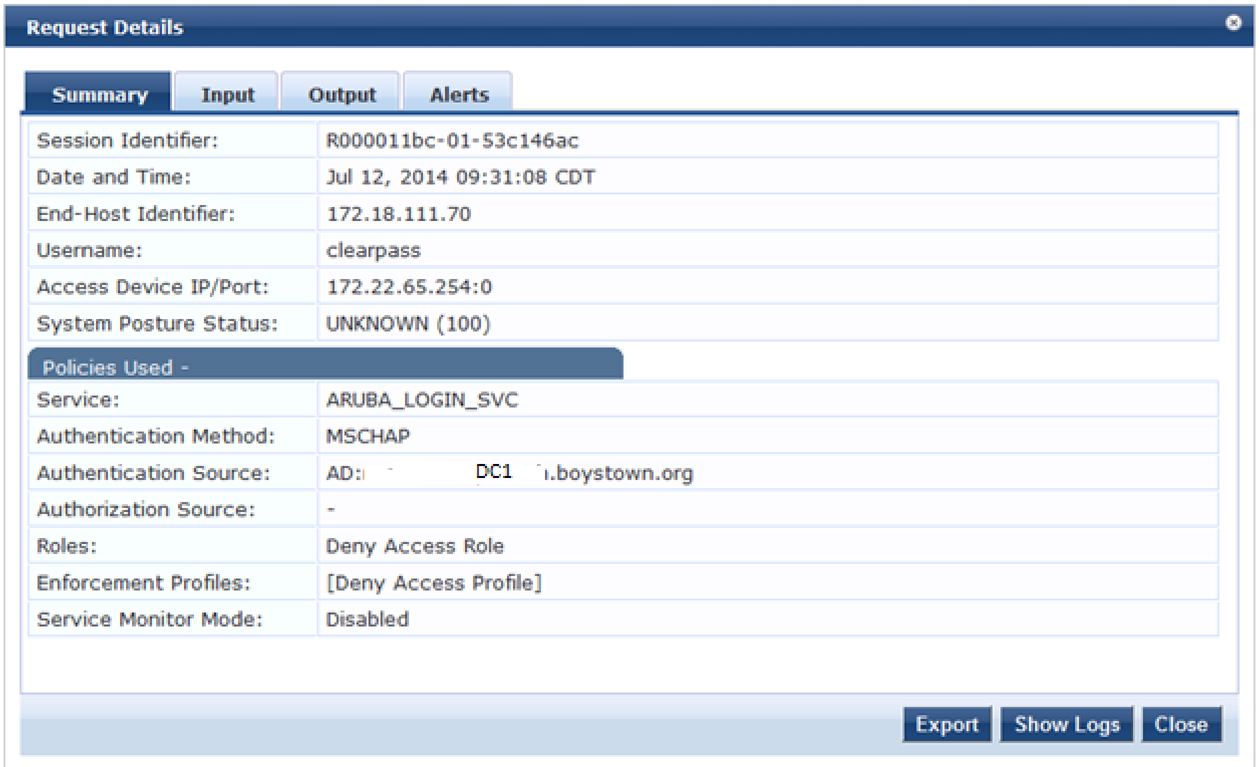
Troubleshoot User Authentication with CPPM July-MHC

If you have used Microsoft NPS or IAS for radius service and looked at Event Viewer to troubleshoot user denied access, it was probably a pain because Event Viewer lacks crucial information to identify the problem. On the other hand, CPPM Access Tracker is overwhelming with the amount of information it gives. But if you have a better understanding of this information, it will help to identify the problem quickly. In this troubleshooting guide, I will point out the meaning of the message in Access Tracker Request Details.

CASE #1: Fail, account not present in Authentication Sources

I am using CPPM to authenticate all logins to controllers, CPPM and AirWave, thus the service name ARUBA_LOGIN_ SVC. "clearpass" is the generic logon domain account for AirWave to logon to controllers who were denied.



