

# Kopano WebApp Kerberos Single Sign On configuration

- Notice
- Prerequisite:
- Installation
  - Add kopano server to the domain
  - Create a keytab file for the kopano server
- Settings
  - kopano Settings
  - Apache2 settings

## Notice

### Important Notice

Because of the way SSO works the credentials are not available to WebApp.

This can stop plugins from working, or require manual setup of credentials.

The following plugins require WebApp credentials (additional 3rd party plugins might need them as well):

- MDM, does not work with SSO.
- Files, the "Use Kopano Credentials" options will not work, manual setup is still possible.

## Prerequisite:

- Working DNS server
- Working active directory server

Domain = kopano.local

kopano server = mail.kopano.local

## Installation

### Add kopano server to the domain

To add the kopano-server in a domain we use the tool 'PowerBroker Identity Services'

```
$ sudo wget http://download.beyondtrust.com/PBISO/8.2.1/linux.deb.x64/pbis-open-8.2.1.2979.linux.x86_64.deb.sh
$ sudo chmod +x pbis-open-8.2.1.2979.linux.x86_64.deb.sh
```

Start the tool.

```
$ sudo ./pbis-open-8.2.1.2979.linux.x86_64.deb.sh
```

```
$ sudo domainjoin-cli join kopano.LOCAL administrator
```

```
Joining to AD Domain: kopano.LOCAL  
With Computer DNS Name: mail.kopano.LOCAL  
administrator@kopano.LOCAL's password:  
...  
Your system has been configured to authenticate to Active Directory for  
the first time. It is recommended that you restart your system to ensure  
that all applications recognize the new settings.  
SUCCESS
```

## Create a keytab file for the kopano server

Create a user in the active directory for the kopano server in this example it is 'mail'.

Create a Keytab file for the kopano server with the user 'mail'

On a DC run

```
C:\Windows\system32> ktpass -princ HTTP/mail.kopano.local@kopano.LOCAL -  
mapuser mail@kopano.LOCAL -crypto RC4-HMAC-NT -ptype KRB5_NT_PRINCIPAL -  
pass <Password> -out c:\mail.keytab
```

Install mpm-prefork mod-auth-kerb

```
$ sudo apt-get install apache2-mpm-prefork libapache2-mod-auth-kerb
```

Create a directory in /etc/apache2/keytab and move the mail.keytab

```
$ sudo mkdir -p /etc/apache2/keytab  
$ sudo mv /shared/mail.keytab /etc/apache2/keytab/
```

## Settings

### kopano Settings

To enable the sso change the following setting in the server.cfg

```
server_hostname = mail.kopano.local
enable_sso = yes
```

To enable the sso in Webapp change the following in the config.php in the Webapp directory

see [https://documentation.kopano.io/kopanocore\\_administrator\\_manual/configure\\_kc\\_components.html?highlight=ssl#ssl-connections-and-certificates](https://documentation.kopano.io/kopanocore_administrator_manual/configure_kc_components.html?highlight=ssl#ssl-connections-and-certificates) for more information about ssl

```
define("DEFAULT_SERVER", "https://localhost:237/kopano");

// When using a single-signon system on your webserver, but Kopano Core is
// on another server
// you can use https to access the Kopano server, and authenticate using
// an SSL certificate.
define("SSLCERT_FILE", /path/to/ssl/client/cert.pem);
define("SSLCERT_PASS", password-of-cert)

define("LOGINNAME_STRIP_DOMAIN", true);
```

## Apache2 settings

Add the following to the vhost file of webapp for sso to work.

```
<directory /usr/share/kopano-webapp/>
    AuthType          Kerberos
    AuthName          "Login"
    KrbServiceName    HTTP/mail.kopano.local@kopano.LOCAL
    KrbVerifyKDC      on
    KrbMethodNegotiate on
    KrbMethodK5Passwd on
    KrbAuthRealms     kopano.LOCAL
    Krb5KeyTab        /etc/apache2/keytab/mail.keytab
    require           valid-user
</directory>
```