about the business document exchanged.
ICA	In order to enable communication between two parties, a logical communication channel, called I**nterchangeAgreement** (**ICA**), must be created. The interchange agreement is created by linking to a specific Profile, Parties via the Role included in the Profile.
CIPA	Common Infrastructure for Public Administrations.
CIPADMIN	CIPA AdminConsole.
ADM	A user having **General Administrator** role. The General Administrator is the Administrator of the CIPAdmin application.
CBO	A user having **Central Business Owner** role. The Central Business Owner is responsible for the organization and operation of a business domain and uses CIPA in his business context.
LBO	A user having **Local Business Owner** role. The Local Business Owner is the collaboration partner of the Business Owner in the given business context.
SUP	A user having Support role. The **Support** user can search and visualize data pertaining to the business domain he / she is authorized for.
ECAS	European Commission Authentication Service

GS1	http://www.gs1.org/
GLN	Global Location Number
VAT	Value-Added Tax

2. INTRODUCTION

The Common Infrastructure for Public Administrations (CIPA) is an action of EU's ISA Programme which promotes the reuse of infrastructure tools, along with underlying open specifications to support cross-border and cross-sectoral interoperability between European Public Administrations.

Infrastructure tools are highly reusable reference platforms (such as e-TrustEx to facilitate data exchange) and software components (such as the Service Metadata Publisher and Locator for registering digital services and making them accessible on the web).

The reuse of a common set of infrastructure tools by Pan-European initiatives will help Public Administrations to build well-defined and interoperable interfaces in the EU Member States. This will greatly simplify, streamline and accelerate the deployment of cross-border e-services for any sector.

CIPAdmin Console is an *infrastructure tool* that facilitates the configurability of reusable reference platforms. Each instance of such platforms would have a CIPAdmin Console. At the time this vision is written, CIPAdmin Console supports only the configuratbility of e-TrustEx platform.

3. GENERAL CONSIDERATIONS

You can find here a list of general considerations to take into account while using the application. They are presented by category in the following subsections.

3.1. Creation and Modification Considerations

Please see here below a list of general considerations to take into account when creating any type of configuration via the administration console:

- Mandatory fields are marked in red and followed by a star (eg. Party name [   ] *).

- Leading and trailing spaces are trimmed before saving any configuration (does not apply to password fields).

- Checking for unicity is done case insensitive.

- You can always go back to the previous screen by using Cancel button.

- Creation only: You can always clear all fields on screen by using Clear button.

- Modification only: You can always load the original field values by using Reset button.
- Saving is always done by using Save button.

3.2. Search Considerations

Please see here below a list of general considerations to take into account when searching any type of configuration via the administration console:

- Search page is structured in two sections:
    - the Search Criteria section where the search criterion are filled in by the user
    - the Search Results section where the results are displayed
- Search Criteria considerations
    - At least one search field needs to be filled in.
    - When more than one criterion is filled in, the application will search for all records that satisfy all filled in search criterions.
    - When filling in text input fields, you need to specify at least two characters.
    - It is case insensitive.
    - It is not take into account the leading and trailing spaces.
    - Partial match for the text input fields is supported.
    - You can clear all criterions on screen by using Clear button.
    - Search is always executed by using Search button.
- Search Results considerations
    - Search result elements are interactive, meaning that by clicking on a result line you can either visualise its details (if accessed via the main menu, so it is a main screen), or return the details to a parent screen (if accessed via a button in another screen, so it is a secondary screen or popup).
    - Above the search result list, you can see
        - At the left, the number of records found (eg. Found 3 party(s).)
        - At the right, a filter that will allow you to show even more precise results (eg. Filter). If any of the displayed fields of a line contained the text in the filter, then that line will be displayed, otherwise it will be hidden to the view (Figure 1 - Search filter). The filter is case insensitive, works with partial match, and does not trim spaces.
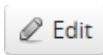
Figure 1 - Search filter

3.3. Visualisation Considerations

Please see here below a list of general considerations to take into account when visualising any type of configuration via the administration console:

- All fields are read-only.
- You can navigate to the modification screen by using [Edit] button.
- You can delete the record by using [Delete] button.
- You can go back to previous screen by using [Cancel] button.

3.4. Deletion Considerations

Please see here below a list of general considerations to take into account when deleting any type of configuration via the administration console:

- The deletion is always preceded by a confirmation request.

4. CONTACT SECTION

The Digit Cipa Support team is always available for any kind of issues or questions regarding the use of the CIPAdmin Console.

We'd Be Happy to Help You.

You contact us via email to the following address:

DIGIT-CIPA-SUPPORT@ec.europa.eu

5. USER ROLE

CIPAdmin supports currently four user roles based on which the user is allowed to access specific features. These user roles and the features they give access to are described in the next sub sections.

5.1. General Administrator (aka ADM)

The General Administrator is the Administrator of the CIPAdmin application. A user having ADM role has full access on all CIPAdmin features.

The application supports global General Administrator role which is authorized for all business domains and this will only be granted to a member of the CIPA team, as well as business specific General Administrator role which is authorized only for a specific business domain.

5.2. Central Business Owner (aka CBO)

The Central Business Owner is responsible for the organization and operation of a business and uses CIPA in his business context.

A user having CBO role is able to perform the following actions:
• Manage parties and their associated certificates
• Manage interchange agreements (aka ICA), having also the possibility to create a batch of interchange agreements
• Manage users for his/her business domain and change his/her own password
• Manage party agreements (in a future release
• View system information

5.3. Local Business Owner (aka LBO)

The Local Business Owner is the collaboration partner of the Central Business Owner in the given business context.

The Local Business Owner is able to perform the following actions:
• Manage parties and their associated certificates (the modification and deletion of a party are only allowed if the concerned party has been created by an user with LBO role)
• Manage interchange agreements (the modification and deletion of an interchange agreement are only allowed if the concerned interchange agreement has been created by an user with LBO role)
• Change his/her own password
Manage party agreements
• View system information

5.4. Support (aka SUP)

The Support user is the point of contact for CIPAdmin user requests and is the first that can investigate.

As for the General Administrator role, the application supports global Support role which is authorized for all business domains and this will only be granted to a member of the CIPA team, as well as business specific Support role which is authorized only for a specific business domain.

The Support user is able to access the following features:

- Support specific features:
    - o Inspect CIPAdmin and eTrustEx logs
    - o Inspect Messages
    - o View System Information
- Search and Visualization on all other features

6. LOGIN INTO THE APPLICATION

Accessing the application implies that the following conditions are met:

1. You have an ECAS account

2. Your ECAS account is configured in the administration console

If you do not have an ECAS account, you need to contact the European Commission Helpdesk, as this is out of the administration console scope.

If you do have an ECAS account, but your ECAS user is not configured in CIPAdmin application, you need to send a request specifying the concerned business domain and desired access rights to the CIPA support team (for more information on how to contact the support team, please see 4 Contact Section).

To access the application:

1. Go to the link specific to the desired environment

    - *PRODUCTION*
      http://wetrust1p.cc.cec.eu.int:1043/etrustex-admin-web/
    - *ACCEPTANCE*
      http://wladig05.cc.cec.eu.int:1043/etrustex-admin-web/
    - *TEST*
      http://wltdig07.cc.cec.eu.int:1045/etrustex-admin-web/

2. Enter your ECAS username and password and click Login (Figure 2 - ECAS Login)

3. The application home page will be displayed (Figure 3 - CIPAdmin Home Page)

If you are given access rights for more than one business domain, you can choose the desired business domain from the business domain list in the top right corner (eg. Welcome, batrian. Role General Administrator for : Generic). This can be done from any page of the application. Note that changing the business domain will lead to a reload of the current page, so if there is a creation or modification in progress the new data will be lost.
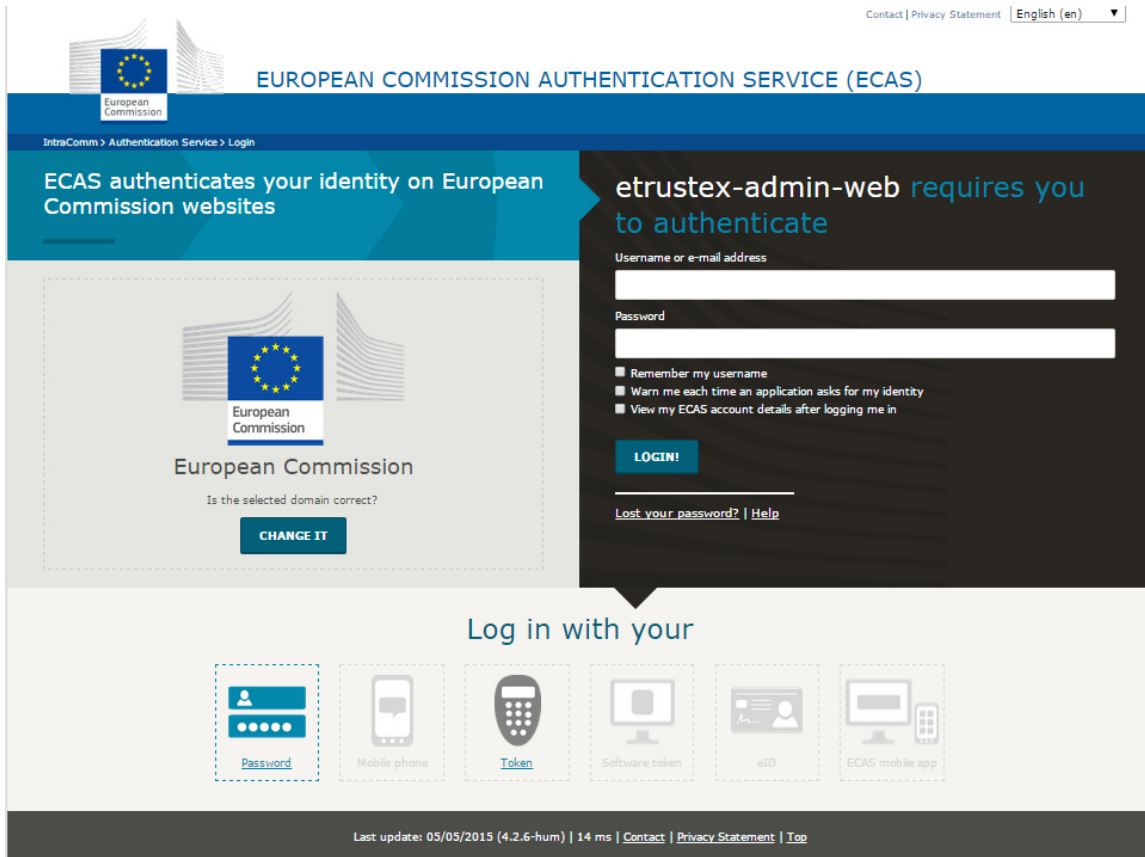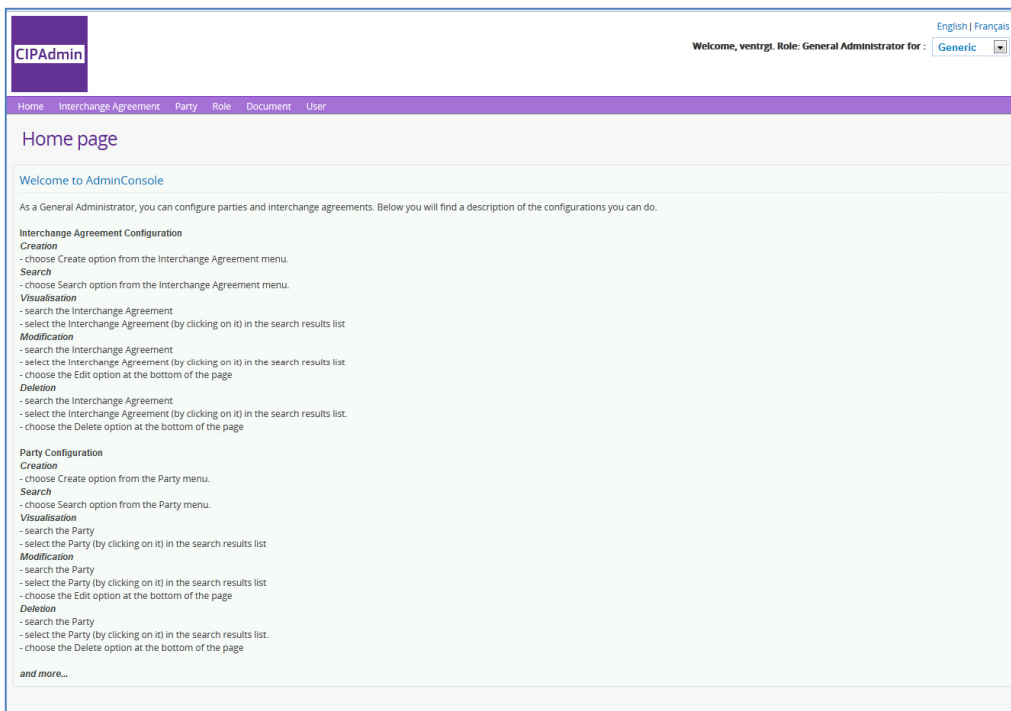
Figure 2 - ECAS Login

