aruba
a Hewlett Packard Enterprise company

CLEARPASS - DOT1X: PURPOSE OF DOMAIN JOINING

Technical Climb Webinar

10:00 GMT | 11:00 CET | 13:00 GST
Nov 29th, 2016

Presenter: Barath Srinivasan

barath.srinivasan@hpe.com

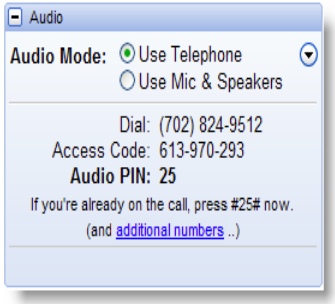
AIRHEADS COMMUNITY

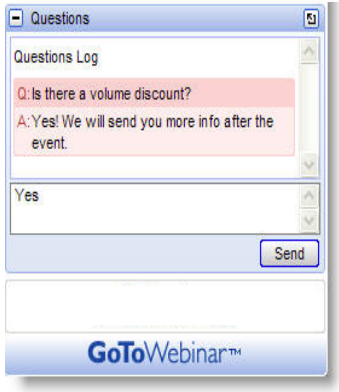
Welcome to the Technical Climb Webinar

Listen to this webinar using the computer audio broadcasting or dial in by phone.

The dial in number can be found in the audio panel, click additional numbers to view local dial in numbers.

If you experience any difficulties accessing the webinar contact us using the questions panel.



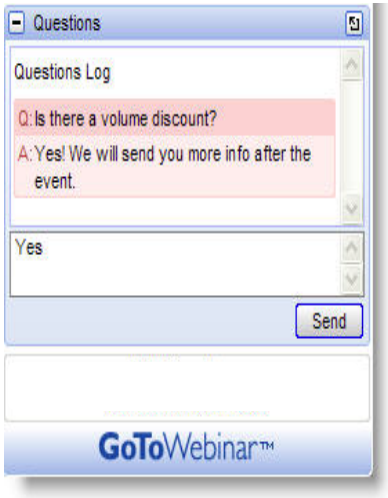


Housekeeping

This webinar will be recorded

All lines will be muted during the webinar

How can you ask questions?
Use the question panel on your screen



The recorded presentation will be posted on Arubapedia for Partners (https://arubapedia.arubanetworks.com/afp/)

CLEARPASS - NEED FOR DOMAIN ACCOUNT AND DOMAIN JOINING

aruba
a Hewlett Packard Enterprise company

Need for domain account & domain join

- The first task in preparing Clearpass for Active Directory (AD) authentication via EAP-PEAP-CHAP-v2 is to join the Clearpass server to an Active Directory domain.
- Joining Clearpass Policy Manager to an AD domain allows you to authenticate users and computers that are members of an AD domain.
- It also creates a computer account for the clearpass node in the AD database.
- Users can then authenticate to the network using 802.1X and EAP methods, such as PEAP-MsCHAPv2, with their own AD credentials.
- A one-time procedure to join ClearPass Policy Manager (CPPM) to the domain must be performed from an account that has the ability to join a computer to the domain.

Need for domain account & domain join

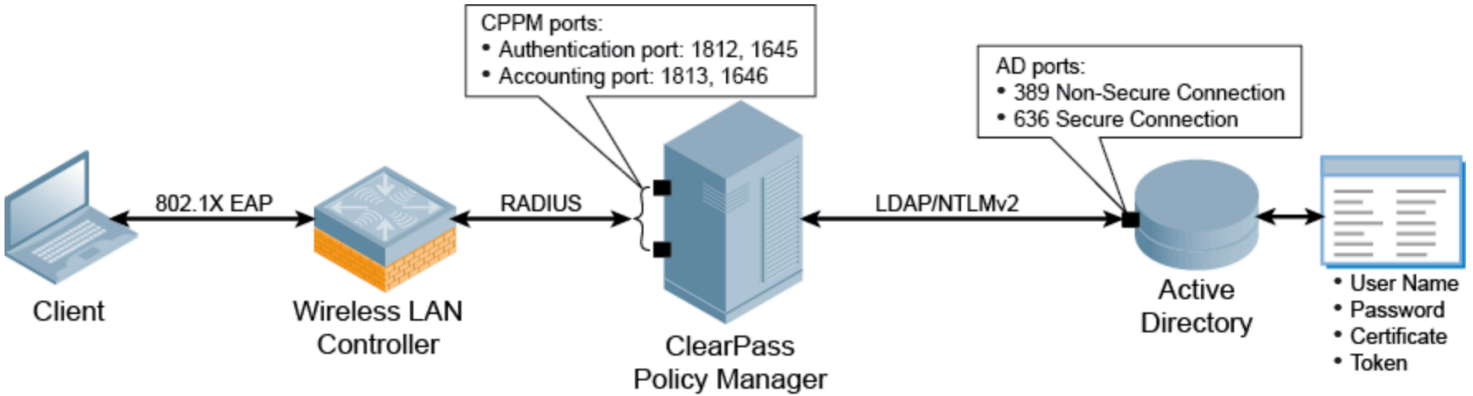
Why does Clearpass need to join AD to perform EAP-PEAP-MS-CHAP-v2 authentication for 802.1x?

