

# Beheben gängiger Probleme mit dem Gastzugriff der ISE

## Inhalt

[Einleitung](#)

[Voraussetzung](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Gastdatenfluss](#)

[Allgemeine Bereitstellungsleitfäden](#)

[Häufig auftretende Probleme](#)

[Umleitung zum Gastportal funktioniert nicht](#)

[Dynamische Autorisierung fehlgeschlagen](#)

[SMS-/E-Mail-Benachrichtigungen werden nicht gesendet](#)

[Seite "Konten verwalten" ist nicht erreichbar](#)

[Best Practices für Portalzertifikate](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie gängige Gastprobleme in der Bereitstellung behoben, wie das Problem isoliert und geprüft wird, und es werden einfache Problemumgehungen für den Versuch beschrieben.

## Voraussetzung

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ISE-Gastkonfiguration
- CoA-Konfiguration auf Netzwerkzugriffsgeräten (Network Access Devices, NAD)
- Auf Workstations müssen Aufnahmegeräte zur Verfügung stehen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco ISE Version 2.6 und:

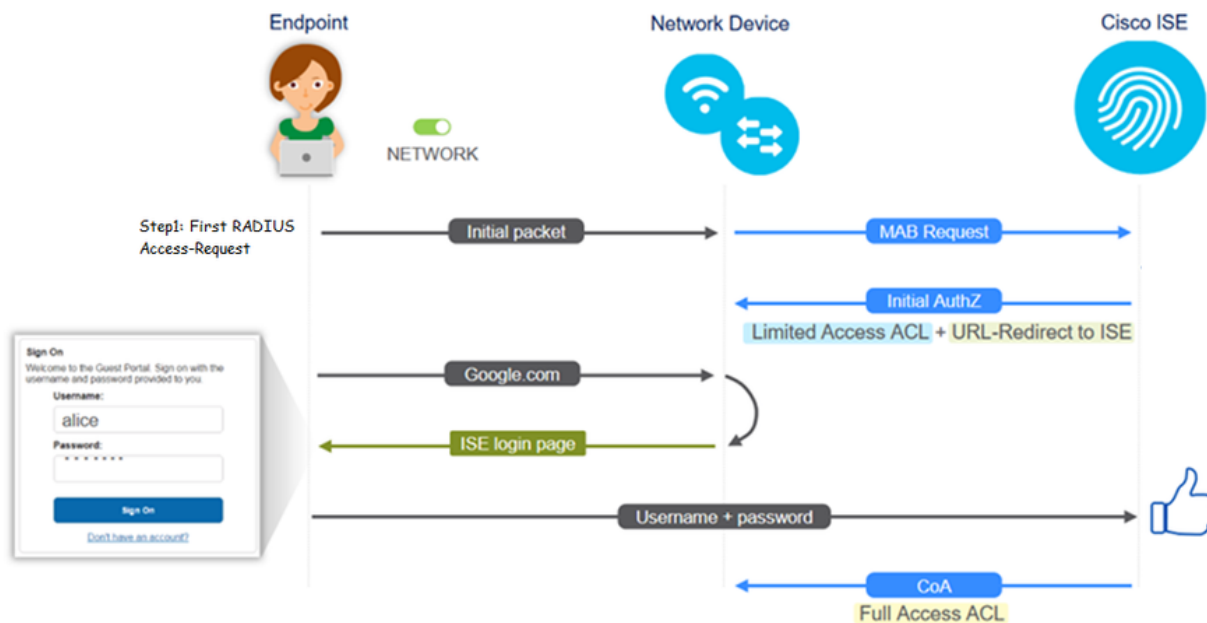
- WLC 5500
- Catalyst Switch 3850 15.x Version
- Windows 10-Workstation

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Gastdatenfluss

Die Übersicht des Gastdatenflusses ähnelt der kabelgebundenen oder Wireless-Einrichtung. Dieses Bild des Flussdiagramms kann im gesamten Dokument verwendet werden. Es hilft, den Schritt und die Entität zu visualisieren.



