Single Sign-On

Bitte beachten Sie, dass dies eine lizenzpflichtige Funktion ist. Sollten Sie keine entsprechende Lizenz erworben haben, wenden Sie sich bitte an Ihren Account Manager.

Hier können Sie die Funktion: Single Sign-On aktivieren.

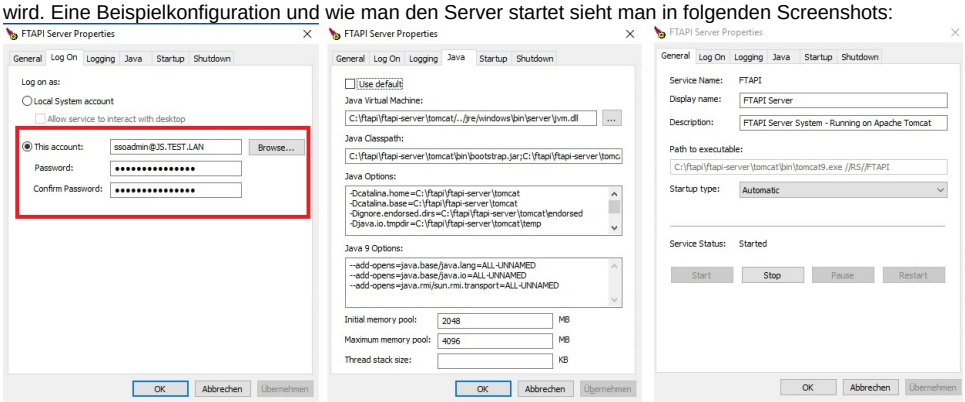
Um Single Sign-On nutzen zu können, müssen mehrere Schritte erledigt werden.

FTAPI-Server

1. Der FTAPI-Server muss auf einem Windowsaccount (und damit auch auf Windows) laufen, der Teil des Active Directory ist. Es bietet sich daher an, einen eigenen Domänenaccount für den Server anzulegen. In folgenden Beispielen heißt dieser Account *ssoadmin* und ist Teil der Domäne *JS.TEST.LAN.*

   Zudem muss der FTAPI-Server bzw. die Tomcat als Windows-Dienst laufen (.bat-File/.exe-File ist **nicht** ausreichend!).

   Dieser Dienst muss zudem explizit einen Benutzeraccount der Domäne benutzen. Es empfiehlt sich, den FTAPI-Server über die Tomcat GUI zu starten, diese befindet sich im Tomcat Ordner unter bin\Tomcat9w.exe. Eventuell muss diese Datei in FTAPIw.exe umbenannt werden, damit der FTAPI Tomcat Service gefunden wird.
   Es muss darauf geachtet werden, dass der Server von der GUI aus mit den richtigen Parametern (DB-Adresse/IP, DB Passwort, etc.) gestartet wird. Eine Beispielkonfiguration und wie man den Server startet sieht man in folgenden Screenshots:



2. **Konfiguration des Active Directorys**
   Im FTAPI-Server muss zuerst ein gültiges Active Directory konfiguriert werden. Diese Einstellungen sind unter Administration System LDAP and Active Directory zu finden. Ein Neustart des Servers ist nach dem Speichern nötig.
   Um zu testen, dass das Active Directory richtig konfiguriert ist, kann man versuchen, sich mit einem Account aus eben diesem Active Directory beim FTAPI-Server anmelden.

3. **Aktivierung des Single-Sign Ons**
   Diese Einstellung ist unter Administration System Single Sign-On zu finden. Dort muss der Single Sign-On lediglich aktiviert werden.
   Ab jetzt wird auf der Loginseite des FTAPI-Servers der Button für den SSO angezeigt.

Active Directory

1. **Konfigurieren eines SPNs**
   Öffnen von cmd.exe als Domänenadministrator

   "setspn -A HTTP/[ServerURL]:[port] [tomcatusername]"
   wobei
   -[ServerURL] für die URL Ihres FTAPI Servers, (in unserem Fall testldap.ftapi.com)
   - [port] für den Port den der Tomcat Server benutzt steht (in unserem Fall 443)
   - [tomcatusername] für den Domänenaccount auf dem der Server läuft (in unserem Fall ssoadmin) steht
   Es empfiehlt sich zudem, den gleichen SPN nochmals hinzuzufügen, allerdings **ohne** die Portangabe.
   Wir führen also folgende Befehle aus:

   ```
   setspn -A HTTP/testldap.ftapi.com:443 ssoadmin
   setspn -A HTTP/testldap.ftapi.com ssoadmin
   ```

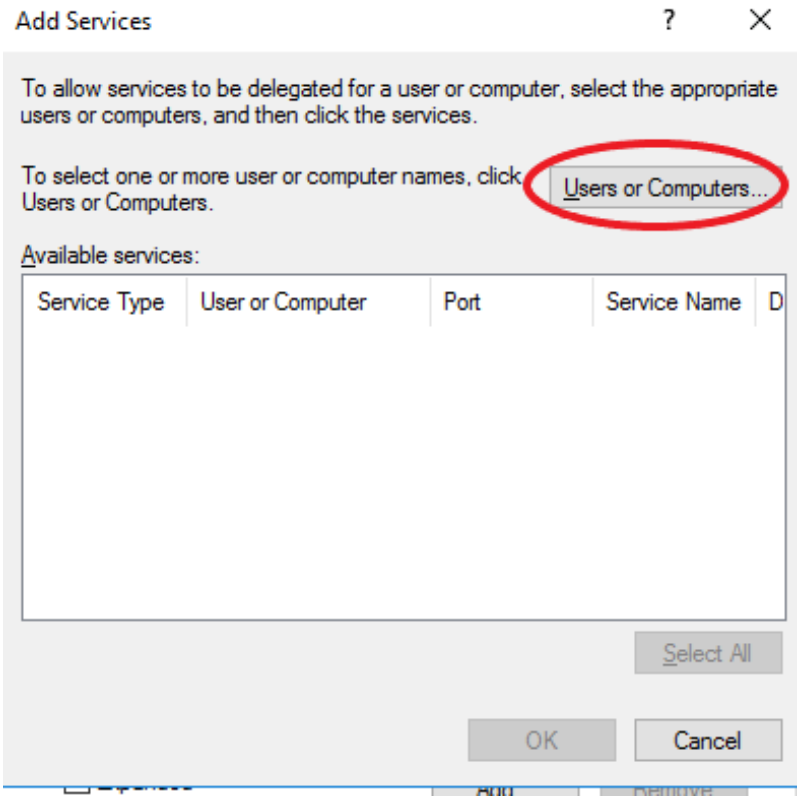
   Die Liste der SPNs (zum Nachprüfen) kann sich dann mittels

   ```
   setspn -l ssoadmin
   ```

   angezeigt werden lassen.

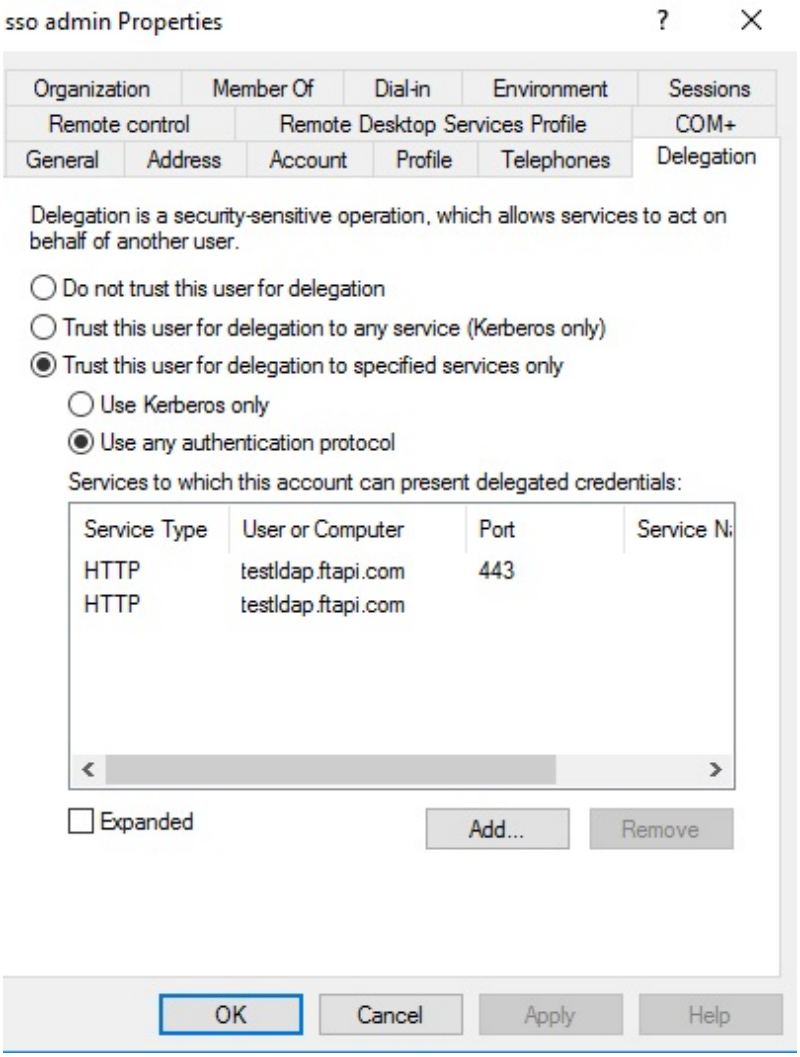
   ```
   C:\Windows\system32>setspn -l ssoadmin
   Registrierte Dienstprinzipalnamen (SPN) für CN=sso admin,CN=Users,DC=JS,DC=TEST,DC=LAN:
          HTTP/testldap.ftapi.com
          HTTP/testldap.ftapi.com:443
   ```

1. **Windows-Delegationzulassen**
   Dazu wird die Active Directory Benutzer und Computer Konsole (Ausführen (WIN+R) dsa.msc) geöffnet und anschließend der Benutzer auf dem Tomcat läuft gesucht und ein Doppelklick drauf gemacht.
   Dann öffnet man den Tab Delegation, danach kreuzt man "Trust this user for delegation to specified services only" und "Use any authentication protocol" an und klickt auf "Add".
   Folgender Dialog erscheint:

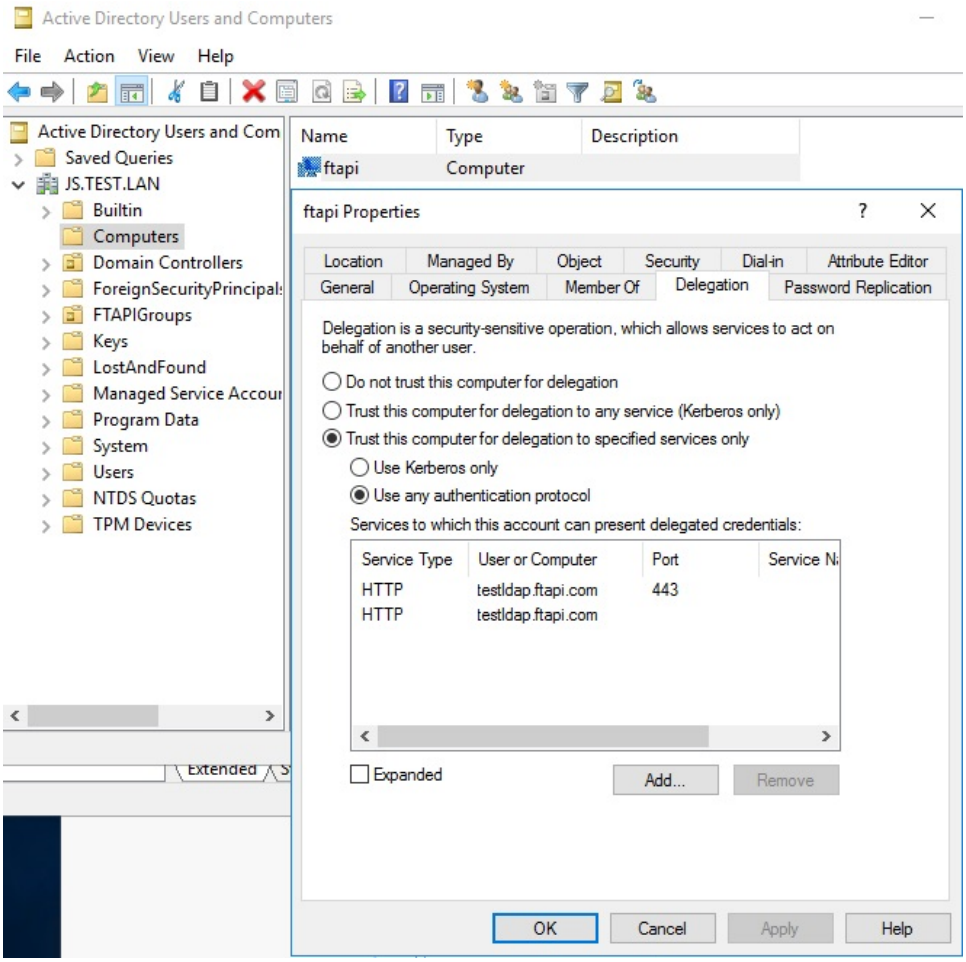


   Dort klickt man auf "Users or Computers" und tippt den Usernamen des Konto auf dem Tomcat läuft ein (in unserem Fall ssotomcat) und drückt Enter.
   Anschließend sollten die eben im ersten Schritt angelegten SPNs angezeigt werden.

   Man klickt "Select All" und bestätigt mit OK. Das Ergebnis sollte so aussehen:



Exakt das selbe Prozedere wird nun mit dem Computer ausgeführt, auf dem Tomcat läuft. Dazu geht man auf den Tab Computer in der Users and Computers Konsole und führt die selben Schritte aus.
Das Ergebnis sieht dann so aus:



Client (Browsereinstellungen)

1. Für die korrekte Einrichtung der Browser wird auf https://github.com/Waffle/waffle/blob/master/Docs/ConfiguringBrowsers.md verwiesen. Zu beachten ist, dass Google Chrome die Internet Explorer Einstellungen benutzt, d.h. es empfiehlt sich in jedem Fall den Internet Explorer richtig zu konfigurieren, damit Google Chrome funktioniert.

Sammlung von bekannten Konfigurationsfehlern

- Falls der Nutzer dazu aufgefordert wird, Username und Passwort einzugeben, hat Kerberos nicht funktioniert. Dies hat vielfältige Gründe, es empfiehlt sich in dem Fall die Konfiguration von oben nochmals durchzugehen und Kerberos- und NTML-Logging zu aktivieren (siehe https://support.microsoft.com/en-us/help/262177/how-to-enable-kerberos-event-logging und https://support.symantec.com/en_US/article.HOWTO79508.html) Anschließend sind bei einer fehlerhaften Kerberos Authentifizierung Einträge in der Windows Ereignisanzeige zu finden. Sowohl auf dem Domänenserver, als auch auf dem Benutzerauf dem FTAPI läuft und auf dem Client-PC.
- der Nutzer, der sich über SSO anmeldet, muss eine Mail Adresse im Active Directory hinterlegt haben
- der Server muss ein korrektes SSL-Zertifikat haben