

HowTo - Setup a Reverse Proxy in IIS for webchat

INFORMATION

Setting up a reverse proxy for Multimedia Contact Center chat on an IIS web server requires specific configuration options to be enabled. IIS must have the Application Request Routing and URL Rewrite add-ons installed before IIS can be installed. These add-ons are available from <http://www.iis.net/downloads/microsoft/application-request-routing>.

To set up a reverse proxy, the web administrator must configure Application Request Routing to enable server proxying and then configure Inbound and Outbound rules. Depending on the web administrator's preference, that can be done in IIS or in the website's web.config file. If compression is enabled for your website, you must enable writing to HTTP_ACCEPT_ENCODING.

To set up a reverse proxy with IIS, you must:

- Configure Application Request Routing
- Enable writing to HTTP_ACCEPT_ENCODING (optional)
- Configure Inbound and Outbound rules using IIS
- Set up proxy rewrite to support SSL

Inbound and Outbound rules can be configured using either IIS or web.config.

Optionally, as an additional step, you can configure your reverse proxy to dynamically use multiple host addresses without having to change your existing settings whenever you want to test or make changes to access. This requires an additional custom server variable in order to support multiple host addresses to be reverse proxied.

To configure Application Request Routing

1. Start Internet Information Services (IIS) Manager.
2. In the Connections pane, select your website.
3. In the Applications pane, double-click Application Request Routing Cache.
4. In the Actions pane, select Server Proxy Setting.
5. Select Enable proxy.
6. In the Actions pane, click Apply.
7. Click Back to ARR Cache.

To enable writing to HTTP_ACCEPT_ENCODING

1. Start Internet Information Services (IIS) Manager.
2. In the Connections pane, select your website.
3. In the Applications pane, double-click URL Rewrite.
4. In the Actions pane, select View Server Variables....
5. In the Actions pane, click Add... and enter HTTP_ACCEPT_ENCODING.
6. Click OK.
7. In the Actions pane, select Back to Rules.

To configure your Inbound and Outbound rules using IIS

1. Start Internet Information Services (IIS) Manager.
2. In the Connections pane, select your website.
3. In the Applications pane, double-click URL Rewrite.
4. In the Actions pane, click Add Rule(s)..
5. Select Reverse Proxy and click OK.
6. Under Inbound Rules, enter the Enterprise Server IP address.
7. Optionally, if you are using HTTPS communications and have SSL enabled and your certificate(s) set up, clear Enable SSL Offloading.

8. Select Rewrite the domain names of the links in HTTP responses.
9. After To:, enter the DNS for your corporate website.
10. Click OK.
11. Select the Inbound rule and in the Actions pane, click Edit.
12. Under Pattern, enter ccmwa/(.*).
13. If you are using HTTP_ACCEPT_ENCODING, under Conditions, click Add and add it with a non-blank value. This is required as IIS does not let you save a blank value. It must be removed from the web.config file after setting up your Inbound and Outbound rules using IIS.
- NOTE:** You must have enabled writing to HTTP_ACCEPT_ENCODING previously.
14. Under Rewrite URL, update the IP address to include /ccmwa/ in the path.
15. In the Actions pane, click Apply.
16. Click Back to Rules.
17. Select the Outbound rule and in the Actions pane, click Edit.
18. Under Match the content within field, select everything except Use Custom Tags.
19. After Pattern:, update the URL address to include /ccmwa/.
20. Under Action Properties, update the Value field to include ccmwa in the path.
21. In the Actions pane, click Apply.
22. Click Back to Rules.
23. If you are using HTTP_ACCEPT_ENCODING, open your web.config file and remove the HTTP_ACCEPT_ENCODING value.

To configure your Inbound and Outbound rules using web.config

1. Navigate to your website's web.config file and open it in an editor.
2. Add the following rules to the system.webServer section:

```

<rewrite>
  <rules>
    <clear />
    <rule name="ReverseProxyInboundRule1" stopProcessing="true">
      <match url="ccmwa/(.*)" />
      <action type="Rewrite" url="http://192.168.0.1/ccmwa/{R:1}" />
    </rule>
  </rules>
</outboundRules>
<remove name="ReverseProxyOutboundRule1" />
<rule name="ReverseProxyOutboundRule1" preCondition="ResponselsHtml1">
  <match filterByTags="A, Area, Base, Form, Frame, Head, IFrame, Img, Input, Link, Script"
pattern="^http(s)?://192.168.0.1/ccmwa/(.*)" />
  <action type="Rewrite" value="http{R:1}://localhost/{R:2}" />
</rule>
<preConditions>
  <preCondition name="ResponselsHtml1">
    <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" />
  </preConditions>
</outboundRules>
</rewrite>

```

1. Update the Inbound rule action type URL address reference to the address of your Enterprise Server.
3. Update the reference to localhost in the outbound rule action type to the domain of the corporate website.

4. Save and close the editor.

To handle multiple host addresses with IIS reverse proxy

1. Start Internet Information Services (IIS) Manager.
 2. In the Connections pane, select your website.
 3. In the Applications pane, double-click URL Rewrite.
 4. In the Actions pane, select View Server Variables....
 5. In the Actions pane, click Add... and enter HTTP_INCOMMING_HOST.
 6. Click OK.
 7. In the Actions pane, select Back to Rules.
 8. Edit the inbound rule you created earlier.
 9. Under Server Variables, click Add and enter HTTP_INCOMMING_HOST.
 10. Set the value to {HTTP_HOST} and ensure Replace the existing value is selected.
 11. Click OK.
 12. In the Action section, ensure Stop processing of subsequent rules is selected.
 13. Click Apply in the Actions pane and then click Back to Rules
 14. Edit the existing Outbound rule you created earlier.
 15. Under Conditions, click Add.
 16. Set the Condition input to {HTTP_INCOMMING_HOST}. Set "Check if input string:" to
 17. "Matches the Pattern" and in "Pattern:", enter the host value used in the Action Properties of the Action section. Ensure "Ignore case" is selected.
 18. Click OK.
 19. Click Apply and then Back to Rules in the Actions pane.
- Add additional outbound rules for any additional host values you want to support following the same series of steps.

To set up proxy rewrite to support SSL

1. Start Internet Information Services (IIS) Manager.
2. In the Connections pane, select your website.
3. In the Applications pane, select URL Rewrite.
4. Double-click the Inbound Rules.
5. Under Conditions, click Add.
6. Under Condition input, enter {CACHE_URL}.
7. Under Check if input string, select Matches the Pattern.
8. Under Pattern, enter ^(https?)://
9. Select Ignore case.
10. Click OK.
11. Select Track capture groups across conditions.
12. Under Rewrite URL, replace http with {C:1}.
13. Click Apply.

APPLIES TO

MiCC Webchat Version 8.0 and newer

Keywords:

reverse proxy webchat

<http://micc.mitel.com/kb/KnowledgebaseArticle52451.aspx>

Thursday, May 26, 2022