

# Konfigurationsbeispiel für das selbst registrierte Gastportal der ISE-Version 1.3

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Topologie und Fluss](#)

[Konfigurieren](#)

[WLC](#)

[ISE](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Optionale Konfiguration](#)

[Selbstregistrierungseinstellungen](#)

[Gasteinstellungen anmelden](#)

[Gerätregistrierungseinstellungen](#)

[Compliance-Einstellungen für Gastgeräte](#)

[BYOD-Einstellungen](#)

[Vom Sponsor genehmigte Konten](#)

[Bereitstellung von Anmeldeinformationen per SMS](#)

[Gerätregistrierung](#)

[Status](#)

[BYOD](#)

[VLAN-Änderung](#)

[Zugehörige Informationen](#)

## Einführung

Die Cisco Identity Services Engine (ISE) Version 1.3 verfügt über ein neues Gastportal, das Self Registered Guest Portal, das Gastbenutzern die Selbstregistrierung ermöglicht, sobald sie Zugriff auf Netzwerkressourcen erhalten. In diesem Portal können Sie mehrere Funktionen konfigurieren und anpassen. In diesem Dokument wird beschrieben, wie Sie diese Funktion konfigurieren und Fehler beheben.

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, über Erfahrungen mit der ISE-Konfiguration und grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

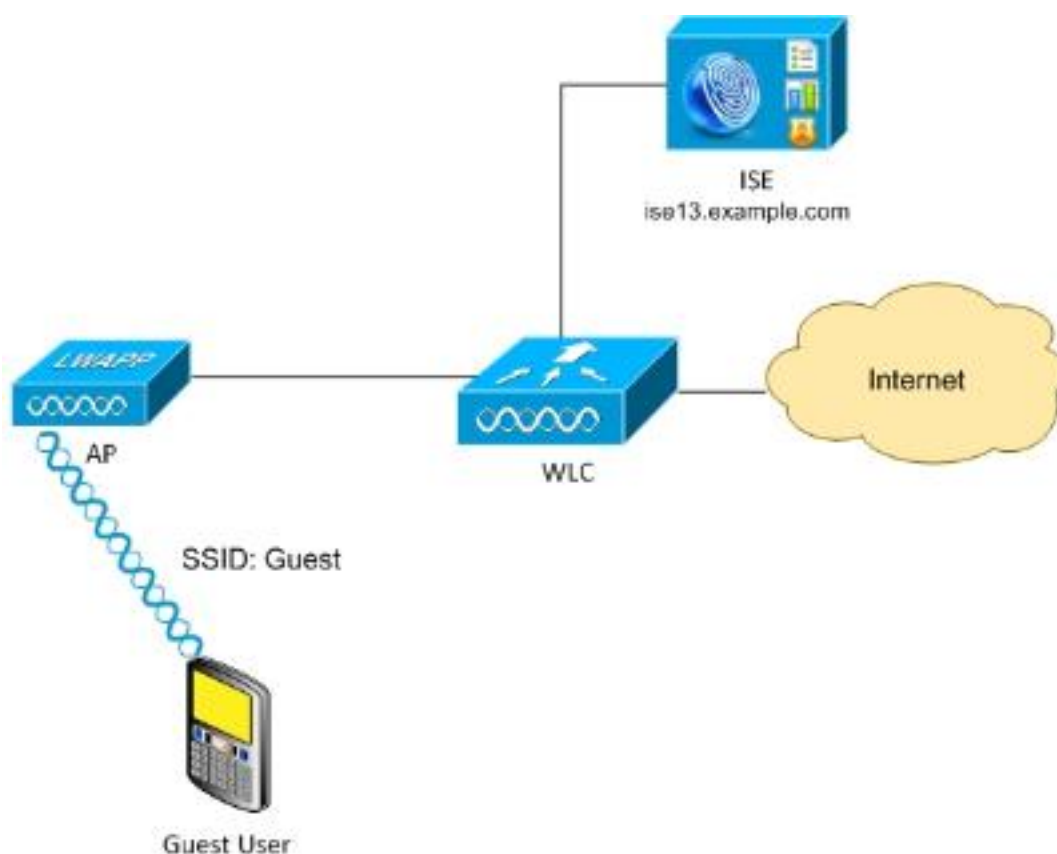
- ISE-Bereitstellungen und Gastdatenströme
- Konfiguration der Wireless LAN Controller (WLC)

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco WLC 7.6 oder höher
- ISE Software, Version 3.1 und höher

## Topologie und Fluss



Dieses Szenario stellt mehrere Optionen für Gastbenutzer dar, wenn sie eine Selbstregistrierung durchführen.

Hier ist der allgemeine Fluss:

**Schritt 1:** Guest User ordnet dem Service Set Identifier (SSID) zu: Gast. Dies ist ein offenes Netzwerk mit MAC-Filterung mit ISE für die Authentifizierung. Diese Authentifizierung stimmt mit der zweiten Autorisierungsregel auf der ISE überein, und das Autorisierungsprofil wird zum selbst registrierten Gastportal umgeleitet. Die ISE gibt einen RADIUS Access-Accept mit zwei cisco-av-

pair-Paaren zurück:

- url-redirect-acl (welcher Datenverkehr umgeleitet werden soll und der lokal auf dem WLC definierte Name der Zugriffskontrollliste (ACL))
- url-redirect (where to redirect the traffic-to-ISE)

**Schritt 2:** Der Gastbenutzer wird an die ISE umgeleitet. Anstatt Anmeldeinformationen anzugeben, klickt der Benutzer auf "Kein Konto". Der Benutzer wird auf eine Seite umgeleitet, auf der das Konto erstellt werden kann. Ein optionaler geheimer Registrierungscode kann aktiviert werden, um die Selbstregistrierungsberechtigung auf Personen zu beschränken, die diesen geheimen Wert kennen. Nachdem das Konto erstellt wurde, erhält der Benutzer Anmeldeinformationen (Benutzername und Kennwort) und meldet sich mit diesen Anmeldeinformationen an.

**Schritt 3:** Die ISE sendet eine RADIUS Change of Authorization (CoA) Reauthentifizierung an den WLC. Der WLC authentifiziert den Benutzer erneut, wenn er die RADIUS Access-Request mit dem Authorize-Only-Attribut sendet. Die ISE reagiert mit Access-Accept- und Air-ACL, die lokal auf dem WLC definiert werden und nur Zugriff auf das Internet bietet (der endgültige Zugriff für Gastbenutzer hängt von der Autorisierungsrichtlinie ab).

Beachten Sie, dass die ISE für EAP-Sitzungen (Extensible Authentication Protocol) einen CoA-Terminat senden muss, um eine erneute Authentifizierung auszulösen, da sich die EAP-Sitzung zwischen der Komponente und der ISE befindet. Für MAB (MAC-Filterung) reicht CoA-Reauthentifizierung jedoch aus. Es ist nicht erforderlich, die Zuweisung/Aufhebung der Authentifizierung für den Wireless-Client aufzuheben.

**Schritt 4:** Der Gastbenutzer hat den gewünschten Zugriff auf das Netzwerk.

Es können mehrere zusätzliche Funktionen wie "Status" und "Bring Your Own Device" (BYOD) aktiviert werden (siehe weiter unten).

## Konfigurieren

### WLC

1. Fügen Sie den neuen RADIUS-Server für Authentifizierung und Abrechnung hinzu. Navigieren Sie zu **Security > AAA > Radius > Authentication**, um RADIUS CoA (RFC 3576) zu aktivieren.

