
Disabling Web Services Security and HTTPS for GridSAM within Campus Grid Toolkit.

Revision: 1.1

Author: Justin Bradley

Title: Disabling WSSecurity and HTTPS for GridSAM within a Campus Grid Toolkit context	Version: 1.1
	Date: 07/05/09

Revision No.	Author	Changes Made	Date Revised
1.0	Justin Bradley	First draft	07/05/09
1.1	Simon Hettrick	Review	12/05/09

Title: Disabling WSSecurity and HTTPS for GridSAM within a Campus Grid Toolkit context	Version: 1.1
	Date: 07/05/09

Table of Contents

<i>1</i>	<i>Introduction</i>	3
<i>2</i>	<i>Disabling message-level security by removing the Axis handlers</i>	3
2.1	Server-side changes	3
2.2	Client-side changes	4
<i>3</i>	<i>Disabling transport-level security: using HTTP instead of HTTPS</i>	5
<i>4</i>	<i>Troubleshooting</i>	6

Title: Disabling WSSecurity and HTTPS for GridSAM within a Campus Grid Toolkit context	Version: 1.1
	Date: 07/05/09

1 Introduction

Dependent on your requirements, the secure aspects of submitting jobs through GridSAM may not be required. These secure aspects exist at two levels:

- Message-level security is implemented by Axis handlers, on both the client and server sides. These are a combination of WSS4J routines and OMII-UK specific extensions.
- Transport-level security is achieved by using HTTPS for communications, rather than HTTP. This offers encryption of the traffic 'over the wire'.

Both message- and transport-level security are enabled by default in Campus Grid Toolkit. Either or both aspects may be disabled if required. Altering the security for CGT only makes sense if you are using the 'Direct GridSAM' interface (this means you are not using AHE to submit jobs to GridSAM).

The instructions described in this document are based on Campus Grid Toolkit version 1.1.3 and GridSAM version 2.1.5.

2 Disabling message-level security by removing the Axis handlers

2.1 Server-side changes

On the server installation, change to the installation directory, typically `campus-grid-toolkit-server`. Stop the container if it is running:

```
bin/stopomii.sh
```

Now edit the `webapps/gridsam/WEB-INF/server-config.wsdd` file, by finding and commenting out the section labeled "GridSAM with OMII WS-Security". Below this section is another section labelled "GridSAM without OMII WS-Security", uncomment this section. The edited file should look like that shown below.

```
<!-- GridSAM with OMII WS-Security -->
<!--
<service name="gridsam" provider="java:MSG" style="message" use="literal">
<wsdlFile>org/icenigrid/gridsam/resource/schema/wsdl/gridsam.wsdl</wsdlFile>
<requestFlow>
<handler type="ServiceContextInitHandler"/>
<handler type="SecurityContextInitHandler"/>
<handler type="InitialiseServiceContextHandler"/>
</requestFlow>
<responseFlow>
<handler type="IntegrityEnforcementHandler" />
</responseFlow>
<parameter name="allowedMethods" value="*"/>
<parameter name="scope" value="application"/>
<parameter name="className"
value="org.icenigrid.gridsam.webservice.axis.GridSAMServiceAxisImpl"/>
</service>
-->
<!-- GridSAM without OMII WS-Security -
Remember to set allowUnauthorised=true in WEB-INF/classes/
```

Title: Disabling WSSecurity and HTTPS for GridSAM within a Campus Grid Toolkit context	Version: 1.1
	Date: 07/05/09

```
GridSAMService.properties -->
<service name="gridsam" provider="java:MSG" style="message" use="literal">
<wsdlFile>org/icenigrd/gridsam/resource/schema/wsdl/gridsam.wsdl</wsdlFile>
<requestFlow>
</requestFlow>
<responseFlow>
</responseFlow>
<parameter name="allowedMethods" value="*" />
<parameter name="scope" value="application" />
<parameter name="className"
value="org.icenigrd.gridsam.webservice.axis.GridSAMServiceAxisImpl" />
</service>
```

Now edit `webapps/gridsam/WEB-INF/classes/GridSAMService.properties` file by changing:

```
allowUnauthorised=false
```

to

```
allowUnauthorised=true
```

This asserts that GridSAM will not check that user credentials have been passed as part of the message. You can now restart the container

```
bin/startomii.sh
```

2.2 Client-side changes

On the client-side, a similar change to the handlers is necessary. Change to the client installation, typically called `campus-grid-toolkit-client`.

