SSO Spark Setup

Author: Benjamin Dreher

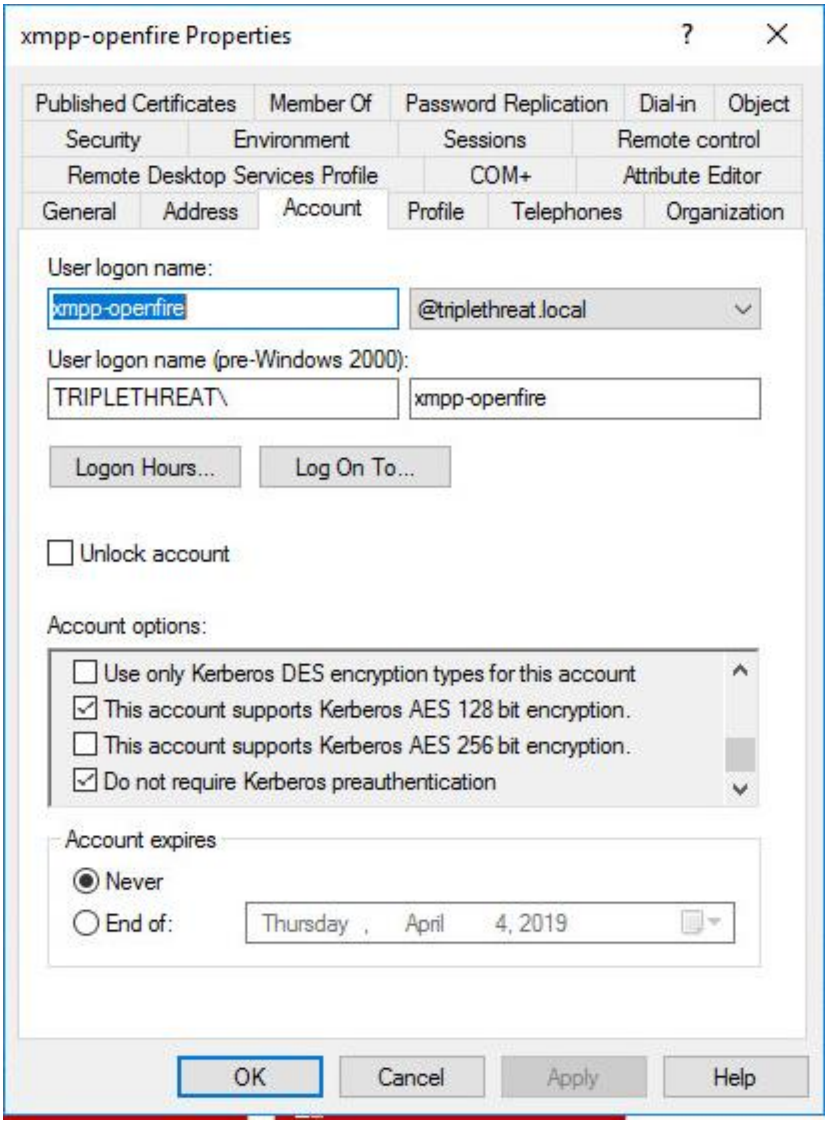
Overview: This guide shows how to set up SSO (single sign-on) for the Spark IM client. Openfire uses Kerberos, which is a common authentication protocol for networks. TCP and UDP port 88 is required for Kerberos.

Kerberos AD Account for Openfire SSO

Username: xmpp-openfire

Password: Alpha238!

User cannot change pw, pw never expires, disable Kerberos preauthentication, enable AES 128-bit Kerberos authentication



xmpp-openfire Properties

User logon name: xmpp-openfire @triplethreat.local

User logon name (pre-Windows 2000): TRIPLETHREAT\ xmpp-openfire

□ Unlock account

Account options:

□ Use only Kerberos DES encryption types for this account
☑ This account supports Kerberos AES 128 bit encryption.
□ This account supports Kerberos AES 256 bit encryption.
☑ Do not require Kerberos preauthentication

Account expires
● Never
○ End of: Thursday , April 4, 2019

Kerberos XMPP Service Principle Name (SPN):
xmpp/openfire.triplethreat.local@TRIPLETHREAT.LOCAL

Create a Kerberos XMPP SPN for the Kerberos XMPP AD account.