**CISCO**      [MONITOR](#)   [WLANS](#)   [CONTROLLER](#)   [WIRELESS](#)   [SECURITY](#)

**Security**

- ▼ **AAA**
  - General
  - ▼ **RADIUS**
    - Authentication
    - Accounting
    - Fallback
    - DNS
  - ▶ TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- ▶ **Local EAP**
- ▶ **Priority Order**
- ▶ **Certificate**
- ▶ **Access Control Lists**

### RADIUS Authentication Servers > Edit

Server Index	2	
Server Address	10.62.97.21	
Shared Secret Format	ASCII	
Shared Secret	●●●	
Confirm Shared Secret	●●●	
Key Wrap	<input type="checkbox"/>	(Designed for FIPS custome
Port Number	1812	
Server Status	Enabled	
Support for RFC 3576	Enabled	
Server Timeout	5	seconds
Network User	<input checked="" type="checkbox"/>	Enable
Management	<input checked="" type="checkbox"/>	Enable
IPSec	<input type="checkbox"/>	Enable

Es gibt eine ähnliche Konfiguration für die Buchhaltung. Es wird außerdem empfohlen, den WLC so zu konfigurieren, dass die SSID im Attribut "Called Station ID" gesendet wird. Dadurch kann die ISE flexible Regeln basierend auf der SSID konfigurieren:

**Security**

- ▼ **AAA**
  - General
  - ▼ **RADIUS**
    - Authentication**

### RADIUS Authentication Servers

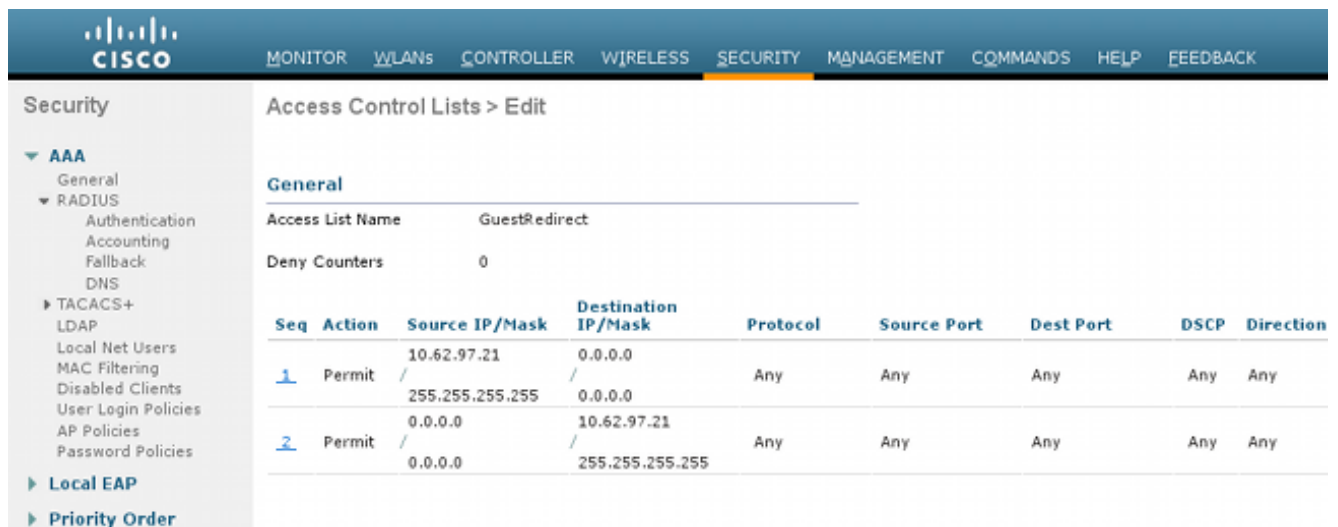
Acct Call Station ID Type <a href="#">?</a>	IP Address
Auth Call Station ID Type	AP MAC Address:SSID

2. Erstellen Sie auf der Registerkarte WLANs (WLANs) den WLAN-Gast, und konfigurieren Sie die richtige Schnittstelle. Setzen Sie die Layer-2-Sicherheit mit MAC-Filterung auf **None**. Wählen Sie unter Security/Authentication, Authorization, and Accounting (AAA) Servers (Sicherheit/Authentifizierung, Autorisierung und Abrechnung) die ISE-IP-Adresse für Authentifizierung und Abrechnung aus. Aktivieren Sie auf der Registerkarte Erweitert die Option **AAA Override**, und legen Sie für Network Admission Control (NAC) State (Status der Netzwerkzugangskontrolle) RADIUS NAC (CoA-Unterstützung) fest.

3. Navigieren Sie zu **Sicherheit > Zugriffskontrolllisten > Zugriffskontrolllisten**, und erstellen Sie zwei Zugriffslisten:

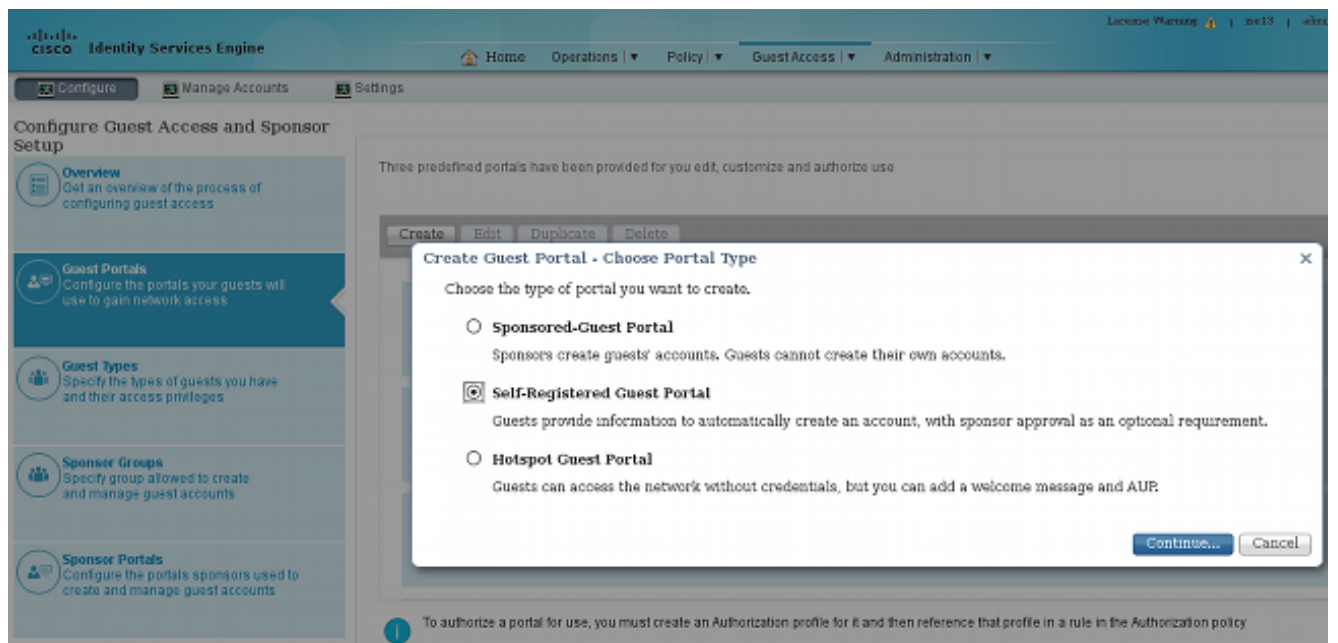
GuestRedirect ermöglicht Datenverkehr, der nicht umgeleitet werden sollte, und leitet den gesamten anderen Datenverkehr um. Internet, das für Unternehmensnetzwerke abgelehnt wird und für alle anderen zugelassen ist

Nachfolgend finden Sie ein Beispiel für eine GuestRedirect-ACL (muss Datenverkehr von/zur ISE von der Umleitung ausschließen):