Der Datenfluss kann auch in ISE-Live-Protokollen [Operations > RADIUS Live Logs] verfolgt werden, indem die Endpunkt-ID gefiltert wird:

- MAB-Authentifizierung erfolgreich - das Feld "username" enthält die MAC-Adresse - URL wird an den NAD weitergeleitet - Benutzer erhält das Portal
- Guest Authentication successfully (Gastauthentifizierung erfolgreich) - Das Feld "username" enthält den Gastbenutzernamen, er wurde als "GuestType\_Daily" (oder als konfigurierter Typ für den Gastbenutzer) identifiziert.
- CoA initiiert - das Feld "Benutzername" ist leer. Der detaillierte Bericht zeigt an, dass die dynamische Autorisierung erfolgreich war.
- Gastzugriff gewährt

Die Reihenfolge der Ereignisse im Bild (von unten nach oben)

May 15, 2020 01:34:18.280 AM	✔	Q	testquest	B4 96 91 26 DD 6D	Windows10...	Guest Access	Guest Acces...	PermAccess	10.106.37.15	DefaultNetwo...	TenGigabitEbe...	User Identity Groups G	sotumu26
May 15, 2020 01:34:18.269 AM	✔	Q		B4 96 91 26 DD 6D						DefaultNetwo...			sotumu26
May 15, 2020 01:34:14.440 AM	✔	Q	testquest	B4 96 91 26 DD 6D					10.106.37.15			GuestType_Daily (defa	sotumu26
May 15, 2020 01:22:50.904 AM	✔	Q		B4 96 91 26 DD 6D	Intel-Device	Guest Acces...	Guest Acces...	Guest_redirect	10.106.37.15	DefaultNetwo...	TenGigabitEbe...	Profiled	sotumu26

## Allgemeine Bereitstellungsleitfäden

Hier finden Sie einige Links zur Konfigurationsunterstützung. Bei der Fehlerbehebung für spezielle Anwendungsfälle ist es hilfreich, die ideale oder erwartete Konfiguration zu kennen.

- [Konfiguration für kabelgebundenen Gast](#)
- [Wireless-Gastkonfiguration](#)
- [Wireless Guest CWA mit FlexAuth APs](#)

# Häufig auftretende Probleme

In diesem Dokument werden in erster Linie folgende Themen behandelt:

## Umleitung zum Gastportal funktioniert nicht

Wenn die Umleitungs-URL und die ACL von der ISE per Push übermittelt wurden, überprüfen Sie Folgendes:

1. Der Client-Status auf dem Switch (bei kabelgebundenem Gastzugriff) mit dem Befehl **show authentication session int <Schnittstelle> 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=0A6
A2511000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbfce930a43142fe26b9d9577971de
  URL Redirect ACL: REDIRECT_ACL

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

2. Der Client-Status auf dem Wireless LAN Controller (bei Wireless-Gastzugriff): **Überwachen > Client > MAC-Adresse**

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. Die Erreichbarkeit vom Endpunkt zur ISE auf dem TCP-Port 8443 mithilfe der Eingabeaufforderung: **C:\Users\user>Telnet <ISE-IP> 8443**

4. Wenn die URL für die Portalumleitung über einen FQDN verfügt, überprüfen Sie, ob der Client über die Eingabeaufforderung aufgelöst werden kann: **C:\Users\user>nslookup guest.ise.com**

5. Stellen Sie bei der Einrichtung der Flex Connect sicher, dass unter ACLs und Flex ACLs derselbe ACL-Name konfiguriert ist. Überprüfen Sie außerdem, ob die ACL den APs zugeordnet ist. Weitere Informationen finden Sie im Konfigurationsleitfaden des vorherigen Abschnitts - Schritte 7 b und c.

The screenshot shows the Cisco Wireless configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The 'WIRELESS' tab is active. On the left, the 'Wireless' menu is expanded to show 'Access Points' (All APs, Radios, Dual-Band Radios, Global Configuration) and 'Advanced' (Mesh, RF Profiles, FlexConnect Groups, FlexConnect ACLs). The main content area is titled 'FlexConnect Access Control Lists' and shows a table with one entry: 'flexred' under the 'Acl Name' column.

