KB1202 – WebFront for Service Manager – Permissions Denied

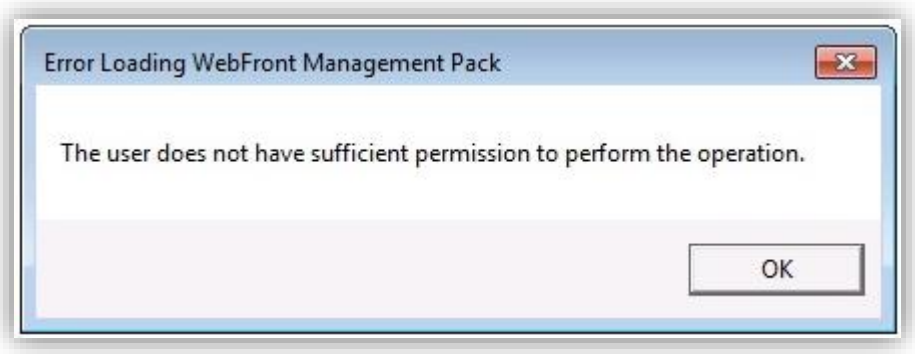
Knowledge Article: Service Principal Names and Kerberos Delegation

Product: WebFront for Service Manager

Note: This is only relevant for scenarios where WebFront is installed on a dedicated server (not on the management server it is configured to work against) WebFront.

SYMPTOM

When accessing WebFront from a remote computer (not “localhost”) an error message occurs during the initial load process with an error message saying “The user does not have sufficient permission to perform the operation”.



CAUSE

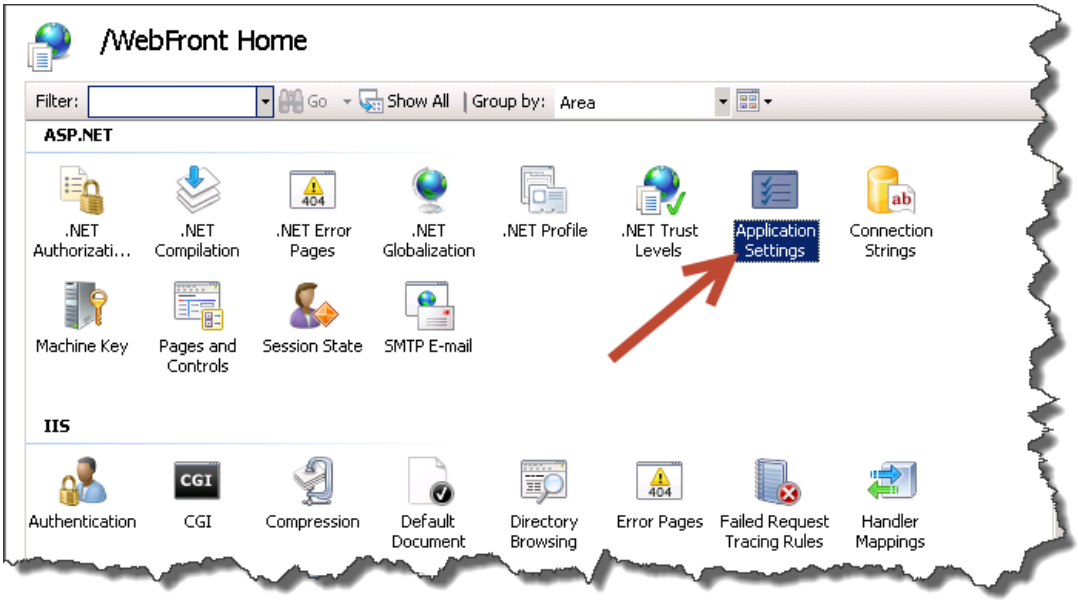
If the user has the required permissions in Service Manager so he/she has the ability to run the standard console, but still receives the error message in WebFront for Service Manager this is most probably caused by an incorrect configuration of Kerberos Delegation.

To further ensure that this is related to Kerberos Delegation, make sure that running WebFront using “localhost”, as the server name locally on the WebFront server, is working correctly (not showing the error message).

TROUBLESHOOTING

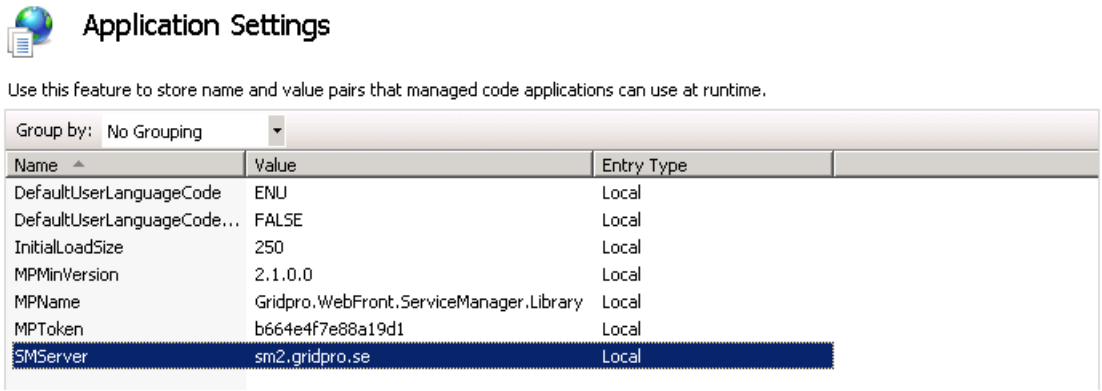
On each WebFront for Service Manager server, go to IIS Manager.

