DHCP Parameter Request List Option 55 Used to Profile Endpoints Configuration Example

Contents

Introduction

This document describes the use of the DHCP Parameter Request List option 55 as an alternative method to profile devices that use the Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have:

- Basic knowledge of the DHCP discovery process
- Experience with the use of ISE to configure custom profiling rules

Components Used

The information in this document is based on these software and hardware versions:

- ISE Version 3.0
- Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

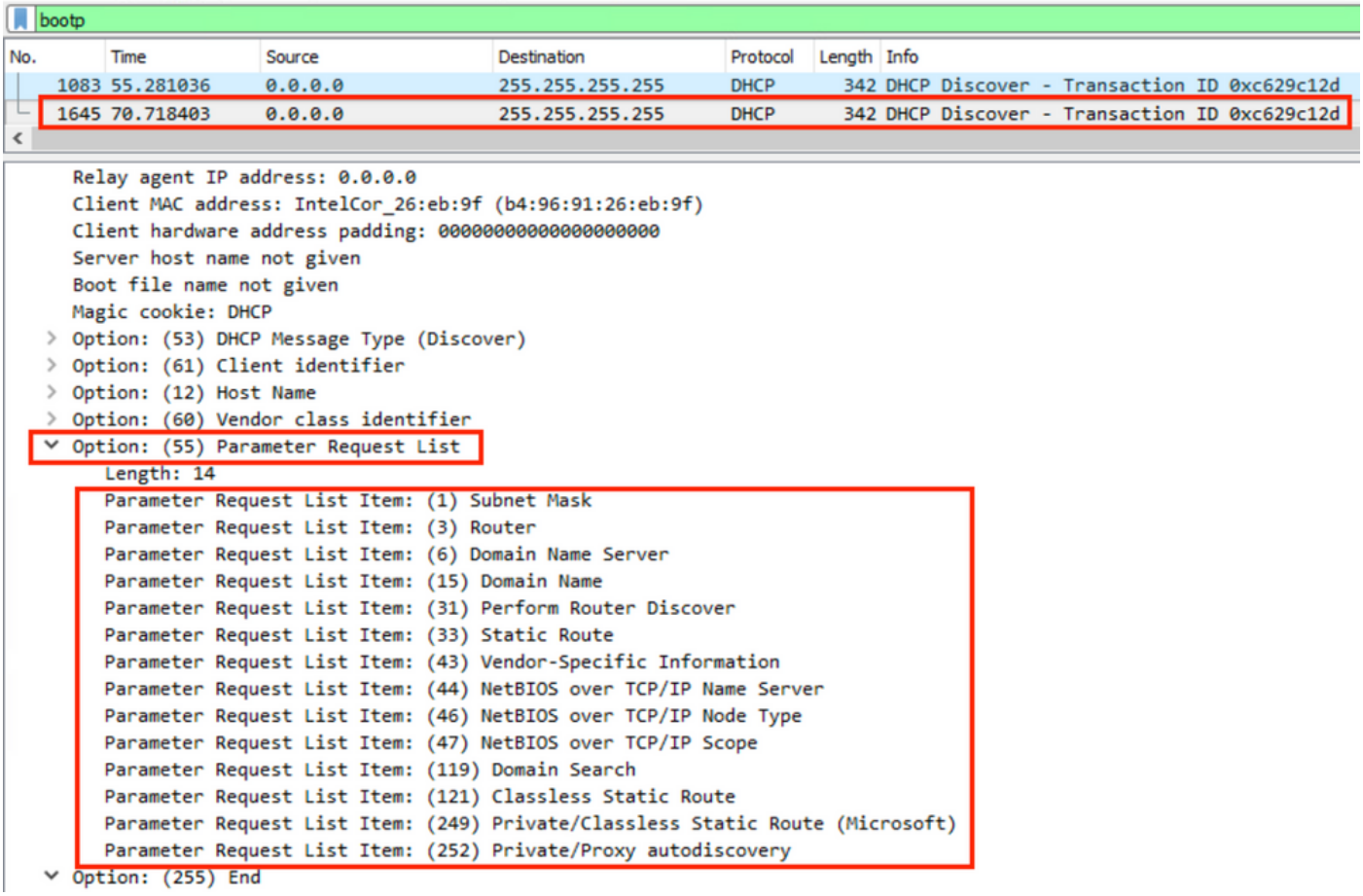
Background Information

In production ISE deployments, some of the more commonly deployed profiling probes include RADIUS, HTTP, and DHCP. With URL redirection in the center of the ISE workflow, the HTTP probe is widely used in order to capture important endpoint data from the User-Agent string. However, in some production use cases, a URL redirection is not desired and Dot1x is preferred, which makes it more difficult to accurately profile an endpoint. For example, an employee PC that connects to a corporate Service Set Identifier (SSID) gets full access while its personal iDevice (iPhone, iPad, iPod) gets Internet access only. In both scenarios, the users are profiled and dynamically mapped to a more specific identity group for authorization profile matching that does not rely on the user to open a web browser. Another commonly used alternative is hostname matching. This solution is imperfect because users might change the endpoint hostname to a non-standard value.

