ISE Self Registered Guest Portal konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration und Fehlerbehebung der ISE-Funktion für selbst registrierte Gastportale beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, Erfahrung mit der ISE-Konfiguration und Grundkenntnisse in den folgenden Bereichen zu haben:

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

Verwendete Komponenten

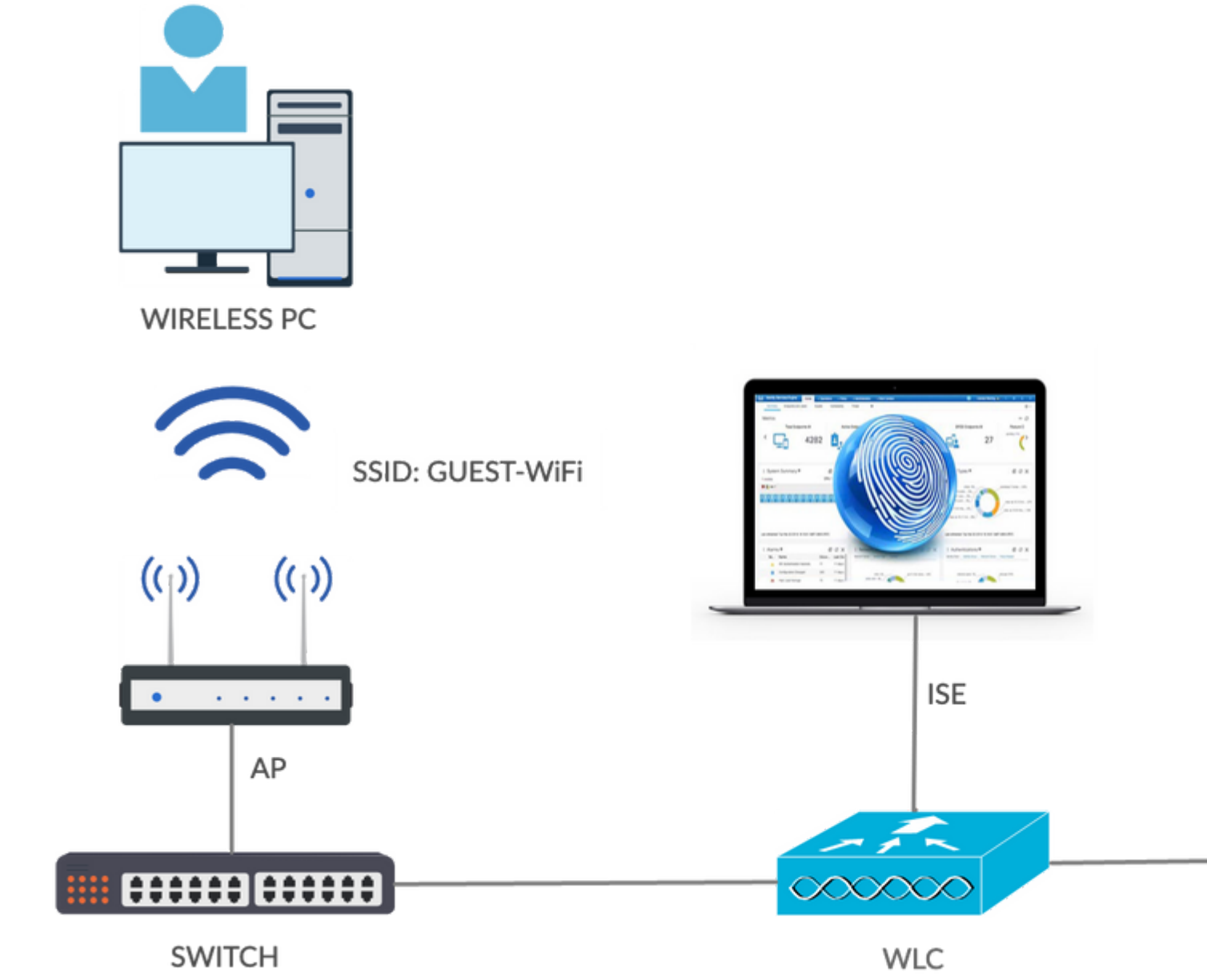
Self Registered Guest Portal: Ermöglicht Gastbenutzern die Selbstregistrierung sowie Mitarbeitern, die ihre AD-Anmeldeinformationen verwenden, um Zugriff auf Netzwerkressourcen zu erhalten. In diesem Portal können Sie mehrere Funktionen konfigurieren und anpassen.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Microsoft Windows 10 Pro
- Cisco WLC 5508 mit Version 8.5.135.0
- ISE-Software, Version 3.0

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.

Topologie und Datenfluss



Dieses Szenario stellt mehrere Optionen zur Verfügung, die Gastbenutzern bei der Selbstregistrierung zur Verfügung stehen.

Dies ist der allgemeine Ablauf:

Schritt 1: Gastbenutzer wird Service Set Identifier (SSID) zugeordnet: Gast-Wi-Fi. Dies ist ein offenes Netzwerk mit MAC-Filterung und ISE zur Authentifizierung. Diese Authentifizierung entspricht der zweiten Autorisierungsregel auf der ISE, und das Autorisierungsprofil wird an das Portal mit der Gastselbstregistrierung weitergeleitet. Die ISE gibt einen RADIUS Access-Accept-Wert mit zwei cisco-av-Paaren zurück:

- url-redirect-acl (welcher Datenverkehr umgeleitet werden muss, und der Name der lokal auf dem WLC definierten Zugriffskontrollliste (ACL))
- url-redirect (where to redirect that traffic- to ISE)

Schritt 2: Der Gastbenutzer wird auf die ISE umgeleitet. Anstatt Anmeldeinformationen für die Anmeldung anzugeben, klickt der Benutzer auf **Für Gastzugriff registrieren.** Der Benutzer wird auf eine Seite umgeleitet, auf der das Konto erstellt werden kann. Ein optionaler geheimer Registrierungscode kann aktiviert werden, um die Berechtigung zur Selbstregistrierung 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)-erneute Authentifizierung an den WLC. Der WLC authentifiziert den Benutzer erneut, wenn er die RADIUS-Zugriffsanforderung mit dem Authorize-Only-Attribut sendet. Die ISE reagiert mit lokal auf dem WLC definierter Access-Accept- und Airespace-ACL, die nur Internetzugang bietet (der endgültige Zugriff für Gastbenutzer hängt von der Autorisierungsrichtlinie ab).

> **Hinweis:** EAP-Sitzungen (Extensible Authentication Protocol) müssen von der ISE eine CoA-Terminierung gesendet werden, um eine erneute Authentifizierung auszulösen, da sich die EAP-Sitzung zwischen dem Supplicant und der ISE befindet. Für MABs (MAC-Filterung) ist eine erneute CoA-Authentifizierung jedoch ausreichend. Eine Trennung bzw. Deauthentifizierung des Wireless-Clients ist nicht erforderlich.

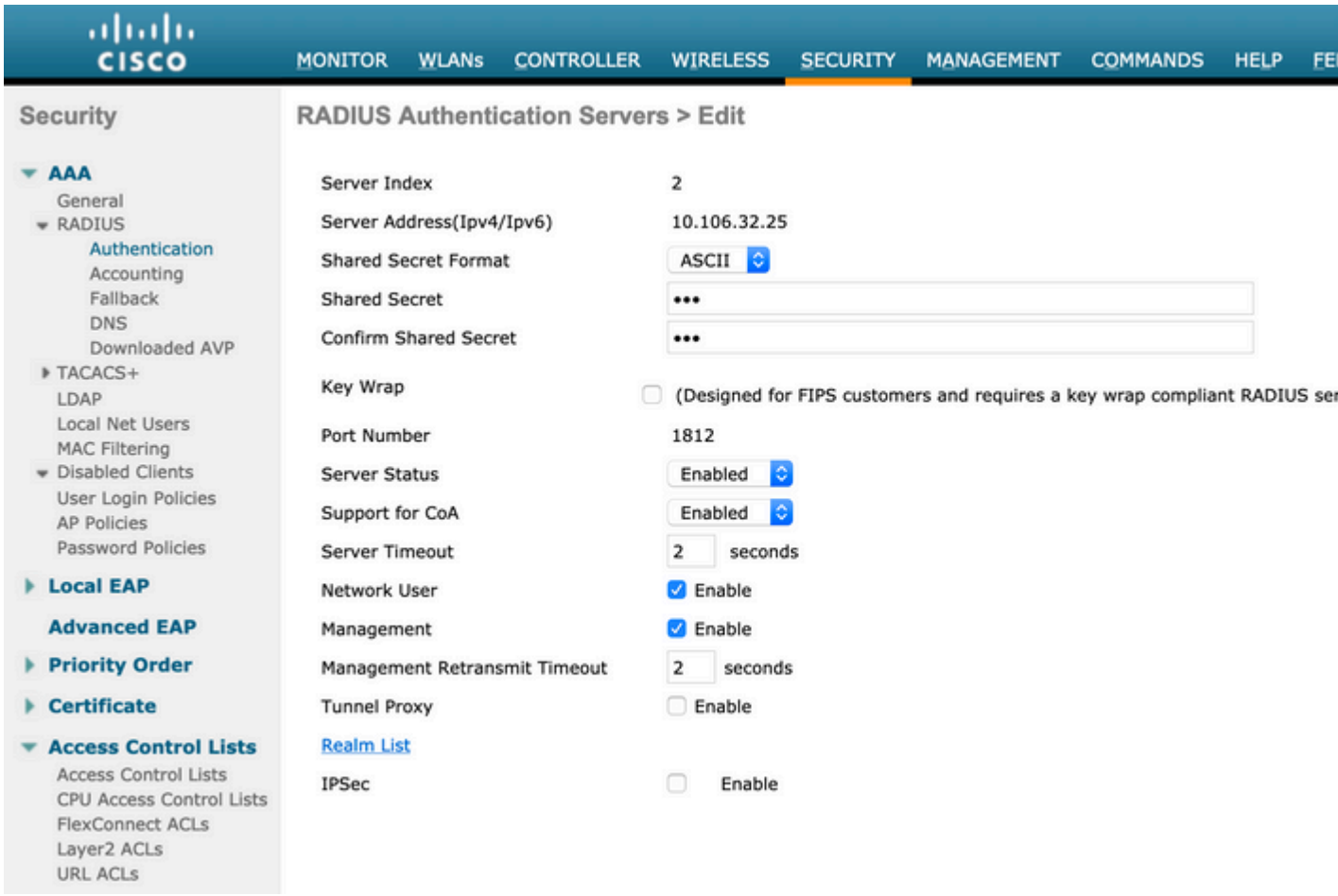
Schritt 4: Der Gastbenutzer hat den gewünschten Zugriff auf das Netzwerk.

Mehrere zusätzliche Funktionen wie Status und Bring Your Own Device (BYOD) können aktiviert werden (auf die später noch eingegangen wird).

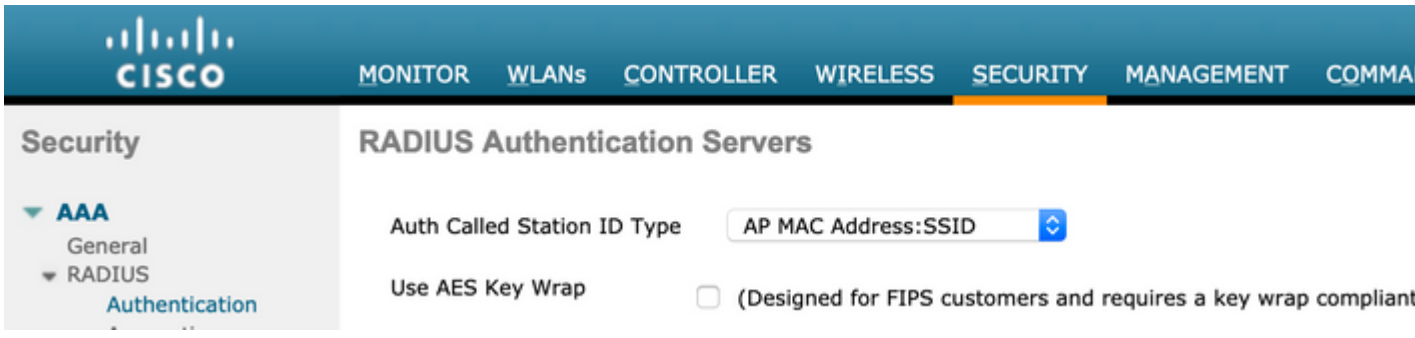
Konfigurieren

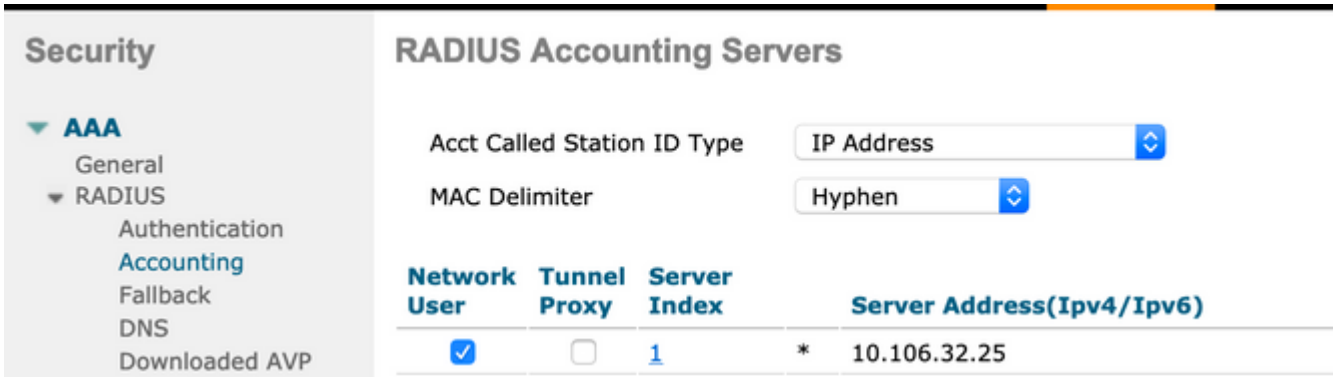
WLC

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



Eine ähnliche Konfiguration gibt es für die Kontoführung. Es wird außerdem empfohlen, den WLC so zu konfigurieren, dass SSID im Attribut "Called Station ID" gesendet wird. Auf diese Weise kann die ISE flexible Regeln auf Basis der SSID konfigurieren:





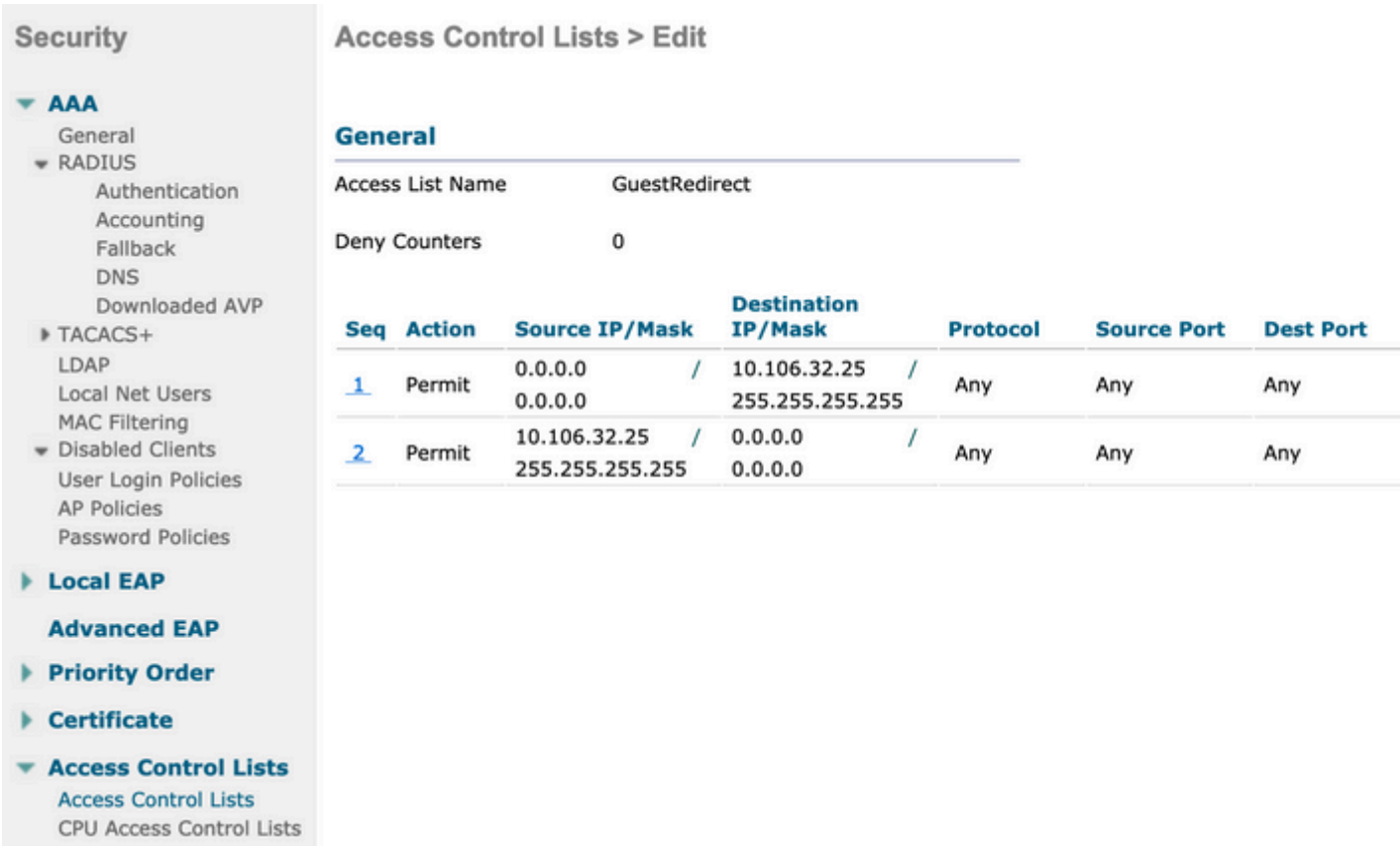
2. Erstellen Sie auf der Registerkarte WLANs das WLAN (Wireless LAN) Guest-WiFi, und konfigurieren Sie die richtige Schnittstelle. Setzen Sie die Layer-2-Sicherheit mit MAC-Filterung auf

None (Keine). Wählen Sie unter Security/Authentication, Authorization, and Accounting (AAA) Servers (Sicherheit/Authentifizierung, Autorisierung und Abrechnung) die ISE-IP-Adresse für die Authentifizierung und die Abrechnung aus. Aktivieren Sie auf der Registerkarte Advanced die Option **AAA Override,** und legen Sie Network Admission Control (NAC) State (Netzwerkzugangskontrolle) auf ISE NAC (CoA-Unterstützung) fest.

