

Résoudre les problèmes courants d'accès invité ISE

Table des matières

[Introduction](#)

[Prérequis](#)

[Exigences](#)

[Composants utilisés](#)

[Flux invité](#)

[Guides de déploiement communs](#)

[Problèmes fréquemment rencontrés](#)

[La redirection vers le portail invité ne fonctionne pas](#)

[Échec de l'autorisation dynamique](#)

[Les notifications par SMS/EMAIL ne sont pas envoyées](#)

[La page Gérer les comptes est inaccessible](#)

[Meilleures pratiques du certificat du portail](#)

[Informations connexes](#)

Introduction

Ce document décrit comment dépanner les problèmes d'invité courants dans le déploiement, comment isoler et vérifier le problème, et des solutions de contournement simples à essayer.

Prérequis

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration d'invité ISE
- Configuration CoA sur les périphériques d'accès réseau (NAD)
- Des outils de capture sont requis sur les stations de travail.

Composants utilisés

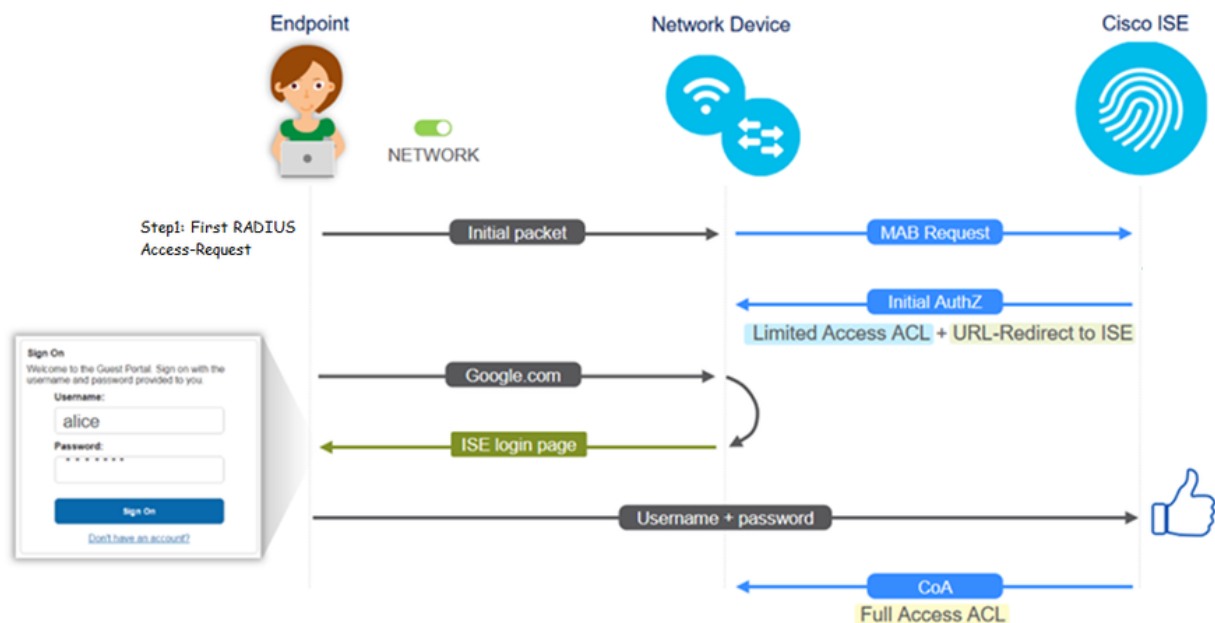
Les informations contenues dans ce document sont basées sur Cisco ISE, version 2.6 et :

- WLC 5500
- Commutateur Catalyst 3850 version 15.x
- station de travail Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Flux invité

La présentation du flux invité est similaire aux configurations filaires ou sans fil. Cette image de l'organigramme peut être utilisée comme référence dans l'ensemble du document. Il aide à visualiser l'étape et l'entité.



