

How to log and trace OAuth2 and OpenID Connect HTTP messages

Detailed logging and tracing of the OpenIDConnect method for the following transactions can be enabled:

- Token request

Additionally, if there is no id_token returned with the access_token (or id_token has otherwise been disabled using none algorithm), also the following

- Userinfo request
- Introspection request

To enable tracing:

On each node, modify ubilogin/ubilogin-ss0/webapps/uas/WEB-INF/log4j.properties

Add the following line

```
log4j.logger.com.ubisecure = TRACE, Diag
```

and redeploy the applications on each node

```
# redeploy applications
cd ubilogin/ubilogin-ss0/config
./tomcat/update.sh
```

Protocol logger must be set to DEBUG.

To do this, in Ubiogin Management, from the Logging tab, verify that
Server Instance: UAS,
Logging level: diag.protocol is set to level Debug.

Logger Settings		
Server Instance:	uas	▼
Logging Level:	diag.protocol	▼
		Debug

After this change has been made, additional logging is made in this uas3_diag log.

Outbound requests can be seen, search for "HttpRequestImpl HttpRequest.invoke()"

Authorization request object is logged after possible encryption.

For token and other requests, only the GET or POST request and parameters are logged, not the request body. The responses are not logged.

If the system is configured only to sign request objects, the request JWT can be decoded and examined.

Debugging encrypted request objects

To debug outbound requests to a partner that requires encryption, the only option is disable encryption temporarily to capture the outbound format. The receiving party may or may not reject the request depending on their security requirements.

When registering the OpenIDConnect method, make sure that signing is on:

request_object_signing_alg="RS256"

and that encryption is turned off by removing the following two keys from the JSON metadata:

request_object_encryption_alg

request_object_encryption_enc



This level of logging exposes sensitive information and degrades performance. It is meant only for testing in test environments.

Related articles

- [Configure Telia FTN authentication using OIDC](#)
- [SSO login screen ui-extension examples](#)
- [Use an unsolicited SSO or an IDP initiated SSO](#)
- [IDP Initiated SSO if SP doesn't initiate login](#)
- [Add Organizations/Users to Ubisecure extranet](#)