Figure 3 - CIPAdmin Home Page

7. PARTY MANAGEMENT

A **Party** is usually an organisation using the platform in the context of a particular Profile to exchange business documents.

The following sub sections describe all the operations provided by the administration console to the user.

7.1. Creating a Party

To create a party:

1. Navigate the menu: Party > Create

2. The creation screen will be displayed as in Figure 4.

3. Fill in the desired information

4. Choose 🖫 Save button to save the data

You can also create a party by using New... button while creating an Interchange Agreement (see sections 8.1 Creating an Interchange Agreement and 8.2 Create Multiple Interchange Agreements at once).

Figure 4 - Party Creation Page

Please see section 3.1 for common creation considerations.

Below you can find some specific party information and the way it is handled.

7.1.1. *Third Party*

A third party is a party that can be delegated by another party to act in its behalf by means of a party agreement. That means that a third party can connect to e-TrustEx web services and exchange documents on behalf of the party that empowered it. That is

why a third party must always have credentials specified in order to be able to access eTrustEx web services.

Click YES radio button next to Is third party field, if you want the party to be a third party.
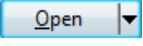
7.1.2. Certificates

Party certificates are used for encryption purposes and have a maximum allowed size of 100k. The application only supports configuration of encryption certificates (X509 certificates) for the moment, other usages could be added in future releases.

A party can have many certificates, but only one certificate per usage can be active at a given time.

The certificates of a party can be managed (added, activated or inactivated, revoked or deleted) via the Manage Party Certificates button that will open the certificates screen as in **Error! Reference source not found.**.

To upload a certificate:

1. Choose 🔍 button next to the Certificate selection field
2. A system search window opens
3. Browse to the folder where the certificate is located
4. Select the certificate and choose Open button
5. The system window closes and you can see now the certificate path in the Certificate selection field
6. Check the default values for certificate usage, activation and revocation state and change if necessary
7. Choose Import button
8. The certificate will be now processed and then displayed in the certificate list.

To activate/inactivate or revoke a certificate (also to change its usage in a future release):

1. Choose 🖉 button in the action column corresponding to the certificate to modify in the certificate list
2. The certificate modification screen is displayed (Figure 6 - Certificate Modification Popup)
3. Do the necessary modifications and choose OK button (certificate serial number cannot be modified)

To delete a certificate:

1. Choose ✖ button in the action column corresponding to the certificate to delete in the certificate list
2. Confirm the deletion (Figure 7 - Certificate Deletion Confirmation)

Figure 5 - Party Certificates Popup

Figure 6 - Certificate Modification Popup

Figure 7 - Certificate Deletion Confirmation

7.1.3. Credentials

The credentials of a party are used for accessing e-TrustEx web services for exchanging documents. They should always be configured if the party is a third party or if the party needs to connect directly to the web services.

The values introduced in Password and Confirm password fields must be identical. The party username need not be the same with the username of any other configured party.

7.1.4. Identifiers

The party identifiers (e.g. GS1's GLN, VAT number of the organisation etc.) are used for party identification and routing purposes. Only one type of identifier is allowed per party (you cannot have for example a party with two different VAT numbers). You always need to specify at least one party identifier, and the party identifiers specified need not be the same with identifiers pertaining to other parties.

You can manage the party identifiers in the Identifiers section, at the bottom of the screen (Figure 4 - Party Creation Page).

To add a new party identifier:

1. Choose ⊕ button
2. A new identifier line is displayed
3. Fill in the identifier type and value

To modify a party identifier:

1. Position the mouse cursor in the identifier field you want to modify
2. Fill in the desired value

To delete a party identifier:

1. Choose 🗑 button
2. The identifier line is removed

7.2. Searching for a Party

To search for a party, follow the next steps:

1. Navigate the application menu: Party > Search

2. Fill in the desired criteria (you can search by party name, business domain, username or identifier value or any combination of them)

3. Choose 🔍 Search button

4. The search result will be shown in the section at the bottom (Figure 8 – Party Search PageFigure 4 - Party Creation Page)

Please see section 3.2 for common search considerations.

Figure 8 – Party Search Page

7.3. Visualising Party Information

To see party information, follow the next steps:

1. Navigate the application menu: Party > Search

2. Fill in the search criterions for the desired party and click Search

3. Click on the party you want to see in the search result list

4. You can now see the party details as in Figure 9 – Party Visualization Page

5. Choose the button View Party Certificates to see the certificates attached to the party (Figure 10 - Party Certificates Visualisation). Choose Cancel to return to the party screen.

Please see section 3.3 for common visualisation considerations.

Figure 9 – Party Visualization Page

Figure 10 - Party Certificates Visualisation

7.4. Modifying a Party

To modify party information, follow the next steps:

1. Navigate the application menu: Party > Search

2. Fill in the search criterions for the desired party and click Search

3. Click on the party you want to modify in the search result list (Figure 8 – Party Search Page)

4. You can now see the party details as in Figure 9 – Party Visualization Page

5. Choose Edit button at the bottom right

6. You can now see the party modification screen (Figure 11 – Party Modification Page) and edit the party

7. Fill in or change the desired information (you cannot change the party name, the party username, and change the revoked state of revoked certificate)

a. Use Change password button if you want to change the password of the party credentials (Figure 12 – Party Change Password popup). Fill in Password and Confirm password fields with the new password. Choose ✓ OK button.

b. Use Manage Party Certificates to add, modify, delete, inactivate, activate or revoke a certificate belonging to the party (Figure 13 - Party Manage Certificates popup). See section 7.1.2 Certificates for more details.

c. Add, change or remove party identifiers in the Identifiers section as described in section 7.1.4 Identifiers.

8. Choose 💾 Save button to save the modifications

Please see section 3.1 for common creation considerations.

Figure 11 – Party Modification Page

Figure 12 – Party Change Password popup

Figure 13 - Party Manage Certificates popup

7.5. Deleting a Party

You cannot delete a Party that belongs to an **Interchange Agreement**, or that pertain to a business domain you are not authorized to use.

If you are a Local Business Owner, you are also not authorized to delete a party created by a more powerful user role (like ADM or CBO). You can only delete parties that pertain to your business domain and have been created by a LBO user role, as long as these parties are not involved in an interchange agreement, as previously stated.

To delete a party, follow the next steps:

1. Navigate the application menu: Party > Search

2. Fill in the search criterions for the desired party and click Search

3. Click on the party you want to delete in the search result list (Figure 8 – Party Search Page)

4. You can now see the party details as in Figure 9 – Party Visualization Page

5. Choose ☐ Delete button at the bottom right

6. Confirm the deletion (Figure 14 - Party Deletion Confirmation popup)

Figure 14 - Party Deletion Confirmation popup
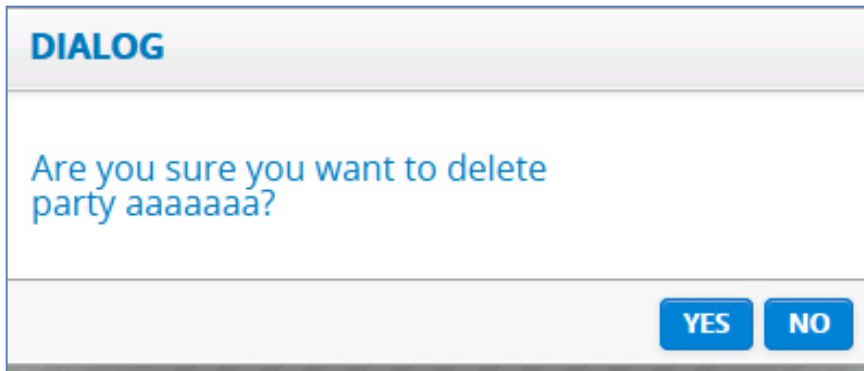
8. INTERCHANGE AGREEMENT

In order to enable communication between two parties, a logical communication channel, called **interchange agreement (aka ICA)**, must be created. This logical entity describes which parties can have a communication channel via e-TrustEx and which types of services the aforementioned parties are allowed to use.

An interchange agreement associates two parties, each being assigned a specific role with a document exchange profile as shown in the Figure 15 - The Interchange Agreement.

Figure 15 - The Interchange Agreement
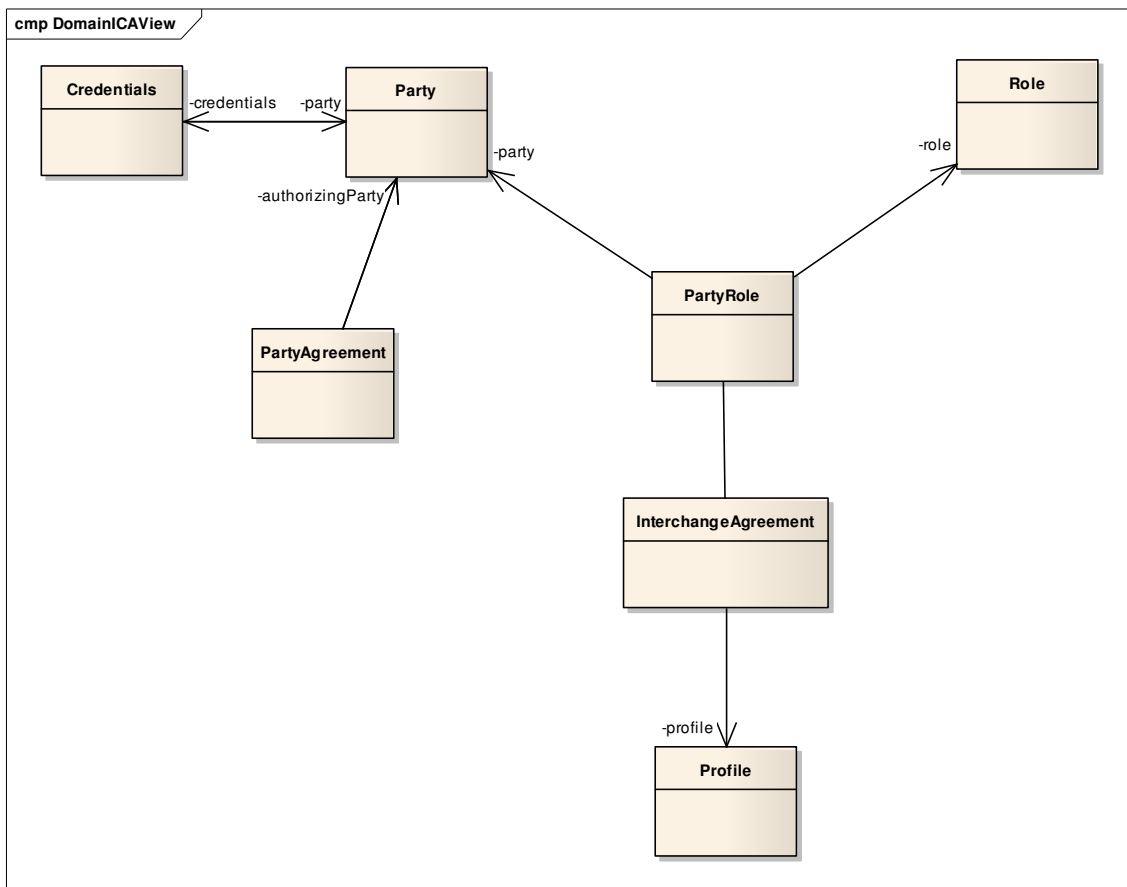
8.1. Creating an Interchange Agreement

To create an interchange agreement:
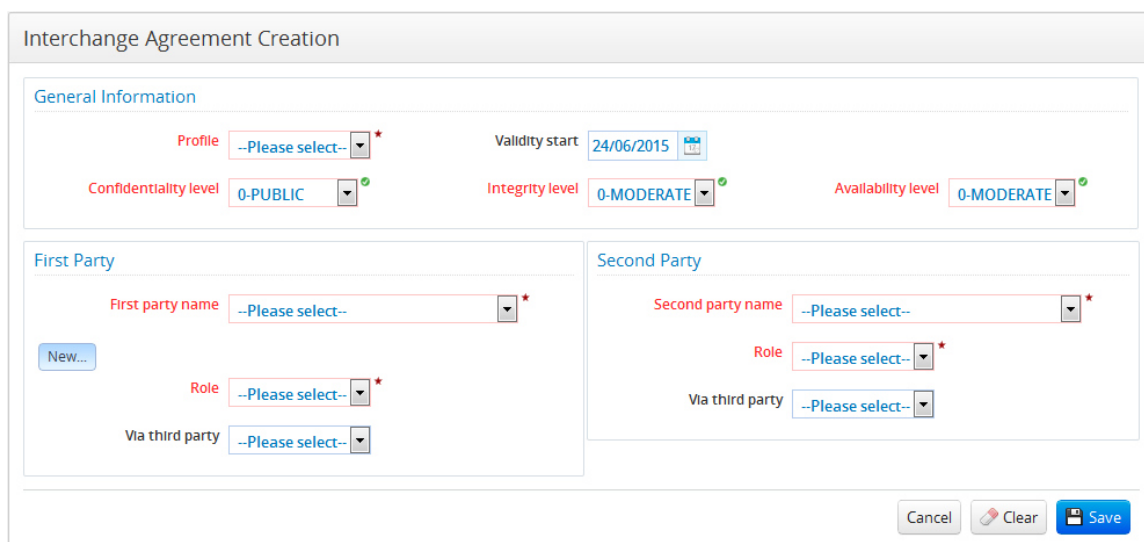
1. Navigate the menu: Interchange Agreement > Create Single

2. The creation screen will be displayed as in Figure 16.

3. Fill in the desired information

4. Choose 🖫 Save button to save the data

Figure 16 - Interchange Agreement Creation Page

Please see section 3.1 for common creation considerations.

Below you can find a short description of the Interchange Agreement data that you can fill in:

- the interchange agreement profile which groups a set of transactions and defines the documents that can be exchanged

- the date from when the interchange agreement applies

- the security levels corresponding to the Confidentiality, Integrity and Availability of data

- the information concerning each of the parties involved in the interchange agreement:
    - party name
    - party role
    - delegated party if needed

Note that if a party of the interchange agreement does not have credentials (so no means to authenticate to the system for exchanging documents), then you need to specify a third party (see Section 7.1.1 Third Party for a definition of the third party. This third party will be the one that will initiate the connection to the system, and will be able to send documents on behalf of the party without credentials.

If you need to create an interchange agreement for a new party, you can do both configurations via the same screen:

- Choose New... button, which opens the Party Creation screen (Figure 4 - Party Creation Page)

- Fill in the party data

- Choose option 💾 Save in the party screen

- The party screen is closed and the interchange agreement screen is displayed with the new party already selected in the first party section

- Fill in the remaining interchange agreement data

- Choose 💾 Save button to save the data

8.2. Create Multiple Interchange Agreements at once

This functionality is intended to facilitate the creation of interchange agreements in the case a new party is configured for the business. This is done by allowing the creation of multiple interchange agreements at once between this new party and the other parties that should exchange documents in the context of the chosen business profile.

To create an interchange agreement:

1. Navigate the menu: Interchange Agreement > Create Multiple

2. The creation screen will be displayed as in Figure 17.

3. Fill in the desired information

4. Choose 💾 Save button to save the data

5. When the creation is complete:

    - A summary is displayed indicating how many interchange agreements have been successfully created and how many are in error (Figure 18 and Figure 19)

    - The lines corresponding to the second parties for which the interchange agreements were successfully created will be displayed in green, and the others, for which an error occurred, in red (Figure 18 and Figure 19).

    - To see the error corresponding to a red line, position the mouse cursor above it: a tooltip with the corresponding error message will be temporary displayed (Figure 20).

Please see section 3.1 for common creation considerations and section 8.1 Creating an Interchange Agreement for the information that can be provided during the creation. Also, note that all the second parties that will be chosen for the multiple interchange agreement creation will fulfil the same role (chosen at the beginning of the section Second Parties. If you need to use different roles for second parties then you need to create the interchange agreements one by one as in 8.1 Creating an Interchange Agreement.

Figure 17 - Interchange Agreement Multiple Creation Page

Figure 18 - Mass Creation of Interchange Agreements – Completed with success

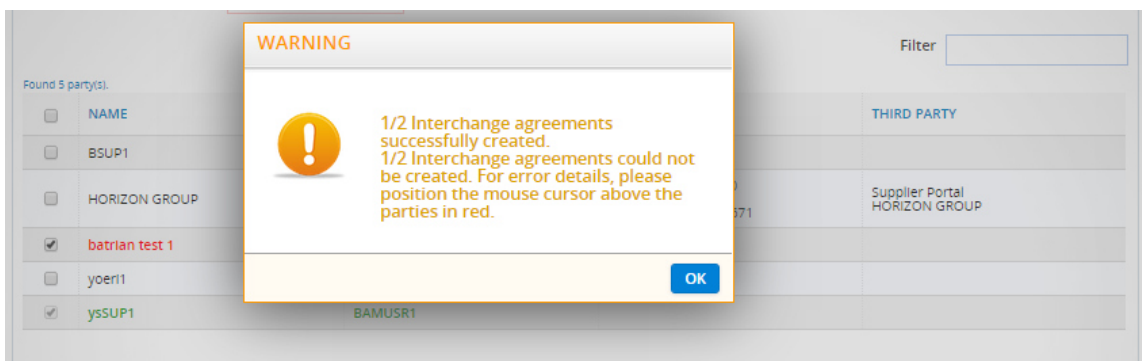**Figure 19 - Mass Creation of Interchange Agreements - Completed with errors**