6. Nehmen Sie eine Paketerfassung vom Client, und überprüfen Sie, ob die Umleitung erfolgt. Das Paket HTTP/1.1 302 Page Moved dient zum Angeben, dass der WLC/Switch die Website, auf die zugegriffen wurde, zum ISE-Gastportal umgeleitet hat (umgeleitete URL):

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\r\n
    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/\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.002626000 seconds]
    [Request in frame: 218]
    [Request URI: http://2.2.2.2/]
  
```

7. Das HTTP(s)-Modul ist auf den Netzwerkzugriffsgeräten aktiviert:

Auf dem Switch:

```

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

Auf dem WLC:

The screenshot shows the Cisco WLC Management interface. The 'Management' tab is selected, and the 'HTTP-HTTPS Configuration' page is displayed. The configuration is as follows:

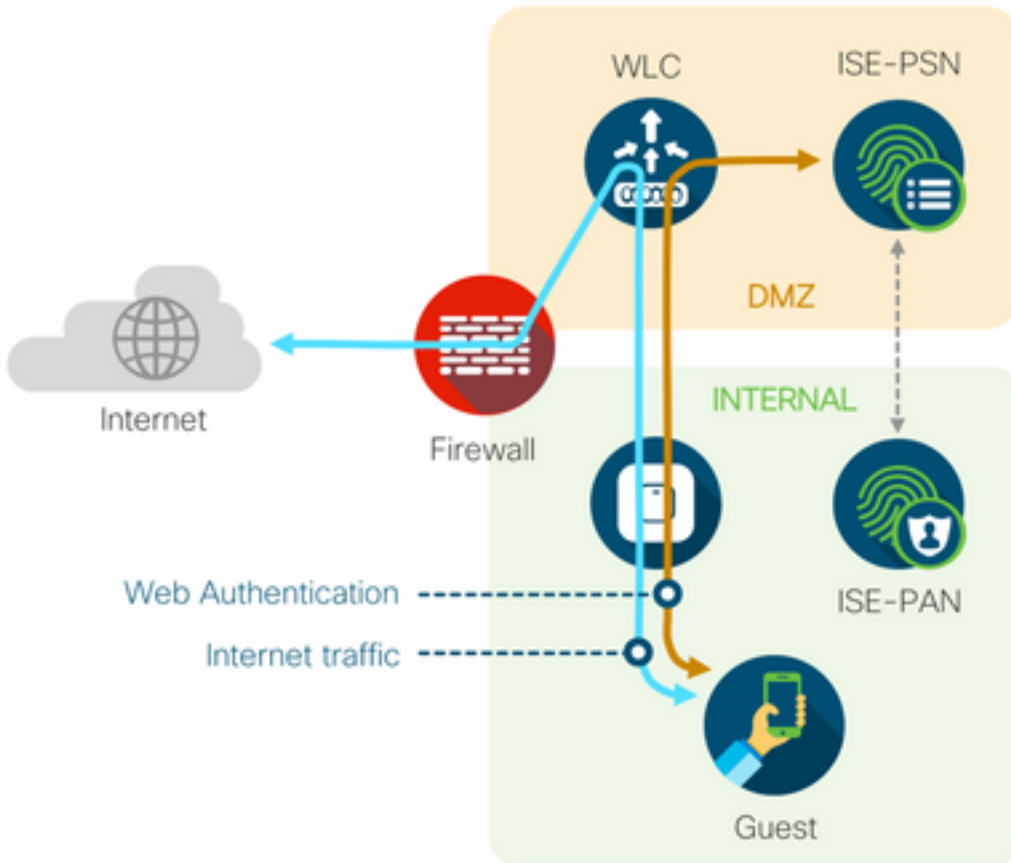
- HTTP Access: Enabled
- HTTPS Access: Enabled
- WebAuth SecureWeb: Enabled
- HTTPS Redirection: Disabled
- Web Session Timeout: 30 Minutes

8. Wenn sich der WLC in einer Fremdaner-Konfiguration befindet, überprüfen Sie Folgendes:

Schritt 1: Der Client-Status muss auf beiden WLCs gleich sein.

