User and Security Module (USM)
User manual

Contents of this manual:

1. Introduction

1.1. Purpose of the User and Security module

The **User and Security Module (USM)** is a functionality within SFC2007 Front-Office that allows Member State Liaison Officers (and Member State Liaison Deputy Officers) to enter access requests for the node(s) and fund(s) they manage.

1.2. How to access the User and Security Module?

The USM is a functionality within SFC2007 Front-Office. This means that a MS liaison (deputy) who has access to SFC2007 Front-Office can use his/her nominative ECAS username and password to log in to SFC2007 Front-office and access the USM.

IMPORTANT	MS liaisons (and deputies) should never share their access codes with anyone else! Any misuse of their access codes is under their responsibility!

The SFC2007 application has different environments used for different purposes:

- The PRODUCTION environment is the real working environment where users enter real data.
- The ACCEPTANCE environment is used for training purposes. This environment does not contain real data. In this environment the users can "play" with SFC2007 and learn how to use it (if they want to). This environment is also used by Technical (IT) teams of countries dealing with web-services (no manual data entry but automatic processing between local systems in the Member State and SFC2007).
- The BETA environment is used by IT teams of countries dealing with web-services. This environment contains features that are being developed and are not yet available in the production nor in the acceptance environment.

Concretely, this means that the MS liaison (deputy) must connect to the environment concerned to enter a request!

However, to facilitate the task of the MS liaison (deputy), an extra feature in the production environment allows the MS liaison (deputy) to create the request in ACCEPTANCE (i.e. the training environment) automatically if they want to. For the BETA environment this option doesn't exist.

Link to the different environments:

- **PRODUCTION**: https://webgate.ec.europa.eu/sfc2007/frontoffice
- **ACCEPTANCE**: https://webgate.acceptance.ec.europa.eu/sfc2007/frontoffice
- **BETA**: https://webgate.acceptance.ec.europa.eu/sfc2007/beta/frontoffice

1.3. The User and Security Module menus

The USM is accessible from SFC2007 Front-Office via the menu **UTILITIES.**

The following sub-menus allow the creation of requests and consulting existing users:

- **ACCESS REQUESTS**: via this submenu, the MS liaison (deputy) can enter the requests for access. This submenu is visible to MS liaisons and deputies only.
- **CONTACTS/USER ACCOUNTS**: via this submenu it is possible to view the list of existing users managed by the MS liaison (deputy). This submenu is visible to MS liaisons and deputies only.

2. Types of request that can be managed in the USM

An MS liaison (deputy) can create and send requests for different actions on users:

- Create new account for web User
- Create new account for Certificate
- Update existing account for Web User
- Update existing account for Certificate
- Disable existing account for Web User
- Disable existing account for Certificate
- Renew certificate
- Grant access to an existing web-user managed by another Member State Liaison

IMPORTANT	A **certificate** user account enables local information systems to authenticate when communicating with SFC2007 through **web-services**. Requests for certificate user accounts should only be created by countries using the web-services! Unlike the web user accounts that access the application SFC2007 with a nominative ECAS user account, certificate user accounts remain generic user accounts starting with **w005**…

The following chapters explain step by step how to manage these types of requests.

2.1. Request to create new account for web user

You can request the creation of a new account when a user doesn't exist yet and has never existed in SFC2007 before.

- If a user existed but is inactive because he/she was disabled, you can create a request to UPDATE EXISTING ACCOUNT FOR WEB USER (see chapter 2.2)
- If the user exists but is managed by another MS liaison, you can request to GRANT ACCESS TO AN EXISTING WEB-USER MANAGED BY ANOTHER MEMBER STATE LIAISON (see chapter 2.3)
- If the user already exists and is active, you can create a request to UPDATE EXISTING ACCOUNT FOR WEB USER (see chapter 2.2)

BEFORE YOU START	Ensure that the user does not yet exist by verifying in the list of users (please refer to section 3) Ensure that the user is not managed by another MS liaison (see chapter 2.3.1) Ensure that you have all necessary information about the user including the **ECAS-uid**[1]. The request must be created and sent in a single operation!

Workflow

[1] The user must have an ECAS nominative account and communicate his/her ECAS-uid to the MS Liaison (deputy). Please refer to the quick guides section of the SFC2007 Help page for the presentation on how to create an ECAS nominative account: http://ec.europa.eu/employment_social/sfc2007/quick-guides/New_ECAS nominative_account_creation for SFC2007 migration_EN.pdf

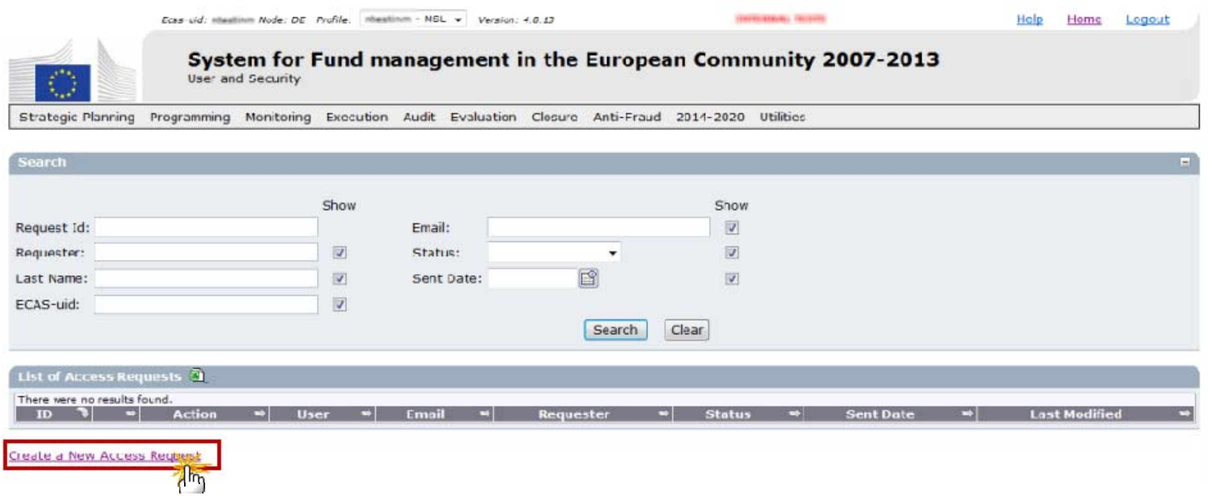
Select the type of request ⇒ Enter personal information of the user ⇒ Select nodes* ⇒ Grant roles and permissions ⇒ Send the request ⇒ Request is Processed, Returned or Cancelled

* only for multi-node countries

2.1.1. Select the type of request you want to create

Step by step…

1. On the menu UTILITIES > ACCESS REQUESTS click the **Create a New Access Request** link.



2. The wizard appears. Select the action CREATE NEW ACCOUNT FOR WEB USER 1.
3. Click NEXT 2.

2.1.2. Enter the user information

The Edit User Information screen appears. Fields marked with an asterisk (*) are mandatory:

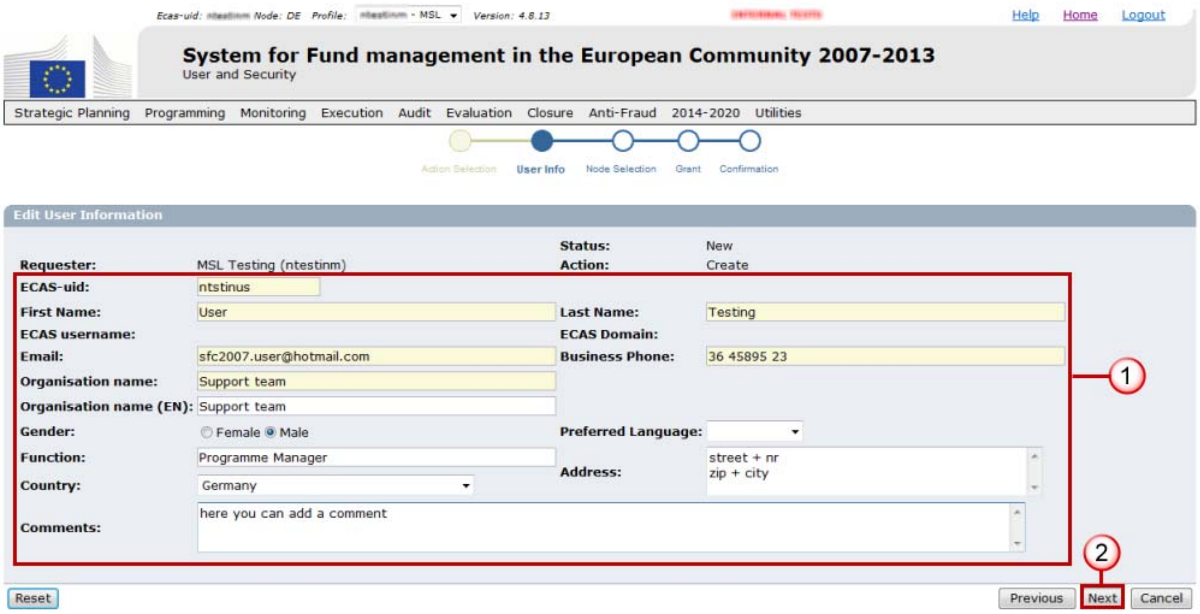
- ECAS-uid*

- First Name*
- Last Name*
- Email*
- Business Phone*
- Organisation name*
- Organisation name (EN)
- Gender
- Preferred Language (for the notifications)
- Function
- Country
- Address
- Comments

TIP	Start typing the first letters of the Organisation name. If the organisation has already been entered before in the system, the full name will be displayed in a list where you can select it from.

Step by step…

4. Enter the requested information 1.
5. Click **NEXT** to continue 2.



- You can click **PREVIOUS** to go back to the previous step or click **CANCEL** to cancel the creation of the whole request. Click **RESET** if you want to clear the information entered in the fields.

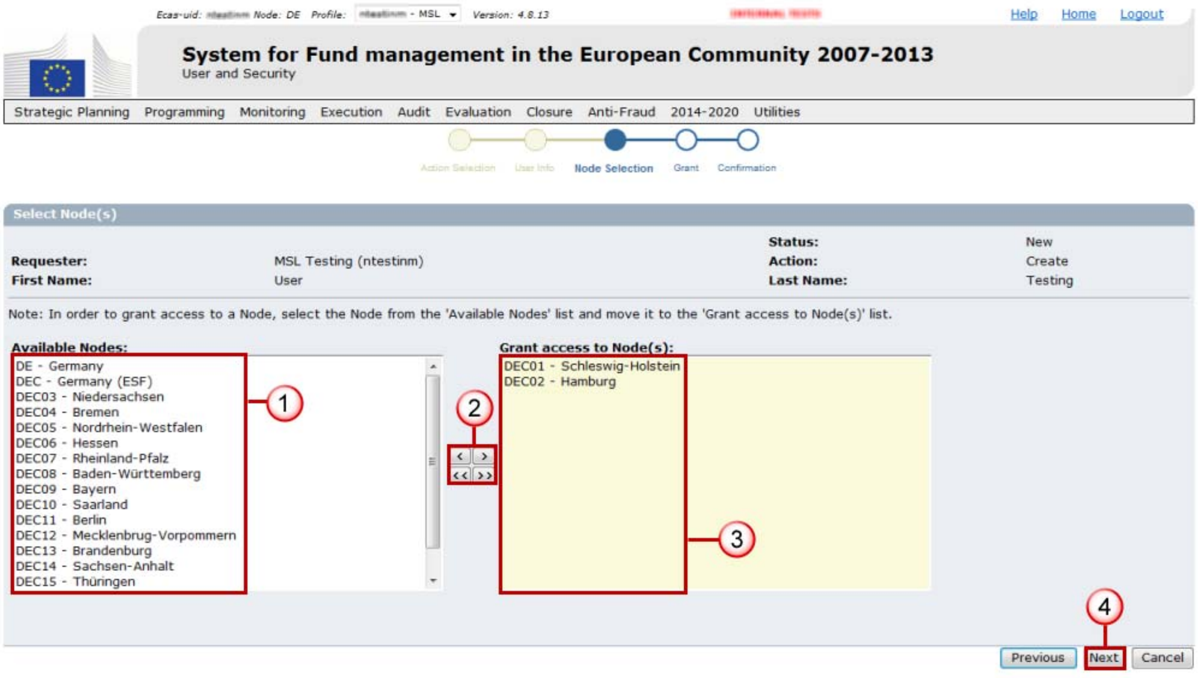
2.1.3. Choose nodes (only for multi-node countries)

IMPORTANT	This step is only available for the MS liaison (deputy) from countries having a multi-node structure (Examples: Germany, Italy, France, Spain…). For countries with a single node structure (Examples: Czech Republic, Portugal, Sweden…) this step is skipped by the wizard! You can continue to chapter 2.1.4

You must define the nodes the user will have access to. As there are different nodes within your country, the user probably needs only access to one or some of them, so you must specify this.

Step by step…

6. On the select nodes window, select the node from the left pane (AVAILABLE NODES)1.
7. Click the right-arrow button > in the middle of the panes2.
8. The node is added to the pane in the right (GRANT ACCESS TO NODE(S))3.
9. Repeat these steps for each node you want to select.
10. When finished, click NEXT to go to the next step4.



TIP	To select all nodes in the list, click on the double right-arrow button >>. To deselect all the nodes selected in the right pane, click the double left-arrow button <<.

Once the user has been created, each node defined for the user will become a profile. When connected in SFC2007 the user has to choose the profile he/she wants to use and will have access to the node corresponding to the profile selected.

2.1.4. Grant roles and permissions

The GRANTS ROLES TO USER ON SPECIFIC NODE(S) screen appears. On this screen you must select the roles and permissions you want to grant for this user.

The roles and permissions shown correspond to the roles and permissions that the MS liaison (deputy) can request for as well as the Directorate General (according to Funds) for which the MS liaison (deputy) can request access.

- **EMPL**: ESF - IPA Component IV
- **REGIO**: ERDF - CF - IPA Component II and III
- **MARE**: EFF - IPA component

- **AGRI**: EAFRD - IPA Component V

The roles and permissions are created on the Node for which the MS liaison (deputy) can request (or on each of the nodes selected in previous step).

IMPORTANT	The USM automatically detects incompatible roles. The roles that are incompatible with the role you selected are greyed. You cannot select these. **Example**: You select "MS Managing Authority EMPL Send". The roles, "MS Certifying Authority EMPL Send" and "MS Audit Authority EMPL Send" are greyed.

IMPORTANT	Please note that the MS Managing Authority Send role includes Update access unlike the MS Certifying Authority and MS Audit Authority roles where users having the Send role cannot Update!

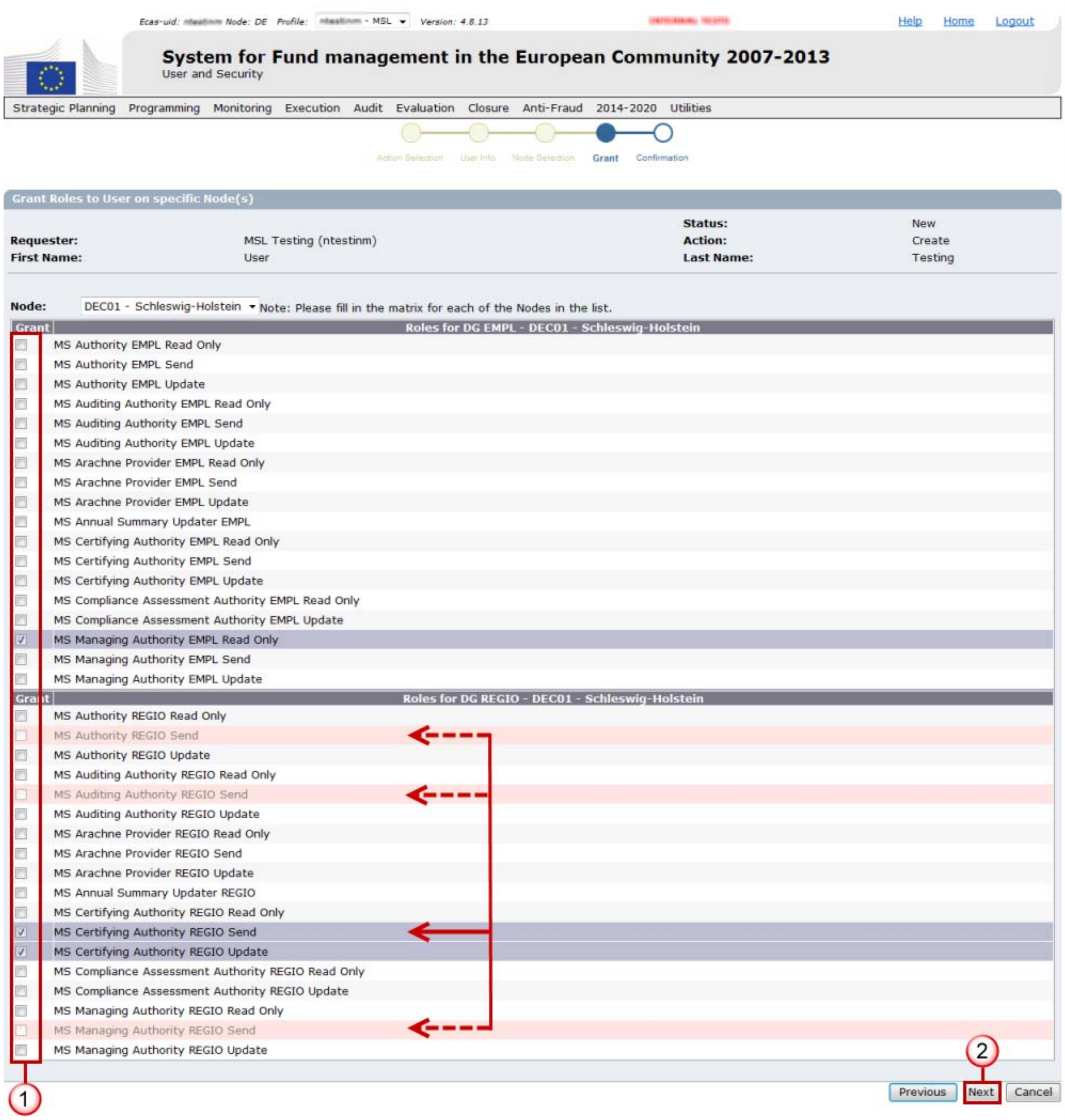
Step by step…

11. If you are dealing with a multi-node country, you must first select each of the nodes you chose in the previous step.

