Lab 1.3: Authentication Methods

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:

- SMS One-time Password
- Social Login (Google)

Part 1: Configuring authentication via SMS One-time Password for MySmartPlan

How SMS OTP works?

When a user attempts to access a resource protected by Ubisecure:

1. The user enters a username and password and presses next

2. An SMS message is sent to the user's mobile phone containing an eight digit one-time password

3. The user enters the one-time-password and presses next

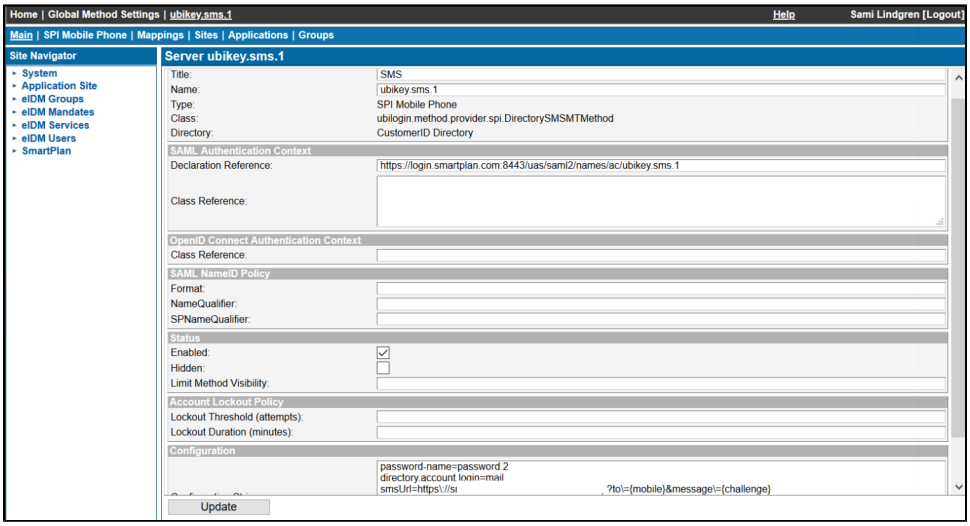
4. Authorisation is performed according to the configuration of the Ubisecure SSO Server and the user is redirected to the target application and granted access if permitted

The user's telephone number is retrieved from the user account stored in the local Ubisecure Directory or in an external directory (AD, LDAP or SQL).

Step 1: Configure SMS OTP on SSO

SMS OTP method is partly pre-configured on your SSO environment.

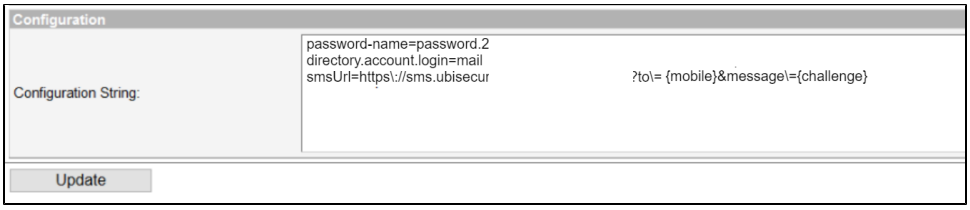
1. Go to Global Method Settings and open SMS method. Click "SPI Mobile Phone" tab. You will see the URL of the SMS service, which will look something like this: https://XXXXXXXXX?to={mobile}&message={challenge}



2. Open the link and test that you can receive a SMS on your mobile phone. Note that + prefix must be given as URL encoded (%2B).

Test Message
`https://XXXXXXXXX?to=%2B3584056277673&message=Test`

3. On SSO Management console, add SMS as authentication method on the SmartPlan site.
   Select the site "SmartPlan", Site Methods, and select Add Methods... and choose **ubikey.sms.1** authentication methods that will need to be used on this site.
4. In order to login using email address, you must add `directory.account.login=mail` to the ubikey.sms.1 configuration string. In Global Method Settings, select SMS. Add the string and click the Update button.



5. Restart UbiloginServer in order the changes to take effect. This must be done after configuring authentication methods.