Le flux peut également être suivi sur les journaux en direct ISE [Operations > RADIUS Live Logs] en filtrant l'ID de point d'extrémité :

- Authentification MAB réussie - le champ du nom d'utilisateur contient l'adresse MAC- L'URL est envoyée au NAD - L'utilisateur obtient le portail
- Authentification de l'invité réussie : le champ du nom d'utilisateur contient le nom d'utilisateur de l'invité, il a été identifié comme GuestType_Daily (ou le type configuré pour l'utilisateur invité)
- CoA initié - le champ du nom d'utilisateur est vide, le rapport détaillé indique que l'autorisation dynamique a réussi
- Accès invité fourni

Séquence des événements dans l'image (de bas en haut)

May 18, 2020 01:34:18.290 AM	✔	🔍	testquest	84.96.91.26 DD 6D	Windows 10...	Guest Access	Guest Acces...	PermiAccess	10.106.37.18	DefaultNetwork...	TenGigabitEther...	User Identity Groups G	sotumu26
May 18, 2020 01:34:18.269 AM	✔	🔍		84.96.91.26 DD 6D						DefaultNetwork...			sotumu26
May 18, 2020 01:34:14.446 AM	✔	🔍	testquest	84.96.91.26 DD 6D					10.106.37.18			GuestType_Daily (defa	sotumu26
May 18, 2020 01:22:50.904 AM	✔	🔍		84.96.91.26 DD 6D	Intel-Device	Guest Acces...	Guest Acces...	Guest_redirect	10.106.37.18	DefaultNetwork...	TenGigabitEther...	Profiled	sotumu26

Guides de déploiement communs

Voici quelques liens pour obtenir de l'aide sur la configuration. Pour tout cas d'utilisation spécifique

de dépannage, il aide à être conscient de la configuration idéale ou attendue.

- [Configuration d'invité filaire](#)
- [Configuration invité sans fil](#)
- [CWA invité sans fil avec points d'accès FlexAuth](#)

Problèmes fréquemment rencontrés

Le présent document traite principalement des questions suivantes :

La redirection vers le portail invité ne fonctionne pas

Une fois que l'URL de redirection et la liste de contrôle d'accès sont envoyées depuis ISE, vérifiez les points suivants :

1. État du client sur le commutateur (en cas d'accès invité câblé) avec la commande show authentication session int <interface> details :

```
questlab#sh auth sess int T1/0/48 de
      Interface: TenGigabitEthernet1/0/48
      IIF-ID: 0x1096380000001DC
      MAC Address: b496.9126.dd6d
      IPv6 Address: Unknown
      IPv4 Address: 10.106.37.18
      User-Name: B4-96-91-26-DD-6D
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      Session timeout: N/A
      Restart timeout: N/A
      Common Session ID: 0A6A2511000012652C64B014
      Acct Session ID: 0x0000124F
      Handle: 0x5E00014D
      Current Policy: POLICY_Tel/0/48

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy: Should Secure
  Security Status: Link Unsecure

Server Policies:
  URL Redirect: https://10.127.197.212:8443/portal/gateway?sessionId=0A6A2511000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&token=66bbfce930a43142fe26b9d9577971de
  URL Redirect ACL: REDIRECT_ACL

Method status list:
  Method      State
  mab         Authc Success
```

2. État du client sur le contrôleur de réseau local sans fil (si l'accès invité sans fil) : Monitor > Client > MAC address

Security Information	
Security Policy Completed	No
Policy Type	N/A
Auth Key Mgmt	N/A
Encryption Cipher	None
EAP Type	N/A
SNMP NAC State	Access
Radius NAC State	CENTRAL_WEB_AUTH
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	cwa_redirect
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	http://10.10.10.10:8443/portal/gateway?sessionId=0

3. L'accessibilité du point d'extrémité à l'ISE sur le port TCP 8443 à l'aide de l'invite de commandes : C:\Users\user>telnet <ISE-IP> 8443

4. Si l'URL de redirection du portail possède un nom de domaine complet, vérifiez si le client peut résoudre le problème à partir de l'invite de commandes : C:\Users\user>nslookup guest.ise.com

5. Dans la configuration de la connexion flexible, assurez-vous que le même nom de liste de contrôle d'accès est configuré sous ACL et ACL flexibles. Vérifiez également si la liste de contrôle d'accès est mappée aux points d'accès. Reportez-vous au guide de configuration de la section précédente - Étapes 7b et 7c pour plus d'informations.