If you are dealing with a single-node country, the node is automatically displayed.

12. Tick the boxes to select the roles and permissions you want to grant 1. The USM automatically detects incompatible roles. The roles that are incompatible with the role you select are greyed. You cannot select these ones (see example below).

13. Click NEXT to get to the final step (reviewing and sending the request for the Commission) 2.



- You can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

2.1.5. Send the request to the SFC2007 Support team

After entering the User Information, the nodes and the roles and permissions to grant, you are ready to send the request to the SFC2007 Support team.

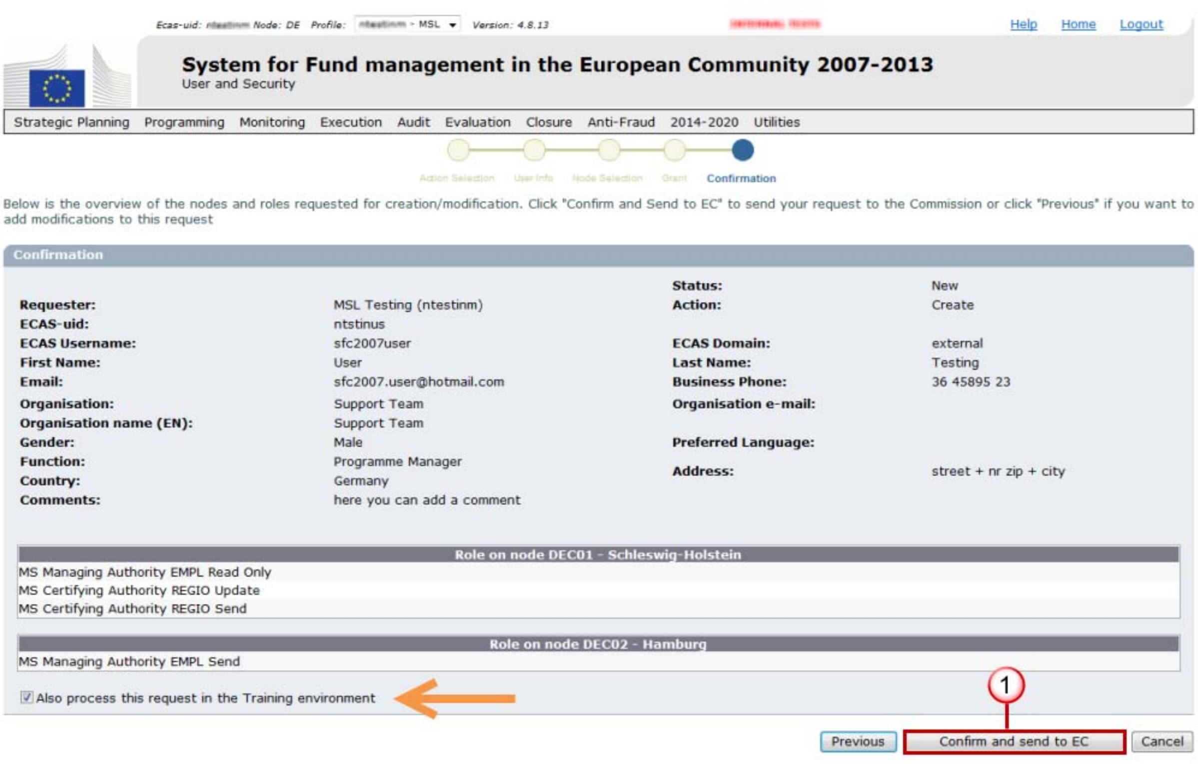
The overview of your request is shown. You see:

- The user information you entered.
- The roles and permissions you selected to be granted for the selected nodes.
- Before sending the request, you can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

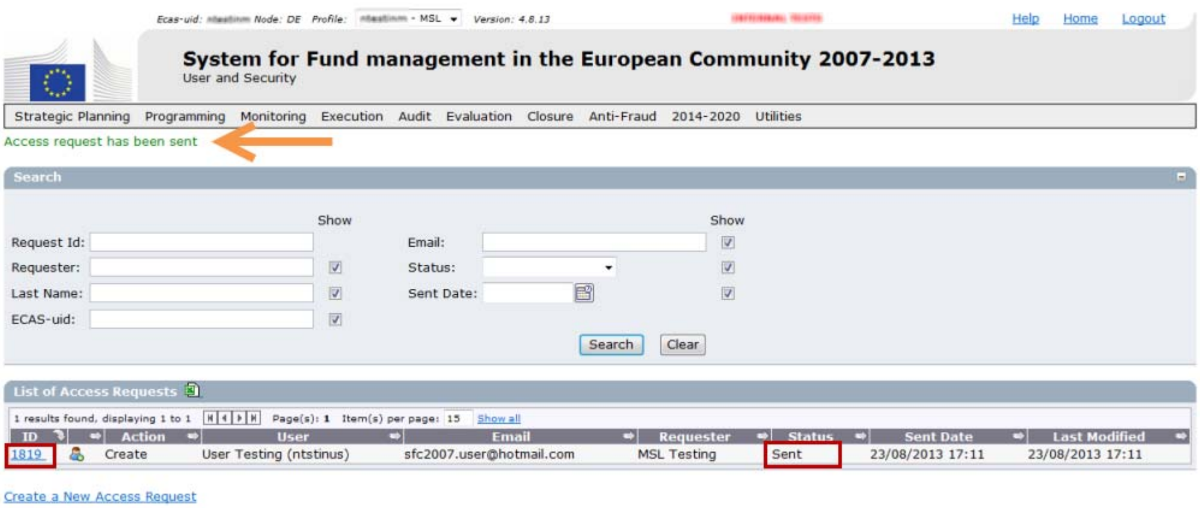
Step by step…

14. Only for the PRODUCTION environment: The option "Also process this request in the Training environment" is checked. Leave it checked if you want the request to be automatically processed in the training environment too. You can uncheck this option if you want the request only to be processed in production environment (and not in training).

15. Click the button CONFIRM AND SEND to send the request to the SFC2007 Support team 1



Once the request is sent, you are redirected to the list of requests. Your request is given a unique identifier number (ID). The status of the request is SENT.



The request can now be processed by the SFC2007 Support team. If there are mistakes or other issues, the request is returned to you by the SFC2007 Support team.

2.1.6. If the request is processed…

If the request is processed, the status becomes PROCESSED and two automatic e-mails are sent:

- One e-mail to the **MS liaison or MS liaison Deputy** who created the request containing:
  - A link with the request identifier (ID) to view the processed request.
- One mail to the **concerned user** containing:
  - The access details and roles and permissions granted for each node.

2.1.7. If the request is returned (not processed)…

If the Support team detects problems or missing information, or if the user appears to exist already, the status becomes RETURNED and one e-mail is sent to the MS liaison or MS liaison Deputy with an explanation on the reason for returning.

The MS liaison (deputy) can:

- Correct the request and send it again (see 2.9) or
- Cancel the request (see 2.10)

2.2. Create a request for updating an existing web user

You can create a request to update (modify) a user if any information must be updated:

- the user information (personal details);
- the node(s) the user should have access to;
- the roles and permissions needed;

and to re-activate a disabled user account.

IMPORTANT	Disabled web users have not been migrated to nominative user accounts in SFC2007. If you want to re-activate a user, which was disabled at the time of migration, you will have to create and send an access request to UPDATE the existing (disabled) w005… user account. Please add the **user's ECAS-uid** in the COMMENT field on the EDIT USER INFO screen when creating the request!

BEFORE YOU START	Ensure that you have all necessary information about the user. The request must be created and sent in a single operation!

Workflow

Select the type of request	⇒	Modify personal information of the user	⇒	Modify nodes*	⇒	Modify roles and permissions	⇒	Send the request	⇒	Request is Processed, Returned or Cancelled

* only for multi-node countries

2.2.1. Select the type of request you want to create

Step by step…

1. On the menu UTILITIES > ACCESS REQUESTS click the **Create a New Access Request** link.
2. The wizard appears. Select the action UPDATE EXISTING ACCOUNT FOR WEB USER1.
3. On the blank field that appears next to the selected type of request, you can enter the **last name**, **ECAS-uid** or the **e-mail** address of the user you want to update2.
4. The user appears in the list, so you can select it.
5. After selecting the user, click NEXT3.

2.2.2. Modify the user information

You can modify the information on the user or you can skip this step by clicking NEXT. The Edit User Information screen appears.

Following information can be modified. Please remember that fields marked with an asterisk (*) are mandatory:

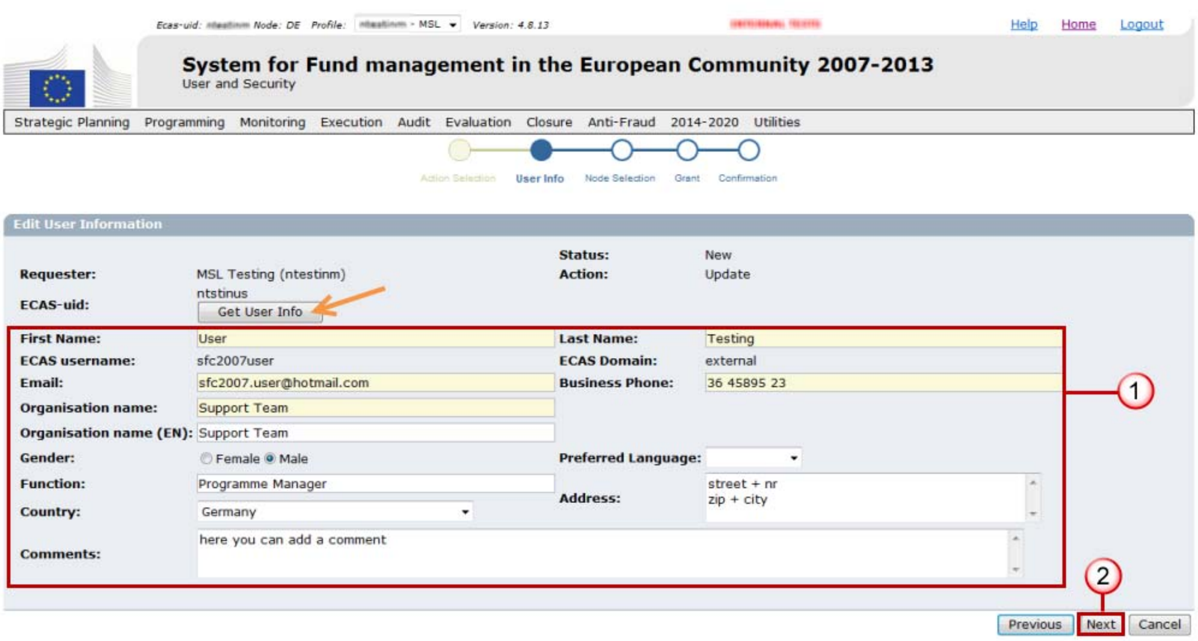
- First Name*
- Last Name*
- Email*
- Business Phone*
- Organisation name*
- Organisation name (EN)
- Gender
- Preferred language (for the notifications)
- Function (within the organisation)
- Country
- Address
- Comments

IMPORTANT	The following fields cannot be modified: ▪ ECAS-uid

	▪ ECAS username ▪ ECAS Domain

Step by step…

6. Modify the requested information if necessary①.
7. Click **NEXT** to continue②.



- You can click on the button **GET USER INFO** to retrieve the details available in ECAS for this user. The following information will be retrieved from ECAS: First name, Last name, Email, Business Phone, Organisation name. Please note that if the fields are blank in ECAS, the current information in SFC2007 will be overwritten. If this occurs you should first contact the user and request to them to update their information in their ECAS account.
- You can click **PREVIOUS** to go back to the previous step or click **CANCEL** to cancel the creation of the whole request. Click **RESET** to clear the information entered in the fields.

2.2.3. Modify nodes (only for multi-node countries)

IMPORTANT	This step is only available for the MS liaison (deputy) from countries having a multi-node structure (Examples: Germany, Italy, France, Spain…). For countries with a single node structure (Examples: Czech Republic, Portugal, Sweden…) this step is skipped by the wizard! You can continue to chapter 2.2.4.

You can modify the nodes the user will have access to. In case you only want to modify roles and permissions, you can skip this step by clicking **NEXT**.

Step by step…

8. On the select nodes window, select the node from the left pane (**AVAILABLE NODES**)①.

9. Click the right-arrow button [>] in the middle of the panes②.
10. The node is added to the pane in the right (**GRANT ACCESS TO NODE(S)**)③. To remove a node select the node on the right pane and click on the left-arrow button [<].
11. Repeat these steps for each node you want to select.
12. When finished, click **NEXT** to go to the next step④.

TIP	To select all nodes in the list, click on the double right-arrow button [>>]. To deselect all the nodes selected in the right pane, click the double left-arrow button [<<].

2.2.4. Modify the user's roles and permissions

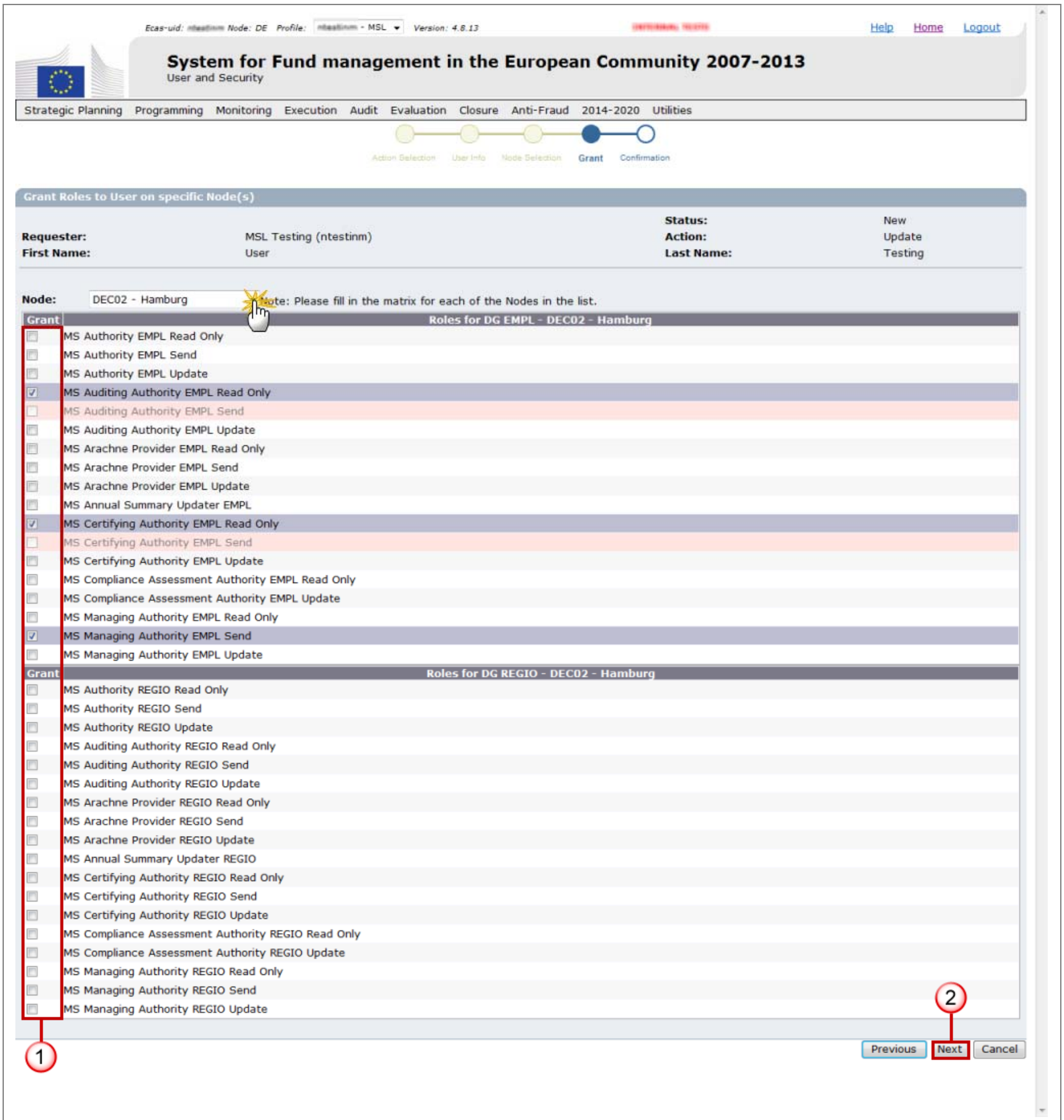
You can modify the roles and permissions for the user or you can skip this step by clicking **NEXT**.

