Lab 1.3b: Authentication Methods // Telia training version

Purpose
The purpose of this module is to learn • Basics of Ubisecure SSO authentication methods • How to configure Ubisecure SSO internal authentication methods • How to configure authentication via external authentication services (federation) • How to view SSO and CustomerID logs

Requirements
• SSO and CustomerID installed

Ubisecure Identity Server supports an extensive list of authentication methods. The article Authentication methods - SSO shows how to configure the most common authentication methods.

The external authentication methods can be divided into four main categories: social, business, federated networks and verified identities. Here are some common examples:

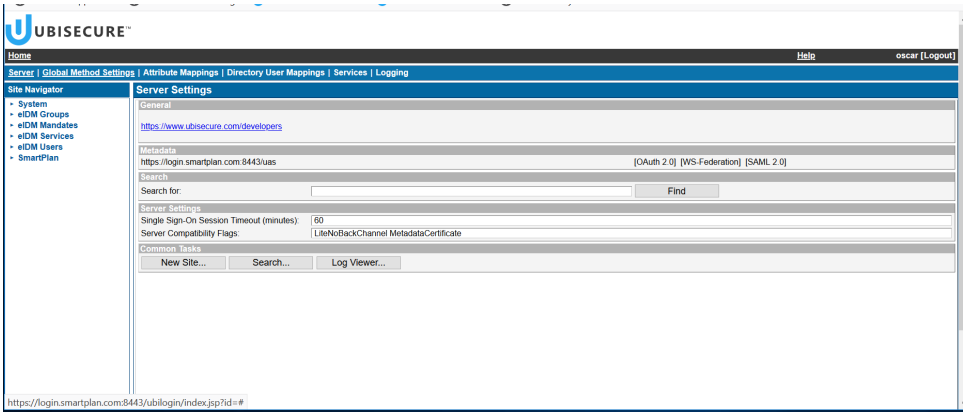
In addition, you can use the Multifactor Authentication (MFA) methods as seen in the Picture above.

During this training session we will work on two of them:

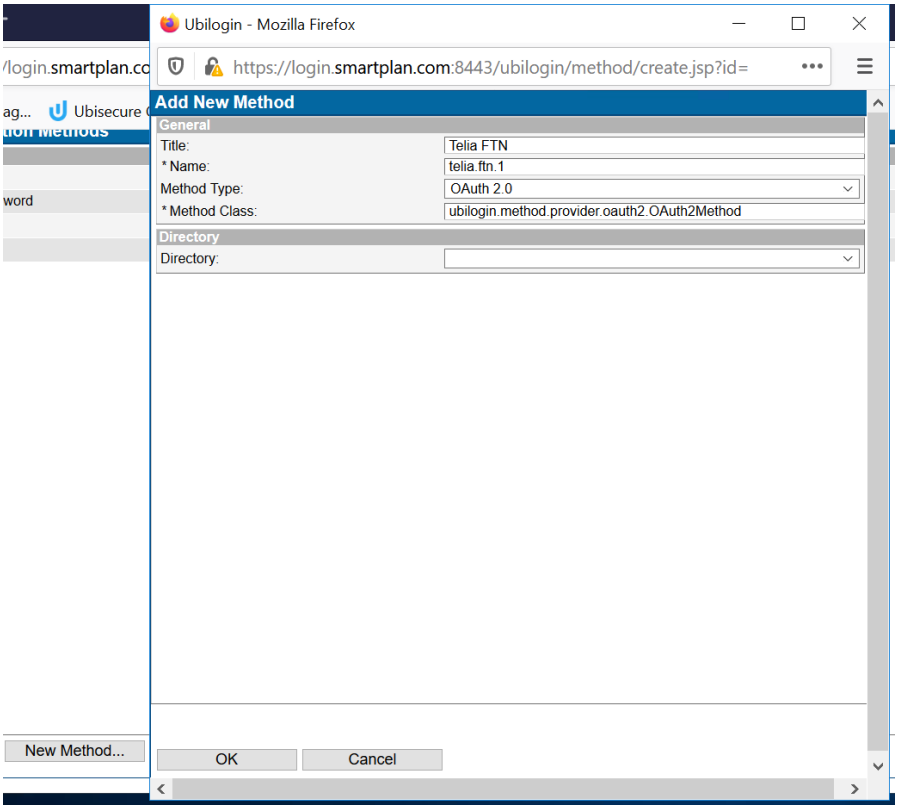
- Finnish Trust Network
- Social Login (Google)