CISCO **MONITOR** **WLANs** **CONTROLLER** **WIRELESS** **SECURITY**

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
 - Mesh
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs

FlexConnect Access Control Lists

Acl Name

[flexred](#)

6. Effectuez une capture de paquets à partir du client et vérifiez la redirection. Le paquet HTTP/1.1 302 Page Moved indique que le WLC/commutateur a redirigé le site accédé vers le portail invité ISE (URL redirigée) :

ip.addr==2.2.2.2

No.	Arrival Time	Source	Destination	Protocol	Info
190	May 18, 2020 14:29:13.49400500...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
191	May 18, 2020 14:29:13.49657400...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
192	May 18, 2020 14:29:13.49670300...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
194	May 18, 2020 14:29:13.69293900...	2.2.2.2	10.106.37.18	TCP	[TCP Dup ACK 191#1] 80 → 54571 [ACK] Seq=1 Ack=1 Win=4128 Len=0
218	May 18, 2020 14:29:16.34762700...	10.106.37.18	2.2.2.2	HTTP	GET / HTTP/1.1
219	May 18, 2020 14:29:16.35025300...	2.2.2.2	10.106.37.18	HTTP	HTTP/1.1 302 Page Moved
220	May 18, 2020 14:29:16.35047200...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [FIN, PSH, ACK] Seq=279 Ack=329 Win=3800 Len=0
221	May 18, 2020 14:29:16.35050600...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [ACK] Seq=329 Ack=280 Win=63962 Len=0
222	May 18, 2020 14:29:16.35064600...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [FIN, ACK] Seq=329 Ack=280 Win=63962 Len=0
224	May 18, 2020 14:29:16.35466100...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [ACK] Seq=280 Ack=330 Win=3800 Len=0

219 May 18, 2020 14:29:16.3502... 2.2.2.2 10.106.37.18 HTTP HTTP/1.1 302 Page Moved

```

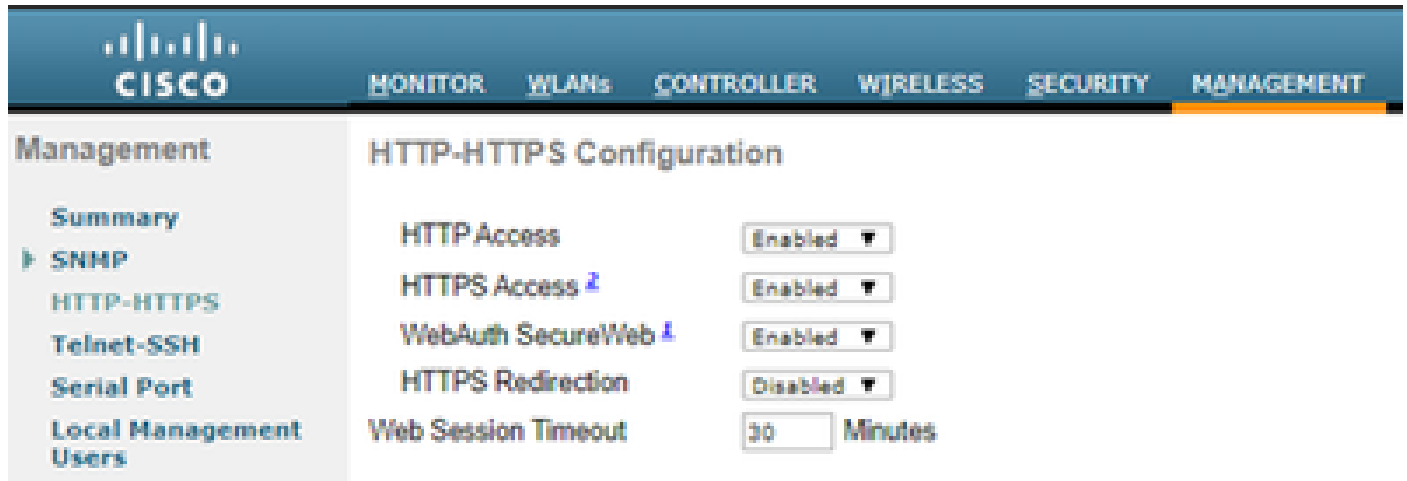
> Frame 219: 332 bytes on wire (2656 bits), 332 bytes captured (2656 bits) on interface 0
> Ethernet II, Src: Cisco_ca:0e:c5 (00:87:31:ca:0e:c5), Dst: IntelCor_26:dd:6d (b4:96:91:26:dd:6d)
> Internet Protocol Version 4, Src: 2.2.2.2, Dst: 10.106.37.18
> Transmission Control Protocol, Src Port: 80, Dst Port: 54571, Seq: 1, Ack: 329, Len: 278
  > Hypertext Transfer Protocol
    > HTTP/1.1 302 Page Moved
      Location: https://10.127.197.212:8443/portal/gateway?sessionId=0A6A2511000012652C648014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&token=66bbfce930a43142fe26b9d9577971de&redirect=http://2.2.2.2/
      Pragma: no-cache
      Cache-Control: no-cache
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.002626000 seconds]
      [Request in frame: 218]
      [Request URI: http://2.2.2.2/]
  
