Configurer l'autorisation de point d'accès dans un réseau sans fil unifié

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Autorisation AP légère **Configuration** Configuration à l'aide de la liste d'autorisation interne sur le WLC Vérification Autorisation AP sur un serveur AAA Configurer Cisco ISE pour autoriser les points d'accès Configurer un nouveau profil de périphérique où MAB ne nécessite pas d'attribut de type de port NAS Configurer le WLC en tant que client AAA sur Cisco ISE Ajoutez l'adresse MAC AP à la base de données des terminaux sur Cisco ISE Ajouter l'adresse MAC AP à la base de données utilisateur sur Cisco ISE (facultatif) Définir un ensemble de stratégies Vérification Dépannage

Introduction

Ce document décrit comment configurer le WLC pour autoriser le point d'accès (AP) basé sur l'adresse MAC des AP.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base sur la configuration d'un moteur Cisco Identity Services Engine (ISE)
- Connaissance de la configuration des points d'accès Cisco et des WLC Cisco
- Connaissance des solutions Cisco Unified Wireless Security

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• WLC exécutant le logiciel AireOS 8.8.11.0Points d'accès Wave1 : 1700/2700/3700 et 3500 (les versions 1600/2600/3600 sont toujours prises en charge, mais la prise en charge d'AireOS prend fin avec la version 8.5.x)Points d'accès Wave2 : 1800/2800/3800/4800, 1540 et 1560 version ISE 2.3.0.298

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Autorisation AP légère

Pendant le processus d'enregistrement des AP, les AP et les WLC s'authentifient mutuellement à l'aide de certificats X.509. Les certificats X.509 sont gravés dans la mémoire flash protégée sur l'AP et le WLC en usine par Cisco.

Sur le point d'accès, les certificats installés en usine sont appelés certificats installés en fabrication (MIC). Tous les points d'accès Cisco fabriqués après le 18 juillet 2005 sont dotés de MIC.

Outre cette authentification mutuelle qui se produit pendant le processus d'enregistrement, les WLC peuvent également restreindre les AP qui s'enregistrent auprès d'eux en fonction de l'adresse MAC de l'AP.

L'absence d'un mot de passe fort avec l'utilisation de l'adresse MAC AP n'est pas un problème parce que le contrôleur utilise MIC pour authentifier l'AP avant d'autoriser l'AP via le serveur RADIUS. L'utilisation de MIC fournit une authentification forte.

L'autorisation AP peut être effectuée de deux manières :

- Utilisation de la liste d'autorisation interne sur le WLC
- Utilisation de la base de données d'adresses MAC sur un serveur AAA

Les comportements des points d'accès diffèrent en fonction du certificat utilisé :

- AP avec SSC : le WLC utilise uniquement la liste d'autorisation interne et ne transmet pas de requête à un serveur RADIUS pour ces AP
- AP avec MIC : le WLC peut utiliser la liste d'autorisation interne configurée sur le WLC ou utiliser un serveur RADIUS pour autoriser les AP

Ce document traite de l'autorisation AP avec l'utilisation de la liste d'autorisation interne et du serveur AAA.

Configuration

Configuration à l'aide de la liste d'autorisation interne sur le WLC

Sur le WLC, utilisez la liste d'autorisation AP pour restreindre les AP en fonction de leur adresse MAC. La liste des autorisations AP est disponible sous **Security > AP Policies** dans la GUI du WLC.

Cet exemple montre comment ajouter l'AP avec l'adresse MAC 4c:77:6d:9e:61:62.

- 1. Dans l'interface graphique du contrôleur WLC, cliquez sur Security > AP Policies et la page AP Policies s'affiche.
- 2. Cliquez sur le bouton Add sur le côté droit de l'écran.

cisco	MONITOR WLANS CONTROLLE	R WIRELESS	<u>s</u> ecurity	MANAGEMENT	C <u>O</u> MMANDS	HELP	Sa <u>v</u> e Configuration	n <u>P</u> ing	Logout <u>R</u> efresh
Security	AP Policies							Apply	Add
▼ AAA General ▼ RADIUS	Policy Configuration								
Authentication Accounting	Accept Self Signed Certificate (SSC)							
Auth Cached Users Fallback	Accept Manufactured Installed Cert	ficate (MIC)							
DNS Downloaded AVP	Accept Local Significant Certificate	(LSC)							
▶ TACACS+	Authorize MIC APs against auth-list	or AAA							
LDAP Local Net Users MAC Filtering	Authorize LSC APs against auth-list								
 Disabled Clients User Login Policies 	AP Authorization List			Ent	ries 1 - 5 of 5				
AP Policies Password Policies	Search by MAC	Searc	h						
Local EAP									
Advanced EAD	MAC address / Serial Number	Certificate	Type SI	HA1 Key Hash					

