Configuration des flux ISE Wireless CWA et Hotspot avec AireOS et les WLC de nouvelle génération

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Configurer Diagramme du réseau Configuration du WLC Unified 5508 Configuration globale Configurez le SSID (Service Set Identifier) de l'invité : Configurer la liste de contrôle d'accès Redirect **Redirection HTTPS Basculement agressif Dérivation Captive** Configuration du NGWC convergent 3850 Configuration globale **Configuration SSID** Configuration d'une liste de contrôle d'accès de redirection Configuration de l'interface de ligne de commande (CLI) Configuration d'ISE Tâches de configuration ISE courantes Exemple d'utilisation 1 : CWA avec authentification des invités dans chaque connexion utilisateur Exemple d'utilisation 2 : CWA avec Device Registration appliquant l'authentification des invités une fois par jour. Exemple d'utilisation 3 : portail HostSpot Vérifier Cas d'utilisation 1 Cas d'utilisation 2 Cas d'utilisation 3 Commutation locale FlexConnect dans AireOS Scénario D'Ancrage À L'Étranger Dépannage États cassés courants sur AireOS et le WLC d'accès convergé WLC AireOS NGWC ISE Informations connexes

Introduction

Ce document décrit comment configurer trois cas d'invité dans le moteur Identity Services avec Cisco AireOS et les contrôleurs LAN sans fil de nouvelle génération.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleurs LAN sans fil Cisco (accès unifié et convergé)
- Identity Services Engine (ISE)

Composants utilisés

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

- Cisco Identity Services Engine version 2.1
- Contrôleur LAN sans fil Cisco 5508 avec 8.0.121.0
- Contrôleur sans fil nouvelle génération (NGWC) Catalyst 3850 (WS-C3850-24P) avec 03.06.04.E

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.

Configurer

Diagramme du réseau



Les étapes décrites dans ce document décrivent la configuration type sur les WLC d'accès unifié et convergé pour prendre en charge n'importe quel flux invité avec ISE.

Configuration du WLC Unified 5508

Quel que soit le cas d'utilisation configuré dans ISE, du point de vue du WLC, tout commence par un point d'extrémité sans fil qui se connecte à un SSID ouvert avec le filtrage MAC activé (plus AAA override et RADIUS NAC) qui pointe vers ISE comme serveur d'authentification et de comptabilité. Cela garantit qu'ISE peut transmettre dynamiquement les attributs nécessaires au WLC pour l'application réussie d'une redirection vers le portail invité d'ISE.

Configuration globale

- 1. Ajoutez ISE globalement en tant que serveur d'authentification et de comptabilité.
 - Accédez à Security > AAA > Authentication et cliquez sur New

Security	RADIUS Authentication Se	rvers > Edit
 ▼ AAA General ▼ RADIUS Authentication Accounting 	Server Index Server Address(Ipv4/Ipv6) Shared Secret Format	6 ASCII T
Fallback. DNS	Shared Secret	•••
Downloaded AVP	Confirm Shared Secret	•••
LDAP Local Net Users	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Filtering Disabled Clients	Port Number	1812
User Login Policies	Server Status	Enabled *
AP Policies Password Policies	Support for RFC 3576	Enabled *
Local EAP	Server Timeout	S seconds
Advanced EAP	Network User	🗹 Enable
Priority Order	Management	C Enable
Certificate	Realm List	
Access Control Lists	IPSec	Enable Enable

- Saisissez l'adresse IP du serveur ISE et le secret partagé
- Assurez-vous que l'état du serveur et la **prise en charge de RFC 3676** (modification d'autorisation ou prise en charge CoA) sont tous deux définis sur **Activé**.
- Sous le délai d'attente du serveur par défaut, les WLC AireOS ont 2 secondes. En fonction des caractéristiques du réseau (latence, ISE et WLC à différents emplacements), il peut être avantageux d'augmenter le délai d'attente du serveur à au moins 5 secondes pour éviter des événements de basculement inutiles.
- Cliquez sur Apply.
- S'il y a plusieurs noeuds de services de stratégie (PSN) à configurer, continuez à créer des entrées de serveur supplémentaires.

Remarque : cet exemple de configuration particulier inclut 2 instances ISE

- Accédez à Security > AAA > RADIUS > Accounting et cliquez sur New
- Saisissez l'adresse IP du serveur ISE et le secret partagé
- Assurez-vous que l'état du serveur est défini sur Activé
- Augmentez le délai d'attente du serveur si nécessaire (la valeur par défaut est 2 secondes).
- 2. Configuration de secours.

Dans un environnement unifié, une fois le délai d'attente du serveur déclenché, le WLC passe au serveur configuré suivant. Prochain dans la ligne à partir du WLAN. Si aucune autre option n'est disponible, le WLC sélectionne la suivante dans la liste des serveurs globaux. Lorsque plusieurs serveurs sont configurés sur le SSID (principal, secondaire) une fois que le basculement se produit, le WLC continue par défaut à envoyer le trafic d'authentification et (ou) de comptabilité de manière permanente à l'instance secondaire, même si le serveur principal est de nouveau en ligne.

Afin d'atténuer ce comportement, activez le fallback. Accédez à **Security > AAA > RADIUS > Fallback.** Le comportement par défaut est désactivé. La seule façon de récupérer à partir d'un événement de serveur arrêté nécessite une intervention de l'administrateur (rebondir globalement l'état d'administrateur du serveur).

Pour activer la reprise, vous avez deux options :

- Passif : en mode passif, si un serveur ne répond pas à la demande d'authentification WLC, le WLC déplace le serveur vers la file d'attente inactive et définit un minuteur (option Intervalle en secondes). Lorsque le minuteur expire, le WLC déplace le serveur vers la file d'attente active indépendamment de l'état réel des serveurs. Si la demande d'authentification entraîne un événement de délai d'attente (ce qui signifie que le serveur est toujours arrêté), l'entrée du serveur est déplacée à nouveau vers la file d'attente Inactive et le minuteur s'enclenche à nouveau. Si le serveur répond correctement, il reste dans la file d'attente active. Les valeurs configurables ici vont de 180 à 3600 secondes.
- Actif : en mode actif, lorsqu'un serveur ne répond pas à la demande d'authentification WLC, le WLC marque le serveur comme étant mort, puis déplace le serveur vers un pool de serveurs non actifs et commence à envoyer des messages d'analyse périodiquement jusqu'à ce que ce serveur réponde. Si le serveur répond, alors le WLC déplace le serveur mort vers le pool actif et arrête d'envoyer des messages de sonde.

Dans ce mode, le WLC vous demande d'entrer un nom d'utilisateur et un intervalle d'analyse en secondes (180 à 3600).

Remarque : la sonde WLC ne nécessite pas une authentification réussie. Dans les deux cas, une authentification réussie ou échouée est considérée comme une réponse du serveur qui est suffisante pour promouvoir le serveur dans la file d'attente active.

Configurez le SSID (Service Set Identifier) de l'invité :

• Accédez à l'onglet WLANs et sous l'option Create New, cliquez sur Go :



- Saisissez le nom du profil et le nom SSID. Cliquez sur Apply.
- Sous l'onglet Général, sélectionnez l'interface ou le groupe d'interfaces à utiliser (VLAN invité).

Radio Policy	All	•
Interface/Interface Group(G)	guest2	T

 Sous Security > Layer 2 > Layer 2 Security, sélectionnez None et activez la case à cocher Mac Filtering.

General	Security	QoS	Policy-Mapping	Advanced
Layer 2	Layer 3	AAA S	ervers	
Layer 2	Security 🧕 🚺	lone	¥	

• Sous l'onglet **AAA Servers**, définissez Authentication and Accounting servers sur **enabled** et sélectionnez vos serveurs principal et secondaire.

eneral	Security	QoS	Policy-	Mapping	Advanced
Layer 2	Layer 3	AAA S	Servers		
Select AAA s Radius Serv Radius Se	servers belo ers erver Overwr Authentica	w to ove ite interfa tion Serv	rride use o ce 🛛 Ena	abled	ervers on this WLAI
	Persona		ers	Recountin	g Servers
Server 1	Enabled	57.210, P	ort:1812 V	Enabled	g Servers
Server 1 Server 2	Enabled	57.210, P	ort:1812 ¥	Enabled	g Servers 157.210, Port:1813 ¥ 157.21, Port:1813 ¥
Server 1 Server 2 Server 3	Enabled IP: 11	57.210, P 57.21, Po	ort:1812 ¥ rt:1812 ¥	Enabled IP	g Servers 157.210, Port:1813 ¥ 157.21, Port:1813 ¥
Server 1 Server 2 Server 3 Server 4	Enabled IP: 11 IP: 11 None None	57.210, P 57.21, Po	ort:1812 ¥ rt:1812 ¥ ¥	Enabled IP IP None None	g Servers 157.210, Port:1813 ¥ 157.21, Port:1813 ¥ ¥
Server 1 Server 2 Server 3 Server 4 Server 5	C Enabled IP: 11 IP: 11 None None None	57.210, Pi 57.21, Po	ort:1812 * rt:1812 * *	Cenabled IP IP IP None None None	g Servers 157.210, Port:1813 ¥ 157.21, Port:1813 ¥ ¥

Mise à jour provisoire : il s'agit d'une configuration facultative qui n'ajoute aucun avantage à ce flux. Si vous préférez l'activer, le WLC i doit exécuter le code 8.x ou supérieur :
 Disabled : la fonctionnalité est complètement désactivée.

Enabled with 0 Interval : le WLC envoie des mises à jour de comptabilité à ISE chaque fois qu'il y a une modification dans l'entrée Mobile Station Control Block (MSCB) du client (ie. Affectation ou modification d'adresse IPv4 ou IPv6, événement d'itinérance client.) Aucune mise à jour périodique supplémentaire n'est envoyée.

Activé avec un intervalle temporaire configuré : Dans ce mode, le WLC envoie des notifications à ISE lors des modifications d'entrée MSCB du client et il envoie également des notifications de comptabilité périodiques supplémentaires à l'intervalle configuré (quelles que soient les modifications).

- Sous l'onglet Avancé, sélectionnez Autoriser le remplacement AAA et Sous l'état NAC, sélectionnez RADIUS NAC. Cela garantit que le WLC applique toutes les paires de valeurs d'attribut (AVP) qui proviennent d'ISE.
- Accédez à l'onglet SSID general et définissez l'état SSID sur Enabled

```
WLANs > Edit 'Guest'
```

General	Security	QoS	Policy-Mapping	Advanced				
Profile Na	ime	Gu	jest					
Туре		W	WLAN					
SSID		Gu	iest					
Status			Enabled					

• Appliquez les modifications.

Configurer la liste de contrôle d'accès Redirect

Cette liste de contrôle d'accès est référencée par ISE et détermine le trafic qui est redirigé et le trafic autorisé.

- Accédez à l'onglet Sécurité > Listes de contrôle d'accès et cliquez sur Nouveau
- Voici un exemple de liste de contrôle d'accès

Acci	ess Con	trol Lists > Edit									i i	< Back
Gene	ral											
Acces	s List Nam	e Guest_Rei	direct									
Deny	Counters	0										
Seq	Action	Source IP/Mask		Destination IP/	Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	DNS	Any	Any	0	
2	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DNS	Any	Any	Any	0	
2	Permit	0.0.0.0	/ 0.0.0.0	.157.210	/ 255.255.255.255	TCP	Any	8443	Any	Any	0	•
4	Permit	157.210	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	8443	Any	Any	Any	0	
2	Permit	0.0.0.0	/ 0.0.0.0	.157.21	/ 255.255.255.255	TCP	Any	8443	Any	Any	0	
<u>6</u>	Permit	157.21	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	8443	Any	Any	Any	0	

Cette liste de contrôle d'accès doit autoriser l'accès aux services DNS et aux noeuds ISE via le port TCP 8443. Il y a un refus implicite en bas qui signifie que le reste du trafic est redirigé vers l'URL du portail invité d'ISE.

Redirection HTTPS

Cette fonctionnalité est prise en charge dans AireOS versions 8.0.x et ultérieures, mais elle est désactivée par défaut. Pour activer la prise en charge de HTTPS, accédez à **Gestion** WLC > **HTTP-HTTPS > Redirection HTTPS** et définissez-la sur **Activé** ou appliquez la commande suivante dans CLI :

(Cisco Controller) >config network web-auth https-redirect enable Avertissements de certificat après activation de la redirection HTTPS

Une fois que https-redirect est activé, l'utilisateur peut rencontrer des problèmes d'approbation de certificat pendant la redirection. Ceci est visible même s'il y a un certificat enchaîné valide sur le contrôleur et même si ce certificat est signé par une autorité de certification tierce approuvée. La raison est que le certificat installé sur le WLC est émis vers son nom d'hôte d'interface virtuelle ou son adresse IP. Lorsque le client tente https://cisco.com, le navigateur s'attend à ce que le certificat soit émis vers cisco.com. Cependant, pour que le WLC puisse intercepter l'GET émis par le client, il doit d'abord établir la session HTTPS pour laquelle le WLC présente son certificat d'interface virtuelle pendant la phase de connexion SSL. Cela entraîne l'affichage d'un avertissement par le navigateur, car le certificat présenté lors de la connexion SSL n'a pas été émis vers le site Web d'origine auquel le client tente d'accéder (par exemple, cisco.com par opposition au nom d'hôte de l'interface virtuelle du WLC). Vous pouvez voir différents messages d'erreur de certificat dans différents navigateurs, mais tous sont liés au même problème.

Basculement agressif

Cette fonctionnalité est activée par défaut dans les WLC AireOS. Lorsque le basculement agressif est activé, le WLC marque le serveur AAA comme ne répondant pas et il passe au serveur AAA configuré suivant après qu'un événement de délai d'attente RADIU affecte un client.

Lorsque la fonctionnalité est désactivée, le WLC bascule vers le serveur suivant uniquement si l'événement de délai d'attente RADIUS se produit avec au moins 3 sessions client. Cette fonction peut être désactivée par cette commande (aucun redémarrage n'est requis pour cette commande) :

(Cisco Controller) >config radius aggressive-failover disable Pour vérifier l'état actuel de la fonction :

(Cisco Controller) > show radius summary

Vendor Id Backward Compatibility	Disabled
Call Station Id Case	lower
Acct Call Station Id Type	Mac Address
Auth Call Station Id Type	AP's Radio MAC Address:SSID
Extended Source Ports Support	Enabled
Aggressive Failover	Disabled

Dérivation Captive

Les terminaux qui prennent en charge un mécanisme CNA (Captive Network Assistant) pour détecter un portail captif et lancer automatiquement une page de connexion le font généralement via un pseudo-navigateur dans une fenêtre contrôlée, tandis que les autres terminaux lancent un navigateur entièrement capable de déclencher ce mécanisme. Pour les terminaux où le CNA lance un pseudo-navigateur, cela peut interrompre le flux lorsqu'il est redirigé vers un portail captif ISE. Cela affecte généralement les périphériques Apple IOS et a des effets particulièrement

négatifs dans les flux qui nécessitent l'enregistrement des périphériques, la libération DHCP VLAN, le contrôle de conformité.

En fonction de la complexité du flux utilisé, il peut être recommandé d'activer le contournement captif. Dans un tel scénario, le WLC ignore le mécanisme de détection du portail CNA et le client doit ouvrir un navigateur pour lancer le processus de redirection.

Vérifiez l'état de la fonctionnalité :

(Cisco Controller) > show network summary

Web	Auth	CMCC Support	Disabled
Web	Auth	Redirect Ports	80,3128
Web	Auth	Proxy Redirect	Disable
Web	Auth	Captive-Bypass	Disabled
Web	Auth	Secure Web	Enable
Web	Auth	Secure Redirection	Enable

Pour activer cette fonction, entrez cette commande :

(Cisco Controller) >config network web-auth captive-bypass enable Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect.

Le WLC avertit l'utilisateur que pour que les modifications prennent effet, un système de réinitialisation (redémarrage) est nécessaire.

À ce stade, un **show network summary** montre la fonctionnalité comme étant activée, mais pour que les modifications prennent effet, le WLC doit être redémarré.

Configuration du NGWC convergent 3850

Configuration globale

1. Ajouter ISE globalement en tant que serveur d'authentification et de comptabilité

- Accédez à Configuration > Security > RADIUS > Servers et cliquez sur New
- Saisissez l'adresse IP du serveur ISE, le secret partagé, le délai d'attente du serveur et le nombre de tentatives qui reflètent vos conditions environnementales.
- Assurez-vous que la prise en charge de RFC 3570 (prise en charge CoA) est activée.
- Répétez la procédure pour ajouter une entrée de serveur secondaire.

