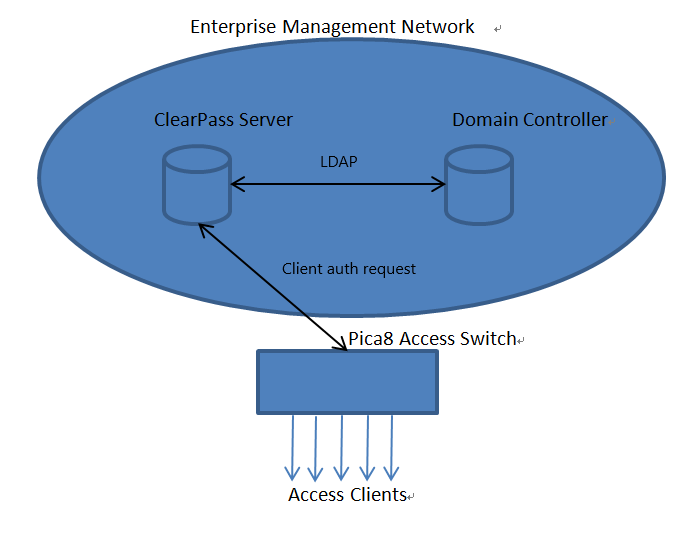
# Pica8 Solution Document

# Integrating ClearPass with Active Directory

ClearPass can be integrated with an Active Directory. Active Directory Domain Controller (AD-DC) can then be used as an authentication source on ClearPass Policy Manager (CPPM) to perform authentication and authorization on the clients requesting access on the Pica8 switch ports. As depicted in the graphics below, clients connected to the switch port request access to the network. The switch ports are configured for 802.1X authentications and clients use **EAP-MSCHAPv2** username password based authentication mechanism. When CPPM receives the client authentication request, CPPM uses the LDAP protocol to request AD-DC to authenticate the users. Using AD-DC as an authentication source on CPPM eliminates the need for creating user identities on CPPM’s local user repository. Clients can use their AD credentials to login to the network. CPPM in this case acts as a relay between the authenticating client and the AD-DC.



### Environment

For this example we are using Microsoft Windows Server 2016 as our Active Directory server. The ClearPass version we are using is 6.8. We are using a Windows 10 laptop as our test client on which 802.1X security is enabled. We are not using any of dynamic VLAN, dynamic filter or downloadable filter for this example. The switch hardware model used is AS4610\_30T. And the PICOS version used is 2.11.23. Versions higher than 2.11.23 can also be used for this example.

### Pre-requisites:

1. Make sure the Primary DNS address on CPPM is that of the Active Directory DNS server to make sure the active directory fully qualified domain name (FQDN) can be successfully resolved to its IP address on the CPPM. Alternatively, you can use any DNS server that can resolve the fully qualified domain name of the AD-DC but the recommended DNS is that of the AD-DC. We are using the DNS server of our AD-DC server for this example.
2. Make sure that the time and date of both the ClearPass server and the Active Directory servers are synchronized. The maximum skew time allowed between the ClearPass server and the Active Directory server is 5 minutes. The best way would be if both the servers are synchronized against the same NTP server. For this example, we used our local lab NTP server 10.10.50.10.

***Important Note1: Configuring AD-DC and DNS server is beyond the scope of this document, the users of this guide are advised to follow the instruction for configuring the above two systems according to their respective vendor documentation. For Windows Server 2016 documentation, follow*** [***this link***](https://docs.microsoft.com/en-us/windows-server/get-started/server-basics)***.***

***Important Note2: Changing the time or the NTP configuration of ClearPass will render invalid the server certificates on ClearPass. You will need to reset the server certificates on ClearPass should you chose to perform these actions on the ClearPass server. Use this command to reset server certificates on ClearPass server CLI: system reset-server-certificate***

## PICOS Configuration

We will use the following switch configuration to test 802.1X EAP-MSCHAPv2 authentication for this sample setup. We are using the out-of-band management port for this example so the inband configuration is not given here. Please refer to our documentation [***here***](https://docs.pica8.com/display/PicOS35sp/Typical+Configuration+of+NAC) for inband configuration.

1. Put interface ge-1/1/1 in trunk mode

*set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode "trunk"*

1. Choose auth-mode 802.1X for interface ge-1/1/1

*set protocols dot1x interface ge-1/1/1 auth-mode 802.1x*

1. Set the NAS-IP to 10.10.51.141, this is the IP address of the switch management interface

*set protocols dot1x aaa radius nas-ip 10.10.51.141*

1. Configure AAA Radius server IP and shared key

*set protocols dot1x aaa radius authentication server-ip 10.10.50.65 shared-key test*

1. Configure AAA Radius dynamic authorization client IP and shared key

*set protocols dot1x aaa radius dynamic-author client 10.10.50.65 shared-key test*

1. Save the configuration

*commit*

## Join ClearPass to Active Directory Domain

Below are some details about our Active Directory setup that we have created for the purpose of this example in our lab.

*Active Directory FQDN:* *win-aqbv4lqe777.pica8.testdomain.com*

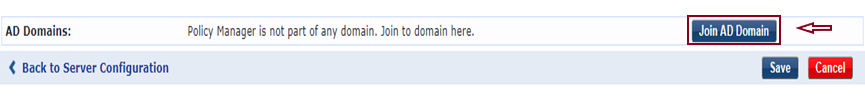
*Active Directory DNS server IP: 10.10.50.71*

*Active Directory Server IP: 10.10.50.71*

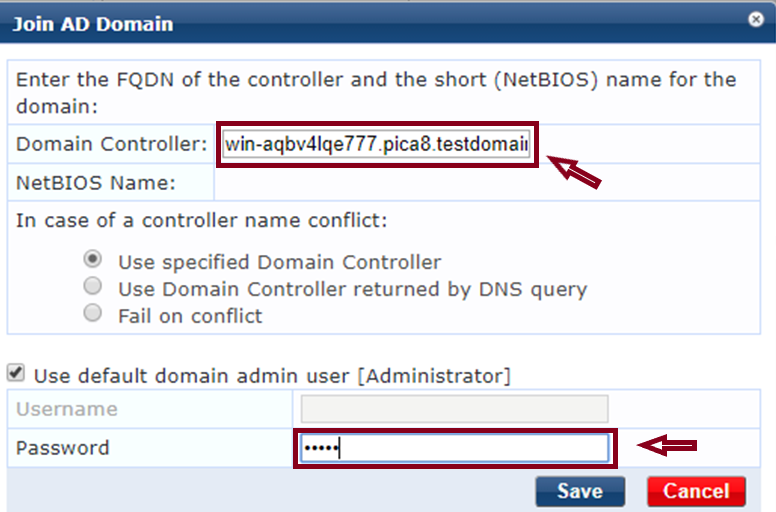
The next section describes the list of steps used to join a ClearPass server to an Active Directory Domain Controller.