The **GRANT ROLES TO USER ON SPECIFIC NODE(S)** screen appears. You can check additional roles or you can uncheck roles that are no longer needed.

If you manage several nodes and you have selected more than 1 node for the user in the previous screen you will have to grant roles and permissions for each node separately and thus select each of the nodes first.

Step by step…

13. Tick the boxes to select the additional roles and permissions you want to grant or uncheck the boxes of the roles that are no longer needed①.
14. Click **NEXT** to get to the final step (sending the request to the Commission)②.



- You can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

IMPORTANT	Please note that the MS Managing Authority Send role includes Update access unlike the MS Certifying Authority and MS Audit Authority roles where users having the Send role can't Update!

2.2.5. Send the request to the SFC2007 Support team

After modifying the User Information, nodes, roles and permissions to grant, you are ready to send the request to the SFC2007 Support team.

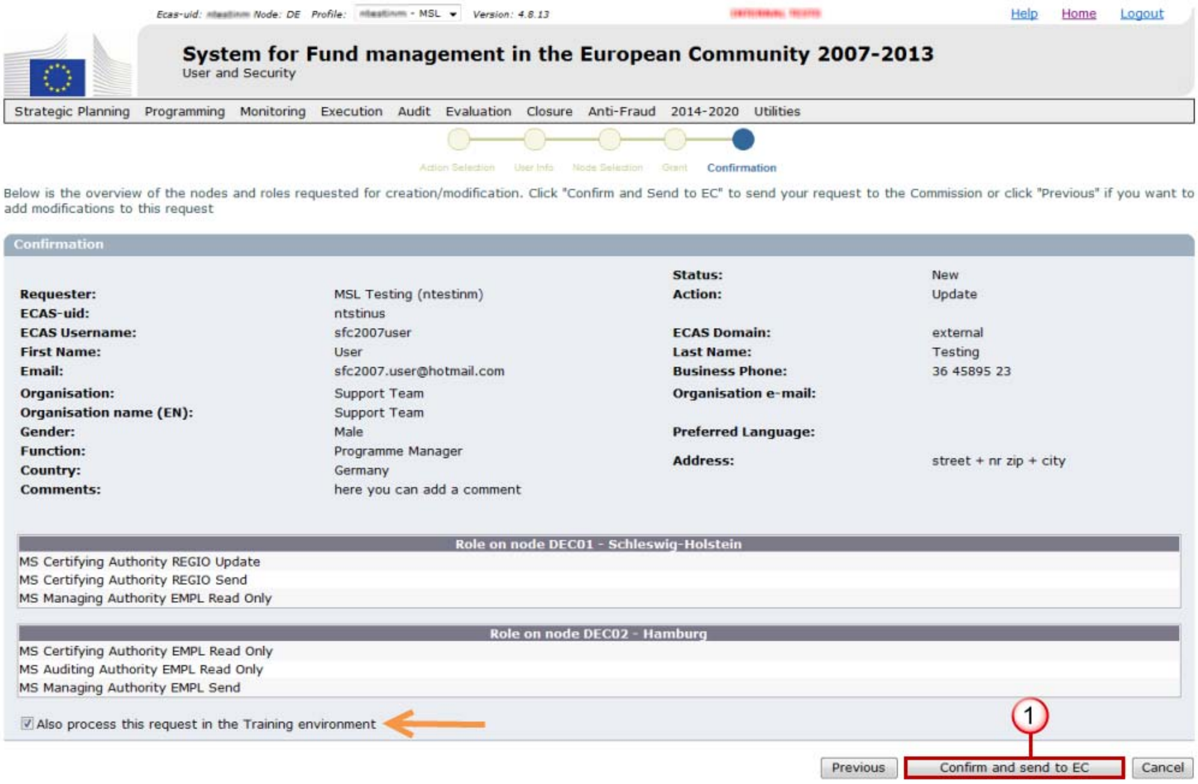
The overview of your request is shown. You see:

- The user information you entered.
- The roles and permissions you selected to be granted for the selected nodes.
- Before sending the request you can click **PREVIOUS** to go back to the previous step or click **CANCEL** to cancel the creation of the whole request.

Step by step…

15. Only for the **PRODUCTION** environment: The option "Also process this request in the Training environment" is checked. Leave it checked if you want the request to be automatically processed in the training environment too. You can uncheck this option if you want the request only to be processed in production environment (and not in training).

16. Click the button **CONFIRM AND SEND TO EC** to send the request to the SFC2007 Support team①.



Once the request is sent, you are redirected to the list of requests. Your request is given a unique identifier number (**ID**). The status of the request is **SENT.**

The request can now be processed by the SFC2007 Support team. If there are mistakes or other issues, the request is returned to you by the SFC2007 Support team.

2.2.6. If the request is processed…

If the request is processed, the status becomes **PROCESSED** and two automatic e-mails are sent:

- One e-mail to the **MS liaison or MS liaison Deputy** who created the request containing:
  - A link with the request identifier (**ID**) to view the processed request.
- One mail to the **concerned user** containing:
  - The updated access information.

2.2.7. If the request is returned (not processed)…

If the Support team detects problems or missing information the status becomes RETURNED and one e-mail is sent to the MS liaison or MS liaison Deputy with an explanation on the reason for returning.

The MS liaison (deputy) can:

- Correct the request and send it again (see 2.9) or
- Cancel the request (see 2.10)

2.3. Create a request for granting access to a web user managed by another MS liaison

You can grant roles and permissions to a user that exists already but is managed by another MS liaison and has roles and permissions on other nodes different than the ones you manage. This is very useful for users dealing with Cross-border programmes or for users of countries having different MS liaisons for each Fund, region or community.

Examples: Belgium (different MS liaison (and deputies) for regions and communities), Germany (different MS liaison (and deputies) for fund) etc…

When you grant access to a user, SFC2007 creates a "profile" for this user. The user can then choose between the profiles he has (one profile per node).

BEFORE YOU START	Ensure that you have all necessary information about the user. The request must be created and sent in a single operation.

Workflow

Select the type of request	⇒	Select nodes*	⇒	Grant roles and permissions	⇒	Send the request	⇒	Request is Processed, Returned or Cancelled

* only for multi-node countries

2.3.1. Select the type of request you want to create

Step by step…

1. On the menu UTILITIES > ACCESS REQUESTS click the **Create a New Access Request** link.
2. The wizard appears. Select the action GRANT ACCESS TO AN EXISTING WEB-USER MANAGED BY ANOTHER MEMBER STATE LIAISON①.
3. On the blank field that appears next to the selected type of request, you can enter the **last name**, **ECAS-uid** or the **e-mail** address of the user you want to grant access to on the nodes you manage.
4. The user appears in the list, so you can select it②.
5. After selecting the user, click NEXT③.

INFO	As this user is managed by another MS liaison, you cannot modify her/his user information. This step is therefore skipped by the wizard.

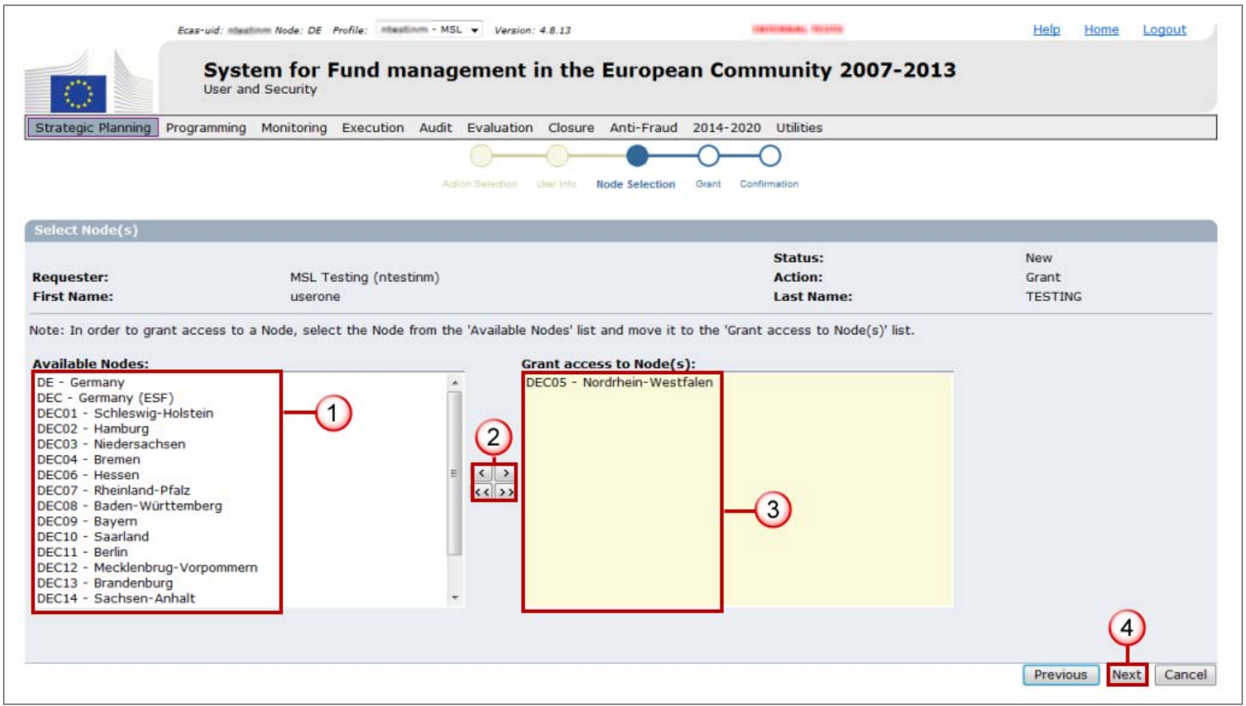
2.3.2. Chose nodes (only for multi-node countries)

IMPORTANT	This step is only available for the MS liaison (deputy) from countries having a multi-node structure (Examples: Germany, Italy, France, Spain…). For countries with a single node structure (Examples: Czech Republic, Portugal, Sweden…) this step is skipped by the wizard! You can continue to chapter 2.3.3.

You must define the nodes the user will have access to. As there are different nodes within your country, the user probably needs only access to one or some of them, so you must specify this.

Step by step…

6. On the select nodes window, select the node from the left pane (**AVAILABLE NODES**)1.
7. Click the right-arrow button in the middle of the panes2.
8. The node is added to the pane in the right (**GRANT ACCESS TO NODE(S)**)3.
9. Repeat these steps for each node you want to select.
10. When finished, click **NEXT** to go to the next step4.



TIP	To select all nodes in the list, click on the double right-arrow button >>. To deselect all the nodes selected in the right pane, click the double left-arrow button <<.

2.3.3. Grant roles and permissions

The **GRANTS ROLES TO USER ON SPECIFIC NODE(S)** screen appears. On this screen you can select the roles and permissions you want to grant for this user on the nodes you manage (the nodes you selected in the previous step).

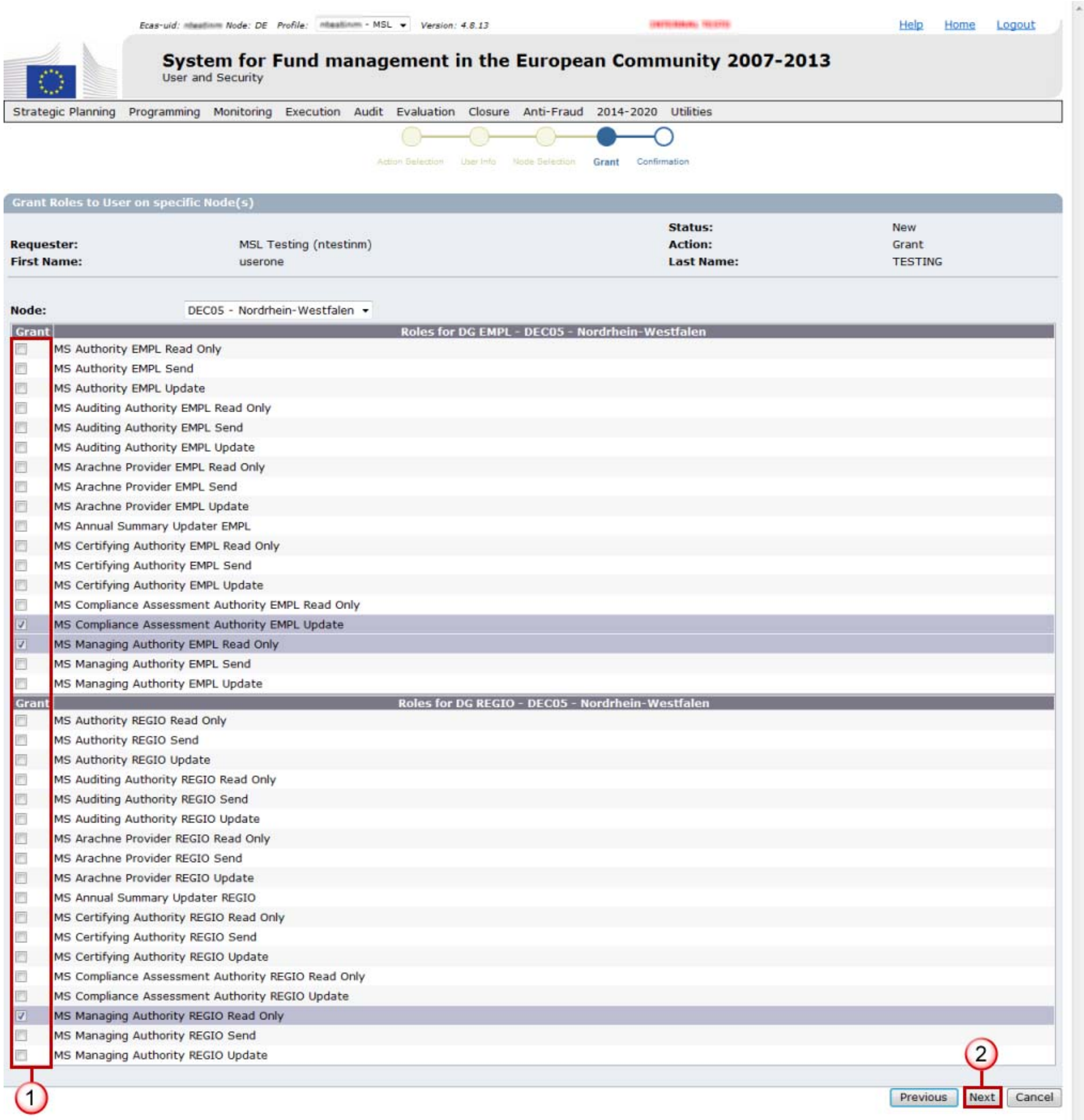
Step by step…

11. If you are dealing with a **multi-node** country, you first must select each of the nodes you chose in the previous step (choose nodes).

If you are dealing with a **single-node** country, the node is automatically displayed.

12. Tick the boxes to select the roles and permissions you want to grant 1. The incompatible roles will be marked in grey automatically by the system.

13. Click NEXT to get to the final step (reviewing and sending the request to the Commission)2.



- You can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

IMPORTANT	Please note that the MS Managing Authority Send role includes Update access unlike the MS Certifying Authority and MS Audit Authority roles where users having the Send role can't Update!

2.3.4. Send the request to the SFC2007 Support team

After having selected the nodes and the roles and permissions to grant, you are ready to send the request to the SFC2007 Support team.