Part 1: Configuring authentication via Finnish Trust Network

1. On the SSO Management Console, from the Home page, click on "Global Method Settings"

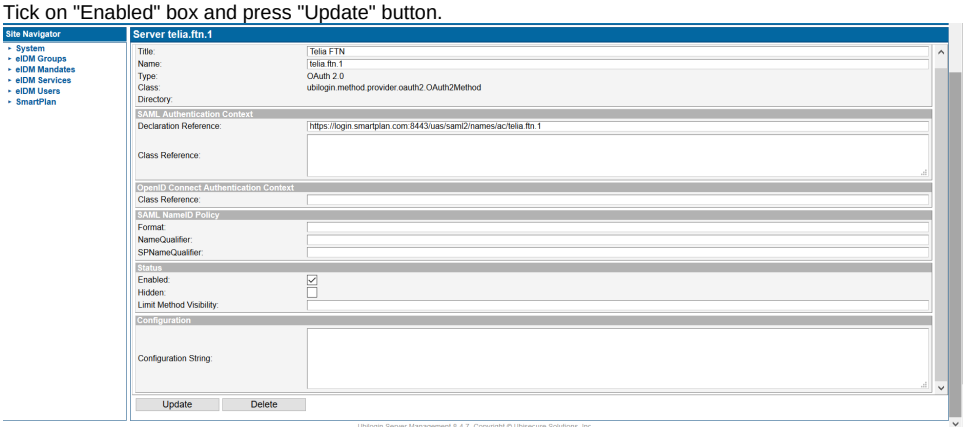


2. Then click "New Method." Fill in as in the image below.
   Title = Telia FTN
   Name: telia.ftn.1
   Method Type: OAuth 2.0



3. Press "OK" to create the method.

4. Tick on "Enabled" box and press "Update" button.

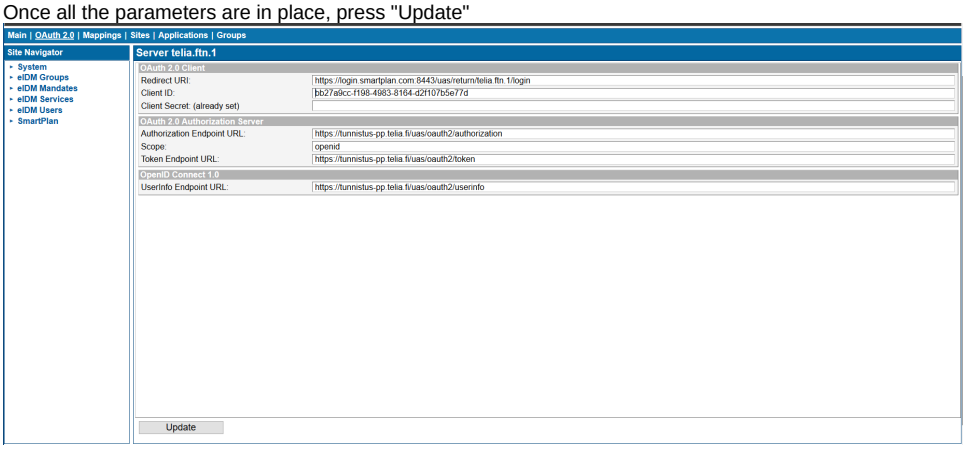


5. Go to "OAuth 2.0" tab on the method.
6. Now fill in the information shown in the table below.

Parameter	value
Client ID	bb27a9cc-f198-4983-8164-d2f107b5e77d
Client Secret:	Will be given by the instructors
Authorization Endpoint URL:	https://tunnistus-pp.telia.fi/uas/oauth2/authorization
Scope:	openid
Token Endpoint URL:	https://tunnistus-pp.telia.fi/uas/oauth2/token
UserInfo Endpoint URL:	https://tunnistus-pp.telia.fi/uas/oauth2/userinfo