3. Sous Add AP to Authorization List, entrez la commande AP MAC (et non l'adresse MAC radio AP). Choisissez ensuite le type de certificat et cliquez sur Add.Dans cet exemple, un AP avec un certificat MIC est ajouté.Note: Pour les AP avec SSC, choisissez ssc sous Type de certificat.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	A Home
Security	AP Policies	Apply
▼ AAA General ▼ RADIUS	Policy Configuration	
Authentication Accounting Auth Cached Users	Accept Self Signed Certificate (SSC)	
Fallback	Accept Manufactured Installed Certificate (MIC)	
DNS Downloaded AVP	Accept Local Significant Certificate (LSC)	
TACACS+	Authorize MIC APs against auth-list or AAA	
Local Net Users MAC Filtering	Authorize LSC APs against auth-list	
User Login Policies	Add AP to Authorization List	
AP Policies Password Policies	MAC Address 4c:77:6d:9e:61:62	
Local EAP	Certificate Type MIC 🔻	
Advanced EAP		
Priority Order	Add	
Certificate	AP Authorization List Entries 0 - 0 of 0	
Access Control Lists	Search by MAC Search	
Wireless Protection Policies	MAC address / Certificate	
Web Auth	Serial Number Type SHA1 Key Hash	
TrustSec		
Local Policies		
▶ Umbrella		
Advanced		

Le point d'accès est ajouté à la liste d'autorisation des points d'accès et est répertorié sous AP Authorization List.

4. Sous Policy Configuration, cochez la case correspondant à Authorize MIC APs against authlist or AAA.Lorsque ce paramètre est sélectionné, le WLC vérifie d'abord la liste d'autorisation locale. Si l'adresse MAC AP n'est pas présente, il vérifie le serveur RADIUS.

ahaha						Sa <u>v</u> e Confi	iguration <u>P</u> ing Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLE	r W <u>i</u> reless <u>s</u> ecu	RITY MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK	🔒 Home
Security	AP Policies						Apply Add
▼ AAA General ▼ RADIUS	Policy Configuration						\square
Authentication Accounting Auth Cached Users Fallback DNS	Accept Self Signed Certificate (SSC) Accept Manufactured Installed Certi	ficate (MIC)					
Downloaded AVP TACACS+ LDAP Local Net Users	Accept Local Significant Certificate (Authorize MIC APs against auth-list Authorize LSC APs against auth-list	or AAA					
MAC Filtering Disabled Clients Disabled Policies	AP Authorization List		En	tries 1 - 5 of 5	4		
Password Policies	Search by MAC	Search					
Advanced FAD	MAC address / Serial Number	Certificate Type	SHA1 Key Hash				
Advanced EAP	4c:77:6d:9e:61:62	MIC					
Priority Order	70:d3:79:26:39:68	MIC					
Certificate	88:f0:31:7e:e0:38	MIC					
Access Control Lists	f4:db:e6:43:c4:b2	MIC					
Wireless Protection Policies	fc:5b:39:e7:2b:30	MIC					
▶ Web Auth							
▶ TrustSec							

Vérification

Afin de vérifier cette configuration, vous devez connecter l'AP avec l'adresse MAC 4c:77:6d:9e:61:62 au réseau et à la surveillance. Utilisez debug capwap events/errors enable et debug aaa all enable pour effectuer cette opération.

Ce résultat montre les débogages quand l'adresse MAC AP n'est pas présente dans la liste d'autorisation AP :

Note: Certaines lignes du résultat ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

(Cisco Controller) >debug capwap events enable (Cisco Controller) >debug capwap errors enable (Cisco Controller) >debug aaa all enable *spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256 *spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request *spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Allocate database entry for AP 192.168.79.151:5256, already allocated index 277 *spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 AP Allocate request at index 277 (reserved) *spamApTask4: Feb 27 10:15:25.593: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from temporary database. *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc.

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response, state Capwap_no_state

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0 *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Request failed! *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5256 *aaaQueueReader: Feb 27 10:15:25.593: Unable to find requested user entry for 4c776d9e6162 *aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9 *aaaQueueReader: Feb 27 10:15:25.593: ReProcessAuthentication previous proto 8, next proto 40000001 *aaaQueueReader: Feb 27 10:15:25.593: AuthenticationRequest: 0x7f01b4083638 *aaaQueueReader: Feb 27 10:15:25.593: proxyState.....70:69:5A:51:4E:C0-00:00 *aaaQueueReader: Feb 27 10:15:25.593: Packet contains 9 AVPs: *aaaQueueReader: Feb 27 10:15:25.593: AVP[01] User-Name.....4c776d9e6162 (12 bytes) 51-4e-c0 (17 bytes) 9e-61-62 (17 bytes) *aaaQueueReader: Feb 27 10:15:25.593: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes) *aaaQueueReader: Feb 27 10:15:25.593: AVP[05] Nas-Ip-(28271) (2 bytes) *aaaQueueReader: Feb 27 10:15:25.593: AVP[08] Service-Type.....0x0000000a (10) (4 bytes) *aaaQueueReader: Feb 27 10:15:25.593: AVP[09] Message-Authenticator.....DATA (16 bytes) *aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Error Response code for AAA Authentication : -7 *aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Returning AAA Error 'No Server' (-7) for mobile 70:69:5a:51:4e:c0 serverIdx 0 *aaaQueueReader: Feb 27 10:15:25.593: AuthorizationResponse: 0x7f017adf5770 *aaaQueueReader: Feb 27 10:15:25.593: RadiusIndexSet(0), Index(0) *aaaQueueReader: Feb 27 10:15:25.593: protocolUsed..... *aaaQueueReader: Feb 27 10:15:25.593: proxyState.....70:69:5A:51:4E:C0-00:00