### Join AD Domain

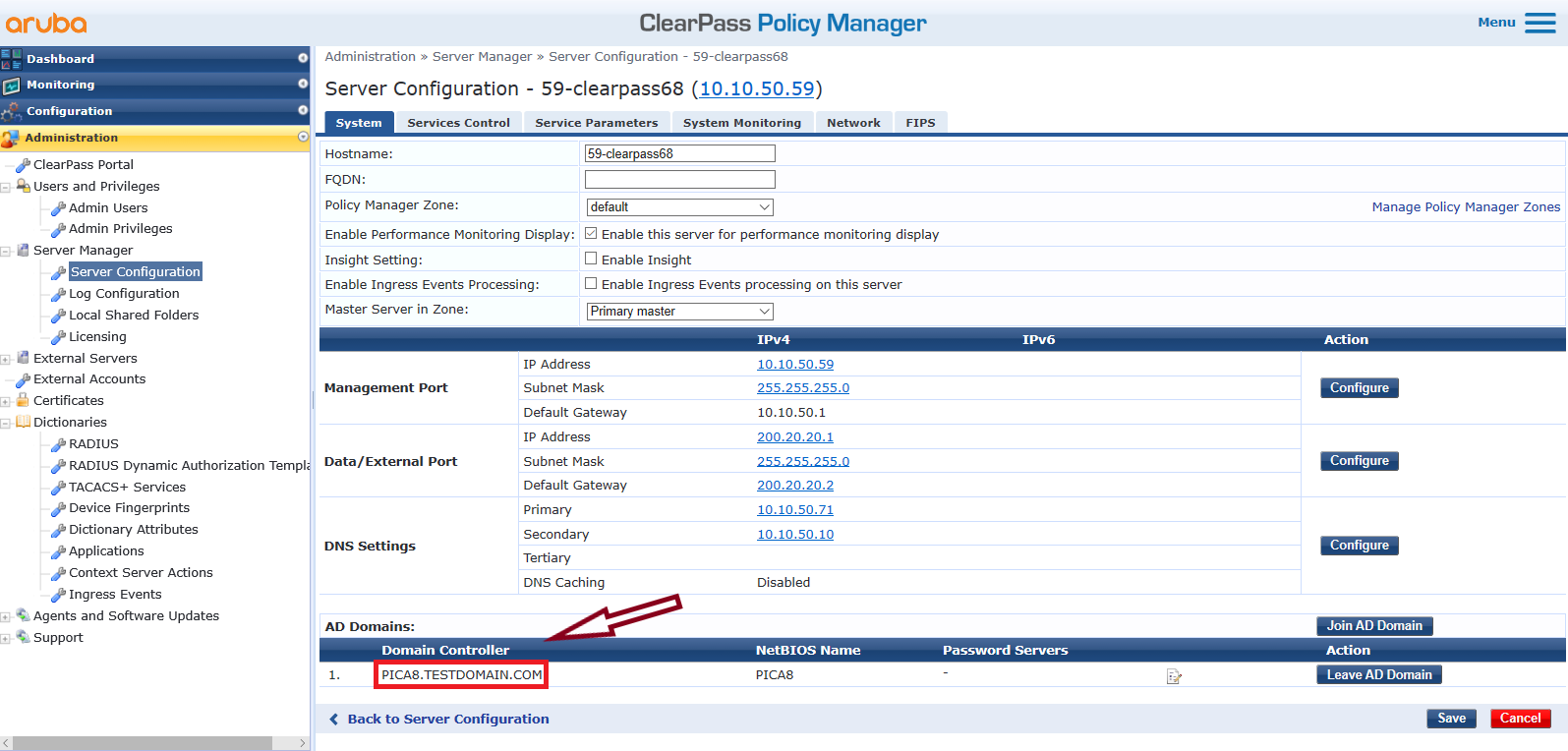
Login to CPPM and navigate to **Administration** 🡪 **Server** **Manager** 🡪 **Server** **Configuration.** Click on the ClearPass server that you would like to join with AD-DC. If you have multiple servers, then choose one of them but if you just have one instance then click on that and then click on **Join AD Domain.** Refer to the image below for details.



In the **Join AD Domain** window**,** type the FQDN of the Domain Controller. We use the FQDN *win-aqbv4lqe777.pica8.testdomain.com* in this example. After inputting the FQDN, hit the tab button on your keyboard or click in another field will cause the ClearPass to look for the NetBIOS Name of the Active Directory server and load it in the NetBIOS Name field. Enter the Active Directory default Administrator account password in the password field and click **Save**. Refer to the image below for details.