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

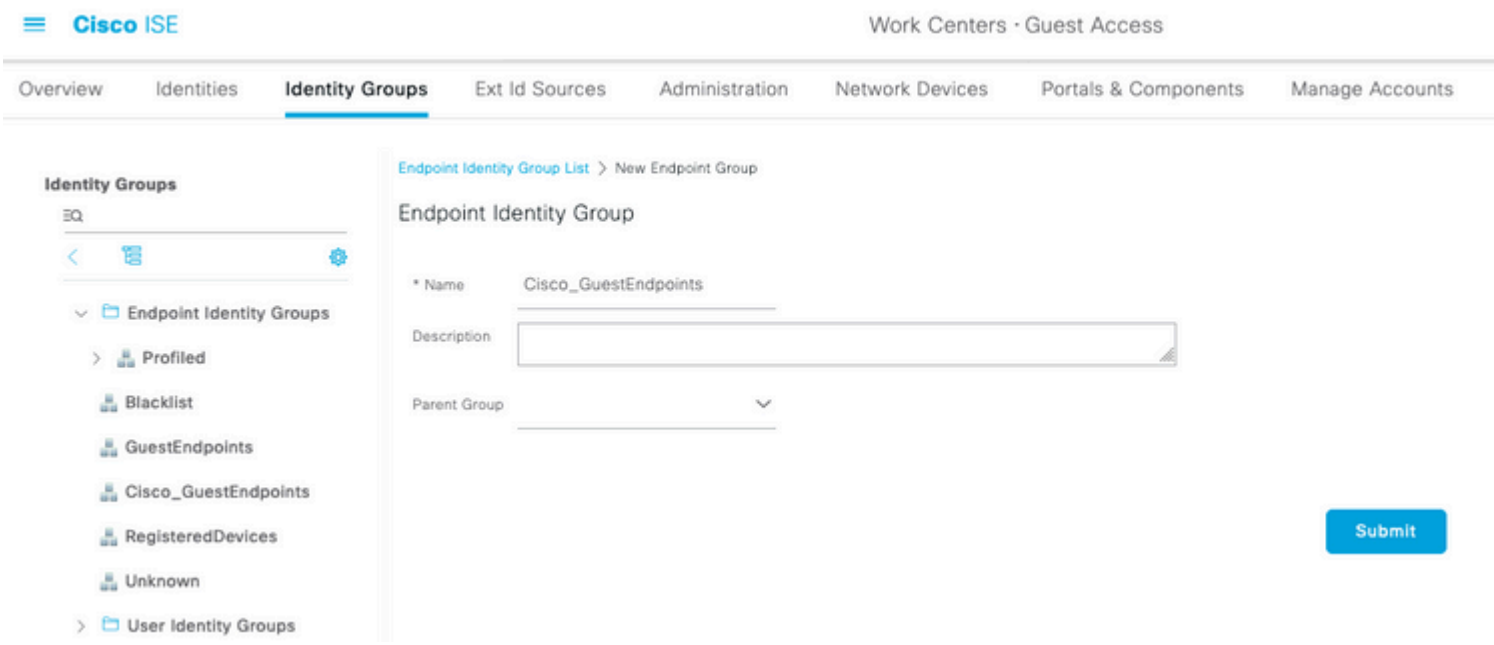
   - GuestRedirect ermöglicht die Weiterleitung von Datenverkehr, der nicht umgeleitet werden darf, und leitet den gesamten anderen Datenverkehr um.
   - Internet, das für Unternehmensnetzwerke verweigert wird und für alle anderen zulässig ist

   Ein Beispiel für die GuestRedirect ACL (die Notwendigkeit, Datenverkehr zur/von der ISE von der Umleitung auszuschließen):

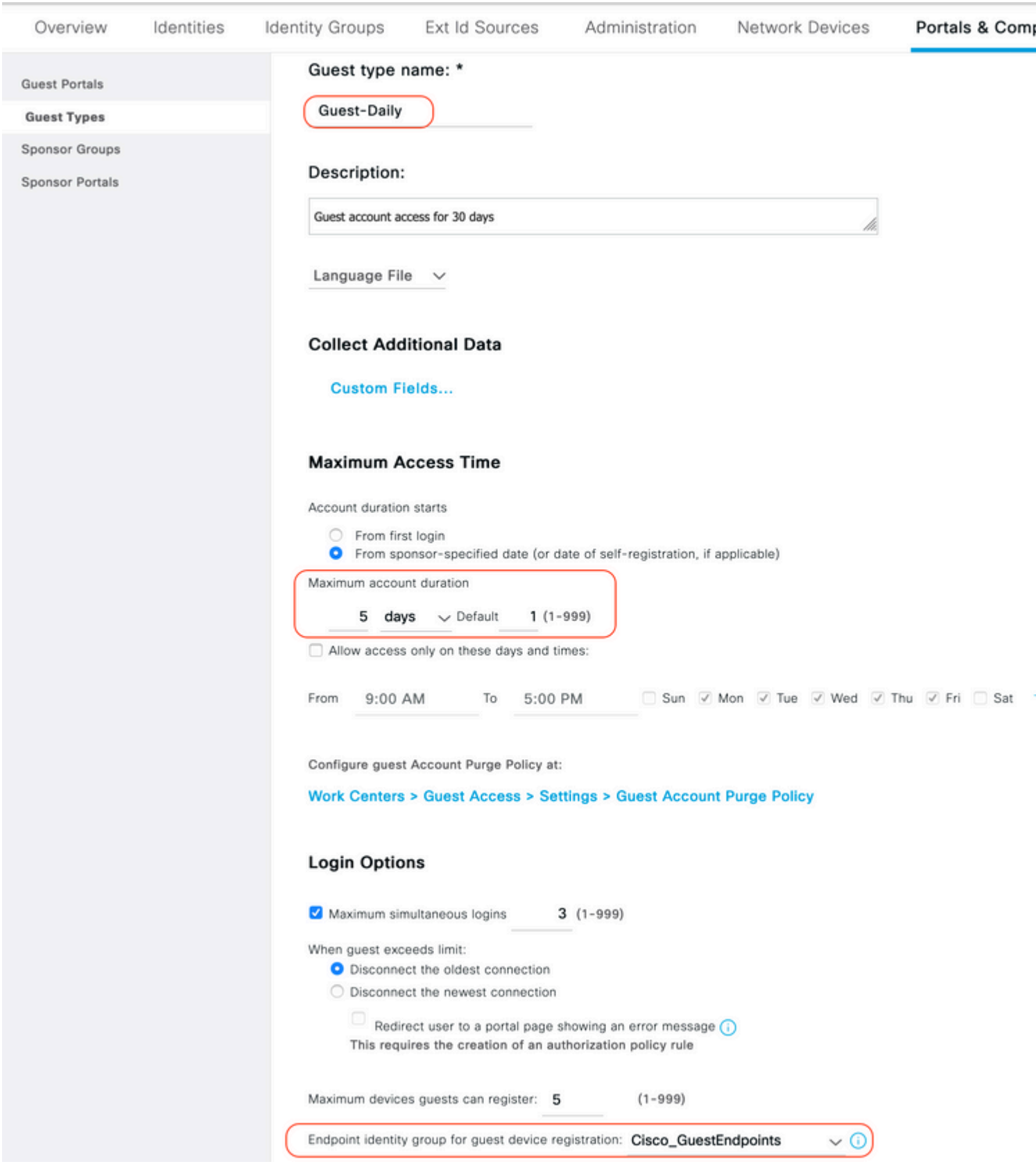


ISE

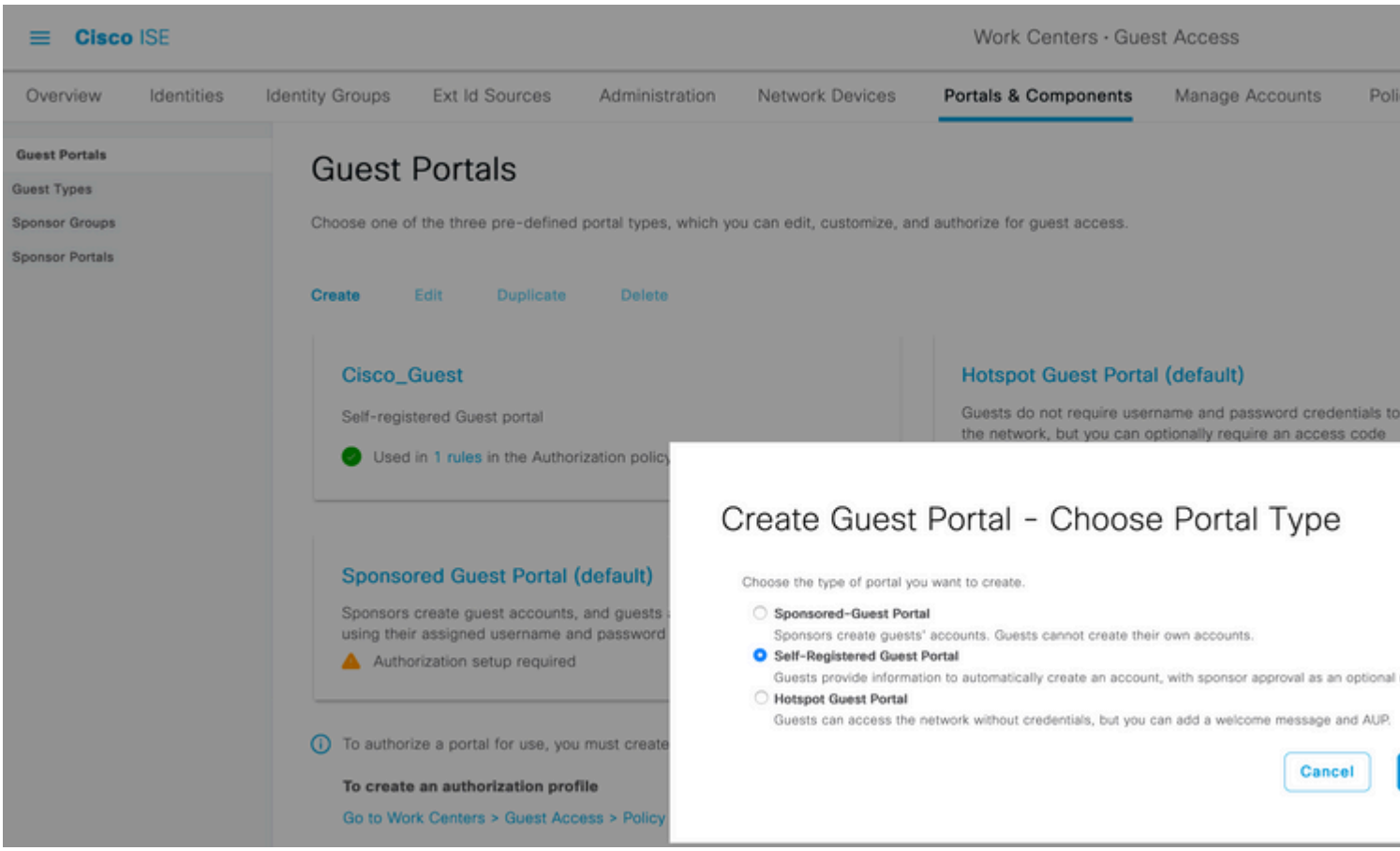
1. Fügen Sie den WLC als Netzwerkzugriffsgerät hinzu, und zwar von **Work Centers > Guest Access > Network Devices aus**.
2. Erstellen einer Endpunkt-Identitätsgruppe Navigieren Sie zu **Work Centers > Guest Access > Identity Groups > Endpoint Identity Groups.**



3. Erstellen Sie einen Gasttyp, indem Sie zu **Work Centers > Guest Access > Portal & Components > Guest Types** navigieren**.** Weitere Informationen finden Sie unter diesem neuen Gasttyp und unter Speichern unter der zuvor erstellten Endpoint Identity Group.



4. Erstellen Sie einen neuen Gastportaltyp: Selbst registriertes Gastportal. Navigieren Sie zu **Work Centers > Guest Access > Guest Portals.**

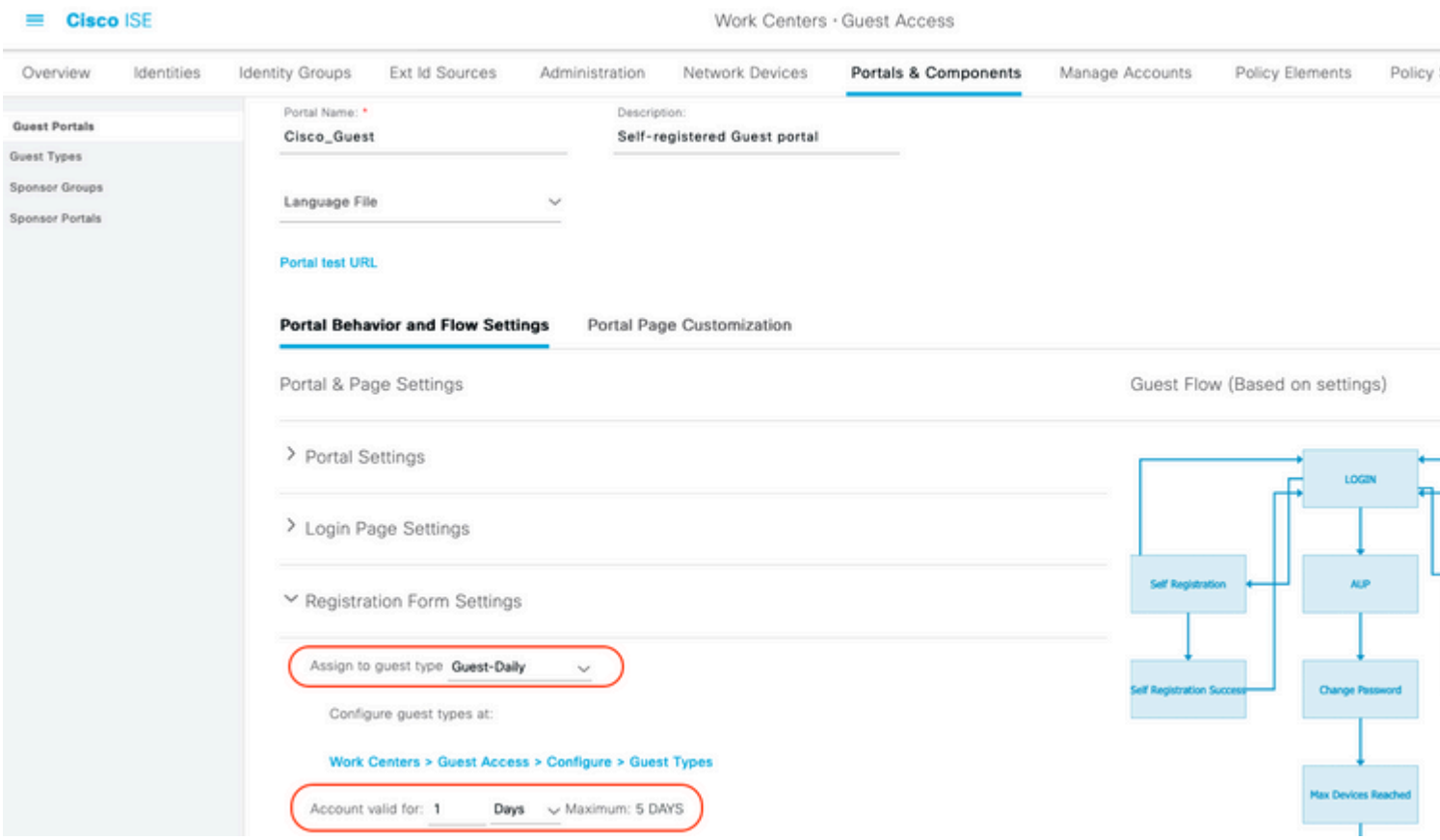


5. Wählen Sie den Portalnamen aus, lesen Sie den zuvor erstellten Gasttyp, und senden Sie die Benachrichtigungseinstellungen unter Registrierungsformular, um die Anmeldeinformationen per E-Mail zu senden.

In diesem Dokument wird beschrieben, wie Sie den SMTP-Server auf der ISE konfigurieren:

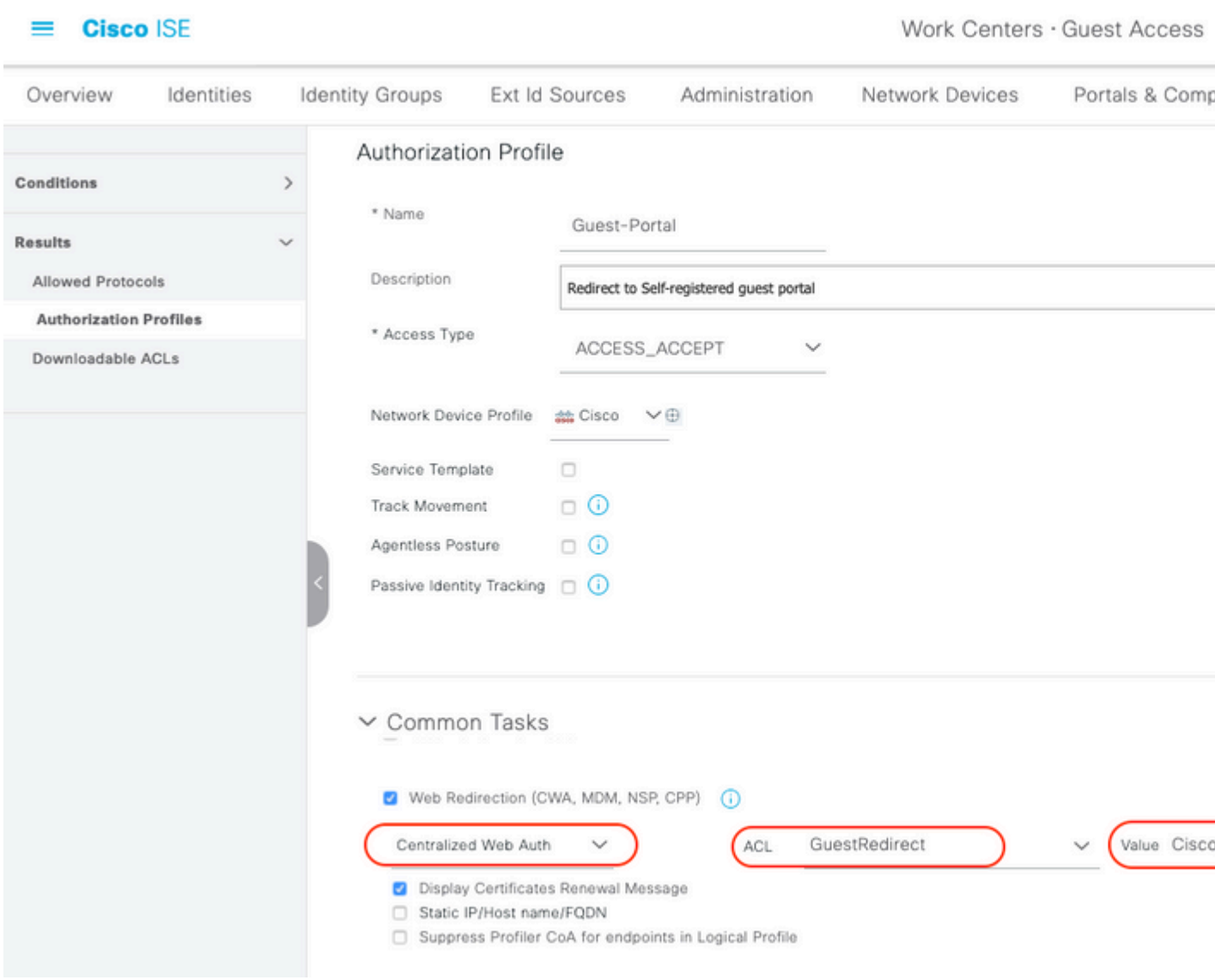
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216187-configure-secure-smtp-server-on-ise.html

Lassen Sie alle anderen Einstellungen auf dem Standardwert. Unter Portalseitenanpassung können alle präsentierten Seiten angepasst werden. Das Gastkonto ist standardmäßig für einen Tag gültig und kann auf die Anzahl der Tage erweitert werden, die für den jeweiligen Gasttyp konfiguriert wurden.

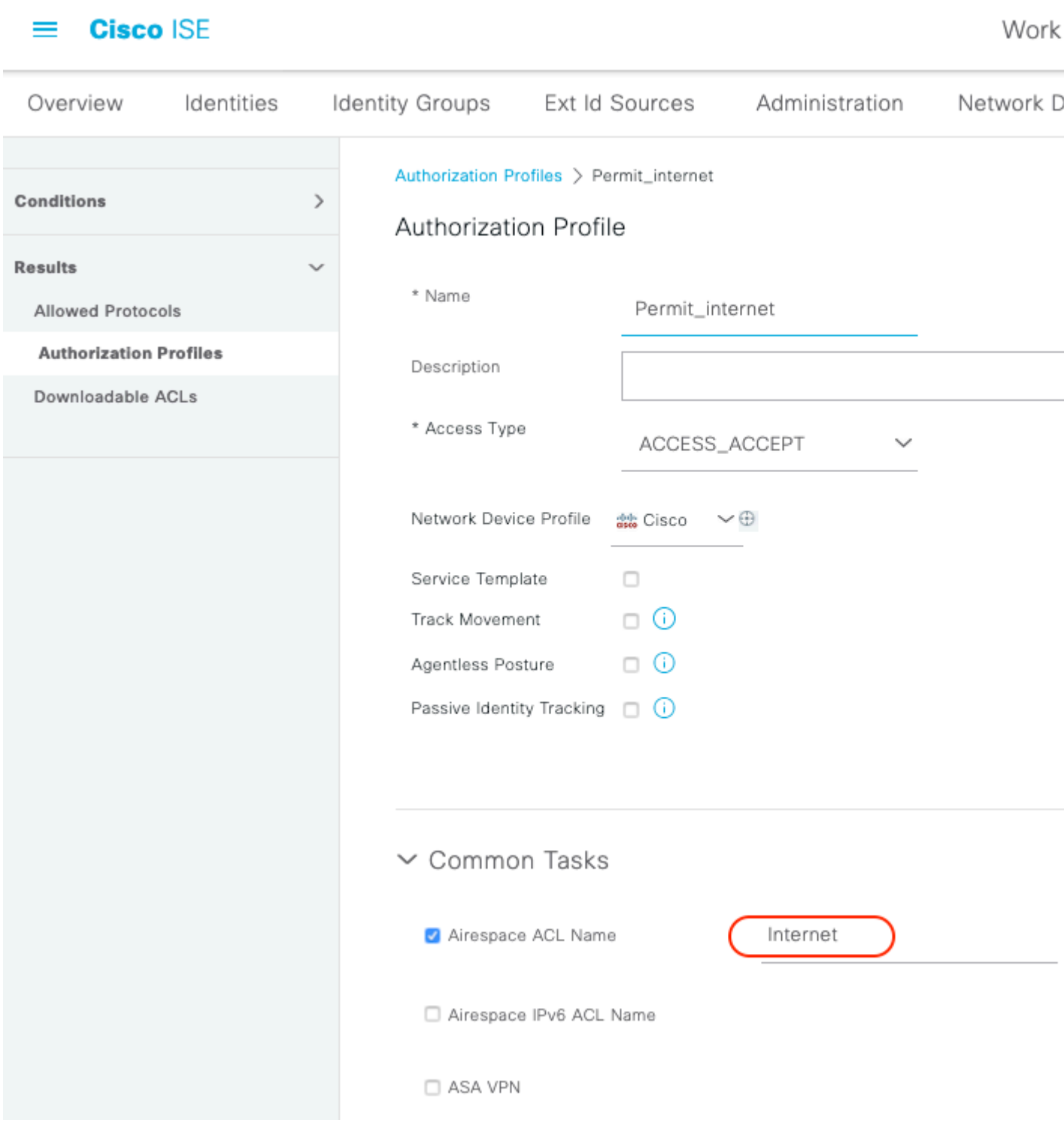


6. Konfigurieren Sie diese beiden Autorisierungsprofile durch Navigieren zu **Work Centers > Guest Access > Policy Elements > Results > Authorization Profiles (Arbeitscenter > Gastzugriff > Richtlinienelemente > Autorisierungsprofile).**

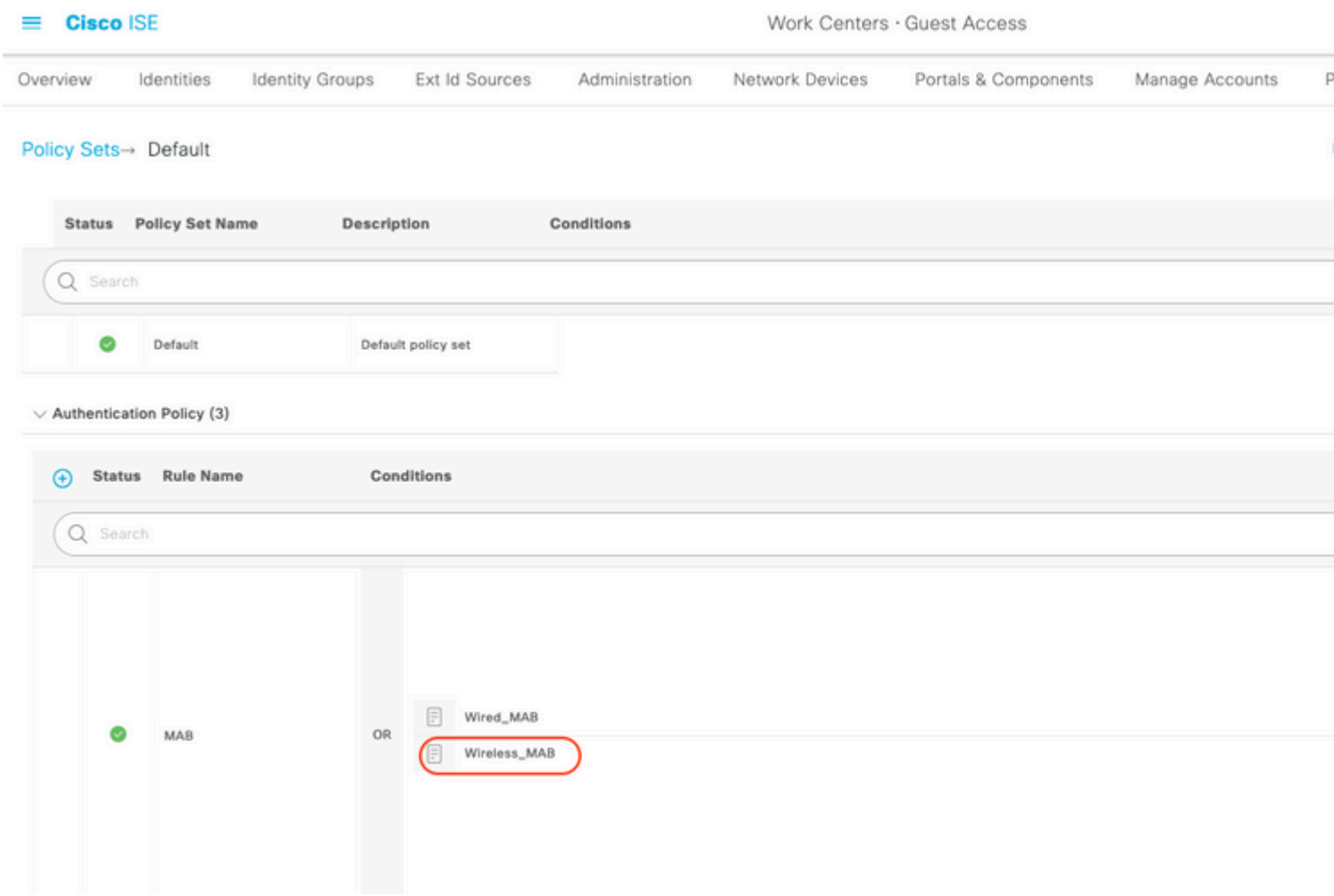
- Guest-Portal (mit Umleitung zum Guest-Portal **Cisco_Guest** und einer Redirect ACL namens **GuestRedirect**). Diese GuestRedirect ACL wurde zuvor auf WLC erstellt.



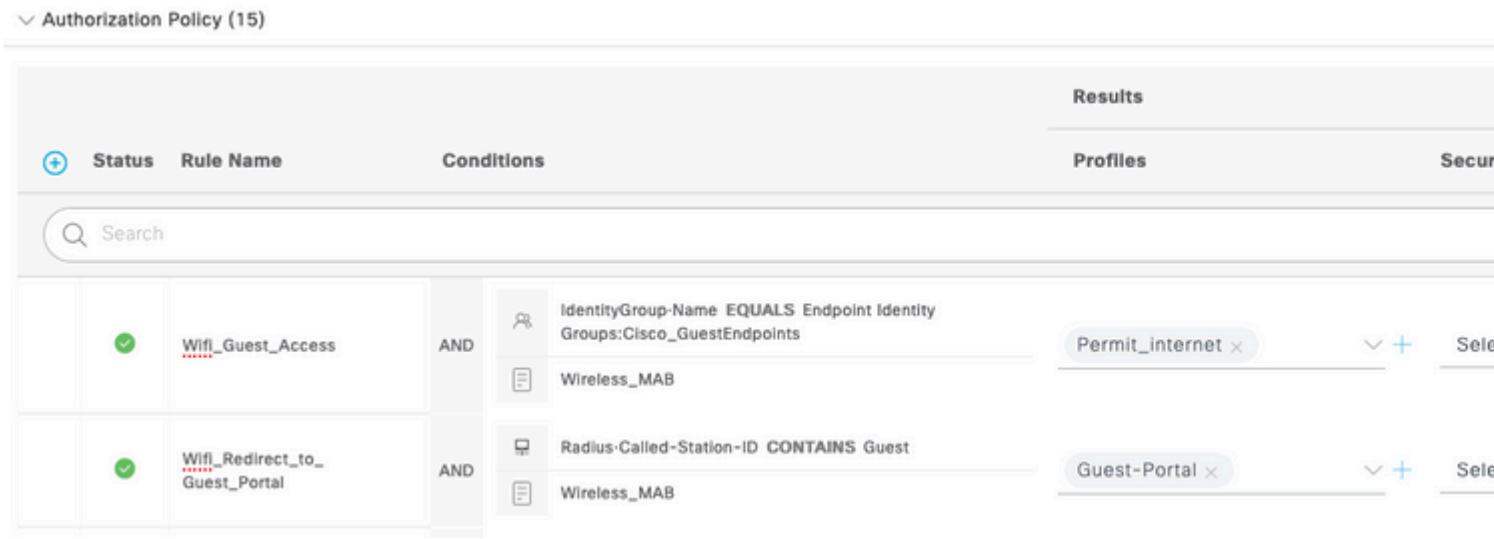
- Permit_Internet (mit Airespace ACL gleich Internet)



7. Ändern Sie den Richtliniensatz mit dem Namen Standard. Der Standardrichtliniensatz ist für den Gastportalzugriff vorkonfiguriert. Eine **Authentifizierungsrichtlinie** mit dem Namen MAB ist vorhanden, die es ermöglicht, die MAB-Authentifizierung (MAC Authentication Bypass) für unbekannte MAC-Adressen fortzusetzen (nicht abzulehnen).