- ClearPass Policy Manager needs to be joined to AD because when performing authentication for a client using EAP-PEAP-MS-CHAPv2, only the password hashes supplied by the user are used to authenticate against AD.
- This process is done NT LAN Manager (NTLM) authentication. Which requires AD domain membership.
- If you need to authenticate users that belong to multiple AD forests or domains in your network, and there is no trust relationship between these entities, then you must join Clearpass to each of these untrusting forests or domains
- You do not need to join Clearpass to multiple domains belonging to the same AD forest, because a one-way trust relationship exists between these domains. In this case, you should join CPPM to the root domain.

AUTHENTICATION WORKFLOW

aruba
a Hewlett Packard
Enterprise company

Workflow



- User connects to the WLAN network from his laptop and an 802.1x EAP-PEAP authentication process begins
- The client's authentication request is sent to the mobility controller.
- When the mobility controller receives the authentication request, it sends a RADIUS access-request to Clearpass with encrypted username and password
- The Clearpass server checks the AD database for a matching username and password
    - If the match is a success – Clearpass server sends an access-accept message to the mobility controller
    - If the match is a failure – Clearpass server sends an access-reject message to the mobility controller

CONFIRMING DATE/TIME SETTING AND JOINING PROCEDURE

aruba
a Hewlett Packard Enterprise company

Domain Controller

- A domain is defined as a logical group of network objects (computers, users and devices) that share the same AD.
- The domain controller is the Microsoft AD server responsible for responding to requests for authentication from users and computer accounts (for example, logging in and checking permissions)
- It is common for an AD domain controller to function as a DNS server. AD domain controllers can also be LDAP servers, as well as perform any number of additional functions that are loaded on the same server.
- By default, a domain controller stores one domain directory partition consisting of information about the domain in which it is located, plus the schema and configuration directory of the entire forest.

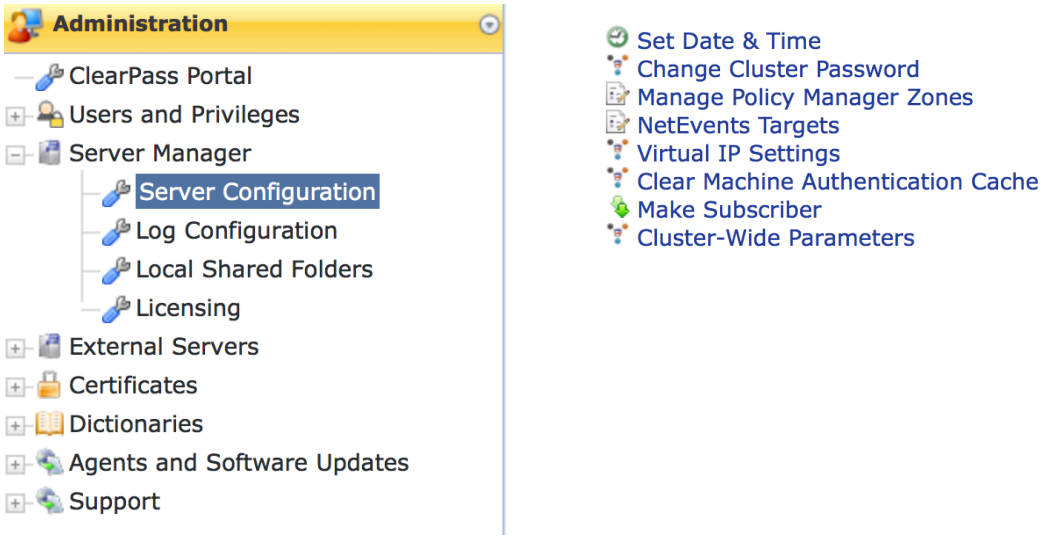
Confirming Date/Time are in Sync

Assuming that the Clearpass server has never been joined to the AD domain before, first make sure that the date and time are correct and in sync on both the clearpass server and the AD domain controller that you will use for the join domain operation.

