

Lab 1.4: Log Files

Purpose

The purpose of this module is to learn

- Learn the type and location of the main log files of the SSO and CustomerID
- View the SSO logs with the Log Viewer tool and a text editor
- View The CustomerID logs with a text editor

Requirements

- SSO and CustomerID installed

Part 1: Viewing log files

There are several logs available for SSO and CustomerID. These files can be used e.g. to monitor authentication, technical or statistical events. You can view the log files with a text editor. SSO logs can be viewed also with a log viewer tool which is a part of the SSO Management System.

Ubisecure SSO provides three types of logs:

- Diagnostic log
- Statistics log
- Audit log

Diagnostic log is used for troubleshooting problems. Audit log is used for reviewing events that have occurred in the system. Statistics log is the same as the audit log, except the personal identifying user principal information is not shown. The location of the files is **C:\Program Files\Ubisecure\ubilogin-ss\ubilogin\logs**. Read more about the SSO logs from here: [Logging - SSO](#)

CustomerID has two log files at the application level.

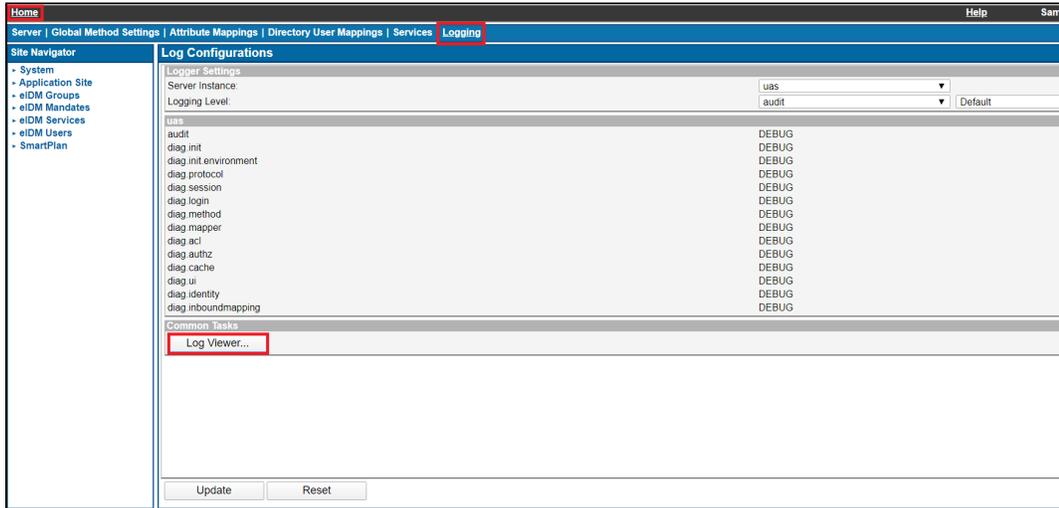
- `customerid_audit.log` – This log file contains the audit log.
- `customerid_diag.log` – This log file contains additional technical information, such as errors.

Additional log files can be generated by the application server inside the WildFly installation. Read more about CustomerID logs from here: [Logging - CustomerID](#)

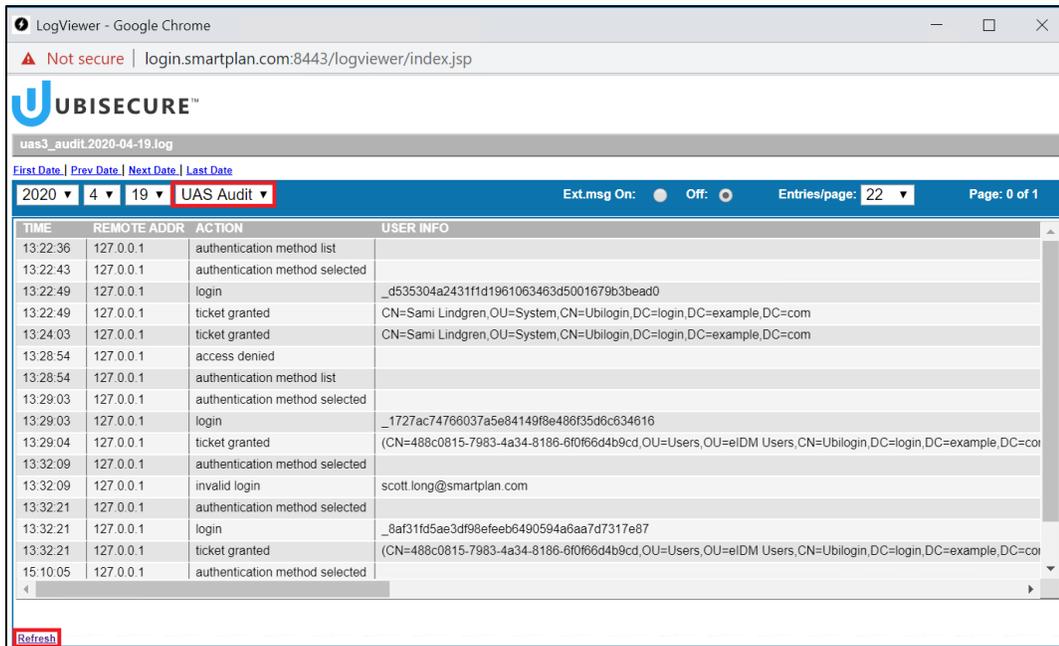
Task 1: View the SSO log files for authentication information using the Log Viewer tool and text editor.