Schritt 2: Die Umleitungs-URL muss auf beiden WLCs angezeigt werden.

Schritt 3: RADIUS-Accounting muss auf dem Anker-WLC deaktiviert werden.



## Dynamische Autorisierung fehlgeschlagen

Wenn der Endbenutzer auf das Gastportal zugreifen und sich erfolgreich anmelden kann, ist als nächster Schritt eine Autorisierungsänderung erforderlich, um dem Benutzer den vollständigen Gastzugang zu gewähren. Wenn dies nicht funktioniert, liegt ein Fehler bei der dynamischen Autorisierung der ISE Radius Live-Protokolle vor. Um das Problem zu beheben, überprüfen Sie Folgendes:

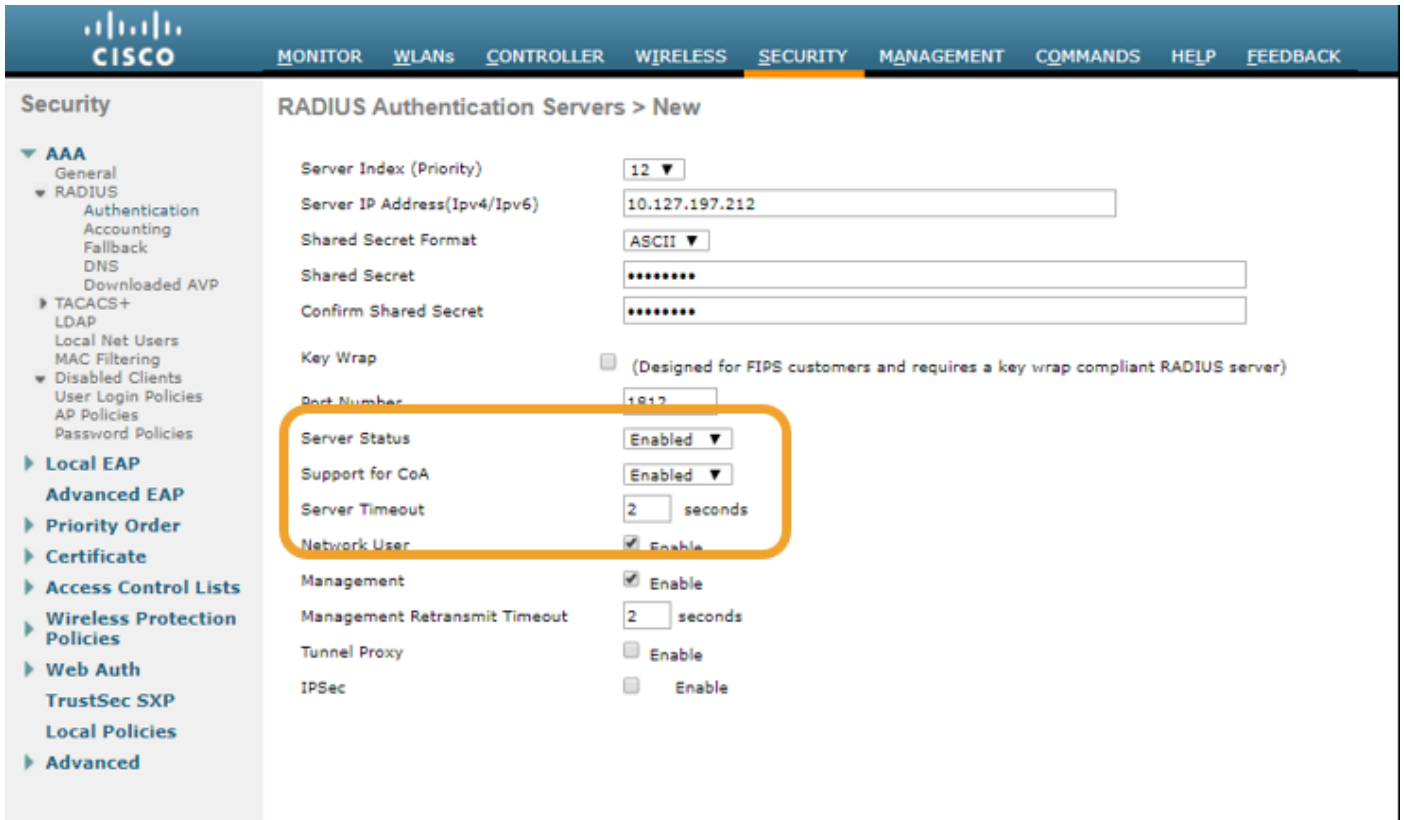
Overview	
Event	5417 Dynamic Authorization failed
Username	
Endpoint Id	MAC ADDRESS
Endpoint Profile	
Authorization Result	