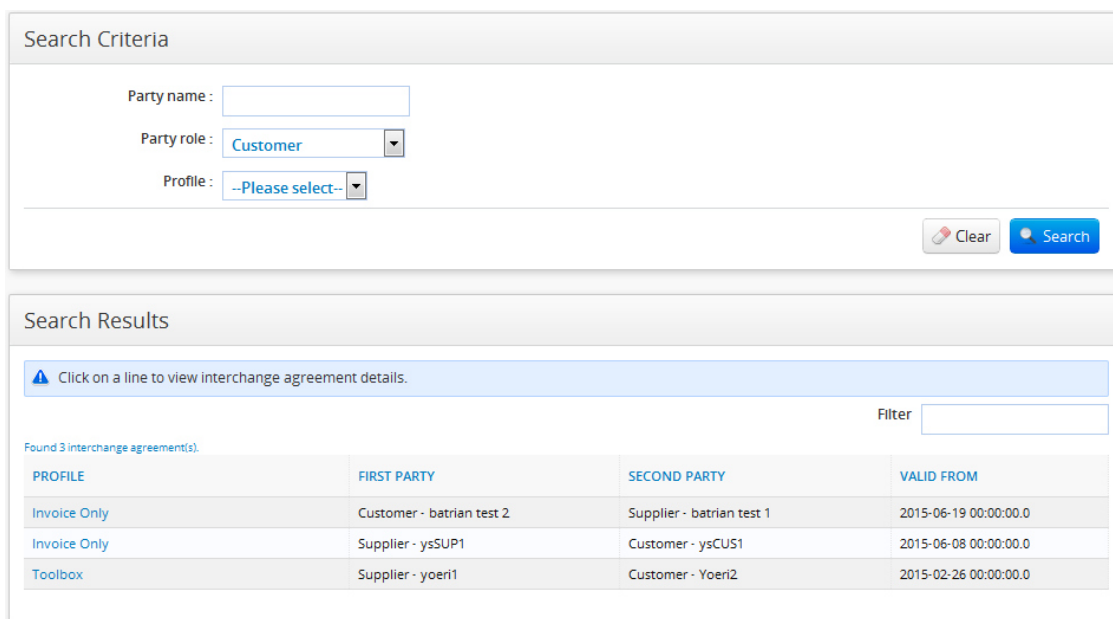**Figure 20 - Mass Creation of Interchange Agreements - Error tooltip**

8.3. Searching for an Interchange Agreement

To search for an interchange agreement, follow the next steps:

1. Navigate the application menu: Interchange Agreement > Search

2. Fill in the desired criteria: you can search by party name, party role or profile. *Note:* If you search by both party name and party role then you will get all the interchange agreements involving the specified party fulfilling precisely the specified role (a logical AND, not OR like commonly used in the search).

3. Choose [Search] button

4. The search result will be shown in the section at the bottom (Figure 21 - Interchange Agreement Search PageFigure 4 - Party Creation Page)

Please see section 3.2 for common search considerations.

Figure 21 - Interchange Agreement Search Page

8.4. Visualisation of Interchange Agreement Information

To see information of an interchange agreement, follow the next steps:

1. Navigate the application menu: Interchange Agreement > Search

2. Fill in the search criterions for the desired interchange agreement and click Search

3. Click on the interchange agreement you want to see in the search result list

4. You can now see the interchange agreement details as in Figure 22 - Interchange Agreement Visualisation Page

Please see section 3.3 for common visualisation considerations.

Figure 22 - Interchange Agreement Visualisation Page

8.5. Modifying an Interchange Agreement

To modify interchange agreement information, follow the next steps:

1. Navigate the application menu: Interchange Agreement > Search

2. Fill in the search criterions for the desired interchange agreement and click Search

3. Click on the interchange agreement you want to modify in the search result list (Figure 21 - Interchange Agreement Search Page)

4. You can now see the interchange agreement details as in Figure 22 - Interchange Agreement Visualisation Page

5. Choose [Edit] button at the bottom right

6. You can now see the interchange agreement modification screen (Figure 23 - Interchange Agreement Modification Page)

7. Fill in or change the desired information (you cannot change neither the profile nor the parties involved in the interchange agreement and their roles)

8. Choose [Save] button to save the modifications

Please see section 3.1 for common creation considerations.

Figure 23 - Interchange Agreement Modification Page

8.6. Deleting an Interchange Agreement

You cannot delete an interchange agreement if there are endpoint configurations referring to it, messages sent that have been authorized due to it etc. Also, if the interchange agreement belongs to a business domain you are not authorized to use, you will not be able to delete it.

If you are a Local Business Owner, you are also not authorized to delete an interchange agreement created by a more powerful user role (like ADM or CBO). You can only delete interchange agreements that pertain to your business domain and have been created by a LBO user role, as long as these interchange agreements are not used in any configuration and there are no messages sent under their authorisation.

To delete an interchange agreement, follow the next steps:

1. Navigate the application menu: **Interchange Agreement** > **Search**

2. Fill in the search criterions for the desired interchange agreement and click **Search**

3. Click on the interchange agreement you want to delete in the search result list (Figure 21 - Interchange Agreement Search Page)

4. You can now see the interchange agreement details as in Figure 22 - Interchange Agreement Visualisation Page

5. Choose 🗑 Delete button at the bottom right

6. Confirm the deletion (Figure 24 - Interchange Agreement Deletion Confirmation popup)

Figure 24 - Interchange Agreement Deletion Confirmation popup
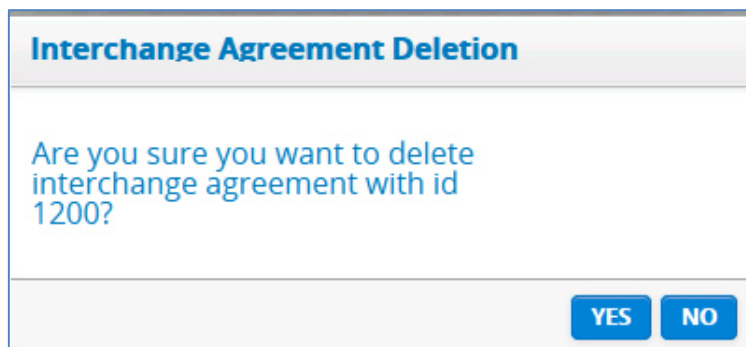
9. USER MANAGEMENT

The User is a person that can use the CIPAdmin Console for configuring and managing different entities. To do that the User must be configured and given access. This can be done via the administration console.

9.1. Creating a User

To create a user:

1. Navigate the menu: User > Create

2. The creation screen will be displayed as in Figure 25.

3. Fill in the desired information

4. Choose [Save] button to save the data

If you are a General Administrator, you can create any type of user.

If you are Central Business Owner, you can create only users having Local Business Owner role for your business domain. If you need a second Central Business Owner for your business domain you need to contact the support team (see chapter 4 Contact Section).
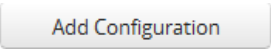
If you are a Local Business Owner or Support user, you cannot create any user configurations.

Below you can find the specificity corresponding to the configuration of different types of users. In all cases the username is mandatory and you can have a user fulfilling different roles on different business domains (this is ensured by adding more user configurations, one for each specific role of the user). Note that though passwords fields are present they are not used, as the application use ECAS authentication to authenticate the user to the application.

- Configuring ADM users:
    - o You must add a configuration with ADM user role.
    - o If you want to create an ADM with the same rights as yourself, you only need to add one configuration in which you do not specify any business domain.

- If you have ADM rights on 5 business domains, and you want to create an ADM for only 2 of them, you need to add 2 configurations in which you specify the ADM user role, one for each of the 2 business domains.

- Configuring CBO users:
    - You must add a configuration with CBO user role and specify one of the business domains you are authorized with.

- Configuring LBO users:
    - You must add a configuration with LBO user role, specify one of the business domains you are authorized with and choose a party from this business domain to which to associate the user.

To add a new access rights configuration:

1. Fill in the access rights data in the ▸ New User Access Rights section
2. Choose [Add Configuration] button
3. The new access rights configuration is displayed in the configuration list under the section ▸ User Access Rights

To modify an access rights configuration:

1. Choose [🖉] button in the actions column corresponding to the configuration to modify in the access rights configuration list
2. The configuration is loaded in the section ▸ New User Access Rights which becomes ▸ Edit User Access Rights
3. Do the necessary modifications and choose [Add Configuration] button or choose [Cancel] button if you changed your mind.
4. The configuration is updated in the access rights list to reflect the latest changes

To delete an access rights configuration:

1. Choose [✖] button in the action column corresponding to the configuration to delete in the access rights configuration list
2. Confirm the deletion of the selected configuration

Figure 25 - User Creation Page

9.2. Searching for a User

To search for a user, follow the next steps:

1. Navigate the application menu: **User** > **Search**

2. Fill in the desired criteria (you can search by username, user role, business domain, user party or any combination of them)

3. Choose [Search] button

4. The search result will be shown in the section at the bottom (Figure 26 - User Search PageFigure 4 - Party Creation Page)

Please see section 3.2 for common search considerations.

Figure 26 - User Search Page

9.3. Visualising User Information

To see user information, follow the next steps:

6. Navigate the application menu: **User** > **Search**

7. Fill in the search criterions for the desired user and click **Search**

8. Click on the user you want to see in the search result list

9. You can now see the user details as in Figure 27 - User Visualisation Page

Please see section 3.3 for common visualisation considerations.

Figure 27 - User Visualisation Page

9.4. Modifying a User

You cannot modify your own user details.

If you are ADM, you can modify any user pertaining to the business domains you are authorized with.

If you are CBO, you can only modify LBO users belonging to the business domain you are configured with.

Other user roles like LBO and SUP cannot modify users or their access rights.

To modify user information, follow the next steps:

1. Navigate the application menu: **User** > **Search**

2. Fill in the search criterions for the desired user and click **Search**

3. Click on the user you want to modify in the search result list (Figure 26 - User Search Page)

4. You can now see the user details as in Figure 27 - User Visualisation Page

5. Choose ✎ Edit button at the bottom right

6. You can now see the user modification screen (Figure 28 - User Modification Page)

7. Fill in or change the desired information (you cannot change the username)

   a. As the application is using ECAS authentication, the password fields are not used.

   b. Add, change or remove user access rights configurations as described in the end of section 9.1 Creating a User.

8. Choose 💾 Save button to save the modifications

Please see section 3.1 for common creation considerations.

Figure 28 - User Modification Page

9.5. Deleting a User

You cannot delete your user account.

If you are ADM, you can delete any user pertaining to the business domains you are authorized with.

If you are CBO, you can only delete LBO users belonging to your business domain.

Both for ADM and CBO, there is an exception: if the user you want to delete has access rights for a business domain you don't. In this case you can modify the user, and remove the access rights granted on the business domains you are authorized with.

Other user roles like LBO and SUP cannot delete users or their access rights.