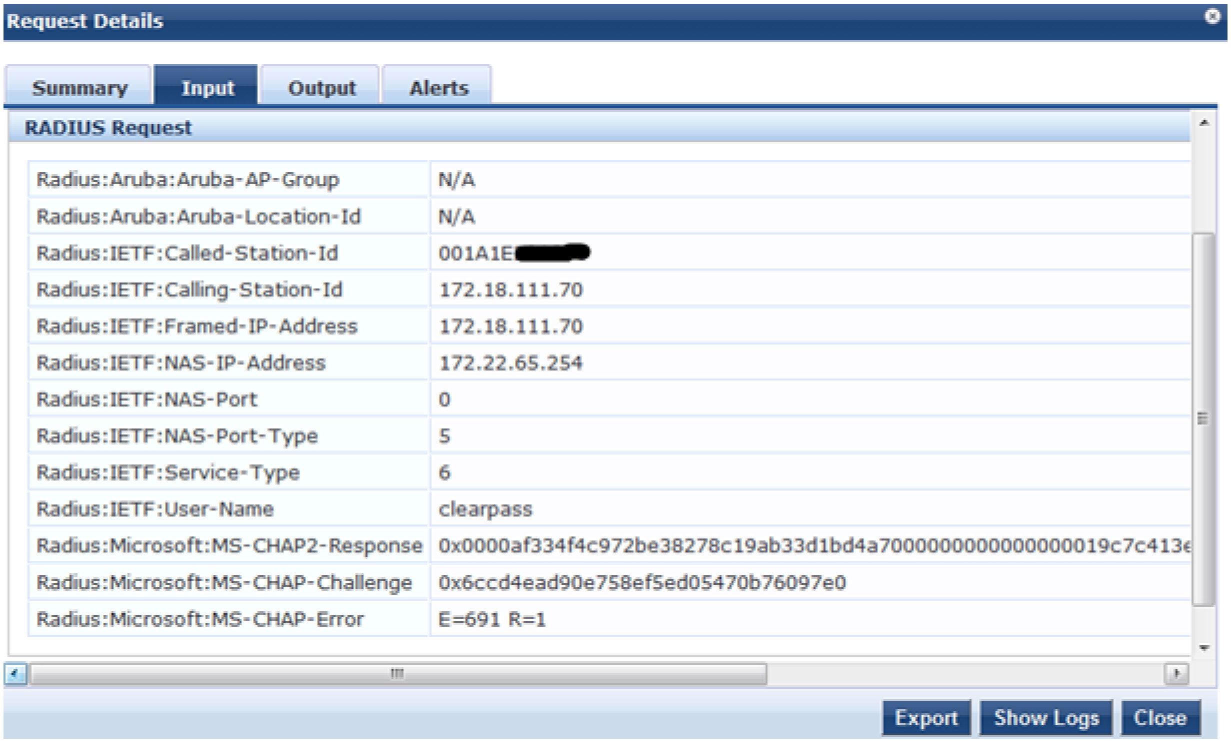
Request Details

Session Identifier:	R000011bc-01-53c146ac
Date and Time:	Jul 12, 2014 09:31:08 CDT
End-Host Identifier:	172.18.111.70
Username:	clearpass
Access Device IP/Port:	172.22.65.254:0
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	ARUBA_LOGIN_SVC
Authentication Method:	MSCHAP
Authentication Source:	AD:[redacted] DC1 [redacted].boystown.org
Authorization Source:	-
Roles:	Deny Access Role
Enforcement Profiles:	[Deny Access Profile]
Service Monitor Mode:	Disabled