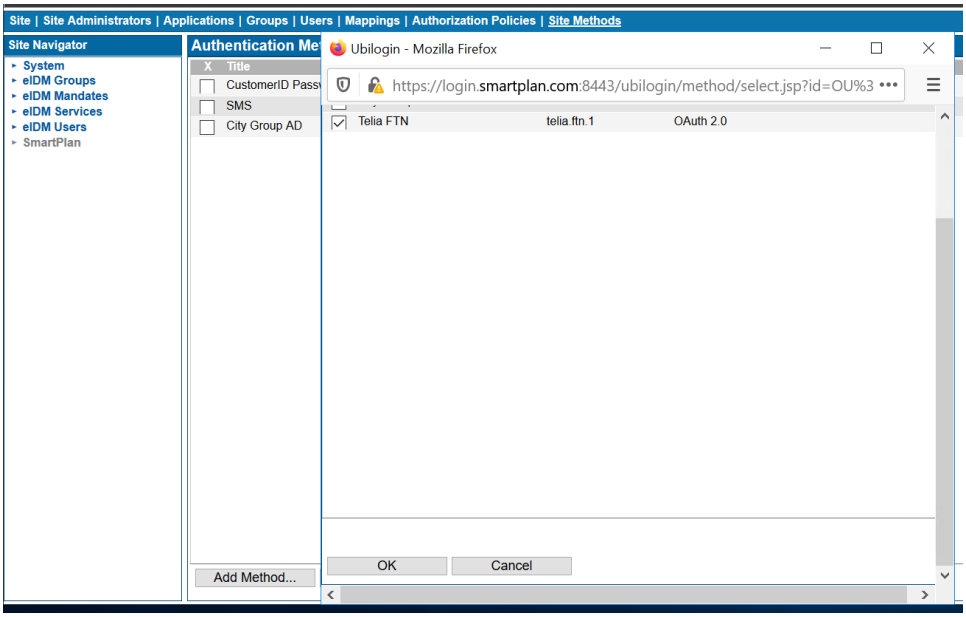
Obs: The full configuration parameters of Telia pre-production environment is on this URL: https://tunnistus-pp.telia.fi/uas/.well-known/openid-configuration

7. Once all the parameters are in place, press "Update"

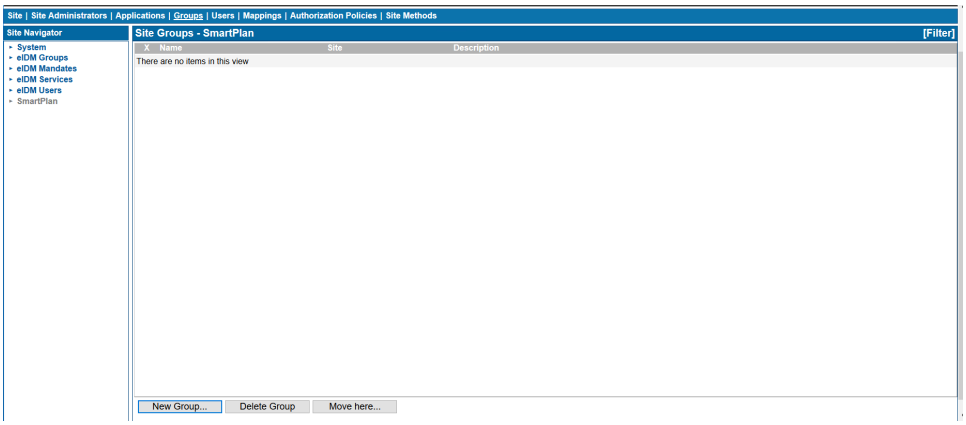


8. Now add the method to SmartPlan site.
   Go to "Site Navigator" on the left menu and click on "SmartPlan" and then to "Site Methods" tab.