To delete a user, follow the next steps:

1. Navigate the application menu: **User** > **Search**

2. Fill in the search criterions for the desired user and click **Search**

3. Click on the user you want to delete in the search result list (Figure 26 - User Search Page)

4. You can now see the user details as in Figure 27 - User Visualisation Page

5. Choose 🗑 Delete button at the bottom right

6. Confirm the deletion (Figure 29 - Confirmation of User Deletion)

Figure 29 - Confirmation of User Deletion
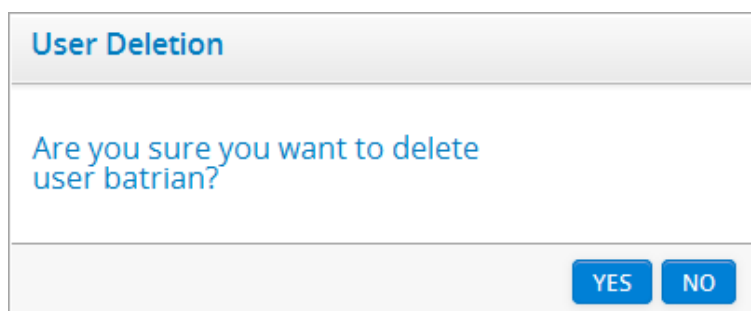
10. PARTY ROLE

A Party Role contains the information about the job function or title which is associated with expected behaviour or responsibilities of a party.

The configuration and management of party roles is done using a single screen (Figure 30).

Figure 30 - Party Role Page
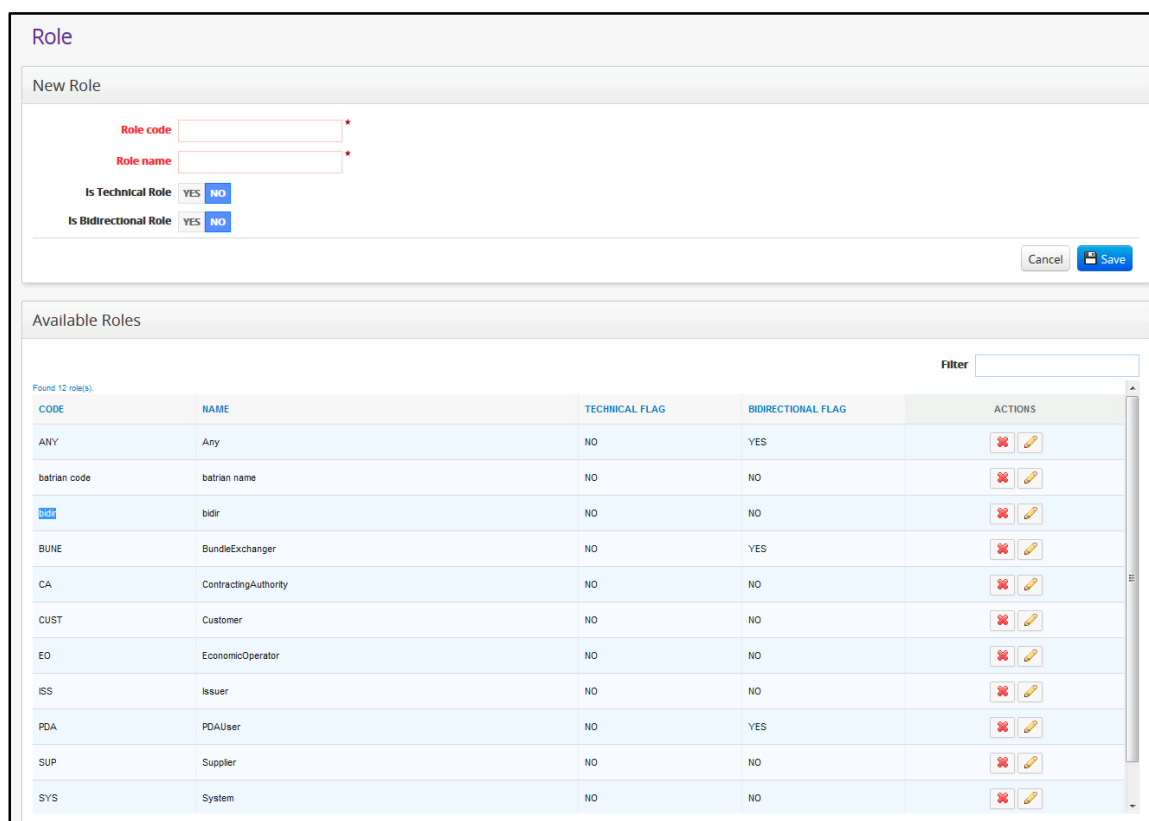
10.1. Creating a Party Role

To create a party role:

1. Navigate the menu: **Role**

2. The Party Role screen will be displayed as in Figure 30.

3. Fill in the party role information in the **New Role** section

- **Role code** is mandatory and must be unique

- **Role name** or description is mandatory and must be unique

- The **technical flag** is reserved to ADM users

- The **bidirectional flag** is used to indicate if the role can be used by both parties of an interchange agreement. E.g. BundleExchanger role can be used by both parties of an interchange agreement, whilst Supplier and Customer roles can only be used by one of the parties of an interchange agreement

4. Choose 💾 Save button to save the data

Please see section 3.1 for common creation considerations.

10.2. Searching for a Party Role

To search for a party role, follow the next steps:

1. Navigate the application menu: **Role**

2. In the **Available Roles** section of the party role screen (Figure 30) :

- Either scroll to the desired party role in the party role

- Or use the **Filter** in the top right corner to quickly filter the lines corresponding to the entered criteria

10.3. Visualising a Party Role

To view a party role, you can follow the same steps as for Searching for a Party Role. All the party role information is shown at the line level.

10.4. Modifying a Party Role

To modify a party role, follow the steps:

1. See steps for Searching for a Party Role

2. Choose ✏️ button on the line of the party role you want to modify

3. The role is loaded in the **Edit Role** section (Figure 31 - Edit Role Section) at the top of the screen

4. Make the desire changes. You cannot modify the role code. You cannot change a bidirectional flag set to Yes, if the role is used in an interchange agreement configuration.

5. Choose 💾 Save button to save the modifications

6. The modified role can now be seen in the section **Available Roles**

Figure 31 - Edit Role Section

10.5. Deleting a Party Role

You cannot delete a party role, if it is used in an interchange agreement or transaction configuration.

To delete a party role, follow the steps:

1. See steps for Searching for a Party Role

2. Choose [×] button on the line of the party role you want to delete

3. Confirm the deletion

4. The list of roles is refreshed

11. DOCUMENT

A document is a type of data that can be exchanged between two parties that have an interchange agreement in the context of a profile.

11.1. Creating a Document

You can only create documents if you have ADM role.

To create a document:

1. Navigate the menu: **Document** > **Create**

2. The creation screen will be displayed as in **Error! Reference source not found.**.

3. Fill in the document information

4. Choose [Save] button to save the data

Please see section 3.1 for common creation considerations.

Figure 32 - Document Creation Page

11.2. Searching for a Document

You can search for a document if you have ADM or SUP role.

To search for a document, follow the next steps:

1. Navigate the application menu: **Document** > **Search**

2. Fill in the desired criteria in **Search Criteria** section (Figure 33 - Document Search Page). You can search by document name, local name, document type code or any combination of them.

3. Choose Search button

4. The search result will be shown in the section at the bottom (Figure 33 - Document Search PageFigure 4 - Party Creation Page)

Please see section 3.2 for common search considerations.

Figure 33 - Document Search Page

11.3. Visualising a Document

You can visualise documents if you have ADM or SUP role.

To see document information, follow the next steps:

1. Navigate the application menu: **Document** > **Search**

2. Fill in the search criterions for the desired document and click [Search] button

3. Click on the document you want to see in the search result list

4. You can now see the document details as in Figure 34 - Document Visualization Page

Please see section 3.3 for common visualisation considerations.

Figure 34 - Document Visualization Page
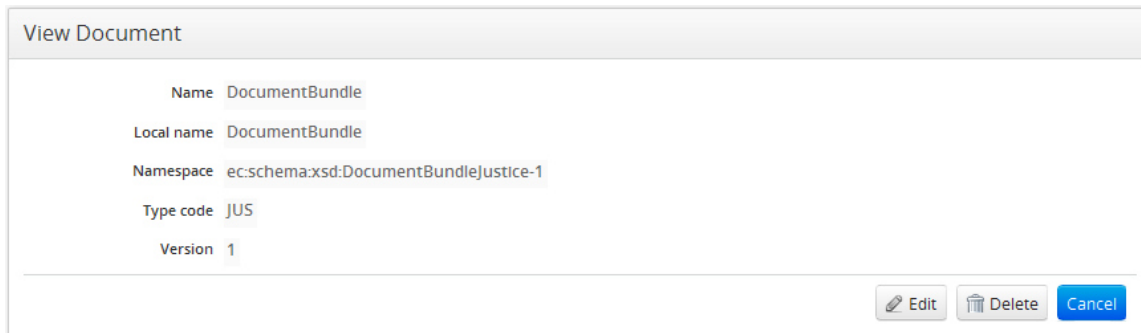
11.4. Modifying a Document

You can modify documents if you have ADM role.

To modify document information, follow the next steps:

1. Navigate the application menu: **Document** > **Search**

2. Fill in the search criterions for the desired document and click [Search] button

3. Click on the document you want to modify in the search result list (Figure 33 - Document Search Page)

4. You can now see the document details as in Figure 34 - Document Visualization Page

5. Choose [Edit] button at the bottom right

6. You can now see the document modification screen (Figure 35 - Document Modification Page) and edit the document

7. Fill in or change the desired information (you cannot change the document name)

8. Choose [Save] button to save the modifications

Figure 35 - Document Modification Page

11.5. Deleting a Document

You can delete documents if you have ADM role. You cannot delete a document if it is attached to a transaction.

To delete a document, follow the next steps:

1. Navigate the application menu: **Document** > **Search**

2. Fill in the search criterions for the desired document and click [Search] button

3. Click on the document you want to delete in the search result list (Figure 33 - Document Search Page)

4. You can now see the document details as in Figure 34 - Document Visualization Page

5. Choose [Delete] button at the bottom right

6. Confirm the deletion

12. METADATA

A Metadata Item represents a property configured in the system. . You can use it for example to configure the location of xsd files, different xpaths for extraction purposes, human readable templates to apply, specify if validation should be use or not etc.