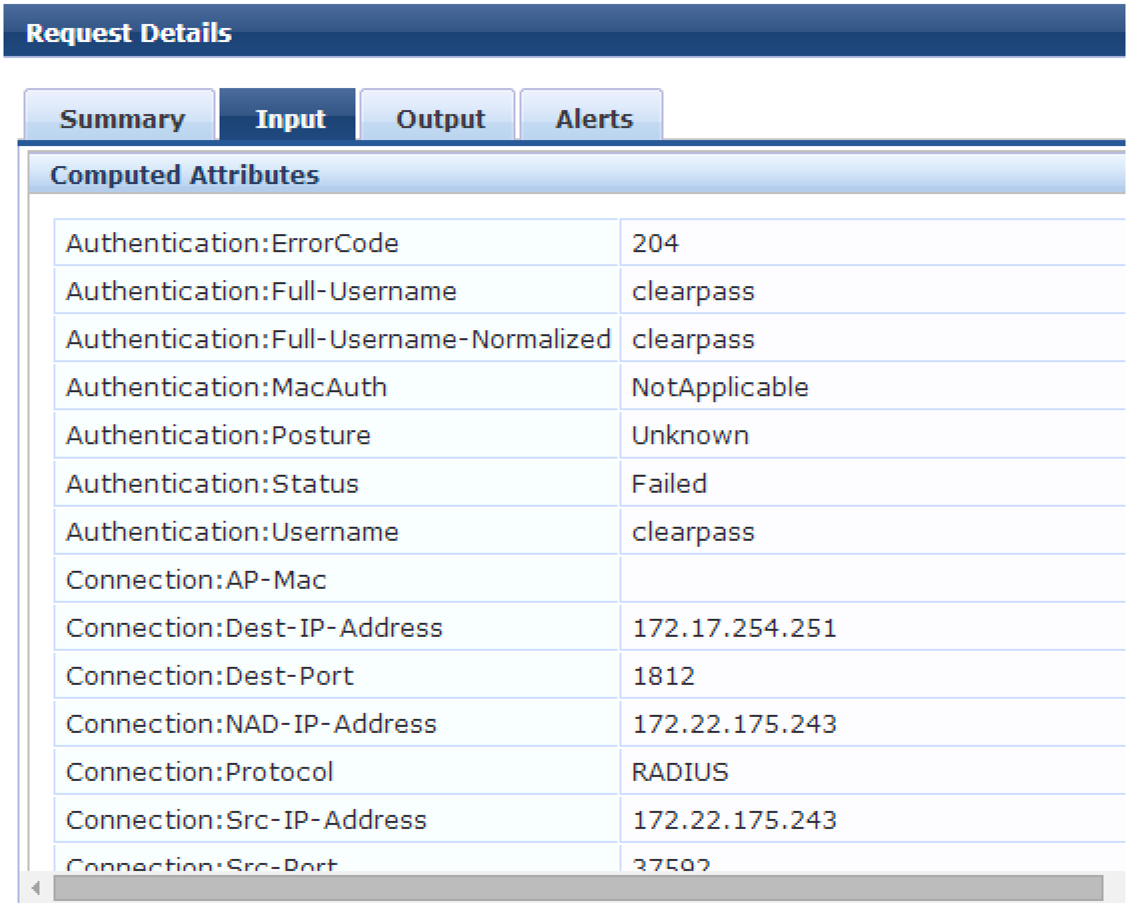
Figure 1: Start with Access Tracker Summary. By looking at Authentication Source and Roles you can tell this user was denied by DC1.boystown.org