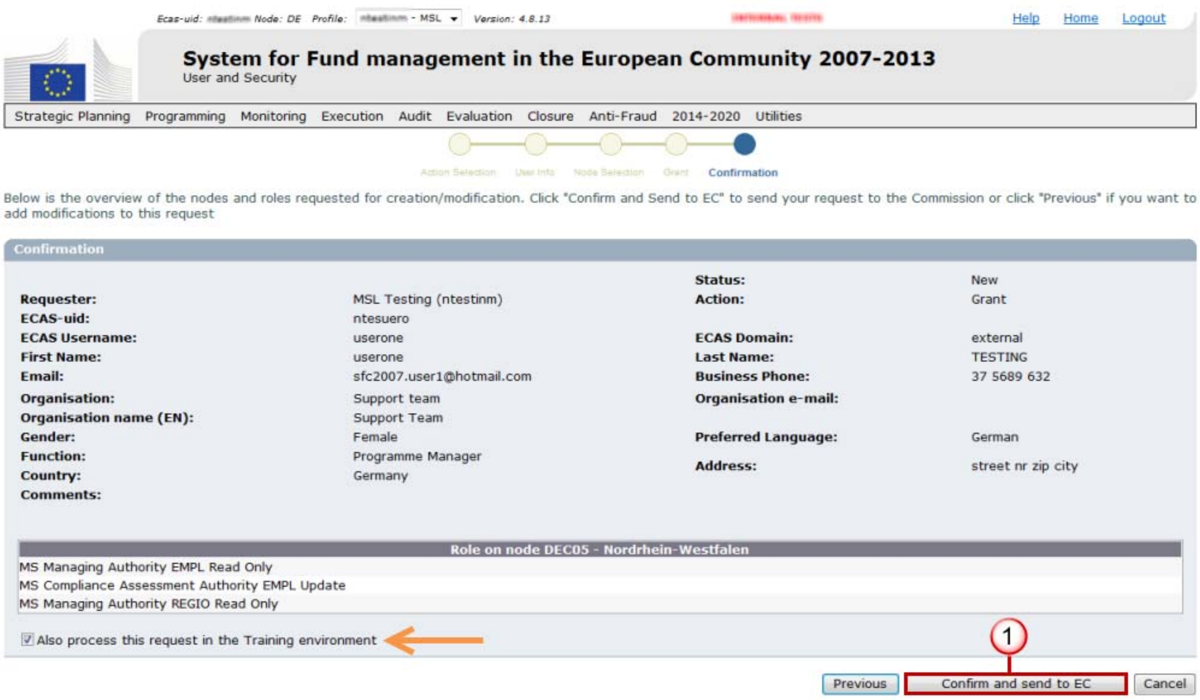
The overview of your request is shown. You see:

- The user information.
- The roles and permissions you selected to be granted for the selected nodes.
- Before sending the request you can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

Step by step…

14. Only for the PRODUCTION environment: The option "Also process this request in the Training environment" is checked. Leave it checked if you want the request to be automatically processed in the training environment too. You can uncheck this option if you want the request only to be processed in production environment (and not in training).

15. Click the button CONFIRM AND SEND TO EC to send the request to the SFC2007 Support team 1.



Once the request is sent, you are redirected to the list of requests. Your request is given a unique identifier number (ID). The status of the request is SENT.

The request can now be processed by the SFC2007 Support team. If there are mistakes or other issues, the request is returned to you by the SFC2007 Support team.

2.3.5. If the request is processed…

If the request is processed, the status becomes PROCESSED and two automatic e-mails are sent:

- One e-mail to the **MS liaison or MS liaison Deputy** who created the request containing:
  - o A link with the request identifier (ID) to view the processed request.
- One mail to the **concerned user** containing:
  - o The existing roles and permissions (the ones the user had already from the other MS liaison) and the roles and permissions granted by you on your node (s). For each node, there will be a profile the user can choose when connected to SFC2007.

2.3.6. If the request is returned (not processed)…

If the Support team detects problems or missing information, the status becomes RETURNED and one e-mail is sent to the MS liaison or MS liaison Deputy with an explanation on the reason for returning.

The MS liaison (deputy) can:

- Correct the request and send it again (see 2.9) or
- Cancel the request (see 2.10)

2.4. Create a request for disabling a web user

When a user no longer needs access to SFC2007 the MS liaison (and deputies) can create a request to disable (deactivate) the user.

Workflow

Select the type of request	⇒	Send the request	⇒	Request is Processed, Returned or Cancelled

IMPORTANT	If you request for disabling a user that has roles and permissions granted by another MS liaison, the USM will simply deactivate the user profile corresponding to the nodes, roles and permissions you manage. However, the user remains active for the other MS liaison (deputy) who deals with the user. The user only becomes totally inactive when ALL MS liaisons dealing with this user have requested the deactivation of the user.

2.4.1. Select the type of request you want to create

Step by step…

1. On the menu UTILITIES > ACCESS REQUESTS click the **Create a New Access Request** link.
2. The wizard appears. Select the action DISABLE EXISTING ACCOUNT FOR WEB USER 1.
3. On the blank field that appears next to the selected type of request, you can enter the **last name**, **ECAS-uid** or the **e-mail** address of the user you want to update.
4. The user appears in the list, so you can select it 2.
5. After selecting the user, click NEXT 3.

INFO	As this user will be completely deactivated, it is not necessary to modify or remove the User information or the Roles and Permissions. These steps are therefore skipped by the wizard.

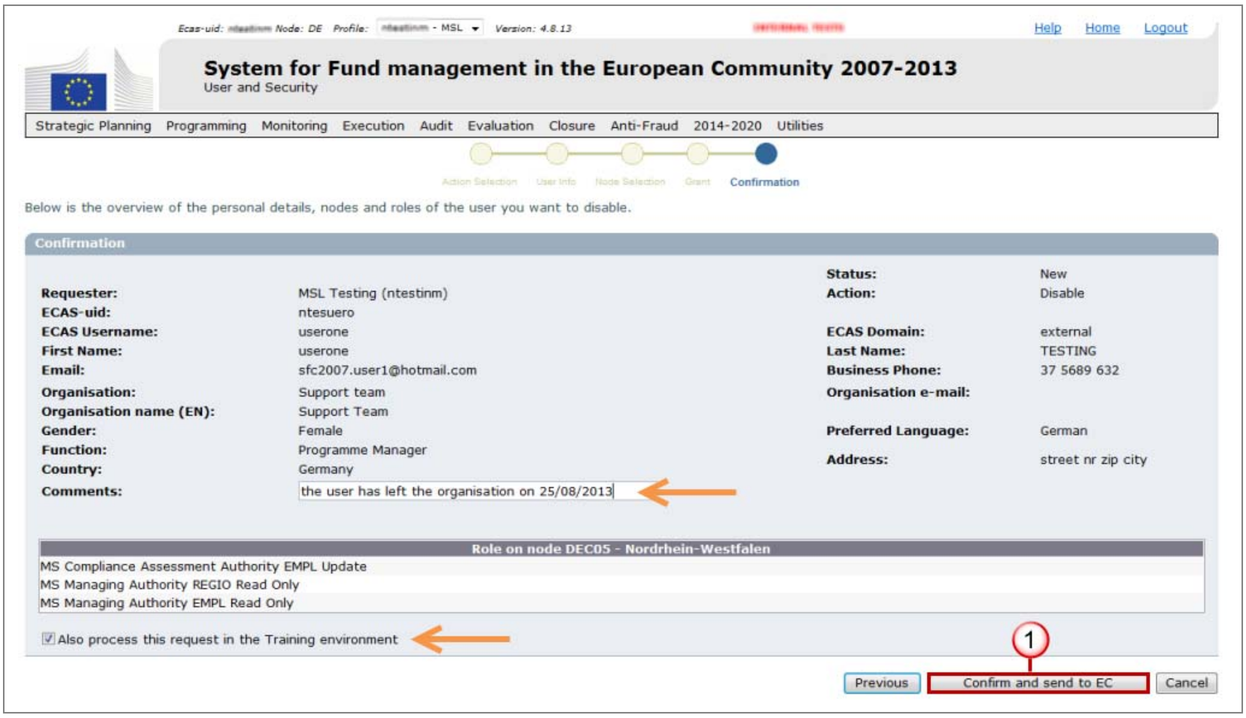
2.4.2. Send the request to the SFC2007 support team

The overview of your request is shown. You see:

- The user information and the nodes, roles and permissions the user had.
- You can add comment in the 'Comments' field.
- Before sending the request you can click **PREVIOUS** to go back to the previous step or click **CANCEL** to cancel the creation of the whole request.

Step by step…

6. Only for the **PRODUCTION** environment: The option "Also process this request in the Training environment" is checked. Leave it checked if you want the request to be automatically processed in the training environment too. You can uncheck this option if you want the request only to be processed in production environment (and not in training).
7. Click the button **CONFIRM AND SEND TO EC** to send the request to the SFC2007 Support team 1.



Once the request is sent, you are redirected to the list of requests. Your request is given a unique identifier number (ID). The status of the request is SENT.

The request can now be processed by the SFC2007 Support team. If there are mistakes or other issues, the request is returned to you by the SFC2007 Support team.

2.4.3. If the request is processed…

If the request is processed, the status becomes PROCESSED and one e-mail is sent to the **MS liaison or MS liaison Deputy** informing that the request has been processed successfully. No e-mail is sent to the user (as the user no longer needs the account, the USM assumes the user doesn't expect to be notified).

2.4.4. If the request is returned (not processed)…

If the Support team detects problems or missing information the status becomes RETURNED and one e-mail is sent to the MS liaison (deputy) with an explanation on the reason for returning.

The MS liaison (deputy) can:

- Correct the request and send it again (see 2.9) or
- Cancel the request (see 2.10)

2.5. Create a request for a new certificate

IMPORTANT	A **certificate** user account enables local information systems to authenticate when communicating with SFC2007 through **web-services**. Requests for certificate user accounts should only be created by countries using the web-services! Unlike the web user accounts that access the application SFC2007 with a nominative ECAS user account, certificate user accounts remain generic user accounts starting

	with **w005**…

You can request the creation of a new certificate when no certificate exists for the purposes you need to (i.e. currently no other certificate exists for the same fund, node and with the same roles and permissions as the one you want to request for).

- If a certificate exists but has expired, you can create a request to **RENEW CERTIFICATE** (see chapter 2.7).
- If the certificate exists but there are changes on the information of the user linked to the certificate or in the IT contact person, you can request to **UPDATE EXISTING ACCOUNT FOR CERTIFICATE** (see chapter 2.6).

BEFORE YOU START	Ensure that you have all necessary information about the certificate, the user linked to the certificate and the IT contact person. Ensure that you have the .csr file[2] ready as you will need to upload the file in the USM. The request must be created and sent in a single operation!

Workflow

Select the type of request	⇒	Enter information about the user, the person of contact and the certificate (csr file)	⇒	Select nodes*	⇒	Grant roles and permissions	⇒	Send the request	⇒	Request is Processed, Returned or Cancelled

* only for multi-node countries

2.5.1. Select the type of request you want to create

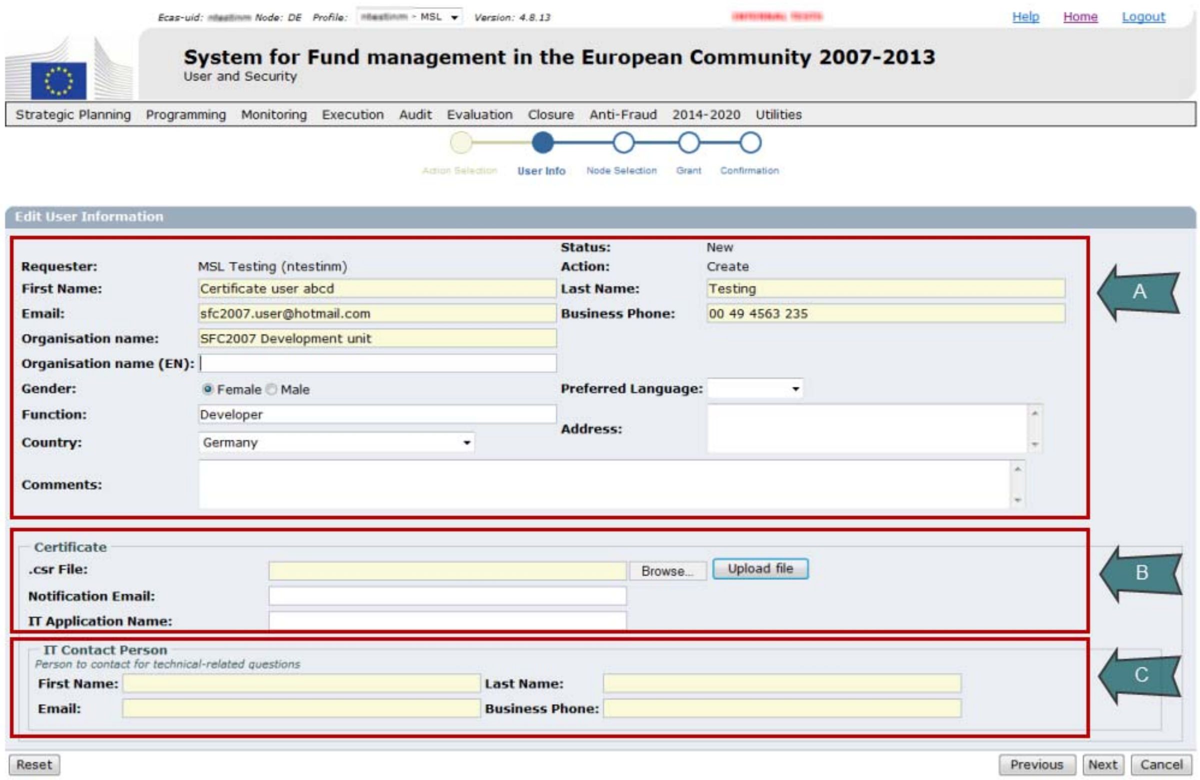
Step by step…
1. On the menu **UTILITIES** > **ACCESS REQUESTS** click the **Create a New Access Request** link. 2. The wizard appears. Select the action **CREATE NEW ACCOUNT FOR CERTIFICATE** 1. 3. Click **NEXT** 2.

[2] When requesting the creation of a new certificate, the MS liaison (deputy) must upload a Certificate Signing Request file (.csr). This file must be prepared in advance so it can be uploaded into the USM when creating the request. For more information on how the IT teams can create the csr file, please refer to the procedure "PM-103-Access Control Management" available in the Library of the SFC2007 Interest Group on CIRCABC: https://circabc.europa.eu/w/browse/3b3d67b0-7309-40f2-a1b4-b68a2f040a09

2.5.2. Enter the information on the user linked to the certificate

The Edit User Information screen appears. This screen contains three sections:

- **A. User information** (the user linked to the certificate).
- **B. Certificate** (the .csr file, the local IT application name and the notification e-mail).
- **C. IT Contact Person** (Person to contact for technical-related questions).



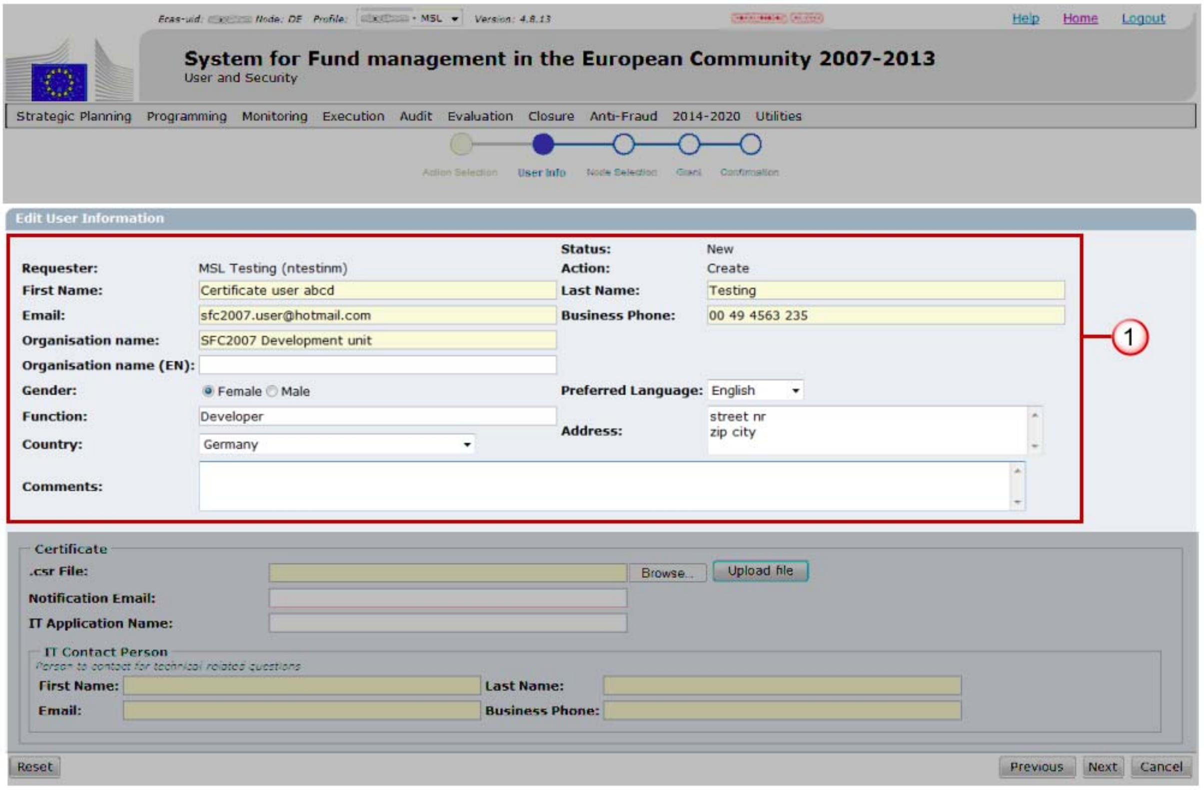
On the **User information section** (A) the following information must be entered. Fields marked with an asterisk (*) are mandatory:

- First Name*
- Last Name*
- Email*
- Business Phone*
- Organisation name*
- Organisation name (EN)
- Gender
- Preferred Language (for the notifications)
- Function
- Country
- Address
- Comments

TIP	Start typing the first letters of the Organisation name. If the organisation has already been entered before in the system, the full name will be displayed in a list where you can select it from.