12.1. Creating a Metadata Item

You can only create metadata items if you have ADM role.

To create a metadata item:

1. Navigate the menu: **Configuration** > **Metadata** > **Create**

2. The creation screen will be displayed as in Figure 36 - Metadata Creation Page.

3. Fill in the metadata item information

4. Choose [Save] button to save the data

Please see section 3.1 for common creation considerations.

Figure 36 - Metadata Creation Page

12.2. Searching for a Metadata Item

You can search metadata if you have ADM or SUP role.

To search for a metadata item, follow the next steps:

1. Navigate the application menu: **Configuration** > **Metadata** > **Search**

2. Fill in the desired criteria in **Search Criteria** section (Figure 37 - Metadata Search Page). You can search by the type of metadata, the document, interchange agreement, profile or transaction for which it is configured or any combination of them.

3. Choose Search button

4. The search result will be shown in the section at the bottom (Figure 37 - Metadata Search PageFigure 4 - Party Creation Page)

Please see section 3.2 for common search considerations.

Figure 37 - Metadata Search Page

12.3. Visualising a Metadata Item

You can visualise metadata if you have ADM or SUP role.

To see metadata item information, follow the next steps:

1. Navigate the application menu: **Configuration** > **Metadata** > **Search**

2. Fill in the desired criteria in **Search Criteria** section (Figure 37 - Metadata Search Page) and click [Search] button

3. Click on the metadata item you want to see in the search result list

4. You can now see the metadata details as in Figure 38 - Metadata Visualization Page

Please see section 3.3 for common visualisation considerations.

Figure 38 - Metadata Visualization Page

12.4. Modifying a Metadata Item

You can modify metadata items if you have ADM role.

To modify a metadata item, follow the next steps:

1. Navigate the application menu: **Configuration** > **Metadata** > **Search**

2. Fill in the search criterions for the desired metadata item and click [Search] button

3. Click on the metadata you want to modify in the search result list (Figure 37 - Metadata Search Page)

4. You can now see the metadata details as in Figure 38 - Metadata Visualization Page

5. Choose [Edit] button at the bottom right

6. You can now see the metadata modification screen (Figure 39 - Metadata Modification Page)

7. Fill in or change the desired information

8. Choose [Save] button to save the modifications

Figure 39 - Metadata Modification Page

12.5. Deleting a Metadata Item

You can delete metadata items if you have ADM role.

To delete a metadata item, follow the next steps:

1. Navigate the application menu: **Configuration** > **Metadata** > **Search**

2. Fill in the search criterions for the desired metadata item and click [Search] button

3. Click on the metadata you want to delete in the search result list (Figure 37 - Metadata Search Page)

4. You can now see the metadata details as in Figure 38 - Metadata Visualization Page

5. Choose [Delete] button at the bottom right

6. Confirm the deletion (Figure 40 - Metadata Deletion Confirmation popup)

Figure 40 - Metadata Deletion Confirmation popup
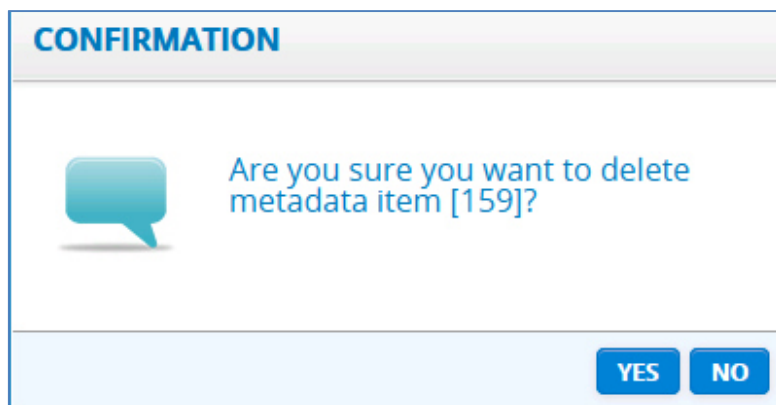
13. ROUTING ENDPOINTS

In order to forward messages from a party to another, or to send response messages to sender parties, the destination needs to be known. This destination is represented by routing endpoints which can be of two types: JMS endpoints and Web Services endpoints. Both types of routing endpoints can be configured via the Administration Console.

13.1. Endpoint Information

Specific JMS Endpoint information (Figure 41 - JMS specific configuration):

1. The JMS destination queue of the message

2. The initial JNDI context factory to be used

3. The JMS connection factory to use

4. If it is using a temporary reply queue or not

5. The JMS provider URL

6. The java message converter class used for converting the message in a specific format before sending it, if such format is needed in the receiver system

Figure 41 - JMS specific configuration

Specific Web Services Endpoint information (Figure 42 - Web Services specific configuration):

1. The web service URL

2. If the message needs to be signed before sending or not

3. If the response to the message should be signed or not by the sending endpoint

Figure 42 - Web Services specific configuration

Common information – used for both JMS and Web Services endpoints (Figure 43 - Common configuration):

1. **Message type** – the type of message the endpoint receives: Generic, Notification or Typed

2. **Endpoint status** – if the endpoint is active or not

3. **Authentication information:**

   a. If authentication is required for connecting to the endpoint

   b. Authentication credentials which is mandatory if authentication is required: authentication username and password

4. **Proxy information:**

   a. If endpoint is using proxy

   b. Proxy information. All proxy information is mandatory if proxy is used :

      i. Proxy host and port

      ii. Proxy credentials (username and password)

5. Information that is used to identify the messages that will be routed to this endpoint:

    a. Business domain

    b. Profile

    c. Transaction

    d. Interchange agreement

    e. Party

Figure 43 - Common configuration

13.2. Creating an Endpoint Configuration

You can only create endpoint configurations if you have ADM role.

To create an endpoint configuration:

1. Navigate the menu:

   - For JMS configurations: **Configuration** > **Routing Endpoints** > **Create** > **JMS Configuration**

   - For Web Services configurations: **Configuration** > **Routing Endpoints** > **Create** > **Web Services Configuration**

2. The creation screen will be displayed

   - As in Figure 44 - JMS Routing Endpoint Creation Page, if JMS configuration

   - As in Figure 45 - Web Service Routing Endpoint Creation Page, if Web Services configuration

3. Fill in the endpoint data

4. Choose 🖫 Save button to save the endpoint configuration

Please see section 3.1 for common creation considerations.

Figure 44 - JMS Routing Endpoint Creation Page

Figure 45 - Web Service Routing Endpoint Creation Page

13.3. Searching for an Endpoint Configuration

You can search endpoint configurations if you have ADM or SUP role.

To search for an endpoint configuration, follow the next steps:

1. Navigate the application menu: **Configuration** > **Routing Endpoints** > **Search**

2. Fill in the desired criteria in **Search Criteria** section (Figure 46 - Routing Endpoint Search Page). You can search by:

   - Endpoint type (JMS or Web Services)

   - Endpoint status (active or inactive)

   - Type of the message the endpoint is expecting

   - Authentication username

   - Proxy username

   - Business domain, profile, transaction, interchange agreement or party configured

3. Choose [Search] button

4. The search result will be shown in the section at the bottom (Figure 46 - Routing Endpoint Search PageFigure 4 - Party Creation Page)

Please see section 3.2 for common search considerations.

Figure 46 - Routing Endpoint Search Page

13.4. Visualising Endpoint Configurations

You can visualise endpoint configurations if you have ADM or SUP role.

To see endpoint configuration information, follow the next steps:

1. Navigate the application menu: **Configuration** > **Routing Endpoints** > **Search**

2. Fill in the desired criteria in **Search Criteria** section (Figure 46 - Routing Endpoint Search Page) and click ⊙ Search button

3. Click on the endpoint configuration you want to see in the search result list

4. You can now see the configuration details (e.g. Figure 47 - Endpoint Visualisation Page (web service configuration))

Please see section 3.3 for common visualisation considerations.

Figure 47 - Endpoint Visualisation Page (web service configuration)

13.5. Modifying an Endpoint Configuration

You can modify endpoint configurations if you have ADM role. The endpoint configuration will not be changed if there are messages configured to use it and not yet dispatched.

To modify an endpoint configuration, follow the next steps:

1. Navigate the application menu: **Configuration** > **Routing Endpoints** > **Search**

2. Fill in the search criterions for the endpoint configuration to modify and click Search button

3. Click on the configuration you want to modify in the search result list (Figure 46 - Routing Endpoint Search Page)

4. You can now see the configuration details

5. Choose Edit button at the bottom right

6. You can now see the configuration modification screen (e.g. Figure 48 - Endpoint Modification Page (web service configuration))

7. Fill in or change the desired information

8. Choose ![Save] button to save the modifications

Figure 48 - Endpoint Modification Page (web service configuration)

13.6. Deleting an Endpoint Configuration

You can delete endpoint configurations if you have ADM role. You cannot delete an endpoint configuration, if one of the messages for which it is configured has not been successfully processed.

To delete an endpoint configuration, follow the next steps:

1. Navigate the application menu: **Configuration** > **Routing Endpoints** > **Search**

2. Fill in the search criterions for the configuration to delete and click ![Search] button

3. Click on the configuration you want to delete in the search result list (Figure 46 - Routing Endpoint Search Page)

4. You can now see the configuration details

5. Choose ![Delete] button at the bottom right

6. Confirm the deletion (Figure 49 - Routing Endpoint Deletion Confirmation popup)

Figure 49 - Routing Endpoint Deletion Confirmation popup
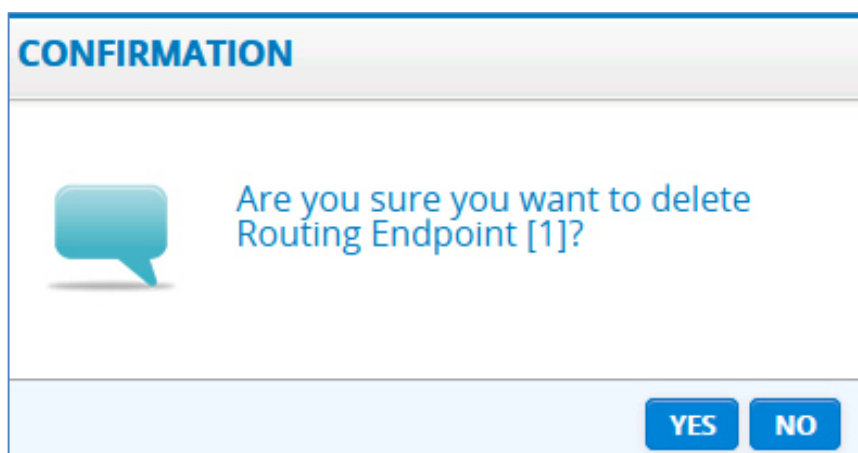
14. TRANSACTION

The Transaction describes one possible information exchange scenario. This would include the roles involved in the information exchange and the type of document.