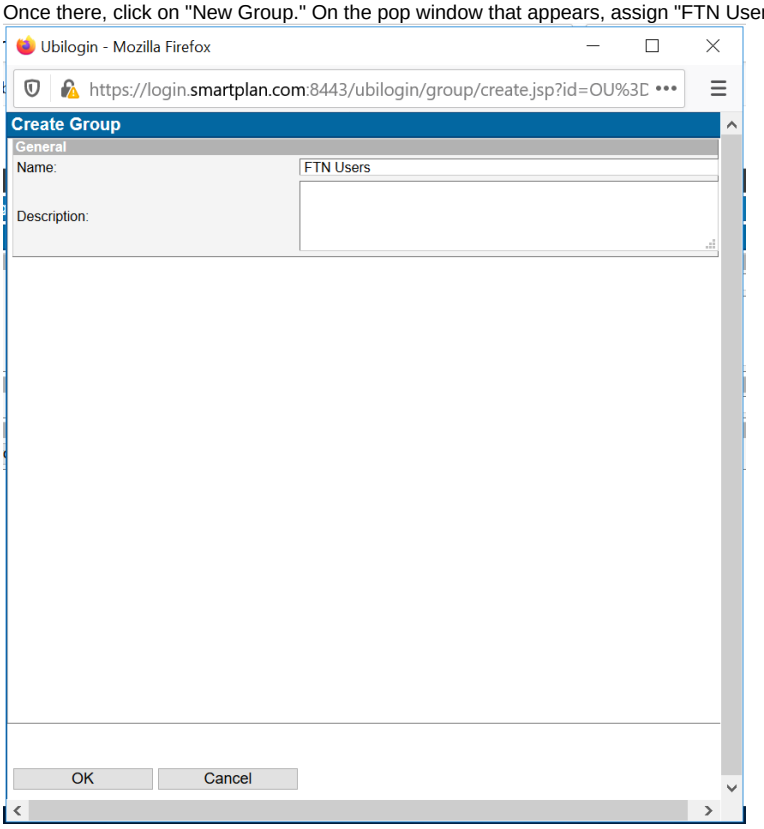
9. Click on "Add Method" button, and when the pop up window appears, tick on "Telia FTN" method and press OK.



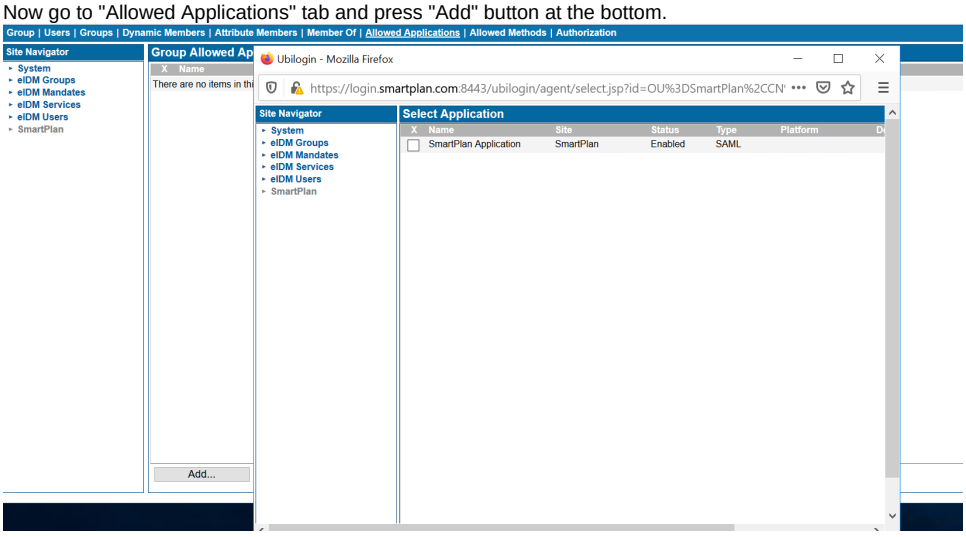
10. Now we have to create a Group for the authorized users. As you are already on "SmartPlan" site, go to the blue horizontal bar and click on "Groups" tab.



11. Once there, click on "New Group." On the pop window that appears, assign "FTN Users" as the group name. Click "OK" to save.

