Blast-RADIUS Protocol Spoofing Mitigation (CVE-2024-3596)

Contents

Introduction

Overview

Background

Mitigation

- Message-Authenticator
- Encrypt with TLS/IPSec
  - RADIUS over DTLS
  - RADIUS over TLS
  - IPSec

Partial Mitigation

- RADIUS Segmentation

Identity Services Engine Vulnerability Status

- ISE as a RADIUS Server
- ISE as a RADIUS Client

ISE as a RADIUS Client Updates

- Case
- NAD included Message Authenticator in request
- NAD did not include Message Authenticator in request
- RADIUS Token Server
- External RADIUS Server
- Change of Authorization (CoA)

Introduction

This document describes how to mitigate Blast RADIUS protocol spoofing.

Overview

On July 7, 2024, security researchers disclosed this vulnerability in the RADIUS protocol: CVE-2024-3596: RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by an on-path attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. They have published a paper detailing their findings in this white paper which demonstrates a successful response forgery against flows that do not utilize the Message-Authenticator attribute.

For an up to date list of Cisco products impacted by this vulnerability and versions that contain fixes please visit: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024. This article covers general mitigation techniques as well as how they apply to some, but not all Cisco products, individual product documentation must be consulted for specifics. As the Cisco flagship RADIUS server, Cisco Identity Service Engine is covered in more detail.

Background

This attack takes advantage of an MD5 chosen-prefix attack utilizing collisions in MD5, which allows an attacker to add additional data to the RADIUS response packet while modifying existing attributes of the response packet. An example demonstrated was the ability to change a RADIUS Access-Reject into a RADIUS Access-Accept. This is possible because RADIUS by default does not include a hash of all attributes in the packet. RFC 2869 does add the Message-Authenticator attribute but it is currently only required to be included when using EAP protocols, meaning the attack describe in CVE-2024-3596 is possible against any non-EAP exchange where the RADIUS Client (NAD) does not include the Message-Authenticator attribute.

Mitigation

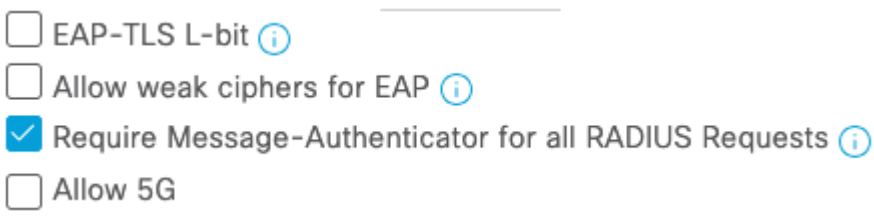
Message-Authenticator

1.- RADIUS client must include Message-Authenticator attribute.

When the Network Access Device (NAD) includes the Message-Authenticator attribute in the Access-Request, Cisco Identity Services Engine includes Message-Authenticator in the resulting Access-Accept, Access-Challenge, or Access-Reject packet in all versions.

2.- The RADIUS server must enforce receiving the Message-Authenticator attribute.

It is not enough to just include the Message-Authenticator in the Access-Request as the attack makes it possible to strip the Message-Authenticator from the Access-Request before it is forwarded to the RADIUS Server. The RADIUS Server must also require the NAD to include Message-Authenticator in the Access-Request. This is not default on Cisco Identity Services Engine but can be enabled at the allowed protocols level, which applies at the policy set level. The option under the Allowed Protocols configuration is **Require Message-Authenticator** for all RADIUS Requests:



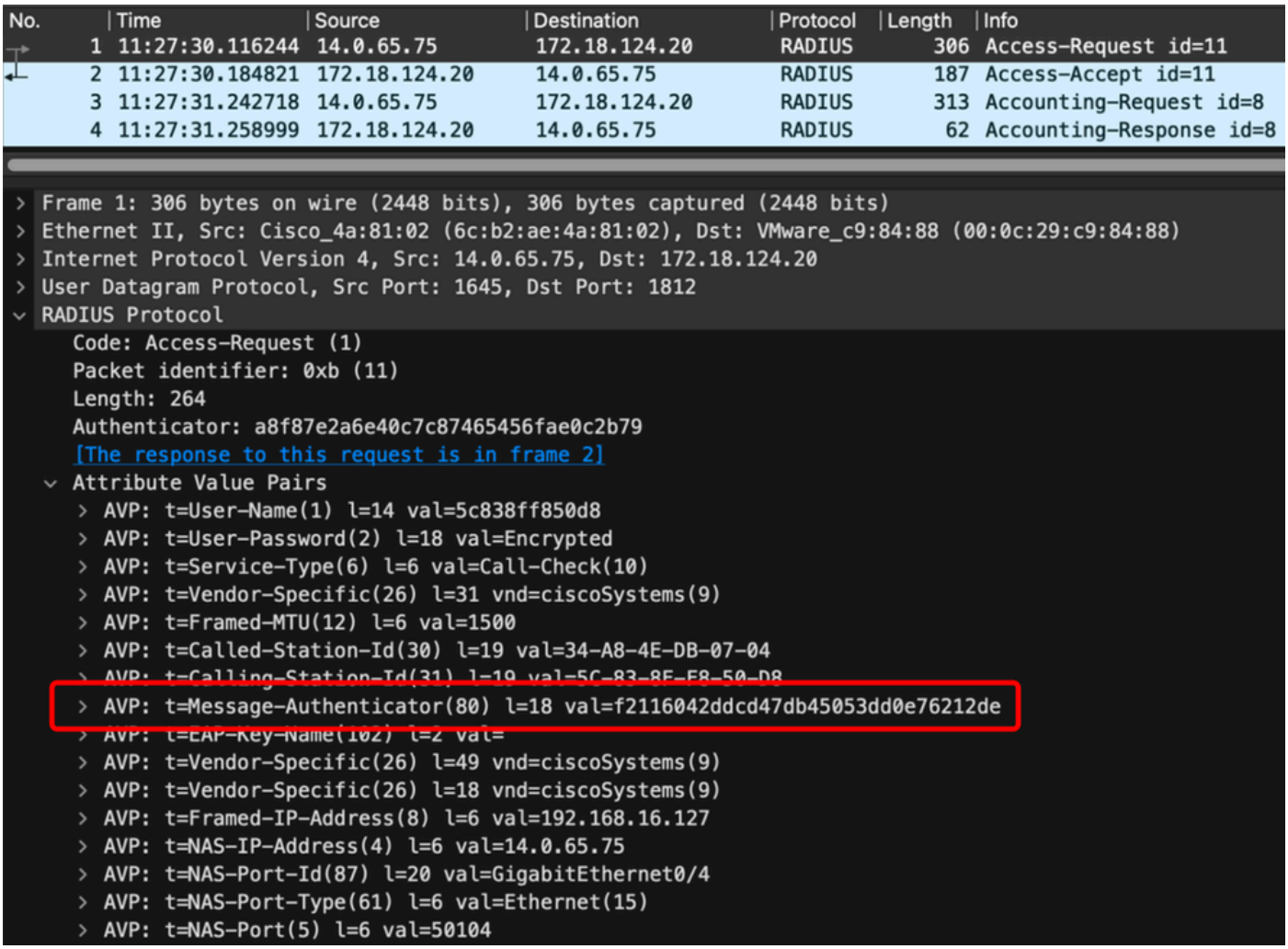
Allowed Protocols Option in Identity Services Engine

Authentications that match a policy set where the Allowed Protocols configuration requires Message-Authenticator, but where the Access-Request does not contain the Message-Authenticator attribute is dropped by ISE:

Event	5405 RADIUS Request dropped
Failure Reason	11057 Message-Authenticator attribute is missing in RADIUS Access-Request

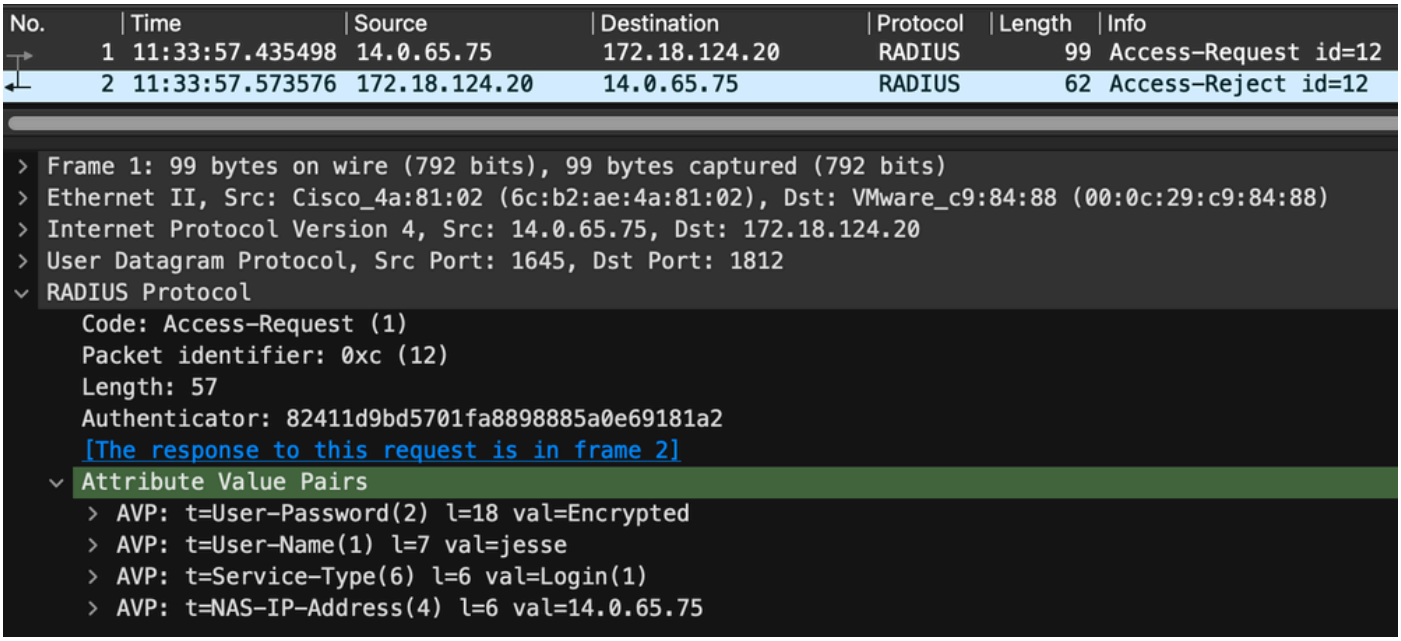
It is important to verify whether the NAD is sending Message-Authenticator before being require by the RADIUS Server as this is not a negotiated attribute, it is up to the NAD to send it either by default or be configured to send it. Message-Authenticator is not one of the attributes reported by ISE, a packet capture is the best way to determine if a NAD/Use Case is including Message-Authenticator. ISE has built in packet capture functionality under **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump**. Keep in mind that different use cases from the same NAD can either include or not include Message-Authenticator.

