Kerberos Configuration Manager for IIS Server

learn.microsoft.com/en-us/archive/blogs/surajdixit/kerberos-configuration-manager-for-internet-information-services-server

- Article
- 02/07/2018

Many of us find troubleshooting Kerberos configured for a website on IIS Server quite a tedious task since it involves multiple levels of troubleshooting. This blog is meant to demystify the art of troubleshooting Kerberos on IIS Server.

Why is Kerberos painful at times?

1. First, understanding Kerberos is quite tricky.
2. Configuration takes a lot of time as we need to look at configuration of IIS server, Domain controller and Client side.
3. Once a site breaks because of some configuration related issues, it's really difficult to identify the exact cause because of the complexity.

Let's see what exactly happens "Under the Hood":

At a high level, the following steps needs to be followed to configure Kerberos for a website:

On IIS Server:

1. Disable all the authentication methods except windows authentication
2. In windows authentication section, in Providers we should see negotiate should be a priority
3. ASP.NET Impersonation should enabled if you want to configure Pass-through Authentication(Kerberos double hop)
4. Based on the Application pool credentials,
    - useAppPoolCredentials to true if we are using a custom account
    - useAppPoolCredentials to false and useKernelMode to true if we are using a machine account

On Domain Controller:

1. Based on the Application pool credentials on the IIS we set Service Principle names on the DC.
    - If we use a Machine account, set SPNs on Machine account
    - If we use a custom account, set SPNs on custom account
2. The above also depends on whether we are using a hostname or machine name to browse the website

3. Delegation need to be enabled for the Application pool credentials if you want configure pass-through authentication (This tab will come up after we set the SPNs).

On Client Browser(Internet Explorer):

Based on whether we use hostname or not, we need to add the host/machine name to Trusted sites/Local Intranet Zone.

You can find more information regarding Configuration of Kerberos in the following blogs:

1. https://blogs.msdn.microsoft.com/chiranth/2013/09/20/all-about-kerberos-the-three-headed-dog-with-respect-to-iis-and-sql/
2. https://blogs.msdn.microsoft.com/chiranth/2014/04/17/setting-up-kerberos-authentication-for-a-website-in-iis/

Now just imagine if we can automate the above process through a nifty application which can help us troubleshoot/configure Kerberos in just a few minutes – Is it possible? The good news is that **NOW IT IS POSSIBLE :)**

I have developed a simple troubleshooter "**Kerberos Configuration Manager for IIS**" which allows one to do the following tasks on the server:

1. Review the current settings related to Kerberos for any specific website in IIS.
    - Checks and displays the site properties
    - Checks and displays Application pool properties like Application pool identity
    - Checks and displays Anonymous authentication properties
    - Checks and displays Basic authentication properties
    - Checks and displays Digest authentication properties
    - Checks and displays ASP.NET Impersonation properties
    - Checks and displays Windows authentication
        - whether Windows authentication is enabled or disabled
        - What are the Providers settings
    - Checks and displays Configuration editor settings for windows authentication
        - UseAppPoolCredentials settings
        - UseKernelMode settings
    - Based on the Application pool identity,
        - Checks for the existing SPNs for that identity and displays them
        - Displays the necessary SPNs required for Kerberos to work
        - Checks and displays existing Delegation settings in case you want to go with the Pass-through authentication.
        - Displays the necessary Delegation settings in case you want to go with the Pass-through authentication.

2. Configures Kerberos for the affected website:
    - Disables Anonymous authentication if enabled
    - Disables Basic authentication if enabled
    - Disables Digest authentication if enabled
    - Disables ASP.NET Impersonation if enabled
    - Enables Windows authentication if disabled

        Once the above is enabled, checks whether we have Negotiate on priority or no. If not, Negotiate is moved to the top
    - Based on the application pool credentials,
        - Either it will enable useAppPoolCredentials or disables it
        - Either it will enable useKernelMode or disables it
    - Based on the Application pool identity,
        - Checks for the existing SPNs for that identity and displays them
        - Displays the necessary SPNs required for Kerberos to work
        - Checks and displays existing Delegation settings in case you want to go with the Pass-through authentication.
        - Displays the necessary Delegation settings in case you want to go with the Pass-through authentication.
    - Generates the script for setting the required SPNs in the same directory if you want to configure single hop
    - Generates the script for setting the required SPNs and setting the delegation properties for the application pool identity in the same directory if you want to configure Pass-through authentication.

