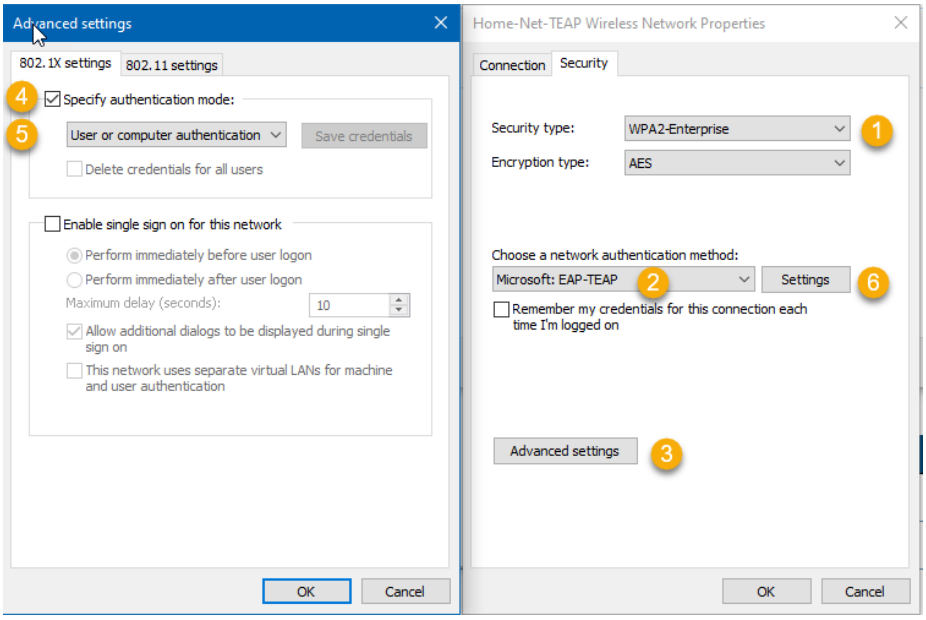
How to Configure EAP-TEAP (EAP-Chaining)

Change Log

Version	Date	Modified By	Comments
2020-04	04/28/2020	Zak Emerick	Initial Release

Windows/Supplicant Configuration

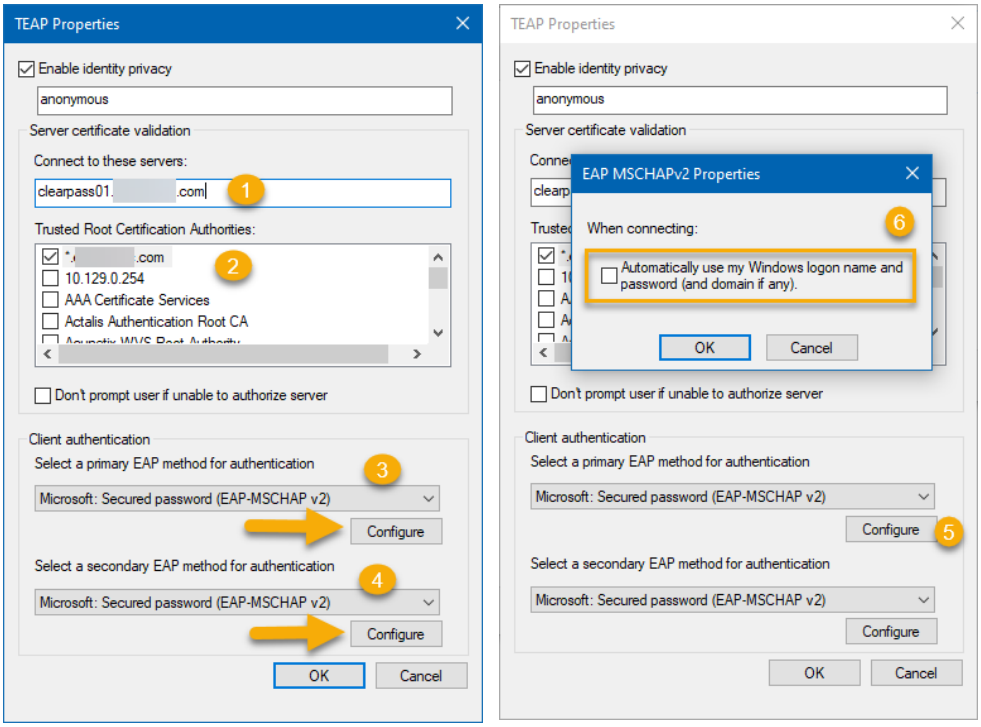
1. Open Network and Sharing Center
2. Select "Set up a new connection or network"
3. Walk-through the wizard but do not close the window at the end. Instead, click "Change connection settings" at the last screen
4. Under the Properties of the connection select the Security tab.
   a. NOTE: In a Windows Domain environment these settings should be pushed out with GPO.
5. Change the Authentication Method to **Microsoft: EAP-TEAP**.
6. Under Advanced Settings, select the Authentication mode as ***"User or Computer authentication".***



