# Select Between Multiple Network Access Resources with the Edge Client

**Seth Cooper, 2015-26-02**

The recent announcements that web browsers will be removing plugin support means that customers will no longer be able to provide Network Access resources to their end users via the APM web top. Instead customers will require their end users to install the Edge Client for their Network Access connections. This poses a problem to customers who require that their end users have the ability to manually choose which Network Access resource they will connect to. Currently (as of this article's posting date) the Edge Client does not have the ability for end users to select from multiple Network Access resources. Instead end users will automatically connect to only one Network Access resource based on which resource was provisioned first. See AskF5 solution SOL15326 for more information (https://support.f5.com/kb/en-us/solutions/public/15000/300/sol15326).

I have created a customized way to provide end users the ability to select which Network Access resource to connect to within the Edge Client. This customization is pretty straightforward and can be further customized to fit the needs of your organization. I have tried to make this solution flexible and easy to implement but if you have any questions or need any help with adapting it to your organization please comment below.

NOTE: There are limitations on this workaround compared to the full browser web top.

Limitations:
- To change between Network Access resources you must disconnect and reconnect which requires re-authentication.
- Using the iOS Edge Client you must select "Web Logon".

Considerations:
- This solution assumes that all of the AD Groups for VPN access are in a dedicated OU. You can work around this implementation if you need to but these instructions assume all AD groups in "OU=VPN,DC=fr,DC=del,DC=corp" have a corresponding Network Access resource configured and mapped in the VPE.
- The name of the AD group will be the name listed on the dropdown list that end users select from. This means you SHOULD have meaningful group names for end users to select from. Spaces in the group name for better formatting is allowed.
- I have only tested this on Windows 7.
- These instructions are written for TMOS build version 11.6.0

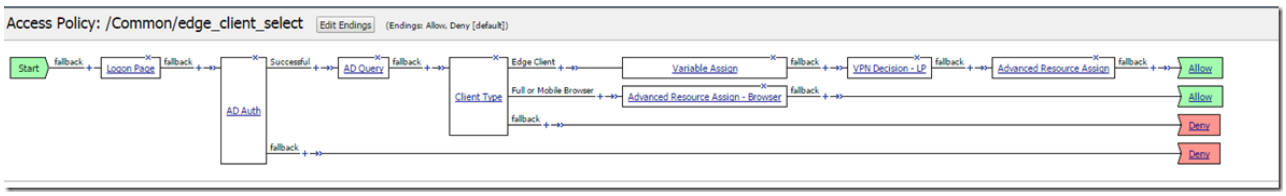
**NOTE:** I wrote a new article to cover using LocalDB Auth instead of AD Auth.

https://devcentral.f5.com/articles/select-between-multiple-network-access-resources-with-the-edge-client-local-db-auth

## Overall View of Config:

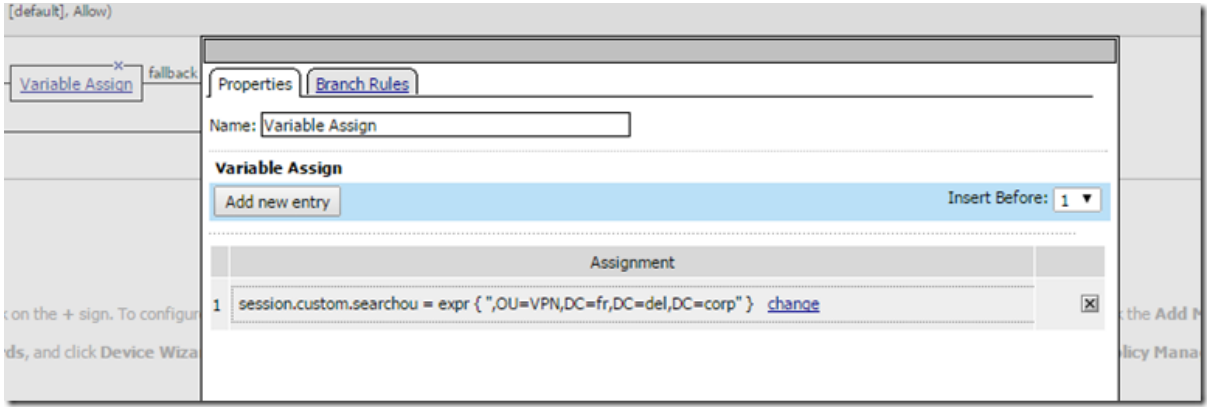
Here I will show screen captures of the config with a little bit of a description of each section and below I will give step by step instructions to configure.

