

# SSO to AD domain

CzechIdM supports Single-Sign-On of the AD domain users. The mechanism uses web server, which handles the Kerberos authentication and provides the login of the authenticated user in the HTTP header. Then CzechIdM processes this header and authenticates the user automatically.



The SSO implementation works by looking up a username returned by Kerberos in IdM. This means that the user must have the same sAMAccountName in AD and username in IdM. Also, AD is not case-sensitive but IdM is, i. e., if your sAMAccountName is "jnovak", you can log in to AD as "JNovak" but this is not the case in IdM. **Make sure that usernames in IdM are the same as sAMAccountNames in AD, otherwise, SSO will fail.**

If the user is the Application Admin (e.g. has assigned the role superAdminRole), SSO authentication is disabled for security reasons.

This tutorial shows how to configure an Apache web server and enable SSO in CzechIdM.



When enabling SSO, be sure that your Apache Tomcat application server listens only on localhost (as in standard configuration by [install guide](#)), so no one can forge the HTTP headers and gain access pretending to be one of the users.

During the tutorial, we use the name of the AD domain COMPANY.CZ. CzechIdM will be accessible from the address <https://idm.company>.

## AD - configure a new service

A new service for CzechIdM must be configured in AD. The service must be linked to a specific user. We recommend using only one user per one service (linking multiple services to one user is theoretically possible, but linking one service to multiple users breaks the Kerberos authentication).

Create a new AD user (no special privileges required), e.g. "idm-sso".

Choose the name of the service: HTTP/idm.company@COMPANY.CZ (this doesn't have to contain the exact name of the IdM server, but it helps).

In AD domain controller, start the CMD and generate the keytab:

```
ktpass -out idm.company.keytab -princ HTTP/idm.company@COMPANY.CZ -mapUser idm-sso@company.cz -crypto all -pass * -ptype KRB5_NT_PRINCIPAL
```

The command will prompt for a password.

Download the generated file idm.company.keytab, which will be used in the next steps.

# Configure Apache httpd - Linux

We expect that Apache is installed according to the [admin guide](#).

Install mod\_auth\_kerb:

```
yum install mod_auth_kerb
```

Put the file `idm.company.keytab` in `/etc/httpd/keytabs/` and set correct permissions:

```
mkdir /etc/httpd/keytabs/  
chmod 755 /etc/httpd/keytabs/  
mv idm.company.keytab /etc/httpd/keytabs/idm.company.keytab  
chown apache:apache /etc/httpd/keytabs/idm.company.keytab  
chmod 600 /etc/httpd/keytabs/idm.company.keytab
```

Configure Kerberos realm in `/etc/krb5.conf` and the addresses of the domain controllers. We use DC `dc.company.cz` in our example:

```
[logging]  
default = FILE:/var/log/krb5libs.log  
kdc = FILE:/var/log/krb5kdc.log  
admin_server = FILE:/var/log/kadmind.log  
  
[libdefaults]  
default_realm = COMPANY.CZ  
dns_lookup_realm = false  
dns_lookup_kdc = false  
ticket_lifetime = 24h  
renew_lifetime = 7d  
forwardable = true  
  
[realms]  
COMPANY.CZ = {  
    kdc = dc.company.cz  
    admin_server = dc.company.cz  
}  
  
[domain_realm]  
.company.cz = COMPANY.CZ  
company.cz = COMPANY.CZ
```

Check that the keytab works:

```
yum install krb5-workstation  
kinit -k -t /etc/httpd/keytabs/idm.company.keytab  
HTTP/idm.company@COMPANY.CZ  
klist -e
```

Edit proxy settings in the `/etc/httpd/conf.d/ssl.conf`

```
change this:
ProxyPass / ajp://localhost:8009/
ProxyPassReverse / ajp://localhost:8009/

to this:
ProxyPass /idm/ ajp://localhost:8009/idm/
ProxyPassReverse /idm/ ajp://localhost:8009/idm/
```

Add Kerberos configuration and setting the `REMOTE_USER` header inside the **VirtualHost** tag in `/etc/httpd/conf.d/ssl.conf`. And exclude `/idm/api/v1/status` from authentication so everyone can access it:

```
<Location /idm>
    AuthName "Kerberos Login"
    AuthType Kerberos
    KrbMethodNegotiate On
    KrbMethodK5Passwd On
    KrbAuthRealms COMPANY.CZ
    KrbServiceName HTTP/idm.company@COMPANY.CZ
    Krb5KeyTab /etc/httpd/keytabs/idm.company.keytab
    require valid-user
</Location>

RequestHeader set REMOTE_USER %{REMOTE_USER}s
<Location /idm/api/v1/status>
Satisfy Any
</Location>
```

This configuration enables **Negotiate** (the users logged in domain computer will be automatically authenticated - this must be enabled in the browser), as well as **Basic Auth** (the user, who is not logged in domain computer, will be first prompted for username and password with the message "Kerberos Login" and the credentials will be sent to AD for authentication). Negotiate can be disabled by `KrbMethodNegotiate`, Basic Auth can be disabled by `KrbMethodK5Passwd`.