Step by step…

4. Enter the requested information 1.



IMPORTANT	When a certificate request is processed, the CN Name of the certificate (CN) is added to the user's last name: this allows easy identification of users (persons) and users linked to certificates!

2.5.3. Upload the .csr file

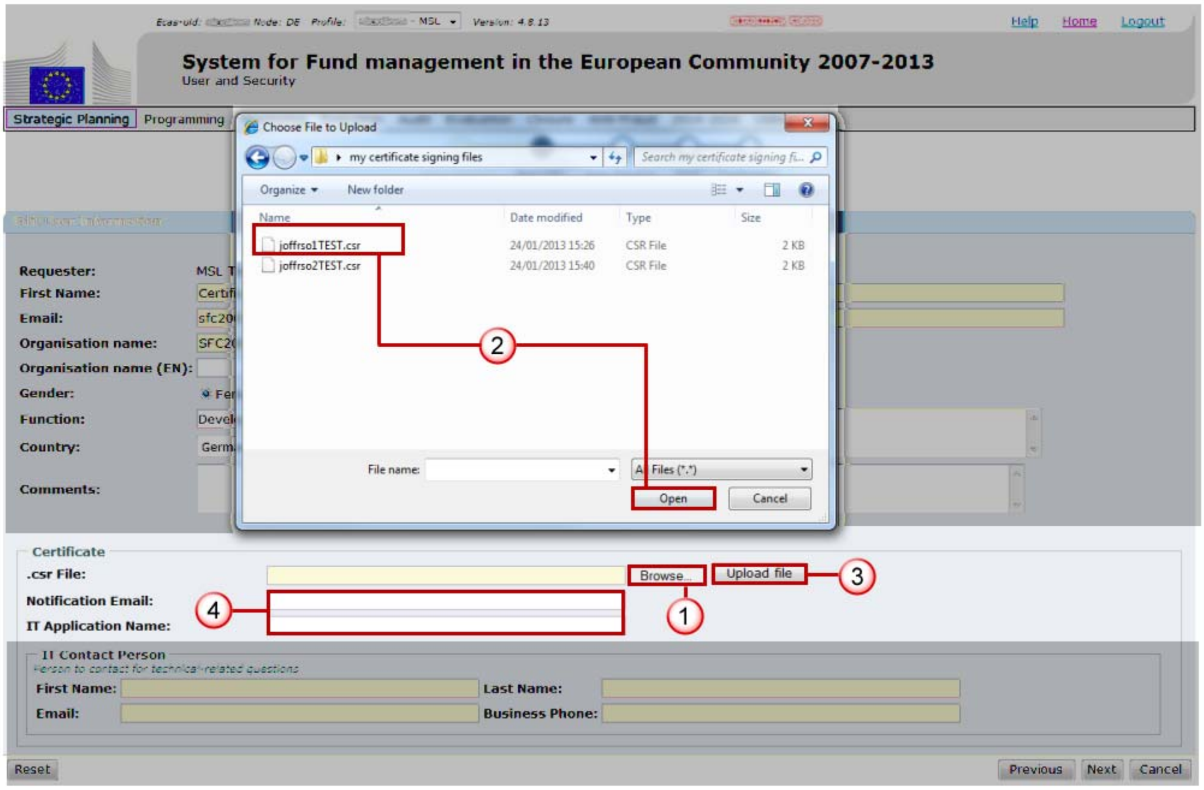
For more information on how the IT teams can create the csr file, please refer to the procedure "PM-103-Access Control Management" available in the Library of the SFC2007 Interest Group on CIRCABC: https://circabc.europa.eu/w/browse/3b3d67b0-7309-40f2-a1b4-b68a2f040a09

When the .csr file is uploaded, SFC2007 verifies the correctness of the file and reads the Distinguished Name of the certificate (**DN**). The DN is the information related to the certificate.

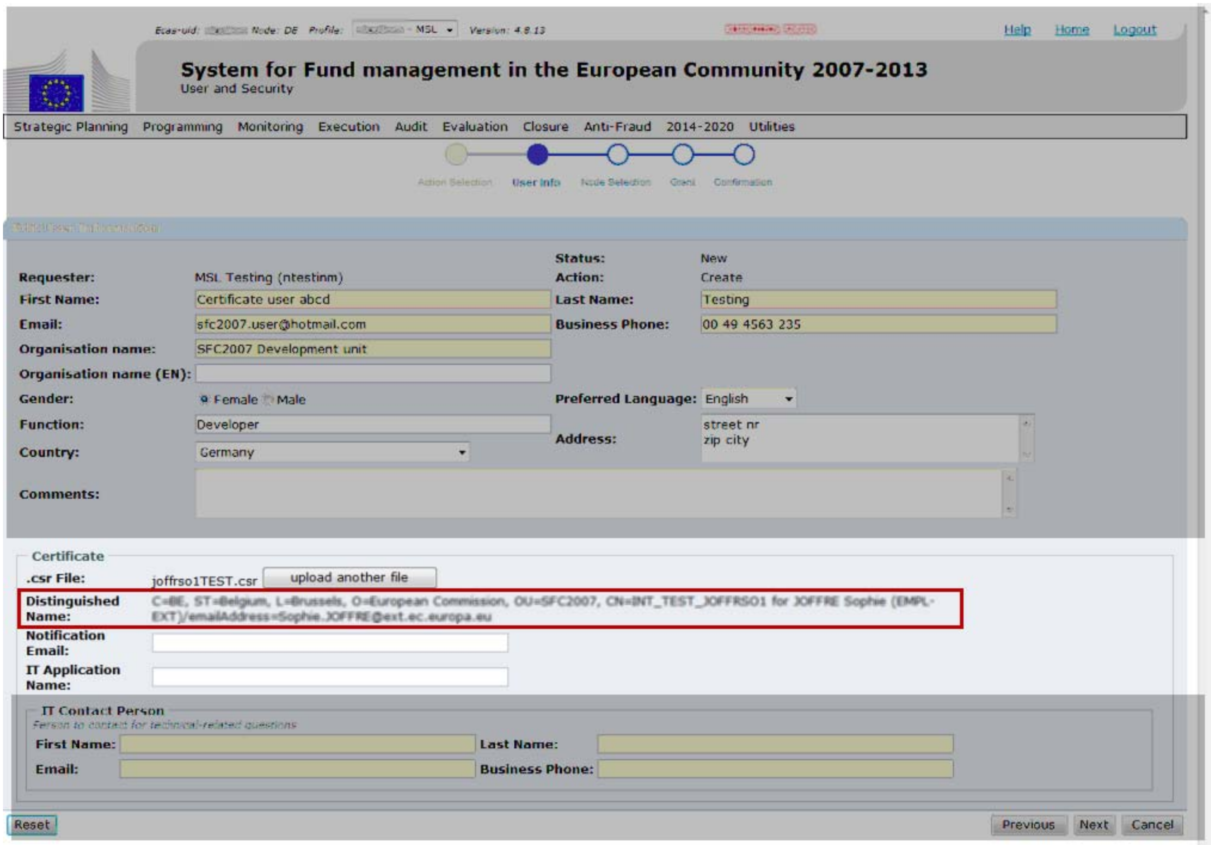
IMPORTANT	There's a validation rule on the CN string: For BETA environment, the CN string should contain 'BETA' (case sensitive). For example CN=SFC_EAFRD_Axel Baum_DEA03_BETA_01. For ACCEPTANCE environment, the CN string should contain 'TEST' (case sensitive). For example: CN=IT19_ERDF_MSMA_TEST1. An error message will be raised if for example the CN string contains TEST at the end for PRODUCTION environment and the requester won't be able to submit a request in ACCEPTANCE environment if the CN string does not contain the word 'TEST'.

Additionally, it is recommended to indicate the Notification E-mail address (if the notifications related to operations made with this certificate are to be sent to a different address than the Email address of the user linked to the certificate, see chapter 2.5.2).

Step by step…
5. On the certificate section, click the **BROWSE** button to search for the .csr file(1). 6. Search for the file in your computer, select the file and click **OPEN**(2). 7. When the file is selected, click on the **UPLOAD FILE** button(3). 8. Enter the remaining information (**NOTIFICATION EMAIL ADDRESS** and **IT APPLICATION NAME**)(4).



9. When the file is uploaded the **Distinguished Name** of the certificate (**DN**) is displayed.



2.5.4. Enter the information on the IT contact person

The IT contact person is the person who deals with technical issues linked to the certificate or the web-services.

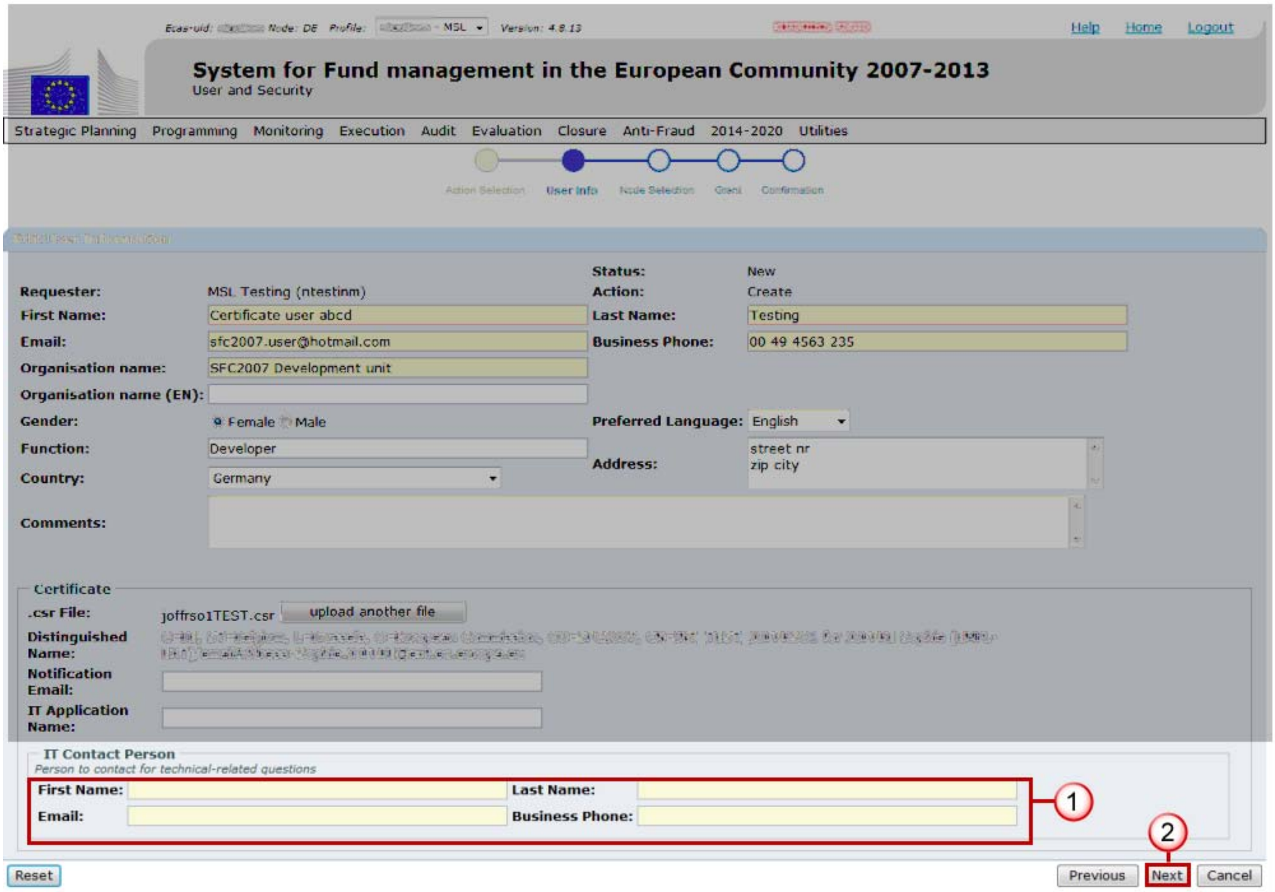
Entering this information is mandatory in order to ensure that there is a contact person for any exchange of information with the SFC2007 Support team.

The information to be completed is the following. All fields are mandatory!!!

- First Name*
- Last name*
- Email*
- Business Phone*

Step by step…

10. Enter the IT Contact information 1.
11. Click NEXT to go to the next step 2.



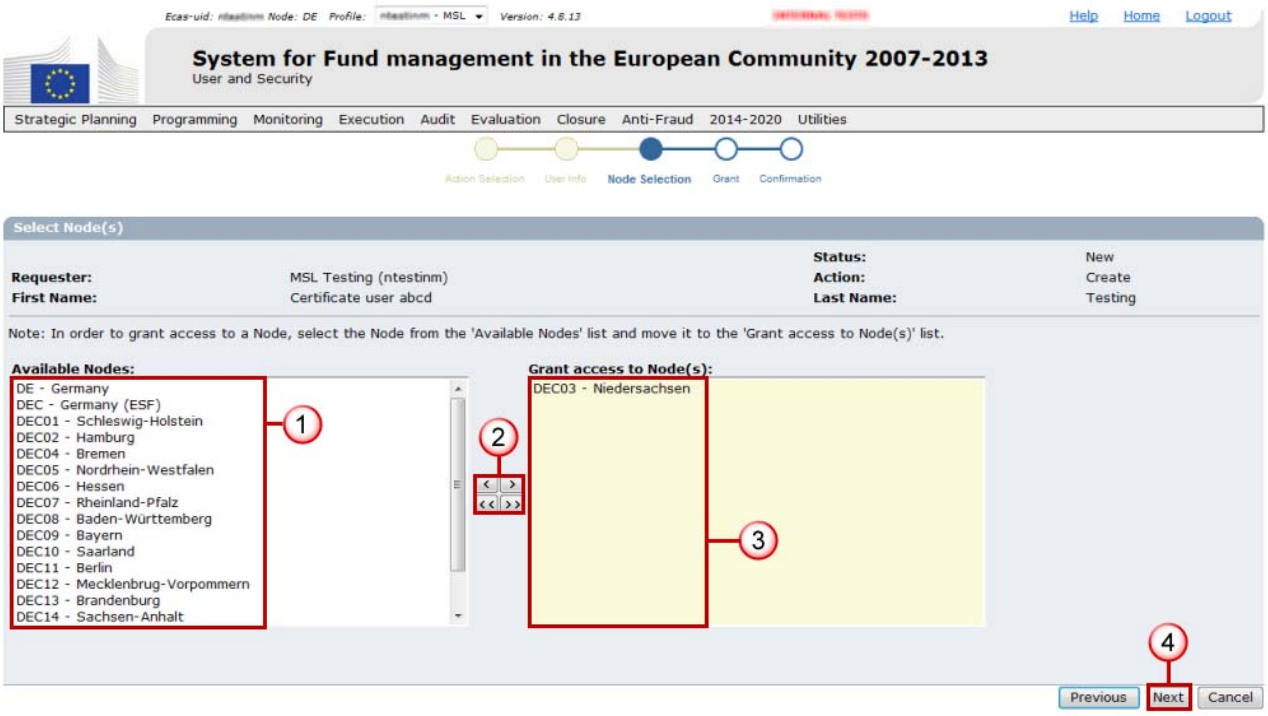
2.5.5. Choose nodes (only for multi-node countries)

IMPORTANT	This step is only available for the MS liaison (deputy) from countries having a multi-node structure (Examples: Germany, Italy, France, Spain…). You must define the node the user linked to the certificate will have access to. **Please note that unlike web users (persons), the certificates can only have access to one node!**

	For countries with a single node structure (Examples: Czech Republic, Portugal, Sweden…) this step is skipped by the wizard! You can continue to chapter 2.5.6.

Step by step…

12. On the select nodes window, select the node from the left pane (AVAILABLE NODES)①.
13. Click the right-arrow button in the middle of the panes②.
14. The node is added to the pane in the right (GRANT ACCESS TO NODE(S))③.
15. When finished, click NEXT to go to the next step④.



2.5.6. Grant roles and permissions

The GRANTS ROLES TO USER ON SPECIFIC NODE(S) screen appears. On this screen you can select the roles and permissions you want to grant for this certificate.

The roles and permissions shown correspond to the roles and permissions that the MS liaison (deputy) can request for as well as the Directorate General (according to Funds) for which the MS liaison (deputy) can request access.

- **EMPL**: ESF - IPA Component IV
- **REGIO**: ERDF - CF - IPA Component II and III
- **MARE**: EFF - IPA component
- **AGRI**: EAFRD - IPA Component V

The roles and permissions are created on the Node for which the MS liaison (deputy) can request.