In the clearpass policy manager, navigate to –

Administration > Server Manager > Server configuration

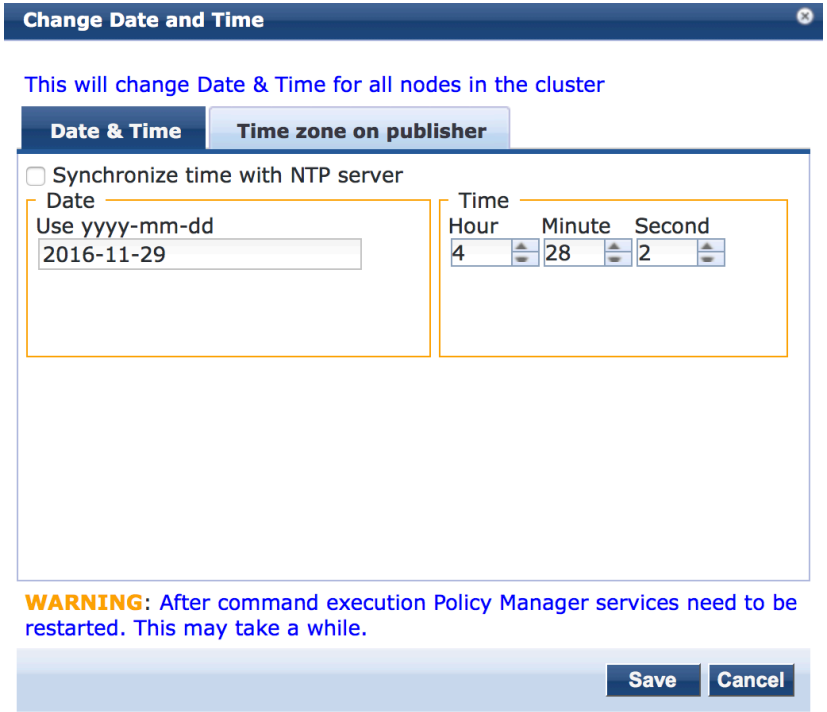
Once the server configuration screen appears,
On the top right corner, you will see "**Set Date & Time**"



Confirming Date/Time are in Sync

In the Change Date and Time dialog box, there are couple of options, you can either set the date and time or sync time with NTP server

- To synchronize with a NTP server, the **Synchronize time with NTP server** check box must be enabled. Not more than two NTP servers can be specified.
- You can return to the server configuration page by clicking **cancel**
- Compare the clock time displayed at the bottom of the Clearpass Server Configuration page against the clock time on the AD server.
- Max allowed clock skew between Clearpass server and AD server is 5 mins



Joining an Active Directory Domain

To join a Clearpass server to an Active Directory Domain,

In the **Server Configuration** screen, click the name of the Clearpass server that you want to join to the domain.

The server configuration screen for the selected server opens, you can now join the Active Directory domain.