Step 2: Configure SMS OTP on CustomerID

On CustomerID you must edit **eidm2.properties** file.

1. Open template version of the file C:\Program Files\Ubisecure\customerid\tools\examples\custom\template_eidm2.properties
2. Search for "# SMS gateway"

```
# SMS gateway
# - This property defines the URL for the SMS gateway. The URL will be used as is, except for
#   substituting {mobile} and {challenge} for the mobile number and the challenge to be sent by SMS
#   to the mobile number, respectively.
# - Default: <not defined>
# - Example:
methods.sms.gateway =
```

3. Copy all the configuration lines above to your working eidm2.properties file in C:\Program Files\Ubisecure\customerid\application\custom\eidm2.properties
4. Then do the following edit. In "methods.sms.gateway = " write the URL you found in Step 1 (something like this: https://XXXXXXXXX?to={mobile}&message={challenge}).
5. Add the following lines to eidm2.properties file

```
methods.sms = ubikey.sms.1
methods.protected = methods.password, methods.sms
```

6. Restart Wildfly

Step 3: Test that SMS OTP is working

If you have configured your SAML application (during Lab 1.2), you can test SMS OTP now. Otherwise leave this for later.

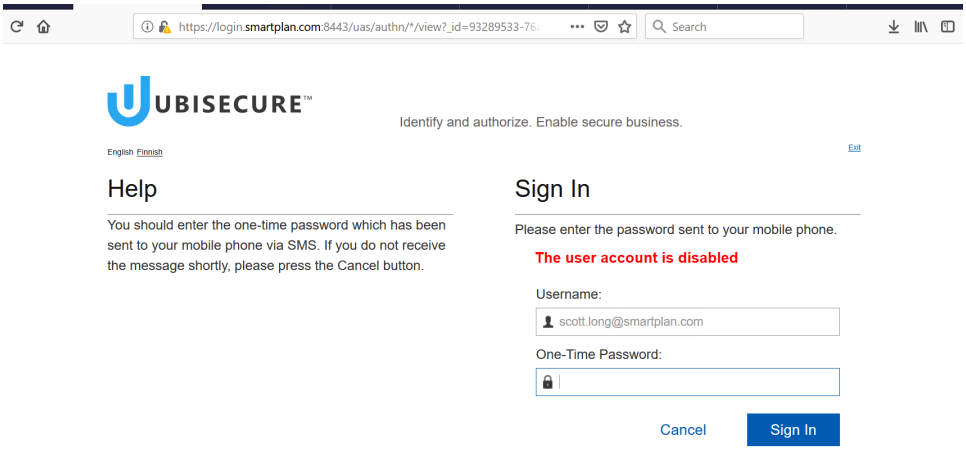
First of all, configure SMS OTP for your sample application "SmartPlan Application"

To configure, on SSO Management console:

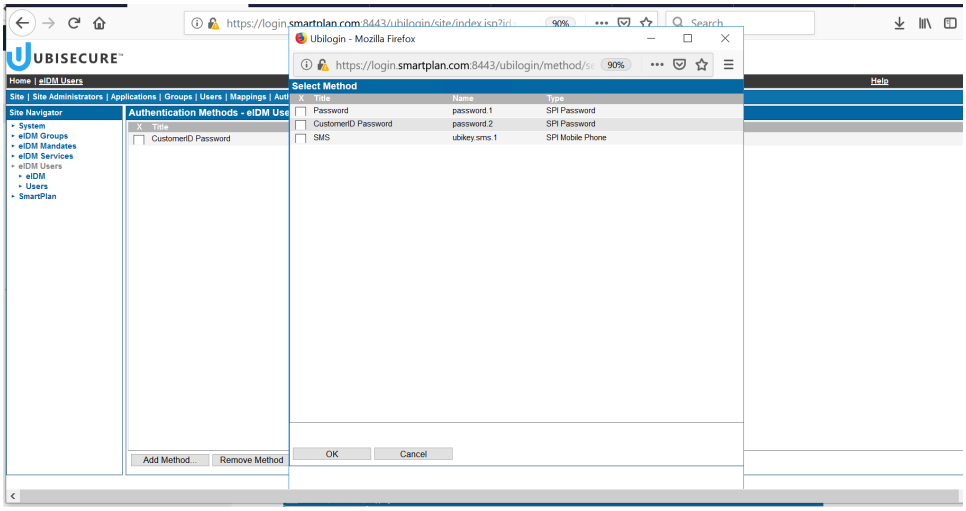
1. Go to "SmartPlan" site and select Applications tab
2. Open sample application (SmartPlan application)
3. Select Methods tab
4. Uncheck method ”password.2”
5. Check method ”ubikey.sms.1” and click Update