RADIUS Servers		6
Radius Servers > New		
Server Name	ISE1	
Server IP Address	.157.210	
Shared Secret	*****	
Confirm Shared Secret		
Auth Port (0-65535)	1812	
Acct Port (0-65535)	1813	
Server Timeout (1-1000)secs	5	
Retry Count (0-100)	2	
Support for RFC 3576	Enable 💌	
0		

2. Créer le groupe de serveurs ISE

- Accédez à Configuration > Security > Server Groups et cliquez sur New
- Attribuez un nom au groupe et entrez une valeur **Dead-time** en minutes. Il s'agit du temps pendant lequel le contrôleur maintient le serveur dans la file d'attente Inactive avant qu'il ne soit promu à nouveau dans la liste des serveurs actifs.
- Dans la liste Serveurs disponibles, ajoutez-les à la colonne Serveurs affectés.

Radius Server Group			
Radius Server Group > New			
Name	ISE_Group		
MAC-delimiter	colon 💌		
MAC-filtering	none 💌		
Dead-time (0-1440) in min	nutes 10		
Group Type	radius		
	Available Servers	Assigned Server	s
		▲ ISE2 ISE1	-
Servers In This Group		< >	
	2		*

3. Activer globalement Dot1x

Accédez à Configuration > AAA > Method Lists > General et activez Dot1x system Auth

Control

General	
Dot1x System Auth Control	
Local Authentication	None 💌
Local Authorization	None 💌

- 4. Configurer les listes de méthodes
 - Accédez à Configuration > AAA > Method Lists > Authentication et créez une nouvelle liste de méthodes. Dans ce cas, il s'agit de Type Dot1x et Group ISE_Group (groupe créé à l'étape précédente). Cliquez ensuite sur Apply

Authentication Authentication > New				
Method List Name	ISE_Method			
Type: Group Type: Fallback to local	dot1x O login group O local			
and a state of the second s	Available Server Groups		Assigned Server Groups	
Groups In This Method		*	ISE_Group	÷.
		+		*

Procédez de même pour la comptabilité (Configuration > AAA > Listes de méthodes > comptabilité) et l'autorisation (Configuration > AAA > Listes de méthodes > Autorisation). Ils doivent ressembler à ça

Accounting > New		
Method List Name	ISE_Method	
Type:	O dot1x O exec identity O network	rk O commands
1000	Available Server Groups	Assigned Server Groups
Groupe In This Mothod	*	ISE_Group ^
Gloups in This Medido	<	>
	*	*

Authorization Authorization > New		
Method List Name	ISE_Method	
Type: Group Type:	network O exec O credential-download oroun O local	
Gloup Type.	Available Server Groups	Assigned Server Groups
Groups In This Method	^ < >	ISE_Group
	Ψ.	¥

5. Créez la méthode MAC-filter d'autorisation.

Ceci est appelé à partir des paramètres SSID plus tard.

- Accédez à Configuration> AAA > Method Lists > Authorization et cliquez sur New.
- Saisissez le nom de la liste de méthodes. Choisissez Type = Network and Group Type Group.
- Ajoutez ISE_Group au champ Assigned Server Groups.

Authorization Authorization > New				
Method List Name	MacFilterMethod			
Type: Group Type:	 ● network ○ exec ○ credential-dow ● group ○ local 	nload		
	Available Server Groups	1	Assigned Server Groups	
Groups In This Method	-	< >	ISE_Group	*
	*			*

Configuration SSID

1. Créer le SSID invité

- Accédez à Configuration > Wireless > WLANs et cliquez sur New
- Saisissez I'ID WLAN, le SSID et le nom du profil, puis cliquez sur Apply.
- Une fois dans les paramètres SSID sous Interface / Interface Group, sélectionnez l'interface de couche 3 du VLAN invité.

WLAN > Edit	QOS	AVC	Policy Mapping	Advanced		
Profile Name	Guest					
Туре	WLAN					
SSID	Guest					
Status	Enabled	1				
Security Policies	[WPA2][Au (Modific	th(802.1x) ations done) e under security tab wil	l appear after ap	olving the change	s.)
Radio Policy	All		Interface/I	nterface Grou	un Dialog	~)
Interface/Interface Group(5) default	1		internace oron	ip bialog	
Broadcast SSID			Interface/Inter	face Group(G)	default	F
Multicast VLAN Feature					default VLAN0010 VLAN0011 VLAN0050 VLAN0301	Î

- Sous **Security** > **Layer 2**, sélectionnez **None** et, à côté de **Mac Filtering**, entrez le nom de la liste de méthodes de filtre Mac que vous avez précédemment configurée (MacFilterMethod).
- Sous Security > AAA Server Tab, sélectionnez les listes appropriées de méthodes d'authentification et de comptabilité (ISE_Method).

WLAN WLAN > Edit General	Security	QOS	AVC		
Layer2	Layer3	AAA Ser	ver		
Layer 2 Secu MAC Filtering	nity None 💌	lethoc			
WLAN > Edit General	Securi	ty J	QOS	AVC	Policy Mapping
Layer2	Layer	3	VA Serve	a.	
Authentic Accountir Local EAP	ation Metho ng Method Authenticat	d	ISE_M	ethod J	0

• Sous l'onglet **Avancé**, activez **Autoriser le remplacement AAA** et l'**état NAC.** Les autres paramètres doivent être ajustés en fonction de chaque configuration requise pour le déploiement (délai d'expiration de la session, exclusion du client, prise en charge des

extensions Aironet).

WLAN WLAN > Edit				
General	Security	QOS	AVC	Policy Mapping Advanced
Allow AAA Ov	rentide			DHCP
Session Time	out (secs)	28800		DHCP Server IP Address 0.0.0.0
Aironet IE				DHCP Address Assignment required
Diagnostic Ch	nannel			DHCP Option 82
P2P Blocking	Action	Disabled	*	DHCP Option 82 Format None 💌
Media Stream	Multicast-direc	t 🗆		DHCP Option 82 Ascii Mode
Client Exclusi	on			DHCP Option 82 Rid Mode
Timeout Valu	e(secs) 60)		NAC
Max Allowed	Client 0			NAC State 🗹

• Accédez à l'onglet Général et définissez le statut sur Activé. Appuyez ensuite sur Apply.

Configuration d'une liste de contrôle d'accès de redirection

Cette liste de contrôle d'accès est référencée par ISE plus loin dans la commande access-accept en réponse à la demande MAB initiale. Le NGWC l'utilise pour déterminer le trafic à rediriger et le trafic à autoriser.

- Accédez à configuration > security > ACL > Access Control Lists et cliquez sur Add New.
- Sélectionnez Étendu et saisissez le nom de la liste de contrôle d'accès.
- Cette image présente un exemple typique de liste de contrôle d'accès de redirection :

ACC	ess Contr > ACL deta	rol Lists ail					
Det	ails :						
Name: Guest_Redirect							
Туре	90	IPv4 Extende	ed				
Add	Sequence	Remove					
	Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port
0	10	deny	icmp	any	any	-	
0	20	deny	udp	any	any	-	eq 67
0	30	deny	udp	any	any		eq 68
0	40	deny	udp	any	any		eq 53
0	50	deny	tcp	any	.157.210	×	eq 8443
0	60	deny	tcp	any	.157.21	-	eq 8443
0	70	permit	tcp	any	any		eq 80
0	80	permit	tcp	any	any		eq 443

Remarque : la ligne 10 est facultative. Cette valeur est généralement ajoutée pour les

propositions de dépannage. Cette liste de contrôle d'accès doit autoriser l'accès aux services DHCP et DNS, ainsi qu'au port TCP 8443 des serveurs ISE (refuser les entrées ACE). Le trafic HTTP et HTTPS est redirigé (Autoriser les ACE).

Configuration de l'interface de ligne de commande (CLI)

Toutes les configurations décrites dans les étapes précédentes peuvent également être appliquées via l'interface de ligne de commande.

