Blast-RADIUS协议欺骗缓解(CVE-2024-3596)

目录

简介

概述

背景

缓解

- 消息验证器
- 使用TLS/IPSec加密
  - DTLS上的RADIUS
  - TLS上的RADIUS
  - IPsec

部分缓解

- RADIUS分段

身份服务引擎漏洞状态

- ISE作为RADIUS服务器
- ISE作为RADIUS客户端

ISE作为RADIUS客户端更新

- 案例
- NAD在请求中包含消息验证器
- NAD在请求中不包括消息验证器
- RADIUS令牌服务器
- 外部 RADIUS 服务器
- 授权更改(CoA)

简介

本文档介绍如何缓解Blast RADIUS协议欺骗。

概述

2024年7月7日，安全研究人员在RADIUS协议中发现了以下漏洞：CVE-2024-3596:RFC 2865下的RADIUS协议易受路径上攻击者的伪造攻击，攻击者可以利用针对MD5响应身份验证器签名的selected-prefix collision attack修改任何其他响应的任何有效响应（Access-Accept、Access-Reject或Access-Challenge）。他们发布了一篇文章，详细介绍他们在本白皮书中的发现，该白皮书展示了对未使用Message-Authenticator属性的流的成功响应伪造。

有关受此漏洞影响的思科产品的最新列表以及包含修复程序的版本，请访问：RADIUS协议欺骗漏洞(Blast-RADIUS):2024年7月。本文涵盖一般缓解技术以及它们如何适用于某些（但不是全部）思科产品，具体内容必须参阅个别产品文档。作为思科旗舰RADIUS服务器，思科身份服务引擎将详细介绍。

背景

此攻击利用MD5中利用冲突的MD5选择前缀攻击，使得攻击者能够在修改响应数据包的现有属性的同时向RADIUS响应数据包添加其他数据。演示的示例是将RADIUS Access-Reject更改为RADIUS Access-Accept的能力。这是可能的，因为RADIUS默认情况下不包含数据包中所有属性的哈希。RFC 2869确实添加了Message-Authenticator属性，但当前仅在使用EAP协议时才需要包含它，这意味着对于任何非EAP交换(其中RADIUS客户端(NAD)不包括Message-Authenticator属性)，都可能出现CVE-2024-3596中描述的攻击。

缓解

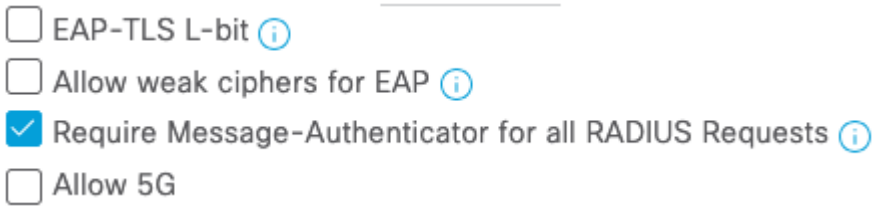
消息验证器

1.- RADIUS客户端必须包含消息身份验证器属性。

当网络接入设备(NAD)在Access-Request中包含Message-Authenticator属性时，思科身份服务引擎会在所有版本中生成的Access-Accept、Access-Challenge或Access-Reject数据包中包含Message-Authenticator。

2.- RADIUS服务器必须强制接收Message-Authenticator属性。

在访问请求中仅包含消息身份验证器是不够的，因为攻击可以在将消息身份验证器转发到RADIUS服务器之前将消息身份验证器从访问请求中删除。RADIUS服务器还必须需要NAD在访问请求中包含消息身份验证器。这不是思科身份服务引擎的默认设置，但可以在允许的协议级别（在策略集级别应用）启用。Allowed Protocols配置下的选项是Require Message-Authenticator，用于所有RADIUS请求：



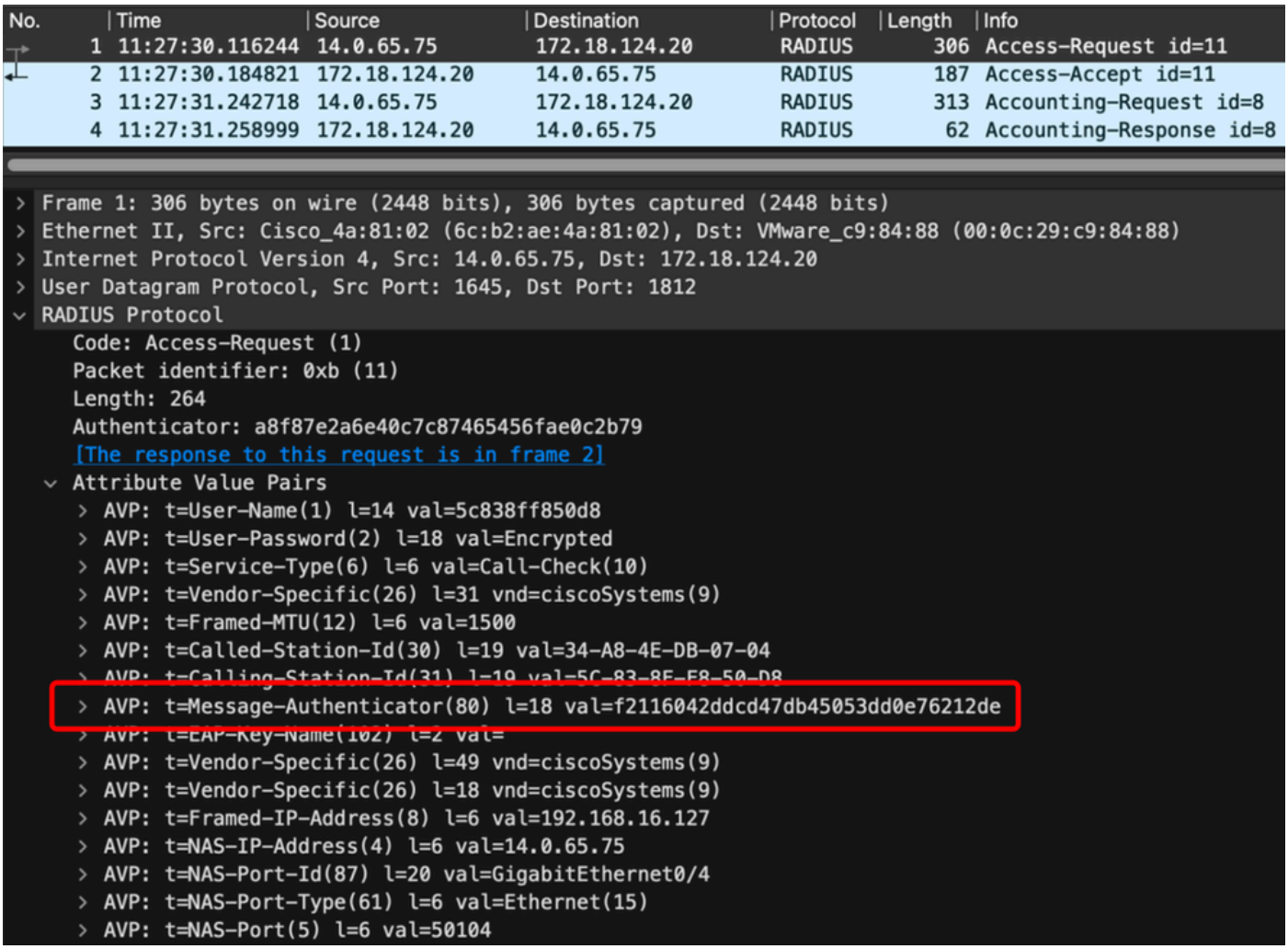
身份服务引擎中的允许协议选项

与Allowed Protocols配置需要Message-Authenticator但Access-Request不包含Message-Authenticator属性被ISE丢弃的策略集的身份验证：

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

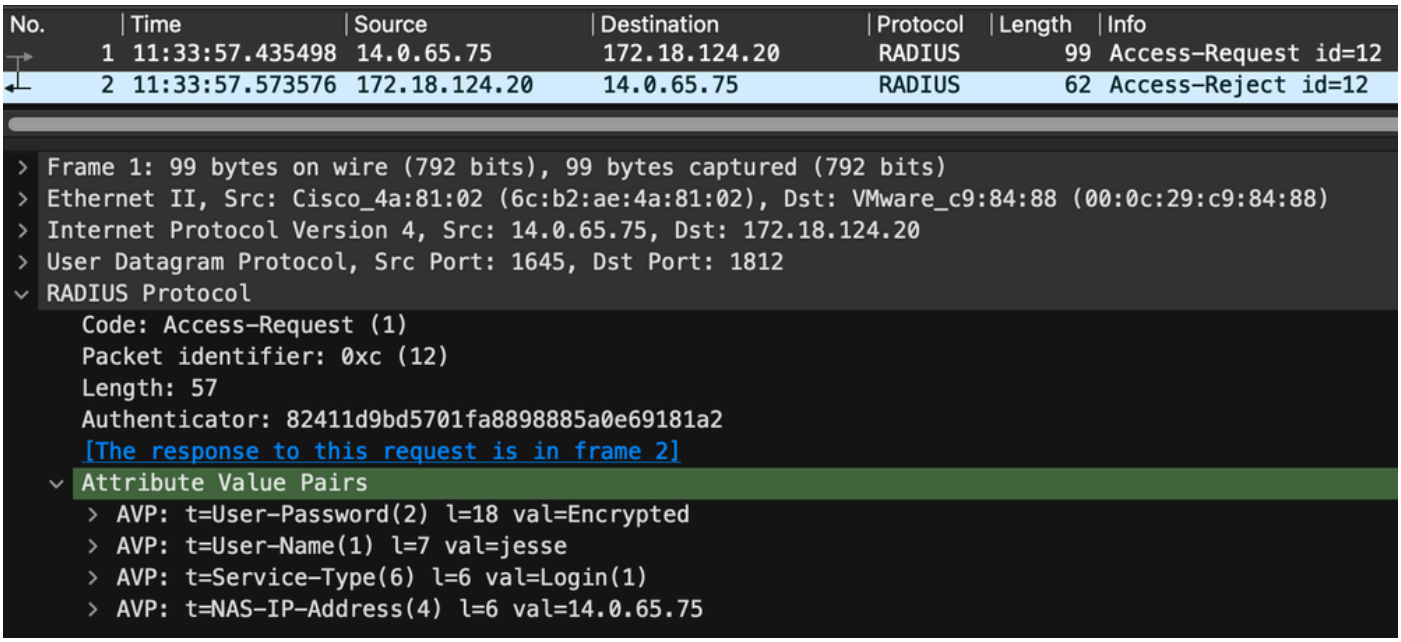
在RADIUS服务器要求之前验证是否需要发送消息身份验证器非常重要，因为这不是一个协商的属性，NAD在默认情况下发送消息或将其配置为发送消息。Message-Authenticator不是ISE报告的属性之一，数据包捕获是确定NAD/Use Case是否包括Message-Authenticator的最佳方法。ISE在Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump下内置数据包捕获功能。请记住，同一NAD的不同用例可以包括或不包括消息验证器。

以下是包括Message-Authenticator属性的Access-Request的示例捕获：



Radius access-request中的Message-authenticator属性

以下是不包含消息身份验证器属性的Access-Request的示例捕获：



使用TLS/IPSec加密

保护RADIUS的最有效的长期解决方案是加密RADIUS服务器和NAD之间的流量。与仅依赖MD5-HMAC派生的消息验证器相比，这增加了隐私性和更强的加密完整性。如果可在RADIUS服务器和NAD之间使用上述任何选项，则取决于支持加密方法的两端。

业内对RADIUS的TLS加密使用的广泛术语包括：

- RadSec — 指RFC 6614
- RadSec TLS — 指RFC 6614
- RadSec DTLS — 指RFC 7360

必须以受控的方式推广加密，因为TLS加密有性能开销，而且需要考虑证书管理。证书也必须定期更新。

DTLS上的RADIUS

数据报传输层安全(DTLS)作为RADIUS的传输层由RFC 7360定义，它使用证书对RADIUS服务器进行相互身份验证，然后NAD使用TLS隧道加密完整的RADIUS数据包。传输方法仍为UDP，需要在RADIUS服务器和NAD上部署证书。请记住，当通过DTLS部署RADIUS时，必须严格管理证书到期和替换，以防止过期的证书中断RADIUS通信。ISE支持ISE到NAD通信的DTLS，自ISE 3.4起，RADIUS代理或RADIUS令牌服务器不支持通过DTLS的RADIUS。许多充当NAD的Cisco设备也支持DTLS上的RADIUS，例如运行Cisco IOS-XE®的交换机和无线控制器。

TLS上的RADIUS

RADIUS的传输层安全(TLS)加密由RFC 6614定义，将传输更改为TCP并使用TLS完全加密RADIUS数据包。通常以Eduroam服务为例。自ISE 3.4起，不支持基于TLS的RADIUS，但许多作为NAD的Cisco设备都支持RADIUS，例如运行Cisco IOS-XE的交换机和无线控制器。

IPsec

身份服务引擎对ISE和NAD之间的IPSec隧道提供本地支持，也支持终止IPSec隧道。这是一个不错的选项，其中不支持RADIUS over DTLS或RADIUS over TLS，但必须谨慎使用，因为每个ISE策略服务节点仅支持150个隧道。ISE 3.3及更高版本不再需要IPSec许可证，现在可在本地使用。

部分缓解

RADIUS分段

将RADIUS流量分段到管理VLAN和安全的加密链路，例如可以通过SD-WAN或MACSec提供。这种策略不会将攻击风险降至零，但可以大大减少漏洞的攻击面。当产品推出消息验证器要求或DTLS/RadSec支持时，这可以作为一种很好的停止间隙措施。此漏洞需要攻击者成功通过RADIUS通信实现中间人(MITM)，因此，如果攻击者无法通过该流量进入网段，攻击将不可行。这仅是部分缓解的原因是，网络配置错误或网络部分受到危害可能暴露RADIUS流量。