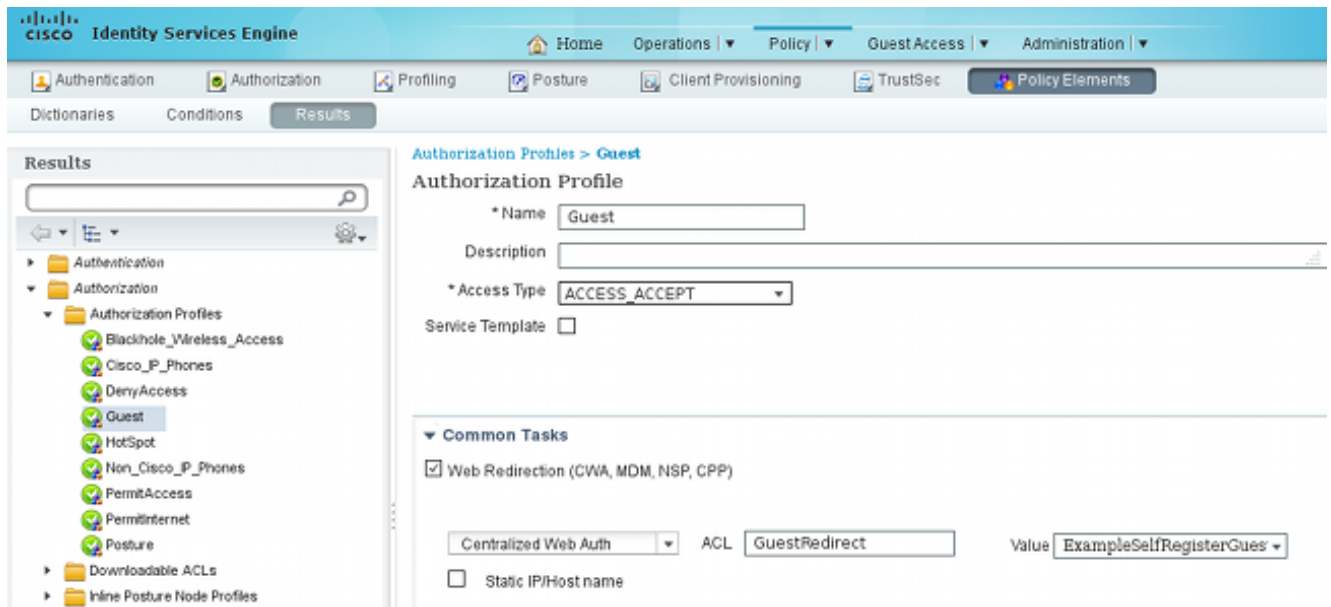
## ISE

1. Navigieren Sie zu **Gastzugriff > Konfigurieren > Gastportale**, und erstellen Sie einen neuen Portaltyp, das selbst registrierte Gastportal:

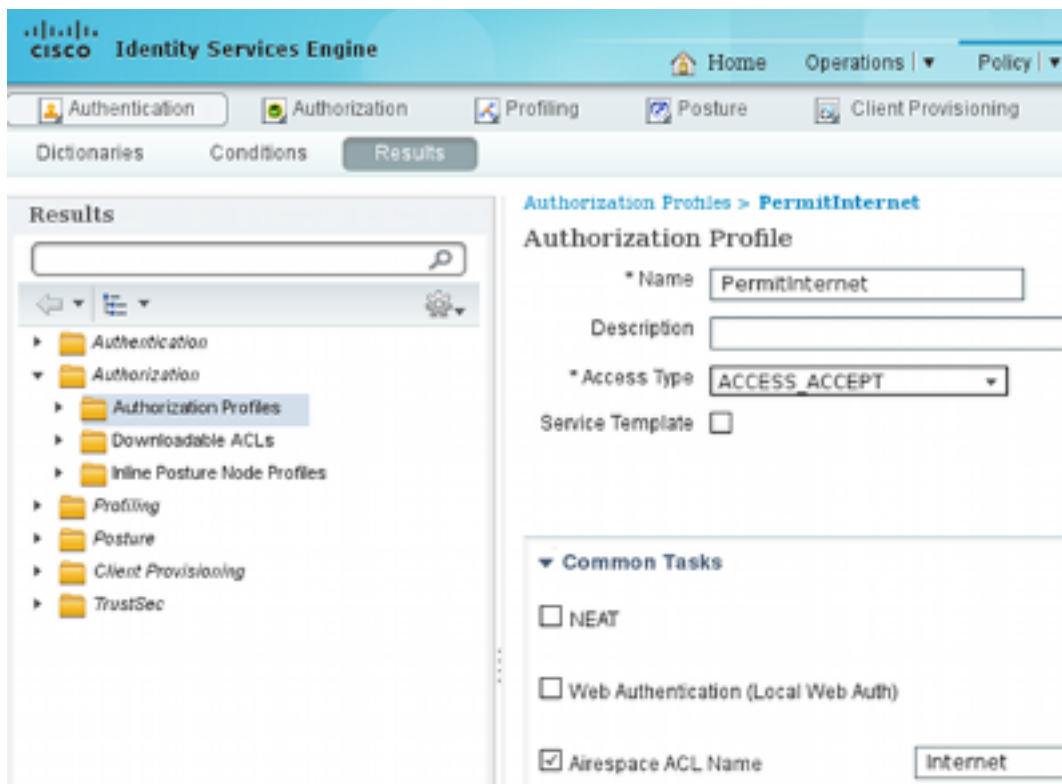


2. Wählen Sie den Portnamen aus, auf den im Autorisierungsprofil verwiesen wird. Legen Sie alle anderen Einstellungen auf die Standardeinstellungen fest. Unter Anpassung der Portalseite können alle angezeigten Seiten angepasst werden.
3. Autorisierungsprofile konfigurieren:

Guest (mit Umleitung zum Namen des Gastportals und ACL GuestRedirect)



PermitInternet (mit Airespace ACL gleich Internet)



- Um die Autorisierungsregeln zu überprüfen, navigieren Sie zu **Richtlinien > Autorisierung**. In der ISE-Version 1.3 wird standardmäßig die Authentifizierung für den fehlgeschlagenen MAC Authentication Bypass (MAB)-Zugriff (MAC-Adresse nicht gefunden) fortgesetzt (nicht abgelehnt). Dies ist sehr nützlich für Gastportale, da die Standardauthentifizierungsregeln nicht geändert werden müssen.

**Authorization Policy**

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Guest	if <b>GuestEndpoints</b> AND Radius:Called-Station-ID CONTAINS Guest	then PermitInternet
✓	Guest_Authenticate	if Radius:Called-Station-ID CONTAINS Guest	then Guest

Neue Benutzer, die der Gast-SSID zugeordnet sind, sind noch nicht Teil einer Identitätsgruppe. Aus diesem Grund werden sie mit der zweiten Regel übereinstimmen, die das Gastautorisierungsprofil verwendet, um sie an das richtige Gastportal umzuleiten.

Nachdem ein Benutzer ein Konto erstellt und sich erfolgreich angemeldet hat, sendet die ISE ein RADIUS-CoA, und der WLC führt eine erneute Authentifizierung durch. Diesmal wird die erste Regel zusammen mit dem Autorisierungsprofil PermitInternet zugeordnet und gibt den ACL-Namen zurück, der auf den WLC angewendet wird.

5. Fügen Sie den WLC als Netzwerkzugriffsgerät von **Administration > Network Resources > Network Devices** (Verwaltung > Netzwerkressourcen > Netzwerkgeräte) hinzu.

## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Nachdem Sie eine Verbindung zur Gast-SSID hergestellt und eine URL eingegeben haben, werden Sie zur Anmeldeseite umgeleitet:

https://ise13.example.com:8443/portal/PortalSetup.action?portal=6f48b7c0-1967-11e4-a20e-0050569c3f63& ☆ Google

**CISCO** Sponsored Guest Portal

**Sign On**  
Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Passcode:

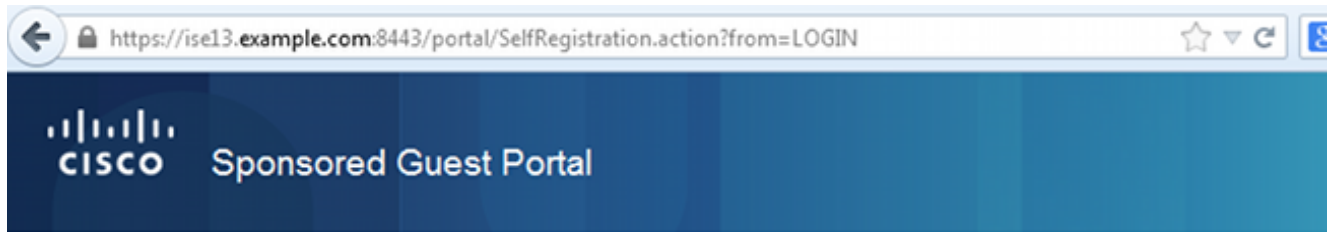
**Sign On**

[Don't have an account?](#)

[Contact Support](#)

2. Da Sie noch keine Anmeldeinformationen haben, müssen Sie die Option **Kein Konto haben** auswählen. Option. Eine neue Seite, die die Kontoerstellung ermöglicht, wird angezeigt. Wenn die Option Registrierungscode unter der Konfiguration des Gastportals aktiviert wurde, ist dieser geheime Wert erforderlich (dies stellt sicher, dass nur Personen mit den richtigen Berechtigungen zur Selbstregistrierung berechtigt sind).