Setspn.exe command to set SPN:

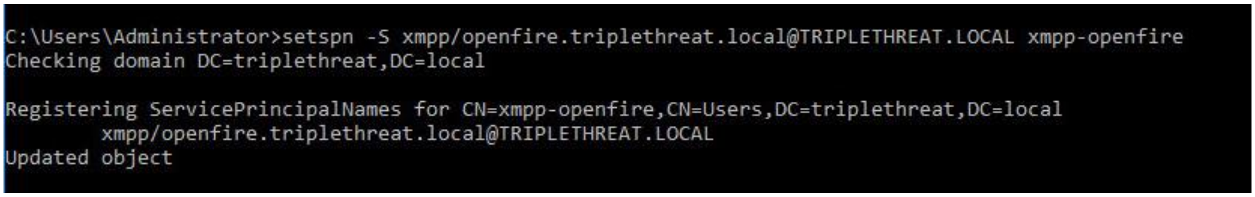
setspn -S xmpp/openfire.triplethreat.local@TRIPLETHREAT.LOCAL xmpp-openfire

Service: xmpp

FQDN: openfire.triplethreat.local

Realm: TRIPLETHREAT.LOCAL

Kerberos AD Account: xmpp-openfire



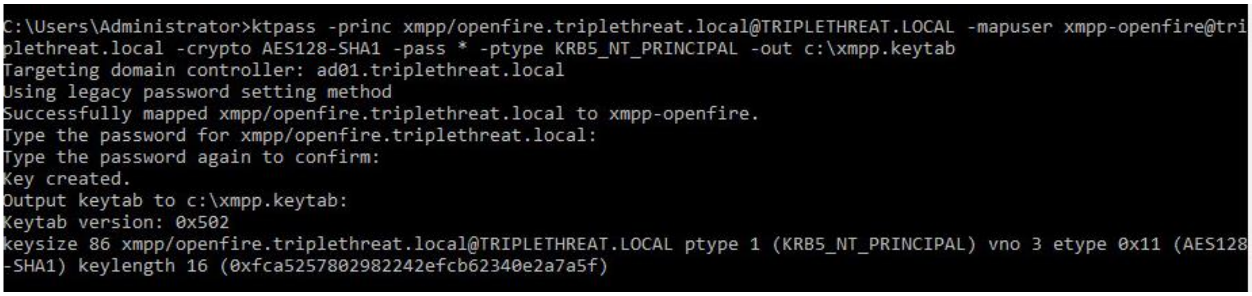
```
C:\Users\Administrator>setspn -S xmpp/openfire.triplethreat.local@TRIPLETHREAT.LOCAL xmpp-openfire
Checking domain DC=triplethreat,DC=local

Registering ServicePrincipalNames for CN=xmpp-openfire,CN=Users,DC=triplethreat,DC=local
        xmpp/openfire.triplethreat.local@TRIPLETHREAT.LOCAL
Updated object
```

Now we must use the ktpass.exe tool to map the newly created Kerberos XMPP SPN to the Kerberos AD account.

Ktpass -princ xmpp/openfire.triplethreat.local@TRIPLETHREAT.LOCAL -mapuser xmpp-openfire@triplethreat.local -crypto AES128-SHA1 -pass * -ptype KRB5__NT_PRINCIPAL -out c:\xmpp.keytab

We're using AES128-SHA1 cryptography (supported in Windows server 2016, and we checked this option for this account earlier in AD for xmpp-openfire). Kerberos 5 version. We outputted the keytab to the root of C and called it xmpp.keytab.