8. Navigieren Sie auf derselben Seite zur **Autorisierungsrichtlinie**. Erstellen Sie diese Autorisierungsregeln, wie in diesem Bild dargestellt.

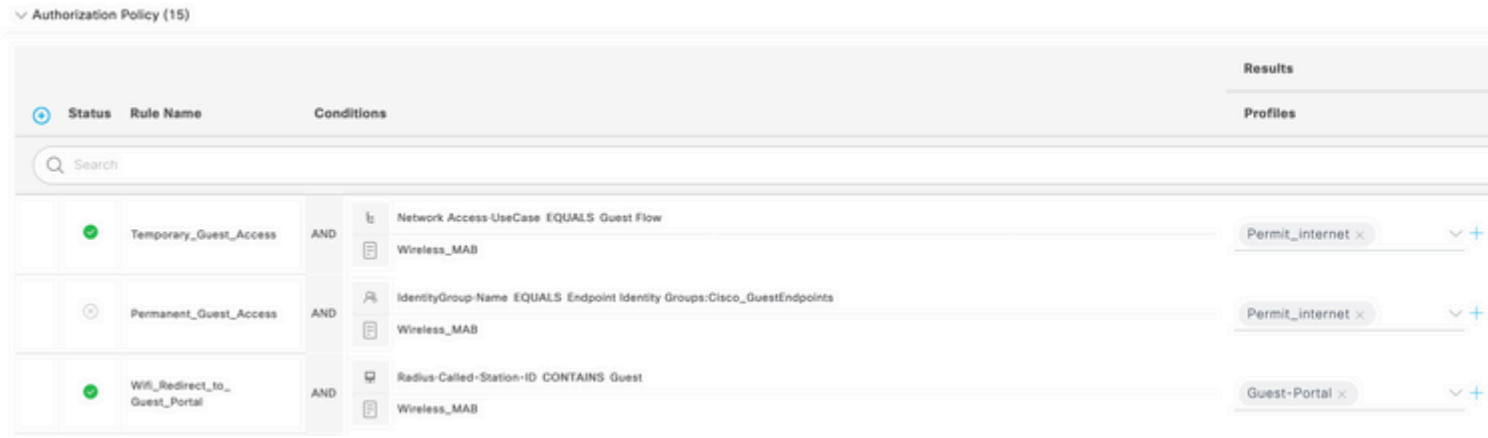


Neue Benutzer, die der Gast-SSID zugeordnet werden, sind noch nicht Teil einer Identitätsgruppe und entsprechen daher der zweiten Regel und werden zum Gastportal weitergeleitet.

Nachdem sich der Benutzer erfolgreich angemeldet hat, sendet die ISE eine RADIUS-CoA, und der WLC führt eine erneute Authentifizierung durch. Diesmal wird die erste Autorisierungsregel zugeordnet (wenn der Endpunkt Teil einer definierten Endpunkt-Identitätsgruppe wird), und der Benutzer erhält das

Permit_internet-Autorisierungsprofil.

9. Wir können auch temporären Zugriff für die Gäste bereitstellen, indem wir die Bedingung Guest flow verwenden. Diese Bedingung prüft aktive Sitzungen auf der ISE und wird zugewiesen. Wenn diese Sitzung über das Attribut verfügt, das angibt, dass der zuvor authentifizierte Gastbenutzer erfolgreich authentifiziert wurde, wird die Bedingung abgeglichen. Nachdem die ISE die RADIUS Accounting Stopp-Nachricht vom Netzwerkzugriffsgerät (Network Access Device, NAD) erhalten hat, wird die Sitzung beendet und später entfernt. Zu diesem Zeitpunkt ist die Bedingung "Network Access:UseCase = Guest Flow" nicht mehr erfüllt. Das Ergebnis: Alle nachfolgenden Authentifizierungen dieses Endpunkts treffen auf die generische Regelumleitung für die Gastauthentifizierung.



> **Hinweis**: Sie können entweder den temporären Gastzugriff oder den permanenten Gastzugriff, aber nicht beides verwenden.

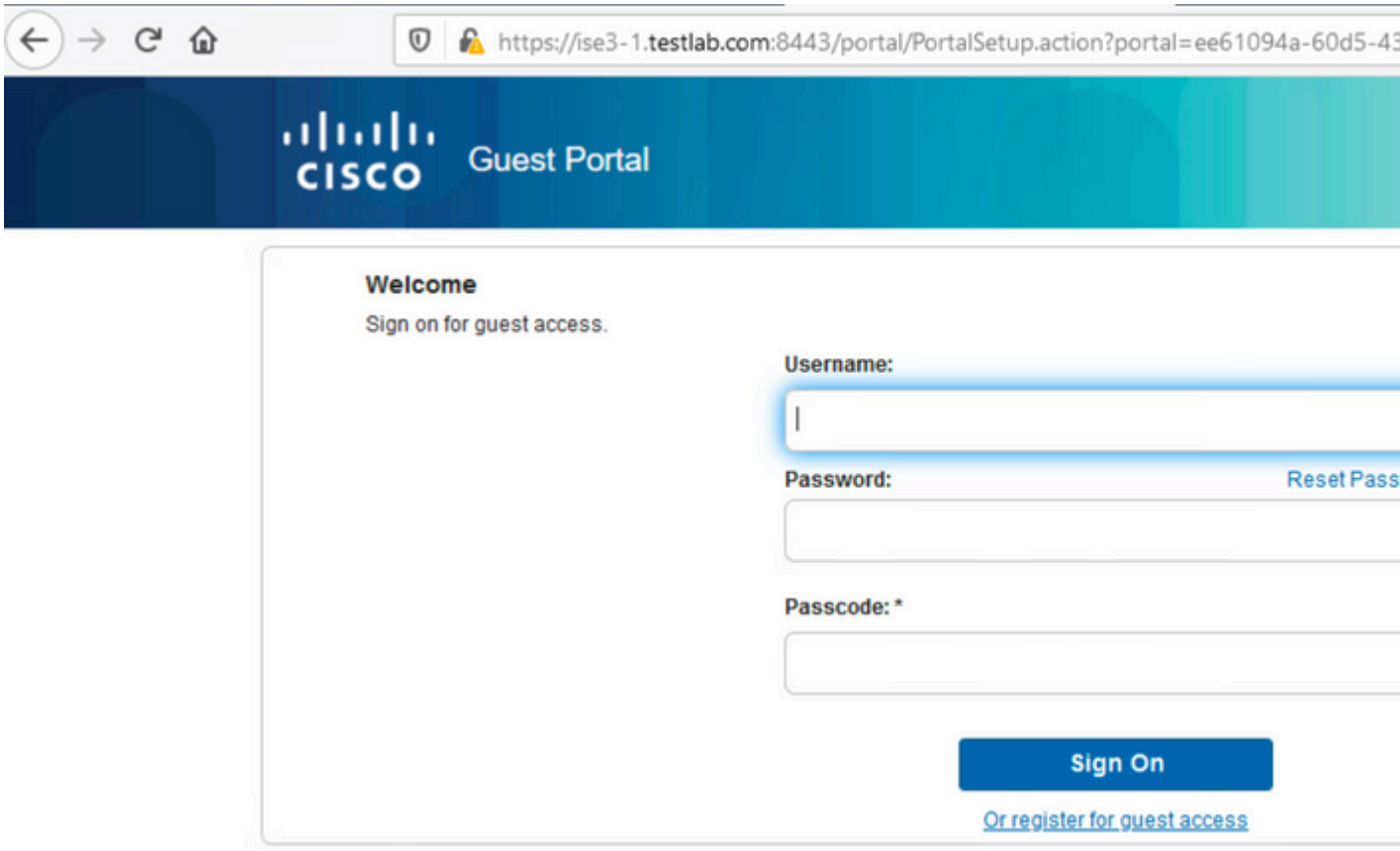
Detaillierte Informationen zur Konfiguration des temporären und permanenten ISE-Gastzugriffs finden Sie in diesem Dokument.

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200273-Configure-ISE-Guest-Temporary-and-Perman.html

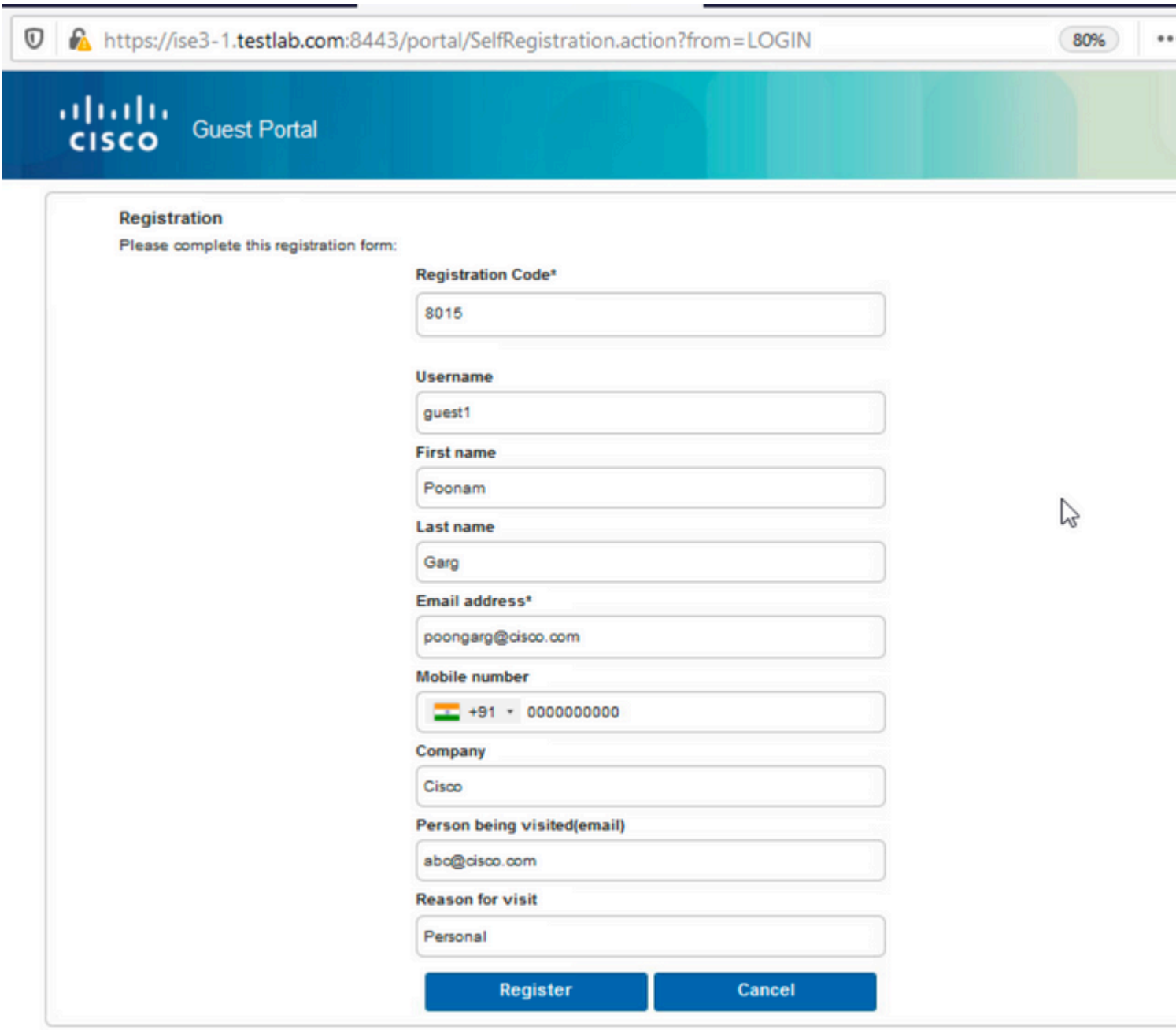
Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

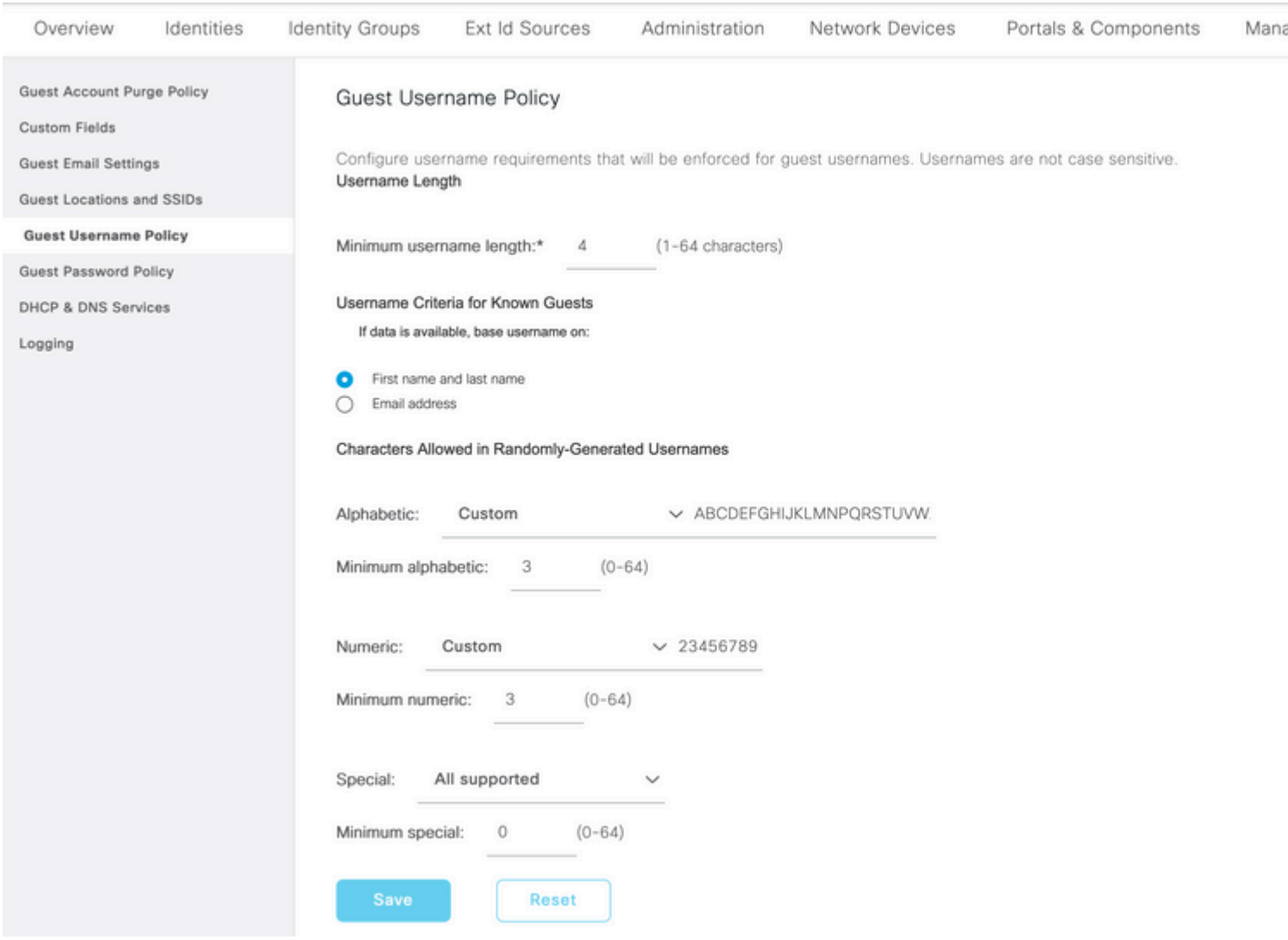
1. Nachdem Sie eine Zuordnung zur Gast-SSID vorgenommen und eine URL eingegeben haben, werden Sie, wie im Bild dargestellt, zur Seite "Guest Portal" weitergeleitet.