In corner cases such as these, the DHCP probe and DHCP Parameter Request List option 55 can be used as an alternative method to profile these devices. The Parameter Request List field in the DHCP packet can be used in order to fingerprint an endpoint operating system much like an Intrusion Prevention System (IPS) uses a signature in order to match a packet. When the endpoint operating system sends a DHCP discover or request packet on the wire, the manufacturer includes a numeric list of DHCP options that it intends to receive from the DHCP server (default router, Domain Name Server (DNS), TFTP server, etc.). The order by which the DHCP client requests these options from the server is fairly unique and can be used in order to fingerprint a particular source operating system. The use of the Parameter Request List option is not as exact as the HTTP User-Agent string, however, it is far more controlled than the use of hostnames and other statically-defined data.

> **Note**: The DHCP Parameter Request List option is not a perfect solution because the data it produces is vendor-dependent and can be duplicated by multiple device types.

Before you configure the ISE profiling rules, use Wireshark captures from an endpoint/Switched Port Analyzer (SPAN) or Transmission Control Protocol (TCP) Dump captures on ISE in order to evaluate the Parameter Request List options in the DHCP packet (if present). This sample capture displays the DHCP Parameter Request List options for a Windows 10.

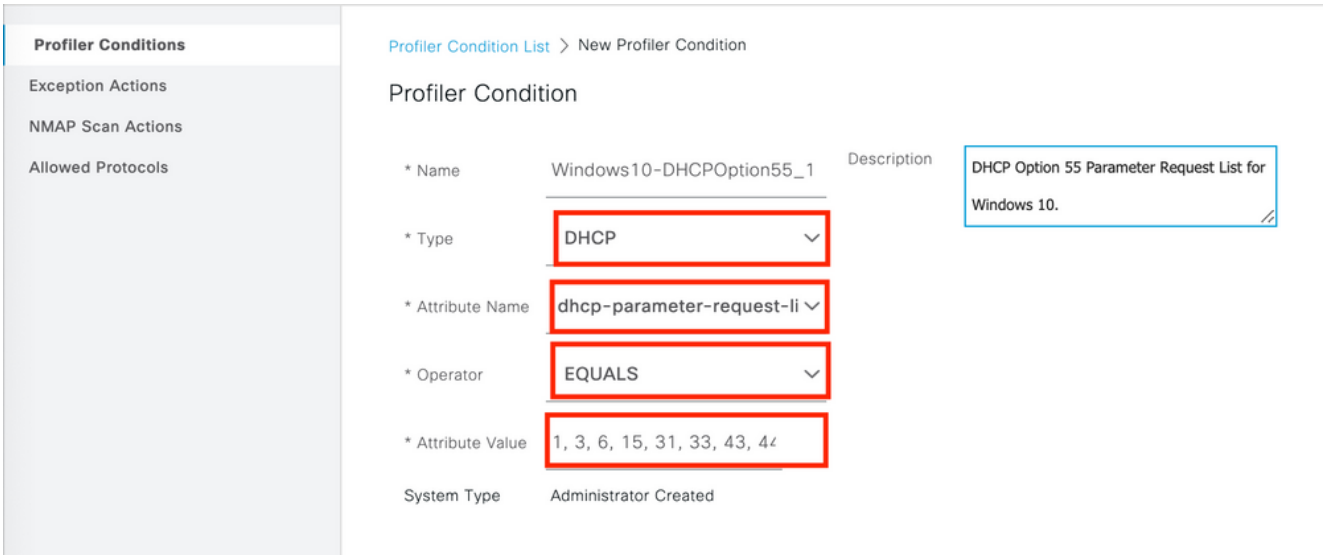


The Parameter Request List string that results is written in the following comma-separated format: 1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252. Use this format when configuring custom profiling conditions in ISE.

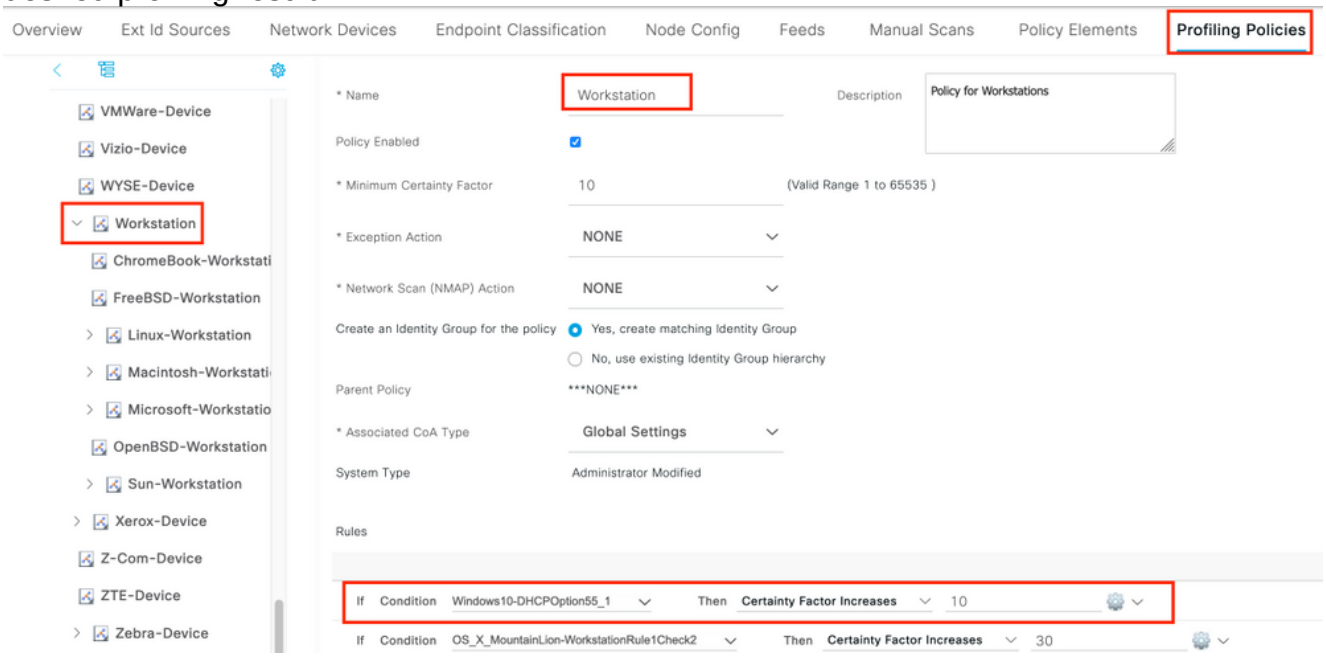
The configuration section demonstrates the use of custom profiling conditions to match Windows 10 workstation into a **Windows10-Workstation**.