*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 0 AVPs:

*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client.

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Failure Response sent to 0.0.0.0:5256

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Radius Authentication failed. Closing dtls Connection. *spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Disconnecting DTLS Capwap-Ctrl session 0xd6f0724fd8 for AP (192:168:79:151/5256). Notify(true) *spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 CAPWAP State: Dtls tear down

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 acDtlsPlumbControlPlaneKeys: lrad:192.168.79.151(5256) mwar:10.48.71.20(5246)

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS keys for Control Plane deleted successfully for AP 192.168.79.151

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS connection closed event receivedserver (10.48.71.20/5246) client (192.168.79.151/5256) *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Entry exists for AP (192.168.79.151/5256) *spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Unable to find AP 70:69:5a:51:4e:c0 *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 No AP entry exist in temporary database for *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 No AP entry exist in temporary database for

192.168.79.151:5256

Cette sortie montre les débogages quand l'adresse MAC LAP est ajoutée à la liste d'autorisation AP :

Note: Certaines lignes du résultat ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

(Cisco Controller) >debug capwap events enable (Cisco Controller) >debug capwap errors enable (Cisco Controller) >debug aaa all enable

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 using already alloced index 274
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Allocate database entry for AP 192.168.79.151:5256, already allocated index 274

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP Allocate request at index 274 (reserved)
*spamApTask4: Feb 27 09:50:25.393: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response, state Capwap_no_state *spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is not allowed to send in state Capwap_no_state for AP 192.168.79.151 *spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0 *spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Request failed! *aaaQueueReader: Feb 27 09:50:25.394: User 4c776d9e6162 authenticated *aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : 0 *aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Returning AAA Success for mobile 70:69:5a:51:4e:c0 *aaaQueueReader: Feb 27 09:50:25.394: AuthorizationResponse: 0x7f0288a66408 *aaaQueueReader: Feb 27 09:50:25.394: resultCode.....0 *aaaQueueReader: Feb 27 09:50:25.394: proxyState.....70:69:5A:51:4E:CO-00:00 *aaaQueueReader: Feb 27 09:50:25.394: Packet contains 2 AVPs: *aaaQueueReader: Feb 27 09:50:25.394: AVP[01] Service-Type.....0x00000065 (101) (4 bytes) *aaaQueueReader: Feb 27 09:50:25.394: AVP[02] Airespace / WLAN-Identifier.....0x00000000 (0) (4 bytes) *aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 User authentication Success with File DB on WLAN ID :0 *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Version: = 134770432 *spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K *spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType: 0x36 bundleApImageVer: 8.8.111.0 *spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0 *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len = 79 *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5256 *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 CAPWAP State: Join *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 capwap_ac_platform.c:2095 - Operation State 0 ===> 4*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Capwap State Change Event (Reg) from capwap_ac_platform.c 2136 *apfReceiveTask: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Register LWAPP event for AP 70:69:5a:51:4e:c0 slot 0

Autorisation AP sur un serveur AAA

Vous pouvez également configurer des WLC pour utiliser des serveurs RADIUS pour autoriser

des AP utilisant des MIC. Le WLC utilise une adresse MAC AP comme nom d'utilisateur et mot de passe lors de l'envoi des informations à un serveur RADIUS. Par exemple, si l'adresse MAC du point d'accès est 4c:77:6d:9e:61:62, le nom d'utilisateur et le mot de passe utilisés par le contrôleur pour autoriser le point d'accès sont cette adresse MAC en utilisant le délimiteur défini.

Cet exemple montre comment configurer les WLC pour autoriser les AP à l'aide de Cisco ISE.