如果无法对RADIUS流量进行分段或实施加密附加功能，以防止在有风险的数据段上成功执行MITM，例如：IP源保护、动态ARP检测和DHCP监听。还可以使用其他基于身份验证流类型的身份验证方法，例如TACACS+、SAML、LDAPS等。

身份服务引擎漏洞状态

下表介绍思科ISE 3.4中可用于使身份验证流防御爆炸RADIUS的哪些内容。

要总结一下，以下三项必须适用于仅使用消息验证器而不使用DTLS/RadSec/IPSec加密的流，以便该流不易受攻击：

- 网络接入设备必须发送Access-Request中的Message-Authenticator属性。
- RADIUS服务器必须要求Access-Request中的Message-Authenticator属性。
- RADIUS服务器必须使用Access-Challenge、Access-Accept和Access-Reject中的Message-

Authenticator属性进行响应。

请参阅Cisco Bug ID CSCwk67747，当Cisco ISE充当RADIUS客户端时，该漏洞跟踪更改以关闭漏洞。

ISE作为RADIUS服务器

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作为RADIUS客户端

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作为RADIUS客户端更新

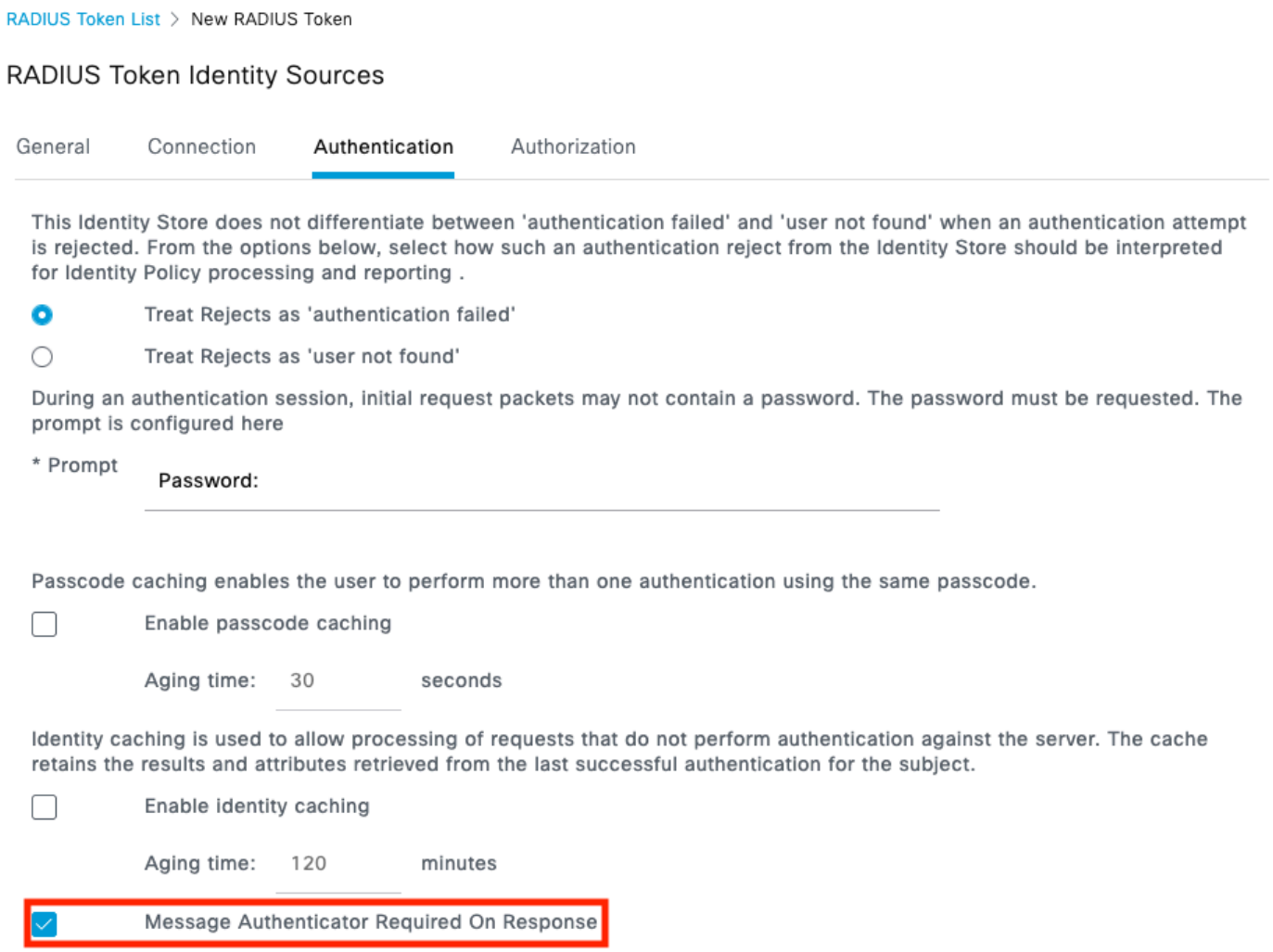
作为RADIUS客户端的Cisco ISE的增强功能包含在版本中：3.1补丁10、3.2补丁8、3.3补丁5、3.4补丁2、3.5及更高版本（通过Cisco Bug ID CSCwk6747）。在补丁或升级后，创建的任何新资源默认采用新的、更安全的配置。必须修改现有资源，才能使用更安全的补丁或升级后配置。已添加新的复选框："响应时需要消息验证器"，如果选中该复选框，则消息验证器具有双重用途：思科ISE始终发送消息身份验证器，如果收到没有消息身份验证器的响应，则身份验证失败。行为如下：