```

7. Le moteur HTTP(s) est activé sur les périphériques d'accès réseau :

Sur le commutateur :

```
guestlab#sh run | in ip http
ip http server
ip http secure-server
```

Sur le WLC :



The screenshot shows the Cisco WLC Management interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The 'MANAGEMENT' tab is selected. On the left, the 'Management' menu is expanded, showing options like 'Summary', 'SNMP', 'HTTP-HTTPS', 'Telnet-SSH', 'Serial Port', 'Local Management', and 'Users'. The main content area is titled 'HTTP-HTTPS Configuration' and displays the following settings:

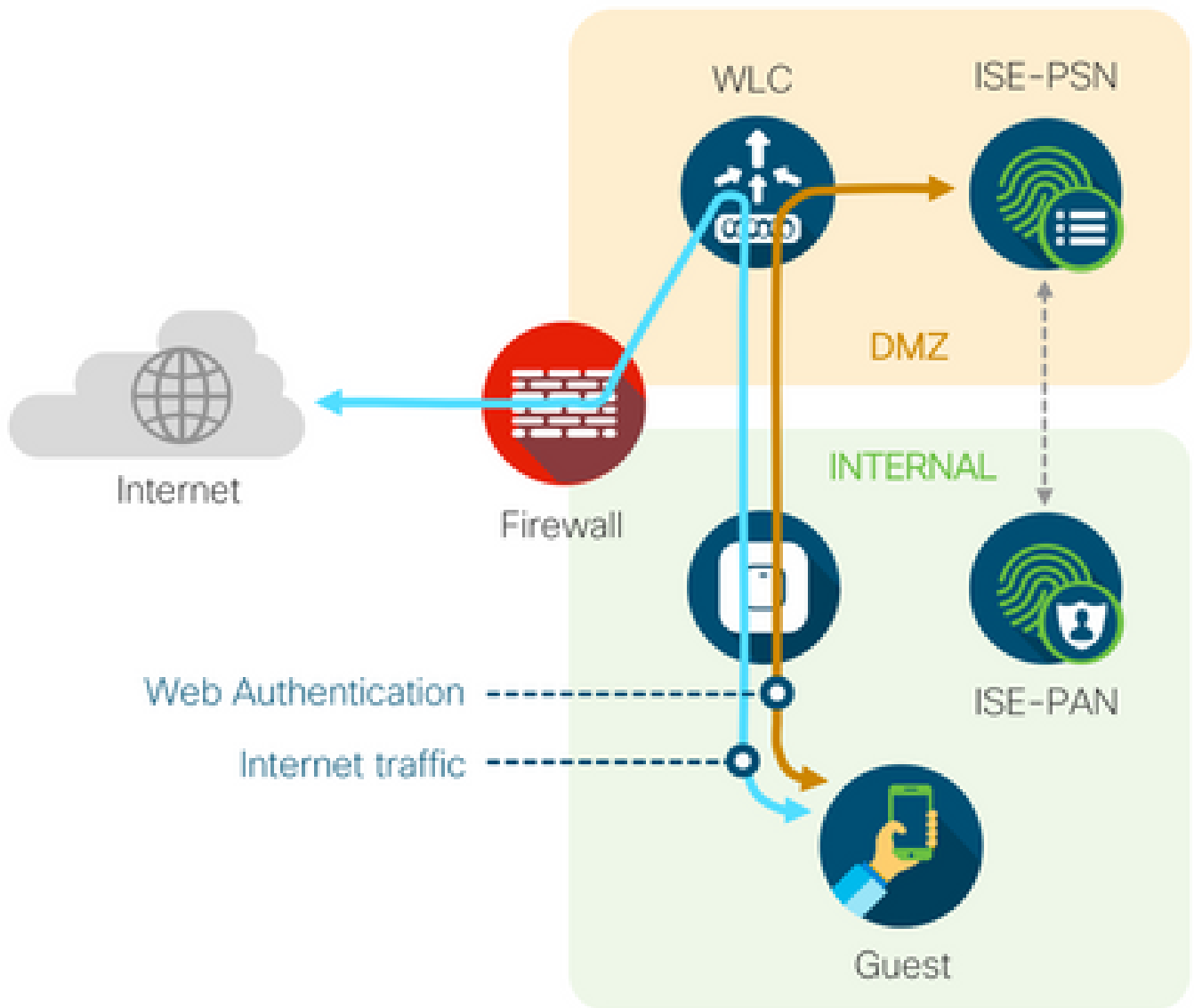
Configuration Item	Value
HTTP Access	Enabled
HTTPS Access	Enabled
WebAuth SecureWeb	Enabled
HTTPS Redirection	Disabled
Web Session Timeout	30 Minutes