### Create Account

Please provide us with some information so we can create an account for you.

Registration Code\*

cisco

Username

guest1

First name

Michal

Last name

garcarz

Email address

mgarcarz@cisco.com

Phone number

666666666

3. Wenn Probleme mit dem Kennwort oder der Benutzerrichtlinie auftreten, navigieren Sie zu **Guest Access > Settings > Guest Password Policy** oder **Guest Access > Settings > Guest Username Policy (Gastzugriff > Einstellungen > Gastbenutzername-Richtlinie)**, um die Einstellungen zu ändern. Hier ein Beispiel:



Configure

Manage Accounts

Settings

▶ Guest Email Settings

Identify the SMTP server and specify

▶ Guest Locations and SSIDs

Specify the locations where you want

▶ Guest Password Policy

Specify the policy settings that will

▼ Guest Username Policy

Specify the policy settings that will

Configure username requirements that will be enforced for guest usernames. Usernames

Username Length

Minimum username length:  (1-64 characters)

Username Criteria for Known Guests

If data is available, base username on:

- First name and last name
- Email address

Characters Allowed in Randomly-Generated Usernames

Alphabetic:

Minimum alphabetic:  (0-64)

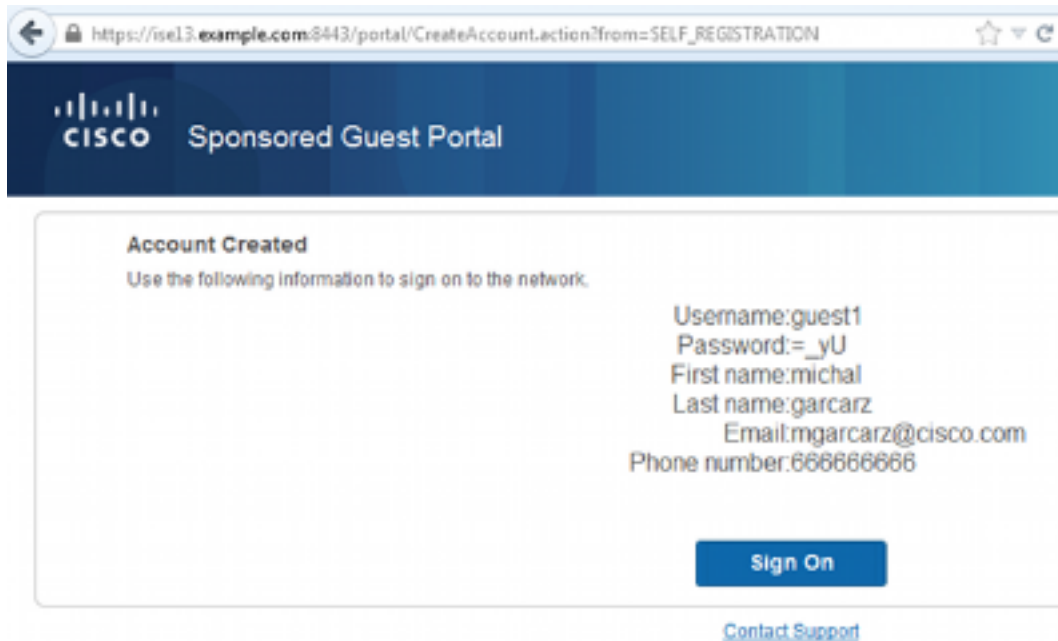
Numeric:

Minimum numeric:  (0-64)

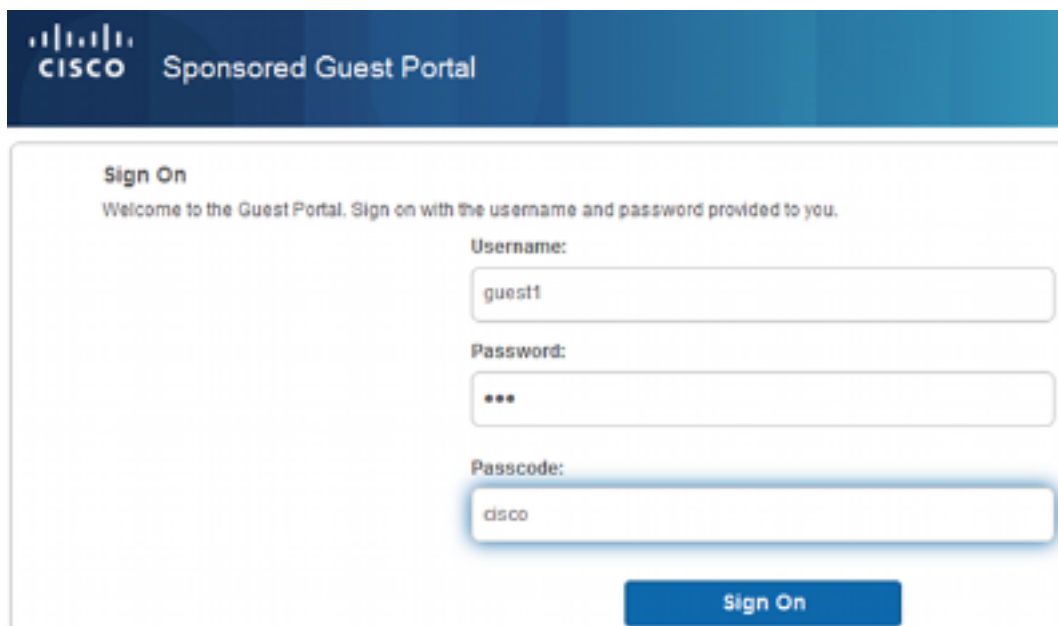
Special:

Minimum special:  (0-64)

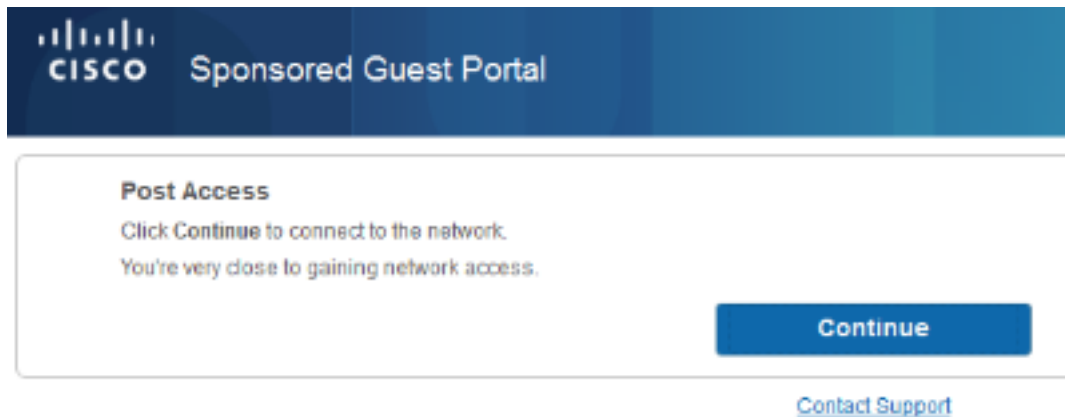
4. Nach der erfolgreichen Kontoerstellung erhalten Sie die Anmeldeinformationen (das Kennwort wird gemäß den Richtlinien für das Gastkennwort generiert):