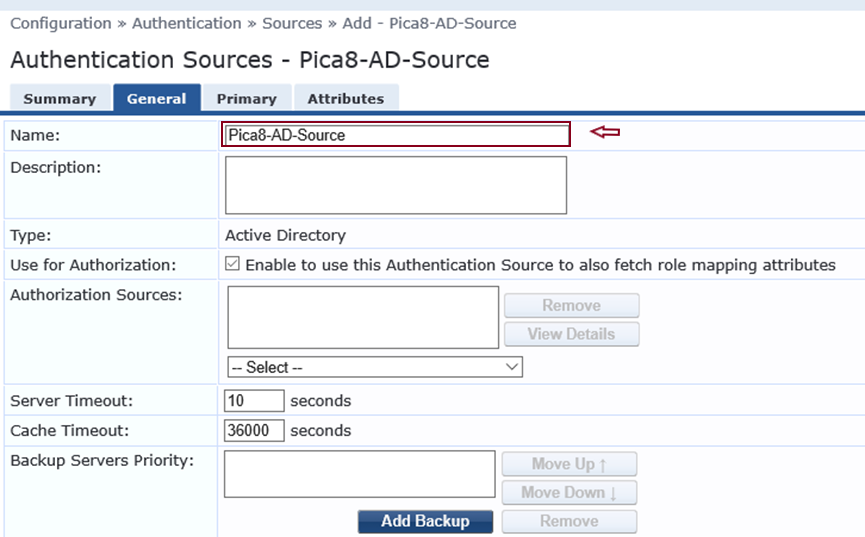


Once you hit **Save,** it will take ClearPass some time to join the AD. Log-in to ClearPass again once the process is completed. After you have joined the AD Domain, you can confirm your settings by clicking on **Administration** 🡪 **Server** **Manager** 🡪 **Server** **Configuration**. As you can see in the screen shot below, we have successfully joined the PICA8.TESTDOMAIN.COM. Click **Save** to finish this configuration step.



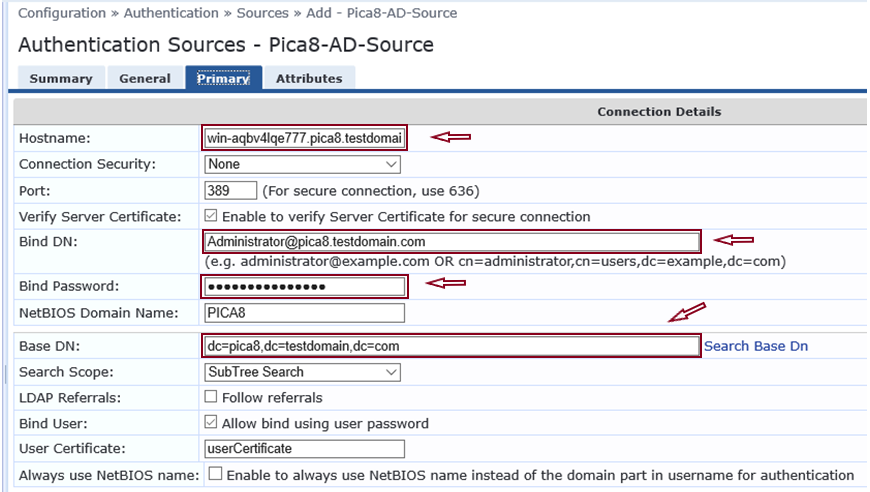
### Add AD Authentication Source

To add an authentication source for Active Directory, click on **Configuration** 🡪 **Authentication** 🡪 **Sources**. On the General Tab, type a name for this authentication source and fill in other details, refer to the image below for details. We use the name *Pica8-AD-Source* in this example*.* Leave the other options to default.

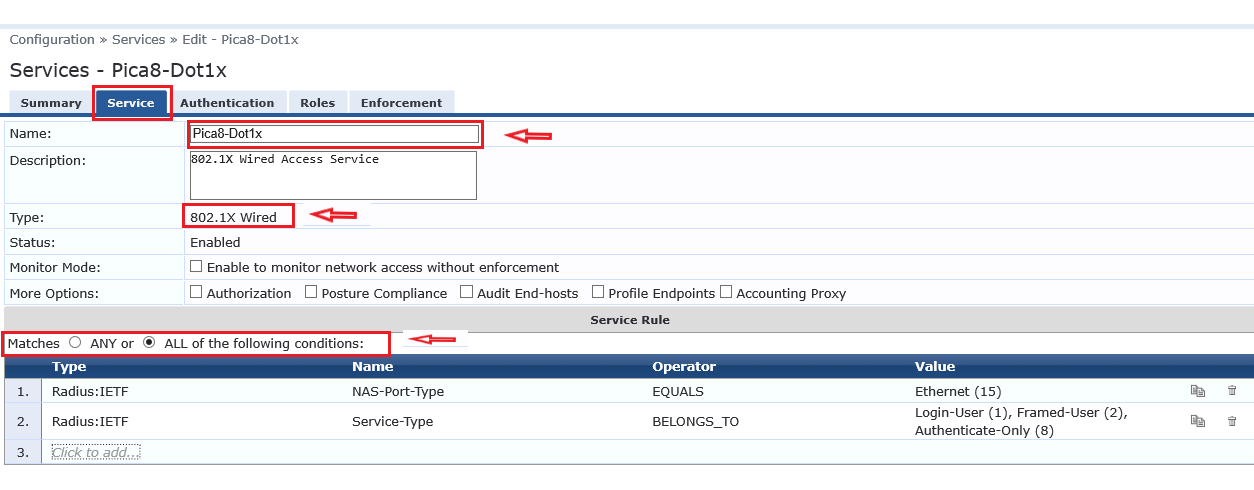


On the Primary tab, type the FQDN of the Active Directory server, we are using win-aqbv4lqe777.pica8.testdomain.com in this example as this is the FQDN of our Active Directory server. For the Bind DN name, we are using the name *Administrator@pica8.testdomain.com.* Here, Administrator is the AD domain controller’s default Administrator account. In the Bind Password field, type the AD Administrator password.

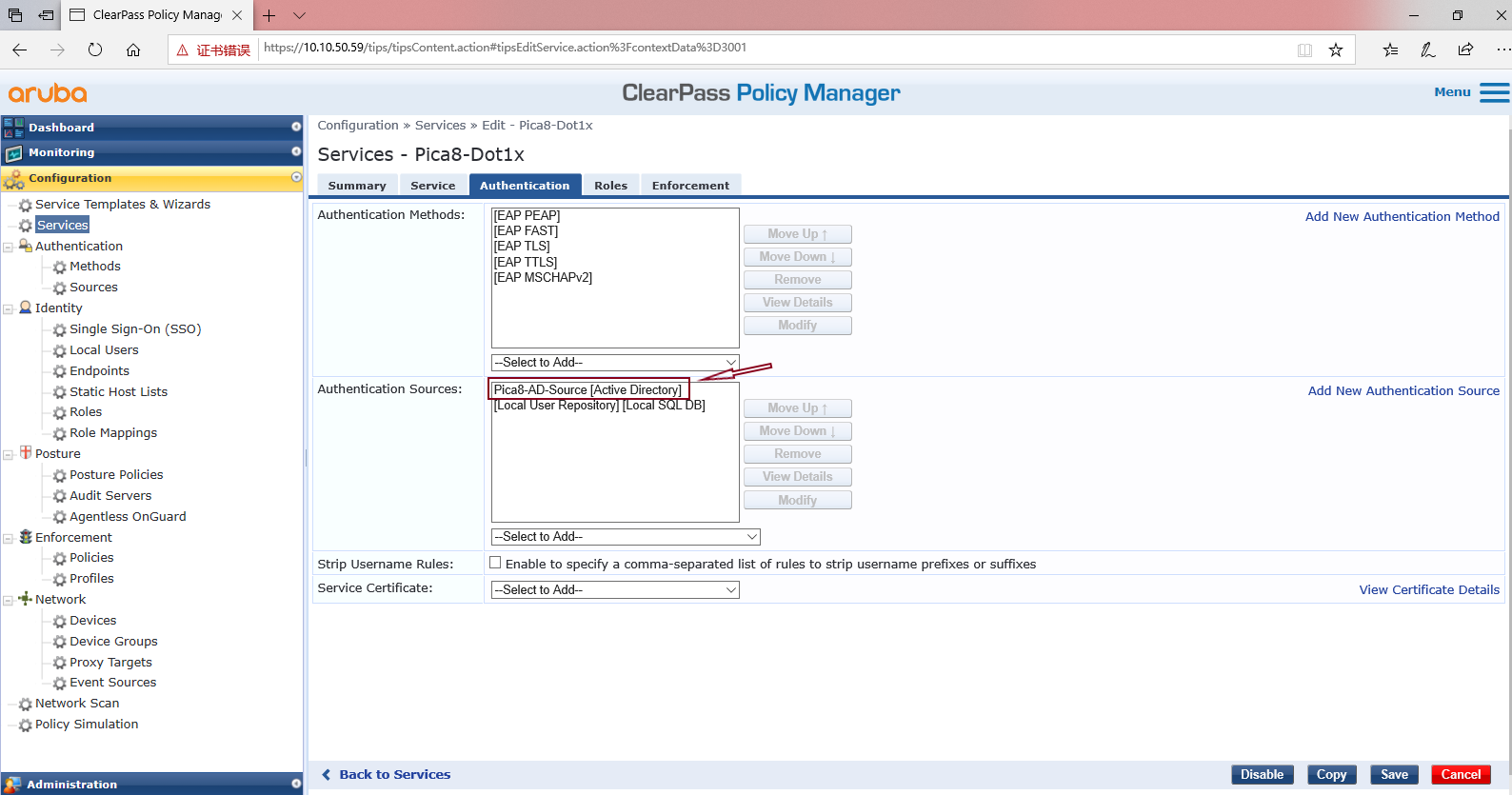
For Base DN we use *dc=pica8,dc=testdomain,dc=com.* Click on **Save** to finish. Refer to the Screen shot below for details.