RADIUS Request

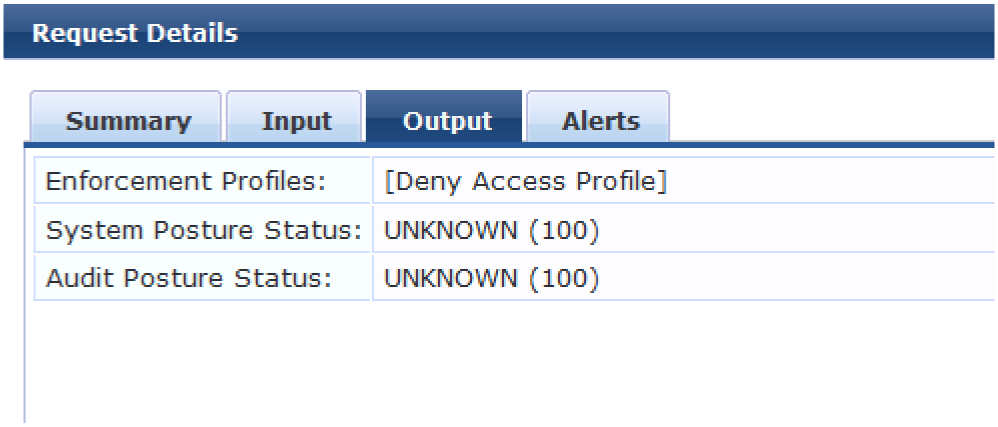
Radius:Aruba:Aruba-AP-Group	N/A
Radius:Aruba:Aruba-Location-Id	N/A
Radius:IETF:Called-Station-Id	001A1E[redacted]
Radius:IETF:Calling-Station-Id	172.18.111.70
Radius:IETF:Framed-IP-Address	172.18.111.70
Radius:IETF:NAS-IP-Address	172.22.65.254
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	5
Radius:IETF:Service-Type	6
Radius:IETF:User-Name	clearpass
Radius:Microsoft:MS-CHAP2-Response	0x0000af334f4c972be38278c19ab33d1bd4a70000000000000000019c7c413e
Radius:Microsoft:MS-CHAP-Challenge	0x6ccd4ead90e758ef5ed05470b76097e0
Radius:Microsoft:MS-CHAP-Error	E=691 R=1

Figure 2: Move to the next tab Input/RADIUS Request. This tab shows the request sent from the controller to CPPM. Called-Station-Id is the mac address of the client, which is my computer trying to ssh to the controller; Calling-Station-Id and Framed-IP-Address are the IP address of the client; NAS-IP-Address is the controller ip address



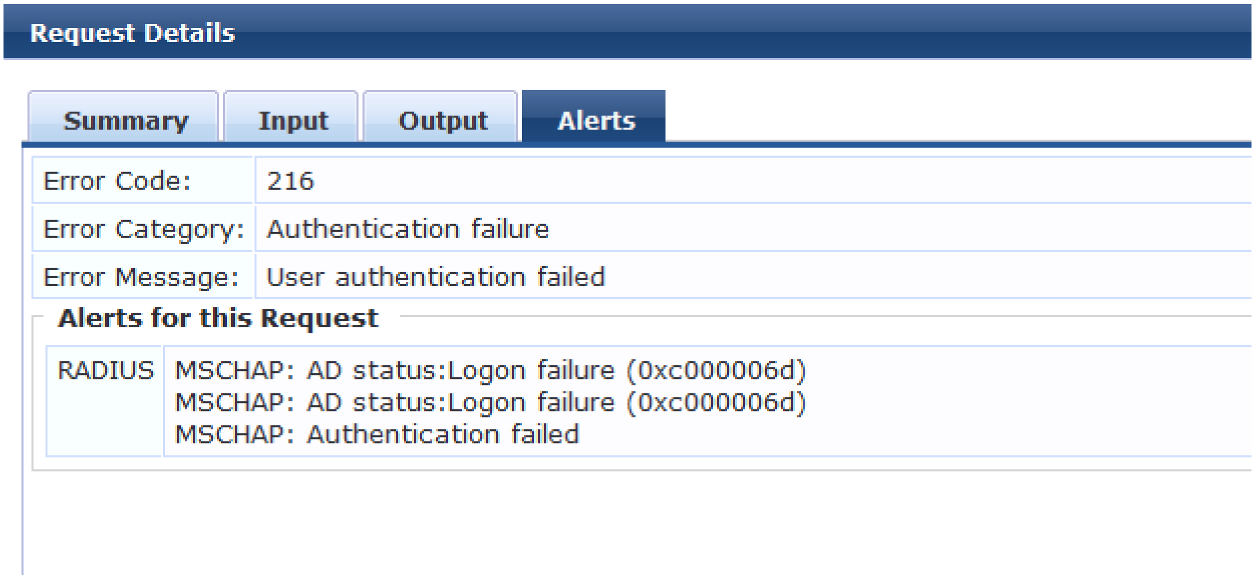
Authentication:ErrorCode	204
Authentication:Full-Username	clearpass
Authentication:Full-Username-Normalized	clearpass
Authentication:MacAuth	NotApplicable
Authentication:Posture	Unknown
Authentication:Status	Failed
Authentication:Username	clearpass
Connection:AP-Mac	
Connection:Dest-IP-Address	172.17.254.251
Connection:Dest-Port	1812
Connection:NAD-IP-Address	172.22.175.243
Connection:Protocol	RADIUS
Connection:Src-IP-Address	172.22.175.243
Connection:Src-Port	37592