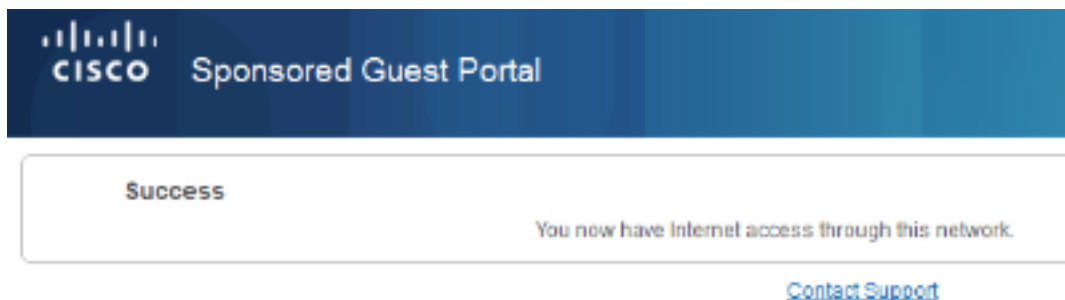
5. Klicken Sie auf **Anmelden**, und geben Sie Anmeldeinformationen an. (Möglicherweise ist ein zusätzlicher Zugriffskenncode erforderlich, wenn dieser im Gastportal konfiguriert wird.) Dies ist ein weiterer Sicherheitsmechanismus, der es nur denjenigen erlaubt, die das Kennwort kennen, sich anzumelden).



6. Wenn der Vorgang erfolgreich ist, wird möglicherweise eine optionale Richtlinie für akzeptable Nutzung (Acceptable Use Policy, AUP) angezeigt (wenn diese im Gastportal konfiguriert ist). Die Seite "Post Access" (auch unter "Guest Portal" konfigurierbar) kann ebenfalls angezeigt werden.



Auf der letzten Seite wird bestätigt, dass der Zugriff gewährt wurde:



## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

In diesem Stadium stellt die ISE folgende Protokolle vor:

Time	Status	Det...	Repeat Count	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2014-08-01 13:19:52...	!		0	guest1					Session State is Started
2014-08-01 13:19:52...	✓			guest1	Default >> MAB	Default >> Guest	PermitInternet	User Identity Gro...	Authorize-Only succeeded
2014-08-01 13:19:52...	✓			guest1					Dynamic Authorization succeeded
2014-08-01 13:18:29...	✓			guest1				GuestType_DAILY	Guest Authentication Passed
2014-08-01 13:16:31...	✓			64:66:B3:08:23	Default >> MAB >> ..	Default >> Guest_...	Guest		Authentication succeeded

Hier ist der Ablauf:

- Der Gastbenutzer erhält die zweite Autorisierungsregel (Guest\_Authenticate) und wird an Guest ("Authentifizierung erfolgreich") umgeleitet.
- Der Gast wird zur Selbstregistrierung umgeleitet. Nach erfolgreicher Anmeldung (mit dem neu erstellten Konto) sendet die ISE den CoA-Reauthentifizierungsdienst, der vom WLC bestätigt wird ("Dynamic Authorization Succeeded").

- Der WLC führt eine erneute Authentifizierung mit dem Authorize-Only-Attribut durch, und der ACL-Name wird zurückgegeben ("Authorize-Only Succeeded"). Der Gast erhält den richtigen Netzwerkzugriff.

Berichte (**Operations > Reports > ISE Reports > Guest Access Reports > Master Guest Report**) bestätigen außerdem:

Master Guest Report <span style="float: right;">Favorite</span>							
From 08/01/2014 12:00:00 AM to 08/01/2014 02:42:34 PM <span style="float: right;">Page &lt;&lt; 1 &gt;&gt;</span>							
Logged At	Guest User Name	MAC Address	IP Address	Operation	User Name	Message	AUP Acceptance
2014-08-01 13:18:49.9	guest1	64-66-83-08-23-A3	10.221.0.218				Guest user has accepted the use policy
2014-08-01 13:18:08.7	guest1	64-66-83-08-23-A3	10.221.0.218	Add	SelfRegistration		

Ein Sponsor-Benutzer (mit den richtigen Berechtigungen) kann den aktuellen Status eines Gastbenutzers überprüfen.

In diesem Beispiel wird bestätigt, dass das Konto erstellt wurde, der Benutzer sich jedoch nie angemeldet hat ("Wartet auf erste Anmeldung"):

The screenshot shows the Cisco Sponsor Portal interface. At the top, there are navigation buttons: "Create Accounts", "Manage Accounts (1)", "Pending Accounts (0)", and "Notices (0)". Below these are action buttons: "Resend", "Extend", "Edit", "Suspend", "Reinstate", "Delete", "Reset Password", and "Print".

The main content area displays the following account details:

- First name: michal
- Last name: garcarz
- Username: guest1
- Password: =\_yU
- Email address: mgarcarz@cisco.com
- Company:
- Phone number: 666666666
- Person being visited(email):
- Reason for visit:
- Guest type: DAILY
- SMS provider:
- State: Awaiting Initial Login
- From date: 08/01/2014 12:58
- To date: 08/02/2014 12:58
- Location:
- SSID:
- Language: English
- Group tag:
- Time left: 0,23,47

## Optionale Konfiguration

Für jede Phase dieses Datenflusses können verschiedene Optionen konfiguriert werden. All dies wird über das Gastportal unter **Gastzugriff > Konfigurieren > Gastportale > Portalname > Bearbeiten > Portalverhalten und Ablaufeinstellungen** konfiguriert. Wichtigste Einstellungen:

## Selbstregistrierungseinstellungen

- Gasttyp - Beschreibt, wie lange das Konto aktiv ist, Optionen für das Kennwortablaufen, Anmeldezeiten und Optionen (dies ist eine Mischung aus Time Profile (Zeitprofil) und Guest Role (Gastrolle) aus ISE Version 1.2).
- Registrierungscode: Wenn diese Option aktiviert ist, können sich nur Benutzer registrieren, die den geheimen Code kennen. Das Kennwort muss beim Erstellen des Kontos angegeben werden.
- AUP - Akzeptieren der Nutzungsrichtlinie während der Selbstregistrierung
- Genehmigung/Aktivierung des Gastkontos durch den Sponsor

## Gasteinstellungen anmelden

- Zugriffscode: Wenn diese Option aktiviert ist, können sich nur Gastbenutzer anmelden, die den geheimen Code kennen.
- AUP - Akzeptieren der Nutzungsrichtlinie während der Selbstregistrierung
- Kennwortänderungsoption

## Geräteregistrierungseinstellungen

- Standardmäßig wird das Gerät automatisch registriert.

## Compliance-Einstellungen für Gastgeräte

- Ermöglicht eine Haltung innerhalb des Flusses

## BYOD-Einstellungen

- Ermöglicht Unternehmensbenutzern, die das Portal als Gäste verwenden, die Registrierung ihrer privaten Geräte

## Vom Sponsor genehmigte Konten

Wenn die Option **Autorisierte Gäste zur Genehmigung** vorschreiben aktiviert ist, muss das vom Gast erstellte Konto von einem Sponsor genehmigt werden. Diese Funktion kann E-Mail verwenden, um dem Sponsor eine Benachrichtigung zu senden (zur Genehmigung eines Gastkontos):

Wenn der SMTP-Server (Simple Mail Transfer Protocol) oder die Standardeinstellung aus der Benachrichtigung per E-Mail nicht konfiguriert ist, wird das Konto nicht erstellt:

## Account Created

Use the following information to sign on to the network.

Email send failure

First name:michal

Last name:garcarz

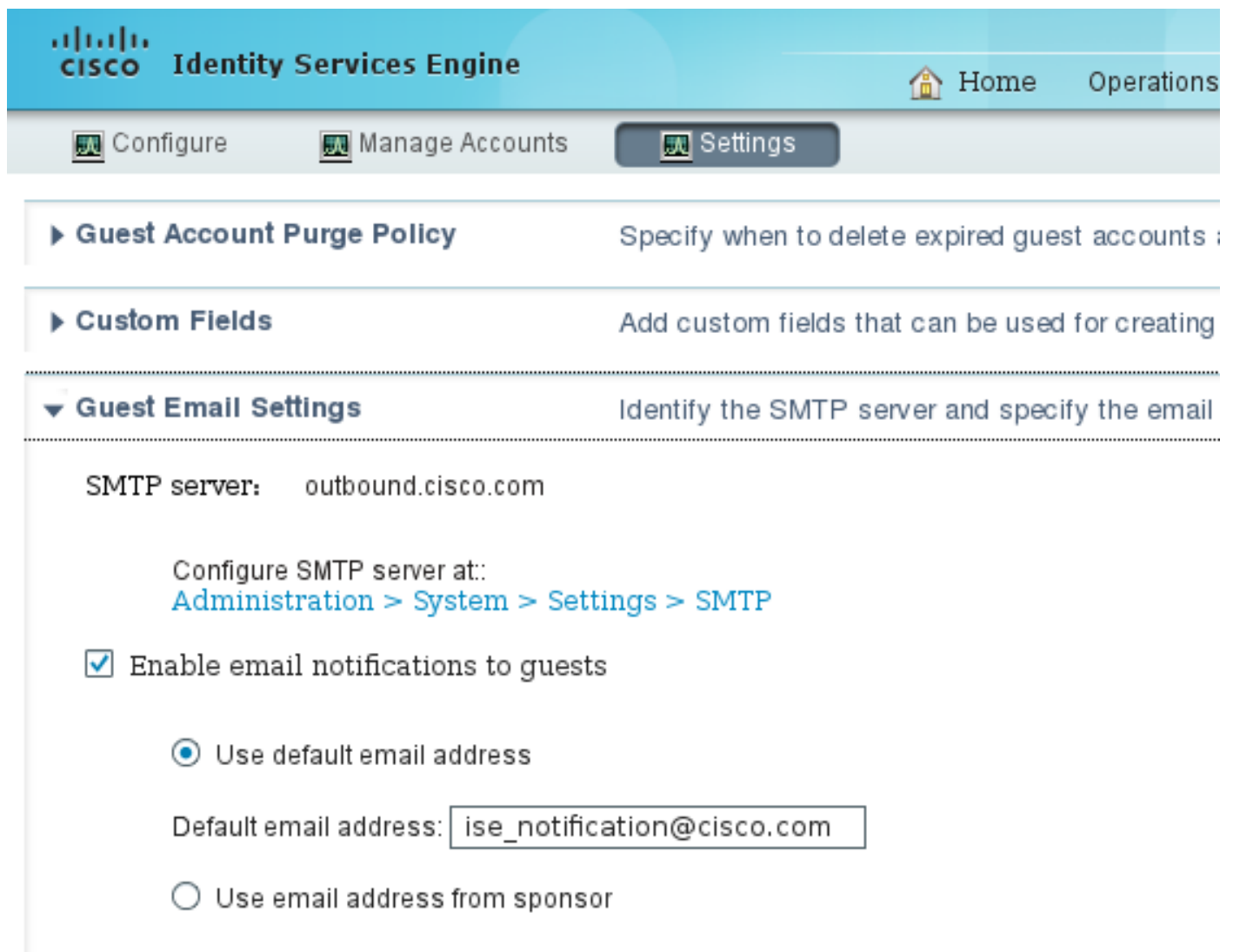
Email:mgarcarz@cisco.com

Sign On

Das Protokoll von guest.log bestätigt, dass die für die Benachrichtigung verwendete globale Absenderadresse fehlt:

```
2014-08-01 22:35:24,271 ERROR [http-bio-10.62.97.21-8443-exec-9][] guestaccess.  
flowmanager.step.guest.SelfRegStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-  
Catch GuestAccessSystemException on sending email for approval: sendApproval  
Notification: From address is null. A global default From address can be  
configured in global settings for SMTP server.
```

Wenn Sie über die richtige E-Mail-Konfiguration verfügen, wird das Konto erstellt:



The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". On the right side of the navigation bar, there are links for "Home" and "Operations". Below the navigation bar, there are three main menu items: "Configure", "Manage Accounts", and "Settings". The "Settings" menu item is currently selected and highlighted. Below the menu items, there are three expandable sections: "Guest Account Purge Policy", "Custom Fields", and "Guest Email Settings". The "Guest Email Settings" section is expanded, showing the following configuration options:

- SMTP server: outbound.cisco.com
- Configure SMTP server at:  
[Administration > System > Settings > SMTP](#)
- Enable email notifications to guests
  - Use default email address
  - Default email address:
  - Use email address from sponsor

## Account Created

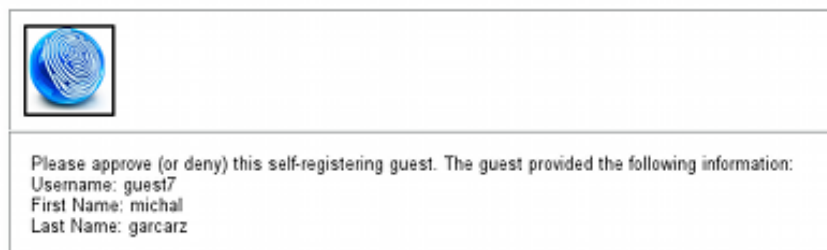
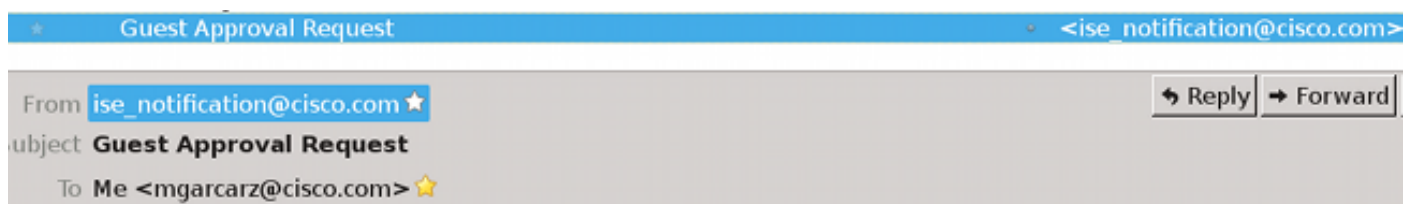
Use the following information to sign on to the network.