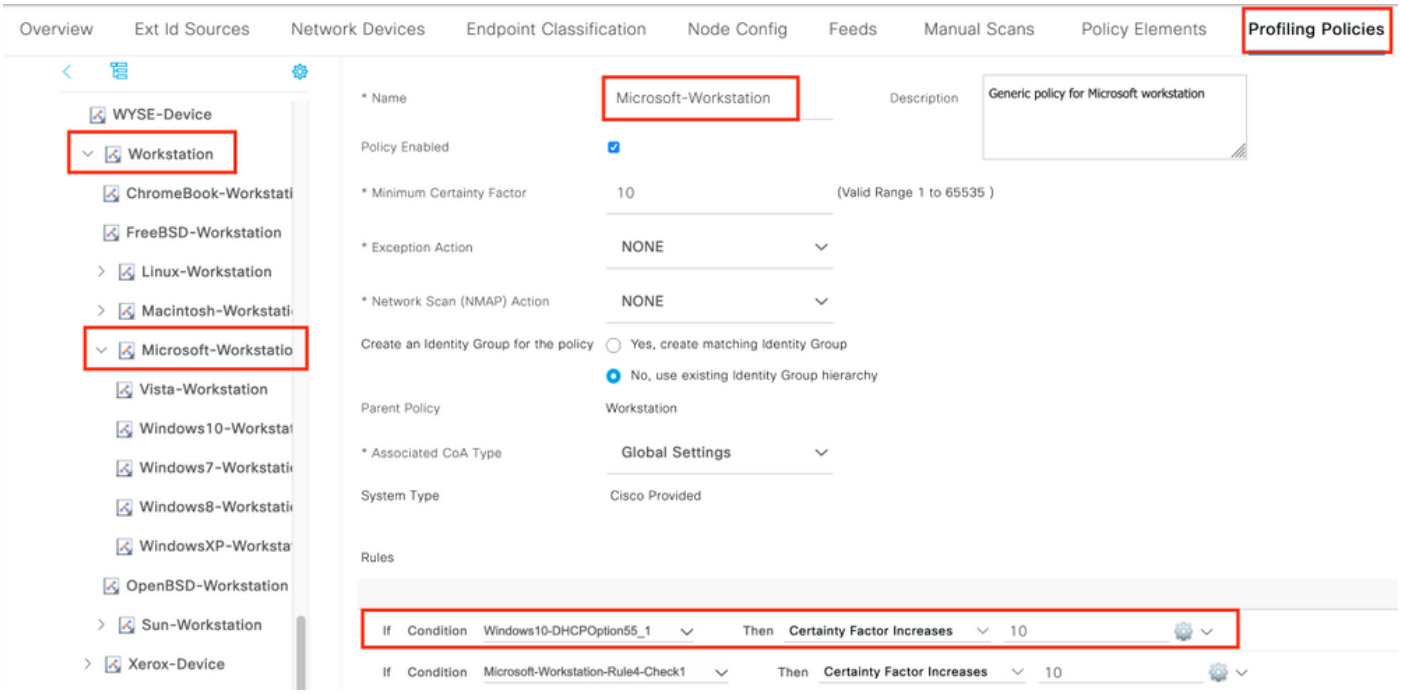
Configure

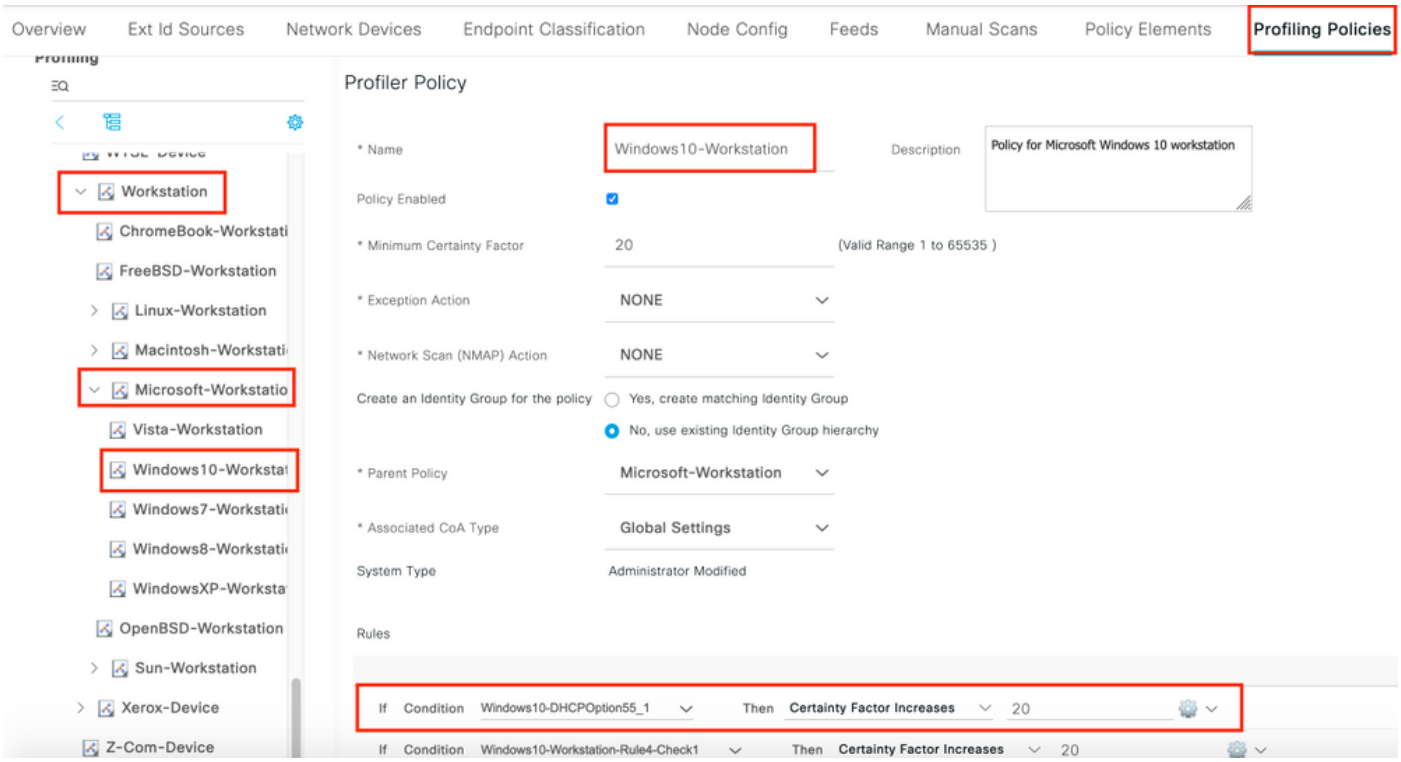
1. Log on to the ISE admin GUI and navigate to **Policy > Policy Elements > Conditions > Profiling**. Click **Add** in order to add a new custom profiling condition. In this example, we are using Windows 10 Parameter Request List fingerprints. Refer to **Fingerbank.org** for a complete list of Parameter Request List values.
   Note: The **Attribute Value** text box might not display all of the numeric options, and you might need to scroll with the mouse or keyboard in order to view the full list.



2. With the custom conditions defined, navigate to **Policy > Profiling > Profiling Policies** in order to modify a current profiling policy or in order to configure a new one. In this example, the default **Workstation, Microsoft-Workstation, Windows10-Workstation** policies are edited in order to include the new Parameter Request List conditions. Add a new compound condition to the **Workstation, Microsoft-Workstation, Windows10-Workstation** profiler policy rule as shown below. Modify the **Certainty Factor** as required in order to achieve the desired profiling result.