Now let's test to verify that SMS OTP authentication is working as expected:

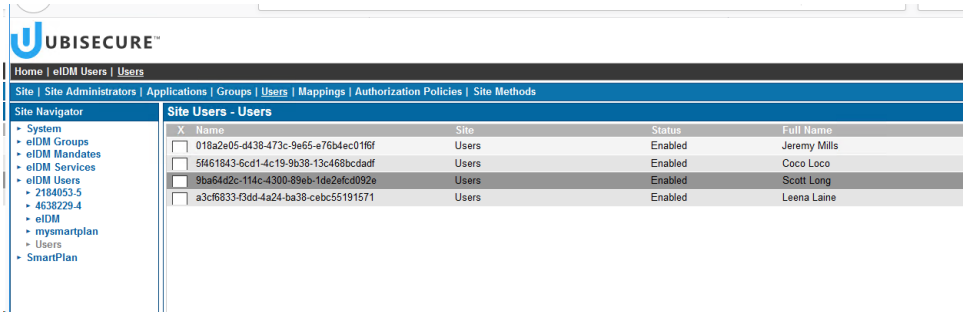
1. Go to your sample application (SmartPlan Application): http://login.smartplan.com:8090/smartplanapplication/ (correct with the exact URL of your installed sample application, if needed)
2. Log in as Scott Long. user = scott.long@smartplan.com ; password = Password2 and verify that the authentication is interrupted, because you have no mobile number in your user profile.

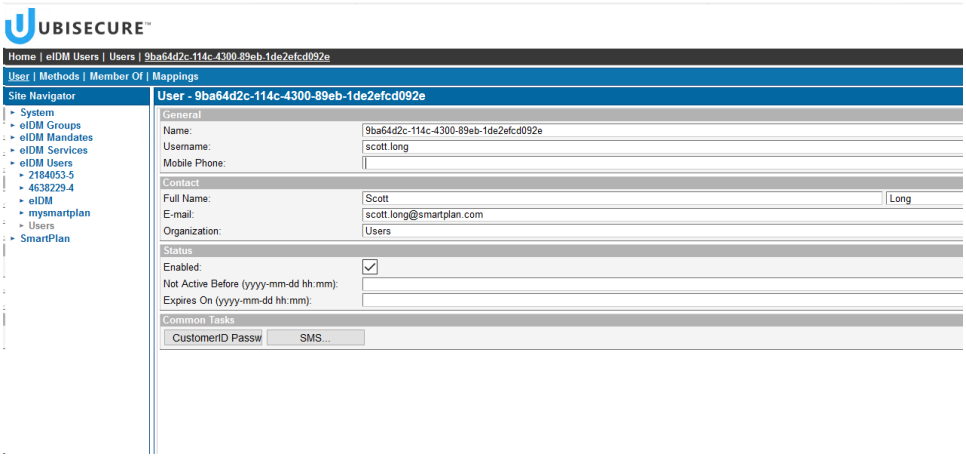


3. Go to Ubisecure SSO management. Add ubikey.sms.1 to Site Methods of "eIDM Users" site.



4. Then open user Scott Long in eIDM Users / Users. On "Methods" tab activate authentication method ubikey.sms.1
5. On "User" tab add your phone number to Scott Long.





