AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID :	ac1cff2a0000002752b0e49e
AAA session ID :	RK2-ISE-01/175651540/196
Date :	December 17,2013

Generated on December 18, 2013 1:36:32 PM EST

Actions
Troubleshoot Authentication
View Diagnostic Messages
Audit Network Device Configuration
View Network Device Configuration
View Server Configuration Changes

Authentication Summary	
Logged At:	December 17,2013 7:29:11.860 PM
RADIUS Status:	Authentication failed:15039 Rejected per authorization profile
NAS Failure:	
Username:	Ian Aquino
MAC/IP Address:	44:94:FC:5B:21:19
Network Device:	RK3W5508-01:172.28.255.42:
Allowed Protocol:	EAP-TLS
Identity Store:	
Authorization Profiles:	DenyAccess
SGA Security Group:	
Authentication Protocol :	EAP-TLS

⊟Authentication Result
RadiusPacketType=AccessReject AuthenticationResult=Passed

⊟Related Events		
Dec 17,13 7:30:06.783 PM	Radius accounting stop	Radius accouting stop

Dec 17,13 6:56:14.244 PM	Radius accounting start	Radius accounting start

⊟Authentication Details

Logged At:	December 17,2013 7:29:11.860 PM
Occurred At:	December 17,2013 7:29:11.859 PM
Server:	RK2-ISE-01
Authentication Method:	dot1x
EAP Authentication Method :	EAP-TLS
EAP Tunnel Method :	
Username:	Ian Aquino
RADIUS Username :	iaquino@aaeng.local
Calling Station ID:	44:94:FC:5B:21:19
Framed IP Address:	
Use Case:	
Network Device:	RK3W5508-01
Network Device Groups:	Device Type#All Device Types#WLC Centers,Location#All Locations#Rack04
NAS IP Address:	172.28.255.42
NAS Identifier:	RK3W5508-01
NAS Port:	13
NAS Port ID:	
NAS Port Type:	Wireless - IEEE 802.11
Allowed Protocol:	EAP-TLS
Service Type:	Framed
Identity Store:	
Authorization Profiles:	DenyAccess
Active Directory Domain:	
Identity Group:	
Allowed Protocol Selection Matched Rule :	WLAN_DOT1X_DVLAN
Identity Policy Matched Rule:	Default
Selected Identity Stores :	
Authorization Policy Matched Rule:	Default
SGA Security Group:	

AAA Session ID:	RK2-ISE-01/175651540/196
Audit Session ID:	ac1cff2a0000002752b0e49e
Tunnel Details:	Tunnel-Type=(tag=0) VLAN,Tunnel-Medium-Type=(tag=0) 802,Tunnel-Private-Group-ID=(tag=0) 128
Cisco-AVPairs:	audit-session-id=ac1cff2a0000002752b0e49e
Other Attributes:	ConfigVersionId=36,Device Port=32769,DestinationPort=1812, RadiusPacketType=AccessRequest,Protocol=Radius,Framed-MTU=1300, State=37CPMSessionID=ac1cff2a0000002752b0e49e;34SessionID=RK2-ISE-01/175651540/196;,attribute-89=00:,attribute-131=00:00:00:01, Airespace-Wlan-Id=17,CPMSessionID=ac1cff2a0000002752b0e49e, EndPointMACAddress=44-94-FC-5B-21-19,Device Type=Device Type# All Device Types#WLC Centers,Location=Location#All Locations# Rack04,Device IP Address=172.28.255.42,Called-Station-ID=34-a8-4e-80-de-50:AAENG-INTERNAL-DV
Posture Status:	
EPS Status:	

⊟Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
Evaluating Service Selection Policy
15048 Queried PIP
15048 Queried PIP
15048 Queried PIP
15048 Queried PIP
15048 Queried PIP
15048 Queried PIP
15004 Matched rule
11507 Extracted EAP-Response/Identity
12500 Prepared EAP-Request proposing EAP-TLS with challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12502 Extracted EAP-Response containing EAP-TLS challenge-response and accepting EAP-TLS as negotiated
12800 Extracted first TLS record; TLS handshake started
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message
12809 Prepared TLS CertificateRequest message
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response

12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
12571 ISE will continue to CRL verification if it is configured for specific CA
12571 ISE will continue to CRL verification if it is configured for specific CA
12811 Extracted TLS Certificate message containing client certificate
12812 Extracted TLS ClientKeyExchange message
12813 Extracted TLS CertificateVerify message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
12509 EAP-TLS full handshake finished successfully
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
11055 User name change detected for the session. Attributes for the session will be removed from the cache
15006 Matched Default Rule
22037 Authentication Passed
12506 EAP-TLS authentication succeeded
11503 Prepared EAP-Success
Evaluating Authorization Policy
15004 Matched rule
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject