

Re: want to ignore/bypass WSE2 policy for local requests...

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2004-11/>

From: Tim Mackey (*tim_at_scootasp.net*)

Date: 11/03/04

Date: Wed, 3 Nov 2004 17:11:29 -0000

hi Julie,

thanks for the reply.

i thought that since the endpoint uri's are case-sensitive, it would work to configure 2 different policies, one for lower-case and one for upper-case. do i understand it right that the lowercase one should apply to any clients that have a reference to it with that case? and then any other clients (i.e. my web pages) with a reference to the upper-case version, should use the different policy.

would it be possible in my custom security token manager to check somehow if the request is coming from the server itself and then accept the request somehow?

thanks

tim

67d0ebfec70e8db3

"Julie Lerman" <jlermanATNOSPAMPLEASEthedatafarm.com> wrote in message news:%23Tw5wxbwEHA.1988@TK2MSFTNGP12.phx.gbl...

Tim-

Are all of these really pointing to the same webserver? I'm sure you can't trick it like that! <g>

I have no idea if it's possible to base an endpoint policy on it's start point - wouldn't that be cool.

But unless someone can give you a cool solution that I don't know about (which is wholly possible), you might just have to have separate web services.

julie

"Tim Mackey" <tim@scootasp.net> wrote in message news:2uq7ctF2doraaU1@uni-berlin.de...

hi, i have a wse2 web service up and running and it serves lots of windows clients, with a custom username token manager. great.

i now have some new webforms on the same server that wish to use the web services. the problem is that the webforms can't obey the policy rules because it doesn't know at runtime any user account info, i want to work around this. i don't want to hard code in a 'SYSTEM' user + password only for use with the web service because someone could open the dll in notepad and use those credentials to abuse the web service.

i tried to set up 2 different policies for the same web service, with the difference being the address used to

access it. using the address: <http://localhost/WinDB.asmx> for the web forms, and a blank policy in policyCache.config. for the winclients then, they use the normal <http://shuttle/WinDB.asmx> address with the #username-token-signed policy or whatever. it doesn't work though. requests made through the local address get a "Server was unable to process request. --> The message must contain a wsa:To header" error.

policyCache.config extract:

```
<endpoint uri="http://localhost/WinDB.asmx">
  <defaultOperation>
    <request policy="" />
    <response policy="" />
    <fault policy="" />
  </defaultOperation>
</endpoint>
<endpoint uri="http://shuttle/winDB.asmx">
  <defaultOperation>
    <request policy="#username-token-signed" />
    <response policy="" />
    <fault policy="" />
  </defaultOperation>
</endpoint>
<policies
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <wsp:Policy wsu:Id="username-token-signed"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing"
xmlns:wssp="http://schemas.xmlsoap.org/ws/2002/12/secext">
    <wsp:MessagePredicate wsp:Usage="wsp:Required"
Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">
      wsp:Body() wsp:Header(wsa:To) wsp:Header(wsa:Action) wsp:Header(wsa:MessageID)
wse:Timestamp()
```

i also tried using the 127.0.0.1 IP address in the policyCache but it didn't change anything.

i really appreciate any suggestions anyone might have.

tim

\\ email: [tim at mackey dot ie](mailto:tim@mackey.ie) //

\\ blog: <http://tim.mackey.ie> //

67d0ebfec70e8db3