案例	NAD在请求中包含消息验证器	NAD在请求中不包括消息验证器
修补/升级前	ISE向RADIUS令牌、外部RADIUS服务器或CoA发送消息身份验证器	ISE不向RADIUS令牌、外部RADIUS服务器或CoA发送消息身份验证器
After patch/upgrade and Message Authenticator Required On Response复选框	ISE向RADIUS令牌、外部RADIUS服务器或CoA发送消息身份验证器	ISE 不向RADIUS令牌、外部RADIUS服务器或CoA发送消息身份验证器

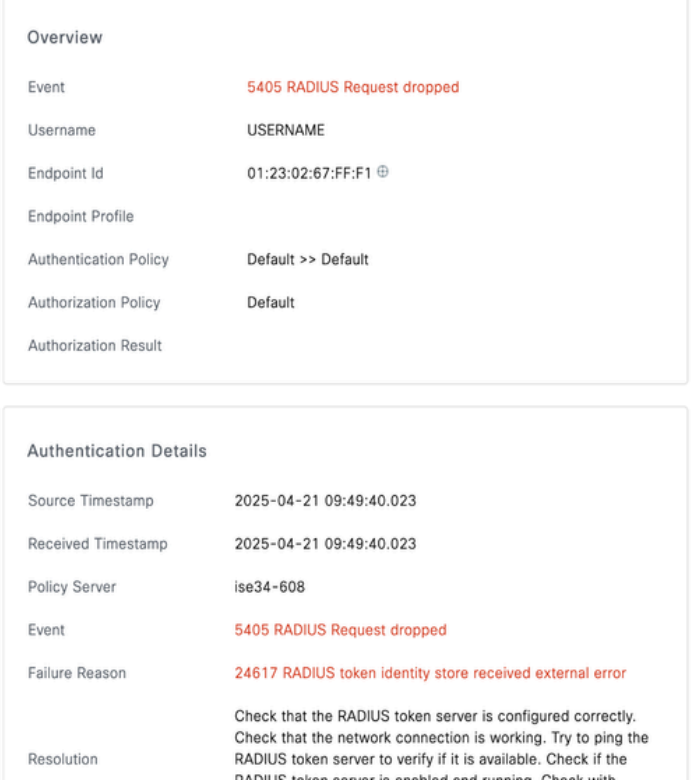
未选中。		
After patch/upgrade and Message Authenticator Required On Response复选框已选中。	ISE向RADIUS令牌、外部RADIUS服务器或CoA发送消息身份验证器	ISE向RADIUS令牌、外部RADIUS服务器或CoA发送消息身份验证器

RADIUS令牌服务器

在RADIUS令牌服务器配置的Authentication选项卡下添加了新复选框Message Authenticator Required On Response:



选中此框后，如果收到RADIUS响应但没有消息身份验证器，则故障消息会记录到可通过实时日志或RADIUS身份验证报告访问的详细身份验证日志中：

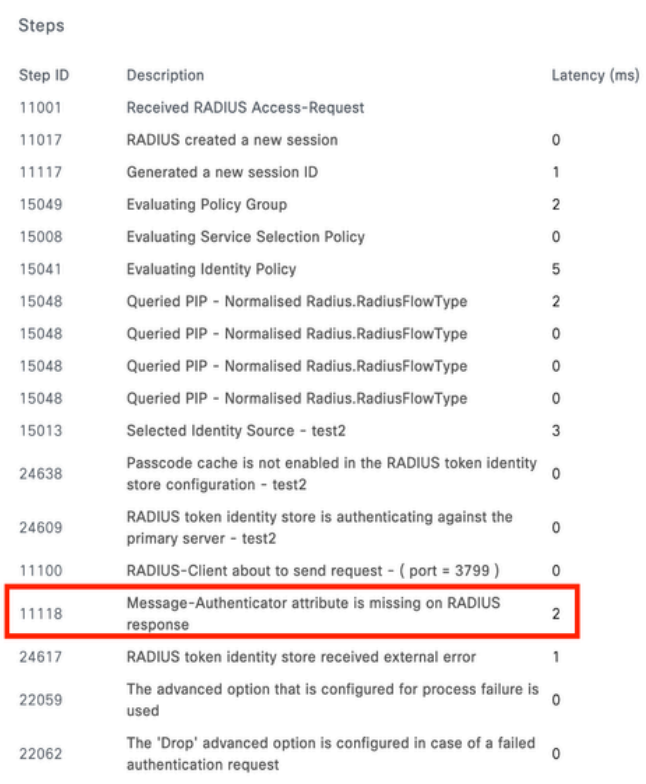


Overview

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



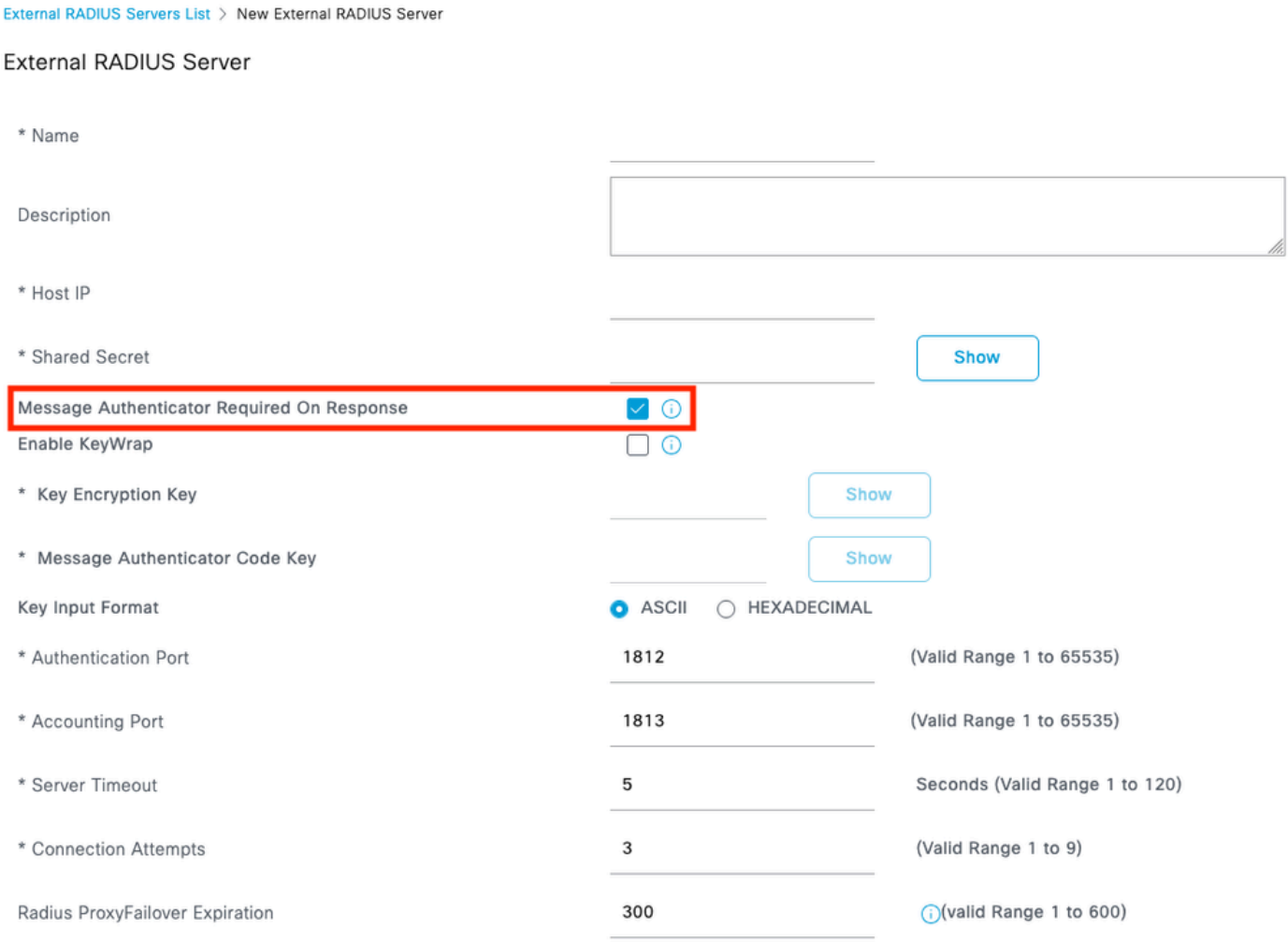
Steps

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

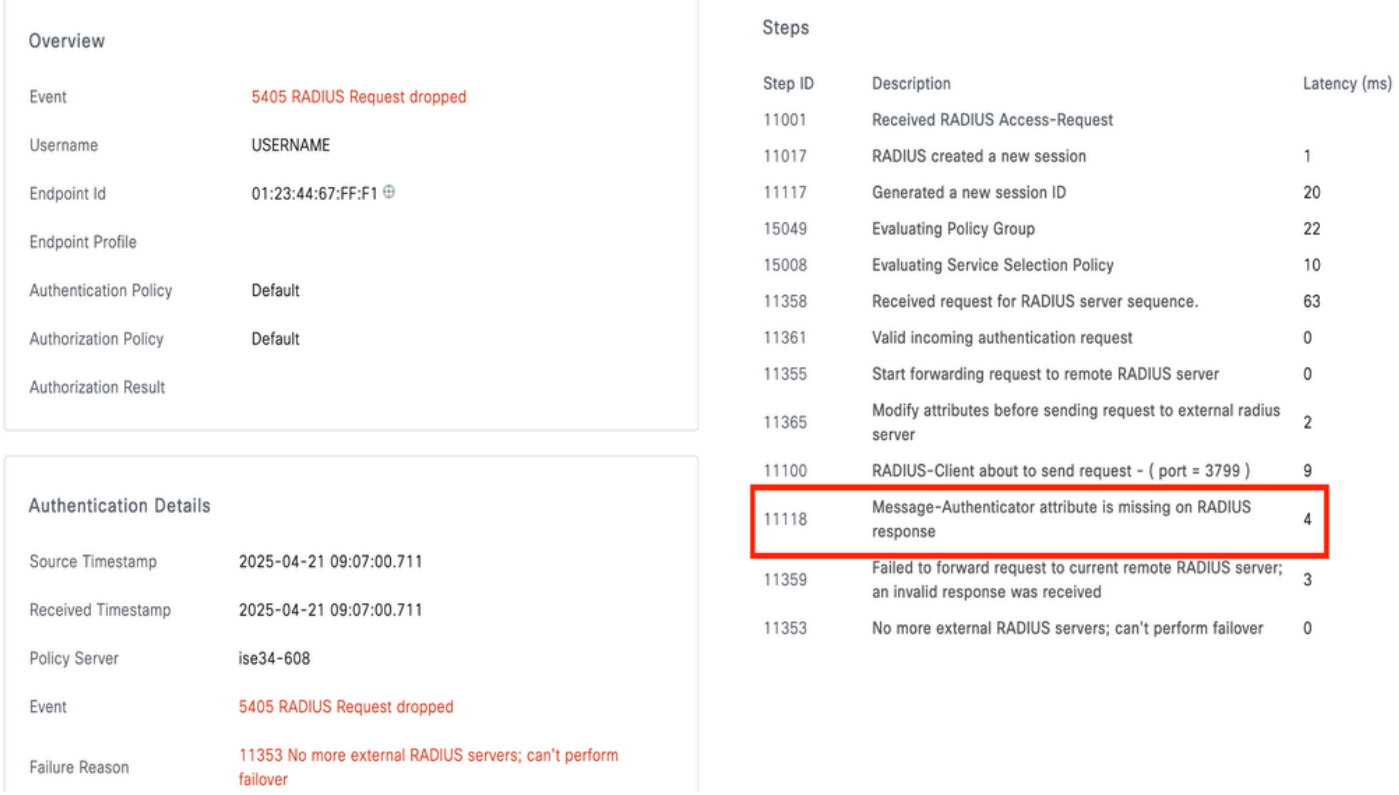
注意：整体身份验证仍可基于策略配置传递，通过身份验证可匹配意外策略。

外部 RADIUS 服务器

新复选框：已添加外部RADIUS服务器配置响应所需的消息验证器：



选中此框后，如果收到RADIUS响应但没有消息身份验证器，则故障消息会记录到可通过实时日志或RADIUS身份验证报告访问的详细身份验证日志中：