VPE:

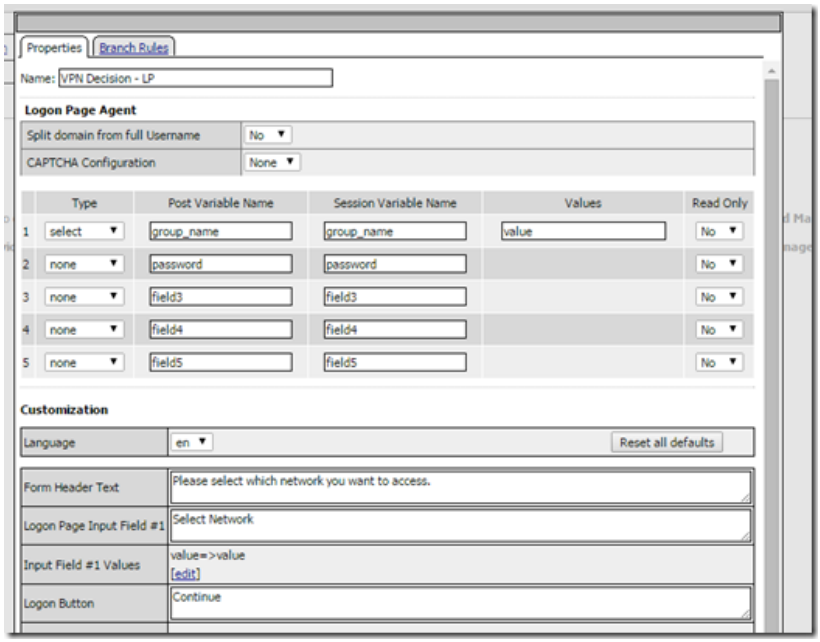


The VPE is pretty straight forward. We start with a standard “Logon Page” with username and password, we then do an “AD Auth” and if successful we go to “AD Query”. The following object is the “Client Type” which determines if the user is connecting from the “Edge Client” or “Browser”. We only need this customization on the “Edge Client” path. The browser resource assign is a standard assign that we are all familiar with. This is all pretty standard at this point.

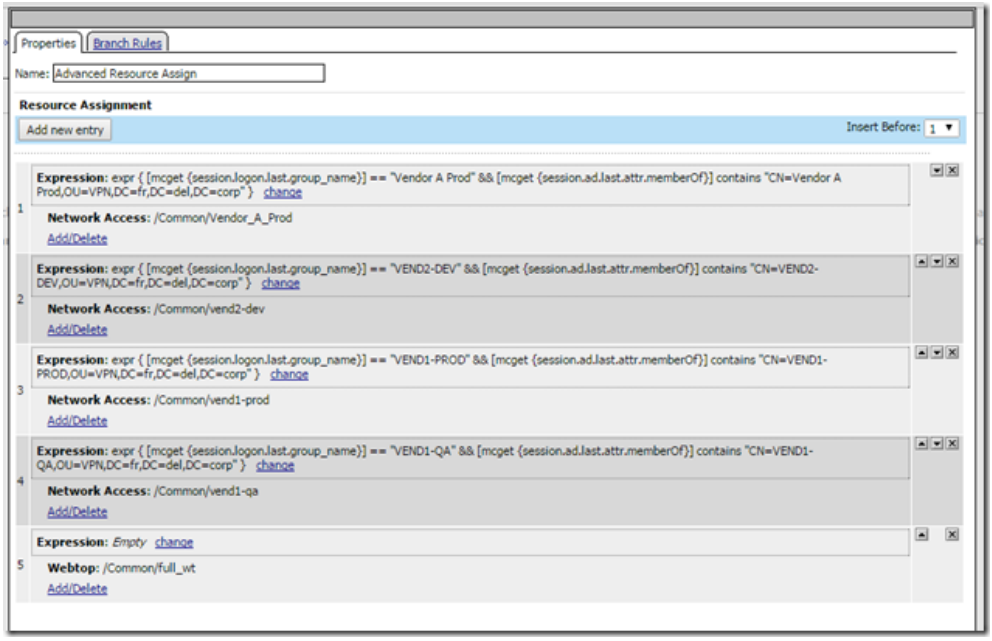
The next object is a Variable Assign where we will set a custom variable (session.custom.searchou) to make it where you don’t need to modify the javascript code. This string will be removed from the full DN to make the dropdown list easier to read so it needs to start with a comma as the full DN for a group is “CN=VEND1-QA,OU=VPN,DC=fr,DC=del,DC=corp”.