First name:michal  
Last name:garcarz  
Email:mgarcarz@cisco.com

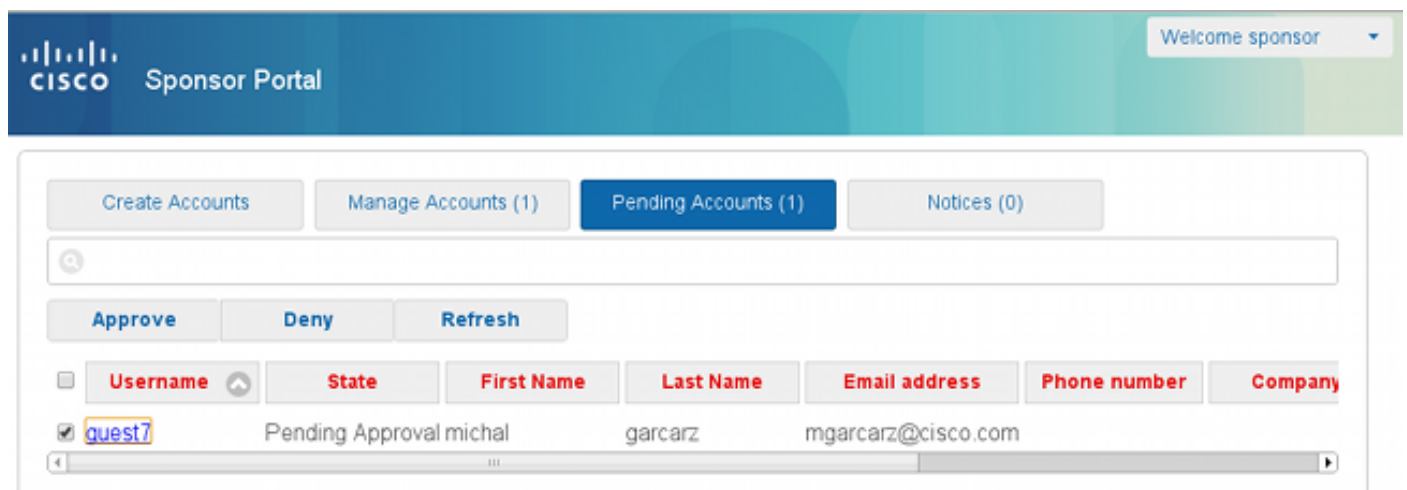
Sign On

Nachdem Sie die Option **Eigene Gäste zur Genehmigung** vorschreiben aktiviert haben, werden die Felder Benutzername und Kennwort automatisch aus dem Abschnitt **Diese Informationen im Abschnitt Selbstregistrierungserfolge einschließen** entfernt. Wenn eine Genehmigung durch den Sponsor erforderlich ist, werden Anmeldeinformationen für Gastbenutzer nicht standardmäßig auf der Webseite angezeigt, die Informationen zum Nachweis der Erstellung des Kontos enthält. Stattdessen müssen sie per SMS oder E-Mail zugestellt werden. Diese Option muss im Abschnitt **"Benachrichtigung bei Genehmigung senden"** (markieren Sie E-Mail/SMS) in der Meldung **"Anmeldeinformationen senden"** aktiviert sein.

Eine Benachrichtigungs-E-Mail wird an den Sponsor gesendet:



Der Sponsor meldet sich beim Sponsorportal an und genehmigt das Konto:





Ab diesem Zeitpunkt kann sich der Gastbenutzer anmelden (mit den Anmeldeinformationen, die per E-Mail oder SMS eingegangen sind).

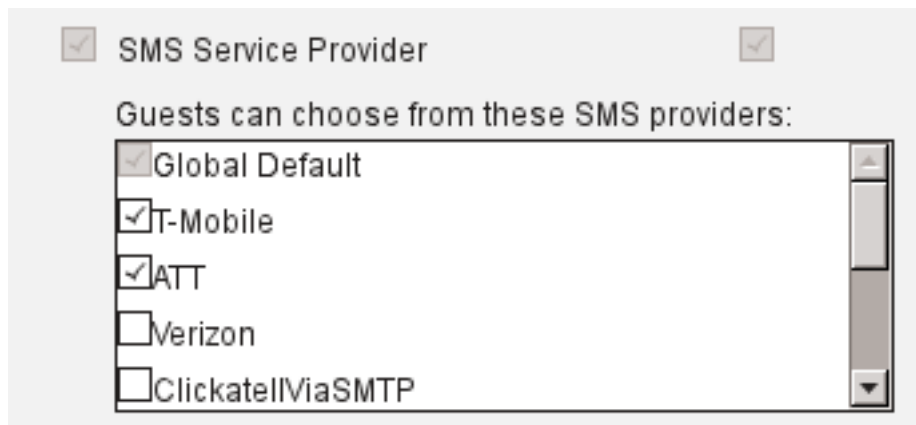
Insgesamt werden in diesem Fluss drei E-Mail-Adressen verwendet:

- Benachrichtigungsadresse "Von". Dies wird statisch definiert oder vom Sponsor-Konto übernommen und als Absenderadresse für beide verwendet: Benachrichtigung des Sponsors (zur Genehmigung) und Anmeldeinformationen für den Gast. Dies wird unter **Gastzugriff > Konfigurieren > Einstellungen > E-Mail-Einstellungen für Gäste** konfiguriert.
- Benachrichtigungsadresse "An". Diese Daten werden verwendet, um dem Sponsor mitzuteilen, dass er ein Konto zur Genehmigung erhalten hat. Dies wird im Gastportal unter **Gastzugriff > Konfigurieren > Gastportale > Portalname > Autorisierte Gäste müssen genehmigt werden > E-Mail-Genehmigungsanfrage an**.
- Adresse des Gasts "An". Diese wird vom Gastbenutzer während der Registrierung bereitgestellt. Wenn **bei Genehmigung per E-Mail eine Benachrichtigung zur Bestätigung der Anmeldeinformationen senden** ausgewählt wurde, wird die E-Mail mit Anmeldeinformationen (Benutzername und Kennwort) an den Gast gesendet.

## Bereitstellung von Anmeldeinformationen per SMS

Die Anmeldeinformationen des Gastes können auch per SMS übermittelt werden. Diese Optionen sollten konfiguriert werden:

1. Wählen Sie den SMS Service Provider:



2. Überprüfen Sie die **Benachrichtigung zur Benachrichtigung bei Genehmigung senden mithilfe von: SMS-Kontrollkästchen** aktivieren.
3. Anschließend wird der Gastbenutzer aufgefordert, bei der Erstellung eines Kontos den verfügbaren Anbieter auszuwählen:

← https://ise13.example.com:8443/portal/SelfRegistration.action?from=LOGIN ☆ ▾ ↻

Phone number\*

666666666

Company

SMS provider\*

T-Mobile

T-Mobile

ATT

Global Default

Reason for visit

4. Eine SMS wird mit dem ausgewählten Anbieter und der gewünschten Telefonnummer zugestellt:

**Account Created**

Use the following information to sign on to the network.

First name:michal  
Last name:garcarz  
Email:mgarcarz@cisco.com  
Phone number:666666666  
SMS Provider:Global Default

**Sign On**

5. Sie können SMS-Provider unter **Administration > System > Settings > SMS Gateway** konfigurieren.

## Gerätregistrierung

Wenn die Option **Gastbenutzer zum Registrieren von Geräten zulassen** aktiviert ist, nachdem sich ein Gastbenutzer angemeldet hat und die AUP akzeptiert, können Sie Geräte registrieren:

### Device Registration

You can add a maximum of \$guest.device\_limit\$ devices. Enter a device ID and device description. The device ID is the MAC address or Wi-Fi address of the device. It is an alphanumeric ID in this format: A1:B3:E5:19:6F:BB

Device ID

Device Description

Manage Devices (1)

64:66:B3:08:23:A3	<input type="button" value="Delete"/>
-------------------	---------------------------------------

Beachten Sie, dass das Gerät bereits automatisch hinzugefügt wurde (es befindet sich in der Liste "Manage Devices" (Geräte verwalten)). Dies liegt daran, dass **Gastgeräte automatisch registriert** wurden.

## Status

Wenn die Option **Compliance** für **Gastgeräte anfordern** aktiviert ist, erhalten Gastbenutzer einen Agenten, der nach der Anmeldung den Status ausführt (NAC/Web Agent) und die AUP akzeptiert (und optional die Geräteregistrierung durchführt). Die ISE verarbeitet Client Provisioning-Regeln, um zu entscheiden, welcher Agent bereitgestellt werden soll. Der Agent, der auf der Station ausgeführt wird, führt den Status aus (gemäß den Posture-Regeln) und sendet Ergebnisse an die ISE, die die CoA-erneute Authentifizierung sendet, um den Autorisierungsstatus ggf. zu ändern.