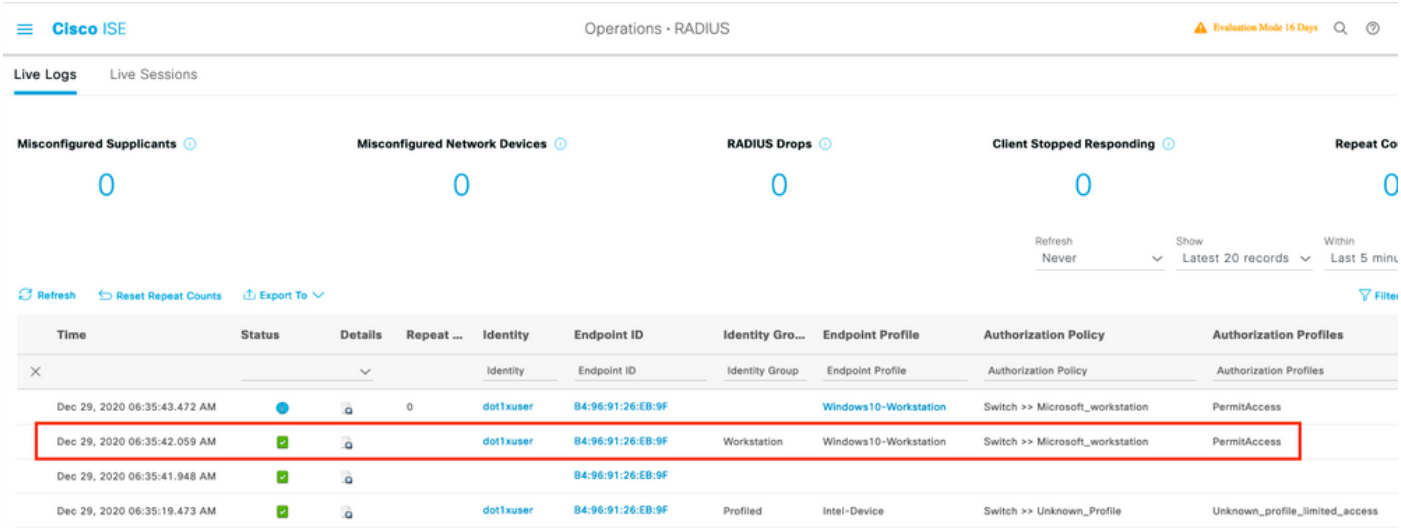


Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Verify

Step 1 -

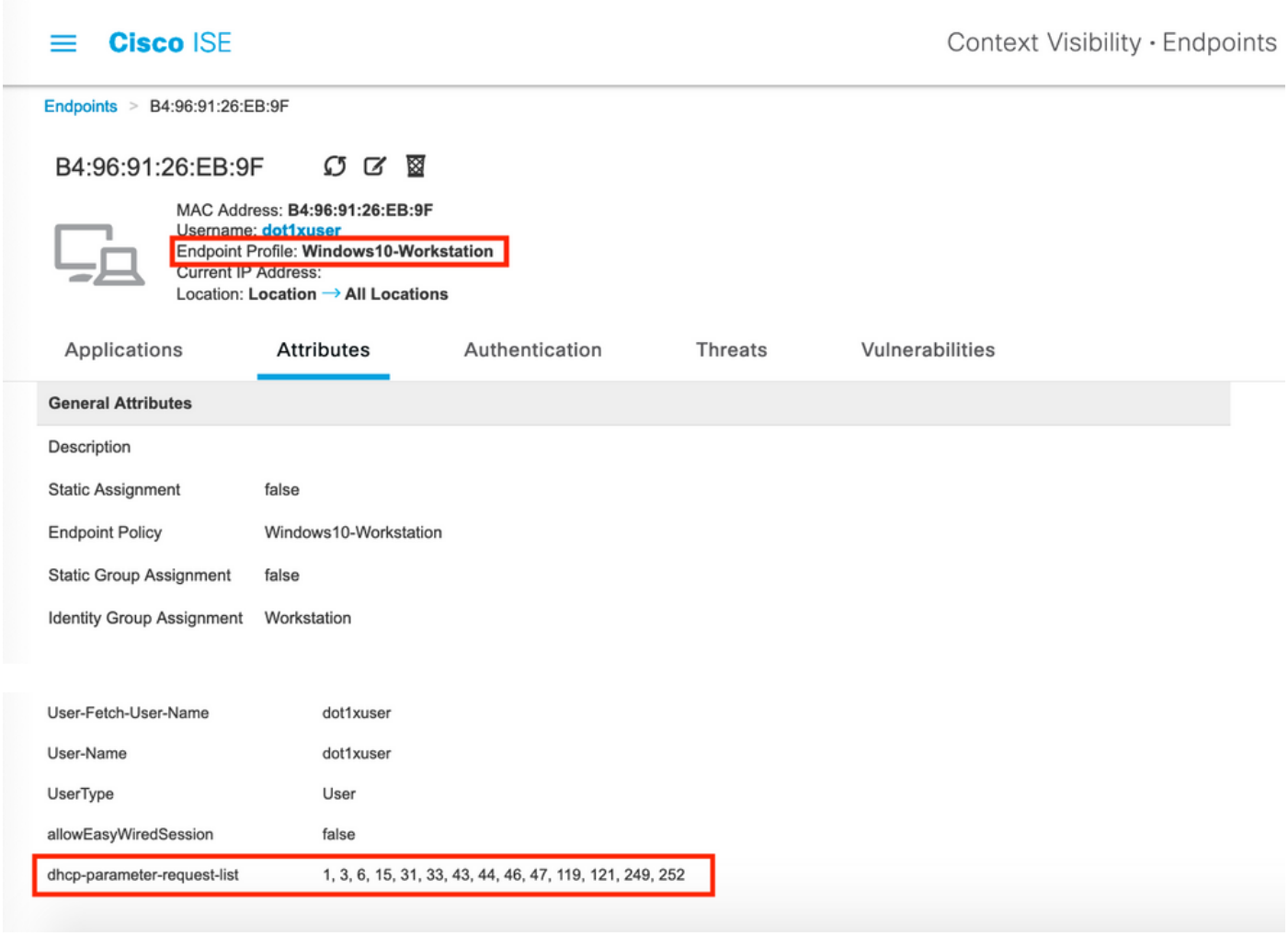
Navigate to ISE > Operations > Live Logs . 1st authentication matches the Unknown Authorization Policy and limited access is given to ISE . After device is profiled , ISE triggers CoA and another authentication request is received on ISE and matches the new profile - Windows10 Workstation .



Step 2 -

Use this section in order to confirm that your configuration works properly.

- Navigate to **Context Visibility > Endpoints,** search the endpoint, click edit.
- Confirm that the **EndPointPolicy** is Window10-Workstation and that the **dhcp-parameter-request-list** values match the condition values previously configured.



Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration.

- Verify that the DHCP packets reached the ISE policy nodes that perform the profiling function (with helper-address or SPAN).
- Use the **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump** tool in order to natively run TCP Dump captures from the ISE admin GUI.
- Enable below debugs on ISE PSN node - -nsf-nsf-session-lightwight Session Directory-profiler-runtime-AAA
- Profiler.log , prrt-server.log and lsd.log show relevant information.
- Refer to the **Fingerbank.org** DHCP fingerprint database for a current list of Parameter Request List options.
- Ensure that the correct Parameter Request List values are configured in the ISE profiling conditions. Some of the more commonly used strings include:

  Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Log Analysis

++Enable below debugs on ISE PSN node -

-nsf

-nsf-session

-lightwight Session Directory

-profiler

-runtime-AAA

++Initial Authentication

++prrt-server.log

++Access Request received on ISE node

Radius,2020-12-29 06:35:19,377,DEBUG,0x7f1cdcbd2700,cntx=0001348461,sesn=isee30-primary/397791910/625,CallingStationID=B4-96-91-26-EB-9F,**RADIUS PACKET:: Code=1(AccessRequest)** Identifier=182 Length=285

++ISE matches the Unknown_profile

AcsLogs,2020-12-29 06:35:19,473,DEBUG,0x7f1cdc7ce700,cntx=0001348476,sesn=isee30-primary/397791910/625,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,**AuthorizationPolicyMatchedRule=Unknown_Profile**, EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=User, CPMSessionID=0A6A270B00000018B44013AC, EndPointMACAddress=B4-96-91-26-EB-9F,

++ISE Sends Access Accept with limited access

Radius,2020-12-29 06:35:19,474,DEBUG,0x7f1cdc7ce700,cntx=0001348476,sesn=isee30-primary/397791910/625,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingS

tationID=B4-96-91-26-EB-9F,RADIUS PACKET:: **Code=2(AccessAccept)** Identifier=186 Length=331

++ISE received Accounting Update with the DHCP information

Radius,2020-12-29 06:35:41,464,DEBUG,0x7f1cdcad1700,cntx=0001348601,sesn=isee30-primary/397791910/627,CPMSessionID=0A6A270B00000018B44013AC,CallingStationID=B4-96-91-26-EB-9F,RADIUS PACKET:: **Code=4(AccountingRequest)** Identifier=45 Length=381

[1] User-Name - value: [dot1xuser]

[87] NAS-Port-Id - value: [GigabitEthernet1/0/13]

[26] **cisco-av-pair - value: [dhcp-option=**

[26] cisco-av-pair - value: [audit-session-id=**0A6A270B00000018B44013AC**]

++ISE Sends back Accounting Response

Radius,2020-12-29 06:35:41,472,DEBUG,0x7f1cdc5cc700,cntx=0001348601,sesn=isee30-primary/397791910/627,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,RADIUS PACKET:: **Code=5(AccountingResponse)** Identifier=45 Length=20,RADIUSHandler.cpp:2216

++Profiler.log

++Once Accounting Update is received with the DHCP option dhcp-parameter-request-list , ISE Starts profiling the device

2020-12-29 06:35:41,470 DEBUG [SyslogListenerThread][] cisco.profiler.probes.radius.SyslogDefragmenter -::::- **parseHeader inBuffer**=<181>Dec 29 06:35:41 isee30-primary CISE_RADIUS_Accounting 0000000655 2 0 2020-12-29 06:35:41.467 +00:00 0000234376 3002 NOTICE **Radius-Accounting: RADIUS Accounting watchdog update**, ConfigVersionId=99, Device IP Address=10.106.39.11, UserName=dot1xuser, RequestLatency=6, NetworkDeviceName=Sw, User-Name=dot1xuser, NAS-IP-Address=10.106.39.11, NAS-Port=50113, Class=CACS:0A6A270B00000018B44013AC:isee30-primary/397791910/625, Called-Station-ID=A0-EC-F9-3C-82-0D, Calling-Station-ID=B4-96-91-26-EB-9F, NAS-Identifier=Switch, Acct-Status-Type=Interim-Update, Acct-Delay-Time=0, Acct-Input-Octets=174, Acct-Output-Octets=0, Acct-Session-Id=0000000b, Acct-Authentic=Remote, Acct-Input-Packets=1, Acct-Output-Packets=0, Event-Timestamp=1609341899, NAS-Port-Type=Ethernet, NAS-Port-Id=GigabitEthernet1/0/13, **cisco-av-pair=dhcp-option=dhcp-parameter-request-list=1\, 3\, 6\, 15\, 31\, 33\, 43\, 44\, 46\, 47\, 119\, 121\, 249\, 252, cisco-av-pair=audit-session-id=0A6A270B00000018B44013AC,** cisco-av-pair=method=dot1x,

2020-12-29 06:35:41,471 DEBUG [RADIUSParser-1-thread-2][] cisco.profiler.probes.radius.RadiusParser -::::- **Parsed IOS Sensor 1: dhcp-parameter-request-list=[1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252]**

Attribute:cisco-av-pair value:dhcp-option=dhcp-parameter-request-list=1\, 3\, 6\, 15\, 31\, 33\, 43\, 44\, 46\, 47\, 119\, 121\, 249\, 252, audit-session-id=0A6A270B00000018B44013AC, method=dot1x

Attribute:dhcp-parameter-request-list value:1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249,

252

2020-12-29 06:35:41,479 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **Owner for this Mac: B4:96:91:26:EB:9F is isee30-primary.anshsinh.local**

2020-12-29 06:35:41,479 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **current owner for the endpoint B4:96:91:26:EB:9Fis isee30-primary.anshsinh.local and message code is 3002**

2020-12-29 06:35:41,479 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **is endpoint source radius true**

++New Attribute

2020-12-29 06:35:41,480 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- **New attribute: dhcp-parameter-request-list**

2020-12-29 06:35:41,482 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:ProfilerCollection:- Endpoint modified attribut set:

2020-12-29 06:35:41,482 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.Forwarder -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**ProfilerCollection:- dhcp-parameter-request-list,**

++Different Rules are matched with different Certainty factor

2020-12-29 06:35:41,484 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:- Policy Intel-Device matched B4:96:91:26:EB:9F (certainty 5)**

2020-12-29 06:35:41,485 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:- Policy Workstation matched B4:96:91:26:EB:9F (certainty 10)**

2020-12-29 06:35:41,486 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:- Policy Microsoft-Workstation matched B4:96:91:26:EB:9F (certainty 10)**

2020-12-29 06:35:41,487 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5**:Profiling:- Policy Windows10-Workstation matched B4:96:91:26:EB:9F (certainty 20)**

++Windows10-Workstation has highest Certainty factor of 40 based on the configuration and hence this choses as the Endpoint Profile for the device

2020-12-29 06:35:41,487 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profiling:- **After analyzing policy hierarchy: Endpoint: B4:96:91:26:EB:9F EndpointPolicy:Windows10-Workstation for:40 ExceptionRuleMatched:false**

2020-12-29 06:35:41,487 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:- Endpoint B4:96:91:26:EB:9F Matched Policy Changed.**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:- Endpoint B4:96:91:26:EB:9F IdentityGroup Changed.**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:- Setting identity group ID on endpoint B4:96:91:26:EB:9F - 3b76f840-8c00-11e6-996c-525400b48521**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profiling:- **Calling end point cache with profiled end point B4:96:91:26:EB:9F, policy Windows10-Workstation, matched policy Windows10-Workstation**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:- Sending event to persist end point B4:96:91:26:EB:9F, and ep message code = 3002**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:**Profiling:- Endpoint B4:96:91:26:EB:9F IdentityGroup / Logical Profile Changed. Issuing a Conditional CoA**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.profiling.ProfilerManager -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5:Profiling:- **ConditionalCoAEvent with Endpoint Details : EndPoint[id=ff19ca00-499f-11eb-b713-1a99022ed3c5,name=<null>]**

MAC: B4:96:91:26:EB:9F

Attribute:Calling-Station-ID value:B4-96-91-26-EB-9F

Attribute:EndPointMACAddress value:B4-96-91-26-EB-9F

Attribute:MACAddress value:B4:96:91:26:EB:9F

++Sending the data to Lightweigth Session Directory

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.**LSDForwarderHelper** -::::- Endpoint.B4:96:91:26:EB:9F **matched Windows10-Workstation**

2020-12-29 06:35:41,489 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.probemgr.**LSDForwarderHelper -::::- Sending event to persist end point while adding for LSD for forwarder,defaultradius,defaultad B4:96:91:26:EB:9F**

++Global CoA is selected as Reauth

2020-12-29 06:35:41,489 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Configured Global CoA command type = Reauth**

2020-12-29 06:35:41,490 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5::- **Updating end point - EP from incoming: B4:96:91:26:EB:9FepSource: RADIUS ProbeSGA: falseSG: Workstation**

2020-12-29 06:35:41,490 DEBUG [RMQforwarder-4][] cisco.profiler.infrastructure.cache.AbstractEndpointCache -:B4:96:91:26:EB:9F:12413370-49a0-11eb-b713-1a99022ed3c5::- **Updating end point - EP after merge: B4:96:91:26:EB:9FepSource: RADIUS ProbeSGA: falseSG:Windows10-Workstation**

++ISE matches the Policy to check if needs to send CoA . ISE will trigger CoA only if it has any policy matching the Profile change

2020-12-29 06:35:41,701 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Process all available Policy in Local Exception PolicySet Switch ,policystatus=ENABLED**

2020-12-29 06:35:41,701 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Policy Name : Switch policystatus : ENABLED**

2020-12-29 06:35:41,702 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- lhsvalue name 6d954800-8bff-11e6-996c-525400b48521 rhs operandID 42706690-8c00-11e6-996c-525400b48521 rhsvaluename Workstation:Microsoft-Workstation:Windows10-Workstation**

2020-12-29 06:35:41,933 DEBUG [CoAHandler-52-thread-1][] com.cisco.profiler.api.Util -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Specified condition AVAILABLE in the Authorization Policy**

2020-12-29 06:35:41,933 DEBUG [CoAHandler-52-thread-1][] com.cisco.profiler.api.Util -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Authorization Policy HAVING Policy : 42706690-8c00-11e6-996c-525400b48521**

++Authorization Policy matches this condition and CoA is triggered

2020-12-29 06:35:41,935 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- applyCoa: Created Descriptor based on Endpoint RADIUS Attributes:**

MAC: [B4:96:91:26:EB:9F]

Session ID: [0A6A270B00000018B44013AC]

AAA Server: [isee30-primary] IP: [10.106.32.119]

AAA Interface: [10.106.32.119]

NAD IP Address: [10.106.39.11]

NAS Port Id: [GigabitEthernet1/0/13]

NAS Port Type: [Ethernet]

Service-Type: [Framed]

Is Wireless: [false]

Is VPN: [false]

Is MAB: [false]

2020-12-29 06:35:41,938 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- About to call CoA for nad IP: 10.106.39.11 for endpoint: B4:96:91:26:EB:9F CoA Command: Reauth**