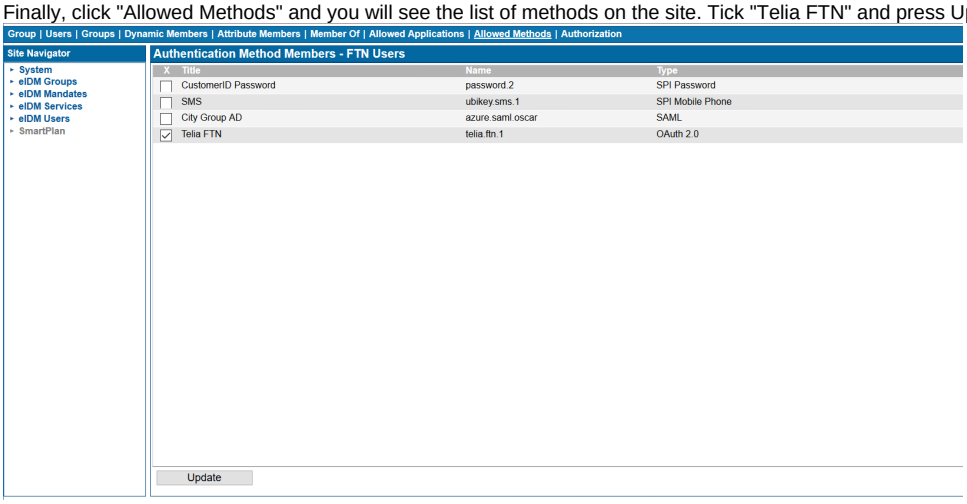


12. Now go to "Allowed Applications" tab and press "Add" button at the bottom.

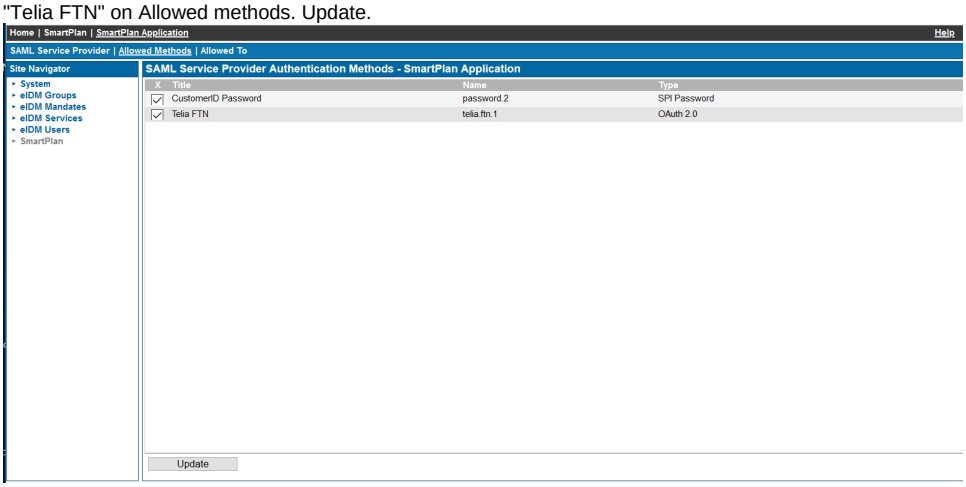


13. Tick "SmartPlan Application" and click OK.

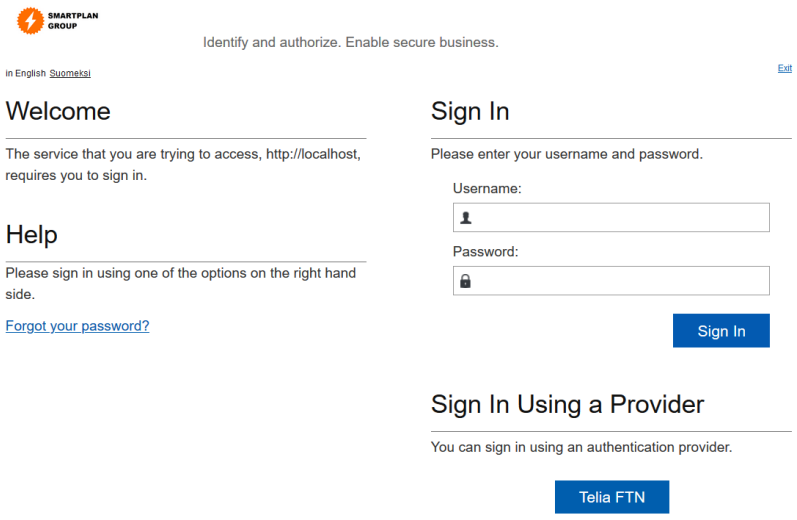
14. Finally, click "Allowed Methods" and you will see the list of methods on the site. Tick "Telia FTN" and press Update.



15. Finally, add the new method Telia FTN to the application. From SmartPlan site, go to Applications, and select SmartPlan Application. Tick "Telia FTN" on Allowed methods. Update.



16. Now the method is configured on the application. Open SmartPlan application: http://localhost:8090/smartplanapplication/
17. Click "Login" button and in the login page you will see Telia FTN



18. Log in using some test users' credentials below.

Identity Provider	Test credentials
Mobiilivarmenne	Only live credentials normally apply.
Nordea	See Nordea's login page. Click the question mark.