14.1. Creating a Transaction

You can only create transactions if you have ADM role.

To create a transaction:

1. Navigate the menu: **Transaction** > **Create**

2. The creation screen will be displayed as in Figure 50 - Transaction Creation Page.

3. Fill in the transaction information

4. Choose [Save] button to save the data

Please see section 3.1 for common creation considerations.

Figure 50 - Transaction Creation Page

14.2. Searching for a Transaction

You can search for a transaction if you have ADM or SUP role.

To search for a transaction, follow the next steps:

1. Navigate the application menu: **Transaction** > **Search**

2. Fill in the desired criteria in **Search Criteria** section (Figure 51 - Transaction Search Page). You can search by transaction name, document name, sender or receiver roles, and associated profiles.

3. Choose [Search] button

4. The search result will be shown in the section at the bottom (Figure 51 - Transaction Search PageFigure 4 - Party Creation Page)

Please see section 3.2 for common search considerations.

Figure 51 - Transaction Search Page

14.3. Visualising a Transaction

You can visualise transactions if you have ADM or SUP role.

To see transaction information, follow the next steps:

1. Navigate the application menu: **Transaction** > **Search**

2. Fill in the search criterions for the desired transaction and click [Search] button

3. Click on the transaction you want to see in the search result list

4. You can now see the transaction details as in Figure 52 - Transaction Visualisation Page

Please see section 3.3 for common visualisation considerations.

Figure 52 - Transaction Visualisation Page

14.4. Modifying a Transaction

You can modify transactions if you have ADM role. You cannot modify a transaction if messages using this transaction configuration have been received.

To modify transaction information, follow the next steps:

1. Navigate the application menu: **Transaction** > **Search**

2. Fill in the search criterions for the desired document and click [Search] button

3. Click on the transaction you want to modify in the search result list

5. You can now see the transaction details as in Figure 52 - Transaction Visualisation Page

4. Choose [Edit] button at the bottom right

5. You can now see the transaction modification screen (Figure 53 - Transaction Modification Page)

6. Fill in or change the desired information

7. Choose [Save] button to save the modifications

Figure 53 - Transaction Modification Page

14.5. Deleting a Transaction

You can delete transactions if you have ADM role. You cannot delete a transaction if messages using this transaction configuration have been received or the transaction is used for other configuration purposes (such as endpoint, profile etc.).

To delete a transaction, follow the next steps:

1. Navigate the application menu: **Transaction** > **Search**

2. Fill in the search criterions for the desired transaction and click [🔍 Search] button

3. Click on the transaction you want to delete in the search result

4. You can now see the transaction details

5. Choose [🗑 Delete] button at the bottom right

6. Confirm the deletion (Figure 54 - Transaction Deletion Confirmation popup)

Figure 54 - Transaction Deletion Confirmation popup
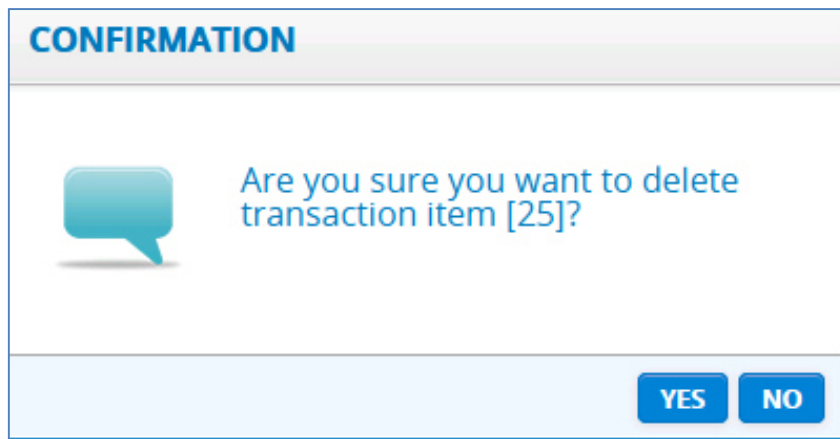
15. PROFILE

A Profile is the entity that captures the aspects of a business collaboration represented by a set of transactions, so certain document types that can be exchanged between parties having specific roles as defined in the profile transactions.

15.1. Creating a Profile

You can only create profiles if you have ADM role.

To create a profile:

1. Navigate the menu: **Profile** > **Create**

2. The creation screen will be displayed as in Figure 55 - Profile Creation Page**Error! Reference source not found.**.

3. Fill in the profile information

4. Choose [💾 Save] button to save the data

Please see section 3.1 for common creation considerations.

Figure 55 - Profile Creation Page

15.2. Searching for a Profile

You can search for a profile if you have ADM or SUP role.

To search for a profile, follow the next steps:

1. Navigate the application menu: **Profile** > **Search**

2. Fill in the desired criteria in **Search Criteria** section (Figure 56 - Profile Search Page). You can search by profile name, business domain, and transaction belonging to the profile.

3. Choose 🔍 Search button

4. The search result will be shown in the section at the bottom (Figure 56 - Profile Search PageFigure 4 - Party Creation Page)

Please see section 3.2 for common search considerations.

Figure 56 - Profile Search Page

15.3. Visualising a Profile

You can visualise profiles if you have ADM or SUP role.

To see profile information, follow the next steps:

1. Navigate the application menu: **Profile** > **Search**

2. Fill in the search criterions for the desired profile and click [Search] button

3. Click on the profile you want to see in the search result list

4. You can now see the profile details as in Figure 57 - Profile View

Please see section 3.3 for common visualisation considerations.

Figure 57 - Profile View

15.4. Modifying a Profile

You can modify profiles if you have ADM role. You cannot modify the profile name and, if the profile is used to define an existing interchange agreement, the associated business domains and transactions.

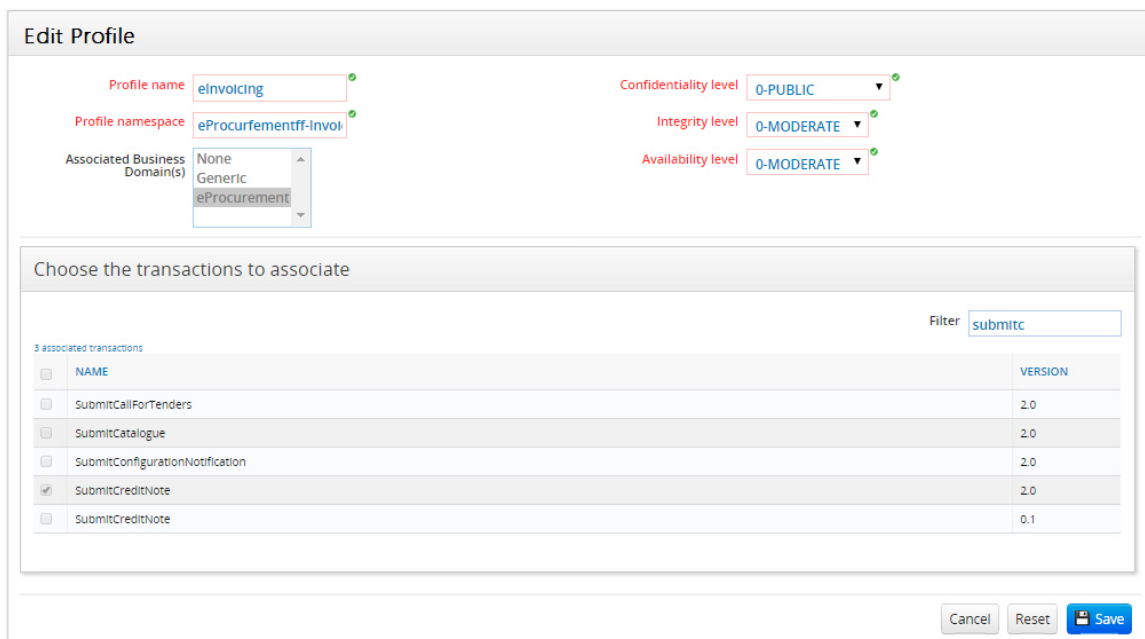To modify profile information, follow the next steps:

1. Navigate the application menu: **Profile** > **Search**

2. Fill in the search criterions for the desired document and click [Search] button

3. Click on the profile you want to modify in the search result list

5. You can now see the profile details

4. Choose [Edit] button at the bottom right

5. You can now see the profile modification screen (Figure 58 - Profile Modification Page)

6. Fill in or change the desired information

7. Choose [Save] button to save the modifications

Figure 58 - Profile Modification Page

15.5. Deleting a Profile

You can delete profiles if you have ADM role. You cannot delete a profile if there is an interchange agreement corresponding to it, or if it is used for configuration purposes (in endpoint configuration, metadata configuration etc.).

To delete a profile, follow the next steps:

1. Navigate the application menu: **Profile** > **Search**

2. Fill in the search criterions for the desired transaction and click [Search] button

3. Click on the transaction you want to delete in the search result

4. You can now see the transaction details

5. Choose ⟨🗑 Delete⟩ button at the bottom right

6. Confirm the deletion (Figure 59 - Profile Deletion Confirmation popup)

Figure 59 - Profile Deletion Confirmation popup

16. CIPADMIN/ETRUSTEX LOGS

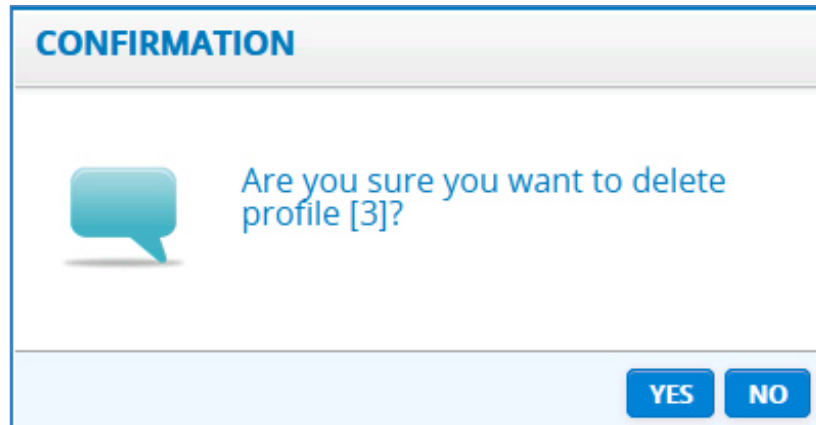The Logs are an important support feature of CIPAdmin. It is here where an investigation will start in case an error is reported. Just by having the log correlation id, a user in charge with error investigation can see every important action that has been taken from the beginning of the flow until the error occurred. This helps in understanding the conditions in which the error occurred, and makes it easier to reproduce it, and thus take the appropriate actions related to it.