7. Select the Settings button.
8. Enter Server Certification Validation information. *(ALWAYS VALIDATE YOUR SERVERS/CERTIFICATES)*

9. Select your Primary and Secondary EAP methods. For my lab I have chosen EAP-MSCHAPv2 for both methods. This will 'submit' your computer account as METHOD-1, and your user account as METHOD-2.
    a. This is where you can decide to send one or both credentials during authentication. This is much different than the EAP-PEAPv0 implementation in the Windows supplicant. By default, the supplicant only sends the username during authentication while logged into the machine. (Assuming you have the User OR Computer authentication option selected in the EAP-PEAPv0 settings, of course.)

10. Select the Configure button and tick the box to auto submit your Windows logon name and password. (In my lab I have left this OFF because I am testing on a non-domain machine and I will submit my credentials manually.)



11. You are finished on the Windows/supplicant side.

Clearpass Configuration

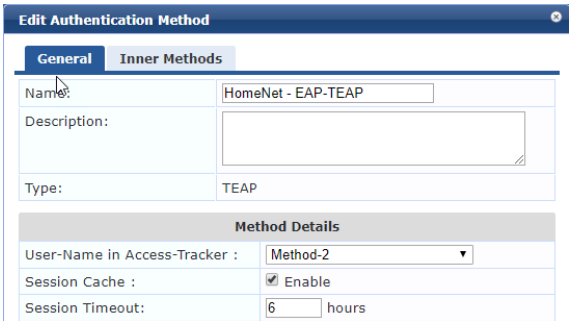
This is where things change a bit. In the traditional operation of Clearpass the Windows *machine* authenticated at (re)boot while sitting at the logon screen, primarily. When the user logged into the machine, the user's credentials were then sent to the controller/AP and passed on to CPPM. CPPM would have a cached machine authentication record for that machine. CPPM would combine the two credentials (by default within 24 hours), and if both succeeded you would be granted access. Typically, you would handle this in an Enforcement Policy by having a rule TIPS ROLE = [Machine Authenticated] & [User Authenticated]. I am of course, speaking very broadly.

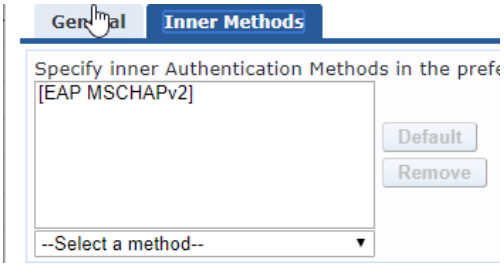
However, with EAP-TEAP (EAP-Chaining) [RFC 7170]. The credentials for both the Machine and User are sent at the same time. So, things can be implemented a bit differently.
This allows you to handle User + Machine authentication much more efficiently and gracefully. The two statuses (authentications) are broken down into METHOD-1 and METHOD-2. There are several other attributes to key off of, but I'm only highlighting the primary ones for a lab environment.

I will be covering a very simple implementation to get started.

Create a new Authentication Method (The EAP-TEAP method is not created after the upgrade to 6.9.x)

1. Navigate to Configuration -> Authentication -> Methods -> Add
   a. Name it appropriately.
   b. Type: **TEAP**
   c. User-Name in Access-Tracker: **Method-2** (The user will show up in the AT instead of the Machine account.)
   d. Inner Method Tab: **[EAP MSCHAPv2]**





Create Roles

I will only be covering key points of setting up the role mapping policy.

1. Create a new role: TEAP - Fully Authenticated
   a. This role will be given to a device that passes both METHOD-1 and METHOD-2 (Machine and User Authenticated)

2. Create a new role: TEAP - User Authenticated
   a. This role will be given to a device that only passes METHOD-2 (User Authentication)

Role Mapping Policy:

	Conditions	Role
1.		
2.		
3.	(Authentication:OuterMethod EQUALS TEAP) AND (Authentication:TEAP-Method-1-Status EQUALS Success) AND (Authentication:TEAP-Method-2-Status EQUALS Success)	HomeNet - TEAP - Fully Authenticated
4.	(Authentication:OuterMethod EQUALS TEAP) AND (Authentication:TEAP-Method-1-Status EQUALS Failure) AND (Authentication:TEAP-Method-2-Status EQUALS Success)	HomeNet - TEAP - User Authenticated

Create Service

I will only be covering key points of setting up the service.