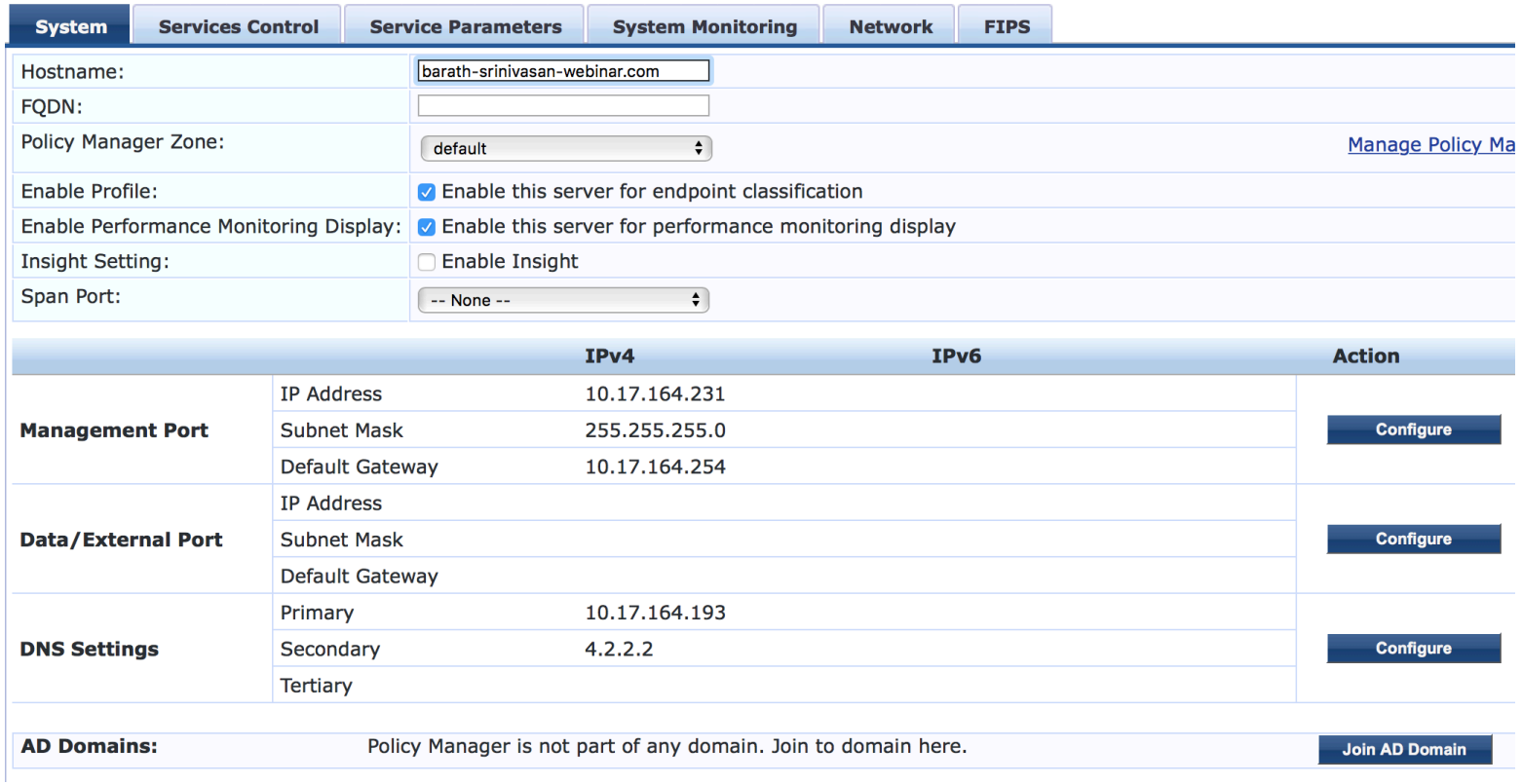
Click **Join AD Domain**

Domain controller: enter the FQDN of the domain controller and then press **Tab**

The following message is displayed,
Trying to determine the NetBIOS name…

Where, Clearpass searches for the NetBIOS name for the domain.

Joining an Active Directory Domain



Joining an Active Directory Domain

Once the NetBIOS domain name has been populated with the correct name,

In case of a controller name conflict,

a. **Use specified Domain controller**: Accept the default setting.

b. **Use default domain admin user [administrator]**: Accept the default setting

In a production environment, it is likely that an Administrative username that has permissions to join machines to the domain would be used for the default domain admin user, In that case, 1) disable (uncheck) the **Use default domain admin user [Administrator]** check box and
Enter the Administrative username and password in the fields provided

c. **Password**: Enter the password for the user account that will join Clearpass with the domain and then click **Save**

The Join AD Domain screen opens. The screen displays the message "*Adding host to AD domain*" and status during the joining process. Once it is complete – you see the message "*Added host to the domain*"

Joining an Active Directory Domain

The **Join AD Domain** status screen indicates that the services have restarted. The final line states that the selected Clearpass server joined the domain.

Click **Close**

You return to the Server Configuration page, and it now shows that the ClearPass server is joined to the domain.

Now that the ClearPass Policy Manager server has joined the domain, the server can authenticate users with the Active Directory.