After the Variable Assign we have another “Logon Page” VPE Event labeled “VPN Decision – LP”. This is the place where the end user will make the decision on which Network Access resource they want to access. This page we configure a “select” box with the post and session variable names of “group_name” with the value of “value=>value”. This will be overwritten later but we need it as a placeholder. I also modified the Form Header, Field Label and Logon Button Label.




Last we have an “Advanced Resource Assign” to provision the access. Here we check to see what the value of “session.logon.last.group_name” and to make sure the user is a member of the group (this is a security check to make sure they are allowed access). In the screen shot below the group mapping is listed in entries 1 through 4 and in entry 5 we have the webtop assign which everybody gets.




The only other piece to this is a customized logon.inc page which will be applied to the second logon page. I will provide the full logon.inc page you can use to replace the current one as an attachment below. The screenshot is here to show you the custom code. This is just basic JavaScript to take the list of groups you are a member of and clean it up, split it into an array, then check to see which groups are in the VPN OU. If the groups is in the VPN OU then we will do a little bit more formatting on the string before we eventually append it to the “dynamicInput” element we will also create on the logon.inc page.

```
    }

    //edge-client-select-onload-start
    function sc_trim (str) {
      str = str.replace(/^\s+/, '');
      for (var i = str.length - 1; i >= 0; i--) {
        if (/\S/.test(str.charAt(i))) {
          str = str.substring(0, i + 1);
          break;
        }
      }
      return str;
    }

    var full_group_list = "%{session.ad.last.attr.memberOf}";
    //chop the first two characters off
    full_group_list = full_group_list.substring(2);
    //chop the last two characters off
    full_group_list = full_group_list.substring(0, full_group_list.length - 2);
    var groupArray = full_group_list.split("|");
    groupArray.sort();
    var newDiv=document.createElement('div');
    var selectHTML = "";
    selectHTML="<select name='group_name' id='input_1' class='credentials_input_select'>";
    for(i=0; i<groupArray.length; i=i+1){
      if( groupArray[i].indexOf("%{session.custom.searchou}") > 0 ) {
        //replace full OU Information
        groupArray[i] = groupArray[i].replace(/%{session.custom.searchou}/g,"");
        //replace CN=
        groupArray[i] = groupArray[i].replace(/CN=/g,"");
        //trim extra spaces
        groupArray[i] = sc_trim(groupArray[i])
        selectHTML+= "<option value='"+groupArray[i]+"'>"+groupArray[i]+"</option>";
      }
    }
    selectHTML += "</select>";
    newDiv.innerHTML= selectHTML;
    document.getElementById("dynamicInput").appendChild(newDiv);
    //edge-client-select-onload-end
}
```

I hope this configure will help with any deployments you need and gives you an idea of how flexible and powerful APM can be for your organization.

If you have any questions about the changes to the logon.inc file and the JavaScript please ask in the comments below.

## Steps to Configure:

I am going to assume that you are familiar with APM and the VPE so I will not go into great detail on most of these steps. If you need clarification on any step please let me know.