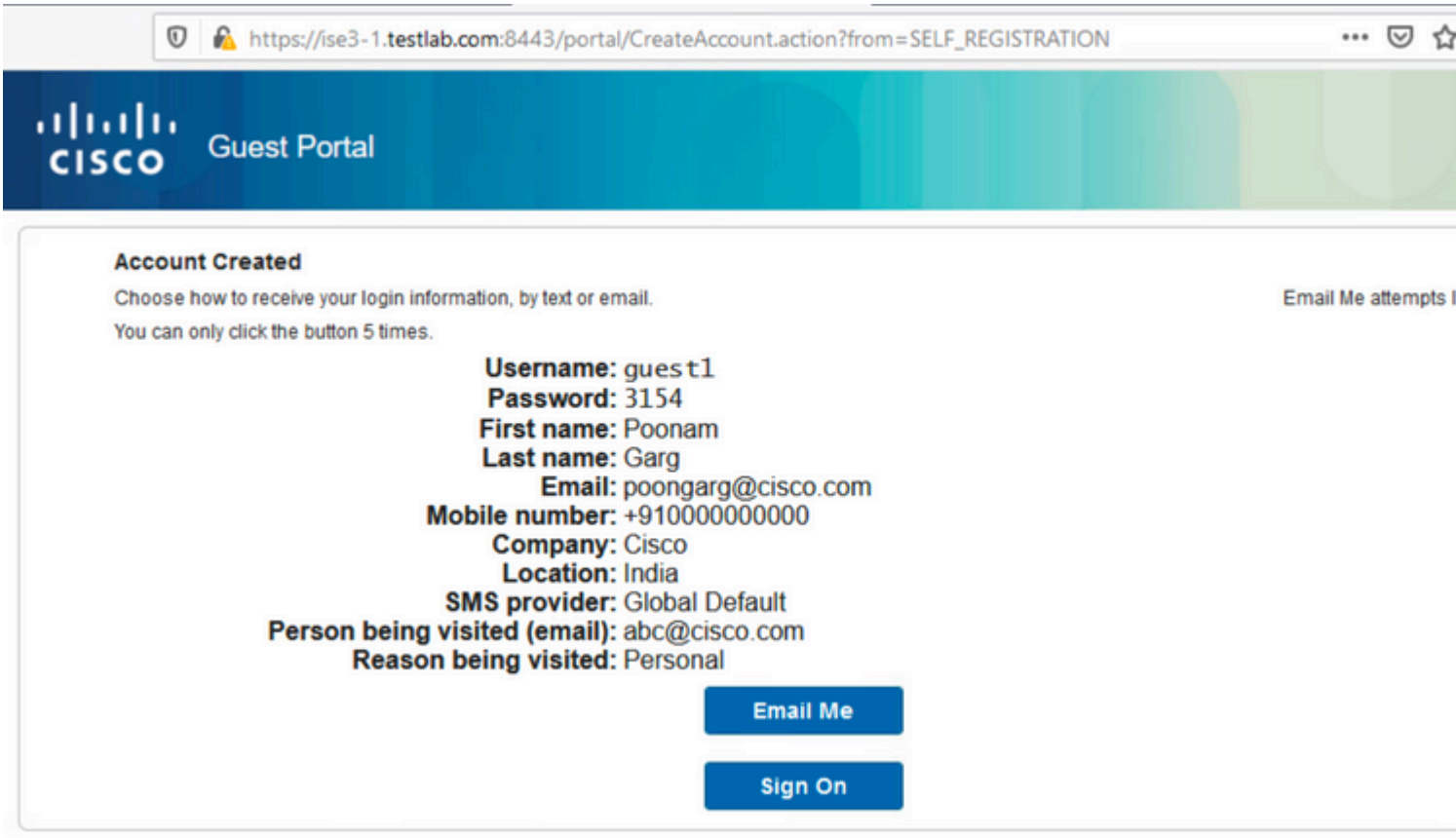
2. Da Sie noch keine Anmeldeinformationen besitzen, müssen Sie die Option **Für Gastzugriff registrieren** auswählen. Sie erhalten das Registrierungsformular, um das Konto zu erstellen. Wenn die Option Registrierungscode in der Konfiguration des Gastportals aktiviert wurde, ist dieser geheime Wert erforderlich (dadurch wird sichergestellt, dass sich nur Personen mit den richtigen Berechtigungen selbst registrieren können).

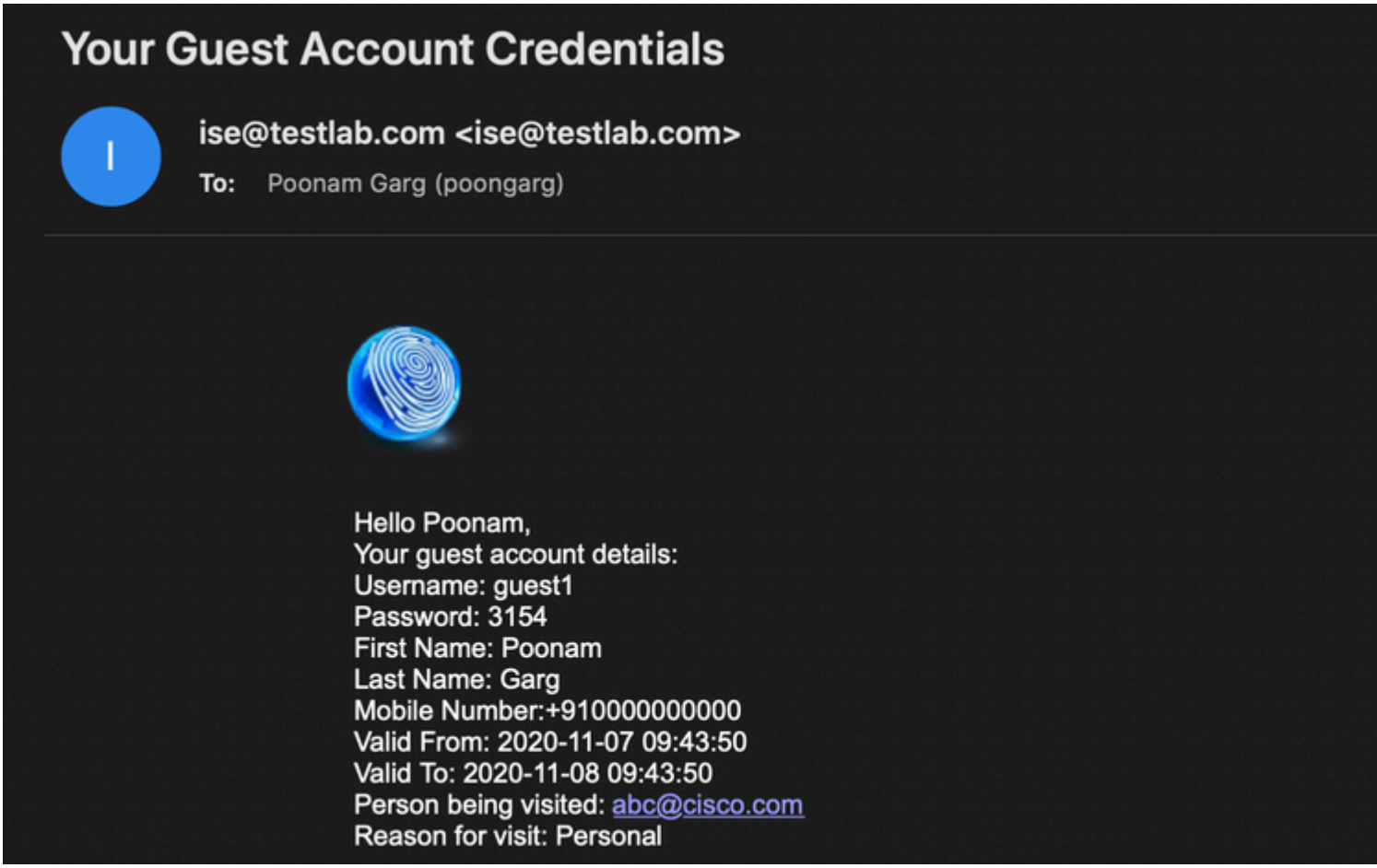


3. Falls Probleme mit dem Kennwort oder der Benutzerrichtlinie auftreten, navigieren Sie zu **Work Centers > Guest Access > Settings > Guest Username Policy,** um die Einstellungen zu ändern. Hier ein Beispiel:



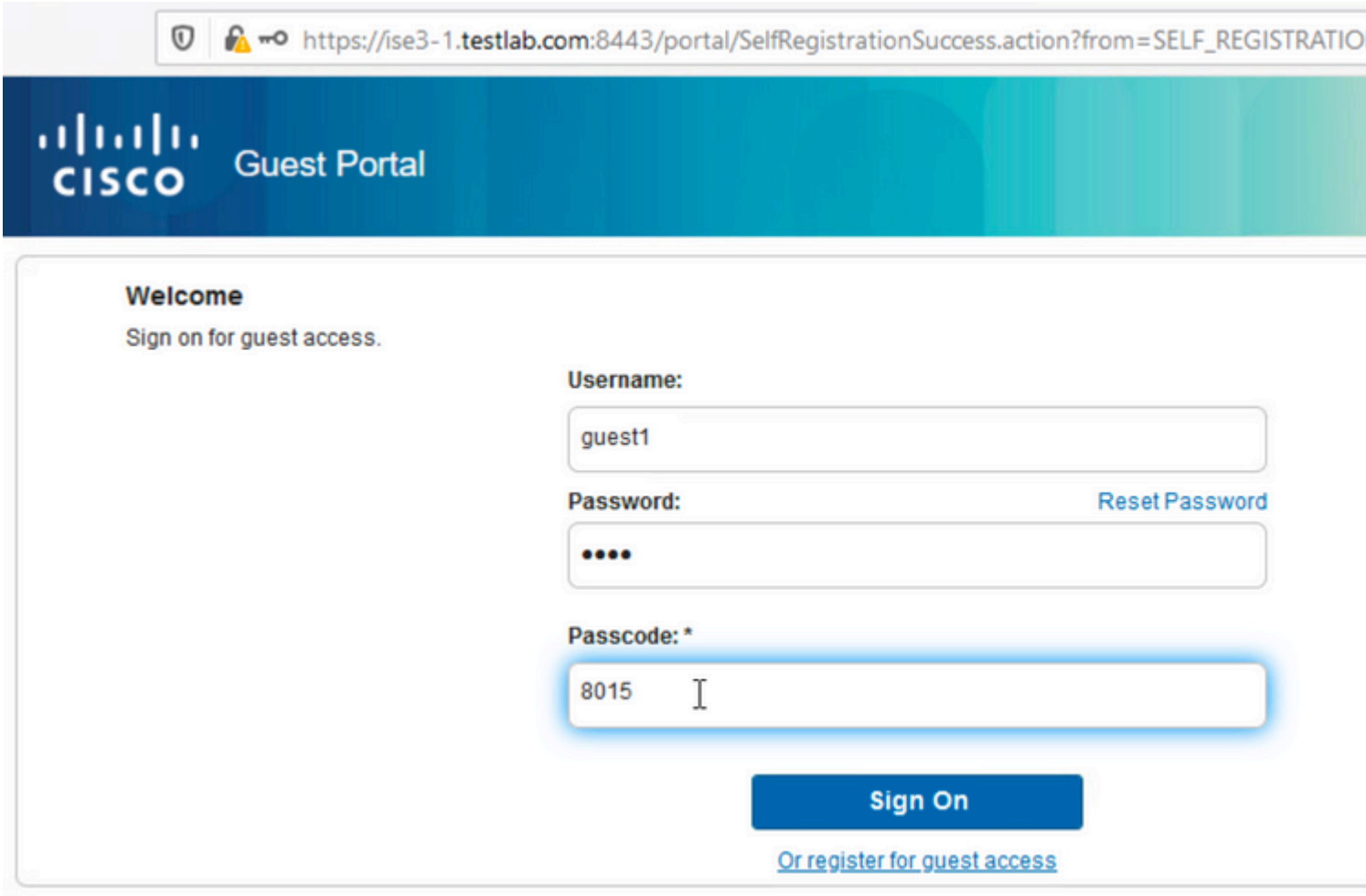
4. Nach der erfolgreichen Kontoerstellung werden Ihnen die Anmeldeinformationen angezeigt (das Kennwort wird gemäß den Richtlinien für das Gastkennwort generiert). Auch Gastbenutzer erhalten die E-Mail-Benachrichtigung, wenn sie konfiguriert sind:



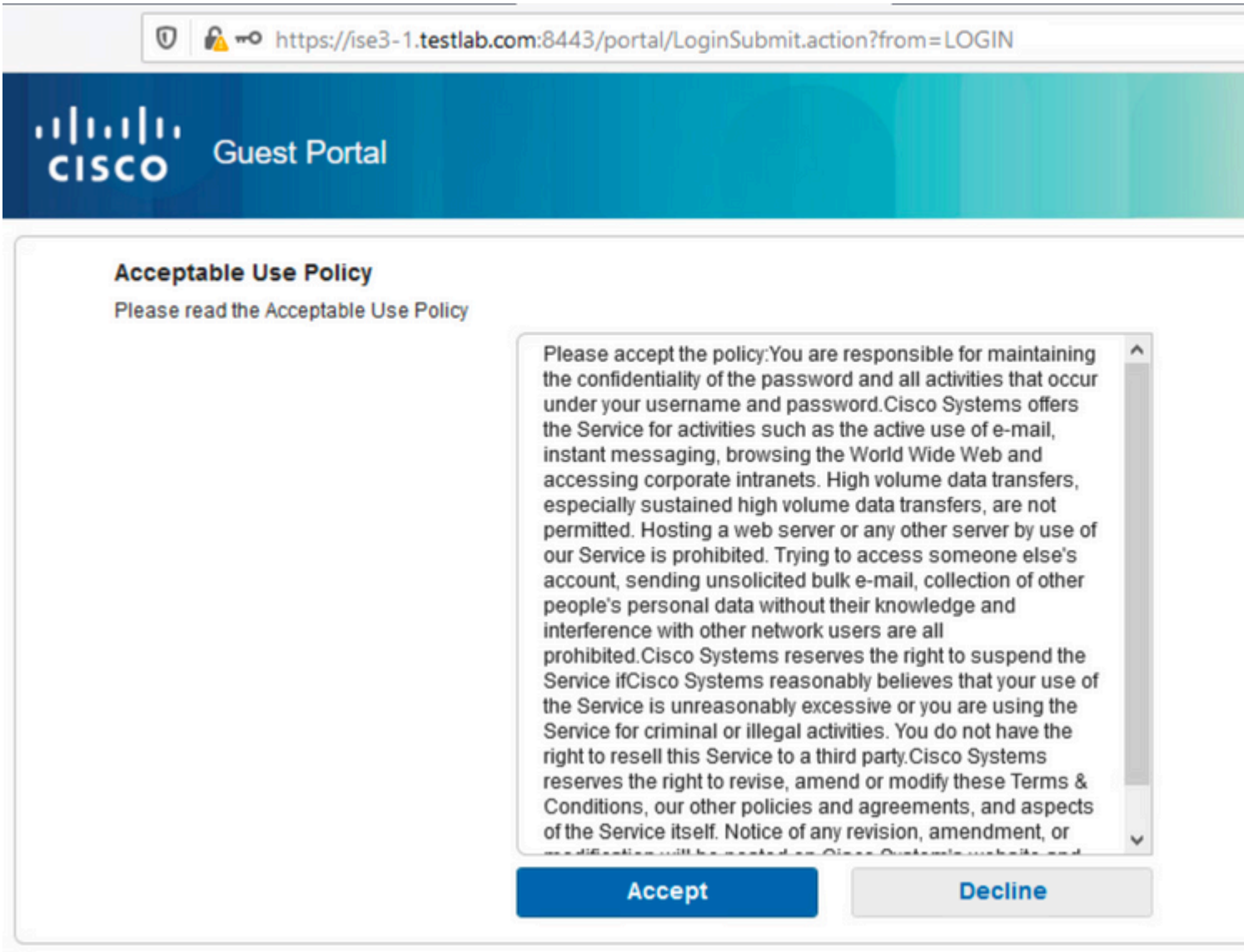


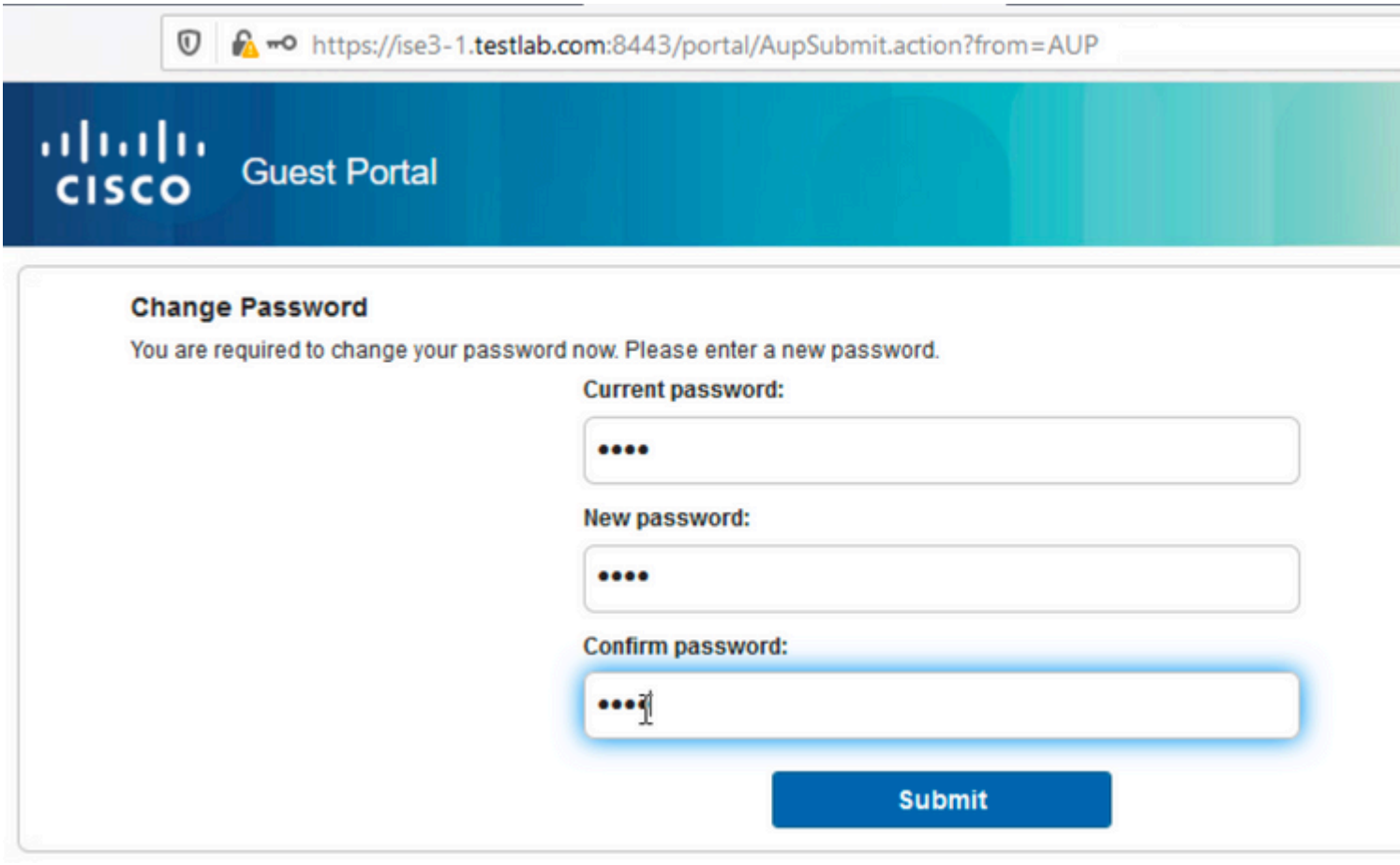
5. Klicken Sie auf **Sign On (Anmelden)** und geben Sie Ihre Anmeldeinformationen an (ein zusätzlicher Zugriffs-Passcode kann erforderlich sein, wenn er unter dem Gastportal konfiguriert wurde; dies ist ein

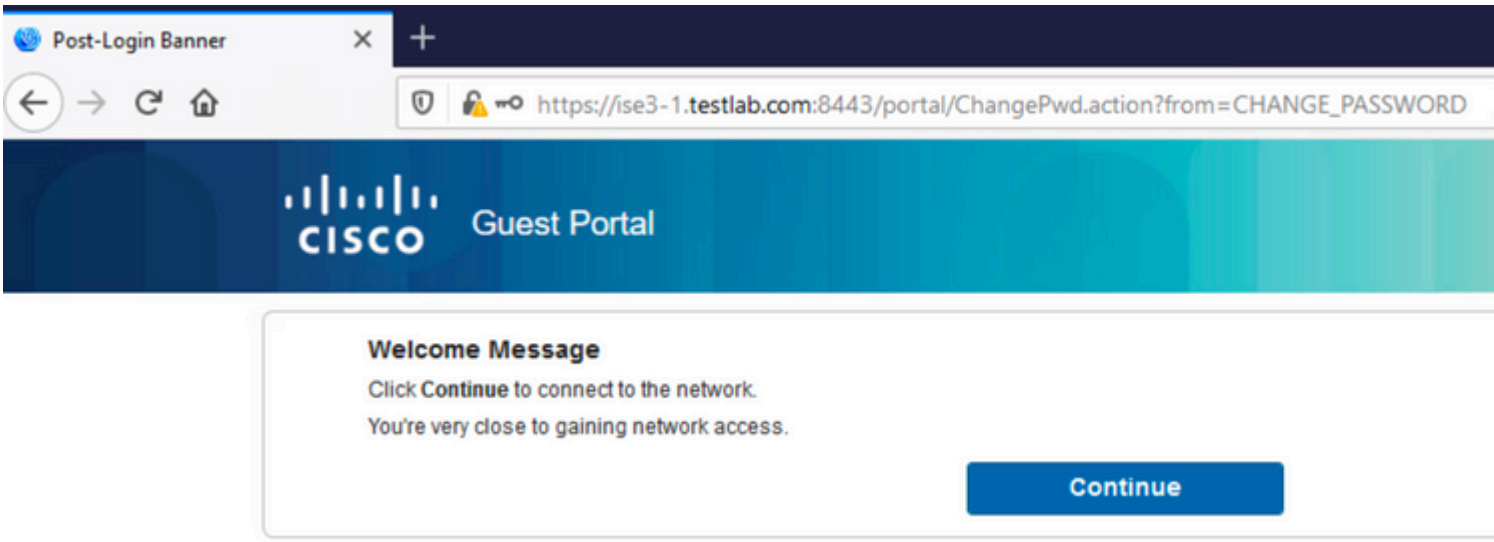
weiterer Sicherheitsmechanismus, der nur Personen, die das Passwort kennen, erlaubt, sich anzumelden).



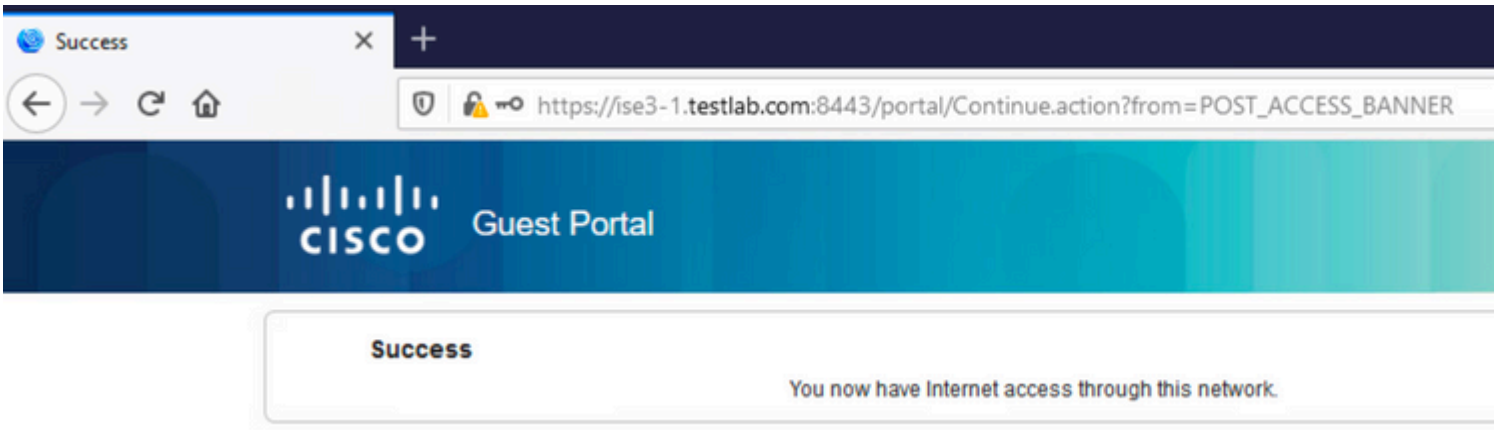
6. Bei erfolgreicher Anmeldung kann eine optionale Richtlinie für akzeptable Nutzung (AUP) angezeigt werden (sofern diese im Gastportal konfiguriert wurde). Dem Benutzer wird die Option zum Ändern des Kennworts angezeigt, und das Banner nach der Anmeldung (das auch unter "Guest Portal" konfiguriert werden kann) kann ebenfalls angezeigt werden.


https://ise3-1.testlab.com:8443/portal/LoginSubmit.action?from=LOGIN
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





7. Die letzte Seite (Post-Login Banner) bestätigt, dass der Zugang gewährt wurde:



Fehlerbehebung

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

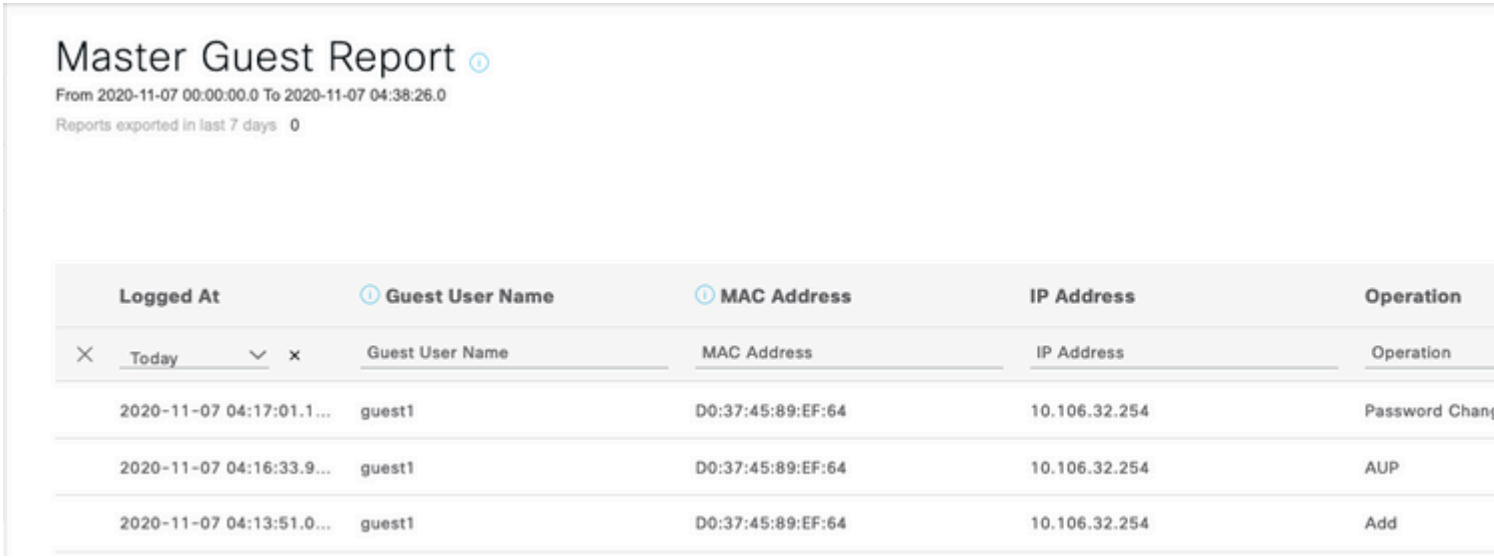
Zu diesem Zeitpunkt werden die Protokolle von der ISE unter **Operations > RADIUS > Live Logs (Betrieb > RADIUS > Live-Protokolle**) angezeigt, wie im Bild dargestellt.

Time	Status	Details	Identity	Endpoint ID	Authenticat...	Authorization Policy	Authorization P...	IP Address
			Identity	Endpoint ID	Authentication	Authorization Policy	Authorization Profile	IP Address
Nov 07, 2020 04:17:32.46...			guest1	D0:37:45:89:EF:64	Default	Default >> Permanent_Guest_Access	Permit_internet	10.106.32.2...
Nov 07, 2020 04:17:32.42...			guest1	D0:37:45:89:EF:64	Default	Default >> Permanent_Guest_Access	Permit_internet	
Nov 07, 2020 04:17:32.39...				D0:37:45:89:EF:64				
Nov 07, 2020 04:16:14.85...			guest1	D0:37:45:89:EF:64				10.106.32.2...
Nov 07, 2020 03:43:30.75...			D0:37:45:89:EF:64	D0:37:45:89:EF:64	Default >> MAB	Default >> Wifi_Redirect_to_ Guest_Portal	Guest-Portal	

Der Ablauf ist wie folgt:

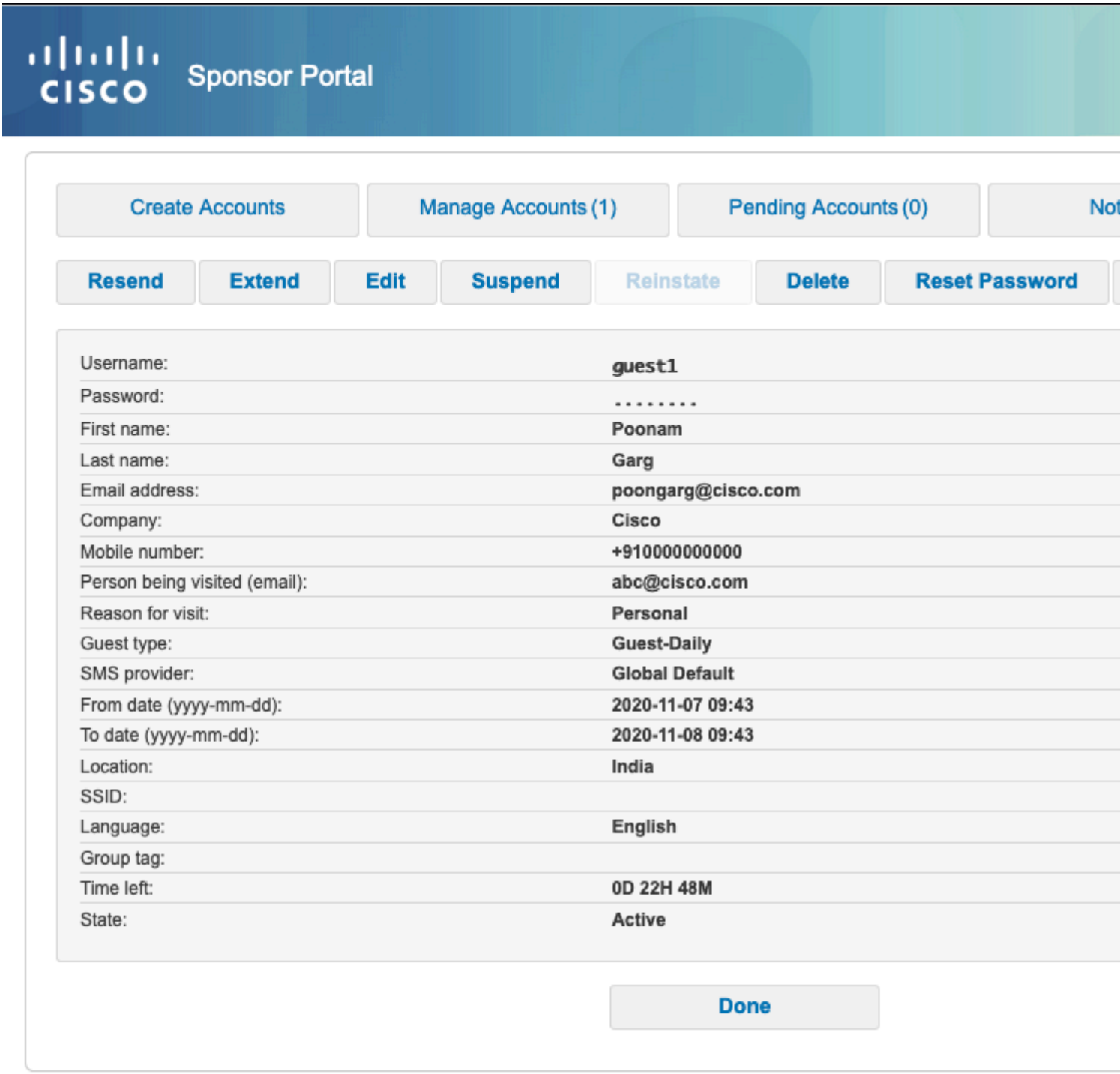
- Der Gastbenutzer erhält die zweite Autorisierungsregel (Wifi_Redirect_to_Guest_Portal) und wird zum Gastportal umgeleitet (**Authentifizierung erfolgreich**).
- Der Gast wird zur Selbstregistrierung weitergeleitet. Nach erfolgreicher Anmeldung (mit dem neu erstellten Konto) sendet die ISE die CoA-Reauthentifizierung, die vom WLC bestätigt wird (**dynamische Autorisierung erfolgreich**).
- Der WLC führt eine erneute Authentifizierung mit dem Authorize-Only-Attribut durch, und der ACL-Name wird zurückgegeben (**Authorize-Only war erfolgreich**). Dem Gast wird der richtige Netzwerkzugriff gewährt.