802.1x activé globalement

```
dot1x system-auth-control
```

Configuration AAA globale

```
aaa new-model
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
1
aaa server radius dynamic-author
client 172.16.157.210 server-key *****
client 172.16.157.21 server-key *****
auth-type any
!
radius server ISE1
address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
timeout 5
retransmit 2
key *****
1
radius server ISE2
address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
timeout 5
retransmit 2
key ****
!
1
aaa group server radius ISE_Group
server name ISE2
server name ISE1
deadtime 10
mac-delimiter colon
!
```

Configuration d'un réseau local sans fil (WLAN)

```
wlan Guest 1 Guest
aaa-override
accounting-list ISE_Method
client vlan VLAN0301
mac-filtering MacFilterMethod
nac
```

```
no security wpa
no security wpa akm dotlx
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dotlx authentication-list ISE_Method
no security ft over-the-ds
session-timeout 28800
no shutdown
```

Exemple de redirection ACL

3850#show ip access-lists Guest_Redirect Extended IP access list Guest_Redirect 10 deny icmp any any 20 deny udp any any eq bootps 30 deny udp any any eq bootpc 40 deny udp any any eq domain 50 deny tcp any host 172.16.157.210 eq 8443 60 deny tcp any host 172.16.157.21 eq 8443 70 permit tcp any any eq www 80 permit tcp any any eq 443

Support HTTP et HTTPS

3850#show run | inc http ip http server ip http secure-server

Remarque : si vous appliquez une liste de contrôle d'accès pour restreindre l'accès au WLC sur HTTP, cela affecte la redirection.

Configuration d'ISE

Cette section décrit la configuration requise sur ISE pour prendre en charge tous les cas d'utilisation abordés dans ce document.

Tâches de configuration ISE courantes

- 1. Connectez-vous à ISE et accédez à Administration > Network Resources > Network Devices et cliquez sur Add
- 2. Entrez le nom associé au WLC et l'adresse IP du périphérique.
- 3. Cochez la case **RADIUS authentication settings** et tapez le **secret partagé** configuré du côté du WLC. Cliquez ensuite sur **Envoyer**.

Network Devices List > Cisco_5508
Network Devices
* Name Cisco_5508
Description LAB_AireOS_WLC
* IP Address:
* Device Profile de Ciero - G
Device Prome
Model Name
Software Version
* Network Device Group
Device Type All Device Types 📀 Set. To Default
Location All Locations Set. To Default
RADIUS Authentication Settings
- reside resident desirgs
Enable Authentication Settings
Protocol RADIUS
* Shared Secret Show

4. Accédez à Policy > Authentication et sous MAB cliquez sur Edit et assurez-vous que sous Use : Internal Endpoints l'option If user is not found est définie sur Continue (II doit y en avoir par défaut).

Authentication Policy

Define the Authentication Policy by selecting the protocols the For Policy Export go to Administration > System > Backup & P Policy Type O Simple • Rule-Based	at ISE should use to communicate with the network devices, and the identity sources that it should use for au Restore > Policy Export Page
MAB : If Wi	red_MAB OR Wireless_MAB 💠 Allow Protocols : Default Network Access 📀 and a
🛛 🕶 Default : Use	Internal Endpoints
	Identity Source Internal Endpoints
Vireless_802.1XAllow Protocols : Default Network Acce	It is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

Exemple d'utilisation 1 : CWA avec authentification des invités dans chaque connexion utilisateur

Présentation du flux

1. L'utilisateur sans fil se connecte au SSID invité.

- 2. WLC authentifie le point d'extrémité en fonction de son adresse MAC sur ISE en tant que serveur AAA.
- 3. ISE renvoie et accepte l'accès avec deux paires de valeurs d'attribut (AVP) : url-redirect et url-redirect-acl. Une fois que le WLC applique ces AVP à la session de point d'extrémité, la station passe à DHCP-Required et une fois qu'elle saisit une adresse IP, elle reste dans CENTRAL_WEB_AUTH. À cette étape, le WLC est prêt à commencer à rediriger le trafic http / https du client.
- 4. L'utilisateur final ouvre le navigateur Web et une fois que le trafic HTTP ou HTTPS est généré, le WLC redirige l'utilisateur vers le portail invité ISE.
- 5. Une fois que l'utilisateur accède au portail invité, il vous invite à saisir les informations d'identification de l'invité (créé par le sponsor dans ce cas).
- 6. Lors de la validation des informations d'identification, ISE affiche la page AUP et une fois que le client accepte, une nouvelle authentification de type CoA dynamique est envoyée au WLC.
- 7. Le WLC retraite l'authentification de filtrage MAC sans émettre de désauthentification à la station mobile. Cela doit être transparent pour le terminal.
- 8. Une fois que l'événement de réauthentification se produit, ISE réévalue les stratégies d'autorisation et cette fois, le point d'extrémité reçoit un accès d'autorisation car il y a eu un événement d'authentification d'invité réussi précédemment.

Ce processus se répète chaque fois que l'utilisateur se connecte au SSID.

Configuration

- 1. Accédez à ISE et à Work Centers > Guest Access > Configure > Guest Portals > Select Sponsored Guest Portal (ou créez un nouveau type de portail Sponsored-Guest).
- 2. Sous Guest Device Registration settings, décochez toutes les options et cliquez sur Save.

 Guest Device Registration Settings 					
	Automatically register guest devices				
	A message displays to guests when they reach the maximum number of supported devices.				
	Allow guests to register devices				
	You can set the maximum number of supported devices in the guest type settings.				
Det	vice information will be stored in the endpoint identity group specified in the guest type				

3. Accédez à **Politique > Eléments de politique > Résultats > Autorisation > Profils d'autorisation**. Cliquez sur **Add**.

4. Ce profil est poussé vers le bas vers le WLC, le **Redirect-URL** et le **Redirect-URL-ACL** en réponse à la demande initiale de contournement d'authentification Mac (MAB).

 Une fois la redirection Web (CWA, MDM, NSP, CPP) cochée, sélectionnez Centralized Web Auth, puis Tapez le nom de la liste de contrôle d'accès de redirection sous le champ ACL et sous Value, sélectionnez le Sponsored Guest Portal (default) (ou tout autre portail spécifique créé dans les étapes précédentes).

Le profil doit être similaire à celui de cette image. Cliquez ensuite sur Enregistrer.

Authorization Profiles > CWA_Redirect

Authorization Profile	
* Name	CWA_Redirect
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	att Cisco 👻 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
✓ Common Tasks ✓ Web Redirection (C)	A MDM NSP (CPP) (2)
Centralized Web Au	ACL Guest_Redirect Value onsored Guest Portal (default)
Display Certifica	tes Renewal Message
Static IP/Host n	me/FQDN

Les détails d'attribut au bas de la page indiquent les paires de valeurs d'attribut (AVP) lorsqu'elles sont envoyées au WLC



5. Accédez à **Stratégie > Autorisation** et insérez une nouvelle règle. Cette règle est celle qui déclenche le processus de redirection en réponse à la demande d'authentification MAC initiale du WLC. (Dans ce cas appelé **Wireless_Guest_Redirect**).

6. Sous **Conditions**, choisissez **Sélectionner une condition existante dans la bibliothèque**, puis sous **nom de condition**, sélectionnez **Condition composée**. Sélectionnez une condition composée prédéfinie appelée **Wireless_MAB**.

Remarque : cette condition se compose de 2 attributs Radius attendus dans la demande d'accès provenant du WLC (NAS-Port-Type= IEEE 802.11 <présent dans toutes les demandes sans fil> et Service-Type = Contrôle d'appel< qui fait référence à une demande spécifique pour un contournement d'authentification MAC>)

7. Sous Results, sélectionnez **Standard > CWA_Redirect** (profil d'autorisation créé à l'étape précédente). Cliquez ensuite sur **Done** et **Save**

Wireless_Guest_Redirect if Wireless_MAB

then CWA_Redirect

8. Accédez à la fin de la règle **CWA_Redirect** et cliquez sur la flèche en regard de **Modifier**. Sélectionnez ensuite **dupliquer ci-dessus**.

9. Modifiez le nom, car il s'agit de la stratégie à laquelle le point d'extrémité correspond une fois que la session est réauthentifiée lors de la CoA d'ISE (dans ce cas, Wireless_Guest_Access).

10. En regard de la condition composée **Wireless_MAB**, cliquez sur le symbole + pour développer les conditions et, à la fin de la condition **Wireless_MAB**, cliquez sur **Add Attribute/Value**.

