AAA Protocol > RADIUS Authentication Detail

ACS session ID : hictatriuse031v/124919754/720950

Date : May 11, 2012

Generated on May 14, 2012 9:41:49 AM CEST

Authentication Summary	
Logged At:	May 11,2012 4:10:31.130 PM
RADIUS Status:	Authentication failed:24408 User authentication against Active Directory failed since user has entered the wrong password
NAS Failure:	
Username:	CTF7200
MAC/IP Address:	0024.3654.adfc
Network Device:	apphili21:10.2.111.168:39473
Access Service:	Wireless
Identity Store:	AD1
Authorization Profiles:	
CTS Security Group:	
Authentication Method:	MSCHAPV1

Actions

Troubleshoot Authentication

View Diagnostic Messages

Audit Network Device Configuration

View Network Device Configuration

View ACS Configuration Changes

⊞Authentication Result

RadiusPacketType=AccessReject
AuthenticationResult=Failed

⊞Session Events

May 11,12 4:10:31.130 PM	**Radius authentication failed for USER: CTF7200 MAC: 0024.3654.adfc AUTHTYPE:**	**Radius authentication failed**

⊞Authentication Details

Logged At:	May 11,2012 4:10:31.130 PM
ACS Time:	May 11,2012 4:10:31.110 PM
ACS Instance:	hictatriuse031v
Authentication Method:	MSCHAPV1
EAP Authentication Method :	LEAP
EAP Tunnel Method :	
User	
ACS Username:	CTF7200
RADIUS Username :	CTF7200
Calling Station ID:	0024.3654.adfc
Framed IP Address:	
Host Lookup:	
Network Device	
Network Device:	apphili21
Network Device Groups:	Device Type:All Device Types:Cisco:Cisco Aironet 1240 AG Series Location:All Locations:Global
NAS IP Address:	10.2.111.168
NAS Identifier:	apphili21
NAS Port:	39473
NAS Port ID:	39473
NAS Port Type:	Wireless - IEEE 802.11
Access Policy	
Access Service:	Wireless
Identity Store:	AD1
Authorization Profiles:	
Exception Authorization Profiles:	
Active Directory Domain:	msnet.railb.be

Identity Group:	
Access Service Selection Matched Rule :	Wireless
Identity Policy Matched Rule:	Compatibility for exotic devices
Selected Identity Stores :	AD1, Internal Users
Query Identity Stores:	
Selected Query Identity Stores:	
Group Mapping Policy Matched Rule:	
Authorization Policy Matched Rule:	
Authorization Exception Policy Matched Rule:	

CTS

CTS Security Group:	

Other

ACS Session ID:	hictatriuse031v/124919754/720950
Audit Session ID:	
Tunnel Details:	
H323 Attributes:	
SSG Attributes:	
Cisco-AVPairs:	
Other Attributes:	ACSVersion=acs-5.2.0.26-B.3075 ConfigVersionId=403 Device Port=1645 RadiusPacketType=AccessRequest Protocol=Radius ExternalErrorCode=-1073741718 Service-Type=Login Framed-MTU=1400 State=42SessionID=hictatriuse031v/124919754/720950; Called-Station-ID=003a.99e7.0072 Device IP Address=10.2.111.168

⊞Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
Evaluating Service Selection Policy	
15004	Matched rule
15012	Selected Access Service - Wireless
11507	Extracted EAP-Response/Identity
12700	Prepared EAP-Request proposing LEAP with challenge.
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12702	Extracted EAP-Response containing LEAP challenge-response and accepting LEAP as negotiated.
Evaluating Identity Policy	
15004	Matched rule
15013	Selected Identity Store - AD1
24430	Authenticating user against Active Directory
24408	User authentication against Active Directory failed since user has entered the wrong password
22057	The advanced option that is configured for a failed authentication request is used.
22061	The 'Reject' advanced option is configured in case of a failed authentication request.
12706	LEAP authentication failed; Finishing protocol.
11504	Prepared EAP-Failure
11003	Returned RADIUS Access-Reject