### 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

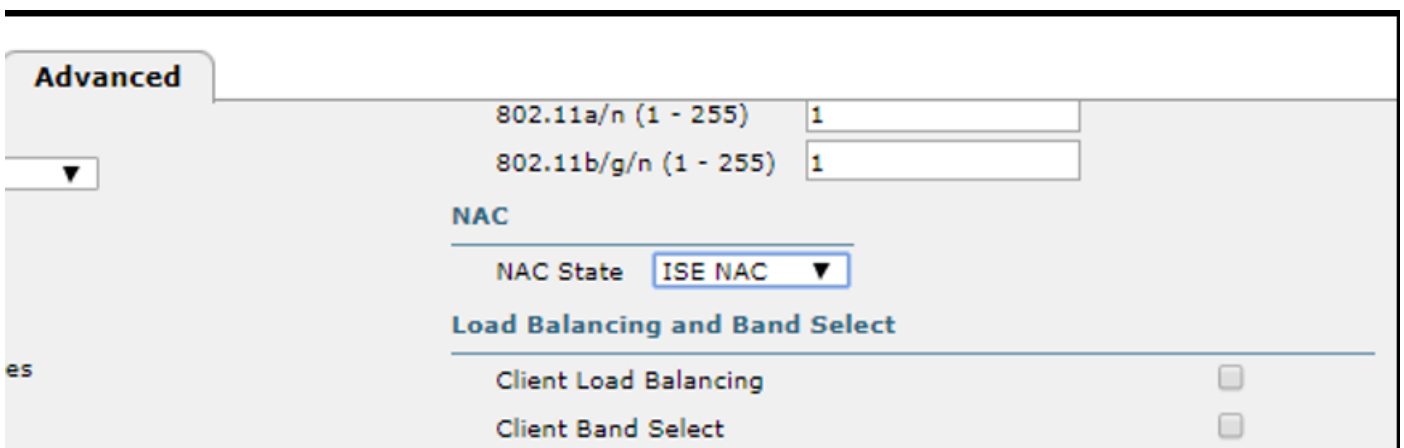
1. Autorisierungsänderung (Change of Authorization, CoA) muss im NAD aktiviert/konfiguriert sein:

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



2. UDP-Port 1700 muss auf der Firewall zugelassen sein.

3. Der NAC-Status auf dem WLC ist falsch. Ändern Sie unter Erweiterte Einstellungen auf der WLC-GUI > WLAN den NAC-Status in ISE NAC.



SMS-/E-Mail-Benachrichtigungen werden nicht gesendet

1. Überprüfen Sie die SMTP-Konfiguration unter **Administration > System > Settings > SMTP**.

2. API für SMS/E-Mail-Gateways außerhalb der ISE prüfen:

Testen Sie die vom Anbieter bereitgestellten URL(s) auf einem API-Client oder einem Browser, ersetzen Sie die Variablen wie Benutzernamen, Kennwörter, Mobiltelefonnummer, und testen Sie die Erreichbarkeit. [**Administration > System > Settings > SMS Gateways**]

[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: \*

Data (Url encoded portion):

Use HTTP POST method for data portion

Alternativ können Sie, wenn Sie von den ISE-Sponsorgruppen [**Workcenters > Guest Access > Portals and Components > Guest Types**] aus testen, eine Paketerfassung auf der ISE und dem SMS/SMTP-Gateway durchführen, um zu überprüfen, ob

1. Das Anforderungspaket erreicht den Server unbehelligt.
2. Der ISE-Server verfügt über die vom Anbieter empfohlenen Berechtigungen/Berechtigungen für das Gateway zur Verarbeitung dieser Anforderung.