Restart httpd service:


```
systemctl restart httpd
```

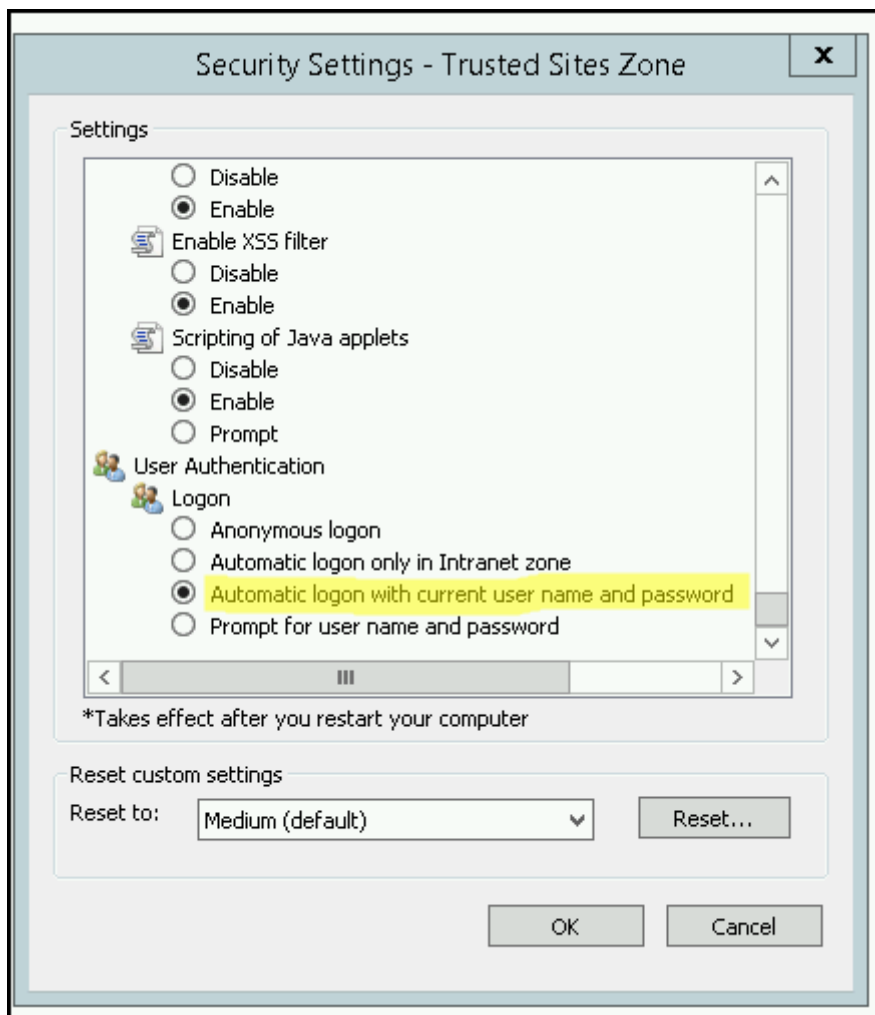
## Enable authentication in browsers

Sending of Kerberos tickets (the method Negotiate) must be enabled in the browsers, otherwise the automatic authentication wouldn't work.

### Internet Explorer:

- Internet Options - Security - Trusted Sites - add <https://idm.company>

-  **Fix Me!** is this necessary as well?: Internet Options - Security - Local Intranet Zone - Custom - User Authentication - Logon - Automatic logon with current user name and password
- IE setup for Automatic logon:



Internet Explorer doesn't support Negotiate, if the address is IP address. If the server name isn't in DNS, you can add it to C:\Windows\System32\drivers\etc\hosts (for testing purposes).

### Mozilla Firefox:

- go to about:config
- network.negotiate-auth.trusted-uris - add <https://idm.company>

For more information about browsers see

<https://www.samuraj-cz.com/clanek/kerberos-cast-10-nastaveni-webovych-prohlizecu/>

## Enable SSO in CzechIdM

SSO must be enabled in IdM configuration. Set the following to the application-SOMEPROFILE.properties:

```
idm.sec.core.authentication-filter.core-sso-authentication-  
filter.enabled=true  
idm.sec.core.authentication-filter.core-sso-authentication-filter.header-  
name=REMOTE_USER  
idm.sec.core.authentication-filter.core-sso-authentication-filter.uid-  
suffixes=@COMPANY.CZ
```

All configuration properties for SSO are described here: [SSO configuration properties](#).