2020-12-29 06:35:41,938 DEBUG [CoAHandler-52-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:B4:96:91:26:EB:9F:9fe38b30-43ea-11eb-b713-1a99022ed3c5:**ProfilerCoA:- Applying CoA-REAUTH by AAA Server: 10.106.32.119 via Interface: 10.106.32.119 to NAD: 10.106.39.11**

2020-12-29 06:35:41,949 DEBUG [SyslogListenerThread][] cisco.profiler.probes.radius.SyslogDefragmenter -::::- parseHeader inBuffer=<181>Dec 29 06:35:41 isee30-primary CISE_Passed_Authentications 0000000656 2 1 StepData=2=(port = 1700 \, type = Cisco CoA), **CoASourceComponent=Profiler, CoAReason=Change in endpoint identity group/policy/logical profile which are used in authorization policies, CoAType=Reauthentication** - last, Network Device Profile=Cisco,

++prrt-server.log

AcsLogs,2020-12-29 06:35:41,938,DEBUG,0x7f1c6ffcb700,cntx=0001348611,Log_Message=[2020-12-29 06:35:41.938 +00:00 0000234379 80006 **INFO Profiler: Profiler is triggering Change Of Authorization Request,** ConfigVersionId=99, **EndpointCoA=Reauth,** EndpointMacAddress=B4:96:91:26:EB:9F, EndpointNADAddress=10.106.39.11, **EndpointPolicy=Windows10-Workstation,** EndpointProperty=Service-Type=Framed\,MessageCode=3002\,EndPointPolicyID=42706690-8c00-11e6-996c-525400b48521\,UseCase=\,NAS-Port-Id=GigabitEthernet1/0/13\,NAS-Port-Type=Ethernet\,Response=\{User-Name=dot1xuser\;

DynamicAuthorizationFlow,2020-12-29 06:35:41,939,DEBUG,0x7f1cdc3ca700,cntx=0001348614,[DynamicAuthorizationFlow::onLoc

alHttpEvent] Received incoming CoA command:

<Reauthenticate id="39c74088-52fd-430f-95d9-a8fe78eaa1f1" type="last">

<session serverAddress="10.106.39.11">

<identifierAttribute name=**"UseInterface">10.106.32.119</identifierAttribute>**

<identifierAttribute name="**Calling-Station-ID">B4:96:91:26:EB:9F</identifierAttribute>**

<identifierAttribute name="NAS-Port-Id">GigabitEthernet1/0/13</identifierAttribute>

<identifierAttribute name=**"cisco-av-pair">audit-session-id=0A6A270B00000018B44013AC</identifierAttribute>**

<identifierAttribute name=**"ACS-Instance">COA-IP-TARGET:10.106.32.119</identifierAttribute>**

</session>

</Reauthenticate>

++CoA Sent -

RadiusClient,2020-12-29 06:35:41,943,DEBUG,0x7f1ccb3f3700,cntx=0001348614,sesn=39c74088-52fd-430f-95d9-a8fe78eaa1f1,CallingStationID=B4:96:91:26:EB:9F, RADIUS PACKET: **Code=43 (CoARequest)** Identifier=27 Length=225

[4] NAS-IP-Address - value: [10.106.39.11]

[31] Calling-Station-ID - value: [B4:96:91:26:EB:9F]

[87] NAS-Port-Id - value: [GigabitEthernet1/0/13]

[26] cisco-av-pair - value: [subscriber:command=reauthenticate]

[26] cisco-av-pair - value: [audit-session-id=0A6A270B00000018B44013AC]

RadiusClient,2020-12-29 06:35:41,947,DEBUG,0x7f1cdcad1700,cntx=0001348614,sesn=39c74088-52fd-430f-95d9-a8fe78eaa1f1,CallingStationID=B4:96:91:26:EB:9F, RADIUS PACKET: **Code=44 (CoAACK)** Identifier=27

++New Access Request

Radius,2020-12-29 06:35:41,970,DEBUG,0x7f1cdc6cd700,cntx=0001348621,sesn=isee30-primary/397791910/628,CallingStationID=B4-96-91-26-EB-9F,RADIUS PACKET:: **Code=1(AccessRequest)** Identifier=187 Length=285

++ISE matches the new Authorization profile matching the Endpoint Policy of the endpoint device

AcsLogs,2020-12-29 06:35:42,060,DEBUG,0x7f1cdcad1700,cntx=0001348636,sesn=isee30-

primary/397791910/628,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9FIdentityPolicyMatchedRule=Default, **AuthorizationPolicyMatchedRule=Microsoft_workstation,** EapTunnel=EAP-FAST, EapAuthentication=EAP-MSCHAPv2, UserType=User, CPMSessionID=0A6A270B00000018B44013AC, EndPointMACAddress=B4-96-91-26-EB-9F, PostureAssessmentStatus=NotApplicable, **EndPointMatchedProfile=Windows10-Workstation,**

++Access Accept is sent -

Radius,2020-12-29 06:35:42,061,DEBUG,0x7f1cdcad1700,cntx=0001348636,sesn=isee30-primary/397791910/628,CPMSessionID=0A6A270B00000018B44013AC,user=dot1xuser,CallingStationID=B4-96-91-26-EB-9F,RADIUS PACKET:: **Code=2(AccessAccept)** Identifier=191 Length=340

Related Information

- **Fingerbank.org DHCP Fingerprint Database**
- **Technical Support & Documentation - Cisco Systems**