

Oct 21, 2020 19:58

## Active Directory Single Sign-On

**i** This Guide describes how to set automatic Single Sign-On via Active Directory.

WMS Version: 5.X0 / 4.0X

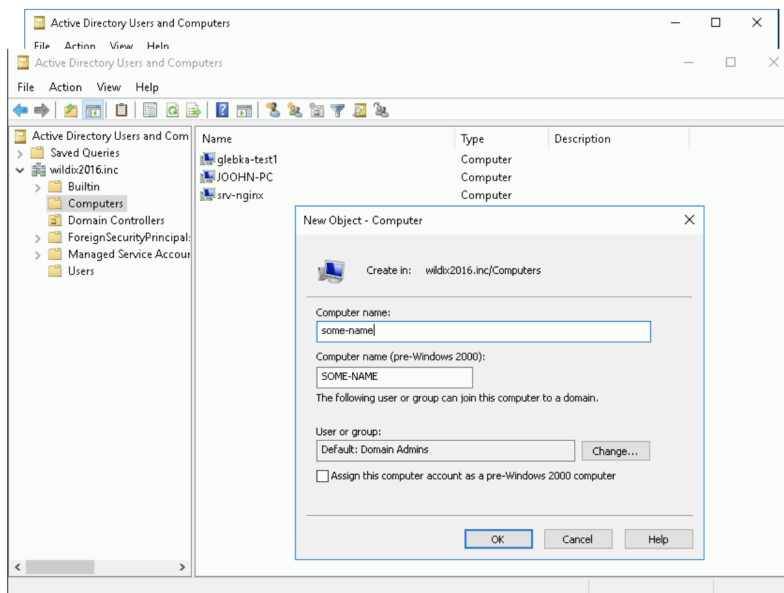
Created: March 2019

Permalink: <https://confluence.wildix.com/x/rABOAg>

- [Step 1. Generate KeyTab file in Active Directory](#)
- [Step 2. Upload KeyTab file to PBX](#)
- [Step 3. Import users from AD](#)
- [Step 4. Active Directory SSO](#)
  - [Browser configuration](#)

### Step 1. Generate KeyTab file in Active Directory

- Go to Active Directory Users and Computers -> Computers
- Create a new computer account. Note, that this account should not contain a user with the same name



- To create KeyTab file and check spn (service principal name) binding to the computer account, run the following commands with Domain Admin privileges:

```

ktpass -princ HTTP/some-name.example.com@EXAMPLE.COM -mapuser some-name$@EXAMPLE.COM -crypto ALL -ptype
KRB5_NT_SRV_HST +rndpass -out d:\some-name.keytab
Reset SOME-NAME's password [y/n]? y
setspn -Q HTTP/some-name.example.com

```

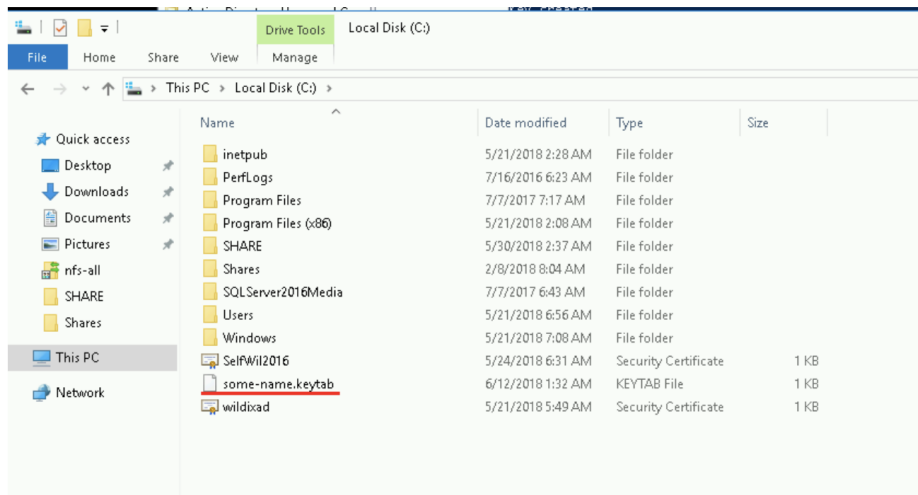
where

some-name\$@EXAMPLE.COM - the computer's name in the asset directory (with \$)

+ rndpass - the password that is generated for the computer account, where the domain is written in capital letters


If HTTP / some-name.example.com is bound to several computers or users, authentication of Kerberos will not work

- When KeyTab is generated, it appears on the disk - d: \ *some-name.keytab*:



## Step 2. Upload KeyTab file to PBX

- Go to WMS *Settings* -> *PBX* -> *Security*
- Enable *Active Directory Single SignOn via Kerberos (Negotiate)*
- Upload KeyTab file previously generated in Active Directory


 Limitation: Only "0-9", "a-z", "A-Z", "\_", " ", "@", "." characters are allowed in KeyTab file name.

- Enter Kerberos FQDN of the KeyTab. It contains encoded domain name/ IP address of PBX:

Active Directory Single SignOn via Kerberos (Negotiate)

Enable

Kerberos FQDN (not required)

glebka-test1.keytab 

Save

## Step 3. Import users from AD

In order to use AD SSO, you need to import users from Active Directory.

Consult [Documentation](#) for details.

## Step 4. Active Directory SSO

- On Windows PC, connected to Active Directory, log in to the system with a user who was previously imported to PBX
- Reach PBX via the domain name configured as Kerberos FQDN (the name must be resolved to PBX IP address). For example, glebka-test1.wildix2016.inc

 Note: Configure your browser to authenticate SSO. Refer to the next chapter [Browser configuration](#)

- If everything is set up correctly, then you log in automatically to Collaboration with the user that you are logged in to Windows PC

## Browser configuration

### Mozilla Firefox

To access Firefox settings, enter *about:config* into the Address bar and press [Enter] to open the list of customizable preferences for the current browser's installation.

You need to add FQDN of your PBX into the list of trusted URIs:

- `network.negotiate-auth.trusted-uris` - FQDN of the Server

On "Login Page" can you find the right for FQDN.

### Chrome

To access Chrome settings:

- `auth-server-whitelist` -Allowed FQDN - Set the FQDN of the IdP Server. Example:

```
chrome --auth-server-whitelist="*aai-logon.domain-a.com"
```

On "Login Page" can you find the right for FQDN.

### Opera

Opera does not currently support Kerberos authentication.