For this example we will be using an 802.1X authentication service. For information on how to configure an 802.1X service and general integration instructions, please refer to Pica8 Integration with Aruba ClearPass document [here](https://docs.pica8.com/display/PicOS35sp/Typical+Configuration+of+NAC), you will also be able to find different switch configurations from that location. For this example we created an 802.1X service by the name **Pica8-Dot1x**. We will provide a brief description of Pica8-Dot1x service here. On the Service tab, make sure you select the items as depicted in the image below.



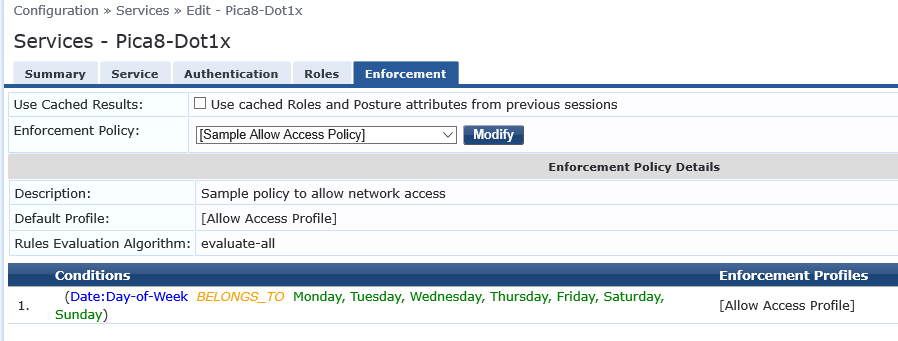
On the Authentication tab of this service, we will choose the AD authentication source we created previously. For the **Authentication Sources**, choose **Pica8-AD-Source**. Make sure this authentication source is at the top of the list. Click **Save** to finish this configuration.