Berichte (**Betrieb > Berichte > Gast > Master Guest Report**) bestätigen außerdem Folgendes:



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

In diesem Beispiel wird bestätigt, dass das Konto erstellt wurde und der Benutzer beim Portal angemeldet wurde:



Optionale Konfiguration

Für jede Phase dieses Ablaufs können verschiedene Optionen konfiguriert werden. All dies wird über das Gastportal unter **Work Centers > Guest Access > Portals & Components > Guest Portals > Portal Name > Edit > Portal Behavior and Flow Settings** konfiguriert. Wichtigere Einstellungen sind:

Einstellungen für die Selbstregistrierung

- Gasttyp - Beschreibt die Dauer der Aktivität des Kontos, Optionen zum Ablauf des Kennworts, Anmeldezeiten und Optionen (dies ist eine Mischung aus Zeitprofil und Gastrolle)
- Registrierungscode - Wenn aktiviert, können sich nur Benutzer, die den geheimen Code kennen, selbst registrieren (bei der Erstellung des Kontos muss das Kennwort eingegeben werden).

- AUP - Nutzungsrichtlinien bei der Selbstregistrierung akzeptieren
- Die Anforderung an den Sponsor, das Gastkonto zu genehmigen/zu aktivieren.

Gasteinstellungen für Anmeldung

- Zugriffscode: Wenn diese Option aktiviert ist, können sich nur Gastbenutzer anmelden, die den geheimen Code kennen.
- AUP - Nutzungsrichtlinien bei der Selbstregistrierung akzeptieren.
- Option zur Kennwortänderung.

Einstellungen für die Geräteregistrierung

- Standardmäßig wird das Gerät automatisch registriert.

Compliance-Einstellungen für Gastgeräte

- Ermöglicht eine Körperhaltung innerhalb des Flusses.

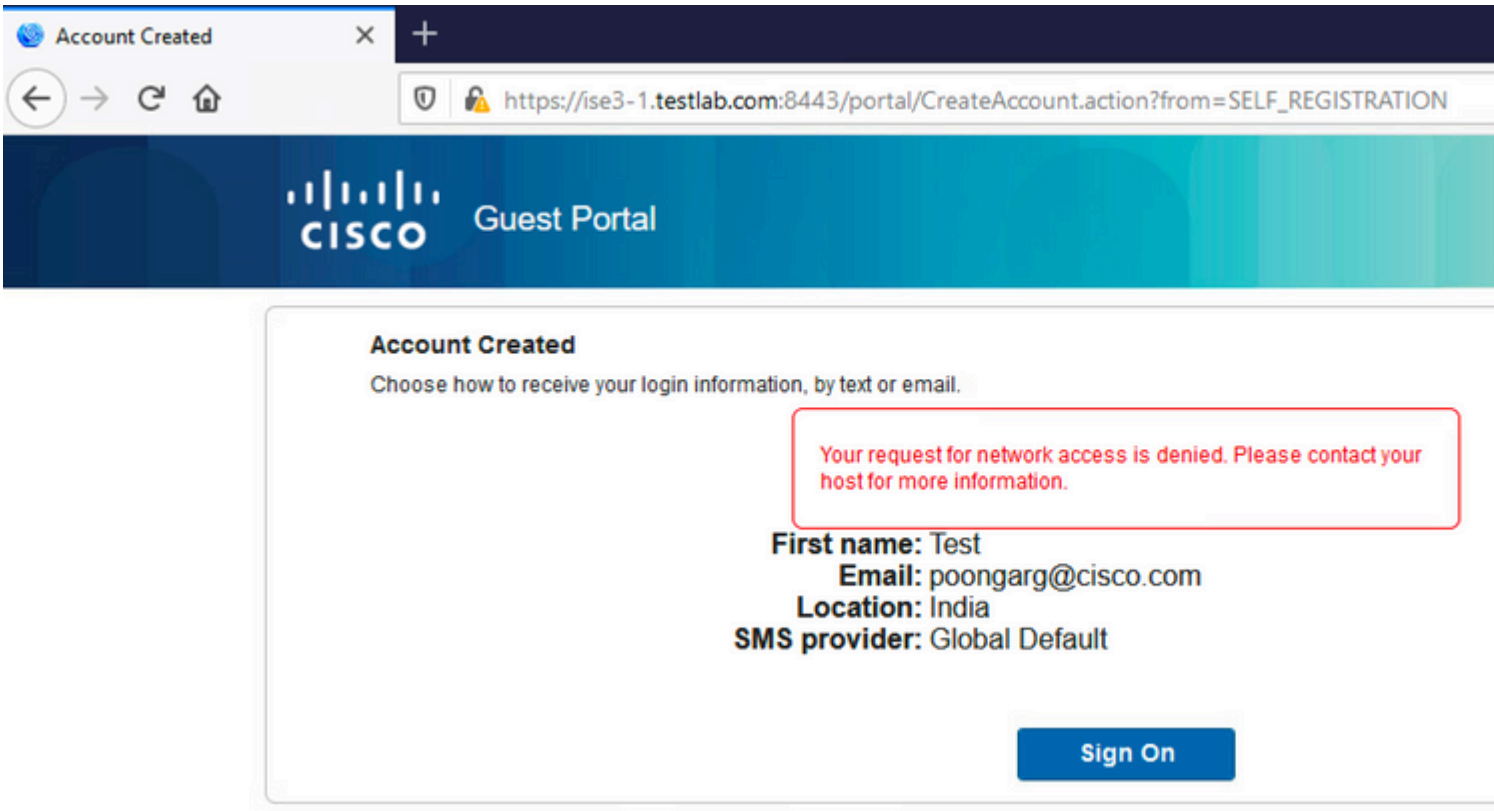
BYOD-Einstellungen

- Benutzer des Unternehmens, die das Portal als Gäste nutzen, können ihre privaten Geräte registrieren.

Vom Sponsor genehmigte Kunden

Wenn die Option **Genehmigung für Gäste erforderlich** unter **Registrierungsformulareinstellungen** ausgewählt ist, muss das vom Gast erstellte Konto von einem Sponsor genehmigt werden. Diese Funktion kann eine E-Mail verwenden, um eine Benachrichtigung an den Sponsor zu senden (zur Genehmigung des Gastkontos):

Wenn der SMTP-Server (Simple Mail Transfer Protocol) falsch konfiguriert ist, wird das Konto nicht erstellt:



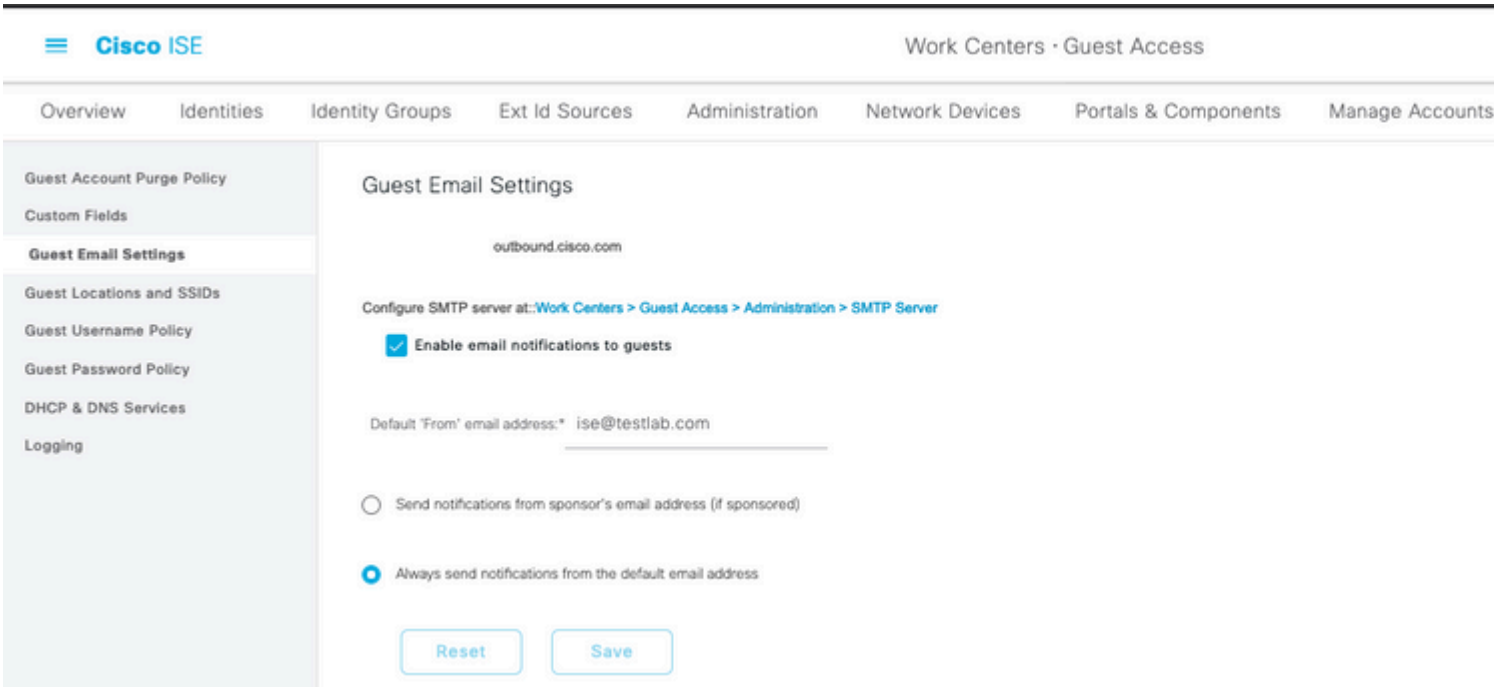
Das Protokoll von guest.log bestätigt, dass beim Senden der Genehmigungsbenachrichtigung an die E-Mail-Adresse des Sponsors ein Problem auftritt, da der SMTP-Server falsch konfiguriert wurde:

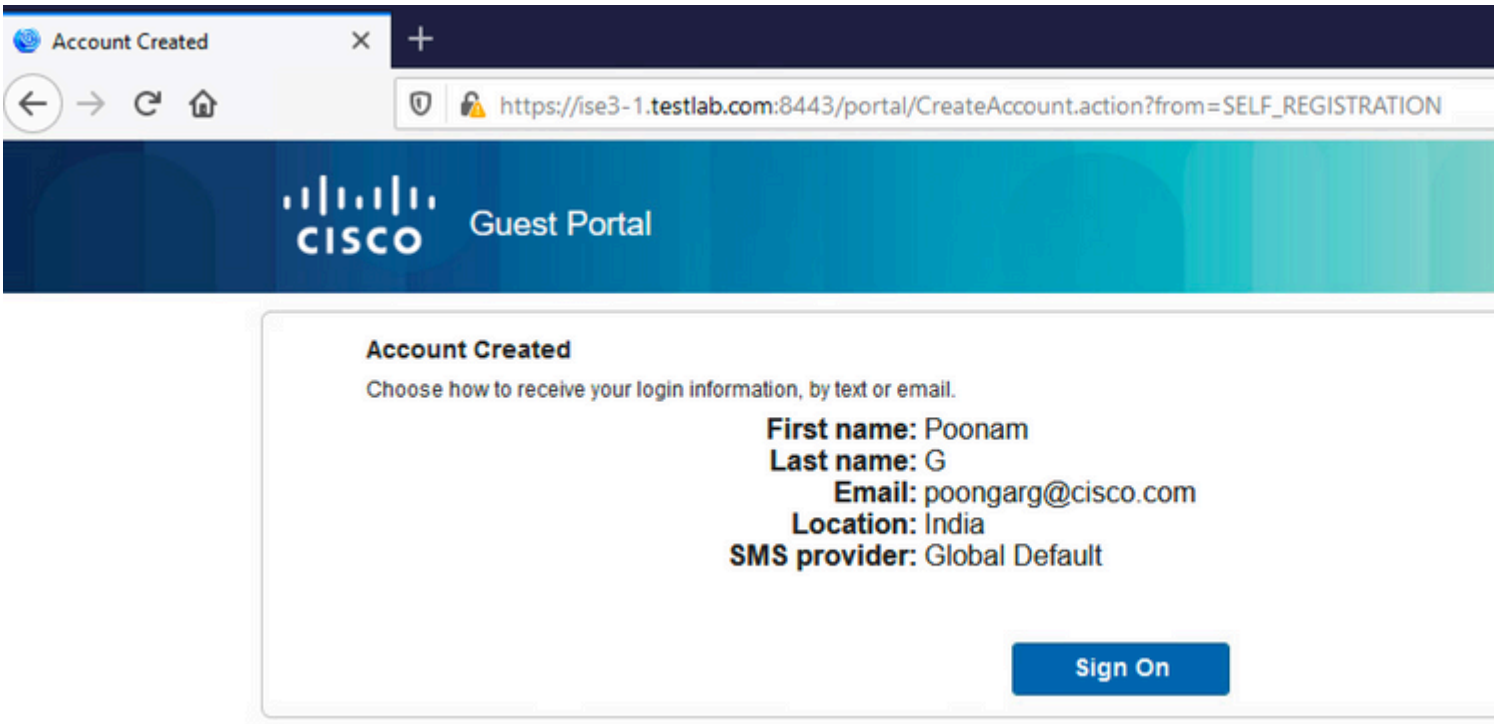
<#root>

```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTP_RETRY_THREAD][] cpm.guestaccess.apiservices.util.SmtpMs
javax.mail.MessagingException: Could not connect to SMTP host: outbound.cicso.com, port: 25, response: 4

2020-11-07 07:16:38,547 ERROR [https-jsse-nio-10.106.32.25-8443-exec-1][] cpm.guestaccess.apiservices.no
com.cisco.cpm.guestaccess.exception.GuestAccessSystemException: com.cisco.cpm.guestaccess.exception.Gues
```