- 1. Dans l'interface graphique du contrôleur WLC, cliquez sur Security > AP Policies. La page AP Policies apparaît.
- 2. Sous Policy Configuration, cochez la case correspondant à Authorize MIC APs against authlist or AAA.Lorsque vous choisissez ce paramètre, le WLC vérifie d'abord la liste d'autorisation locale. Si l'adresse MAC AP n'est pas présente, il vérifie le serveur RADIUS.

aludu								Sa <u>v</u> e Co	nfiguration	Ping	Logout <u>R</u> efresh
CISCO	MONITOR WLANS COM	TROLLER V	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK			🔒 <u>H</u> ome
Security	AP Policies								ſ	Apply	Add
 ▼ AAA General ▼ RADIUS 	Policy Configuration										
Authentication Accounting Auth Cached Users Fallback DNS	Accept Self Signed Certifica Accept Manufactured Insta Accept Local Significant Ce	ate (SSC) lled Certificate (rtificate (LSC)	(MIC)								
Downloaded AVP TACACS+ LDAP	Authorize MIC APs against	auth-list or AAA	A								
Local Net Users MAC Filtering Disabled Clients	Authorize LSC APs against	auth-list			Ent	ries 1 - 5 of 5					
AP Policies Password Policies	Search by MAC		Search	1							
Advanced EAD	MAC address / Serial Num	nber	Certificate	Type S	HA1 Key Hash						
Advanced LAP	4c:77:6d:9e:61:62		MIC								
Priority Order	70:d3:79:26:39:68		MIC								
Certificate	88:f0:31:7e:e0:38		MIC								
Access Control Lists	f4:db:e6:43:c4:b2		MIC								
Wireless Protection Policies	fc:5b:39:e7:2b:30		MIC								
▶ Web Auth											
TrustSec											

3. Naviguez jusqu'à Security > RADIUS Authentication de l'interface graphique du contrôleur pour afficher RADIUS Authentication Servers s'affiche. Dans cette page vous pouvez définir le Délimiteur MAC. Le WLC obtient l'adresse MAC AP et l'envoie au serveur Radius en utilisant le délimiteur défini ici. Ceci est important afin que le nom d'utilisateur corresponde à ce qui est configuré dans le serveur Radius. Dans cet exemple, le No Delimiter est utilisé pour que le nom d'utilisateur soit 4c776d9e6162.

ahaha										Sa <u>v</u> e Configu	uration Ping Logout	Refresh
CISCO	MONITOR	t <u>w</u> lans <u>c</u>	ONTROL	LER WIRELES	S <u>S</u> ECURIT	ry M <u>a</u> nagemen	r c <u>o</u> mmands	HELP	FEEDBACK		î	Home
Security	RADIUS	S Authenticat	tion Se	ervers	1.00						Apply New	v
 ▼ AAA General ▼ RADIUS Authentication 	Auth Ca Use AE	alled Station ID T S Key Wrap	ype [AP MAC Address	SSID) and requires a key wr	ap compliant RADI	IUS server)			
Accounting Auth Cached Users	MAC De	elimiter	p	No Delimiter 🔻								
DNS	Framed	TMIU		Colon								
Downloaded AVP TACACS+ LDAP User Management F				Hyphen	Server Addre	ess(Ipv4/Ipv6)			Port	IPSec	Admin Status	
Local Net Users MAC Filterion		Single Hyphen 10.48			10.48.39.100	.48.39.100				Disabled	Enabled	
 Disabled Clients User Login Policies AP Policies Password Policies 	×			No Delimiter	10.48.39.128				1812	Disabled	Enabled	
Local EAP												
Advanced EAP												
Priority Order												
Certificate												
Access Control Lists												
Wireless Protection Policies												
▶ Web Auth												
TrustSec												
Local Policies												

4. Cliquez ensuite sur New afin de définir un serveur RADIUS.

alialia			Sage Configuration Ping Logout Refresh
CISCO	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP	FEEDBACK A Home
Security	RADIUS Authentication Serve	ers > New	< Back Apply
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disable Clients User Login Policies A Prolicies Pasaword Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies 	Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Confirm Shared Secret Apply Cisco ISE Default settings Apply Cisco ACA Default settings Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Management Retransmit Timeout Tunnel Proxy PAC Provisioning IPSec Cisco ACA	3 ▼ 10.48.39.128 ASCII ▼ 	S server)
h Hashwalls			

 Définissez les paramètres du serveur RADIUS sur le RADIUS Authentication Servers > New S'affiche. Ces paramètres incluent le RADIUS Server IP Address, Shared Secret, Port Number, et Server Status. Lorsque vous avez terminé, cliquez sur Apply. Cet exemple utilise Cisco ISE comme serveur RADIUS avec l'adresse IP 10.48.39.128.

Configurer Cisco ISE pour autoriser les points d'accès

Pour permettre à Cisco ISE d'autoriser des points d'accès, vous devez effectuer les étapes suivantes :

- 1. Configurez le WLC en tant que client AAA sur Cisco ISE.
- 2. Ajoutez les adresses MAC AP à la base de données sur Cisco ISE.

Cependant, vous pouvez ajouter l'adresse MAC AP en tant que terminaux (la meilleure façon) ou en tant qu'utilisateurs (dont les mots de passe sont également l'adresse MAC), mais cela vous oblige à diminuer les exigences des stratégies de sécurité par mot de passe.

Étant donné que le WLC n'envoie pas l'attribut NAS-Port-Type qui est une condition requise sur ISE pour correspondre au flux de travail d'authentification d'adresse Mac (MAB), vous devez modifier ceci.

Configurer un nouveau profil de périphérique où MAB ne nécessite pas d'attribut de type de port NAS

Naviguez jusqu'à Administration > Network device profile et créer un nouveau profil de périphérique. Activez RADIUS et définissez le flux MAB filaire pour exiger service-type=Call-check, comme illustré dans l'image. Vous pouvez copier d'autres paramètres du profil Cisco classique, mais l'idée est de ne pas exiger l'attribut « Nas-port-type » pour un flux de travail MAB filaire.

		Admin	iistiation • Network Resource
letwork Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers
* Name	Ciscotemp		
Description			le le
lcon	the Change icon	o Default 🥡	
Vendor	Cisco		
Supported Protoc	cols		
RADIUS			
TACACS+			
TrustSec			
RADIUS Dictionaries			
Templates			
Expand All / Collapse All			
\sim Authentication	n/Authorization		
✓ Flow Type Co	onditions		
✓ Wired MAB deter	cted if the following condition(s) are a	met :	
Radius:Se	ervice-Type 🗸 =	Call Check	<u>∽</u>

Configurer le WLC en tant que client AAA sur Cisco ISE

- 1. Aller à Administration > Network Resources > Network Devices > Add. La page New Network Device s'affiche.
- 2. Sur cette page, définissez le WLC Name, Interface de

gestion IP Address et Radius Authentications Settings genre Shared Secret. Si vous prévoyez d'entrer les adresses MAC AP en tant que points d'extrémité, assurez-vous d'utiliser le profil de périphérique personnalisé configuré précédemment plutôt que le profil Cisco par défaut !

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers License Warning	<u>a</u> (0 0	- 0
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC			
Network Devices Network Device (3roups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services			
G	Network Devices			
Network Devices	* Name WLC5520			
Default Device	Description			
Device Security Settings				
	IP Address • IP : 10.48.71.20 / 32	- 		
	O IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected			
	* Davida Profile de Clana - D			
	Model Name 👻			
	Software Version			
	* Network Device Group			
	Network Device Oroup			
	Location LAB Set To Default			
	IPSEC No Set To Default			
	Device Type WLC-lab Set To Default			
	RADIUS Authentication Settings			
		-		
	RADIUS UDP Settings			
	Protocol RADIUS			
	* Shared Secret Show			
	CoA Port 1700 Set To Default			
	RADIUS DTLS Settings (7)			
	DTLS Required (7)			
	Shared Secret radius/dtls (7)			

3. Cliquer Submit.

Ajoutez l'adresse MAC AP à la base de données des terminaux sur Cisco ISE

Naviguez jusqu'à Administration > Identity Management > Identities et ajoutez les adresses MAC à la base de données des terminaux.

Ajouter l'adresse MAC AP à la base de données utilisateur sur Cisco ISE (facultatif)

Si vous ne souhaitez pas modifier le profil MAB câblé et que vous choisissez de placer l'adresse MAC AP en tant qu'utilisateur, vous devez diminuer les exigences de la stratégie de mot de passe.

Naviguez jusqu'à Administration > Identity Management. Ici, nous devons nous assurer que la
politique de mot de passe permet l'utilisation du nom d'utilisateur comme mot de passe et la
politique doit également permettre l'utilisation des caractères d'adresse MAC sans avoir
besoin de différents types de caractères. Naviguez
ivegu'à a mune de transference de transferen

jUSQU'à Settings > User Authentication Settings > Password Policy:

cisco Identity Services Engine	Home	.icense Warning 🔺	0,	0	0
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC				
Identities Groups External Iden	ntity Sources Identity Source Sequences - Settings				
User Custom Attributes	Password Policy Account Disable Policy				
User Authentication Settings	Password Policy				2
Endpoint Purge	* Minimum Length: 4 characters (Valid Range 4 to 127)				
Endpoint Custom Attributes	Password must not contain:				
	User name or its characters in reverse order				
	"Cisco" or its characters in reverse order				
	This word or its characters in reverse order:				
	Repeated characters four or more times consecutively				
	Dictionary words, their characters in reverse order or their letters replaced with other characters ()				
	Default Dictionary				
	Custom Dictionary (i) Choose File No file chosen				
	The newly added custom dictionary file will replace the existing custom dictionary file.				
	Password must contain at least one character of each of the selected types:				
	Lowercase alphabetic characters				
	Uppercase alphabetic characters				
	Vurmeric characters				
	Non-alphanumeric characters				
	Password History				

2. Accédez ensuite à Identities > Users et cliquez sur Add. Lorsque la page User Setup apparaît, définissez le nom d'utilisateur et le mot de passe pour ce point d'accès comme indiqué.