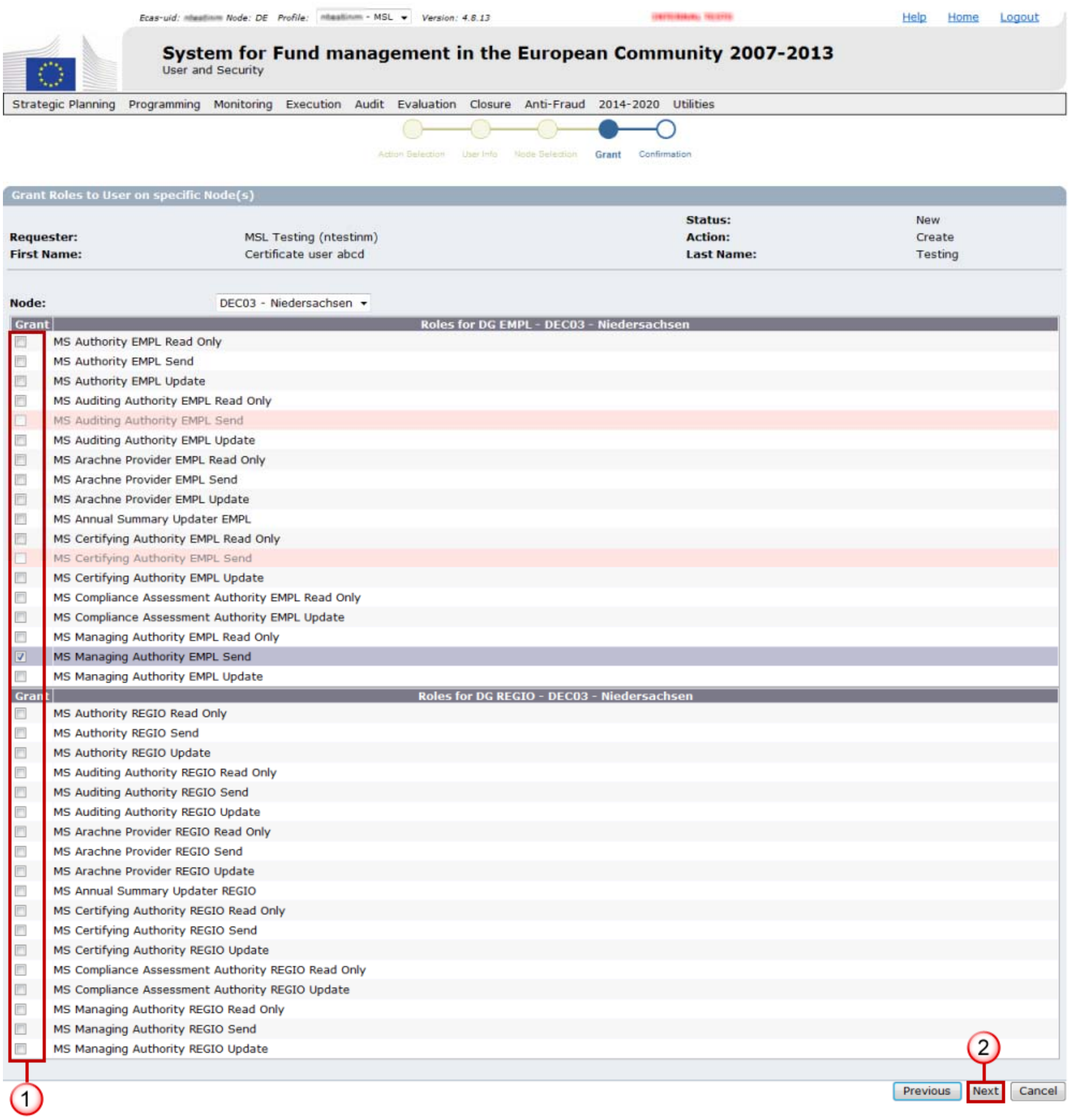
IMPORTANT	The USM automatically detects incompatible roles. The roles that are incompatible with the role you selected are greyed. You cannot select these.

	Example: You select "MS Auditing Authority EMPL Send". The roles "MS Authority EMPL Send", "MS Certifying Authority EMPL Send" and "MS Managing Authority EMPL Send" are greyed.

IMPORTANT	Please note that the MS Managing Authority Send role includes Update access unlike the MS Certifying Authority and MS Audit Authority roles where users having the Send role can't Update!

Step by step…

16. Tick the boxes to select the roles and permissions you want to grant 1.
17. Click NEXT to get to the final step (reviewing and sending the request to the Commission) 2.



- You can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

2.5.7. Send the request to the SFC2007 Support team

After entering the User Information, the certificate information, the IT contact details, the node and the roles and permissions to grant, you are ready to send the request to the SFC2007 Support team.

The overview of your request is shown. You see:

- The user information and the certificate information you entered.
- The roles and permissions you selected to be granted for the selected node.

- Before sending the request you can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

Step by step…

18. Click the button **CONFIRM AND SEND TO EC** to send the request to the SFC2007 Support team 1.

Once the request is sent, you are redirected to the list of requests. Your request is given a unique identifier number (ID). The status of the request is SENT.

The request can now be processed by the SFC2007 Support team. If there are mistakes or other issues, the request is returned to you by the SFC2007 Support team.

2.5.8. If the request is processed…

If the request is processed, the status becomes PROCESSED and two automatic e-mails are sent:

- One e-mail to the **MS liaison or MS liaison Deputy** who created the request containing:
  - A link with the request identifier (**ID**) to view the processed request and to **download the generated certificate**.
  - For BETA and ACCEPTANCE environments, the second half of the user's password is also sent, so this can be communicated to the user linked to the certificate. For PRODUCTION environment, this information is not sent because it is not required.
- One mail to the **user linked to the certificate** containing:
  - The username (w005…) of the account for the certificate

- o The roles and permissions granted and the node
- o For BETA and ACCEPTANCE environments, the first half of the password is sent. For PRODUCTION environment, this information is not sent because it is not required.

2.5.9. If the request is returned (not processed)…

If the Support team detects problems or missing information, or if the certificate account appears to exist already, the status becomes RETURNED and one e-mail is sent to the MS liaison or MS liaison Deputy with an explanation on the reason for returning.

The MS liaison (deputy) can:

- Correct the request and send it again (see 2.9) or
- Cancel the request (see 2.10)

2.6. Create a request to modify a certificate

You can request for a modification of a certificate when the details of the user linked to the certificate have changed, when the details of the IT contact person have changed or when you want to modify the node, roles or permissions.

- If your certificate has expired, you should create a request to RENEW CERTIFICATE (see chapter 2.7)

Workflow

Select the type of request	⇒	Modify information of the user and the certificate	⇒	Modify nodes*	⇒	Modify roles and permissions	⇒	Send the request	⇒	Request is Processed, Returned or Cancelled

* only for multi-node countries

2.6.1. Select the type of request you want to create

Step by step…
1. On the menu UTILITIES > ACCESS REQUESTS click the [Create a New Access Request](#) link. 2. The wizard appears. Select the action UPDATE EXISTING ACCOUNT FOR CERTIFICATE 1. 3. On the blank field that appears next to the selected type of request, you can enter the **last name**, **username** (w005…) or the **e-mail** address of the user linked to the certificate. You can also enter the **Common Name (CN name)**[3] of the certificate you want to modify. 4. The user linked to the certificate appears in the list, so you can select it 2. 5. After selecting the user, click NEXT 3.

[3] The Common Name (CN name) is part of the DN name (Distinguished Name) and starts with 'CN = '. For example CN name: 'CN=Lothman_ESF_DED02'.

2.6.2. Modify the information linked to the certificate

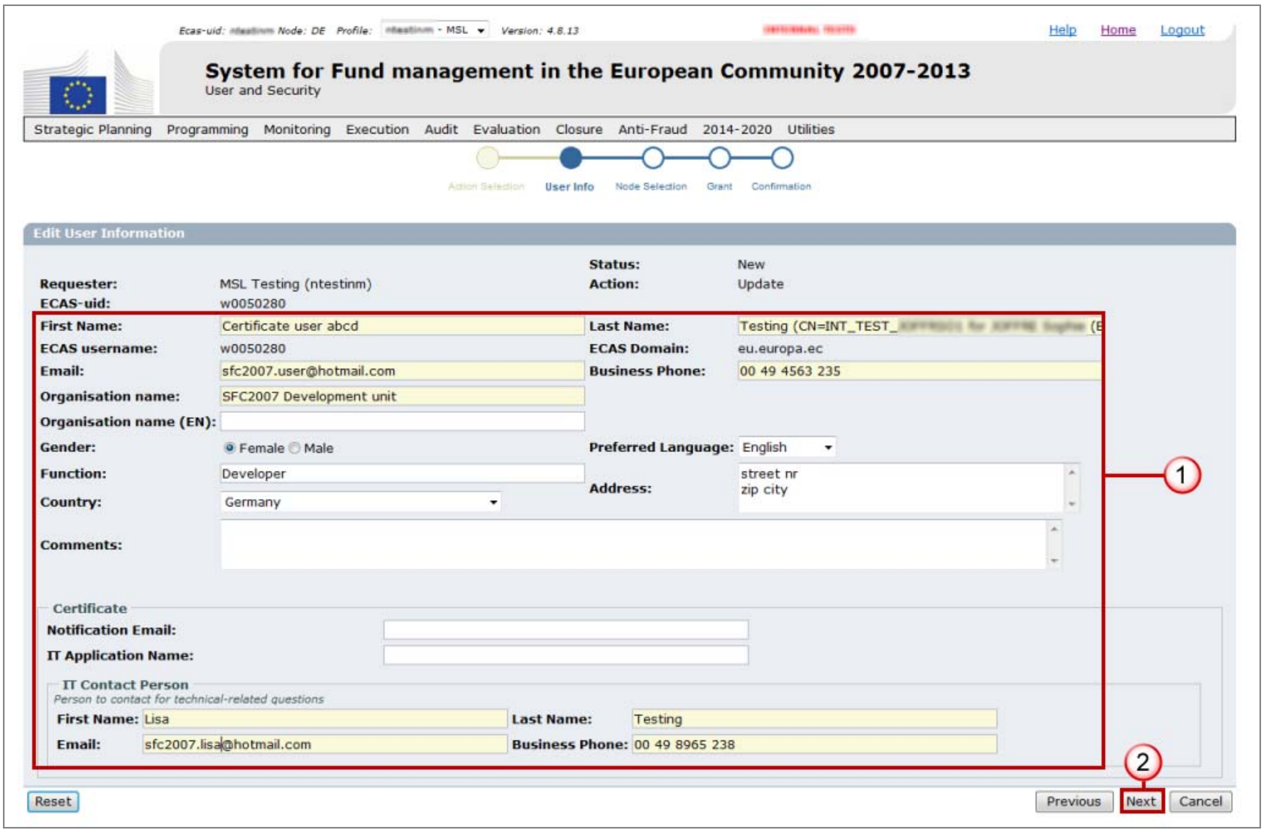
The Edit User Information screen appears. This screen contains three sections:

- **A. User information** (the user linked to the certificate).
- **B. Certificate** (the .csr file, the local IT application name and the notification e-mail).
- **C. IT Contact Person** (person to contact for technical-related questions).

You can modify the existing information. **You don't need to upload the csr file again**! The username (w005…) cannot be modified.

Important	When a certificate request is processed, the CN Name of the certificate (CN) is added to the user's last name: this allows easy identification of users (persons) and users linked to certificates!

Step by step…
6. Modify the requested information if necessary 1.   7. Click Next 2.



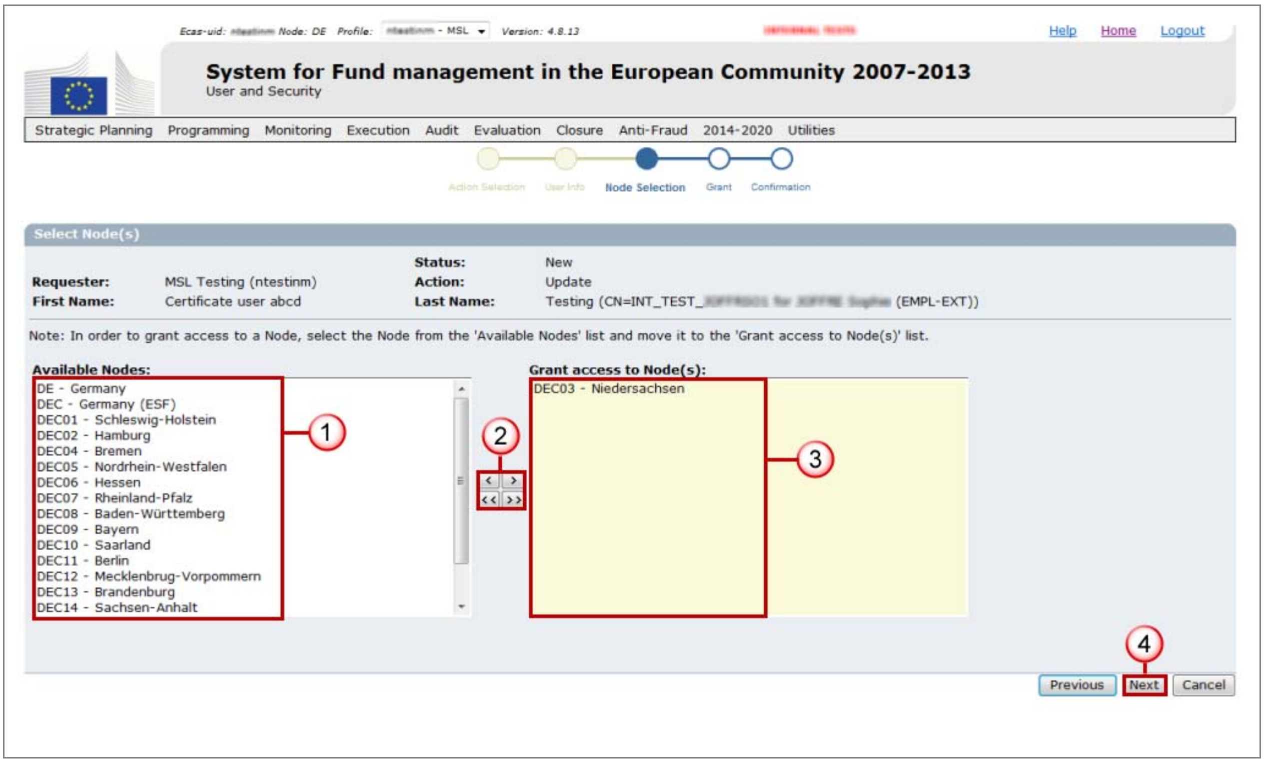
2.6.3. Modify the certificate node (only for multi-node countries)

IMPORTANT	This step is only available for the MS liaison (deputy) from countries having a multi-node structure (Examples: Germany, Italy, France, Spain…). For countries with a single node structure (Examples: Czech Republic, Portugal, Sweden) this step is skipped by the wizard! You can continue to chapter 2.6.4.

You can modify the node the user linked to the certificate will have access to. Please note that unlike web users (persons), the certificates can only have access to **one** node!

Step by step…

8. On the select nodes window, select the node form the left pane (AVAILABLE NODES)1.
9. Click the right-arrow button in the middle of the panes2.
10. The node is added to the pane in the right (GRANT ACCESS TO NODE(S))3.
11. To remove a node for which access is no longer required, select the node from the left pane and click the left-arrow button.
12. When finished, click NEXT to go to the next step4.



2.6.4. Grant roles and permissions

The GRANTS ROLES TO USER ON SPECIFIC NODE(S) screen appears. On this screen you can select the roles and permissions you want to grant for this certificate.

The roles and permissions shown correspond to the roles and permissions that the MS liaison (deputy) can request for as well as the Directorate General (according to Funds) for which the MS liaison (deputy) can request.

- **EMPL**: ESF - IPA Component IV
- **REGIO**: ERDF - CF - IPA Component II and III
- **MARE**: EFF - IPA component
- **AGRI**: EAFRD - IPA Component V

The roles and permissions are created on the Node for which the MS liaison (deputy) can request.