Although the SSO can be configured in the GUI (in configuration properties), we strongly discourage it. In case of broken GUI/authentication, you will have no other means to disable the SSO functionality than manually editing contents of the identity manager's database



Users with superAdminRole cannot login by SSO, they will still be asked for password. This is by design.

## Troubleshooting

General things to check:

- The service principal name must be linked **only to one** user in AD.
- The keytab shouldn't be generated with only some ciphers, so use `-crypto all` in the command as above.

Usual messages in Apache error logs:

- `krb5\_get\_init\_creds\_password() failed: Cannot contact any KDC for requested realm: make sure that DC in /etc/krb5.conf kdc communicates on port 88:`

```
telnet dc.company.cz 88
```

- `krb5\_get\_init\_creds\_password() failed: Client not found in Kerberos database: the given user doesn't exist in AD (nothing wrong with configuration)`
- `krb5\_get\_init\_creds\_password() failed: Preauthentication failed: the given user has different password.`
- `gss\_accept\_sec\_context() failed: No credentials were supplied, or the credentials were unavailable or inaccessible (, Unknown error): the client doesn't trust the address of IdM, i.e. it isn't in Trusted sites in Internet Explorer.`
- `gss\_accept\_sec\_context() failed: An unsupported mechanism was requested (, Unknown error): the client doesn't trust the address of IdM, i.e. it isn't in`

Trusted sites in Internet Explorer. (probably)

- failed to verify krb5 credentials: Key table entry not found: something is wrong with the keytab. Try to compare its version (KVNO) and the version of Kerberos ticket:

```
$ klist -k /etc/httpd/keytabs/idm.company.keytab
Keytab name: FILE:/etc/httpd/keytabs/idm.company.keytab
KVNO Principal
-----
---
  5 HTTP/idm.company@COMPANY.CZ
  5 HTTP/idm.company@COMPANY.CZ
  5 HTTP/idm.company@COMPANY.CZ
  5 HTTP/idm.company@COMPANY.CZ
  5 HTTP/idm.company@COMPANY.CZ

$ kinit -k -t /etc/httpd/keytabs/idm.company.keytab
HTTP/idm.company@COMPANY.CZ
$ kvno HTTP/idm.company@COMPANY.CZ
HTTP/idm.company@COMPANY.CZ: kvno = 5
```

- krb5\\_rd\\_req() failed when verifying KDC followed by failed to verify krb5 credentials: Permission denied: Bad permissions on the keytab file. All httpd processes must have read access to the keytab.

## Users with many AD groups & Internet Explorer

Users who are members of many AD groups (e.g. more than 100) and use IE may have problems authenticating to IdM. They would get HTTP response 400: Bad Request and there would be an error message request failed: error reading the headers in the Apache error log. The reason is, that the Authorization header (holding Kerberos ticket) is longer than the max size of HTTP headers in the Apache webserver. Some browsers, e.g. Chrome, cuts off the tickets, but IE doesn't.

If you can't switch to a different browser and you can't lower the amount of AD group memberships, you may increase the limit of the header size in Apache HTTP Server by the [LimitRequestFieldSize](#) directive. However, the limit may be also on the application server (Apache Tomcat, JBoss). Then you should unset the header so it's not proxied to the application server - put `RequestHeader unset Authorization` in the `/etc/httpd/conf.d/ssl.conf`.

An example of the configuration inside `/etc/httpd/conf.d/ssl.conf`:

```
RequestHeader set REMOTE_USER %{REMOTE_USER}s
# Add following lines to enable access for users with many AD groups
LimitRequestFieldSize 12392
RequestHeader unset Authorization
```

You should estimate the limit for your environment based on the max possible size of the Kerberos ticket

<https://support.microsoft.com/en-us/help/327825/problems-with-kerberos-authentication-when-a-user-belongs-to-many-grou>. Please note that increasing the limit may have impact on your server security (e.g. DDoS attacks).

## See also

[Tips for configuring SSO on Windows \(can be useful on Linux servers as well\)](#)

From:

<https://wiki.czechidm.com/> - **IdStory Identity Manager**

Permanent link:

[https://wiki.czechidm.com/tutorial/adm/sso\\_ad\\_domain](https://wiki.czechidm.com/tutorial/adm/sso_ad_domain)

Last update: **2020/06/15 12:49**