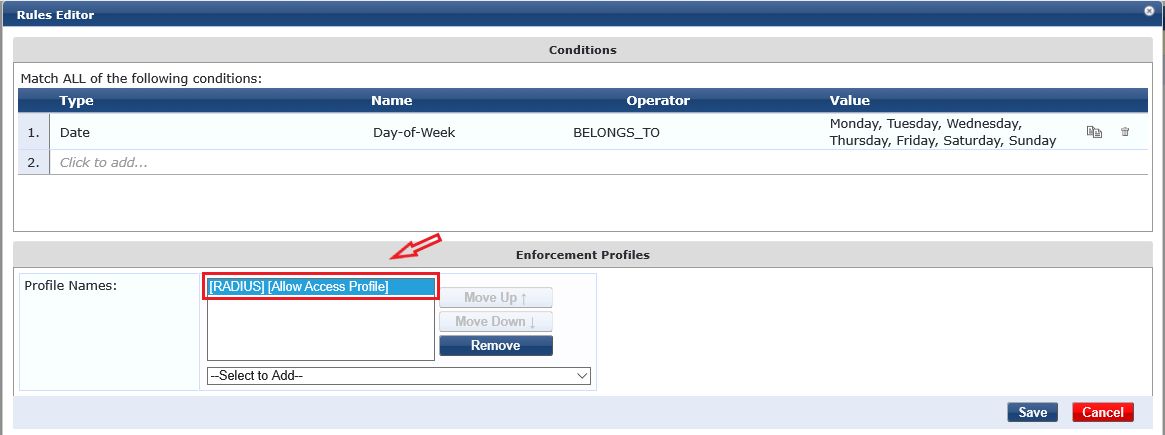
On the Roles tab, we leave the options to default as given below.



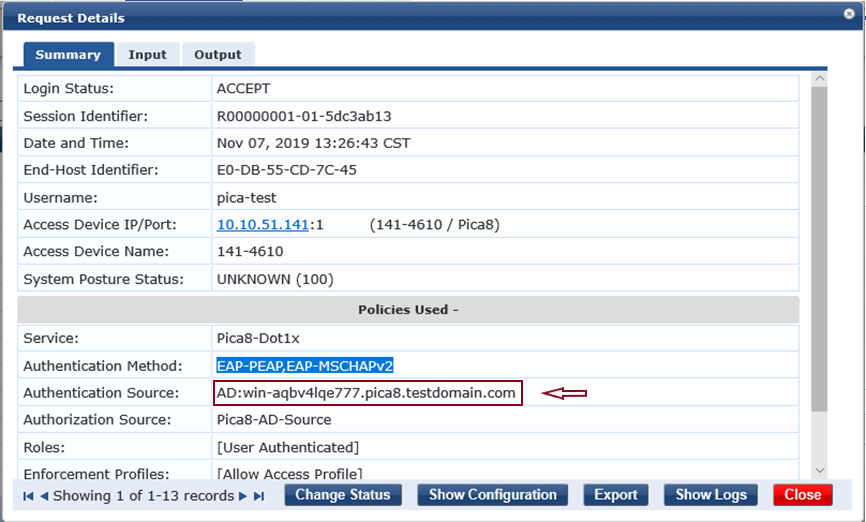
On the Enforcement tab, we are using the ClearPass built-in default Sample Allow Access Policy as shown below.



The Sample Allow Access Policy uses the built-in default **Allow Access Profile** as shown below.



We enabled 802.1X authentication on switch port 1 and connected our laptop with the switch port. A pop up window appeared where we entered the AD username and password. The switch verified the username and password from the AD and allowed access since the username and password were valid on the AD-DC. To verify whether AD authentication source was used for this authentication, click on **Monitoring** 🡪 **Live** **Monitoring** 🡪 **Access** **Tracker** then click on the corresponding authentication entry. Refer to the screen grab below for details. As you can see, for Authentication Source, the name of our AD FQDN is used.



### References:

1. <https://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/Active%20Directory/Joining_AD_domain.htm>
2. <https://docs.pica8.com/display/PicOS35sp/Typical+Configuration+of+NAC>