

RE: IE, Kerberos, and Port Numbers

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2007-01/msg00122.html>

- *From:* briandel@xxxxxxxxxxxxxxxxxxxxxxxx (Brian Delaney [MSFT])
 - *Date:* Thu, 04 Jan 2007 21:17:14 GMT
-

Hi Don,

Which version of IE are you using?

I have found a hotfix for IE6 that I believe is what you are looking for.

Please review the fix: <http://support.microsoft.com/kb/908209>

If this is what you are looking for please let me know and provide an email address and I will provide you with instructions on getting the fix.

Hope this helps,

Brian Delaney
Microsoft Canada

--

This posting is provided "AS IS" with no warranties, and confers no rights.

Thread-Topic: IE, Kerberos, and Port Numbers
thread-index: Accuq+/wmeXISyn5ReCD1peVs62DuA==
X-WBNR-Posting-Host: 66.210.174.40
From: =?Utf-8?B?RG9uIFN0YW5sZXk=?= <Don
Stanley@xxxxxxxxxxxxxxxxxxxxxxxx>
Subject: IE, Kerberos, and Port Numbers
Date: Tue, 2 Jan 2007 12:24:00 -0800

This question has been cross-posted to the IE newsgroup as it has to do

with

IE's implementation of Kerberos ticket requests...

After many trials and tribulations with Kerberos, we have come to the conclusion that you cannot have two web sites on the same server with the same root URL, just differentiated by port number, that both use Kerberos

for

RE: IE, Kerberos, and Port Numbers

authentication unless they run as the same security account.

Our situation was a WS2003 server that has two web sites: one listening on the default port running as a domain account (svc_1), one listening on

port

8080 running as a different domain account (svc_2). We has two sets of

SPNs

registered: One set for the default HTTP port, and one set for port 8080.

In essence, the setspn -L output for each account looked like this:

For svc_1:
HTTP/WEBDEV002.company.net
HTTP/WEBDEV002

For svc_2:
HTTP/WEBDEV002.company.net:8080
HTTP/WEBDEV002:8080

We expected requests for <http://WEBDEV002:8080> to use Kerberos to authenticate (and delegation eventually), however it was always falling

back

to NTLM. When we read the article below, we removed the svc_1 SPN and Kerberos worked on the port 8080 site (but did not work on the port 80

site

any longer).

From <http://blogs.msdn.com/cgideon/archive/2006/09/11/749880.aspx>:

If multiple Web sites are reached by the same URL but on different ports, Kerberos will not work. To make this work, you must use different

hostnames

and different SPNs. When Internet Explorer requests either <http://www.Contoso.com> or <http://www.Contoso.com:81>, Internet Explorer requests a ticket for SPN HTTP/www.contoso.com. Internet Explorer doesn't

RE: IE, Kerberos, and Port Numbers

add

the port or the virtual server/Web Application to the SPN request. This behavior is the same for <http://www.contoso.com/app1> or <http://www.contoso.com/app2>. In this scenario, Internet Explorer will

request

a ticket for SPN <http://www.Contoso.com> from the Key Distribution Center (KDC). Each SPN can be declared only for one identity. Therefore, you

would

also receive a KRB_DUPLICATE_SPN error message if you try to declare this

SPN

for each identity.

My question is: Does IE intentionally omit the port number when

requesting

an SPN to obtain a Kerberos ticket? If not, is this a defect in IE that

can

be fixed? If so, what is the technical reason and is there a workaround? This is happening for both IE6 and IE7.

Thanks,

Don

.