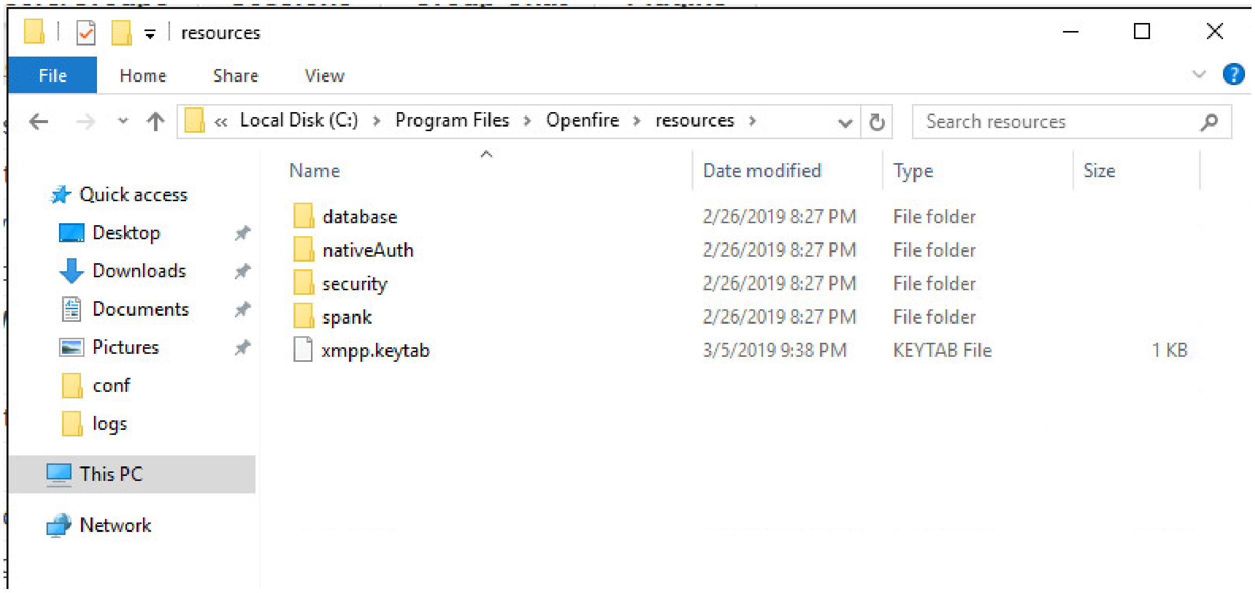


```
C:\Users\Administrator>ktpass -princ xmpp/openfire.triplethreat.local@TRIPLETHREAT.LOCAL -mapuser xmpp-openfire@tri
plethreat.local -crypto AES128-SHA1 -pass * -ptype KRB5_NT_PRINCIPAL -out c:\xmpp.keytab
Targeting domain controller: ad01.triplethreat.local
Using legacy password setting method
Successfully mapped xmpp/openfire.triplethreat.local to xmpp-openfire.
Type the password for xmpp/openfire.triplethreat.local:
Type the password again to confirm:
Key created.
Output keytab to c:\xmpp.keytab:
Keytab version: 0x502
keysize 86 xmpp/openfire.triplethreat.local@TRIPLETHREAT.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x11 (AES128
-SHA1) keylength 16 (0xfca5257802982242efcb62340e2a7a5f)
```

We successfully mapped the Kerberos XMPP SPN to the Kerberos XMPP AD account and created the keytab, which contains the password for the Kerberos XMPP service principal.

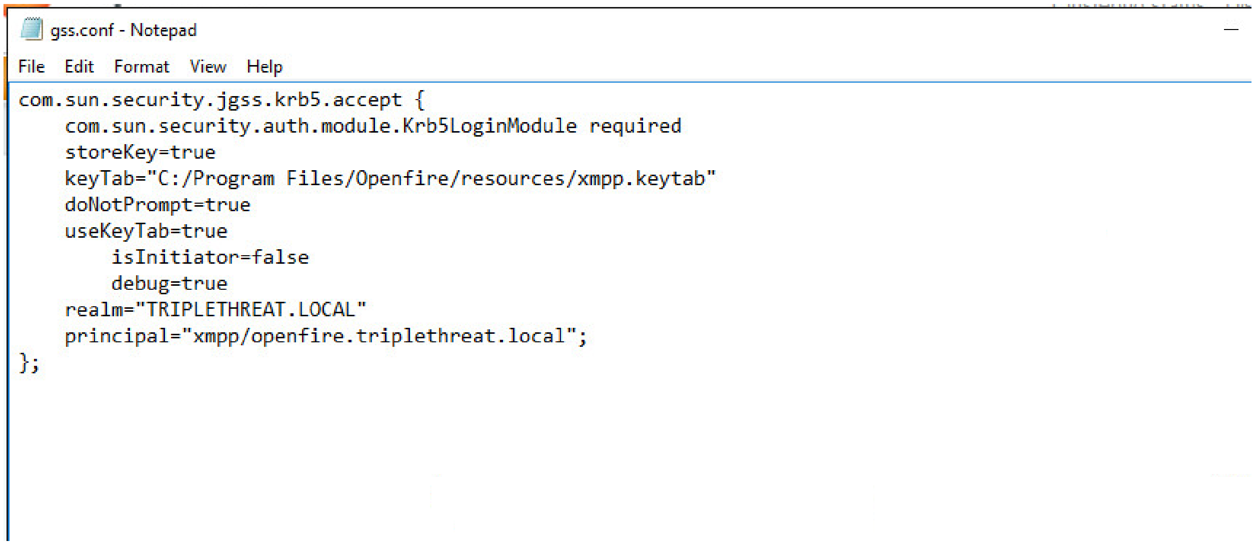
Source for terms: https://discourse.igniterealtime.org/t/sso-configuration/49064

Put the keytab in the Openfire installation resources folder:



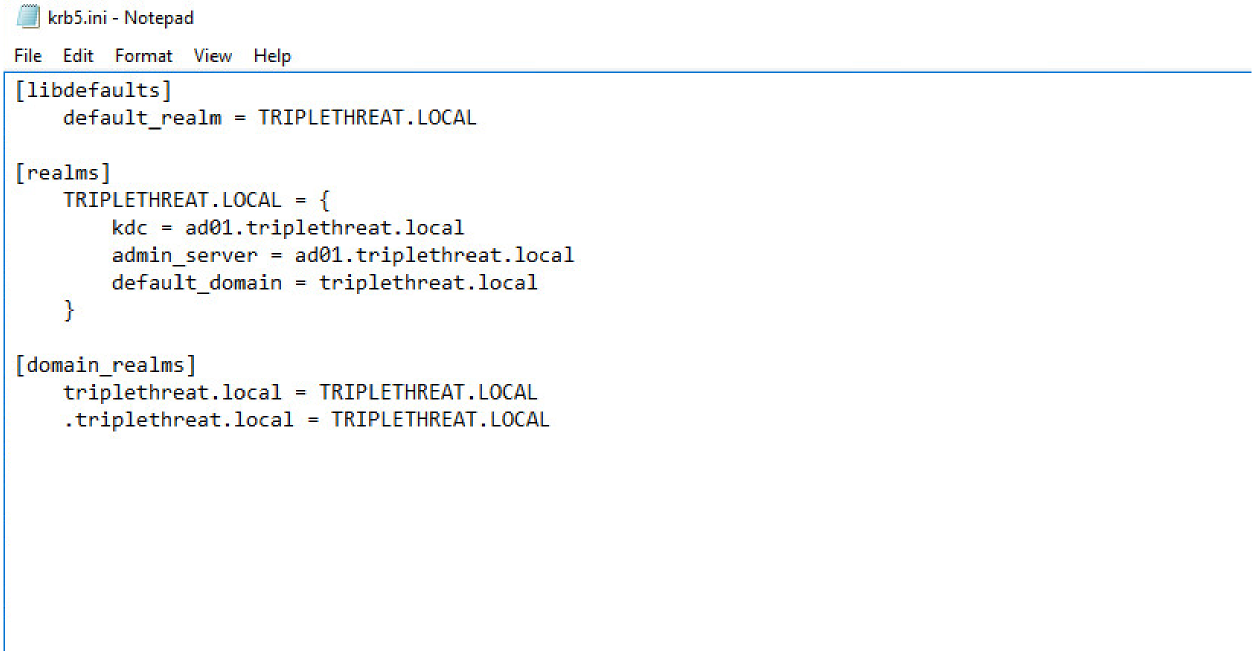
Name	Date modified	Type	Size
database	2/26/2019 8:27 PM	File folder	
nativeAuth	2/26/2019 8:27 PM	File folder	
security	2/26/2019 8:27 PM	File folder	
spank	2/26/2019 8:27 PM	File folder	
xmpp.keytab	3/5/2019 9:38 PM	KEYTAB File	1 KB

Put the gss.conf configuration file in the Openfire installation conf folder



```
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
    storeKey=true
    keyTab="C:/Program Files/Openfire/resources/xmpp.keytab"
    doNotPrompt=true
    useKeyTab=true
        isInitiator=false
        debug=true
    realm="TRIPLETHREAT.LOCAL"
    principal="xmpp/openfire.triplethreat.local";
};
```

Put the krb5.ini file in the C:\Windows directory

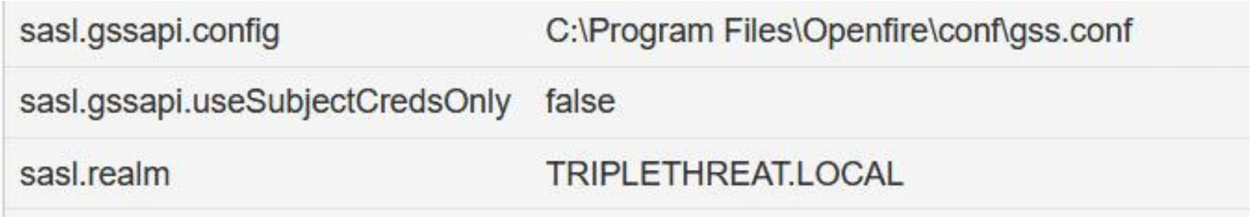


```
[libdefaults]
    default_realm = TRIPLETHREAT.LOCAL

[realms]
    TRIPLETHREAT.LOCAL = {
        kdc = ad01.triplethreat.local
        admin_server = ad01.triplethreat.local
        default_domain = triplethreat.local
    }

[domain_realms]
    triplethreat.local = TRIPLETHREAT.LOCAL
    .triplethreat.local = TRIPLETHREAT.LOCAL
```