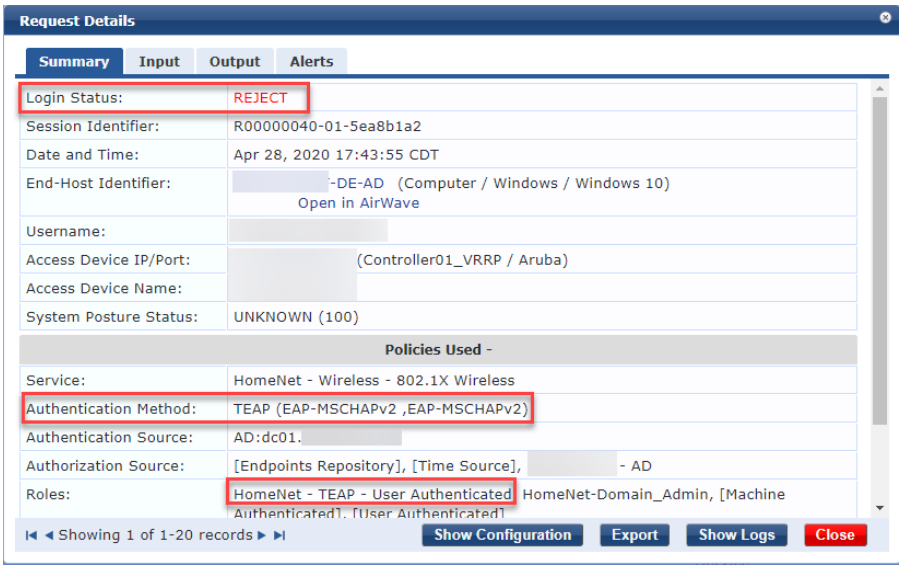
1. Add the new Authentication Source that you created earlier.
2. Make sure you add the Role Mapping policy that you created/modified above.
3. In the new / modified Enforcement Policy implement your Roles accordingly.

Enforcement Policy:

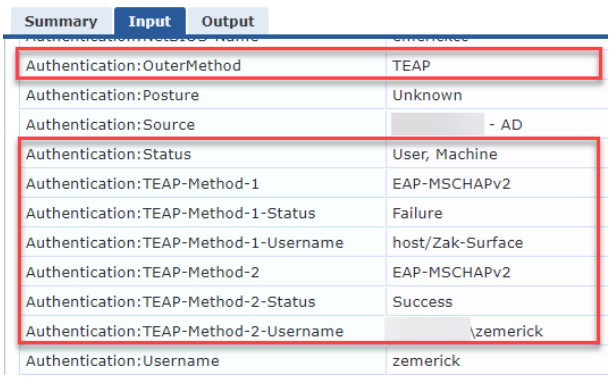
	Conditions	Enforcement Profiles
1.		
2.	(Tips:Role *EQUALS* HomeNet - TEAP - Fully Authenticated)	HomeNet - Wireless - Role - HomeNet-Secure
3.	(Tips:Role *EQUALS* HomeNet - TEAP - User Authenticated)	[Deny Access Profile]

Testing

Access Tracker:



RADIUS Input Tab:

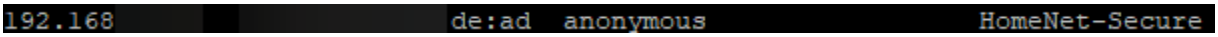


NOTES:

1. EAP-TEAP is not available in the Current Branch of Windows 10. It is only available in the Insider Preview builds (Build: 19613) as of 04/28/2020. I imagine it will be in the Current Branch Feature Update 2004. Clearpass added support for EAP-TEAP in version 6.9.x.

2. Enabling Identity Privacy in the supplicant settings results in the controller identifying the user as whatever is in that box. In my case: *"anonymous".*
   a. To get around this, you either need to untick this in the supplicant, or use an Enforcement Profile to send back the RADIUS:IETF:User-Name attribute.
   I chose this to keep the controller consistent with CPPM: ***%{Authentication:TEAP-Method-2-Username}***

Show User from controller:



Enforcement Profile to send correct username:

Attributes:

	Type	Name		Value
1.	Radius:IETF	User-Name	=	%{Authentication:TEAP-Method-2-Username}

3. For some reason CPPM is marking my device as [Machine Authenticated]. However, my machine cannot pass machine authentication as I am not domain joined. So, I am not sure if this is a bug, or not. I have not dug into this, yet.