You can access this feature if you have ADM or SUP role.

16.1. Searching for a Log

To search for a log record, follow the next steps:

1. Navigate the application menu:

   • For CIPAdmin logs: **Logs** > **CIPAdmin Logs** (Figure 60 - CIPAdmin Logs Search Page)

   • For eTrustEx logs: : **Logs** > **eTrustEx Logs** (Figure 61 - eTrustEx Logs Search Page)

2. Fill in the desired criteria in **Search Criteria** section

   • For CIPAdmin logs, you can search by

     – creation date

     – log type: SUCCESS, ERROR, EXCEPTION

     – operation: creation, modification, etc.

- the entity on which the operation was executed: party, interchange agreement etc.

- the business domain where the event occurred

- the username of the user that was connected to the administration console when the event happened

- the session id of the administration console session

- the id of the entity on which the operation was executed: party id, user id etc.

- for eTrustEx logs, you can search by

  - creation date

  - log type: Authorisation, Dispatch, Retrieve, Store etc

  - operation: creation, modification, etc.

  - the business domain where the event occurred

  - the document type code and id

  - correlation and business correlation id

  - issuer, sender and receiver id

3. Choose [Search] button

4. The search result will be shown in the section at the bottom

Please see section 3.2 for common search considerations.

Figure 60 - CIPAdmin Logs Search Page

CIPAdmin Logs

Search Criteria

Creation date from		Business domain	eProcurement ▼
to		Username	
Type	ERROR ▼	Session Id	
Operation	DELETE ▼	Entity Id	
Entity	InterchangeAgreement ▼		

✎ Clear   ● Search

Search Results

⚠ To select a log, click the log creation date.

Filter

Found 8 results

DATE	TYPE	BUSINESS DOMAIN	USERNAME	USER ROLE	SESSION ID	OPERATION	ENTITY	ENTITY ID
26/05/2015 15:17:01	ERROR	eProcurement	smetsyo	ADM	38IQXc1J29BKlDv2f2yvkDHv9jggvF5-nWdwCGD6K_PXkDXxIazz!1853892621!1432646176099	DELETE	InterchangeAgreement	69997156
29/04/2015 11:44:10	ERROR	eProcurement	smetsyo	ADM	LykEJwuRE3VvJnkdL9KCnc7gCwuHDGJIzfwIAB6cpXE_ILloC5GX!642252268!1430300593041	DELETE	InterchangeAgreement	68571156
29/04/2015 11:44:26	ERROR	eProcurement	smetsyo	ADM	LykEJwuRE3VvJnkdL9KCnc7gCwuHDGJIzfwIAB6cpXE_ILloC5GX!642252268!1430300593041	DELETE	InterchangeAgreement	68295156
29/04/2015 11:44:47	ERROR	eProcurement	smetsyo	ADM	LykEJwuRE3VvJnkdL9KCnc7gCwuHDGJIzfwIAB6cpXE_ILloC5GX!642252268!1430300593041	DELETE	InterchangeAgreement	68935156
29/04/2015 11:45:44	ERROR	eProcurement	smetsyo	ADM	LykEJwuRE3VvJnkdL9KCnc7gCwuHDGJIzfwIAB6cpXE_ILloC5GX!642252268!1430300593041	DELETE	InterchangeAgreement	68295156
29/04/2015 13:15:13	ERROR	eProcurement	smetsyo	ADM	434E4PFc3fRBA2dXU_M8LvP6rvVQvoJ4DYUDeaJOv5OwXan9-OVz!642252268!1430305960284	DELETE	InterchangeAgreement	69104156
29/04/2015 13:15:16	ERROR	eProcurement	smetsyo	ADM	434E4PFc3fRBA2dXU_M8LvP6rvVQvoJ4DYUDeaJOv5OwXan9-OVz!642252268!1430305960284	DELETE	InterchangeAgreement	69104156
29/04/2015 13:15:37	ERROR	eProcurement	smetsyo	ADM	434E4PFc3fRBA2dXU_M8LvP6rvVQvoJ4DYUDeaJOv5OwXan9-OVz!642252268!1430305960284	DELETE	InterchangeAgreement	69064156

Figure 61 - eTrustEx Logs Search Page

16.2. Visualising a Log Record

You can visualise log records if you have ADM or SUP role.

To see a log record, follow the next steps:

1. Reproduce steps from 16.1 Searching for a Log

2. Click on the log record you want to see in the search result list

3. You can now see the log details

   – as in Figure 62 - CIPAdmin Log Details popup, for CIPAdmin logs

   – as in Figure 63 - eTrustEx Log Details popup, for eTrustEx logs

Please see section 3.3 for common visualisation considerations.

Figure 62 - CIPAdmin Log Details popup

Log Details

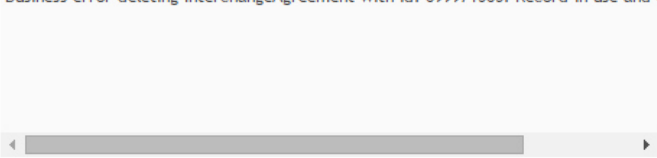|	
Creation date	26/05/2015 15:17:01
Module	CIPADMIN
Business domain	eProcurement
Username	smetsyo
User role	ADM
Session Id	38iQXc1j29BKlDv2f2yvkDHv9jggVF5-hWdwCGD6K_PXkDXxIazz!1833692621!1432646176099
Type	ERROR
Operation	DELETE
Entity	InterchangeAgreement
Entity Id	699971565
Description	Business error deleting InterchangeAgreement with id: 699971565: Record in use and
Authenticated IP address	158.166.148.134
URL	/etrustex-admin-web/ica/699971565/delete.do

Cancel

Figure 63 - eTrustEx Log Details popup
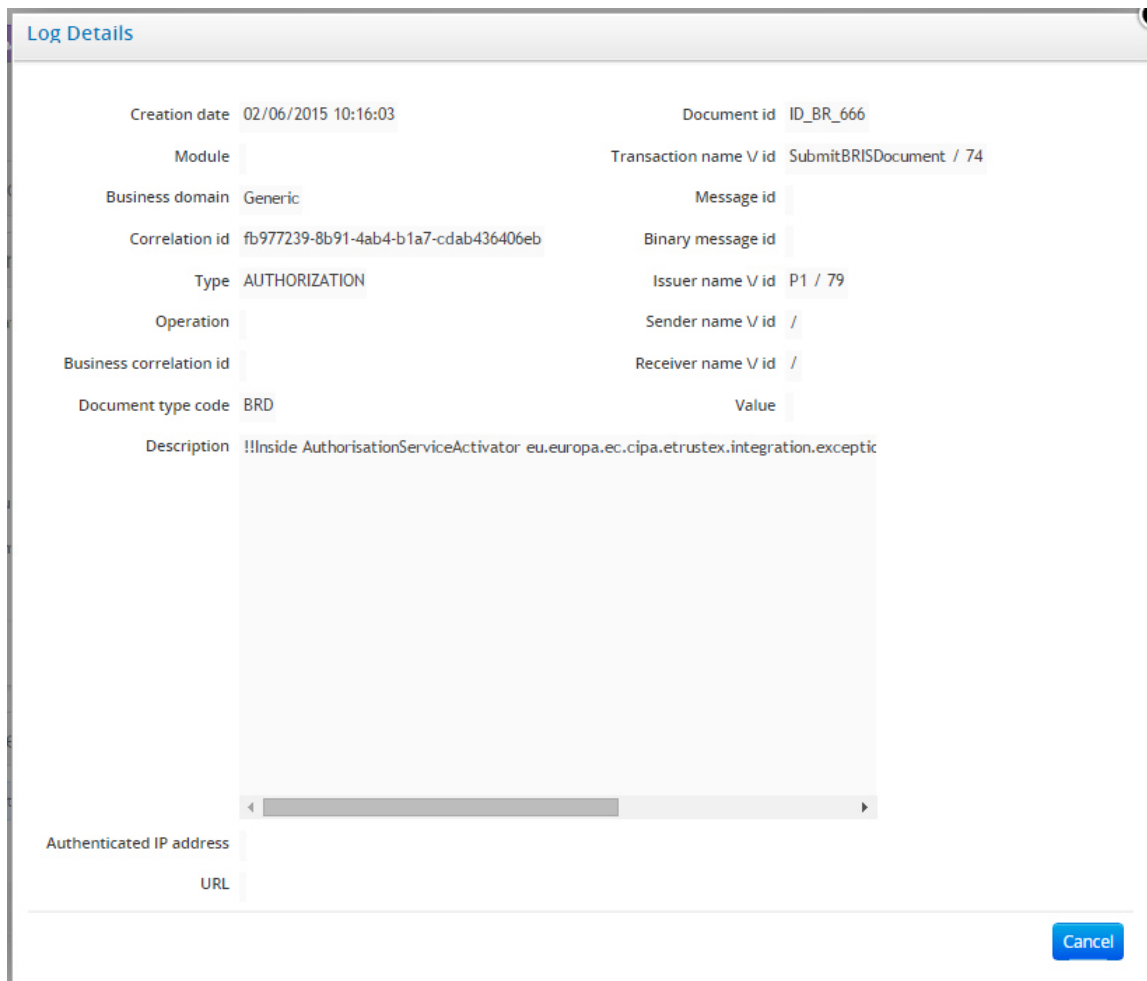
17. ERRORS SECTION

The user can get some errors during the different processing phases supported by the Admin Console.

- In case of validation errors user will be warn what it is wrong so that he/she can correct the issues (an example is presented in Figure 64 - Validation errors);

- In case of authorization problems user will be notified that the operation he/she is trying to do is not allowed (an example is presented in Figure 65 - Authorisation error);

- In case of technical errors user will be informed that an error occurred.

Figure 64 - Validation errors

Figure 65 - Authorisation error