We added three properties under the Openfire Admin Console System Properties page:



sasl.gssapi.config	C:\Program Files\Openfire\conf\gss.conf
sasl.gssapi.useSubjectCredsOnly	false
sasl.realm	TRIPLETHREAT.LOCAL

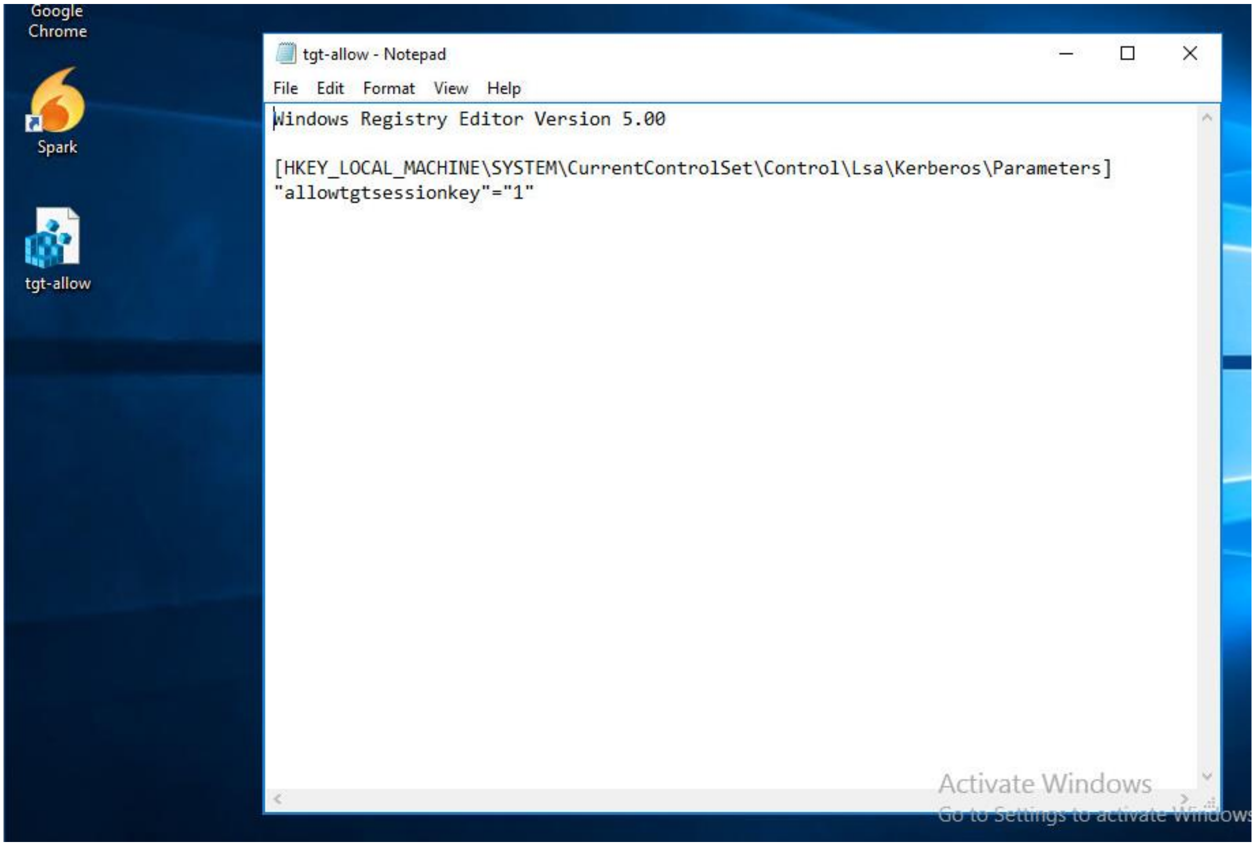
Now go to Server Setting -> Registration & Login

Only enable GSSAPI (this is for the Kerberos 5 SASL authentication we set up for SSO)

The Spark client has to be able to view the krb5 session keys.

Follow this Microsoft article to allow Kerberos tgt session keys by editing the registry (Windows Server 2016):

https://support.microsoft.com/en-us/help/308339/registry-key-to-allow-session-keys-to-be-sent-in-kerberos-ticket-grant



```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"allowtgtsessionkey"="1"
```

References:

- https://discourse.igniterealtime.org/t/sso-configuration/49064
- https://discourse.igniterealtime.org/t/how-to-video-on-setting-up-sso-ad-with-openfire/79384