Astuce : Utilisez **Description** pour entrer le mot de passe afin de pouvoir savoir facilement ce qui a été défini comme mot de passe.

Le mot de passe doit également être l'adresse MAC AP. Dans cet exemple, il est 4c776d9e6162.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	۹ 0	•
► System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC			
Groups External Ident	ty Sources Identity Source Sequences + Settings			
	Network Access Users List > New Network Access User			
Latest Manual Matural Core Days	 Network Access User 			
Latest Manual Network Scan Results	* Name 4c776d9e6162			
	Status 🛃 Enabled 👻			
	Email			
	▼ Passwords			
	Password Type: Internal Users 🔹			
	Password Re-Enter Password			
	* Login Password Generate Password (
	Enable Password Generate Password			
	▼ User Information			
	First Name			
	Last Name			
	▼ Account Ontions			
	Paccount options			
	Description [pass=4c7/00/960102	A		
	Change password on next login			
	▼ Account Disable Policy			
	Disable account if date exceeds 2019-04-28 (yyyy-mm-dd)			
	▼ User Groups			
	APs 🔘 😁	+		
	Submt Cancel			
1			_	

3. Cliquer Submit.

Définir un ensemble de stratégies

 Vous devez définir un Policy Set pour correspondre à la demande d'authentification provenant du WLC. Vous commencez par créer une condition en naviguant jusqu'à Policy > Policy Elements > Conditionset en créant une nouvelle condition pour correspondre à l'emplacement du WLC, dans cet exemple, 'LAB_WLC' et Radius:Service-Type Equals Call Check qui est utilisé pour l'authentification Mac. Ici, la condition est nommée

Type Equals Call Check qui est utilisé pour l'authentification Mac. Ici, la condition est nommé 'AP_Auth'.

Policy Sets Profiling Posture Cleant Provisioning Policy Elements Dictionaries Conditions + Results Smart Conditions Smart Conditions Time and Date Profiling Posture Posture Posture Posture Device Port Network Conditions Device Port Network Conditions <th>cisco Identity Services Engine</th> <th>Home</th> <th>Policy Administration</th> <th>Work Centers</th> <th>License Warning 🔺 🔍 👴</th> <th>• •</th>	cisco Identity Services Engine	Home	Policy Administration	Work Centers	License Warning 🔺 🔍 👴	• •
Dictionaries • Result	Policy Sets Profiling Posture	Client Provisioning Policy Elements				
Library Conditions Smart Conditions Time and Date Profiling Posture • Network Conditions Device Network Conditions Device Network Conditions Device Port Network Conditions Device Network Conditions Device Network Conditions Device Network Conditions Device Port Net	Dictionaries Conditions Res	sults				
Smart Conditions Time and Date Profiling Posture	Library Conditions	C Library	Editor			
Time and Date Profiling Posture Posture Network Conditions Endstation Network Conditions Device Network Conditions Device Network Conditions Device Network Conditions Device Port Network Conditions Device Network Conditions Device Port Network Conditions Default condition used to match authentication requests for Local Web Authe structures Default condition used to match authentication requests for Local Web Authe structures	Smart Conditions	Search by Name				· · ·
Profiling Posture • Posture • Network Conditions Endstation Network Conditions Device Port Network Condition requests for Local Web_Authe ntication Default condition used to match authentication from Cisco Catalyst Switches	Time and Date			Radius Service-Type		
Posture • Posture • Network Conditions Endstation Network Conditions Device Network Conditions Device Port Network Condition requests for Local Web_Authe Device Port Network Conditions	Profiling	♥▫□▰▫ਸ਼ਸ਼₽₪⊻	S 2 2	Equals V Call Check		
Network Conditions Endstation Network Conditions Device Port Network Condition sed to match authentication from Cisco Catalysts Switches	Posture	AP_Auth)	
Endstation Network Conditions BYOD_is_Registered Device Network Conditions Default condition for BYOD flow for any @ device that has passed the NSP or device that has passed the NSP o	- Network Conditions	Condition for authe/authz of APs.	AND T	LAB_WLC		۲
Device Network Conditions Default condition for PrOD Not for any (r) Device Port Network Conditions Catalyst Switch_Local Web_Authe nication Device Port Network Conditions Catalyst Switch_Local Web_Authe nication Device Port Network Conditions Default condition used to match authentication from Cisco Catalyst Switches	Endstation Network Conditions	BYOD_is_Registered				
Device Port Network Conditions Catalyst Switch_Local_Web_Authe nication Default condition used to match authentication from Cisco Catalyst Switches Image: Catalyst Switches	Device Network Conditions	device that has passed the NSP	D	+ New (4	AND OR	
Catalyst_Switch_Local_Web_Authe Set to 'Is not' Duplicate Save ntication Default condition used to match authentication from Cisco Catalyst Switches	Device Port Network Conditions	process			and a second and a second of	
Intradium Intradium		Catalyst_Switch_Local_Web_Authe	Set	to 'Is not'	Duplicate	Save
authentication requests for Local Web Authentication from Cisco Catalyst Switches		Default condition used to match (D			-
Switches		authentication requests for Local Web Authentication from Cisco Catalyst				
		Switches				