AUTHENTICATION SOURCE AND AUTHORIZATION PROCESS

aruba
a Hewlett Packard Enterprise company

Authentication Source & Authorization Process

- During the NTLM authentication process, Clearpass queries Active Directory for a suitable domain controller to use to handle the authentication.

- Please note that when used with 802.1x EAP-PEAP-MsCHAPv2 services, the authentication process is separate from the Active Directory source in Clearpass, which in this context only handles authorization.

- Optionally, you can configure a list of domain controllers to be used for MsCHAPv2 authentication.

- If you do not specify this list of domain controllers, all available domain controllers obtained from DNS will be used for authentication.

Manually Specifying AD DC's for Authentication

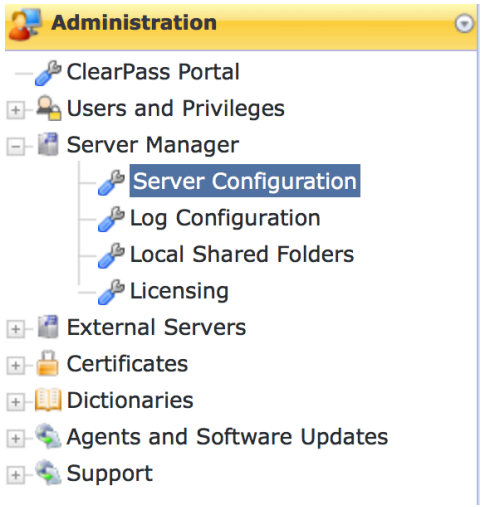
To Manually specify AD domain controllers for authentication

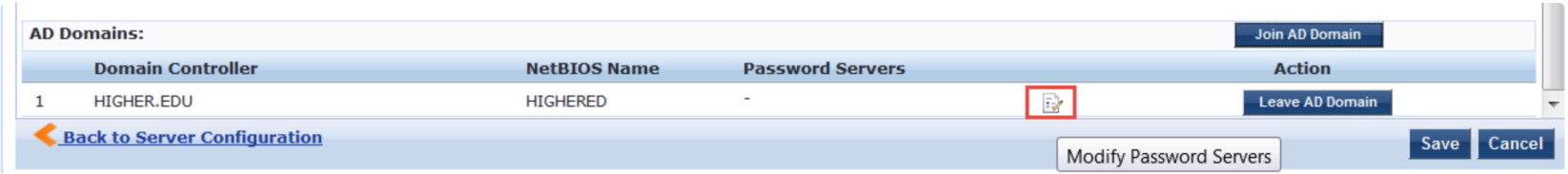
Go to **Administration > Server Manager > Server Configuration**

Select the Clearpass server name

The Server Configuration page for the selected server opens by default on the System tab