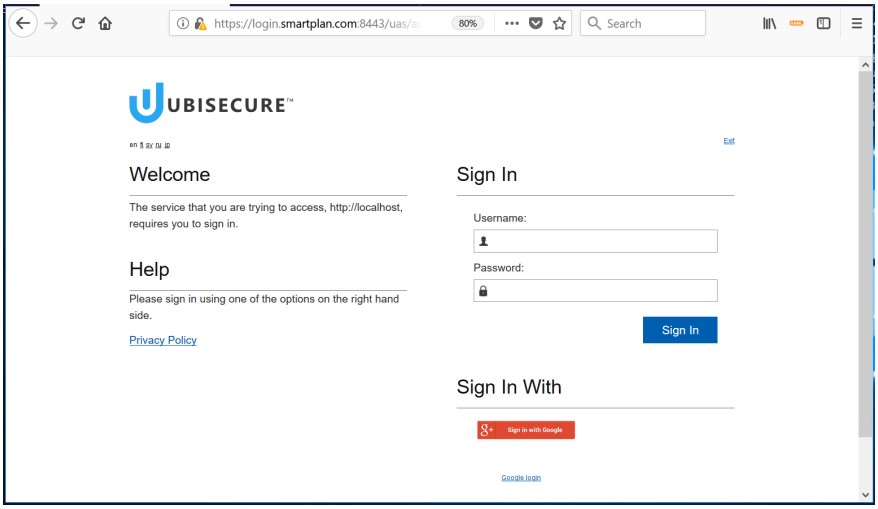
6. You are ready now. Finally, log into SmartPlan application, and verify that you authenticate with SMS OTP.
7. Once you have verified that SMS OTP works as expected, enable password authentication (password.2) again for smartplanapplication. This will be needed in later exercises.

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.

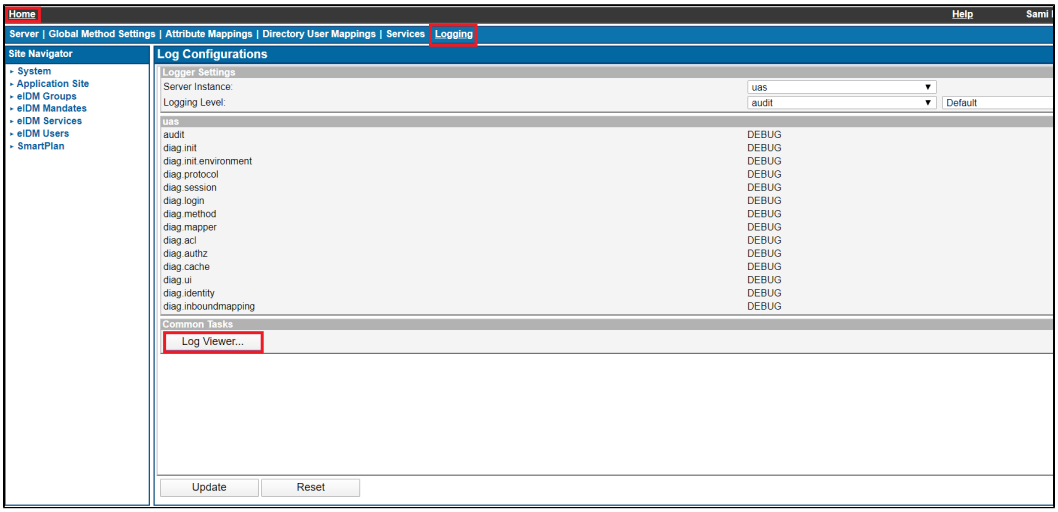
- `customerid_audit.log` – This log file contains the audit log.
- `customerid_diag.log` – This log file contains additional technical information, such as errors.