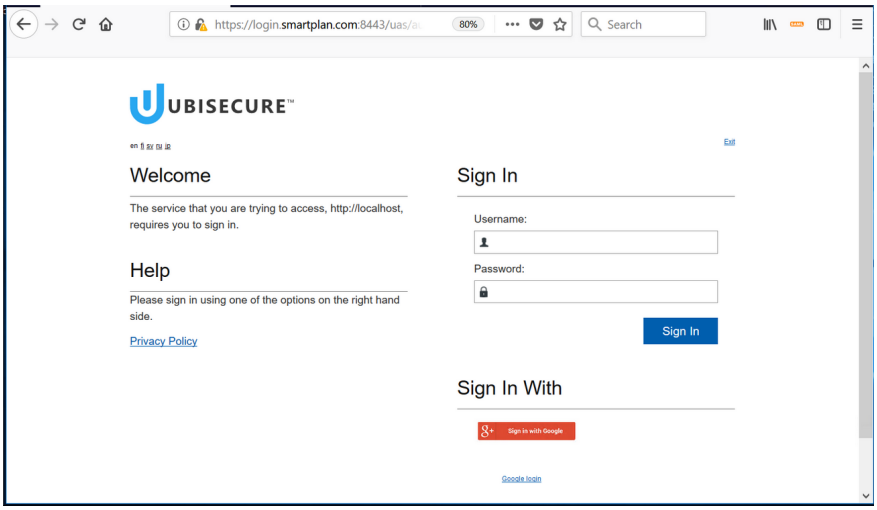
Danske	78985110 / 4545
Handelsbanken	11111111 / 123456
Aktia	See Aktia's login page.
Ålandsbanken	Only live credentials apply.
S-Pankki	Only live credentials apply.
OP	12345678 / 123456
Säästöpankki	11111111 / 123456
POP	11111111 / 123456
OmaSP	11111111 / 123456

Part 2: Configuring authentication via Social Login for MySmartPlan

You can configure authentication using the credentials of your favorite social media. Ubisecure supports most of services that use OAuth2.0 such as Facebook, Google, LinkedIn and others. General parameters for selected OAuth 2.0 Identity Providers - SSO

Follow the instructions in this knowledge base article to configure Google login:

Configure Google login via OAuth2
Obs: Steps 22 and 24 are not needed as you already configured a SAML sample application (during Lab 1.2). Stop at step 33.



Part 3: 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-sso\ubilogin\logs**. Read more about the SSO logs from here: Logging - SSO

CustomerID has two log files at the application level.

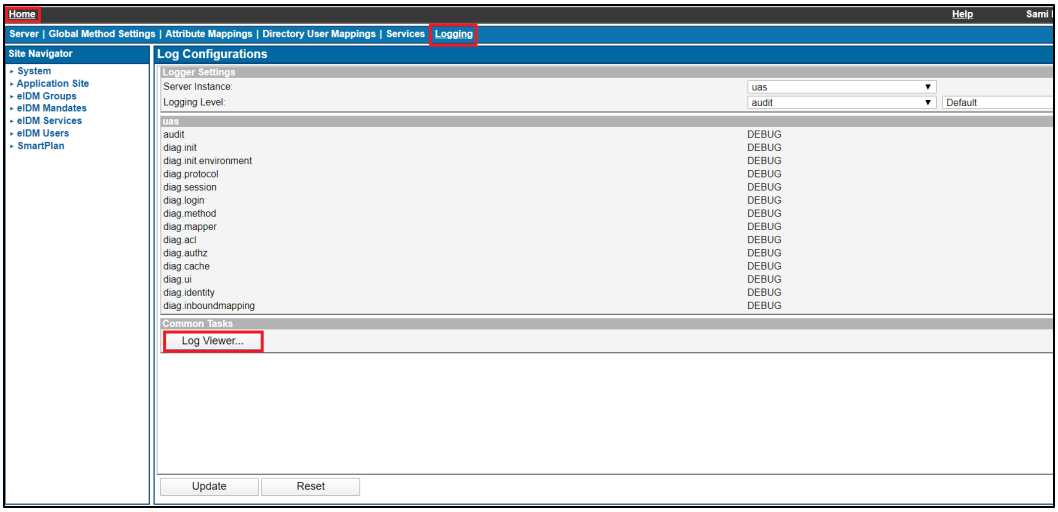
- `customerid_audit.log` – This log file contains the audit log.
- `customerid_diag.log` – This log file contains additional technical information, such as errors.

