Active Directory/OpenLDAP authentication

How the module works

The Active Directory authentication module allows you to link a Shinken account and an Active Directory account in order to connect to the different Web interfaces of Shinken Enterprise.

Both accounts (Shinken and Active Directory) will be linked by a common key.

For example, the authentication module looks for users with a user@domain.com email address in the Shinken database and will link this account with the one in Active Directory with the same email address.

A Shinken account and an Active Directory account must have a common data in order to be linked and authorize the connection.

The steps to configure the data used to link both accounts are explained below.

Conseil d'utilisation

To keep the Shinken and Active Directory accounts synchronized, it is far more easier to import users directly from Active Directory thanks to the Active Directory source.

Please see the corresponding documentation to have more informations about this feature: Active Directory

Configuration steps

This module allows users to authenticate by checking the account password into an Active Directory instead of the one stored in the Shinken configuration. The setup of this authentication method is done in 3 steps:

- Connection setup to the Active Directory server
- Mapping setup between Shinken and Active Directory fields
- Module activation

Active Directory connection setup

First, the authentication module must have the connection credentials in order to connect to the Active Directory server.

This is done by modifying the **/etc/shinken/modules/auth_active_directory.cfg** file.

Uncomment if needed and fill the following lines:

/etc/shinken/modules/auth_active_directory.cfg

```
ldap_uri                ldap://myserver
username                myuser@mydomain.com
password                password
basedn                        DC=mydomain,DC=com
mapping_file        /etc/shinken-user/configuration/modules/auth-active-directory/mapping.json
```

The fields in the configuration example above function as following:

- **ldap_uri**: Active Directory server address. The protocol used can be *ldap* or *ldaps*.
- **username**: Username used to connect to the Active Directory. Username has the following format: "user@mydomain.com" or "mydomain\user".
- **password**: Password used to connect to the Active Directory server.
- **basedn**: DN used as base for user discovery. The module searchs recursively in this DN for users to perform the authentication with.
- **mapping_file**: This field must point to the mapping file used. This field usage is described in the section below.

Shinken and Active Directory fields mappings setup

The Active Directory authentication module does the link between fields in the Shinken database and fields in the Active Directory base to identify the users.

By default, the module looks for contacts with the "*contact_name*" in Shinken base and looks for a contact in Active Directory with the same value into the "*samaccountname*".

It is possible to specify this behaviour by modifying the mapping file.

On a fresh installation, copy *"/etc/shinken-user-example/configuration/modules/auth-active-directory/mapping.json"* into *"/etc/shinken-user /configuration/modules/auth-active-directory/mapping.json"* (create file path if needed).

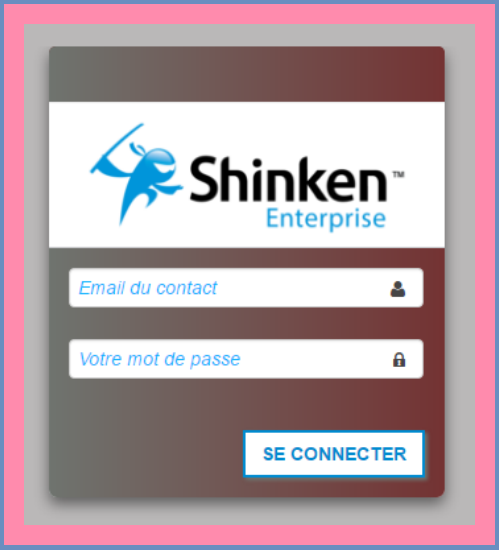
> **Fichiers d'exemple**
>
> The files listed in "*/etc/shinken-user-example*" are in read-only mode. Add write rights after copying into "*/etc/shinken-user*".

In the following example, contacts are joined by the "*mail*" field in Active Directory and the "*email*" field on Shinken.

/etc/shinken-user/configuration/modules/auth-active-directory/mapping.json

```
{
        "ldap_key":                         "mail",
        "shinken_key":                        "email",
        "login_placeholder":          "Email du contact"
}
```

The "login_placeholder" allows you to configure the message displayed on the Login Screen in order to give a visual hint to the user.



Enabling the Active Directory module

At last, the authentication module must be activated in the corresponding configuration files.

Configuration UI

To enable the module on the Configuration UI, replace *Cfg_password* by *auth-active-directory* in the Synchronizer's configuration.

/etc/shinken/synchronizers/synchronizer_master.cfg

```
modules                 auth-active-directory
```

Restart the Synchronizer to account for the latest changes.

/etc/shinken/synchronizers/synchronizer-master.cfg

```
/etc/init.d/shinken-synchronizer restart
```

Visualisation UI

To enable the module on the Visualisation UI, replace *Cfg_password* by *auth-active-directory* in the Broker's configuration (WebUI module).

/etc/shinken/modules/webui.cfg

```
modules                 auth-active-directory, Mongodb, webui-enterprise, sla
```

Restart the Broker to account for the latest changes.

```
/etc/init.d/shinken-broker restart
```

Module Cfg_password

The simultaneous activation of both *Cfg_password* and *auth-active-directory* modules can provoque non-anticipated behaviours. As the *Cfg_password* module checks passwords in Shinken database and the *auth-active-directory* module in the Active Directory, if both modules are loaded, the user will succeed to authentify with both passwords (Shinken and Active Directory).

If this behaviour is wanted, both modules can be enabled in the configuration files as following:

```
modules                 Cfg_password, auth-active-directory, other_modules
```

Use module with OpenLDAP

The module is at first intended for Active Directory use, but functions with OpenLDAP as well.

However, a few steps in module configuration change:

- In the **/etc/shinken/modules/auth_active_directory.cfg** configuration file, the "*mode*" parameter must be "*openldap*".
- In the **/etc/shinken/modules/auth_active_directory.cfg** configuration file, the "*username*" parameter has a different format. With OpenLDAP, a CN must be specified to use for connection.
  The field will look like "*cn=user,dc=mydomain,dc=com*".

The remaining configuration doesn't change.

Values to use for fields mapping

In the mapping file, multiple fields can be specified to join Shinken and Active Directory/LDAP accounts.

The following table lists most used fields:

Shinken	Active Directory	OpenLDAP
contact_name	sAMAccountName	uid
display_name	displayName	displayName
email	mail	mail
pager	telephoneNumber	telephoneNumber