3. It also has a provision to revert the changes made just in case there is a requirement.
4. It also has a feature of auditing through a log file which would capture the below details:
    - Logged in user who used the tool and made changes
    - Timestamp when the changes were made
    - Review, Configure and Revert logs (All settings which were added/modified)

The good news is that we have released the Kerberos Configuration Manager v2.0 which supports **reviewing and configuring the Kerberos Pass-through authentication** also (Kerberos Double Hop).

Whats new in Kerberos Configuration Manager v2.0 ?

1. Double Hop Support - Delegation and Impersonation
2. UI changes
3. Scroll view for the text area
4. Application can run as administrator without any intervention
5. Bug fixes

Why should I use tool?:

1. Troubleshooting Kerberos just becomes much simpler with this tool and it optimizes the time taken to troubleshoot from few hours to few minutes.
2. You can review the Kerberos Configuration for any of your web sites and share the generated log files with support to save precious troubleshooting time.
3. No need to install the tool - it's a standalone executable.
4. Disk space utilization is minimal.
5. Open source, free to download and modify.
6. Auditing support which makes troubleshooting Kerberos easier.

Where do I get it from and how do I use it?

The tool can be downloaded from the open source github repo:

Latest release:
https://github.com/SurajDixit/KerberosConfigMgrIIS/releases/download/v2.1/KerberosConfigMgrIIS.exe

All releases : https://github.com/SurajDixit/KerberosConfigMgrIIS/releases

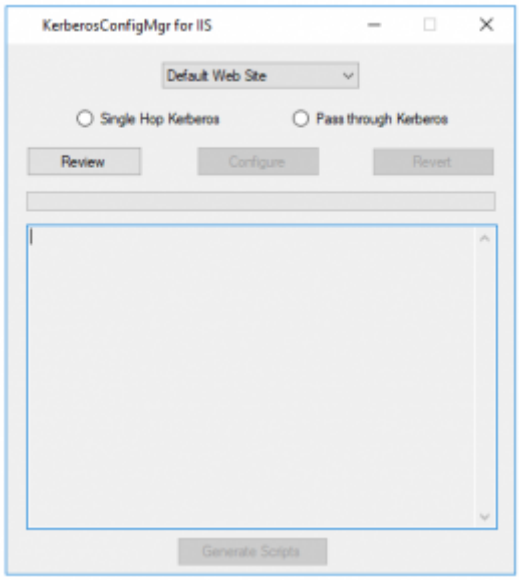
The GUI has a fairly simple layout with the options to Review, Configure, Generate Script and Revert the Kerberos related configuration settings.

Instructions for use:

- Create a folder called KCMI on the server where **IIS** is installed and copy the executable file "KerberosConfigMgrIIS.exe".
- Run the executable "KerberosConfigMgrIIS.exe".
- When you execute the file, you will see the below screen:

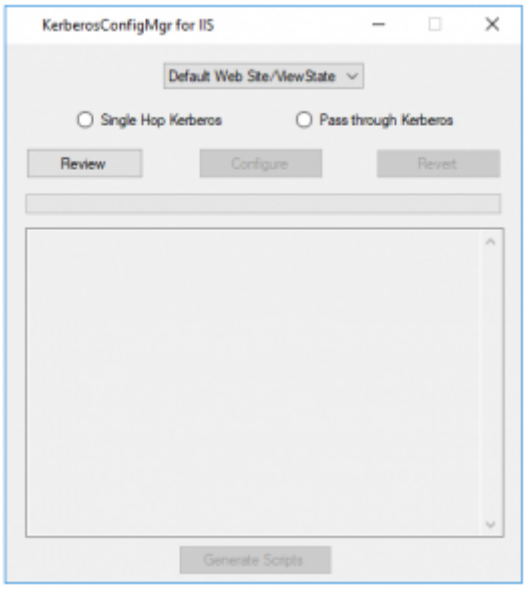
Select the website from the drop down menu for which you want to configure Kerberos.

Now select from the Radio buttons whether you want to configure the website for Single Hop or Double Hop(Pass Through Authentication) and click on Review.



- Once you click on the Review button you will see the current Kerberos configuration for the selected website.
- In-between you will see the Dialogue which is shown below to ask whether we are making use of "Hostname" to browse the website?

If we click “Yes”, we will see one more Dialogue box to input the hostname. If we click “No”, we don’t see any dialogue box and execution will continue.



