```
fr-jo-sw01#sh auth ses int g 6/0/7 det
            Interface:  GigabitEthernet6/0/7
               IIF-ID:  0x2353E022
          MAC Address:  00a6.caxx.ae00
         IPv6 Address:  fe80::2a6:caff:fe28:ae00
         IPv4 Address:  10.x.x.38
            User-Name:  we-accesspoint
               Status:  Unauthorized
               Domain:  UNKNOWN
       Oper host mode:  multi-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0A2425FA0000140BC321E0AC
      Acct Session ID:  Unknown
               Handle:  0xfb000481
       Current Policy:  POLICY_Gi6/0/7


Method status list:
       Method           State
        dot1x           Stopped
```

Overview

Event	5206 PAC provisioned
Username	we-accesspoint
Endpoint Id	00:A6:CA:xx:AE:00
Endpoint Profile	Cisco-AP-Aironet-2700
Authentication Policy	Wired 802.1X >> Default
Authorization Policy	Wired 802.1X >> Accesspoint
Authorization Result	

Authentication Details

Source Timestamp	2018-09-10 12:58:41.594
Received Timestamp	2018-09-10 12:58:41.593
Policy Server	s-our-ise03
Event	5206 PAC provisioned
Username	we-accesspoint
User Type	User
Endpoint Id	00:A6:CA:xx:AE:00
Calling Station Id	00-A6-CA-xx-AE-00
Endpoint Profile	Cisco-AP-Aironet-2700
IPv4 Address	10.x.x.38
IPv6 Address	0xffcfbea870
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:we-accesspoints,Profiled
Audit Session Id	0A2425FA0000140BC321E0AC
Authentication Method	dot1x
Authentication Protocol	EAP-FAST (EAP-MSCHAPv2)
Service Type	Framed
Network Device	fr-jo
Device Type	All Device Types#IOS Devices
Location	All Locations#fr#Jonage
NAS IPv4 Address	10.x.x.250
NAS Port Id	GigabitEthernet6/0/7
NAS Port Type	Ethernet
Response Time	2 milliseconds

Other Attributes

ConfigVersionId	19
DestinationPort	1812
Protocol	Radius
NAS-Port	50607
Framed-MTU	1472
State	37CPMSessionID=0A2425FA0000140BC321E0AC;36SessionID=s-our-ise03/325880615/43752;
cisco-nas-port	GigabitEthernet6/0/7
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	s-our-ise03/325880615/43752
SelectedAuthenticationIdentityStores	AD-ourdomain
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Accesspoint
IssuedPacInfo	Issued PAC type=Tunnel V1A with expiration time: Sun Dec 9 11:58:41 2018
CPMSessionID	0A2425FA0000140BC321E0AC
EndPointMACAddress	00-A6-CA-xx-AE-00
EapChainingResult	No chaining
ISEPolicySetName	Wired 802.1X
IdentitySelectionMatchedRule	Default
IsMachineIdentity	false
TLSCipher	ADH-AES128-SHA
TLSVersion	TLSv1
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Profiled
Network Device Profile	Cisco
Location	Location#All Locations#fr#Jo
Device Type	Device Type#All Device Types#IOS Devices
IPSEC	IPSEC#Is IPSEC Device#No
All BUs	All BUs#All BUs#BU1
EnableFlag	Enabled
RADIUS Username	we-accesspoint
NAS-Identifier	fr-jo-sw-rz01
Device IP Address	10.x.x.250

CiscoAVPair	service-type=Framed, audit-session-id=0A2425FA0000140BC321E0AC, method=dot1x, addrv6=0xffcfbea870, vlan-id=0

Session Events

2018-09-10 12:58:41.593 PAC provisioned

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
15048	Queried PIP - Radius.Called-Station-ID (4 times)
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12101	Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100	Prepared EAP-Request proposing EAP-FAST with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12102	Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12808 Prepared TLS ServerKeyExchange message

12810 Prepared TLS ServerDone message

12811 Extracted TLS Certificate message containing client certificate

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

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

12131 EAP-FAST built anonymous tunnel for purpose of PAC provisioning

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

12125 EAP-FAST inner method started

11521 Prepared EAP-Request/Identity for inner EAP method

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

11522 Extracted EAP-Response/Identity for inner EAP method

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
11808	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated
15041	Evaluating Identity Policy
22072	Selected identity source sequence - OUR_Identity_Source_Seq
15013	Selected Identity Source - AD-ourdomain
24430	Authenticating user against Active Directory - AD-ourdomain
24325	Resolving identity - we-accesspoint
24313	Search for matching accounts at join point - ourdomain.com
24318	No matching account found in forest - ourroot.com
24322	Identity resolution detected no matching account
24352	Identity resolution failed - ERROR_NO_SUCH_USER
24412	User not found in Active Directory – AD-ourdomain
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore - we-accesspoint
24212	Found User in Internal Users IDStore
22037	Authentication Passed
11824	EAP-MSCHAP authentication attempt passed
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
11810	Extracted EAP-Response for inner method containing MSCHAP challenge-response
11814	Inner EAP-MSCHAP authentication succeeded
11519	Prepared EAP-Success for inner EAP method
12128	EAP-FAST inner method finished successfully
12966	Sent EAP Intermediate Result TLV indicating success
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request

11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
12126	EAP-FAST cryptobinding verification passed
12200	Approved EAP-FAST client Tunnel PAC request
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
15048	Queried PIP - Session.EPSStatus
15048	Queried PIP - CERTIFICATE.Issuer - Common Name
15016	Selected Authorization Profile -
22081	Max sessions policy passed
22080	New accounting session created in Session cache
12964	Sent EAP Result TLV indicating success
12169	Successfully finished EAP-FAST tunnel PAC provisioning/update
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
11401	Prepared RADIUS Access-Reject after the successful in-band PAC provisioning
61025	Open secure connection with TLS peer
11504	Prepared EAP-Failure
11003	Returned RADIUS Access-Reject