Figure 3: Scroll down to Input/Computed Attributes: Dest-IP-Address is the CPPM doing the authentication; not useful information for this case.



Enforcement Profiles:	[Deny Access Profile]
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

Figure 4: not much information here, we already know the user was denied in Summary tab



Error Code:	216
Error Category:	Authentication failure
Error Message:	User authentication failed

Alerts for this Request

RADIUS	MSCHAP: AD status:Logon failure (0xc000006d) MSCHAP: AD status:Logon failure (0xc000006d) MSCHAP: Authentication failed

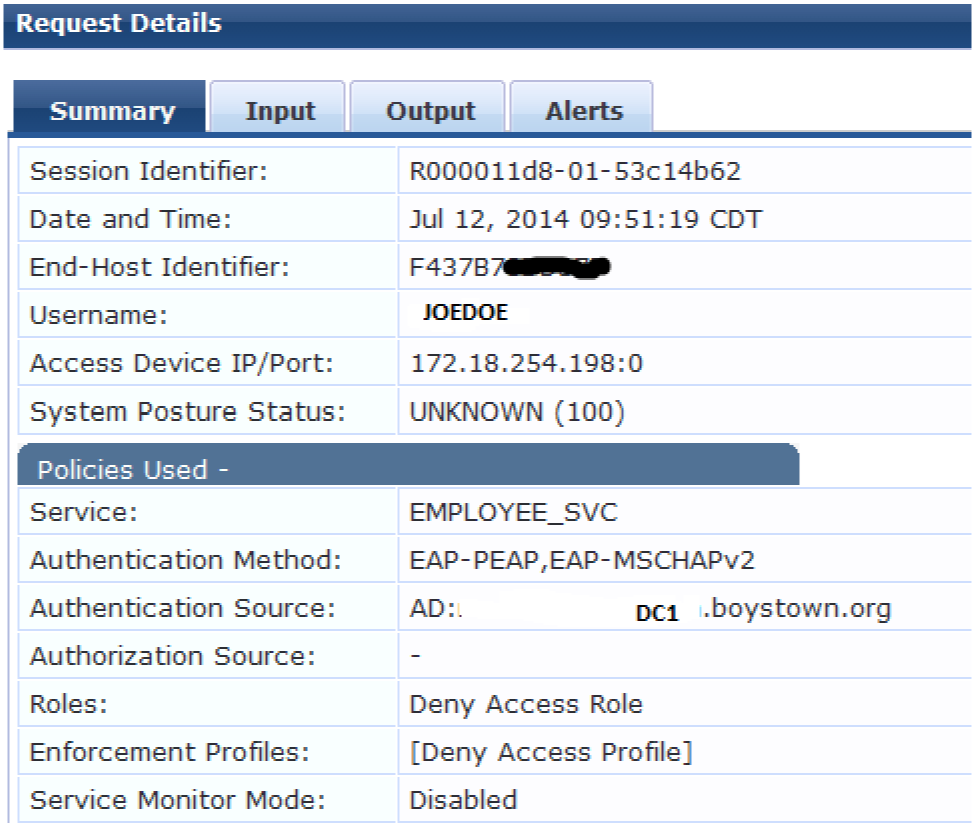
Figure 5: My authentication sources include two domains and Local User Repository; CPPM could not find this user in all three sources.

Conclusion: CPPM performed LDAP query two ADs and Admin User Repository for this user account. It found no user "clearpass" in any of them, so the authentication failed. User received default Deny Access Role.

Tips: If user was not found in AD, CPPM moved to the next Authentication Sources, but if user found and failed authentication, CPPM stopped and denied access immediately after the first Authentication Source.

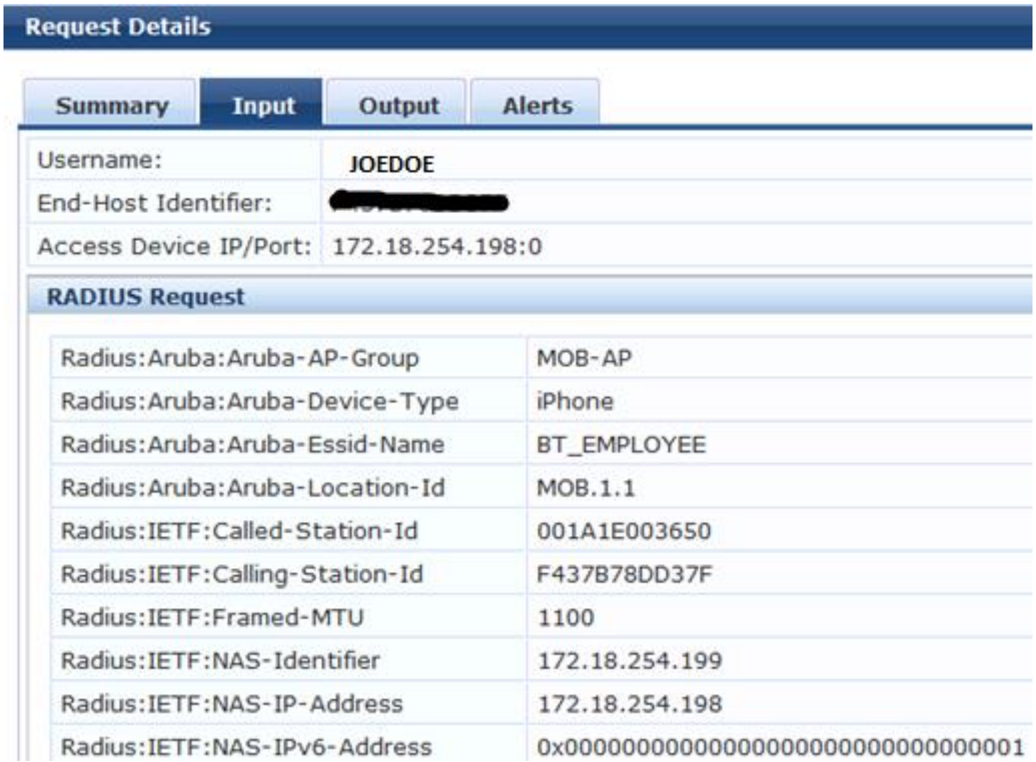
CASE #2: User did not update password in smart devices

Our AD requires that users change their passwords every three months. We support user's smart devices for syncing with Outlook, but when they change passwords on their desktops, they forget to update password in their phones.



