

## EDIT - feature request #7972

### explicitly allow disallow access to HTTP Invoker endpoints (/remoting/\*\*)

01/09/2019 10:37 AM - Andreas Kohlbecker

<b>Status:</b>	Resolved	<b>Start date:</b>	
<b>Priority:</b>	Priority14	<b>Due date:</b>	
<b>Assignee:</b>	Andreas Müller	<b>% Done:</b>	100%
<b>Category:</b>	cdmlib-remote	<b>Estimated time:</b>	0:00 hour
<b>Target version:</b>	Release 5.5		
<b>Severity:</b>	critical		
<b>Description</b>			
Users can always see any data in the Taxeditor, this can be problematic for projects in which private data must not be un-disclosed to arbitrary users.			
The must straight forward approach is to use Spring Security to configure the MultiWebSecurityConfiguration#RemotingWebSecurityConfigurationAdapter accordingly. This involves implementing one of the following rules:			
<ul style="list-style-type: none"><li>• <del>All users can always access /remoting/** unless they have the role `ROLE_REMOTING_DENIED` rejected</del></li><li>• Users need to be assigned with the ROLE_REMOTING to access /remoting/** <b>agreed</b></li></ul>			
If the role is missing in the db it will be created and added to the Groups Editor and EditorExtendedCreate by the FirstDataInserter. The role will however not be added to the editor groups in case the role exist but is missing from one of these groups. This allows removal of the role from the editor groups to withdraw the remote editing permission from editors in general for a project.			
<b>Related issues:</b>			
Precedes EDIT - feature request #7993: Display "Access Denied" dialog in case...			<b>Closed</b>

#### Associated revisions

##### Revision fa4763c1 - 01/14/2019 04:51 PM - Andreas Kohlbecker

ref #7972 FirstdataInserter adding ROLE\_REMOTING to the editor groups

##### Revision 7f87310a - 01/14/2019 05:15 PM - Andreas Kohlbecker

fix #7972 restricting access to /remoting/\*\* to role 'ROLE\_ADMIN', 'ROLE\_REMOTING'

##### Revision c1d9a788 - 01/31/2019 11:47 AM - Andreas Kohlbecker

ref #7972, ref #8042 permitting remoting access to ROLE\_PROJECT\_MANAGER

#### History

##### #1 - 01/09/2019 12:37 PM - Andreas Kohlbecker

- Status changed from New to In Progress

- % Done changed from 0 to 10

The edit team agreed that introducing the positive role ROLE\_REMOTING would be preferred solution.

The new Role would need to be added to all default Editor groups, which are Editor, EditorExtendedCreate (see eu.etaxonomy.cdm.model.common.Group and eu.etaxonomy.cdm.api.application.FirstDataInserter)

##### #2 - 01/14/2019 06:02 PM - Andreas Kohlbecker

- Precedes feature request #7993: Display "Access Denied" dialog in case the remoting service responds with status code = 4xx added

##### #3 - 01/14/2019 06:03 PM - Andreas Kohlbecker

- Status changed from In Progress to Resolved

- % Done changed from 10 to 50

Applied in changeset [cdmlib|7f87310a8313162080add7230915ed67c0316615](#).

**#4 - 01/14/2019 06:03 PM - Andreas Kohlbecker**

- *Status changed from Resolved to Closed*
- *% Done changed from 50 to 100*

**#5 - 01/15/2019 11:39 AM - Andreas Kohlbecker**

- *Description updated*

**#6 - 01/15/2019 11:40 AM - Andreas Kohlbecker**

- *Description updated*

**#7 - 01/17/2019 09:40 AM - Andreas Müller**

- *Status changed from Closed to Resolved*
- *Assignee changed from Andreas Kohlbecker to Andreas Müller*

Just to remind me to have look how it is implemented.

**#8 - 01/25/2019 02:47 PM - Andreas Müller**

- *Priority changed from Highest to Priority14*