Wireless_MAB	
₩ Vireless_Guest_Access if Any ♣ and Wireless_M	AB C then PermitAccess
Add All Conditions Below to Library	en CWA_Redirect
Condition Name Description	en PermitAccess
Wireless_MAB 📀 Normalised Radius:RadiusFlowType EQUALS WirelessMAB	ŵ
	Add Attribute/Value
Save Kesel	Add Condition from Library
	Delete

11. Sous « Select Attribute », choisissez Network Access > UseCase Equals Guest flow

Add Air Conditions Below	to cibrary	
Condition Name	Description	AND +
Wireless_MAB 📀	Normalised Radius:RadiusFlowType EQUALS WirelessMAB	AND
٥	Network Access:U 📀 Equals 💌 Guest Flow	0

12. Sous Autorisations, sélectionnez AutoriserAccès. Cliquez ensuite sur Done et Save

I Ally Q and Wileless_MAD AND Network Acce Q uloit Permin	A 22020
	cess op

Les deux politiques doivent ressembler à ceci :

	Wireless_Guest_Access	if	(Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow)	then	PermitAccess
 Image: A set of the set of the	Wireless_Guest_Redirect	if	Wireless_MAB	then	CWA_Redirect

Exemple d'utilisation 2 : CWA avec Device Registration appliquant l'authentification des invités une fois par jour.

Présentation du flux

- 1. L'utilisateur sans fil se connecte au SSID invité.
- 2. WLC authentifie le point d'extrémité en fonction de son adresse MAC sur ISE en tant que serveur AAA.
- 3. ISE renvoie et access-accept avec deux paires de valeurs d'attribut (AVP) (url-redirect et urlredirect-acl).
- 4. Une fois que le WLC applique ces AVP à la session de point d'extrémité, la station passe à DHCP-Required et une fois qu'elle saisit une adresse IP, elle reste dans CENTRAL_WEB_AUTH. À cette étape, le WLC est prêt à commencer à rediriger le trafic http / https du client.
- 5. L'utilisateur final ouvre le navigateur Web et une fois que le trafic HTTP ou HTTPS est

généré, le WLC redirige l'utilisateur vers le portail invité ISE.

- 6. Une fois que l'utilisateur accède au portail invité, il est invité à saisir les informations d'identification créées par le sponsor.
- 7. Lors de la validation des informations d'identification, ISE ajoute ce terminal à un groupe d'identité de terminal spécifique (préconfiguré) (enregistrement du périphérique).
- 8. La page AUP s'affiche et une fois que le client accepte, un type de CoA dynamique est authentifié à nouveau. Est envoyé au WLC.
- 9. Le WLC doit retraiter l'authentification de filtrage MAC sans émettre de déconnexion à la station mobile. Cela doit être transparent pour le terminal.
- Une fois l'événement de réauthentification survenu, ISE réévalue les stratégies d'autorisation. Cette fois-ci, puisque le terminal est membre du groupe d'identités de terminal droit, ISE renvoie un accès accepté sans restrictions.
- 11. Comme le point de terminaison a été enregistré à l'étape 6, chaque fois que l'utilisateur revient, il est autorisé à accéder au réseau jusqu'à ce qu'il soit supprimé manuellement d'ISE ou qu'une stratégie de purge des points de terminaison exécute le vidage des points de terminaison répondant aux critères.

Dans ce scénario de travaux pratiques, l'authentification est appliquée une fois par jour. Le déclencheur de ré-authentification est la stratégie de purge des points de terminaison qui supprime tous les points de terminaison du groupe d'identités de point de terminaison utilisé chaque jour.

Remarque : il est possible d'appliquer l'événement d'authentification d'invité en fonction du temps écoulé depuis la dernière acceptation AUP. Cela peut être une option si vous devez appliquer l'ouverture de session invité plus souvent qu'une fois par jour (par exemple toutes les 4 heures).

Configuration

- 1. Dans ISE, accédez à Work Centers > Guest Access > Configure > Guest Portals > Select Sponsored Guest Portal (ou créez un nouveau type de portail Sponsored-Guest).
- 2. Sous Guest Device Registration settings, vérifiez que l'option Automatically register guest devices est cochée. Click Save.



Accédez à Work contor > Guast Access > Configure > Quast Turses ou clie

3. Accédez à **Work center > Guest Access > Configure > Guest Types** ou cliquez simplement sur le raccourci spécifié sous Guest Device Registration Settings dans le portail.



4. Lorsque l'utilisateur sponsor crée un compte invité, il lui attribue un type d'invité. Chaque type d'invité individuel peut avoir un point de terminaison enregistré qui appartient à un groupe d'identité de point de terminaison différent.Pour attribuer le groupe d'identité de point de terminaison auquel le périphérique doit être ajouté, sélectionnez le type d'invité que le sponsor utilise pour ces utilisateurs invités (ce cas d'utilisation est basé sur Hebdomadaire (par défaut)).

5. Une fois dans le type d'invité, sous **Options de connexion**, sélectionnez le groupe de terminaux dans le menu déroulant **Groupe d'identités de terminaux pour l'enregistrement du périphérique invité**

Maximum devices guests can register: 5 (1-	199)			
Endpoint identity group for guest device registration	GuestEndpoints	¥	ï)

6. Accédez à **Politique > Eléments de politique > Résultats > Autorisation > Profils d'autorisation**. Cliquez sur **Add**.

7. Ce profil est poussé vers le bas vers le WLC, le **Redirect-URL** et le **Redirect-URL-ACL** en réponse à la demande initiale de contournement d'authentification Mac (MAB).

 Une fois la redirection Web (CWA, MDM, NSP, CPP) cochée, sélectionnez Centralized Web Auth, puis saisissez le nom de la liste de contrôle d'accès de redirection dans le champ ACL et sous Value sélectionnez le portail créé pour ce flux (CWA_DeviceRegistration).

Authorization Profiles > New Authorization Profile					
Authorization Profile					
* Name	CWA_DeviceRegistration				
Description					
* Access Type	ACCESS_ACCEPT T				
Network Device Profile	the Cisco 💌 🕀				
Service Template					
Track Movement					
Passive Identity Tracking					
✓ Common Tasks					
VLAN					
Voice Domain Permiss	sion				
Web Redirection (CV	VA, MDM, NSP, CPP) ()				
Centralized Web Aut	h ACL Guest_Redirect Value CWA_DeviceRegistration				

8. Accédez à **Stratégie > Autorisation** et insérez une nouvelle règle. Cette règle est celle qui déclenche le processus de redirection en réponse à la demande d'authentification MAC initiale du WLC. (Dans ce cas appelé **Wireless_Guest_Redirect**).

9. Sous **Conditions**, sélectionnez **Sélectionner une condition existante dans la bibliothèque**, puis sous **nom de condition**, sélectionnez **Condition composée**. Sélectionnez une condition composée prédéfinie appelée **Wireless_MAB**.

10. Sous Results, sélectionnez **Standard > CWA_DeviceRegistration** (profil d'autorisation créé à l'étape précédente). Cliquez ensuite sur **Done** et **Save**



11. Dupliquez la stratégie ci-dessus, modifiez son nom car il s'agit de la stratégie que le point d'extrémité atteint après son retour de l'événement de réauthentification (appelé Wireless_Guest_Access).

12. Dans la zone **Détails du groupe d'identités**, sélectionnez **Groupe d'identités de point de terminaison** et sélectionnez le groupe auquel vous avez fait référence sous Type d'invité (GuestEndpoints).

13. Sous Results, sélectionnez PermitAccess. Cliquez sur Done et Save the changes.

	Wireless_Guest_Access	if	GuestEndpoints AND Wireless_MAB	then	PermitAccess
~	Wireless_Guest_Redirect	if	Wireless_MAB	then	CWA_DeviceRegistration

14. Créez une stratégie de purge de point de terminaison qui efface quotidiennement le groupe GuestEndpoint.

- Accédez à Administration > Gestion des identités > Paramètres > Purge du point d'extrémité
- Dans les règles **Purge**, il doit y en avoir une par défaut qui déclenche la suppression de GuestEndpoints si le temps écoulé est supérieur à 30 jours.
- Modifiez la stratégie existante pour GuestEndpoints ou créez-en une nouvelle (si la stratégie par défaut a été supprimée). Notez que les stratégies de purge s'exécutent tous les jours à une heure définie.

