How to enable Kerberos authentication

Step-by-step

To enable the kerberos authentication method, the identity provider must have a keytab file that enables it to authenticate users. The steps to get it are described below:

1. First of all, you need to create a net user. You can use the old-fashioned but still useful net user command:

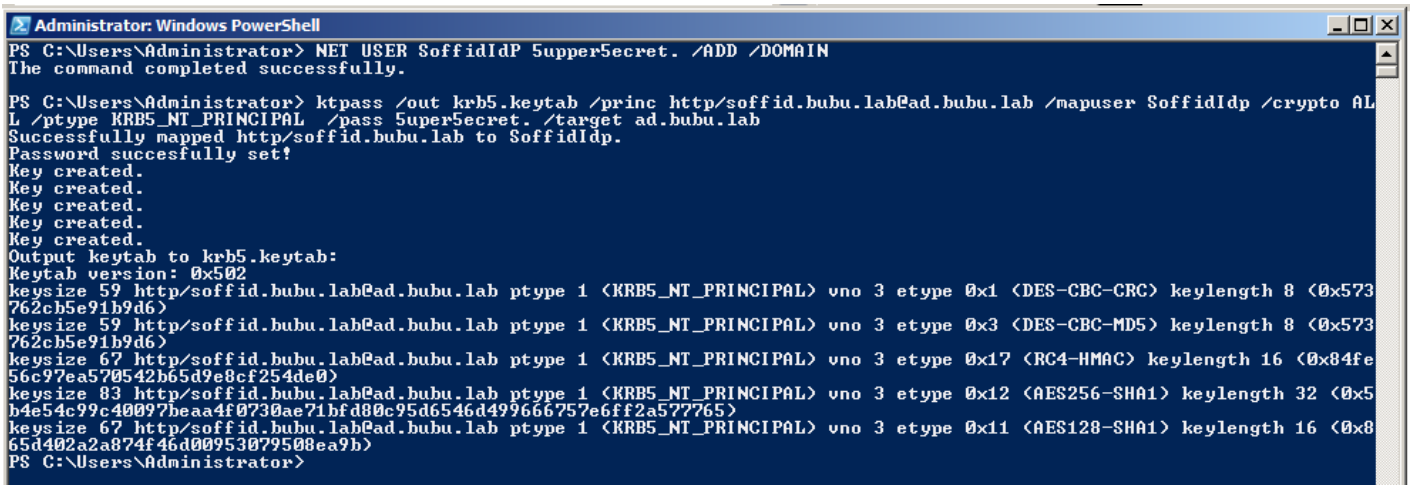
```
NET USER SoffidIdP <NewPassword> /ADD /DOMAIN
```

2. The second step will be to create a service name and generate a keytab file.

```
KTPASS /out krb5.keytab /princ HTTP/<your.idp.host.name.in.lower.case>@<YOUR.AD-DOMAIN.IN.UPPER.CASE> /mapuser SoffidIdp /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass <NewPassword> /target <YOUR.AD-DOMAIN.IN.UPPER.CASE>
```

Mind that the browser expects the server name in the URL bar matches the principal name you have just created.

Warning: It is very important to put the **domain name in uppercase**.



3. Finally, you need to add the keytab file to the identity provider configuration.

3.1. Open the Identity & Service providers page

`Main Menu > Administration > Configure Soffid > Web SSO > Identity & Service providers`

3.2. Click on the Identity Provider you are configuring. Then Soffid will display the Identity Provider detail.

3.3. On the Authentication section, on the Kerberos domain list, you can click on the add button (+) to pick up the keytab file.

3.4. Pick up the keytab file and Soffid will load automatically into the console.

Mind that the active directory agent for this domain must be successfully connected, as it is needed to translate the kerberos identity to a user name.

Revision #12
Created 20 September 2021 06:29:25
Updated 10 July 2026 11:25:28 by Sion Vives