8. Si le WLC est dans une configuration d'ancrage étranger, vérifiez les points suivants :

Étape 1. L'état du client doit être le même sur les deux WLC.

Étape 2. L'URL de redirection doit être visible sur les deux WLC.

Étape 3. La gestion des comptes RADIUS doit être désactivée sur le WLC d'ancrage.



Échec de l'autorisation dynamique

Si l'utilisateur final est en mesure d'accéder au portail invité et de se connecter avec succès, l'étape suivante consiste en une modification de l'autorisation, afin d'accorder un accès invité complet à l'utilisateur. Si cela ne fonctionne pas, vous verrez un échec d'autorisation dynamique sur les journaux en direct ISE Radius. Pour résoudre le problème, vérifiez les points suivants :

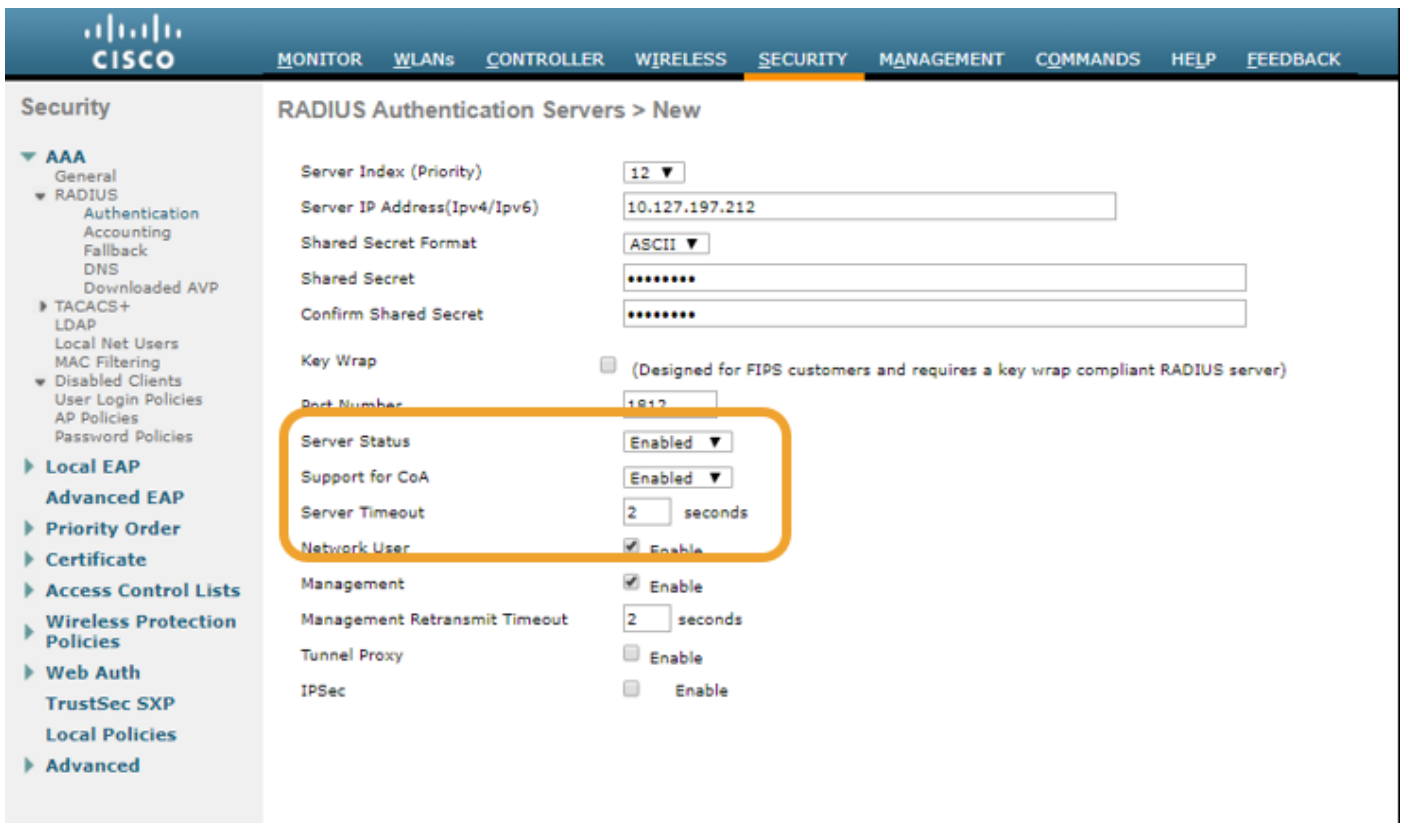
Overview	
Event	5417 Dynamic Authorization failed
Username	
Endpoint Id	MAC ADDRESS
Endpoint Profile	
Authorization Result	