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

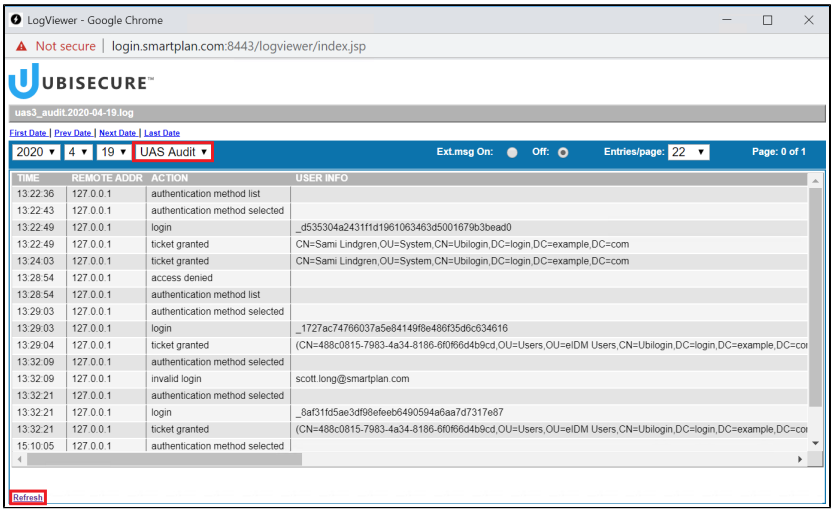
Task 1: View the SSO log files for authentication information using the Log Viewer tool and text editor.

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.

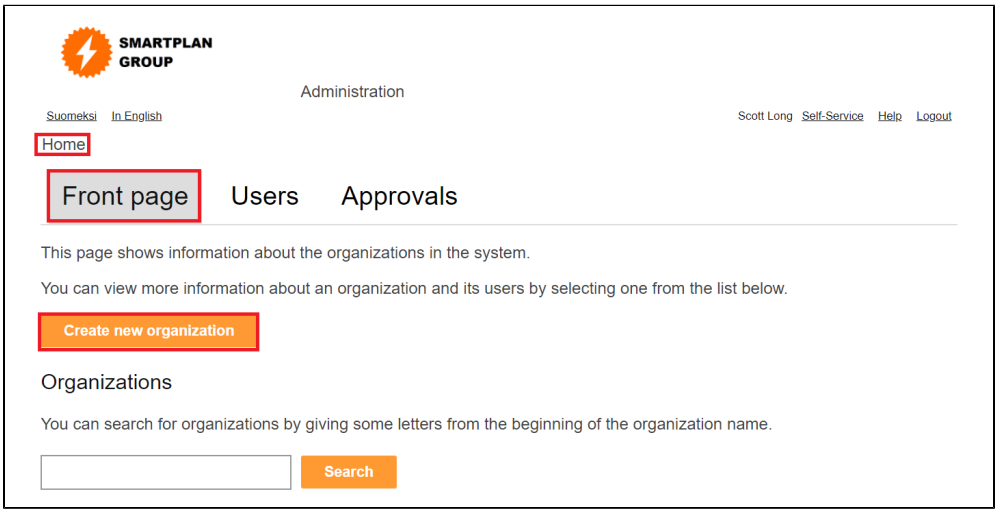


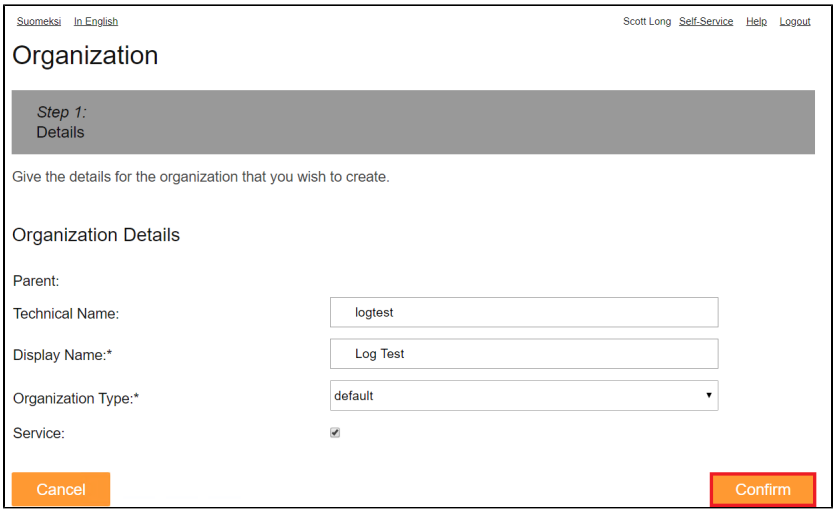
3. Authenticate to the SmartPlan Application with invalid credentials. Open the log file with a text editor and try to find information about the failed authentication attempt. C:\Program Files\Ubisecure\ubilogin-sso\ubilogin\logs\uas3_audit.YYYY-MM-DD.log.