Click the **Modify Password Servers** as shown in the image below



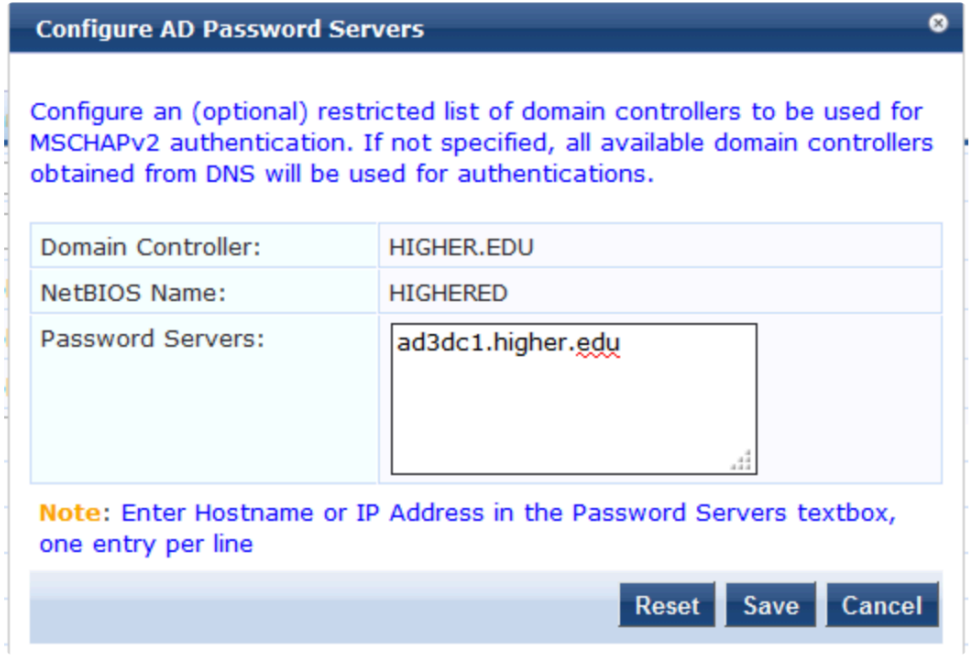


Manually Specifying AD DC's for Authentication

The **Configure AD Password Servers** screen appears

In the Password Servers text box, enter the names of the domain controllers that will be used for authentication (one entry per line)

When finished, click **Save**



DISASSOCIATING THE CLEARPASS SERVER FROM AN AD DOMAIN

aruba
a Hewlett Packard Enterprise company

Disassociating the clearpass server from AD domain

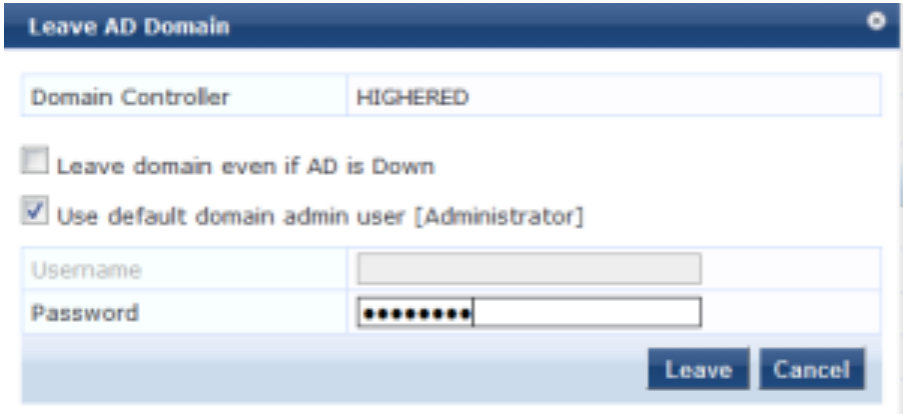
If a Clearpass Policy Manager server is already part of multiple AD domains, follow this procedure to disassociate the Clearpass appliance from an AD domain.

To disassociate a Clearpass server from an Active Directory domain,

Navigate to **Administration > Server Manager > Server Configuration**

Select the name of the Clearpass server which you want to disassociate from the domain

Click **Leave AD Domain**



Disassociating the clearpass server from AD domain

Once the *Leave AD Domain* dialog opens,

Enter the Administrator account password

The administrator account does not have to be the same account that is used to join the server to the domain, it only has to be an account with permissions to do this operation.

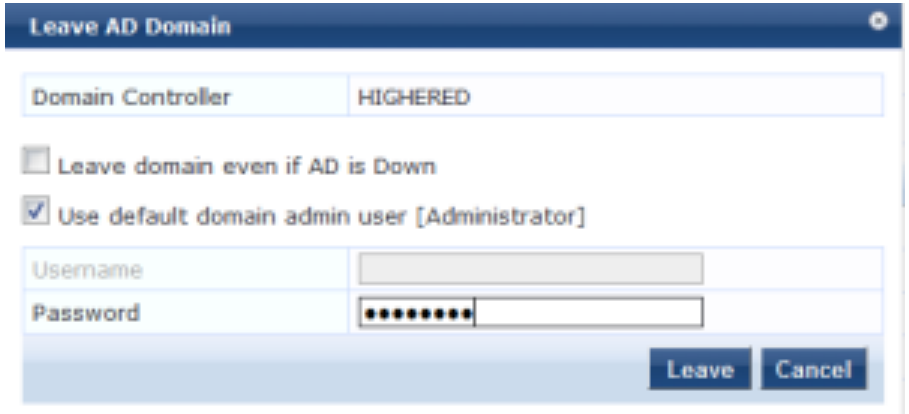
Click **Leave**

The Leave AD Domain status screen appears, with the message "*Removing host from the AD domain*", when the process is complete the status screen displays the message, "*Removed host from the domain*"

Click **Close**

When you return to the Server Configuration > System page, the Clearpass server is no longer listed in the AD Domains section

Click **Save**



THANK YOU!

aruba
a Hewlett Packard
Enterprise company