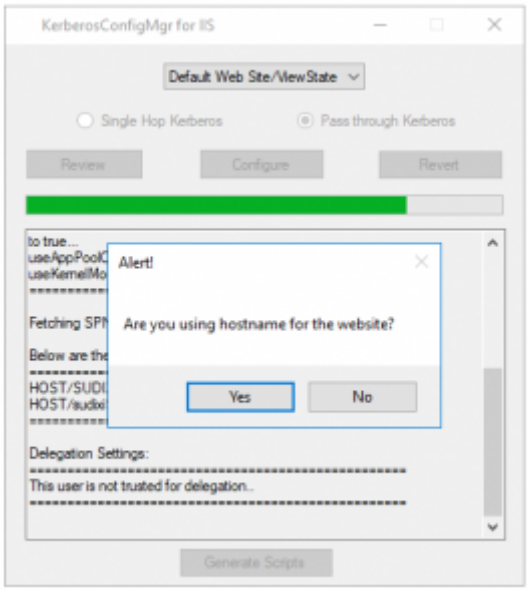
The Kerberos configuration would show all the recommended and non-recommended settings. Please review it carefully.

Once you have reviewed the setting and you are ready to “Fix” the problem, please click on “Configure” button to make the necessary changes.

Once the configuration is implemented, you will see 2 buttons enabled, One is Generate script and other is Revert. Also you will notice that the dropped down will be locked so that we don’t revert the changes for a wrong site by mistake.

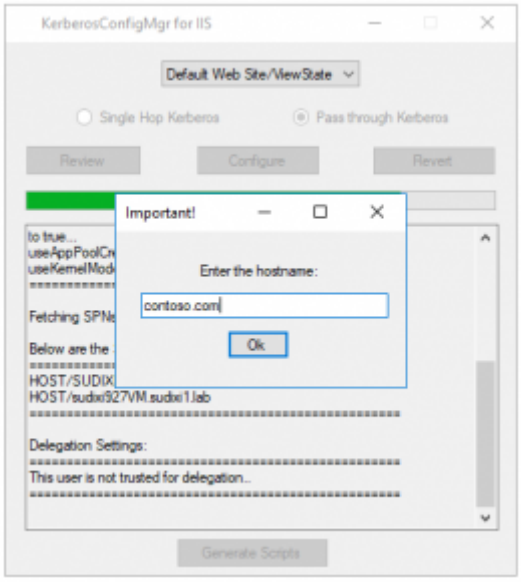
Once you click the Generate Script you will see a .cmd file and .ps1 file (Only if you have selected Pass-Though authentication) in the current folder which has the commands to add SPNs and Set the delegation for the application pool identity user on the Domain controller.

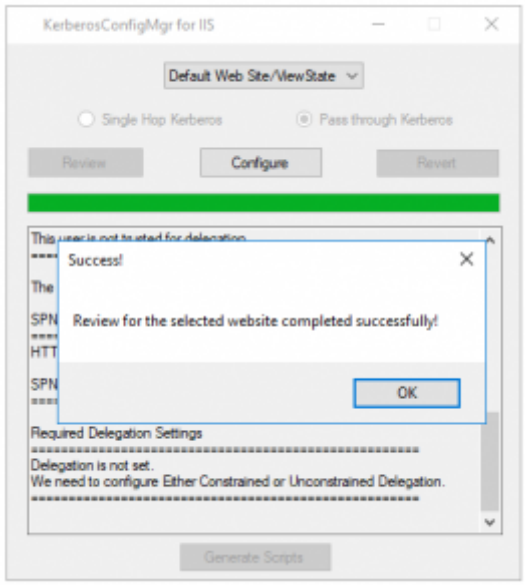
In case you want to revert the changes, simply click on “Revert” button and all the changes which were made earlier will be reverted back with respect to IIS (Note: If you have executed the .cmd file, it will not be reverted).

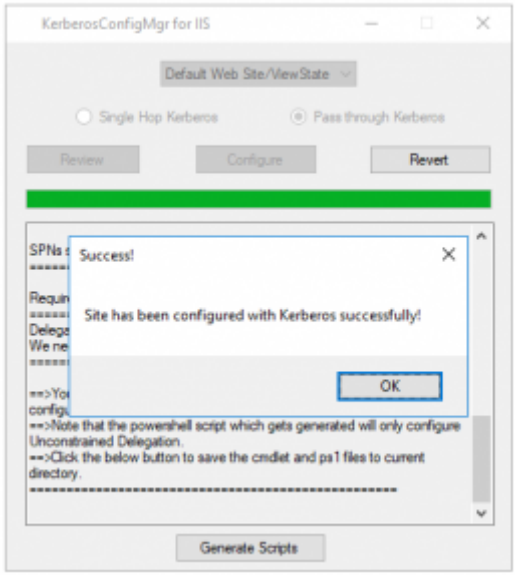


As soon as you start the application, a Log file is generated in the same folder as the executable with the system date timestamp. This log file would capture the timestamp, logged on user and all the series of configuration changes implemented during the session.

In case you want to review changes for new website, Close the tool and reopen it as administrator and follow the above steps from step# 1.







And that's all, you will have your site configured with Kerberos on IIS!

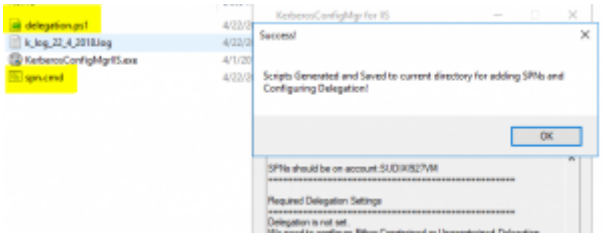
Any pre-requisites?

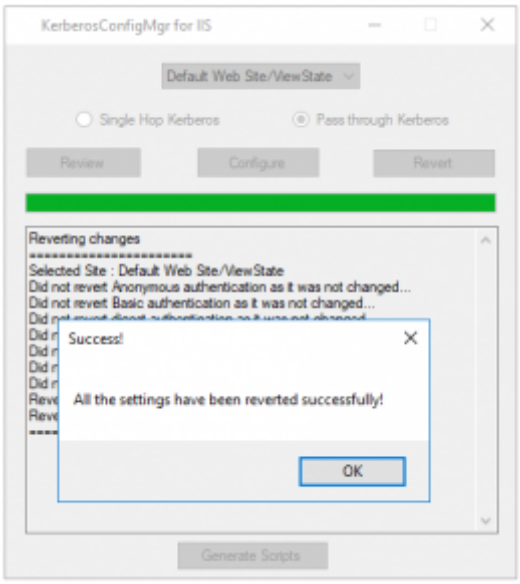
1. **Operating System :** Windows Vista & above
2. **.NET Framework :** 4.5.2 & above
3. **IIS Server Version :** 7.5 and above
4. All the modules should be installed related to Kerberos authentication like windows authentication module etc.

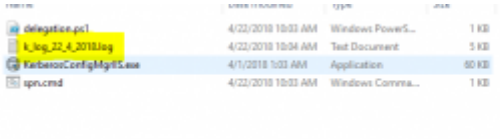
Feedback:

If you have any feedback, inputs, bugs to report about the tool, please comment below.

Happy Troubleshooting!







Comments

- Jawahar Ganesh S February 8, 2018
  Very nice article and Tool.

- Rohit Soni

  February 8, 2018
  Really a nice and helpful tool.

- avis chiropracteur nantes

  February 9, 2018
  Nice post. I was checking continuously this blog and I am impressed! Extremely helpful info specially the last part :) I care for such info a lot. I was seeking this certain info for a very long time. Thank you and best of luck.

- Mayur

  February 13, 2018
  superb tool! Kerberos configurations was never so easy before..Thanks a lot for sharing this, its saving hours of time.!!!

- Gerben

  April 5, 2018
  Hi, After windows authentication is enabled (RECOMMENDED) I get the error: Error ======= System.InvalidOperationException: Element not found! at KerberosConfigMgr.Kerberos.button2_Click(Object sender, EventArgs e) OS: W2012R2 .NET Frmwrk: 6.1 IIS Server 8.5 What can I check to recover....

  > Suraj Dixit April 10, 2018
  > Hello Gerben, This error comes into picture if you don't have the Windows authentication module installed on the IIS or anything related to providers. Try installing windows authentication module and then try to run the app. Refer the below issue on GitHub:
  > https://github.com/SurajDixit/KerberosConfigMgrIIS/issues/3

- Von Skuse

  May 24, 2018
  You sure know what you're talking about. Everyone is going to soon be visiting your site.

- iptv server

  October 5, 2018
  Hello,nice share.

- Francesco Papini November 21, 2018
  Great article and great tool, thanks for sharing it with the community.