Session Identifier:	R000011d8-01-53c14b62
Date and Time:	Jul 12, 2014 09:51:19 CDT
End-Host Identifier:	F437B7[redacted]
Username:	JOEDOE
Access Device IP/Port:	172.18.254.198:0
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	EMPLOYEE_SVC
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD: DC1 .boystown.org
Authorization Source:	-
Roles:	Deny Access Role
Enforcement Profiles:	[Deny Access Profile]
Service Monitor Mode:	Disabled

Figure 6: This Summary tells me user JOEDOE was denied by DC1. I am using certificate, so the Authentication Method EAP-PEAP, EAP-MSCHAPv2 indicates this is NOT a domain computer. If it is a domain computer, the Authentication Method is EAP-TLS



Username:	JOEDOE
End-Host Identifier:	[redacted]
Access Device IP/Port:	172.18.254.198:0

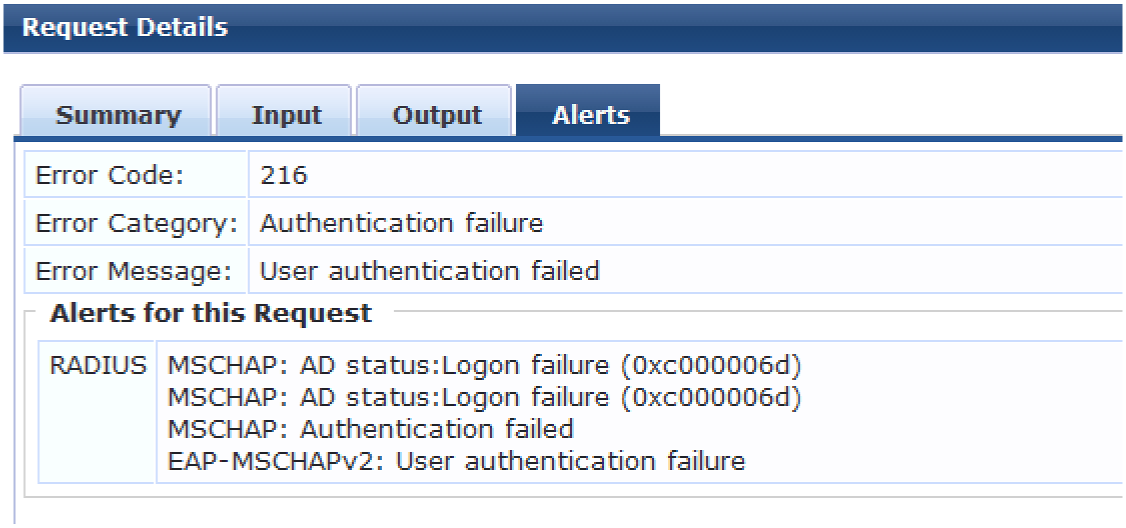
RADIUS Request

Radius:Aruba:Aruba-AP-Group	MOB-AP
Radius:Aruba:Aruba-Device-Type	iPhone
Radius:Aruba:Aruba-Essid-Name	BT_EMPLOYEE
Radius:Aruba:Aruba-Location-Id	MOB.1.1
Radius:IETF:Called-Station-Id	001A1E003650
Radius:IETF:Calling-Station-Id	F437B78DD37F
Radius:IETF:Framed-MTU	1100
Radius:IETF:NAS-Identifier	172.18.254.199
Radius:IETF:NAS-IP-Address	172.18.254.198
Radius:IETF:NAS-IPv6-Address	0x00000000000000000000000000000001

Figure 7: This Input/RADIUS Request has many useful information about this JOEDOE user:

1. End-Host Identifier: user device mac address
2. Access Device IP/Port: the controller that user and AP were terminated at
3. Aruba-AP-Group: what ap-group the AP that user associates belong to
4. Aruba-Device-Type: it is an iPhone, as I mentioned earlier, this is not a domain computer
5. Aruba-Location-Id, Called-Station-Id: the name and wired mac address of the AP
6. NAS-IP-Identifier and NAS-IP-Address: these are local controller and master controller respectively.

