

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:

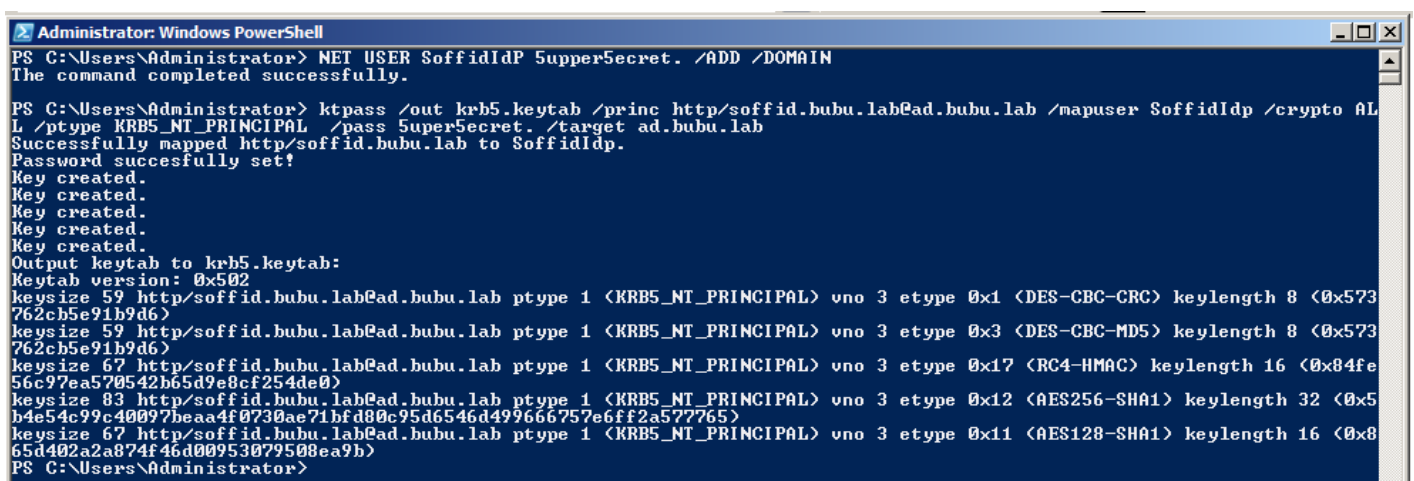
1. First of all, you need to create a net user. You can use the old-fashioned but still useful net user command:

```
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/<YourIdp.Host.Name>@<Your.Ad.Domain> /mapuser SoffidIdp /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass <NewPassword> /target <Your.AD.Domain>
```

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



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> NET USER SoffidIdP 5upper5ecret. /ADD /DOMAIN
The command completed successfully.

PS C:\Users\Administrator> ktpass /out krb5.keytab /princ http/soffid.bubu.lab@ad.bubu.lab /mapuser SoffidIdp /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass 5upper5ecret. /target ad.bubu.lab
Successfully mapped http/soffid.bubu.lab to SoffidIdp.
Password successfully set!
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to krb5.keytab:
Keytab version: 0x502
keysize 59 http/soffid.bubu.lab@ad.bubu.lab ptype 1 <KRB5_NT_PRINCIPAL> vno 3 etype 0x1 <DES-CBC-CRC> keylength 8 <0x573762cb5e91b9d6>
keysize 59 http/soffid.bubu.lab@ad.bubu.lab ptype 1 <KRB5_NT_PRINCIPAL> vno 3 etype 0x3 <DES-CBC-MD5> keylength 8 <0x573762cb5e91b9d6>
keysize 67 http/soffid.bubu.lab@ad.bubu.lab ptype 1 <KRB5_NT_PRINCIPAL> vno 3 etype 0x17 <RC4-HMAC> keylength 16 <0x84fe56c977ea570542b65d9e8cf254de0>
keysize 83 http/soffid.bubu.lab@ad.bubu.lab ptype 1 <KRB5_NT_PRINCIPAL> vno 3 etype 0x12 <AES256-SHA1> keylength 32 <0x5b4e54c99c40097beaa4f0730ae71bfd80c95d6546d499666757e6ff2a577765>
keysize 67 http/soffid.bubu.lab@ad.bubu.lab ptype 1 <KRB5_NT_PRINCIPAL> vno 3 etype 0x11 <AES128-SHA1> keylength 16 <0x865d402a2a874f46d00953079508ea9b>
PS C:\Users\Administrator>
```

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

3.1. Open the Identity & Service providers page

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 #9

Created 20 September 2021 06:29:25 by pgarcia@soffid.com

Updated 13 September 2024 09:25:01 by Gabriel Buades