Mögliche Autorisierungsregeln könnten ähnlich aussehen wie:

▶ Exceptions (0)

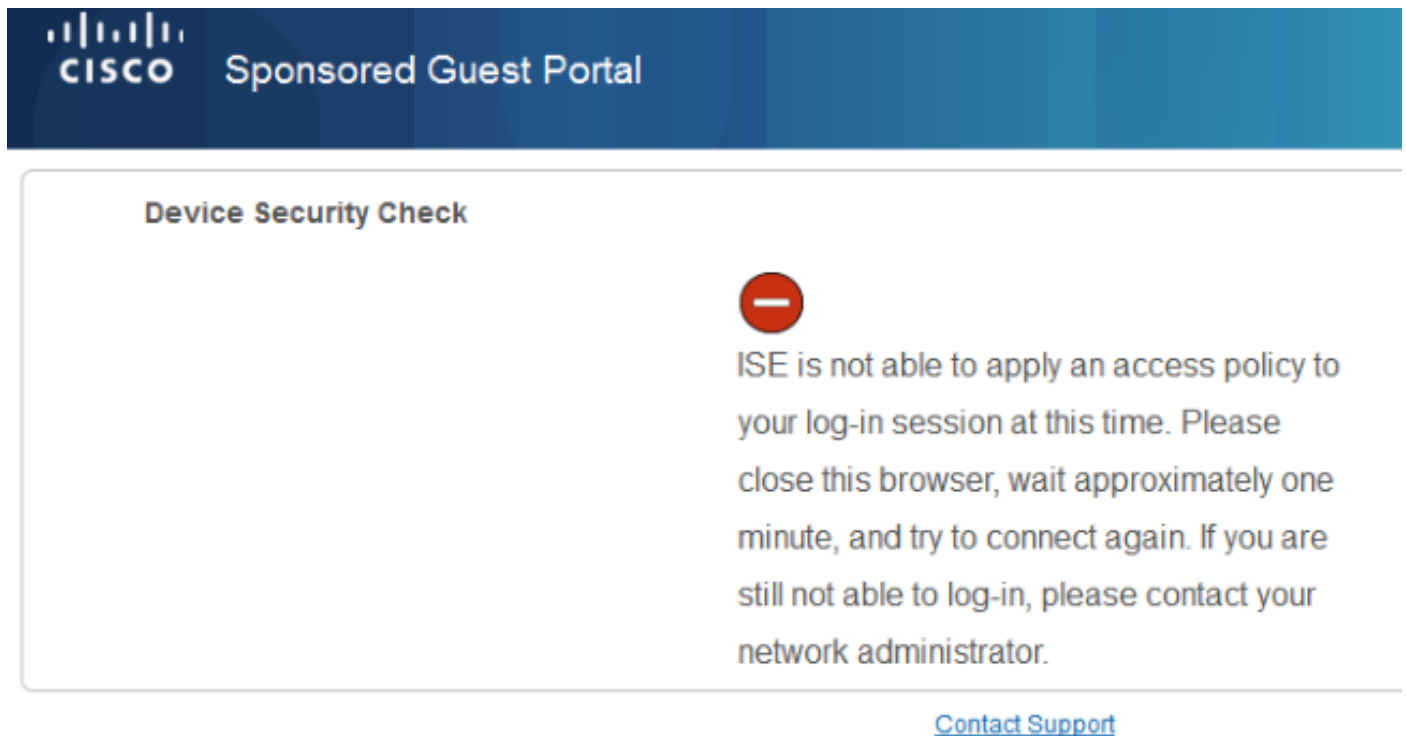
Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Guest_Compliant	if <b>GuestEndpoints</b> AND (Radius:Called-Station-ID CONTAINS Guest AND Session:PostureStatus EQUALS Compliant )	then PermitInternet
✓	Guest	if <b>GuestEndpoints</b> AND Radius:Called-Station-ID CONTAINS Guest	then LimitedAccess
✓	Guest_Authenticate	if Radius:Called-Station-ID CONTAINS Guest	then Guest


Die ersten neuen Benutzer, die auf eine Guest\_Authenticate-Regel stoßen, werden zum Gastportal Self Register umgeleitet. Nachdem sich der Benutzer selbst registriert und sich angemeldet hat, ändert CoA den Autorisierungsstatus, und dem Benutzer wird nur eingeschränkter Zugriff für Statusüberprüfung und Problembehebung gewährt. Erst nachdem der NAC Agent bereitgestellt wurde und die Station den Vorgaben entspricht, ändert CoA den Autorisierungsstatus erneut, um den Zugriff auf das Internet zu ermöglichen.

Typische Schwachstellen bei der Statusanzeige sind fehlende, korrekte Client-

Bereitstellungsregeln:



**Device Security Check**



ISE is not able to apply an access policy to your log-in session at this time. Please close this browser, wait approximately one minute, and try to connect again. If you are still not able to log-in, please contact your network administrator.

[Contact Support](#)

Dies kann auch bestätigt werden, wenn Sie die Datei guest.log (neu in ISE Version 1.3) überprüfen:

```
2014-08-01 21:35:08,435 ERROR [http-bio-10.62.97.21-8443-exec-9][] guestaccess.  
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F:: -  
CP Response is not successful, status=NO_POLICY
```

## BYOD

Wenn die Option **Zulassen der Nutzung privater Geräte durch Mitarbeiter im Netzwerk** aktiviert ist, können Unternehmensbenutzer, die dieses Portal verwenden, den BYOD-Fluss durchlaufen und private Geräte registrieren. Für Gastbenutzer ändert diese Einstellung nichts.

Was bedeutet "Mitarbeiter, die das Portal als Gast verwenden"?

Gastportale werden standardmäßig mit dem **Guest\_Portal\_Sequence**-Identitätsdatenspeicher konfiguriert:

**▼ Portal Settings**

HTTPS port: \*  (8000 - 8999)

Allowed interfaces: \*  Gigabit Ethernet 0  
 Gigabit Ethernet 1  
 Gigabit Ethernet 2  
 Gigabit Ethernet 3

Certificate Group Tag: \*

*Configure certificates at:*  
[Administration > System > Certificates > System Certificates](#)

Identity source sequence: \*

*Configure identity source sequence at:*  
[Administration > Identity Management > Identity Source Sequences](#)

Dies ist die interne Speichersequenz, die zuerst die internen Benutzer (vor Gastbenutzern) testet:

**CISCO Identity Services Engine** Home Operations Policy

System Identity Management Network Resources Device Portal Management

Identities Groups External Identity Sources **Identity Source Sequences** Settings

[Identity Source Sequences List > Guest\\_Portal\\_Sequence](#)

**Identity Source Sequence**

▼ Identity Source Sequence

\* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
Internal Endpoints	>	Internal Users
AD1	<	Guest Users
	>>	All_AD_instances
	<<	

Wenn der Benutzer in dieser Phase im Gastportal Anmeldeinformationen bereitstellt, die im internen Benutzer-Store definiert sind und die BYOD-Umleitung erfolgt:

1

2

3

4

### BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click Start to provide device information before components are installed on your device.

Start

I want guest access only

Auf diese Weise können Unternehmensbenutzer BYOD für private Geräte ausführen.

Wenn anstelle der Anmeldeinformationen für interne Benutzer Anmeldeinformationen für Gastbenutzer angegeben werden, wird der normale Fluss fortgesetzt (kein BYOD).

## VLAN-Änderung

Dies ist eine ähnliche Option wie die für das Gastportal in ISE Version 1.2 konfigurierte VLAN-Änderung. Es ermöglicht Ihnen ActiveX oder ein Java-Applet auszuführen, das DHCP zur Veröffentlichung und Verlängerung veranlasst. Dies ist erforderlich, wenn CoA die Änderung des VLANs für den Endpunkt auslöst. Wenn MAB verwendet wird, ist dem Endpunkt keine Änderung des VLANs bekannt. Eine mögliche Lösung besteht darin, das VLAN (DHCP-Version/Erneuerung) mit dem NAC Agent zu ändern. Eine weitere Option besteht darin, über das auf der Webseite zurückgegebene Applet eine neue IP-Adresse anzufordern. Eine Verzögerung zwischen Release/CoA/Verlängerung kann konfiguriert werden. Diese Option wird für Mobilgeräte nicht unterstützt.

## Zugehörige Informationen

- [Statusservices im Cisco ISE-Konfigurationsleitfaden](#)
- [Wireless BYOD mit Identity Services Engine](#)
- [ISE SCEP-Unterstützung - BYOD-Konfigurationsbeispiel](#)
- [Cisco ISE 1.3 Administratorhandbuch](#)
- [Zentrale Webauthentifizierung im Konfigurationsbeispiel für WLC und ISE](#)
- [Zentrale Webauthentifizierung mit FlexConnect-APs auf einem WLC mit ISE-Konfigurationsbeispiel](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)