Go to the WebFront application and open up Application Settings (see image below).



Make sure the server name stated in the **SMServer** entry is the intended server name.

Make a note of the server name (in our case sm2.gridpro.se).



The first requirement for delegation to work is the Service Principal Names (SPN) are configured correctly for the server accessed by WebFront. To find out the current configuration, execute the following command in a command prompt on the WebFront server:

```
setspn -q MSOMSdkSvc/*
```

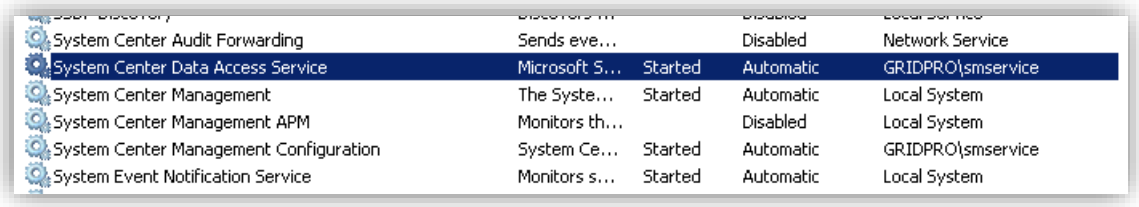
The output should look something like:

```
Checking domain DC=gridpro,DC=se

CN=SM Service,OU=Services,OU=Production,DC=gridpro,DC=se
      MSOMSdkSvc/SM2.gridpro.se
      MSOMSdkSvc/SM2


Existing SPN found!
```

This tells us that “SDK Service SPN” for server “sm2.gridpro.se” is registered on the service account “CN=SM Service,OU=Services,OU=Production,DC=gridpro,DC=se”. This is correct when the service account in the output is the account used by the System Center Data Access Service (SDK Service) as seen in the image below.



Three things could be wrong when it comes to SPNs, Kerberos Delegation and WebFront. The SPN could be missing, registered on the wrong account or registered on multiple accounts.

Service Principal Name Not Registered

If the SPN isn’t registered at all you’ll receive the output “No such SPN found”. To fix this you need to register the SPNs.
Note: Always register SPNs both for the Fully Qualified Domain Name and the NetBIOS name.

Use the commands below to register an SPN for the Service Manager SDK service:

```
setspn -A MSOMSdkSvc/sm2.gridpro.se gridpro\smservice

setspn -A MSOMSdkSvc/sm2 gridpro\smservice
```

Where “sm2.gridpro.se” should be replaced by the fully qualified domain name of the management server used by your WebFront server. And sm2 (second command) should be replaced by the NetBIOS name of the same server.

Service Principal Name registered on the wrong account

The second thing that could be wrong is that you have SPNs configured for the service but they are configured on a different account than the one used by the System Center Data Access Service. A common cause for this is if the Service Manager Service account has domain admin privileges (commonly seen in lab/demo environments) since the service account inaccurately registers the SPN on the management server’s computer object (in our case the **SM2$**). If this was the case the output would have been:

```
Checking domain DC=gridpro,DC=se

CN=sm2,OU=Servers,OU=Production,DC=gridpro,DC=se
      MSOMSdkSvc/SM2.gridpro.se
      MSOMSdkSvc/SM2


Existing SPN found!
```

To fix this we need to remove the incorrect SPN and add the correct ones. To remove an SPN:

```
setspn -D MSOMSdkSvc/sm2.gridpro.se gridpro\sm2$
```

To add the correct SPN follow the instructions in section “Service Principal Name Not Registered”.

Duplicate Service Principal Names

If for any reason you should end up with multiple registrations of the same SPN (but on different accounts) this will also make Kerberos delegation to fail. This could happen in environments where you've installed and re-installed Service Manager and having the different installations using different service accounts.

The way to detect if you have duplicate SPNs is to see if the current configuration contains registration on multiple accounts as seen in the output below where the SPN for our management server is registered on the correct service account and the machine account (of our management server):

```
Checking domain DC=gridpro,DC=se

CN=SM Service,OU=Services,OU=Production,DC=gridpro,DC=se
      MSOMSdkSvc/SM2.gridpro.se
      MSOMSdkSvc/SM2
CN=sm2,OU=Servers,OU=Production,DC=gridpro,DC=se
      MSOMSdkSvc/SM2.gridpro.se
      MSOMSdkSvc/SM2

Existing SPN found!
```

Since in this example the Service Manager Data Access Service is running under the "SM Service" account we need to remove the registrations on the "sm2" machine account. To fix this problem we need to run the following two command lines:

```
setspn -D MSOMSdkSvc/sm2.gridpro.se gridpro\sm2$

setspn -D MSOMSdkSvc/sm2 gridpro\sm2$
```

CONFIGURING DELEGATION

When your SPNs are in order you can continue to configure Kerberos delegation as described in the Administrations Guide, in the section called "Active Directory Configuration (Only remote installation)".