## 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:  Copy text from:

Send test email to me at:

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

SMS

Messages:  Copy text from:

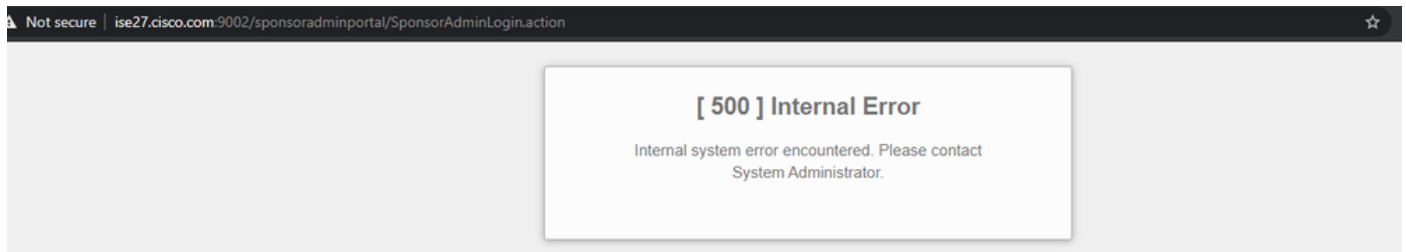
(160 character limit per message)\*Over 160 characters requires multiple messages.

Send test SMS to me at:

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

## Seite "Konten verwalten" ist nicht erreichbar

1. Unter der Schaltfläche **Workcentres > Guest Access > Manage accounts** wird auf den ISE FQDN an Port 9002 umgeleitet, damit der ISE-Administrator auf das Sponsorportal zugreifen kann:



2. Überprüfen Sie mit dem Befehl **nslookup <FQDN von ISE PAN>**, ob der FQDN von der Workstation aufgelöst wird, von der aus auf das Sponsorportal zugegriffen wird.

3. Überprüfen Sie mit dem Befehl **show ports**, ob der ISE TCP-Port 9002 über die CLI der ISE geöffnet ist. | **einschließlich 9002.**

## Best Practices für Portalzertifikate

- Für ein nahtloses Anwendererlebnis muss das für Portale und Admin-Rollen verwendete Zertifikat von einer bekannten öffentlichen Zertifizierungsstelle signiert werden (z. B. GoDaddy, DigiCert, VeriSign usw.), die von Browsern häufig als vertrauenswürdig eingestuft wird (z. B. Google Chrome, Firefox usw.).
- Es wird nicht empfohlen, statische IP-Adressen für die Gastumleitung zu verwenden, da diese die private IP-Adresse der ISE für alle Benutzer sichtbar machen. Die meisten Anbieter stellen keine von Drittanbietern signierten Zertifikate für private IP bereit.

- Wenn Sie von ISE 2.4 p6 zu p8 oder p9 wechseln, gibt es einen bekannten Fehler: Cisco Bug-ID [CSCvp75207](#), wobei die Kästchen **Trust for authentication in ISE** and **Trust for client authentication und Syslog** nach dem Patch-Upgrade manuell aktiviert werden müssen. Dadurch wird sichergestellt, dass die ISE beim Zugriff auf das Gastportal die gesamte Zertifikatkette für den TLS-Fluss sendet.

Wenn durch diese Aktionen keine Probleme mit dem Gastzugriff behoben werden, wenden Sie sich an das TAC. Hierzu wird ein Supportpaket mit den Anweisungen im Dokument "[Debugs to enable on ISE](#)" ([Fehlerbehebungen auf ISE](#)) bereitgestellt.

## Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.