Dans ce cas, la condition est Membres de GuestEndpoints avec des jours écoulés inférieurs à 1 jour

Exemple d'utilisation 3 : portail HostSpot

Présentation du flux

- 1. L'utilisateur sans fil se connecte au SSID invité.
- 2. WLC authentifie le terminal en fonction de son adresse MAC en utilisant ISE comme serveur AAA.
- 3. ISE renvoie une valeur access-accept avec deux paires de valeurs d'attribut (AVP) : urlredirect et url-redirect-acl.
- 4. Une fois que le WLC applique ces AVP à la session de point d'extrémité, la station passe à DHCP-Required et une fois qu'elle saisit une adresse IP, elle reste dans CENTRAL_WEB_AUTH. À cette étape, le WLC est prêt à rediriger le trafic http / https du client.
- 5. L'utilisateur final ouvre le navigateur Web et une fois que le trafic HTTP ou HTTPS est généré, le WLC redirige l'utilisateur vers le portail ISE HotSpot.
- 6. Une fois dans le portail, l'utilisateur est invité à accepter une politique d'utilisation acceptable.
- 7. ISE ajoute l'adresse MAC du point de terminaison (ID du point de terminaison) dans le groupe d'identités du point de terminaison configuré.
- 8. Le noeud de services de stratégie (PSN) qui traite la demande émet une **réinitialisation Admin-Reset de** type CoA dynamique vers le WLC.
- 9. Une fois que le WLC a fini de traiter la CoA entrante, il émet une déconnexion au client (la connexion est perdue pendant le temps nécessaire au client pour revenir).
- 10. Une fois que le client se reconnecte, une nouvelle session est créée de sorte qu'il n'y ait pas de continuité de session côté ISE. Cela signifie que l'authentification est traitée comme un nouveau thread.
- 11. Étant donné que le point de terminaison est ajouté au groupe d'identités de point de terminaison configuré et qu'il existe une stratégie d'autorisation qui vérifie si le point de terminaison fait partie de ce groupe, la nouvelle authentification correspond à cette stratégie. Le résultat est un accès complet au réseau Invité.
- 12. L'utilisateur ne doit pas accepter à nouveau l'AUP à moins que l'objet d'identité de point de terminaison ne soit purgé de la base de données ISE à la suite d'une stratégie de purge de point de terminaison.

Configuration

- Créez un nouveau groupe d'identités de point de terminaison vers lequel déplacer ces périphériques lors de l'enregistrement. Accédez à Work Centers > Guest Access > Identity Groups > Endpoint Identity Groups et cliquez sur
- Entrez un nom de groupe (dans ce cas, HotSpot_Endpoints). Ajoutez une description et

aucun groupe parent n'est nécessaire.

Endpoint Identity Group List > HotSpot_Endpoints					
Endpoint Identity Group					
* Name	HotSpot_Endpoints				
Description	Members of this group will accept AUP every week				
Parent Group					

2. Accédez à Work Centers > Guest Access > Configure > Guest Portals > sélectionnez Hotspot Portal (par défaut).

3. Développez Portal Settings et, sous Endpoint Identity Group, sélectionnez le groupe **HostSpot_Endpoints** sous **Endpoint Identity Group.** Les périphériques enregistrés sont alors envoyés au groupe spécifié.

Endpoint	HotSpot_Endpoints					
identity	Configure endpoint identity groups at: Work Centers > Guest Access > Identity Groups					
group: *						

4. Enregistrez les modifications.

5. Créez le profil d'autorisation qui appelle le portail de point d'accès à chaud lors de l'authentification MAB émise par le WLC.

- Accédez à Policy > Policy elements > Results > authorization > Authorization Profiles et créez-en un (HotSpotRedirect).
- Une fois que la redirection Web (CWA, MDM, NSP, CPP) est cochée, sélectionnez Hot Spot, puis tapez le nom de la liste de contrôle d'accès Redirect dans le champ ACL (Guest_Redirect) et comme valeur sélectionnez le portail correct (Hotspot Portal (par défaut))).

Add New Standard Profi	le
Authorization Profile	
* Name	HotSpotRedirect
Description	
* Access Type	ACCESS_ACCEPT *
Network Device Profile	tta Cisco 💌 🕀
▼ Common Tasks	
Voice Domain Permission	
Web Redirection (CWA, Hot Spot	MDM, NSP, CPP) () ACL Guest_Redirect Value Hotspot Guest Portal (default) *
Static IP/Host name	e/FQDN
▼ Attributes Details	
Access Type = ACCESS_ACC cisco-av-pair = url-redirect-ac cisco-av-pair = url-redirect=h	EPT J=Guest_Redirect ittps://p:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw

6. Créez la stratégie d'autorisation qui déclenche le résultat HotSpotRedirect lors de la demande MAB initiale du WLC.

- Accédez à Policy > Authorization et insérez une nouvelle règle. Cette règle est celle qui déclenche le processus de redirection en réponse à la demande d'authentification MAC initiale du WLC. (Dans ce cas appelé Wireless_HotSpot_Redirect).
- Sous Conditions, choisissez Sélectionner une condition existante dans la bibliothèque, puis sous nom de condition, sélectionnez Condition composée
- Sous Results, sélectionnez **Standard > HotSpotRedirect** (profil d'autorisation créé à l'étape précédente). Cliquez ensuite sur **Done** et **Save**
- 7. Créez la deuxième stratégie d'autorisation.
 - Dupliquez la stratégie ci-dessus, modifiez son nom car il s'agit de la stratégie que le point de terminaison atteint après son retour de l'événement de réauthentification (appelé Wireless_HotSpot_Access).
 - Dans la zone Détails du groupe d'identités, sélectionnez Groupe d'identités de point de terminaison, puis le groupe que vous avez créé précédemment (HotSpot_Endpoints).
 - Sous Résultats, sélectionnez AutoriserAccès. Cliquez sur Done et Save the changes.

 Wireless_HotSpot_Access
 if
 HotSpot_Endpoints AND Wireless_MAB
 then
 PermitAccess

 Wireless_HotSpot_Redirect
 if
 Wireless_MAB
 then
 HotSpotRedirect

8. Configurez la stratégie de purge qui efface les terminaux avec un temps écoulé supérieur à 5 jours.

- Accédez à Administration > Identity Management > Settings > Endpoint Purge et sous les règles de purge créez-en une nouvelle.
- Dans la zone Identity Group Details, sélectionnez Endpoint Identity Group > HotSpot_Endpoints
- Sous conditions, cliquez sur Créer une condition (option avancée) .

 Sous Sélectionner un attribut, choisissez ENDPOINTPURGE : ElapsedDays SUPERIEUR À 5 jours

```
🖉 🖉 👘 HotSpot_Endpoints_PurgeRule
```

HotSpot_Endpoints AND ENDPOINTPURGE:ElapsedDays GREATERTHAN 5

Vérifier

Cas d'utilisation 1

- 1. L'utilisateur se connecte au SSID invité.
- 2. Il ouvre le navigateur et dès que le trafic HTTP est généré, le portail invité s'affiche.
- 3. Une fois que l'utilisateur invité s'est authentifié et a accepté le protocole AUP, une page de réussite s'affiche.
- 4. Une CoA de réauthentification est envoyée (transparente pour le client).
- 5. La session de point d'extrémité est réauthentifiée avec un accès complet au réseau.
- 6. Toute connexion d'invité suivante doit passer l'authentification d'invité avant d'accéder au réseau.

cisco	Sponsored Gues	st Portal		
Sign On Welcome t	to the Guest Portal. Sign or	n with the username and	password provided to you.	
		Username:		
			Sign On Don't have an account?	

CISCO Sponsored Guest Portal

Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's Ξ account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

CISCO Sponsored Guest Portal

Success

You now have Internet access through this network.

Flux à partir des journaux ISE RADIUS Live :

1	Q	t001	68:7F:74:72:18:2E	Windows7-Wo	Default >> MAB	Default >> Wir	PermitAccess	Å	Accounting Start
	0	t001	68:7F:74:72:18:2E	Windows7-Wo	Default >> MAB	Default >> Wir	PermitAccess	Å	Re-Authentication Event
	0		68:7F:74:72:18:2E					Å	CoA Event
~	0	1001	68:7F:74:72:18:2E					Ņ	Guest Authenitcation Event
>	0	68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo	Default >> MA	Default >> Wir	CWA_Redirect	$\langle $	Initial MAB request

Cas d'utilisation 2

- 1. L'utilisateur se connecte au SSID invité.
- 2. Il ouvre le navigateur et dès que le trafic HTTP est généré, le portail invité s'affiche.
- 3. Une fois que l'utilisateur invité s'est authentifié et a accepté le protocole AUP, le périphérique

est enregistré.

- 4. Une page de réussite s'affiche et une CoA de réauthentification est envoyée (transparente pour le client).
- 5. La session de point d'extrémité est réauthentifiée avec un accès complet au réseau.
- 6. Toute connexion d'invité suivante est autorisée sans authentification d'invité tant que le point de terminaison est toujours dans le groupe d'identité de point de terminaison configuré.

CISCO Sponsored Guest Po	ortal
Sian On	
Welcome to the Guest Portal. Sign on with	the username and password provided to you.
	Username: Password:
	Sign On Don't have an account?