- 2. Cliquer Save.
- 3. Créez ensuite un nouveau Allowed Protocols Service pour l'authentification AP. Assurez-vous de choisir uniquement Allow PAP/ASCII:

cisco Identity Services Engine	Home → Context Visibility	Operations Po	Icy Administration	Work Centers	License Warning 🔺	Q,	0	•	0
Policy Sets Profiling Posture	Client Provisioning - Policy Eleme	nts							
Dictionaries + Conditions - Res	ults								
- Authentication	Allowed Protocols Services List Allowed Protocols	> AP_authentication							
Allowed Protocols	Name AP_authentica	tion							
Authorization	Description								
Profiling			10						
Posture	✓ Allowed Protocols								
Client Provisioning	Authentication Bypa	ss okup (j)							
	Authentication Proto	cols							
	Allow CHAP								
	Allow MS-CHAP	/1							
	Allow MS-CHAP	12							
	Allow EAP-MD5								
	Allow EAP-TLS								
	Allow LEAP								
	Allow PEAP								

4. Sélectionnez le service précédemment créé dans la Allowed Protocols/Server Sequence. Développez le View et Authentication Policy > Use > Internal Users afin qu'ISE recherche le nom d'utilisateur/mot de passe de l'AP dans la base de données interne.

cy Sets	Profiling Posture Client Provis	sioning Policy Elements				
cy Sets	s				Reset	Sav
Stat	tus Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits Actio	ns Vie
arch						
0	Policy4APsAuth		AP_Auth	AP_authentication * * +	19 🌣	- D
0	Default	Default policy set		Default Network Access × +	591 Ö	,
					Reset	Sav
Identi	ity Services Engine Home	← Context Visibility → Op	perations Policy Administration Work Centers	License Warning 🔺	۹. 8	0
y Sets	Profiling Posture Client Provi	isioning				
cy Set	s → Policy4APsAuth				Reset	Sav
Sta	atus Policy Set Name	Description	Conditions	Allowed Protocols /	Server Sequen	ce Hi
arch						
6	Policy4APsAuth		AP_Auth	AP_authentication	x	+ 1
Authenti	cation Policy (1)					
+ s	tatus Rule Name	Conditions		Use	Hits	Action
earch						
			+		-	
	Default			Internal Users Options	* * 19	¢
Authoriza	ation Policy - Local Exceptions					
Authoriza	ation Policy - Global Exceptions					

5. Cliquer Save.

Vérification

Afin de vérifier cette configuration, vous devez connecter le point d'accès avec l'adresse MAC 4c:77:6d:9e:61:62 au réseau et au moniteur.

Utilisez debug capwap events/errors enable et debug aaa all enable afin d'effectuer cette opération.

Comme le montrent les débogages, le WLC a transmis l'adresse MAC AP au serveur RADIUS 10.48.39.128, et le serveur a authentifié avec succès l'AP. L'AP s'enregistre alors auprès du contrôleur.

Note: Certaines lignes du résultat ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5248

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 using already alloced index 437
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Allocate database entry for AP

192.168.79.151:5248, already allocated index 437 *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP Allocate request at index 437 (reserved) *spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5248 from temporary database. *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc. *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5248) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response, state Capwap_no_state *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is not allowed to send in state Capwap_no_state for AP 192.168.79.151 *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0 *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request failed! *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5248 *spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Failed to parse CAPWAP packet from 192.168.79.151:5248 *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9 *aaaQueueReader: Feb 27 14:58:07.566: ReProcessAuthentication previous proto 8, next proto 40000001 *aaaQueueReader: Feb 27 14:58:07.566: AuthenticationRequest: 0x7f01b404f0f8 *aaaQueueReader: Feb 27 14:58:07.566: Callback..... *aaaQueueReader: Feb 27 14:58:07.566: proxyState......70:69:5A:51:4E:C0-00:00 *aaaQueueReader: Feb 27 14:58:07.566: Packet contains 9 AVPs: *aaaQueueReader: Feb 27 14:58:07.566: AVP[02] Called-Station-Id......70:69:5a:51:4e:c0 (17 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[03] Calling-Station-Id.....4c:77:6d:9e:61:62 (17 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes) (28271) (2 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[08] Service-Type.....0x0000000a (10) (4 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[09] Message-Authenticator.....DATA (16 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 radiusServerFallbackPassiveStateUpdate:
RADIUS server is ready 10.48.39.128 port 1812 index 1 active 1