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

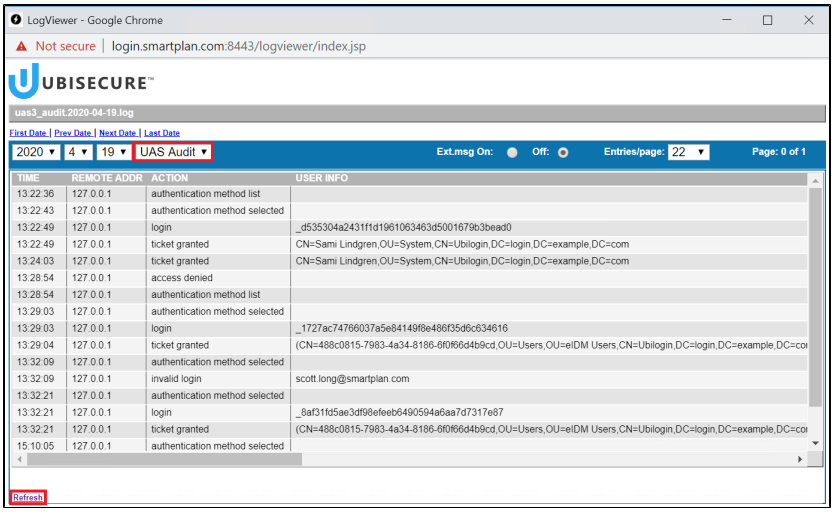
Task 1: View the SSO log files for authentication information using the Log Viewer tool and text editor.

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.

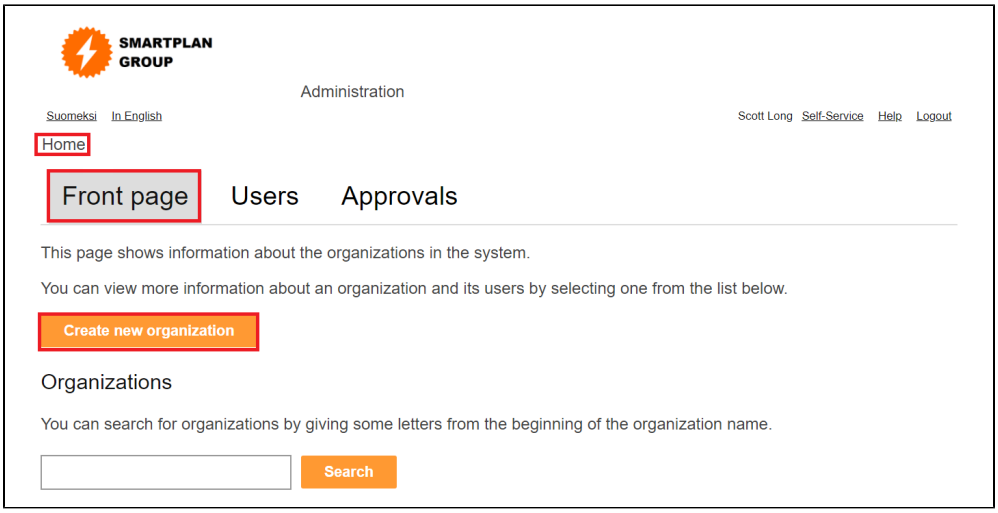


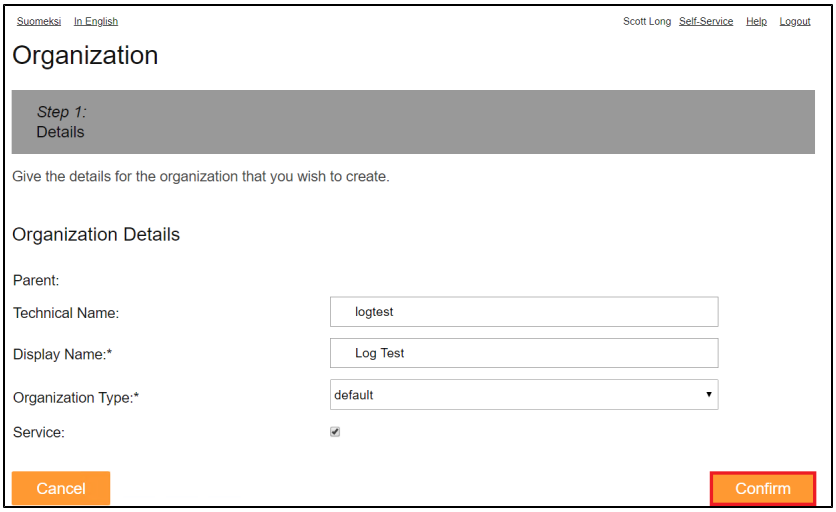
3. Authenticate to the SmartPlan Application with invalid credentials. Open the log file with a text editor and try to find information about the failed authentication attempt. C:\Program Files\Ubisecure\ubilogin-sso\ubilogin\logs\uas3_audit.YYYY-MM-DD.log.

