

SOX – The Safety and Security Engineering Workbench

SOX Server: LDAP User Synchronization

Overview

The LDAP synchronization module embedded in the SOX server installation enables customers to import LDAP users belonging to one or more groups into SOX. Once the LDAP users are created in SOX a periodically running synchronization job collected possible changes of some user attributes and group assignments in LDAP and applies these changes to the SOX users.

LDAP is the leading system. That means changes of user attributes or group assignments in SOX coming from LDAP user attributes or group assignments are reversed during the next synchronization run.

Note

This document as well as the detailed functionality of the LDAP synchronization module might change in the future. Please ensure that the latest version of this document is available.

Details

The SOX LDAP basically works as follows for every periodically run:

- query all groups in LDAP that are configured in the SOX LDAP configuration file
- for each group in the result set
 - create the group if it does not exist in SOX
 - query the LDAP users that belong to that group
 - for each user
 - create a SOX user if the LDAP user does not exist in SOX
 - if the LDAP user has the attributes *company* and *department* create the *company* and - if present – the *department* belonging to the *company* in SOX.
Otherwise create a configured *default company* and assign the SOX user to the *default company*
 - if the SOX user for the LDAP user already exists compare the configured attributes and if there are differences overwrite the SOX user attributes with the values of the corresponding LDAP attributes – only if the LDAP attributes are filled
 - if the SOX user does not have the same group assignments of the configured groups as the corresponding LDAP user has, the SOX group assignments are changed to match the LDAP group assignments

Installation

Because the LDAP synchronization module is contained in the SOX server package no further installation is necessary.

Configuration

A special configuration file is contained in the SOX server package that must be adjusted to meet the needs of the customer's LDAP service. The LDAP configuration file is named

```
sox2server-properties.yml
```

and is contained in the root folder of the SOX server installation.

The SOX LDAP configuration file is well documented in the configuration file itself. Therefore, in this document only a subset of configuration parameters is described – the most important attributes.

The configuration file follows the YAML standard.

Configuration parameters

- `server.ldap.schedule.update.time` update interval in minutes
- `server.ldap.connection`
 - `host` the name or ip address of the host running the LDAP service
 - `port` the default port to communicate with the LDAP service
 - `secured.port` the secured port of the LDAP service – used to retrieve the server certificate
 - `useSsl` whether to use SSL encryption method (must be set to false)
 - `useStartTls` whether to use STARTTLS encryption method (must be set to true)
 - `username` the LDAP username able to read LDAP-Groups and -Users to synchronize with SOX
 - `password` the password for the LDAP username
- `server.ldap`
 - `defaultCompany` the name of the company used to assign LDAP users in SOX if the LDAP user does not have a company attribute assigned
- `server.ldap.user`
 - `userBaseDn` the base DN where the users can be found
 - `userFilter` the filter for the user query: the LDAP groups containing the SOX users must be set to only retrieve users to be synchronized with SOX
- `server.ldap.groups`
 - `groupBaseDn` the base DN where the LDAP groups containing SOX users can be found
 - `groupFilter` the filter for the group query: the LDAP groups containing the SOX users must be set to only retrieve users to be synchronized with SOX
 - `adminGroupName` the name of the LDAP group containing SOX users who become SOX administrators

The LDAP configuration file contains placeholders (“<to be changed>”) that must be adjusted by the customer for the SOX LDAP synchronization to work properly.