Edit the `conf/client-config.wsdd` file by commenting out the security handlers. The edited file should look like that shown below.

```
<?xml version='1.0'?>
<deployment xmlns="http://xml.apache.org/axis/wsdd/"
xmlns:grid-acct="http://www.it-innovation.soton.ac.uk/2004/grid/account"
xmlns:grid-res="http://www.it-innovation.soton.ac.uk/2004/grid/resalloc"
xmlns:grid-job="http://www.it-innovation.soton.ac.uk/2004/grid/job"
xmlns:java="http://xml.apache.org/axis/wsdd/providers/java">
<globalConfiguration>
<parameter name="attachment_encapsulation_format" value="axis.attachment.style.dime"/
>
<requestFlow>
<!--
<handler type="java:uk.ac.omii.security.wss4j.handler.WSOutboundHandler" >
<parameter name="action" value="Timestamp Signature" />
<parameter name="signaturePropFile" value="crypto.properties" />
<parameter name="signatureKeyIdentifier" value="DirectReference" />
```

Title: Disabling WSSecurity and HTTPS for GridSAM within a Campus Grid Toolkit context	Version: 1.1
	Date: 07/05/09

```

<parameter name="signatureParts" value="{http://schemas.xmlsoap.org/soap/envelope/}Body;{http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurityutility-1.0.xsd}Timestamp"/>
<parameter name="passwordCallbackClass"
value="uk.ac.omii.security.utils.PWCallback"/>
</handler>
-->
</requestFlow>
<responseFlow>
<!--
<handler type="java:uk.ac.omii.security.wss4j.handler.PolicyEnforcementHandler">
<parameter name="action" value="Timestamp Signature"/>
<parameter name="signaturePropFile" value="crypto.properties" />
<parameter name="signatureKeyIdentifier" value="DirectReference" />
<parameter name="passwordCallbackClass"
value="uk.ac.omii.security.utils.PWCallback"/>
<parameter name="signatureParts" value="{http://schemas.xmlsoap.org/soap/envelope/}Body;{http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurityutility-1.0.xsd}Timestamp"/>
<parameter name="ignoreEndpointCNmismatch" value="true" />
</handler>
-->
</responseFlow>
</globalConfiguration>
<transport name="http" pivot="java:uk.ac.omii.transport.http.OMIIHTTPSender"/>
</deployment>

```

3 Disabling transport-level security: using HTTP instead of HTTPS

This change is most easily performed by using a set of files shipped as part of the CGT installer, as described below.

Change directory to the installer, typically `campus-grid-toolkit-server-1.1.3`, then into the extension directory.

Next set four shell variables, these examples are given using bash syntax. Substitute your own values where required.

```

export OMII_TOMCAT_PORT=18080
export OMII_TOMCAT_PROTOCOL=http
export OMII_HOME=/home/user/campus-grid-toolkit-server
export OMII_ANT=../apache-ant-1.7.1/bin/ant

```

Now run the supplied `OMIIsupportProtocol.pl` perl script. The container will need to be stopped while the script is running and then restarted:

```
OMII_HOME/bin/stopomii.sh
```

Title: Disabling WSSecurity and HTTPS for GridSAM within a Campus Grid Toolkit context	Version: 1.1
	Date: 07/05/09

```
./OMIISwitchProtocol.pl
```

```
OMII_HOME/bin/startomii.sh
```

The output will be similar to the following.

```
Buildfile: ./OMIISwitchProtocol.xml

switch:
[copy] Copying 1 file to /home/user/campus-grid-toolkit-server/tomcat/conf
[xslt] Processing /home/user/campus-grid-toolkit-server/tomcat/conf/
server.xml.bak to /home/user/campus-grid-toolkit-server/tomcat/conf/server.xml
[xslt] Loading stylesheet /home/user/campus-grid-toolkit-server-1.1.3/extension/
OMIISwitchProtocol.xsl

BUILD SUCCESSFUL
Total time: 0 seconds
```

4 Troubleshooting

1. If the `GridSAMService.properties` file has not been updated, the following will be reported to the client by way of an Axis fault:

```
[GridSAMStatus] (main:) unable to retrieve job status: failed to retrieve status of job:
authentication required
```

This may be fixed by setting “`allowUnauthorised=true`” and restarting the container.

2. If the `server-config.wsdd` file has not been updated properly, the following may be reported to the client by way of an Axis fault:

```
FATAL [GridSAMSubmit] (main:) unable to submit job: failed to submit job: WSDoAllReceiver:
Request does not contain required Security header
```

Follow the above instructions to help remedy this issue. Ensure that the container has been restarted after the changes have been made.

3. If the `client-config.wsdd` file has not been updated properly, the following may be reported to the client by way of an Axis fault:

```
FATAL [GridSAMSubmit] (main:) unable to submit job: failed to submit job: Did not
understand "MustUnderstand" header(s)
```

Follow the above instructions to help remedy this issue. Ensure that you are editing the copy of `client-config.wsdd` that is being used by your client code.

4. Having changed your container over to use HTTP rather than HTTPS, sometimes the start script can inaccurately report the following:

```
bin/startomii.sh
```

```
Starting up tomcat
```

Title: Disabling WSSecurity and HTTPS for GridSAM within a Campus Grid Toolkit context	Version: 1.1
	Date: 07/05/09

Using JRE_HOME: /usr/java/jdk1.5.0_07

Waiting for container... Tomcat is already running.

Assuming that the container has been stopped properly before hand, this message can be ignored. The container does successfully start.