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

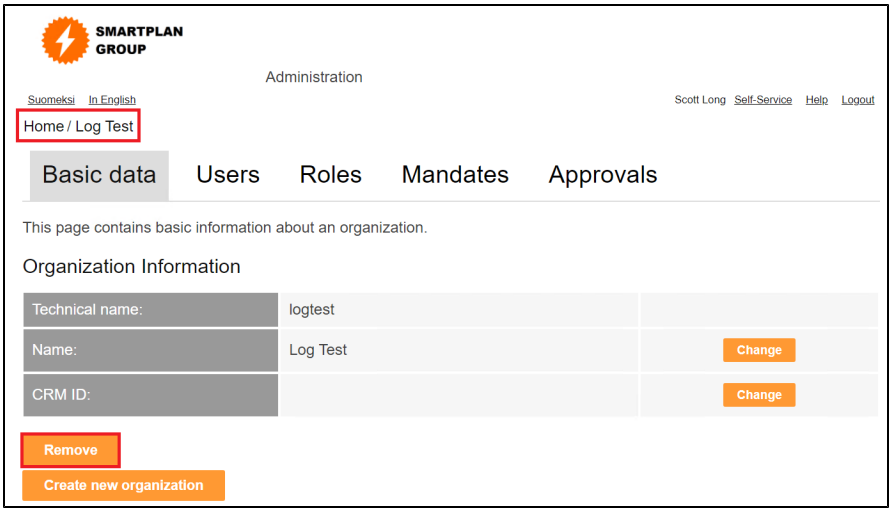
1. Log in to the MySmartPlan (CustomerID) as Scott Long

2. Add a new organization called "Log Test"





3. Delete the organisation "Log Test".

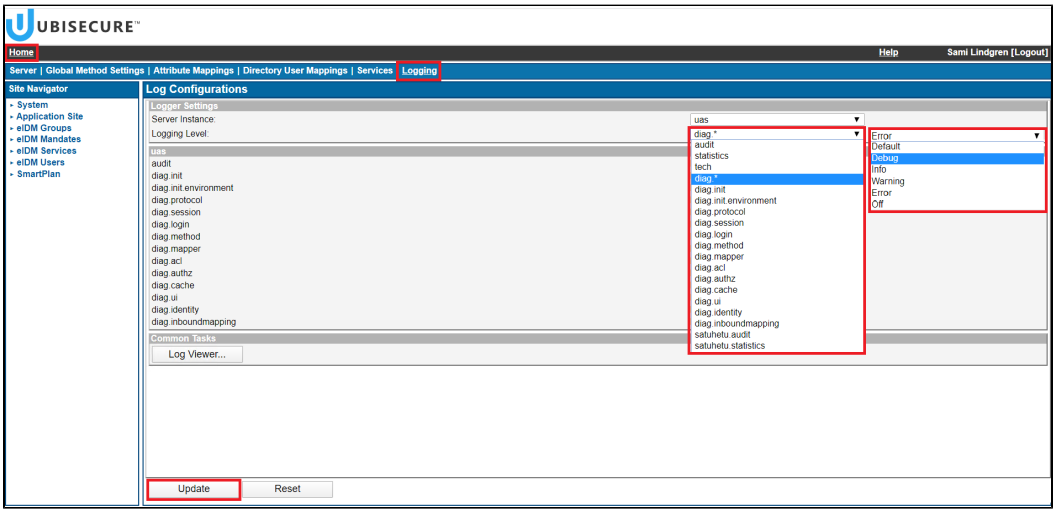


4. Open the C:\Program Files\wildfly-14.0.1.Final\standalone\log\customerid_audit.log file and search indication for a deleted organisation called "Log Test".

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**.



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-14.0.1.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
```