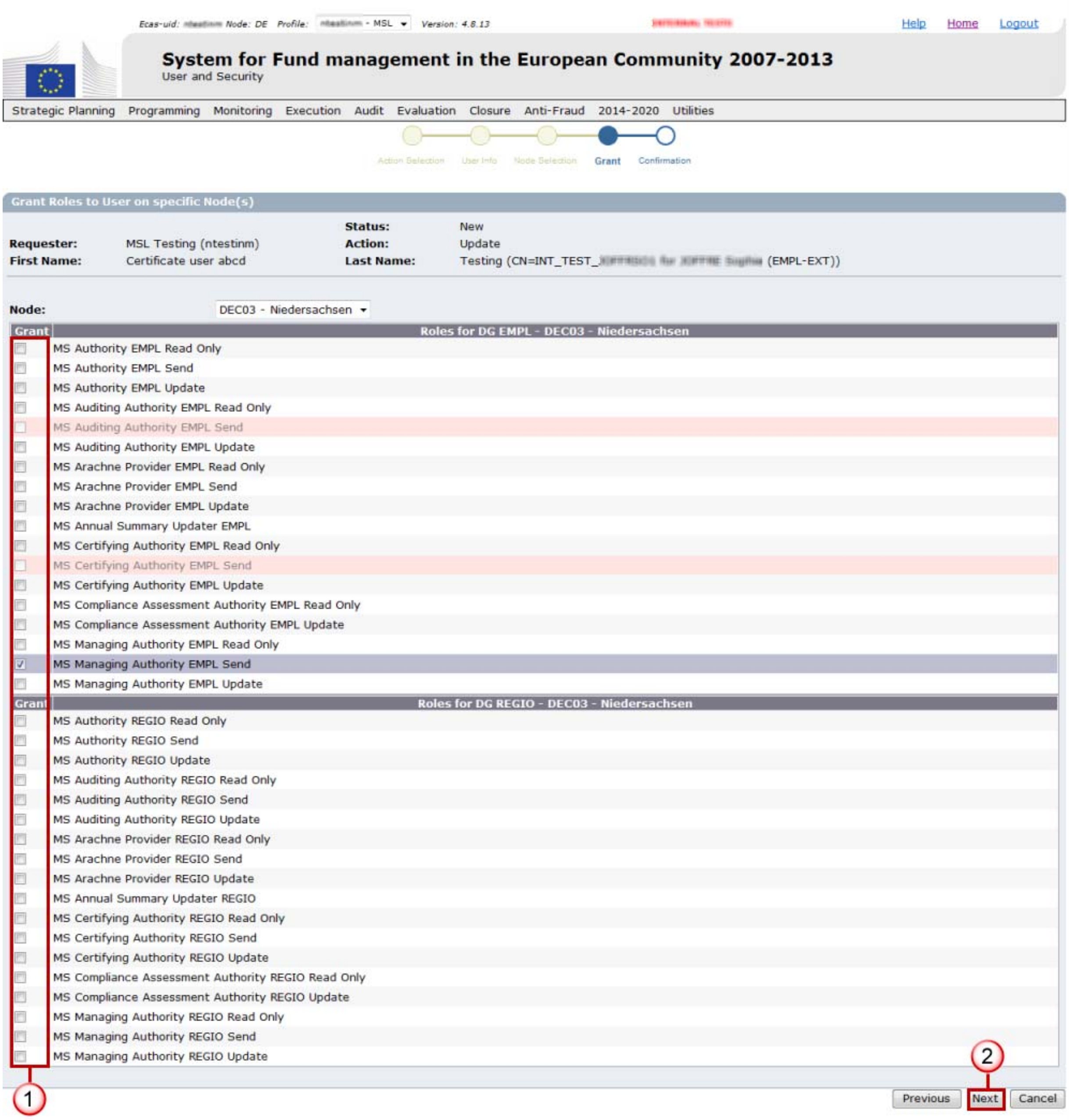
IMPORTANT	The USM automatically detects incompatible roles. The roles that are incompatible with the role you select are greyed. You cannot select these. **Example**: You select "MS Auditing Authority EMPL Send". The roles "MS Authority EMPL Send", "MS Certifying Authority EMPL Send" and "MS Managing Authority EMPL Send" are greyed.

IMPORTANT	Please note that the MS Managing Authority Send role includes Update access unlike the MS Certifying Authority and MS Audit Authority roles where users having the Send role can't Update!

Step by step…

13. Tick the boxes to select the roles and permissions you want to grant①.

14. Click NEXT to get to the final step (reviewing and sending the request to the Commission)②.



- You can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

2.6.5. Send the request to the SFC2007 Support team

After entering the User Information, the certificate information, the IT contact details, the node and the roles and permissions to grant, you are ready to send the request to the SFC2007 Support team.

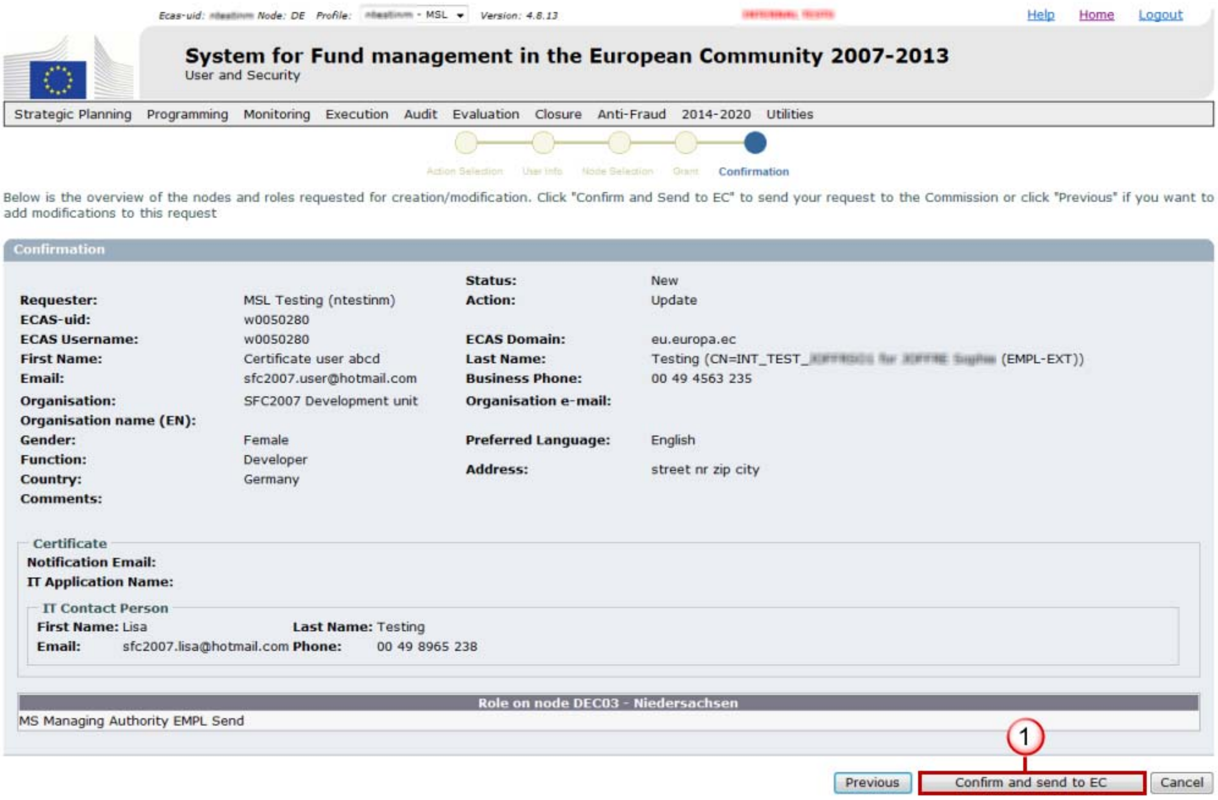
The overview of your request is shown. You see:

- The user information and the certificate information you entered.
- The roles and permissions you selected to be granted for the selected node.

- Before sending the request you can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

Step by step…

15. Click the button CONFIRM AND SEND TO EC to send the request to the SFC2007 Support team 1.



Once the request is sent, you are redirected to the list of requests. Your request is given a unique identifier number (ID). The status of the request is SENT.

The request can now be processed by the SFC2007 Support team. If there are mistakes or other issues, the request is returned to you by the SFC2007 Support team.

2.6.6. If the request is processed…

If the request is processed, the status becomes PROCESSED and two automatic e-mails are sent:

- One e-mail to the **MS liaison or MS liaison Deputy** who created the request containing:
    - A link with the request identifier (ID) to view the processed request.
- One mail to the **user linked to the certificate** containing:
    - The roles and permissions granted and the node.

2.6.7. If the request is returned (not processed)…

If the Support team detects problems or missing information, the status becomes RETURNED and one e-mail is sent to the MS liaison or MS liaison Deputy with an explanation on the reason for returning.

The MS liaison (deputy) can:

- Correct the request and send it again (see 2.9) or
- Cancel the request (see 2.10)

2.7. Create a request for renewal of a(n) (expired) certificate

You can request for a renewal of a certificate when the existing one is about to expire or is expired (the validity of a certificate is two years).

TIP	You can check the validity dates of a certificate via the menu **CONTACTS/USER ACCOUNTS** (please refer to section 3).

IMPORTANT	Please make sure to have the **new csr file**[4] available on your computer before you create the access request in SFC2007. You will have to upload this new csr file in the access request to renew the certificate even if the information in the csr file has not changed!

Workflow

Select the type of request	⇒	Modify information of the user and the certificate	⇒	Modify nodes*	⇒	Modify roles and permissions	⇒	Send the request	⇒	Request is Processed, Returned or Cancelled

* only for multi-node countries

2.7.1. Select the type of request you want to create

Step by step…

1. On the menu **UTILITIES** > **ACCESS REQUESTS** click the **Create a New Access Request** link.
2. The wizard appears. Select the action **RENEW CERTIFICATE** 1.
3. On the blank field that appears next to the selected type of request, you can enter the **last name**, **username** or the **e-mail** address of the user linked to the certificate. You can also enter the **Common Name (CN name)** of the certificate you want to renew 2.
4. The user linked to the certificate appears in the list, so you can select it.
5. After selecting the user, click **NEXT** 3.

[4] When requesting the creation of a new certificate, the MS liaison (deputy) must upload a Certificate Signing Request file (.csr). This file must be prepared in advance so it can be uploaded into the USM when creating the request. For more information on how the IT teams can create the csr file, please refer to the procedure "PM-103-Access Control Management" available in the Library of the SFC2007 Interest Group on CIRCABC: https://circabc.europa.eu/w/browse/3b3d67b0-7309-40f2-a1b4-b68a2f040a09

2.7.2. Modify the information on the user linked to the certificate

Please refer to instructions in chapter 2.5.2

2.7.3. Upload the new csr file and modify the certificate information

Please refer to instructions in chapter 2.5.3. Uploading the .csr file is mandatory.

2.7.4. Modify the IT Contact person details

Please refer to instructions in chapter 2.5.4

2.7.5. Modify the certificate node (only for multi-node countries)

IMPORTANT	This step is only available for MS liaisons from countries having a multi-node structure (Examples: Germany, Italy, France, Spain…). You must define the node the user linked to the certificate will have access to. **Please note that unlike web users (persons), the certificates can only have access to one node!** For countries with a single node structure (Examples: Czech Republic, Portugal, Sweden…) this step is skipped by the wizard! You can continue to chapter 2.7.6.

2.7.6. Grant roles and permissions

Please refer to instructions in chapter 2.5.6

2.7.7. Send the request to the SFC2007 Support team

After entering the User Information and the roles and permissions to grant, you are ready to send the request to the SFC2007 Support team.

The overview of your request is shown. You see:

- The user information and the certificate information you entered.
- The roles and permissions you selected to be granted for the selected node.

- Before sending the request you can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

2.7.8. If the request is processed…

If the request is processed, the status becomes PROCESSED and two automatic e-mails are sent:

- One e-mail to the **MS liaison or MS liaison Deputy** who created the request containing a link with the request identifier (**ID**) to view the processed request and to **download the generated certificate**.
- One mail to the **user linked to the certificate** to notify that the certificate has been renewed and the renewed certificate will be transmitted by the MS liaison or MS liaison Deputy.

2.7.9. If the request is returned (not processed)…

If the Support team detects problems or missing information, the status becomes RETURNED and one e-mail is sent to the MS liaison (deputy) with an explanation on the reason for returning.

The MS liaison (deputy) can:

- Correct the request and send it again (see 2.9) or
- Cancel the request (see 2.10)

2.8. Create a request for disabling a certificate

When a certificate is no longer needed, the MS liaison (and deputies) can create a request to disable (deactivate) the certificate.

Workflow

Select the type of request	⇒	Send the request	⇒	Request is Processed, Returned or Cancelled

2.8.1. Select the type of request you want to create

Step by step…

1. On the menu UTILITIES > ACCESS REQUESTS click the [Create a New Access Request]() link.
2. The wizard appears. Select the action DISABLE EXISTING ACCOUNT FOR CERTIFICATE 1.
3. On the blank field that appears next to the selected type of request, you can enter the **last name**, **username** or the **e-mail** address of the user linked to the certificate. You can also enter the **Common Name (CN name)** of the certificate you want to disable 2.
4. The user linked to the certificate appears in the list, so you can select it.
5. After selecting the user, click NEXT 3.

INFO	As this certificate and the user linked to it will be completely deactivated, it is not necessary to modify or remove the User information, the node or the Roles and Permissions. These steps are therefore skipped by the wizard!

2.8.2. Send the request to the SFC2007 Support team

The overview of your request is shown. You see:

- The user and certificate information.
- You can add comment in the 'Comments' field.
- Before sending the request you can click PREVIOUS to go back to the previous step or click CANCEL to cancel the creation of the whole request.

Step by step…

6. Click the button Confirm and Send to send the request to the SFC2007 Support team1.

Once the request is sent, you are redirected to the list of requests. Your request is given a unique identifier number (ID). The status of the request is SENT.

The request can now be processed by the SFC2007 Support team. If there are mistakes or other issues, the request is returned to you by the SFC2007 Support team.

2.8.3. If the request is processed…

If the request is processed, the status becomes PROCESSED and one e-mail is sent to the **MS liaison or MS liaison Deputy** informing that the request has been processed successfully. No e-mail is sent to the user linked to the certificate (as the user no longer needs the account, the USM assumes the user doesn't expect to be notified).

2.8.4. If the request is returned (not processed)…

If the Support team detects problems or missing information the status becomes RETURNED and one e-mail is sent to the MS liaison (deputy) with an explanation on the reason for returning.

The MS liaison (deputy) can:

- Correct the request and send it again (see 2.9) or
- Cancel the request (see 2.10)

2.9. Editing a returned request

When the SFC2007 Support team returns a request, you can edit the request to make the corrections asked by the Support team.

To do so you can access the request from the link provided in the return notification e-mail or by selecting the request from the list of requests in the UTILITIES > ACCESS REQUESTS menu. Once the overview of the request is displayed, click on the **Edit** link on the upper part of the screen.

The wizard appears and you can add/remove or overwrite the information on each step and then send the request again to the Commission.

2.10. Cancelling a request

You can cancel a created request for the following reasons:

- You have sent the request to the Commission but you realise afterwards you don't need this request to be processed.
- The Commission returned a request sent by you and you realise you don't need this request to be processed.

If the Commission returned your request and you still need the request to be processed, you can edit it. You don't need to cancel it and create a new one (to edit and send the request again see chapter 2.9).

To cancel the request you can access the request from the link provided in the return notification e-mail or by selecting the request from the list of requests in the UTILITIES > ACCESS REQUESTS menu. Once the overview of the request is displayed, click on the **Cancel** link on the upper part of the screen.

You are requested to confirm the cancellation. Click YES to confirm.

The request is not deleted from the list. The request will appear as CANCELLED in the list of requests.

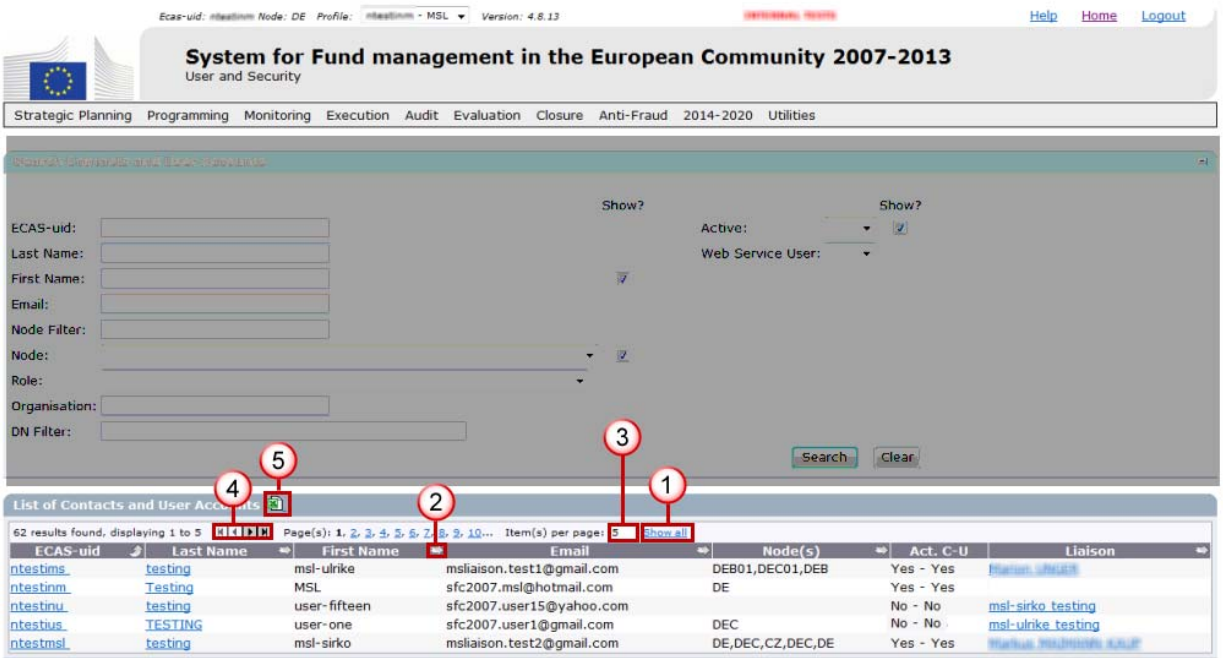
3. Consulting users in the USM

Via the submenu **CONTACTS AND USERS** it's possible to view the list of existing users managed by the MS liaison (deputy) and view the account details of each user.

3.1. Display a list with all existing users

Step by step…

1. On the menu **UTILITIES** select **CONTACTS AND USERS.**
2. Click **SHOW ALL** 1.
3. All existing users managed by the MSL and the deputy, are displayed in the list.