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

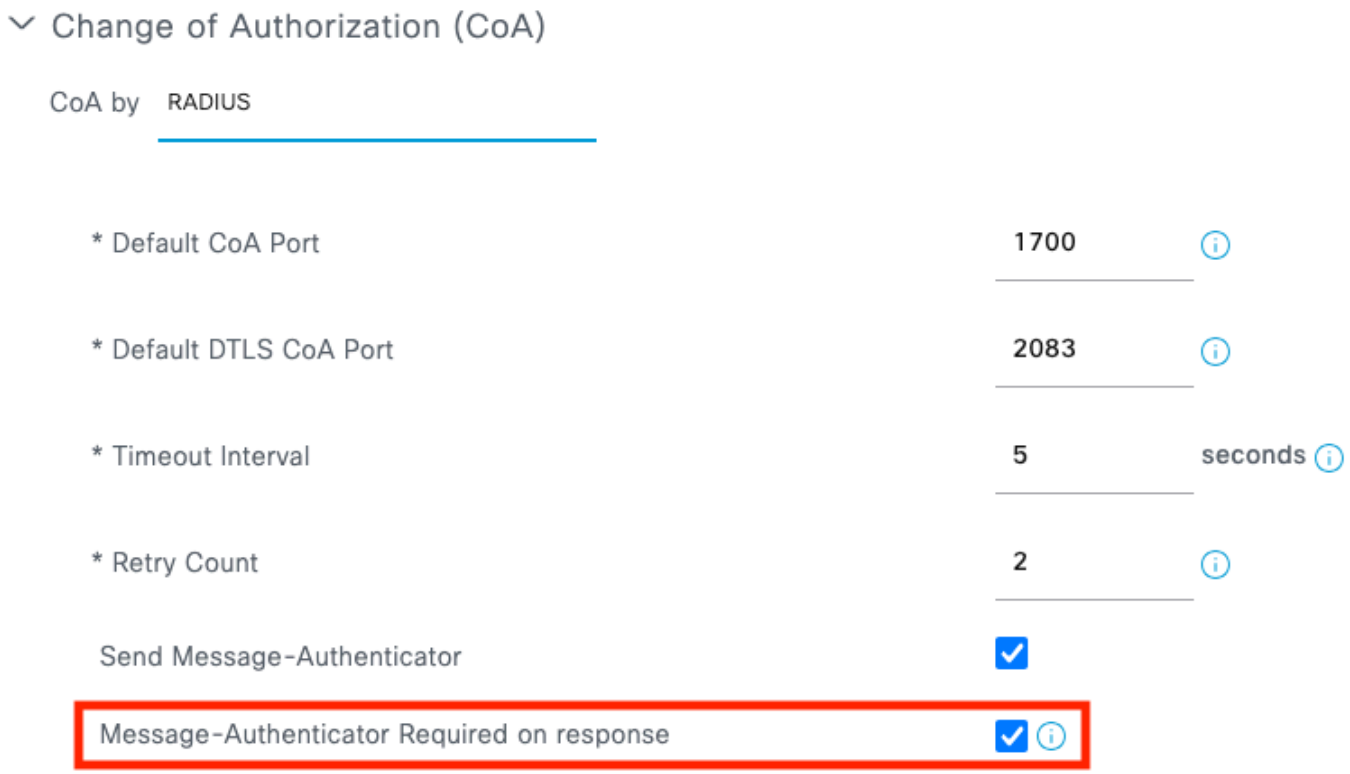
Steps

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

注意：整体身份验证仍可基于策略配置传递，通过身份验证可匹配意外策略。

授权更改(CoA)

在授权更改(CoA)抽屉下对网络设备配置文件进行了CoA更改：



Send Message-Authenticator选项是以前的功能，新选项是Message-Authenticator Required on response。无论是否选中Send Message-Authenticator,Cisco ISE都会在响应上选中Message-Authenticator Required on response时发送Message Authenticator属性。Send Message-Authenticator保留用于现有配置。如果NAD在CoA响应中不包括消息身份验证器，则可在实时日志中提供的详细身份验证报告中看到以下错误：

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

注意：即使在Cisco ISE上记录故障，CoA也可能在NAD上成功，因为NAD可能已经处理了CoA但响应中不包括消息身份验证器。

无法修改默认思科提供的网络设备配置文件，要使用新选项，可以复制网络设备配置文件，并在复制的配置文件上启用设置。然后，需要为网络设备分配新创建的网络设备配置文件。这样做是为了通过引入思科ISE和现有NAD之间的不兼容性，减少补丁或升级后导致网络中断的风险。如果正在使用现有的用户定义配置文件，则建议复制该配置文件，并在对现有网络设备配置文件进行更改之前，使用该配置文件测试网络上每种设备类型的至少1种。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。