This is an example capture of an Access-Request that includes the Message-Authenticator attribute:



Message-authenticator attribute in Radius access-request

This is an example capture of an Access-Request that does not include the Message-Authenticator attribute:



Encrypt with TLS/IPSec

The most effective long term solution to secure RADIUS is to encrypt the traffic between the RADIUS Server and the NAD. This adds both privacy and stronger cryptographic integrity over just relying on the MD5-HMAC derived Message-Authenticator. Which, if any of these can be used between the RADIUS Server and the NAD depend on both sides supporting the encryption method.

The broad terms used across the industry for TLS Encryption of RADIUS are:

- **RadSec** – refers to RFC 6614
- **RadSec TLS** – refers to RFC 6614
- **RadSec DTLS** – refers to RFC 7360

It is important to roll out encryption in a controlled manner as there is performance overhead to TLS encryption as well as certificate management considerations. Certificates also has to be renewed on a regular basis.

RADIUS over DTLS

Datagram Transport Layer Security (DTLS) as a Transport Layer for RADIUS is defined by RFC 7360 which uses certificates to mutually authenticate the RADIUS Server and the NAD then encrypts the full RADIUS packet using a TLS tunnel. The transport method remains UDP and requires certificates to be deployed on both the RADIUS Server and NAD. Keep in mind that when deploying RADIUS over DTLS, it is imperative that certificate expiry and replacement is closely managed to prevent expired certificates from interrupting RADIUS communication. ISE supports DTLS for ISE to NAD communication, as of ISE 3.4 Radius over DTLS is not supported for RADIUS-Proxy or RADIUS Token Servers. RADIUS over DTLS is

also supported by many Cisco devices that act as NADs such as switches and wireless controllers running Cisco IOS-XE®.

RADIUS over TLS

Transport Layer Security (TLS) Encryption for RADIUS is defined by RFC 6614, changes the transport to TCP and uses TLS to fully encrypt RADIUS packets. This is commonly used by the eduroam service as an example. As of ISE 3.4, RADIUS over TLS is not supported, but is supported by many Cisco devices that act as NADs such as switches and wireless controllers running Cisco IOS-XE.

IPSec

Identity Services Engine has native support for IPSec tunnels between ISE and NADs that also support terminating IPSec tunnels. This is a good option where RADIUS over DTLS or RADIUS over TLS is not supported but must be used sparingly as only 150 tunnels are supported per ISE Policy Services Node. ISE 3.3 and later no longer requires a license for IPSec, it is now available natively.

Partial Mitigation

RADIUS Segmentation

Segment RADIUS traffic to management VLANs and secure, encrypted links such as can be provided via SD-WAN or MACSec. This strategy does not bring the risk of the attack to zero but can greatly reduce the attack surface of the vulnerability. This can be a good stop gap measure while products roll out the Message-Authenticator requirement or DTLS/RadSec support. The exploit requires an attacker to successfully Man-in-the-Middle (MITM) the RADIUS communication so if an attacker cannot get onto a network segment with that traffic the attack is not possible. The reason this is only a partial mitigation is that a network mis-configuration or compromise of a portion of the network can expose the RADIUS traffic.

If RADIUS traffic can not be segmented or encrypted additional features can be implemented to prevent successful MITM on at risk segments such as: IP Source Guard, Dynamic ARP Inspection, and DHCP Snooping. It is also be possible to utilize other authentication methods based on the authentication flow type such as TACACS+, SAML, LDAPS, and more.

Identity Services Engine Vulnerability Status

These tables describe what is available as of Cisco ISE 3.4 to make authentication flows protected against Blast-RADIUS.

To recap, these next three items must be in place for a flow utilizing only Message-Authenticator and not DTLS/RadSec/IPSec encryption, for the flow to not be vulnerable:

- The Network Access Device MUST send the Message-Authenticator attribute in the Access-Request.
- The RADIUS Server MUST require the Message-Authenticator attribute in the Access-Request.
- The RADIUS Server MUST respond with the Message-Authenticator attribute in the Access-Challenge, Access-Accept, and Access-Reject.

Please refer to Cisco bug ID CSCwk67747 which is tracking the changes to close the vulnerabilities when Cisco ISE is acting as the RADIUS client.

ISE as a RADIUS Server

AAA Scenario	ISE Config	NAD capabilities	Status	Alternative options
EAP Protocols	--	--	Protected	
MAB, PAP, CHAP, MSCHAPv1/v2, Authorize-Only	Have on the checkbox "Require Message-Authenticator for all protocols"	Supports Message-Authenticator for non-EAP protocols	Protected	
		Doesn't support Message-Authenticator for non-EAP protocols	Vulnerable (because of NAD)	Can use IPsec
	Use RADIUS DTLS for this NAD	Supports RADIUS DTLS	Protected	
		Doesn't support RADIUS DTLS	Vulnerable (because of NAD)	Can use IPsec

ISE as a RADIUS Client

AAA Scenario	ISE Config	Peers' capabilities	Status	Alternative options
ISE as RADIUS Proxy	--	NAD supports Message-Authenticator **AND** RADIUS Server supports Message-Authenticator	Protected	
		NAD doesn't support Message-Authenticator **OR** RADIUS Server doesn't support Message-Authenticator	Vulnerable (ISE must send Message-Authenticator to RADIUS Server and must require it in response)	Can use IPsec Partial mitigation is achieved if both NAD and RADIUS Server use Message-Authenticator
ISE as RADIUS Token Client	--		Vulnerable (ISE must send Message-Authenticator to RADIUS Server and must require it in response)	Can use IPsec Partial mitigation is achieved if RADIUS Token Server uses Message-Authenticator
ISE as CoA Client	Configured to use Message-		Vulnerable (ISE must require	Can use IPsec Partial mitigation is achieved if Device Profiler checked option to use Message-Authenticator

ISE as a RADIUS Client Updates

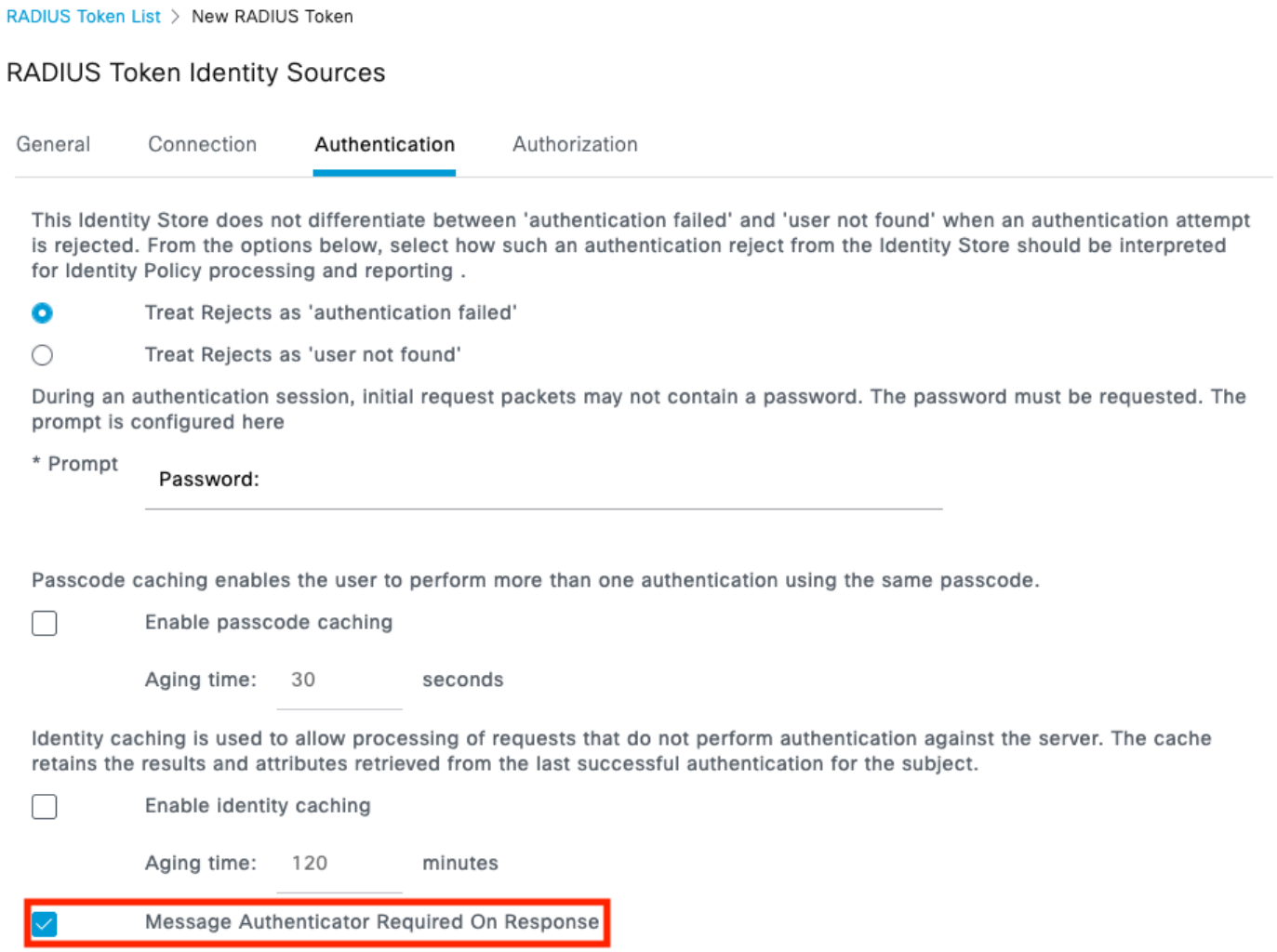
Enhancements to Cisco ISE acting as a RADIUS client are included in releases: 3.1 patch 10, 3.2 patch 8, 3.3 patch 5, 3.4 patch 2, 3.5 and later releases via Cisco bug ID CSCwk67747. Post patch or upgrade, any new resource created defaults to the new, more secure configuration. Existing resources must be modified to use the more secure configuration post patch or upgrade. A new check box has been added: "Message Authenticator Required On Response", if checked it serves a dual purpose: Cisco ISE always sends Message Authenticator, and it fails the authentication if a response is received without a Message Authenticator. The behavior is as follows:

Case	NAD included Message Authenticator in request	NAD did not include Message Authenticator in request
Before patch/upgrade	ISE sends Message Authenticator to the RADIUS Token, External RADIUS Server, or CoA	ISE **does not** send Message Authenticator to the RADIUS Token, External RADIUS server, or CoA
After patch/upgrade and **Message Authenticator Required On Response** checkbox is unchecked.	ISE sends Message Authenticator to the RADIUS Token, External RADIUS Server, or CoA	ISE **does not** send Message Authenticator to the RADIUS Token, External RADIUS server,

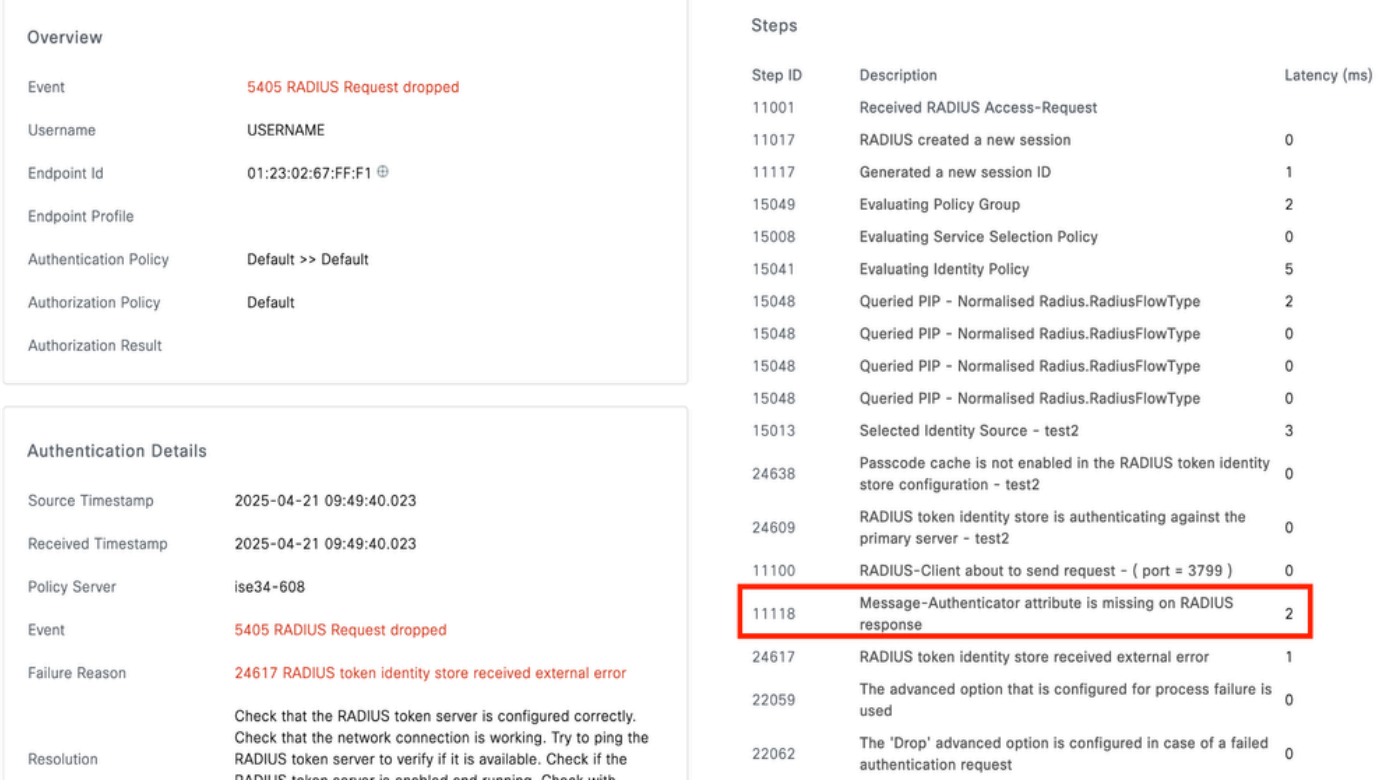
		or CoA
After patch/upgrade and **Message Authenticator Required On Response** checkbox is checked.	ISE sends Message Authenticator to the RADIUS Token, External RADIUS Server, or CoA	ISE sends Message Authenticator to the RADIUS Token, External RADIUS server, or CoA

RADIUS Token Server

A new check box: **Message Authenticator Required On Response** was added under the Authentication tab for the RADIUS Token Server configuration:



With the box checked, if a RADIUS response is received without Message Authenticator, a failure message is logged to the detailed authentication log which can be accessed through Live Logs or a RADIUS authentication report:



Overview

Event	5405 RADIUS Request dropped
Username	USERNAME
Endpoint Id	01:23:02:67:FF:F1
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default
Authorization Result	

Authentication Details

Source Timestamp	2025-04-21 09:49:40.023
Received Timestamp	2025-04-21 09:49:40.023
Policy Server	ise34-608
Event	5405 RADIUS Request dropped
Failure Reason	24617 RADIUS token identity store received external error
Resolution	Check that the RADIUS token server is configured correctly. Check that the network connection is working. Try to ping the RADIUS token server to verify if it is available. Check if the

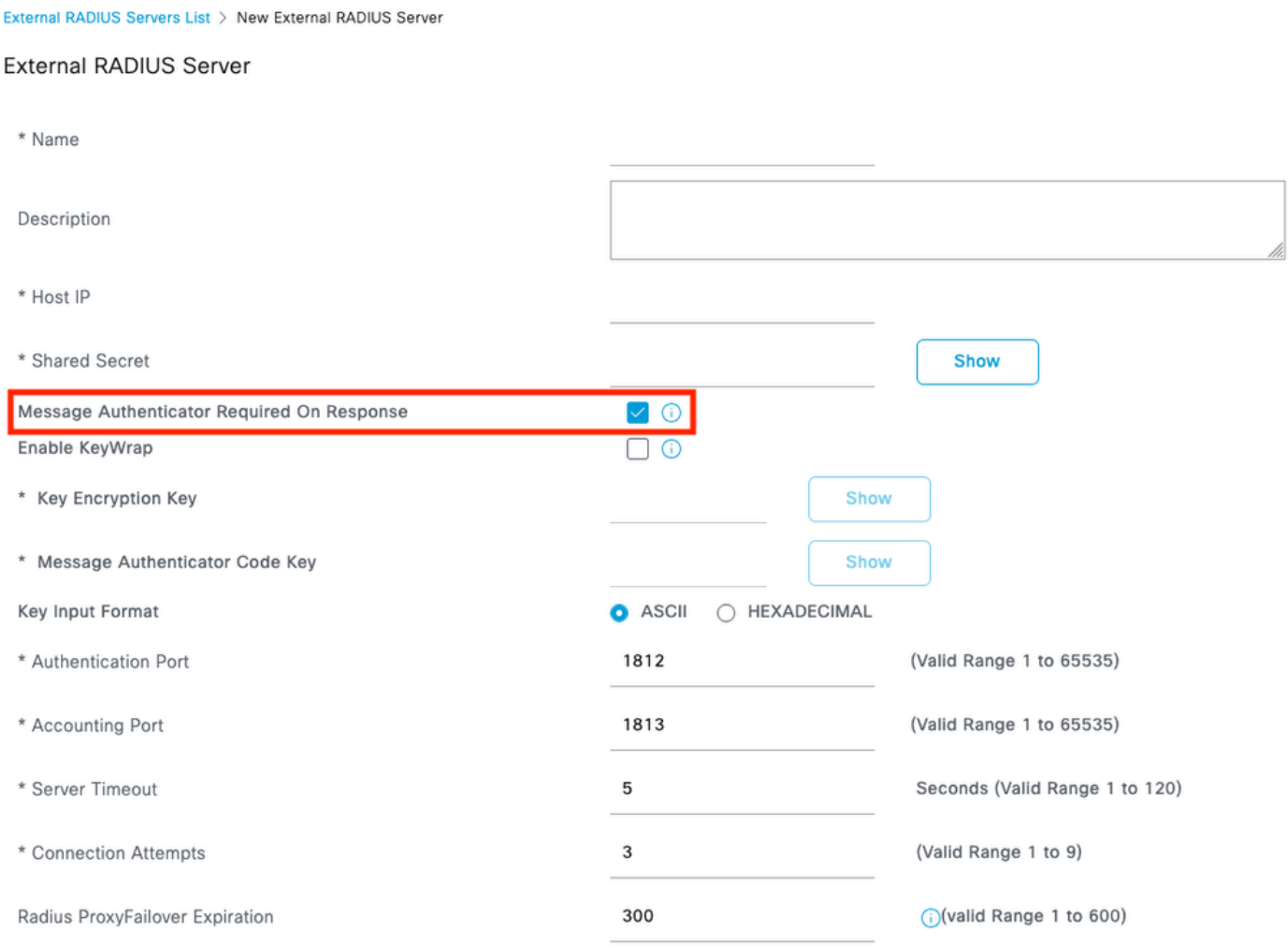
Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11117	Generated a new session ID	1
15049	Evaluating Policy Group	2
15008	Evaluating Service Selection Policy	0
15041	Evaluating Identity Policy	5
15048	Queried PIP - Normalised Radius.RadiusFlowType	2
15048	Queried PIP - Normalised Radius.RadiusFlowType	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	0
15013	Selected Identity Source - test2	3
24638	Passcode cache is not enabled in the RADIUS token identity store configuration - test2	0
24609	RADIUS token identity store is authenticating against the primary server - test2	0
11100	RADIUS-Client about to send request - (port = 3799)	0
11118	Message-Authenticator attribute is missing on RADIUS response	2
24617	RADIUS token identity store received external error	1
22059	The advanced option that is configured for process failure is used	0
22062	The 'Drop' advanced option is configured in case of a failed authentication request	0

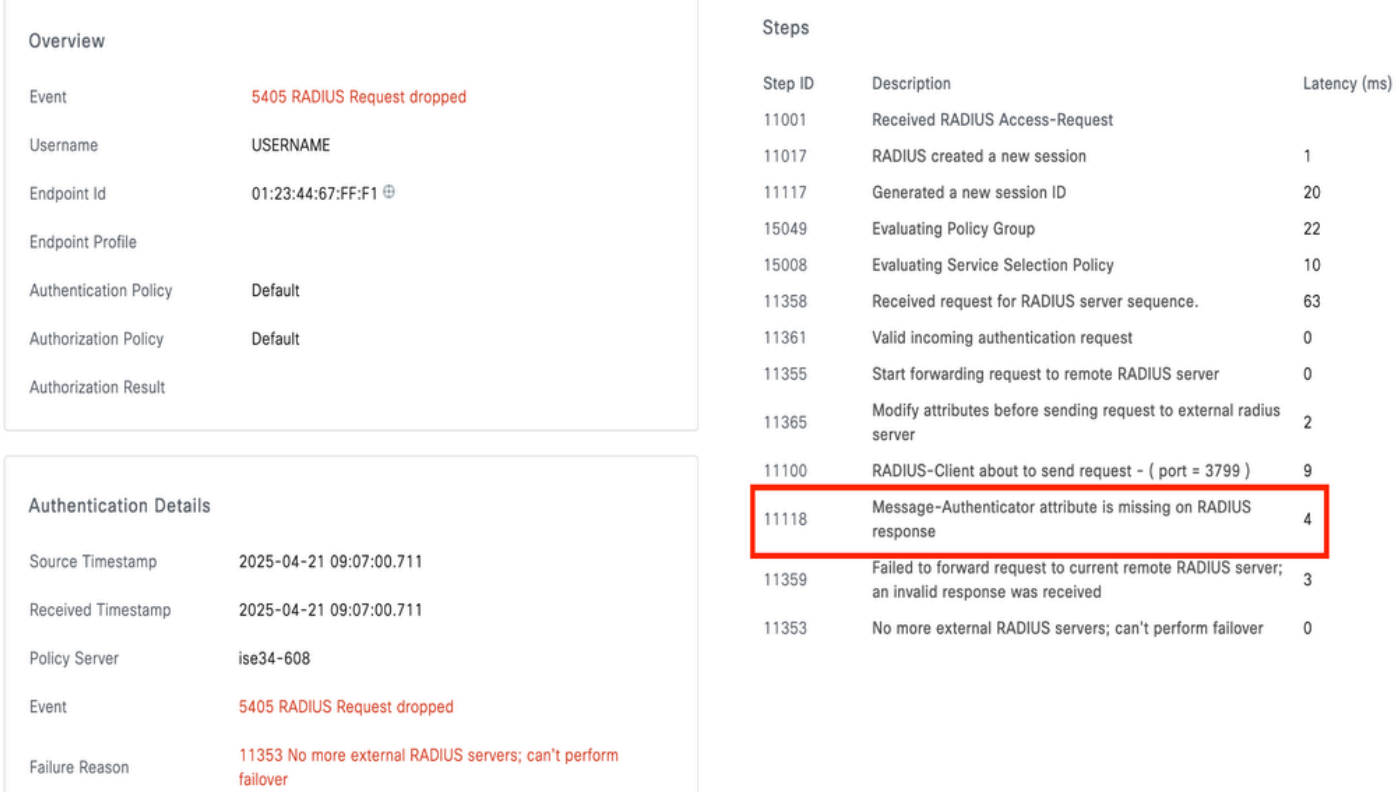
Note: The overall authentication can still pass based on the policy configuration, through the authentication can match an unexpected policy.

External RADIUS Server

A new check box: **Message Authenticator Required On Response** was added the External RADIUS Server configuration:



With the box checked, if a RADIUS response is received without Message Authenticator, a failure message is logged to the detailed authentication log which can be accessed through Live Logs or a RADIUS authentication report:



Overview

Event	5405 RADIUS Request dropped
Username	USERNAME
Endpoint Id	01:23:44:67:FF:F1
Endpoint Profile	
Authentication Policy	Default
Authorization Policy	Default
Authorization Result	

Authentication Details

Source Timestamp	2025-04-21 09:07:00.711
Received Timestamp	2025-04-21 09:07:00.711
Policy Server	ise34-608
Event	5405 RADIUS Request dropped
Failure Reason	11353 No more external RADIUS servers; can't perform failover

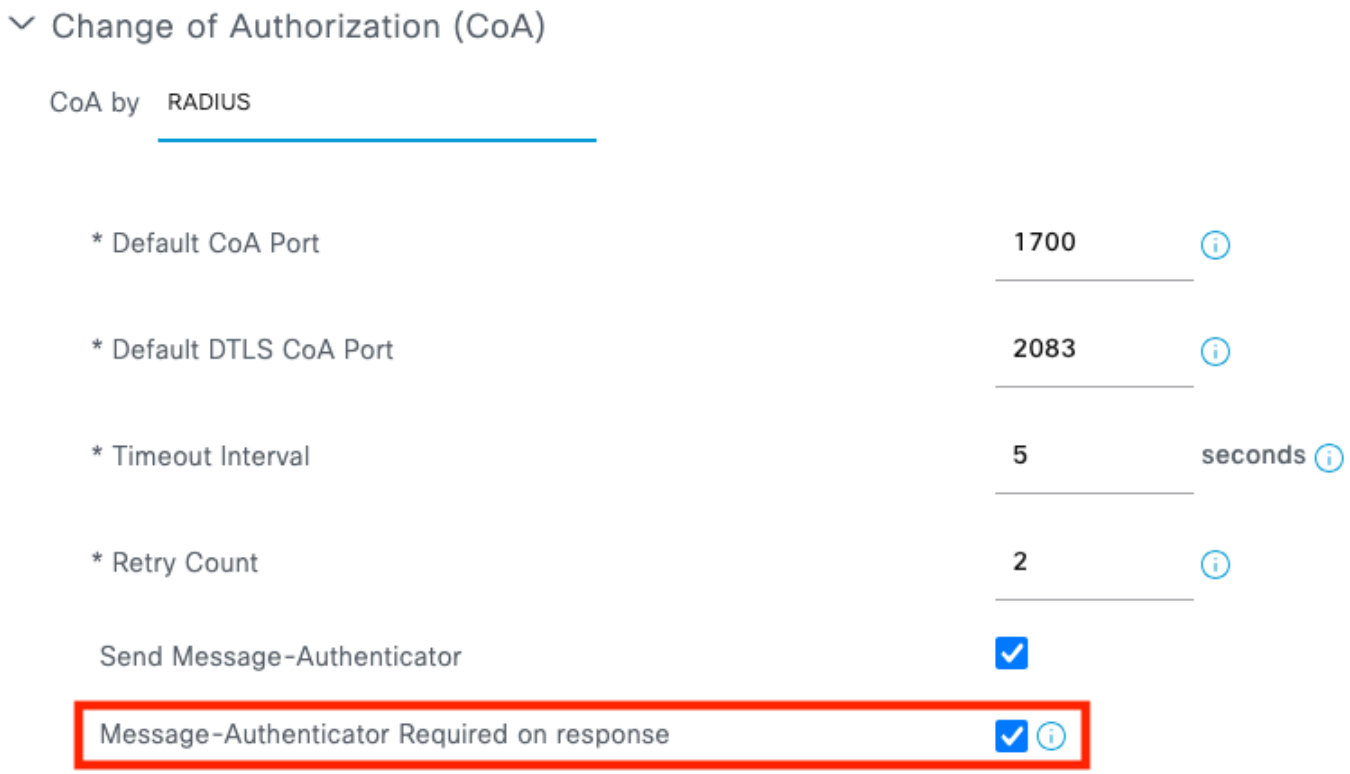
Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	1
11117	Generated a new session ID	20
15049	Evaluating Policy Group	22
15008	Evaluating Service Selection Policy	10
11358	Received request for RADIUS server sequence.	63
11361	Valid incoming authentication request	0
11355	Start forwarding request to remote RADIUS server	0
11365	Modify attributes before sending request to external radius server	2
11100	RADIUS-Client about to send request - (port = 3799)	9
11118	Message-Authenticator attribute is missing on RADIUS response	4
11359	Failed to forward request to current remote RADIUS server; an invalid response was received	3
11353	No more external RADIUS servers; can't perform failover	0

Note: The overall authentication can still pass based on the policy configuration, through the authentication can match an unexpected policy.

Change of Authorization (CoA)

The CoA changes were made to the Network Device Profiles under the Change of Authorization (CoA) drawer:



The **Send Message-Authenticator** option is a previous feature, the new option is **Message-Authenticator Required on response.** Cisco ISE sends the Message Authenticator attribute if the Message-Authenticator Required on response is checked regardless of whether or not **Send Message-Authenticator** is checked or not. **Send Message-Authenticator** is retained for existing configurations. If the NAD does not include Message Authenticator in the CoA Response the following error is seen in the detailed authentication report available through Live Logs:

Event	5417 Dynamic Authorization failed
Failure Reason	11118 Message-Authenticator attribute is missing on RADIUS response
Resolution	The Message-Authenticator attribute is selected as required on RADIUS response. For authentications against external RADIUS server: Go to Administration->Network Resources->External RADIUS servers. Go to the specific External server and see that the checkbox "Message Authenticator Required On Response" is selected. For COA: Go to Administration->Network Resources->Network Devices. Go to the device, and see what is its Profile. Then go the to profile and see that the checkbox "Message Authenticator Required On Response" is selected. Either deselect the checkbox, or enforce the external resource to send valid Message-Authenticator on response.
Root cause	11118 Message-Authenticator attribute is missing on RADIUS response



Note: The CoA could be successful on the NAD even if a failure is logged on Cisco ISE since the NAD could have processed the CoA but not included Message Authenticator in the response.

The default Cisco Provided Network Device Profiles can not be modified, to use the new option the Network Device Profile can be duplicated, and the setting enabled on the duplicated profile. Network devices then needs to be assigned the newly created Network Device Profile. This was done to reduce the risk of causing a network outage following a patch or upgrade by introducing an incompatibility between Cisco ISE and existing NADs. If an existing User Defined profile is in use, it is recommended to duplicate that profile and test at least 1 of each device type on the network using that profile before making a change to the existing Network Device Profile.