Tips: This tab lays out very nicely the authentication processes from user device to AP to local controller and finally to master controller. You can configure local controller to bypass master controller and send authenticate directly to CPPM by configure “ip radius source-interface” and “ip radius nas-ip” at the local controller.



Error Code:	216
Error Category:	Authentication failure
Error Message:	User authentication failed

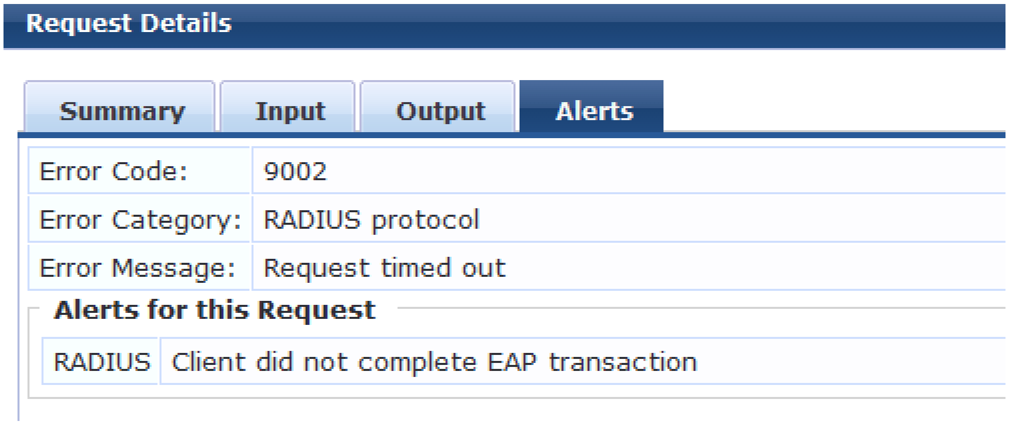
Alerts for this Request

RADIUS	MSCHAP: AD status:Logon failure (0xc000006d) MSCHAP: AD status:Logon failure (0xc000006d) MSCHAP: Authentication failed EAP-MSCHAPv2: User authentication failure

Figure 8: CPPM only tells you User authentication failure.

CASE #3: The "Time-Out" Failure

In Access Tracker you want to see a lot of black (ACCEPT). It is usually not a good sign if you see a lot of red (REJECT) or orange (TIME-OUT). The reason for REJECT is usually easy to find, but the TIME-OUT is not clear. The CPPM alert for TIME-OUT is "Client did not complete EAP transaction", it could be anything!!!



Error Code:	9002
Error Category:	RADIUS protocol
Error Message:	Request timed out

Alerts for this Request

RADIUS	Client did not complete EAP transaction

Figure 9: The Summary, Input and Output tabs are the same as the other cases, the only difference is in Alerts tab where CPPM indicates the client did not complete EAP transaction.

By default, each transaction has 10 seconds to complete or the client will time-out. The complication is where did the time go? Client took too long? Server is too busy? CPPM has bad configuration (it is never the problem with CPPM right?)?

The problems I have seen with client supplicant taking too much time to authenticate are the following: outdated driver, bad wireless card, wrong EAP type, low RSSI (too far from AP).

The problem with severs and domain is the System guys problem; a few times it was the server update the night before. But you can pinpoint this case quickly, because you will experience many domain issues along with slow LADP query, and you can blame another department for this.

Bad CPPM configuration: It happened to me once. My CPPM configured with the wrong DNSs. The DNSs were supposed to be for different domain, so CPPM jumped to another domain for DNS then went back to its domain for LDAP queries. Adding to the complication, the problem was intermittent and only happened during peak 30 min to an hour.

Conclusion:

CPPM is a wonderful product; if you have used it you probably agree it is the best NAC for wireless. But it is a monster. If you take some time to work with it, you will find it is useful to help you with your daily task as a network engineer, either for its quick and secured configuration for wireless access or troubleshooting the issues with authentication.