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

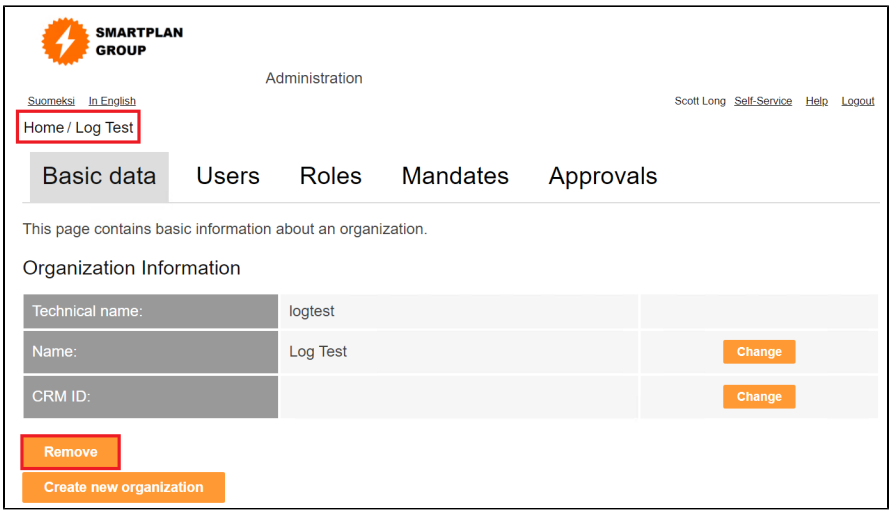
1. Log in to the MySmartPlan (CustomerID) as Scott Long

2. Add a new organization called "Log Test"





3. Delete the organisation "Log Test".

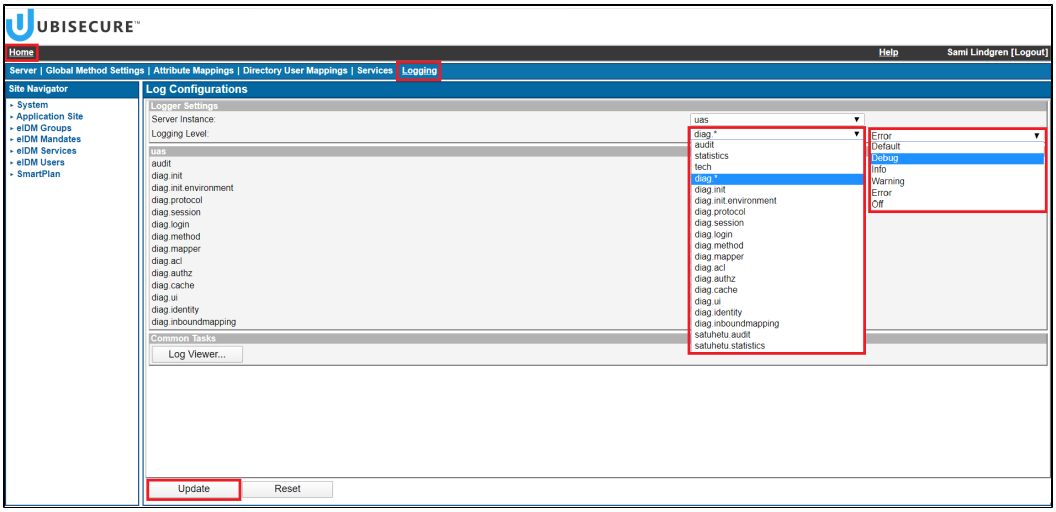


4. Open the C:\Program Files\wildfly-14.0.1.Final\standalone\log\customerid_audit.log file and search indication for a deleted organisation called "Log Test".

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
```