Steps

- 11204 Received reauthenticate request
- 11220 Prepared the reauthenticate request
- 11100 RADIUS-Client about to send request - (port = 1700 , type = Cisco CoA)
- 11104 RADIUS-Client request timeout expired (🚫 Step latency=10003 ms)
- 11213 No response received from Network Access Device after sending a Dynamic Authorization request

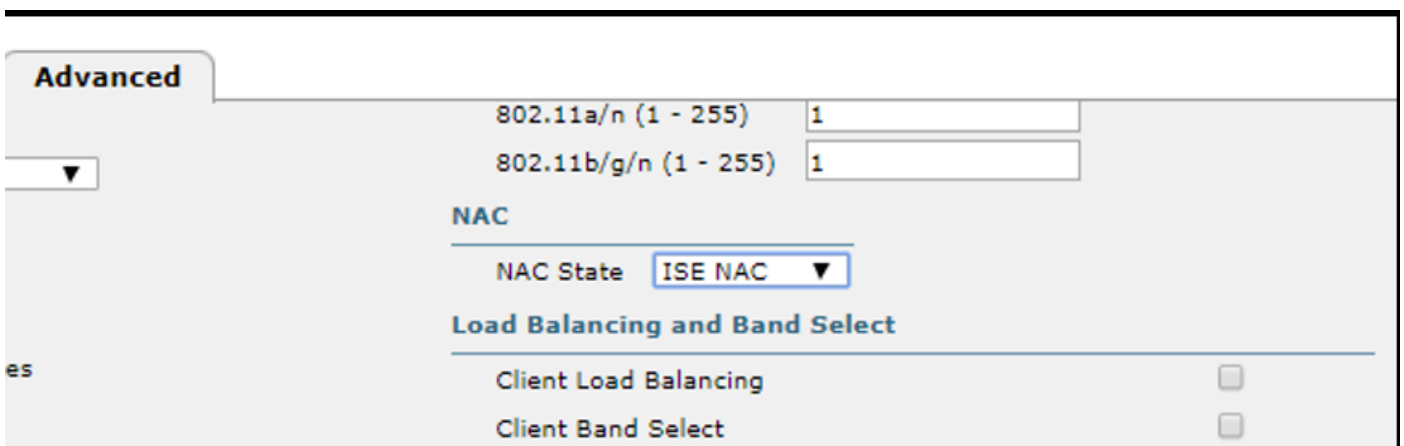
1. La modification de l'autorisation (CoA) doit être activée/configurée sur le NAD :

```
!  
aaa server radius dynamic-author  
  client 10.127.197.209 server-key cisco123  
  client 10.127.197.212 server-key cisco123  
!  
.
```



2. Le port UDP 1700 doit être autorisé sur le pare-feu.

3. L'état NAC sur le WLC est incorrect. Sous Advanced settings on WLC GUI > WLAN changez l'état NAC en ISE NAC.



Les notifications par SMS/EMAIL ne sont pas envoyées

1. Vérifiez la configuration SMTP sous Administration > System > Settings > SMTP.

2. Recherchez dans l'API des passerelles de messagerie/SMS en dehors d'ISE :

Testez la ou les URL fournies par le fournisseur sur un client API ou un navigateur, remplacez les variables telles que les noms d'utilisateur, les mots de passe, le numéro de téléphone portable et testez l'accessibilité. [Administration > Système > Paramètres > Passerelles SMS]