*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 NAI-Realm not enabled on Wlan, radius servers will be selected as usual *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Found the radius server : 10.48.39.128 from the global server list *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Send Radius Auth Request with pktId:185 into gid:0 of server at index:1 *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Sending the packet to v4 host 10.48.39.128:1812 of length 130 *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Successful transmission of Authentication Packet (pktId 185) to 10.48.39.128:1812 from server queue 0, proxy state 70:69:5a:51:4e:c0-00:00 *aaaQueueReader: Feb 27 14:58:07.566: 00000000: 01 b9 00 82 d9 c2 ef 27 f1 bb e4 9f a8 88 5a 6dZm *aaaQueueReader: Feb 27 14:58:07.566: 00000010: 4b 38 1a a6 01 0e 34 63 37 37 36 64 39 65 36 31 K8....4c776d9e61 *aaaQueueReader: Feb 27 14:58:07.566: 00000020: 36 32 1e 13 37 30 3a 36 39 3a 35 61 3a 35 31 3a 62..70:69:5a:51: *aaaQueueReader: Feb 27 14:58:07.566: 00000030: 34 65 3a 63 30 1f 13 34 63 3a 37 37 3a 36 64 3a 4e:c0..4c:77:6d: *aaaQueueReader: Feb 27 14:58:07.566: 00000040: 39 65 3a 36 31 3a 36 32 05 06 00 00 01 04 06 9e:61:62.... *aaaQueueReader: Feb 27 14:58:07.566: 00000050: 0a 30 47 14 20 04 6e 6f 02 12 54 46 96 61 2a 38 .0G...no..TF.a*8 *aaaQueueReader: Feb 27 14:58:07.566: 00000060: 5a 57 22 5b 41 c8 13 61 97 6c 06 06 00 00 00 0a ZW"[A..a.l.... *aaaQueueReader: Feb 27 14:58:07.566: 0000080: 15 f9 .. *aaaOueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client. *radiusTransportThread: Feb 27 14:58:07.587: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9) *radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 *** Counted VSA 150994944 AVP of length 28, code 1 atrlen 22) *radiusTransportThread: Feb 27 14:58:07.588: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9) *radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 AVP: VendorId: 9, vendorType: 1, vendorLen: 22 *radiusTransportThread: Feb 27 14:58:07.588: 00000000: 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 55 6e 6b profile-name=Unk *radiusTransportThread: Feb 27 14:58:07.588: 00000010: 6e 6f 77 6e nown *radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Processed VSA 9, type 1, raw bytes 22, copied 0 bytes *radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Access-Accept received from RADIUS server 10.48.39.128 (qid:0) with port:1812, pktId:185 *radiusTransportThread: Feb 27 14:58:07.588: RadiusIndexSet(1), Index(1) *radiusTransportThread: Feb 27 14:58:07.588: protocolUsed.....0x00000001 *radiusTransportThread: Feb 27 14:58:07.588: proxyState.....70:69:5A:51:4E:C0-00:00 *radiusTransportThread: Feb 27 14:58:07.588: Packet contains 4 AVPs: *radiusTransportThread: Feb 27 14:58:07.588: AVP[01] User-Name.....4c776d9e6162 (12 bytes) *radiusTransportThread: Feb 27 14:58:07.588: AVP[02] State.....ReauthSession:0a302780bNEx79SKIFosJ2ioAmIYNOiRe2iDSY3dr cFsHuYpChs (65 bytes)

*radiusTransportThread: Feb 27 14:58:07.588: AVP[03]
Class.....DATA (83 bytes)

```
*radiusTransportThread: Feb 27 14:58:07.588: AVP[04] Message-
Authenticator......DATA (16 bytes)
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Version: = 134770432
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00 apType: 0x36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5248
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 CAPWAP State: Join
```

Dépannage

Utilisez ces commandes pour dépanner votre configuration :

- debug capwap events enable: configure le débogage des événements LWAPP
- debug capwap packet enable— Configure le débogage de la trace de paquet LWAPP
- debug capwap errors enable— Configure le débogage des erreurs de paquets LWAPP
- debug aaa all enable: configure le débogage de tous les messages AAA

Dans ce cas, ISE signale dans le journal RADIUS en direct le nom d'utilisateur « INVALID » au moment où vous avez des AP autorisés par rapport à ISE, cela signifie que l'authentification est vérifiée par rapport à la base de données de point d'extrémité et que vous n'avez pas modifié le profil MAB câblé comme expliqué dans ce document. ISE considère qu'une authentification d'adresse MAC n'est pas valide si elle ne correspond pas au profil MAB filaire/sans fil, qui par défaut nécessite l'attribut NAS-port-type qui n'est pas envoyé par le WLC.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.