The following information is displayed:

- ECAS-uid; Last Name; First Name; E-mail address,

- **Node (s)**: the node or different node(s) the user has access to.
- **Act C-U**: Active Contact and User.
    - Yes – Yes: (user account is active)
    - No – No: (user account is disabled and cannot access SFC2007)
- **Liaison**: the name of the MS Liaison or MS Liaison deputy who manages the user.

By default, the list is sorted by ECAS-uid. To sort the list on another field, click on the arrow on top of the column you want to sort on 2.

To reduce or increase the number of users displayed per page, change the number of items per page and type ENTER 3.

Use the buttons to navigate through the different pages 4:

- next page
- last page
- previous page
- first page

To generate an excel file of the information displayed in the list click on the excel icon 5.

3.2. Search for a user

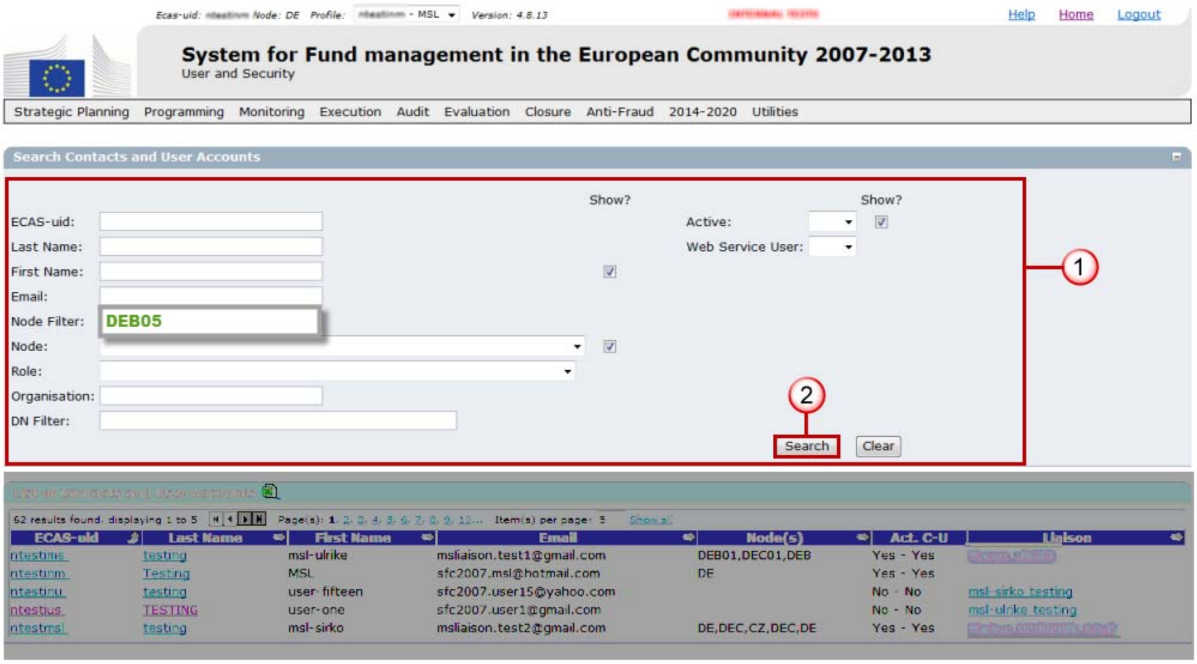
You can enter one or more search criteria to look for a specific user or group of users:

- **ECAS-uid**
- **Last name**
- **First Name**
- **E-mail**
- **Node filter:** to search for users having access to different nodes. For example to list all the users with access to the nodes starting with "FRA" (FRAER, FRADC, FRACO, FRADC, FRAGA, FRAGY, FRAHX, FRAMA, FRARU), enter %FRA% in this field.
- **Node**: search for users on a specific node.
- **Role**: search for users with a specific role.
- **Active**: select Yes or No to display active or disabled users only. All users (active and disabled users) are shown by default.
- **Web service user**: select this option if you want to search for users linked to certificates.

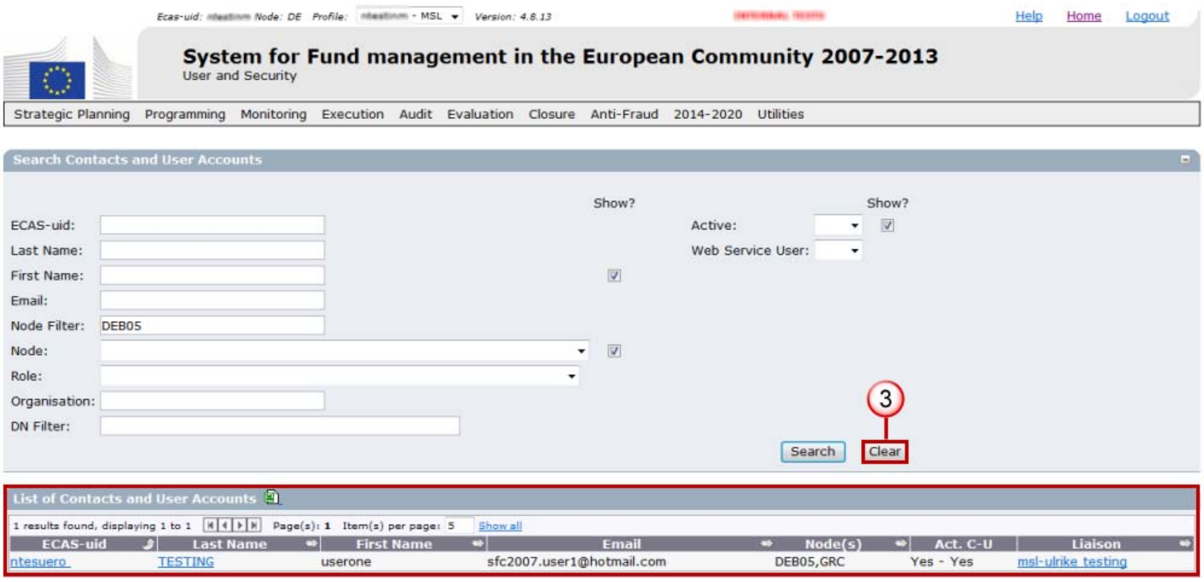
Use a percentage sign (%) to replace one or more characters. For example if you want to search for all users having their Last Name starting with the letter "S" enter in the field **Last Name**: S%

Step by step…

1. On the menu **UTILITIES** select **CONTACTS AND USERS**
2. Enter your search criteria①.
3. Click **SEARCH**②.



The results of your search are displayed:



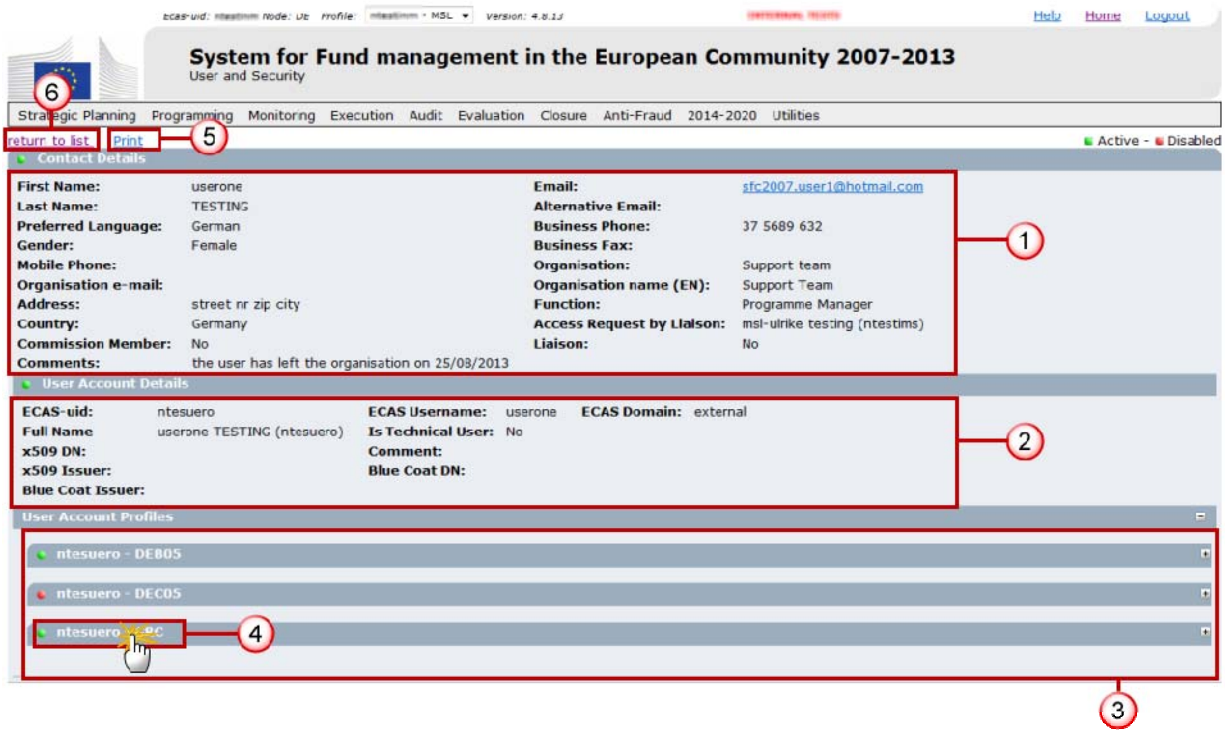
4. Press the Clear button if you want to clear all fields of the search criteria③.

3.3. Display the account details of a user

Step by step…

5. Click on the Username or the Last Name from the list to open the account details of the user.

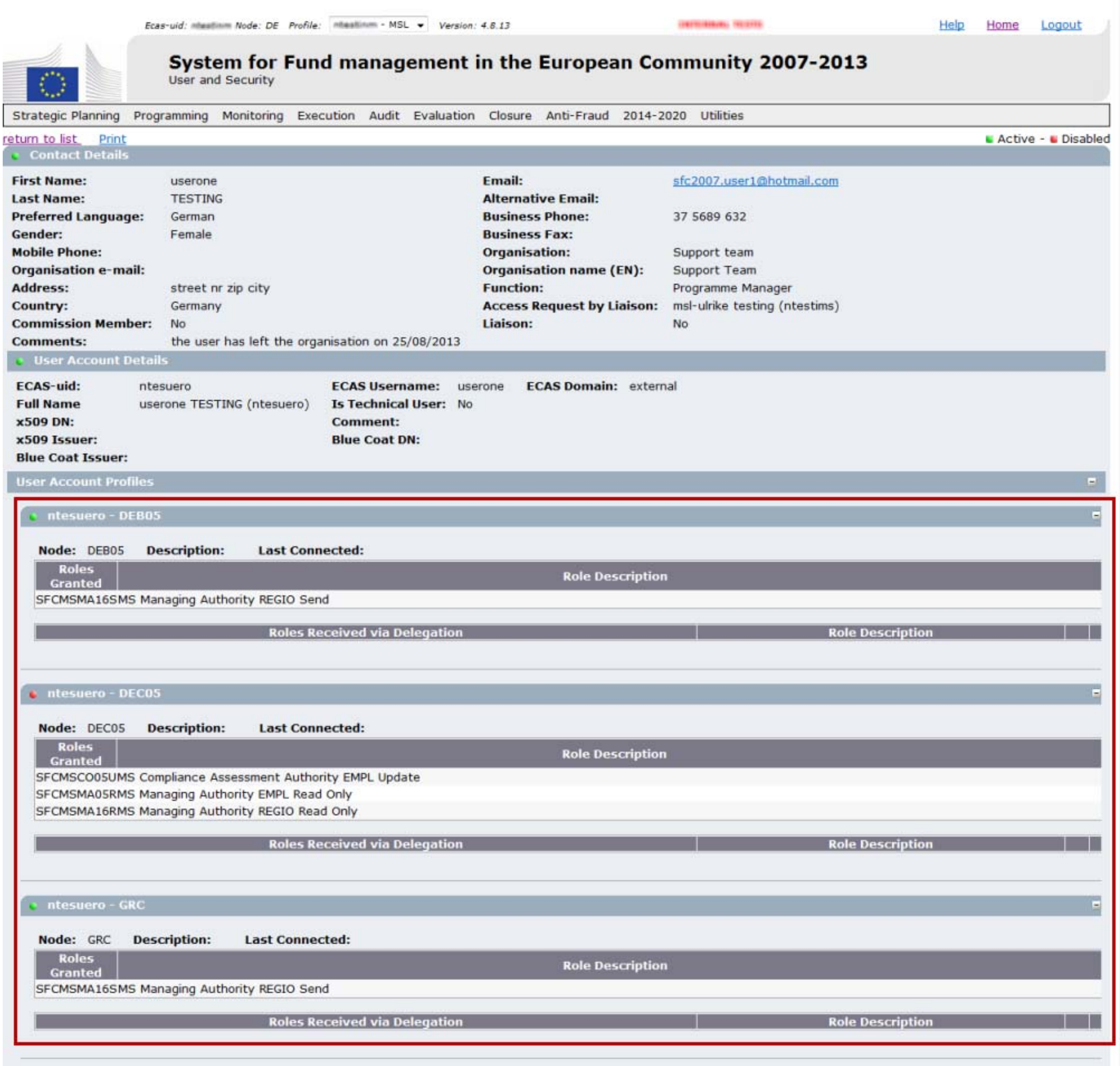
6. The account details are displayed and contain:



Step by step…

- the CONTACT DETAILS of the user①.
- the USER ACCOUNT DETAILS② including the ECAS-uid and the ECAS Username[5].
- the USER ACCOUNT PROFILES③. For each Node the user has access to, there's one User Account Profile.

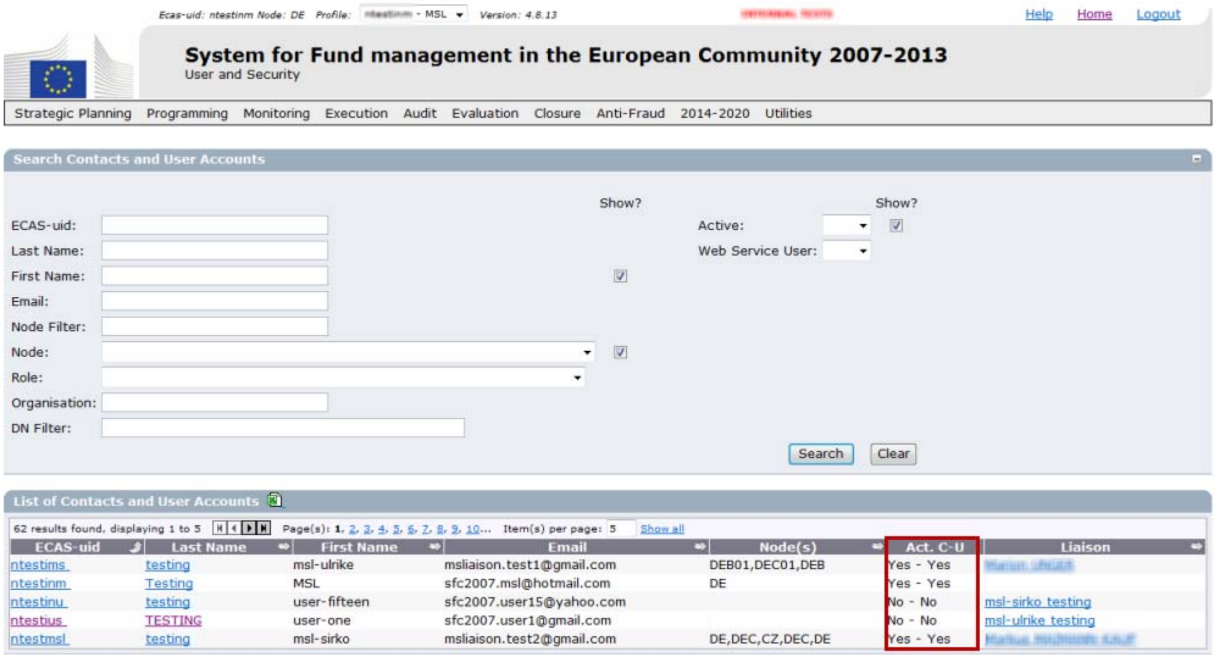
7. To print the account details, click on the **Print** link⑤. Click on the link **Return to list** to go back to the results list of your search⑥.
8. Click on each of the USER ACCOUNT PROFILES to display the roles and permissions of the user on each Node④.



[5] The user needs to enter his/her ECAS Username and password to log in to SFC2007 Front-Office.

3.4. Disabled user

The column 'ACT. C-U' in the results list indicates if a user is active or disabled.



If a user is marked with 'No – No', the user account is disabled and the user will not be able to access SFC2007. In the user account details the user (contact, user account and profiles) will be marked with a red dot. This means the user is disabled:

3.5. Active user with a disabled Profile

If a user has been disabled on one Node but still has access to another Node, the **USER ACCOUNT PROFILE** which is disabled is marked with a red dot, **CONTACT DETAILS** and **USER ACCOUNT DETAILS** remain active and marked with a green dot.

In the example above the user has access to the nodes DEB05 and GRC but cannot access data on the node DEC05 because this profile and the roles & permissions on this profile are disabled.