[SMS Gateway Provider List](#) > **Global Default**

SMS Gateway Provider

SMS Gateway Provider Name: * **Global Default**

Select Provider Interface Type:

SMS Email Gateway

SMS HTTP API

URL: * `http://api.clickatell.com/http/sendmsg?user=[USERNAME]&password=[PASSWORD]&api_i`

Data (Url encoded portion):

`$message$`

Use HTTP POST method for data portion

Si vous effectuez un test à partir des groupes de parrainage ISE [Workcenters > Guest Access > Portals and Components > Guest Types], effectuez une capture de paquets sur ISE et la passerelle SMS/SMTP pour vérifier si

1. Le paquet de requête atteint le serveur sans modification.
2. Le serveur ISE dispose des autorisations/privileges recommandés par le fournisseur pour que la passerelle traite cette demande.

Account Expiration Notification

Send account expiration notification days before account expires ⓘ

View messages in:

Email

Send a copy of the notification email to the Sponsor

Use customization from:

Messages:

Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.

Send test email to me at:

Configure SMTP server at: [Work Centers > Guest Access > Administration > SMTP server](#)

SMS

Messages:

Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.

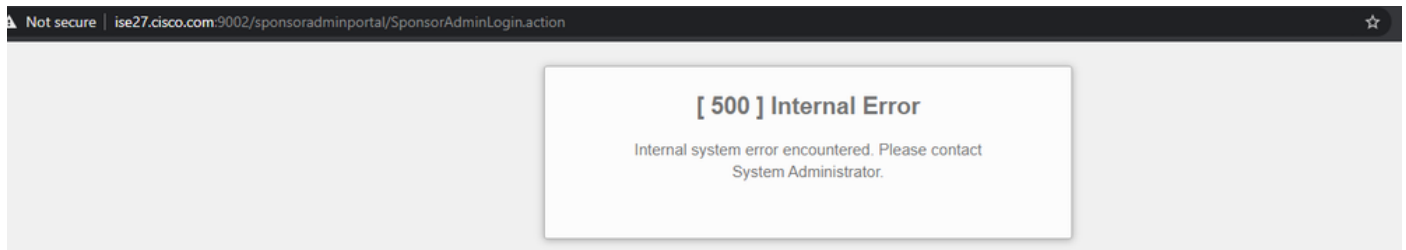
(160 character limit per message)*Over 160 characters requires multiple messages.

Send test SMS to me at:

Configure SMS service provider at: [Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

La page Gérer les comptes est inaccessible

1. Sous le Workcenters > Guest Access > Manage accounts, le bouton redirige vers le FQDN ISE sur le port 9002, pour que l'administrateur ISE accède au portail du sponsor :



2. Vérifiez si le nom de domaine complet (FQDN) est résolu par la station de travail à partir de laquelle Sponsor Portal est accessible à l'aide de la commande nslookup <FQDN of ISE PAN>.

3. Vérifiez si le port TCP 9002 d'ISE est ouvert à partir de l'interface de ligne de commande d'ISE à l'aide de la commande show ports | inclut 9002.

Meilleures pratiques du certificat du portail

- Pour une expérience utilisateur transparente, le certificat utilisé pour les portails et les rôles admin doit être signé par une autorité de certification publique bien connue (par exemple : GoDaddy, DigiCert, VeriSign, etc.), généralement approuvée par les navigateurs (par exemple : Google Chrome, Firefox, etc.).
- Il n'est pas recommandé d'utiliser une adresse IP statique pour la redirection d'invité, car cela rend l'adresse IP privée d'ISE visible par tous les utilisateurs. La plupart des

fournisseurs ne fournissent pas de certificats signés par des tiers pour les adresses IP privées.

- Lorsque vous passez d'ISE 2.4 p6 à p8 ou p9, il y a un bogue connu : l'ID de bogue Cisco [CSCvp75207](#) où les cases Trust pour l'authentification dans ISE et Trust pour l'authentification client et Syslog doivent être vérifiées manuellement après la mise à niveau du correctif. Cela garantit que ISE envoie la chaîne de certification complète pour le flux TLS lors de l'accès au portail invité.

Si ces actions ne résolvent pas les problèmes d'accès invité, veuillez contacter le TAC avec un bundle d'assistance collecté avec les instructions du document : [Debugs to enable on ISE](#).

Informations connexes

- [Assistance technique et téléchargements Cisco](#)

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.