1. Create a new Access Policy

2. Open the VPE and configure the following Actions (see the screenshot above for placement of each action).

3. Add a Logon Page Action: This is a standard logon page with a username and password box.

4. Add an AD Auth Action: This is a standard AD Auth pointed to an existing AD AAA Object.

5. Add an AD Query Action: This is a standard AD Query pointed to an existing AD AAA Object.  Make sure to enable "Fetch Primary Group" and that the AD AAA Object has an admin account configured.

6. Add a Client Type Action: This is a normal Client Type Action with three branches.  Edge Client, Full or Mobile Browser and fallback.

7. Add a Variable Assign Action along the Edge Client Branch: In this variable assign enter the following into the assignment.

```
Custom Variable = session.custom.searchou
Custom Expression = expr { ",OU=VPN,DC=fr,DC=del,DC=corp" }
```

8. Add a Logon Page Action: I labeled this “VPN Decision – LP”

```
In input 1 configure the following:
Type: select
Post Variable Name: group_name
Session Variable Name: group_name
Values:   Value: value   Text: value
Read Only: No

Leave input 2 – 5 as type of “none”.

Modify the following in the bottom Customization section:
Form Header Text: Please select which network you want to access.
Logon Page Input Field #1: Select Network
Logon Button: Continue
```

9. Add an Advanced Resource Assign Action: Create the following entries.  You will need to enter the expression below in the Advanced Tab.

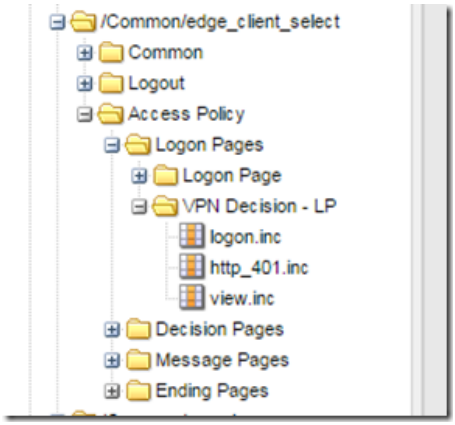
```
ENTRY 1
Expression: expr { [mcget {session.logon.last.group_name}] == "Vendor A Prod" && [mcget {session.ad.l
Assignment:   Network Access: /Common/Vendor_A_Prod (this is a network access resource configured wit

ENTRY 2
Expression: expr { [mcget {session.logon.last.group_name}] == "VEND2-DEV" && [mcget {session.ad.last.
Assignment:   Network Access: /Common/vend2-dev

ENTRY 3
Expression: expr { [mcget {session.logon.last.group_name}] == "VEND1-PROD" && [mcget {session.ad.last
Assignment:   Network Access: /Common/vend1-prod

ENTRY 4
Expression: expr { [mcget {session.logon.last.group_name}] == "VEND1-QA" && [mcget {session.ad.last.a
Assignment:   Network Access: /Common/vend1-qa

ENTRY 5
Expression: Empty
Assignment:   Webtop: /Common/full_wt (this is just a full webtop object)
```

10. Add an Advanced Resource Assign on the browser branch of the Client Type Action: I labeled this one “Advanced Resource Assign – Browser”. This is a standard resource assign where you will need to map a group to a resource. The only difference between this assign and the previous assign is the expression doesn’t need to check for the value of the session.logon.last.group_name variable as this variable will not exist on the browser branch.

11. Now that we have the Access Policy Create and the VPE configured the next step is to go into advanced customization and replace the logon.inc for the second logon page labeled “VPN Decision – LP”.

To modify the page we need to go to Access Policy > Customization > Advanced.

12. Expand the folder tree to get to the logon.inc page. Customization Settings > Access Profiles > /Common/edge_client_select > Access Policy > Logon Pages > VPN Decision – LP > logon.inc




13. Click on the logon.inc and on the right side of the screen select all text and replace with the code at the following link.

https://dl.dropboxusercontent.com/u/27996759/f5/na-edge/logon.inc.txt

14. Click “Save Draft” in upper right hand corner

15. Click “Save” in the tool bar.

16. Apply the Access Policy

17. Attach the Access Policy to a Virtual Server

18. Test your access.

I hope this helps!

Regards,

Seth Cooper

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com