CISCO Sponsored Guest Portal

Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

Ξ

CISCO Sponsored Guest Portal

Welcome Message

Click **Continue** to connect to the network. You're very close to gaining network access.

Continue

cisco	Sponsored Guest Portal
Succes	S You now have Internet access through this network.

Flux à partir des journaux ISE RADIUS Live :

Reset Repeat Cou	nts				🔻 Filter 🗸 🔹 🗸		
Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group		
0	à	68:7F:74:72:1	68:7F:74:72:	PermitAccess		\bigvee	Accounting Start
	à	68:7F:74:72:1	68:7F:74:72:	PermitAccess	GuestEndpoints	\langle	Subsequent MAB request(no redirect to guest portal)
	ò	hfr592	68:7F:74:72:	PermitAccess	User Identity Groups:GuestType_Contractor (default)	$\langle $	Re-Authentication Event
	à		68:7F:74:72:			$\langle $	CoA Reauth Event
	Q	hfr592	68:7F:74:72:		GuestType_Contractor (default)	\bigtriangledown	Guest Authentication and Device Registration
	a	68:7F:74:72:1	68:7F:74:72:	CWA_DeviceRegistration	Profiled		Initial MAB request

Cas d'utilisation 3

- 1. L'utilisateur se connecte au SSID invité.
- 2. Il ouvre le navigateur et dès que le trafic HTTP est généré, une page AUP s'affiche.
- 3. Une fois que l'utilisateur invité a accepté le protocole AUP, le périphérique est enregistré.
- 4. Une page de réussite s'affiche et une CoA de réinitialisation d'administration est envoyée (transparente pour le client).
- 5. Le terminal se reconnecte avec un accès complet au réseau.
- 6. Toute connexion d'invité suivante est autorisée sans application de l'acceptation AUP (sauf configuration contraire) tant que le point de terminaison reste dans le groupe d'identités de point de terminaison configuré.

Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.



Hotspot Portal Connection Successful You have successfully connected to the network.

Commutation locale FlexConnect dans AireOS

Lorsque la commutation locale FlexConnect est configurée, l'administrateur réseau doit s'assurer que :

- La liste de contrôle d'accès Redirect est configurée comme ACL FlexConnect.
- La liste de contrôle d'accès de redirection a été appliquée en tant que stratégie via le point d'accès lui-même sous l'onglet FlexConnect > External WebAuthentication ACLs > Policies > Select Redirect ACL and click Apply

All APs > D	All APs > Details for aaa-ap-3							
General	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced		
VLAN Su	pport 🗸							
Native VL	AN ID 3	01 VI.	AN Mappings					
FlexConn Name	ect Group Not	Configured						
PreAuthent	ication Access Co	ontrol Lists						
External V	VebAuthentication A	ACLS						
Local Split	t ACLs							
Central Di	ICP Processing							
Layer2 ACLs								
Policies								
Policy A	CL CWA Re	direct 🔻						
	Add							
Policy Ac	cess Contro	Lists						
CWA_Redirect								

Vous pouvez également ajouter la liste de contrôle d'accès de stratégie au groupe FlexConnect auquel appartient (**Wireless > FlexConnect Groups >** Select the correct group **> ACL Mapping > Policies** Sélectionnez l'ACL de redirection et cliquez sur Add)

FlexConne	ct Groups > Edit	t 'test'			
General	Local Authentica	tion Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping
AAA VLA	AN-ACL mapping	WLAN-ACL mapping	Policies		
Policies Policy A Policy A	ACL CWA_Redirect	•			
TOR_Red	lirect				

L'ajout d'une liste de contrôle d'accès de stratégie déclenche le WLC pour pousser la liste de contrôle d'accès configurée vers les membres AP du groupe FlexConnect. Si vous ne le faites pas, un problème de redirection Web se produira.

Scénario D'Ancrage À L'Étranger

Dans les scénarios d'ancrage automatique (Foreign-Anchor), il est important de souligner ces faits :

- La liste de contrôle d'accès de redirection doit être définie sur le WLC étranger et le WLC d'ancrage. Même lorsqu'elle n'est appliquée qu'à l'ancre.
- L'authentification de couche 2 est toujours gérée par le WLC étranger. Ceci est essentiel pendant les phases de conception (également pour le dépannage) car tout le trafic d'authentification et de comptabilité RADIUS se produit entre ISE et le WLC étranger.
- Une fois que les AVP de redirection sont appliqués à la session client, le WLC étranger met à jour la session client dans l'ancre par le biais d'un message de transfert de mobilité.
- Àce stade, le WLC d'ancrage commence à appliquer la redirection à l'aide de la liste de contrôle d'accès de redirection qui a été préconfigurée.
- La gestion des comptes doit être complètement désactivée sur le SSID du WLC d'ancrage pour éviter les mises à jour de gestion des comptes vers ISE (référençant le même événement d'authentification) provenant à la fois de l'ancrage et de l'étranger.
- Les listes de contrôle d'accès basées sur URL ne sont pas prises en charge dans les scénarios Foreign-Anchor.

Dépannage

États cassés courants sur AireOS et le WLC d'accès convergé

1. Le client ne peut pas joindre le SSID invité

Un « **show client detailed xx:xx:xx:xx:xx:xx** » indique que le client est bloqué dans **START**. Généralement, il s'agit d'un indicateur du WLC incapable d'appliquer un attribut que le serveur AAA retourne.

Vérifiez que le nom de la liste de contrôle d'accès redirigée par ISE correspond exactement au nom de la liste de contrôle d'accès prédéfinie sur le WLC.

Le même principe s'applique à tout autre attribut que vous avez configuré ISE pour pousser vers le bas vers le WLC (ID de VLAN, noms d'interface, ACL Airespace). Le client doit ensuite passer à DHCP, puis à CENTRAL_WEB_AUTH.

2. Les AVP de redirection sont appliqués à la session du client, mais la redirection ne fonctionne pas

Vérifiez que l'état du gestionnaire de stratégies du client est CENTRAL_WEB_AUTH avec une adresse IP valide alignée sur l'interface dynamique configurée pour le SSID et que les attributs Redirect ACL et URL-Redirect sont appliqués à la session du client.

Redirection ACL

Dans les WLC AlreOS, la liste de contrôle d'accès de redirection doit explicitement autoriser le trafic qui ne doit pas être redirigé, comme DNS et ISE sur le port TCP 8443 dans les deux directions et le deny ip any implicite déclenche le reste du trafic à rediriger.

Dans l'accès convergent, la logique est l'inverse. Refuser les ACE contourne la redirection tandis que autoriser les ACE déclenche la redirection. C'est pourquoi il est recommandé d'autoriser explicitement les ports TCP 80 et 443.

Vérifiez l'accès à ISE sur le port 8443 à partir du VLAN invité. Si tout semble correct du point de vue de la configuration, le moyen le plus simple d'avancer est de capturer une capture derrière l'adaptateur sans fil du client et de vérifier où la redirection se casse.

- La résolution DNS a-t-elle lieu ?
- La connexion TCP en trois étapes est-elle terminée par rapport à la page demandée ?
- Le WLC renvoie-t-il une action de redirection après que le client a initié GET ?
- La connexion TCP en trois étapes avec ISE sur 8443 est-elle terminée ?

3. Le client ne parvient pas à accéder au réseau après qu'ISE a poussé une modification de VLAN à la fin du flux invité

Une fois que le client a saisi une adresse IP au début du flux (état Pré-redirection), si une modification de VLAN est poussée vers le bas après l'authentification de l'invité (après la réauthentification CoA), la seule façon de forcer une libération / un renouvellement DHCP dans le flux de l'invité (sans agent de posture) est par le biais d'une applet java qui, dans les périphériques mobiles, ne fonctionne pas.

Cela laisse le client bloqué dans le VLAN X avec une adresse IP du VLAN Y. Ceci doit être pris en compte lors de la planification de la solution.

4. ISE affiche le message « HTTP 500 Internal error, Radius session not found » dans le navigateur du client invité lors de la redirection

Il s'agit généralement d'un indicateur de perte de session sur ISE (la session a été interrompue). La raison la plus courante est la comptabilisation configurée sur le WLC d'ancrage lorsque Foreign-Anchor a été déployé. Pour résoudre ce problème, désactivez la comptabilité sur l'ancre et laissez le handle étranger Authentification et comptabilité.

5. Le client se déconnecte et reste déconnecté ou se connecte à un autre SSID après avoir accepté AUP dans le portail HotSpot d'ISE.

Ceci peut être attendu dans HotSpot en raison du changement dynamique d'autorisation (CoA) impliqué dans ce flux (CoA Admin Reset) qui amène le WLC à émettre une erreur d'authentification à la station sans fil. La plupart des terminaux sans fil ne rencontrent aucun problème pour revenir au SSID après la désauthentification, mais dans certains cas, le client se connecte à un autre SSID préféré en réponse à l'événement de désauthentification. Rien ne peut être fait à partir d'ISE ou du WLC pour empêcher cela, car c'est au client sans fil de s'en tenir au SSID d'origine, ou de se connecter à un autre SSID disponible (préféré).

Dans ce cas, l'utilisateur sans fil doit se reconnecter manuellement au SSID du point d'accès.

WLC AireOS

Le client de débogage définit pour DEBUG un ensemble de composants impliqués dans les modifications de Client State Machine.

(Cisco Controller) >show debug MAC Addr 1..... AA:AA:AA:AA:AA:AA:AA Debug Flags Enabled: dhcp packet enabled. dot11 mobile enabled. dot11 state enabled dot1x events enabled. dot1x states enabled. dot1x states enabled. mobility client handoff enabled. pem events enabled. pem state enabled. 802.11r event debug enabled. 802.11w event debug enabled. CCKM client debug enabled.

Déboguer les composants AAA

(Cisco Controller) >debug aaa {events, detail and packets} enable

Cela peut avoir un impact sur les ressources selon le nombre d'utilisateurs qui se connectent via MAB ou Dot1X SSID. Ces composants de niveau DEBUG enregistrent les transactions AAA entre WLC et ISE et impriment les paquets RADIUS à l'écran.

Ceci est essentiel si vous pensez qu'ISE ne peut pas fournir les attributs attendus, ou si le WLC ne les traite pas correctement.

Redirection Web-Auth

(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa

Cela peut être utilisé pour vérifier que le WLC déclenche correctement la redirection. Voici un exemple de la façon dont la redirection doit ressembler à partir des débogages :

*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a050000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*type://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a050000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430

*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is HTTP/1.1 200 OK Location: https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44

NGWC

Le client de débogage définit pour DEBUG un ensemble de composants impliqués dans les modifications de Client State Machine.

3850#debug client mac-address <client MAC>

Ce composant imprime les paquets RADIUS (Authentication and Accounting) à l'écran. Cela est pratique lorsque vous devez vérifier que ISE fournit les bons AVP et que la CoA est envoyée et traitée correctement.

3850#debug radius

Toutes les transitions AAA (authentification, autorisation et comptabilité) sont effectuées lorsque des clients sans fil sont impliqués. Ceci est essentiel pour vérifier que le WLC analyse correctement les AVP et les applique à la session client.

^{3850#debug} aaa wireless all Cela peut être activé lorsque vous suspectez un problème de redirection sur le NGWC.

```
3850#debug epm plugin redirect all
3850#debug ip http transactions
3850#debug ip http url
```

ISE

Journaux RADIUS Live

Vérifiez que la demande MAB initiale a été traitée correctement dans ISE et que cette dernière repousse les attributs attendus. Accédez à **Operations > RADIUS > Live logs** et filtrez la sortie en utilisant l'adresse MAC du client sous **Endpoint ID**. Une fois l'événement d'authentification trouvé, cliquez sur les détails, puis vérifiez les résultats envoyés dans le cadre de l'acceptation.



Result	
UserName	68:7F:74:72:18:2E
User-Name	68-7F-74-72-18-2E
State	ReauthSession:0e249a0500000682577ee2a2
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120
cisco-av-pair	url-redirect-acl=TOR_Redirect
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal /gateway?sessionld=0e249a0500000682577ee2a2&portal=9fc44212-2da2-11e6- a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648533fea

pompe TCPD

Cette fonctionnalité peut être utilisée lorsqu'un examen plus approfondi de l'échange de paquets RADIUS entre ISE et le WLC est nécessaire. De cette façon, vous pouvez prouver qu'ISE envoie les attributs corrects dans access-accept sans avoir besoin d'activer les débogages du côté du WLC. Pour démarrer une capture à l'aide de TCDDump, accédez à **Opérations > Dépannage > Outils de diagnostic > Outils généraux > TCPDump.**

Voici un exemple de flux correct capturé par le biais de TCPDump

Destination	Protocol	Length	Info
157.1 3	RADIUS	299	Access-Request(1) (id=0, 1=257)
.154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
.157.13	RADIUS	340	Accounting-Request(4) (id=8, 1=298)
154.5	RADIUS	62	Accounting-Response(5) (id=8, 1=20)
154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
.157.13	RADIUS	80	CoA-ACK(44) (id=1, 1=38)
	RADIUS	299	Access-Request(1) (id=1, 1=257)
.154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)
	Destination	Destination Protocol Interfact 157.13 RADIUS Interfact 154.5 RADIUS Interfact 157.13 RADIUS Interfact 154.5 RADIUS Interfact 154.5 RADIUS Interfact 154.5 RADIUS Interfact 157.13 RADIUS Interfact 157.13 RADIUS Interfact 157.13 RADIUS Interfact 157.13 RADIUS Interfact 154.5 RADIUS	Protocol Length Lingth 157.13 RADIUS 299 Lingth 154.5 RADIUS 443 Lingth 157.13 RADIUS 340 Lingth 157.13 RADIUS 340 Lingth 154.5 RADIUS 62 Lingth 154.5 RADIUS 62 Lingth 154.5 RADIUS 244 Lingth 157.13 RADIUS 80 Lingth 157.13 RADIUS 299 Lingth 154.5 RADIUS 239

Voici les paquets AVP envoyés en réponse à la requête MAB initiale (deuxième paquet dans la capture d'écran ci-dessus).

```
RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0x0 (0)
Length: 401
Authenticator: fleaaffcfaa240270b885a9ba8ccd06d
[This is a response to a request in frame 1]
[Time from request: 0.214509000 seconds]
Attribute Value Pairs
AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
AVP: l=55 t=Class(25): 434143533a306532343961303530303030616130353536...
AVP: l=57 t=Vendor-Specific(26) v=ciscoSystems(9)
VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
VSA: l=189 t=Cisco-AVPair(1): url-
```

Débogages des terminaux :

Si vous avez besoin d'approfondir les processus ISE qui impliquent des décisions de politique, la sélection de portail, l'authentification d'invité, la CoA gérant la façon la plus simple d'aborder ceci est d'activer les **débogages de point d'extrémité** au lieu d'avoir à définir des composants complets au niveau de débogage.

Pour l'activer, accédez à Operations > Troubleshooting > DiagnosticTools > General Tools > EndPoint Debug.

0	verview	
	Event	5200 Authentication succeeded
	Username	00:24:97:BA:84:81
	Endpoint Id	00:24:97:BA:84:81 ⊕ Endpoint Debug
	Endpoint Profile	Cisco-Device
	Authentication Policy	Default >> MAB >> Default
	Authorization Policy	Default >> Wireless_CWA_RedirectSSO
	Authorization Result	GuestSSO_Portal

Une fois dans la page Endpoint debug, entrez l'adresse MAC du point de terminaison et cliquez sur start (démarrer) lorsque vous êtes prêt à recréer le problème.

✓ General Tools	Endpoint Debug
RADIUS Authentication Trouble	
Execute Network Device Com	Ctatue:
Evaluate Configuration Validator	Status. Stopped Start
Posture Troubleshooting	MAC Address () IP 68:7F:74:72:18:2E ()
EndPoint Debug	Automatic disable after
TCP Dump	

Une fois le débogage arrêté, cliquez sur le lien qui identifie l'ID de point de terminaison pour télécharger le résultat du débogage.

Endpoint Debug							
Status:	Processing	Stop					
 MAC Address IP 68:7F:74:72:18:2E ✓ Automatic disable after 10 Minutes () 							
				Selected 0 Total 1			
X Delete Files 👷 Refresh							
File Name	 Host Name 		Modified Date	Size (Bytes)			
68-7f-74-72-18-2e	TORISE21A		Jul 8 12:06	1021448			

Informations connexes

Constructions AireOS recommandées par le TAC

Guide de configuration du contrôleur sans fil Cisco, version 8.0.

Guide de l'administrateur de Cisco Identity Services Engine, version 2.1

Configuration sans fil NGWC universelle avec moteur de services d'identité

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.