1. Open the Log Viewer tool in the SSO Management System. Home - Logging - Log Viewer.

Note, you can also Access Log Viewer tool at <https://login.smartplan.com:8443/logviewer>



2. Choose UAS Audit as the log type and read the authentication information. Study what different authentication methods have been used today. Refresh the page if necessary.



3. Authenticate to the SmartPlan Application with invalid credentials. Open the log file with a text editor and try to find information about the failed authentication attempt. C:\Program Files\UbiSecure\ubilogin-ss\ubilogin\logs\uas3_audit.YYYY-MM-DD.log.

Task 2: View the CustomerID log files for information about deleted organisation.

1. Log in to the MySmartPlan (CustomerID) as Scott Long
2. Add a new organization called "Log Test"

UBISECURE™ Administration
Suomeksi [In English](#) Scott Long [Self-Service](#) [Help](#) [Logout](#)

[Home](#) **Front page** [Users](#) [Approvals](#)

This page shows information about the organizations in the system.
You can view more information about an organization and its users by selecting one from the list below.

[Create new organization](#)

Organizations

You can search for organizations by giving some letters from the beginning of the organization name.

UBISECURE™ Administration
Suomeksi [In English](#) Scott Long [Self-Service](#) [Help](#) [Logout](#)

Organization

Step 1:
Details

Give the details for the organization that you wish to create.

Organization Details

Parent:

Technical Name:

Display Name:*

Organization Type:* ▼

Service:

3. Delete the organisation "Log Test".

UBISECURE™ Administration

Suomeksi In English Scott Long Self-Service Help Logout

Home / Log Test

Basic data Users Roles Mandates Approvals

This page contains basic information about an organization.

Organization Information

Technical name:	logtest	
Name:	Log Test	Change
CRM ID:		Change

[Remove](#)

[Create new organization](#)

4. Open the C:\Program Files\wildfly-21.0.2.Final\standalone\log\customerid_audit.log file and search indication for a deleted organisation called "Log Test".

Extra: Adjusting logging levels

SSO:

Configure your logging levels on the Logging tab of the Home screen. As the levels are read at the server startup, **a restart of the server is needed to apply the changes.**

UBISECURE™

Home Server | Global Method Settings | Attribute Mappings | Directory User Mappings | Services | Logging Help Sami Lindgren [Logout]

Site Navigator

- System
- Application Site
- eIDM Groups
- eIDM Mandates
- eIDM Services
- eIDM Users
- SmartPlan

Log Configurations

Logging Level

uss

- diag *
- audit
- statistics
- tech
- diag *
- diag mit
- diag mit environment
- diag protocol
- diag session
- diag login
- diag method
- diag mapper
- diag acl
- diag authz
- diag cache
- diag ui
- diag identity
- diag inboundmapping
- satuhetu audit
- satuhetu statistics

Common Tasks

[Log Viewer...](#)

[Update](#) [Reset](#)

As the levels are read at the server startup, **a restart of the server is needed to apply the changes.**

```
net stop ubiloginserver
net start ubiloginserver
```

A change in the logging levels should appear in the diag log (uas3_diag.YYYY-MM-DD.log or diag in Log viewer) at startup as a note of the following template:

```
tech Log level updated: ubilogin.<LOG_COMPONENT>: <LEVEL>
```

CustomerID (MySmartPlan):

Adjust your logging levels by editing the configurations in C:\Program Files\wildfly-21.0.2.Final\standalone\configuration\standalone.xml. There you can find these logger elements and change the levels of audit and diag logs by editing the level name attributes:

```
<logger category="com.ubisecure.customerid.log.audit" use-parent-handlers="false">
  <level name="INFO"/> <!--Apply here your value for the audit logs: DEBUG, INFO, WARN, ERROR .-->
  <handlers>
    <handler name="CID_AUDIT_LOG_FILE_HANDLER"/>
  </handlers>
</logger>
<logger category="com.ubisecure" use-parent-handlers="false">
  <level name="INFO"/> <!--Apply here the value for the diag logs.-->
  <handlers>
    <handler name="CID_DIAG_LOG_FILE_HANDLER"/>
  </handlers>
</logger>
<logger category="org.apache.wicket">
  <level name="INFO"/>
</logger>
```

Restart the Wildfly.

```
net stop Wildfly
net start Wildfly
```