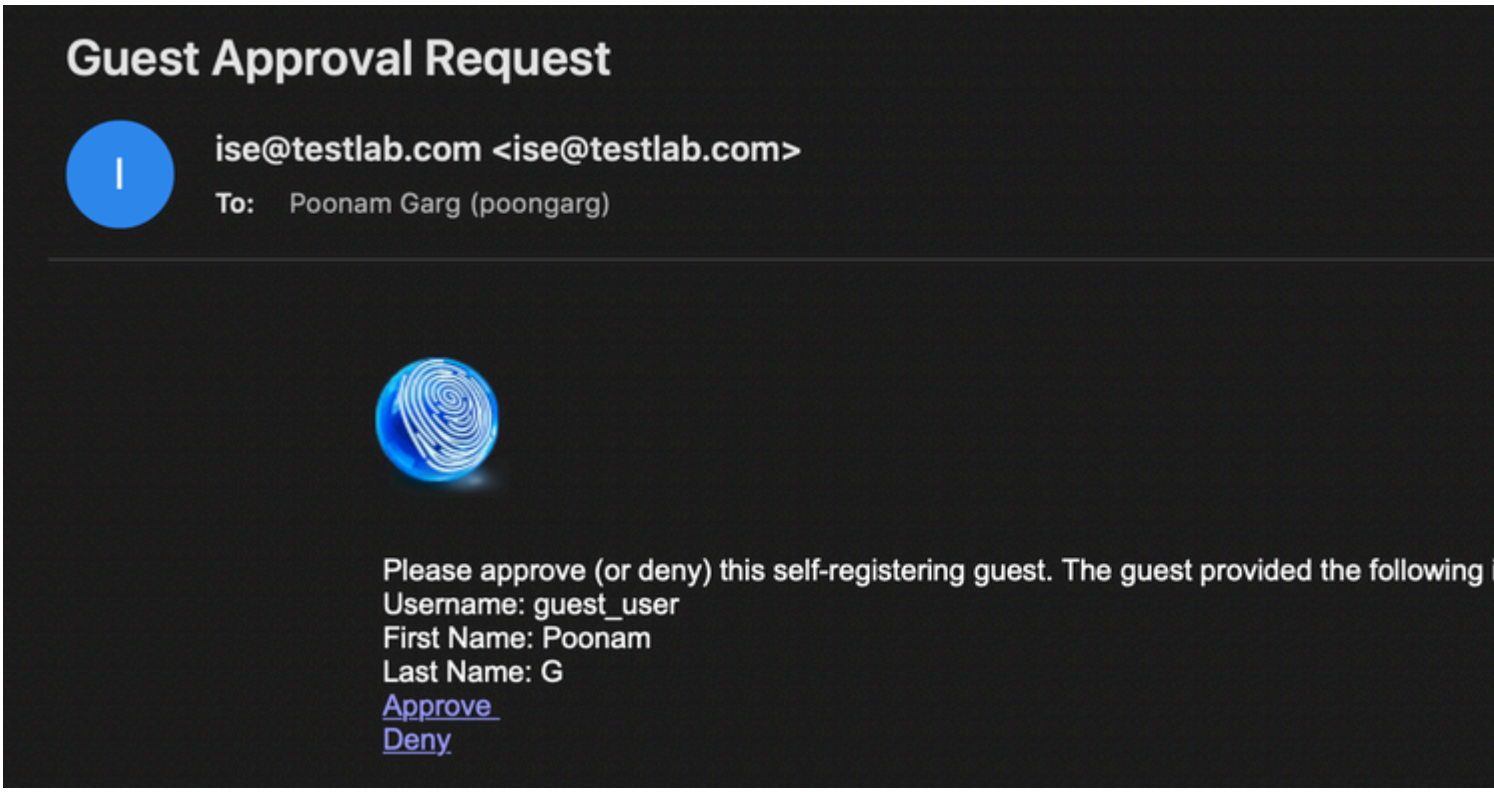
Wenn Sie über die richtige E-Mail- und SMTP-Serverkonfiguration verfügen, wird das Konto erstellt:



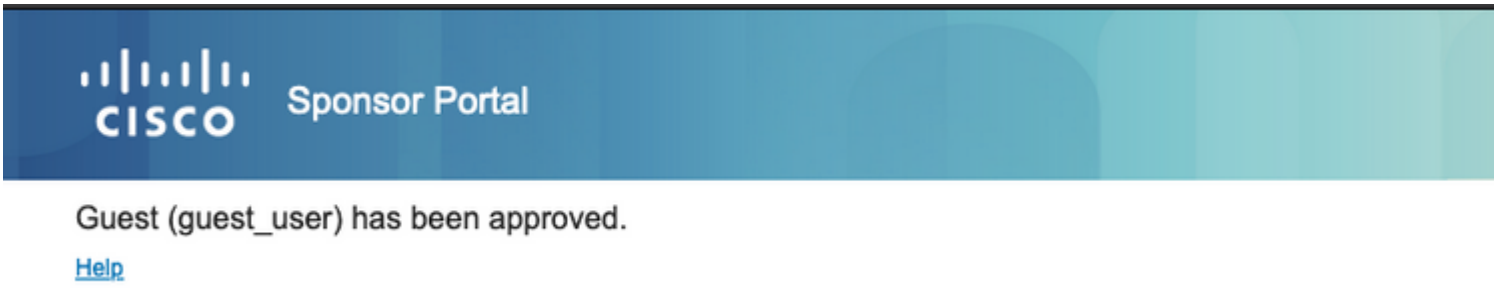


Nachdem Sie die Option **Genehmigung für Gäste anfordern** aktiviert haben, werden die Felder für den Benutzernamen und das Kennwort automatisch aus dem Abschnitt **Diese Informationen auf der Seite Erfolg der Selbstregistrierung einschließen** entfernt. Aus diesem Grund werden Anmeldeinformationen für Gastbenutzer nicht standardmäßig auf der Webseite angezeigt, auf der Informationen zum Erstellen des Kontos angezeigt werden, wenn eine Genehmigung des Sponsors erforderlich ist. Stattdessen müssen sie per SMS oder E-Mail zugestellt werden. Diese Option muss im Abschnitt **Benachrichtigung bei Genehmigung senden über (E**-Mail/SMS markieren) aktiviert werden.

Der Sponsor erhält eine Benachrichtigungs-E-Mail:



Der Sponsor klickt auf den Link "Genehmigung" und meldet sich im Sponsorportal an. Das Konto wurde genehmigt:



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

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

- Benachrichtigungsadresse "Von". Diese wird statisch definiert oder aus dem Sponsorkonto entnommen und als Absenderadresse sowohl für die Benachrichtigung des Sponsors (zur Genehmigung) als auch für die Anmeldeinformationen des Gasts verwendet. Dies wird unter **Work Centers > Guest Access > Settings > Guest Email Settings** konfiguriert.

- "An"-Adresse für Benachrichtigung. Diese wird verwendet, um den Sponsor darüber zu informieren, dass er ein Konto zur Genehmigung erhalten hat. Dies wird im Gastportal unter **Work Centers > Guest Access > Guest Portals > Portals and Components > Portal Name > Registration Form Settings > Require guest to be authorised > Email approval request to (Arbeitscenter > Gastzugriff > Gastportale > Portale und Komponenten > Portalname > Registrierungsformulareinstellungen** konfiguriert.

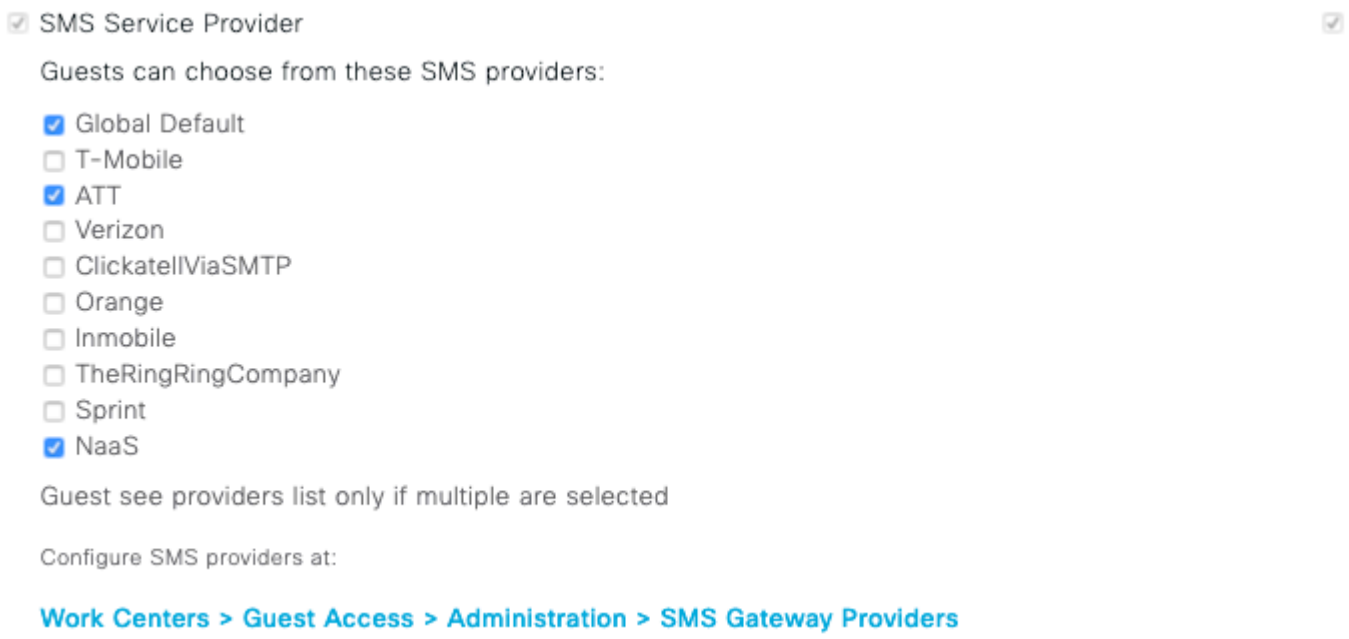
- Gastadresse: Diese wird vom Gastbenutzer während der Registrierung bereitgestellt. Wenn **Benachrichtigung über Anmeldeinformationen bei Genehmigung per E-Mail senden** ausgewählt

ist, wird die E-Mail mit Anmeldeinformationen (Benutzername und Kennwort) an den Gast gesendet.

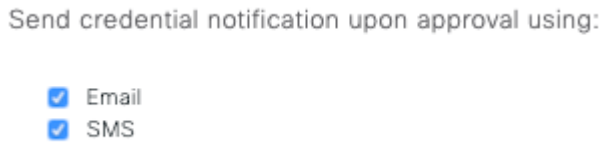
Übermittlung von Anmeldeinformationen per SMS

Gast-Anmeldedaten können auch per SMS zugestellt werden. Diese Optionen müssen konfiguriert werden:

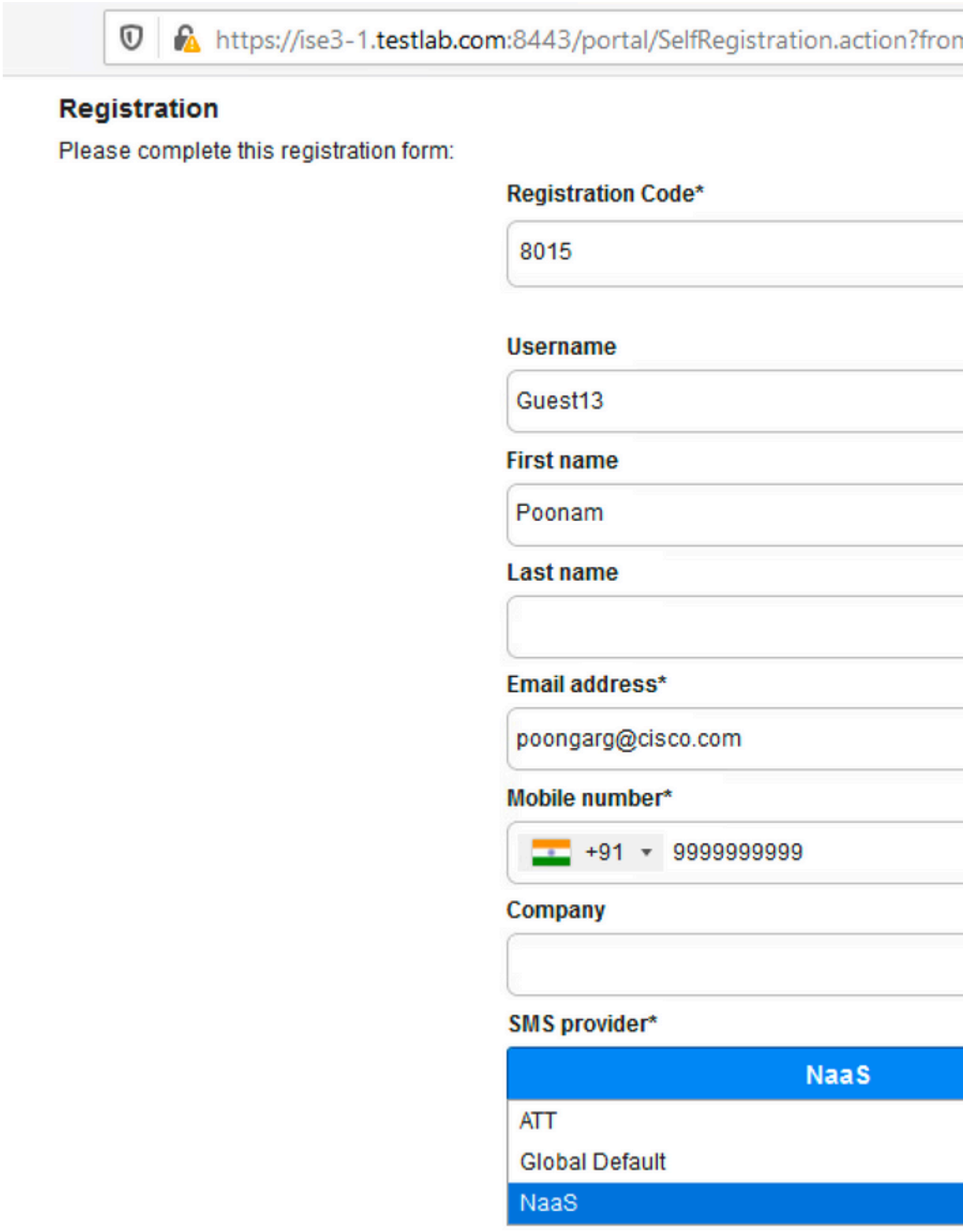
1. Wählen Sie unter Registrierungsformulareinstellungen den SMS-Dienstanbieter aus:



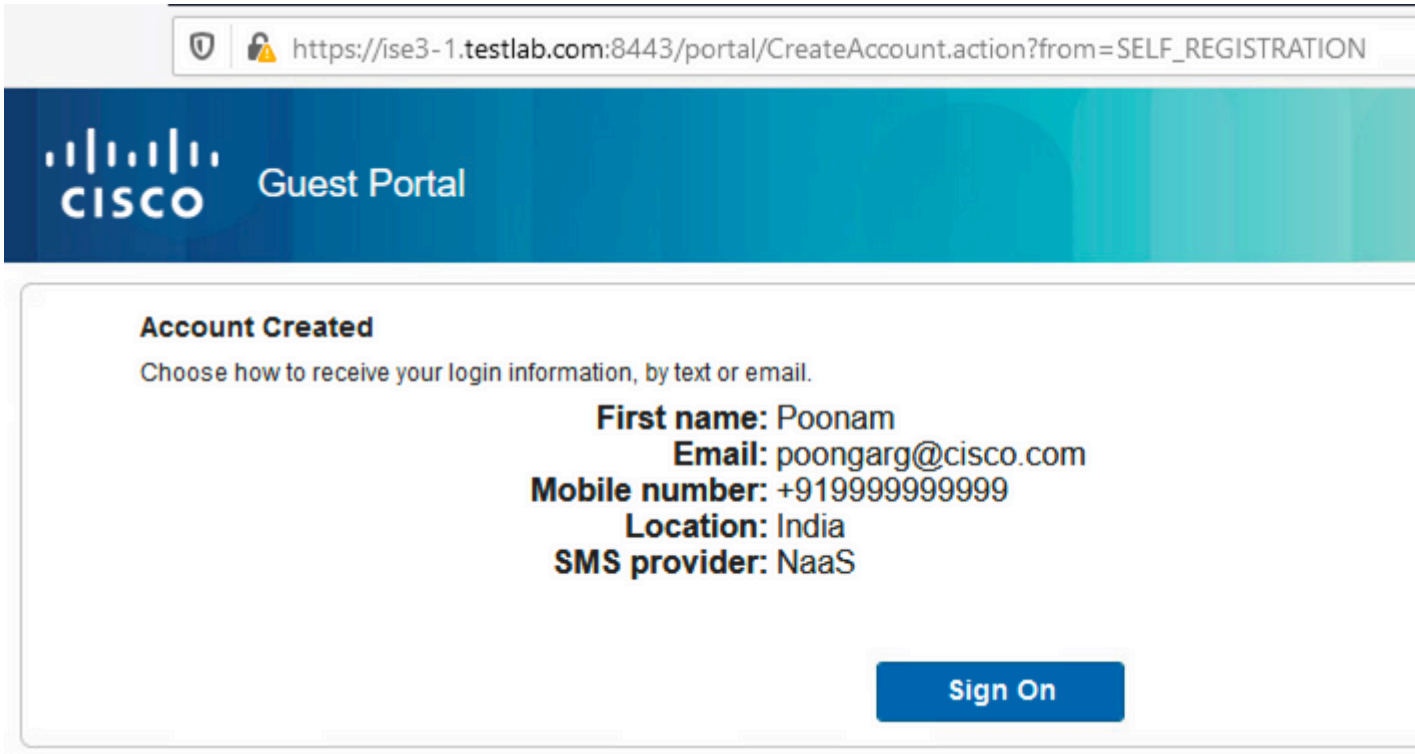
2. Aktivieren Sie das Kontrollkästchen **Benachrichtigung mit Anmeldeinformationen bei Genehmigung senden über: SMS**.



3. Anschließend wird der Gastbenutzer aufgefordert, den verfügbaren Anbieter auszuwählen, wenn er ein Konto erstellt:



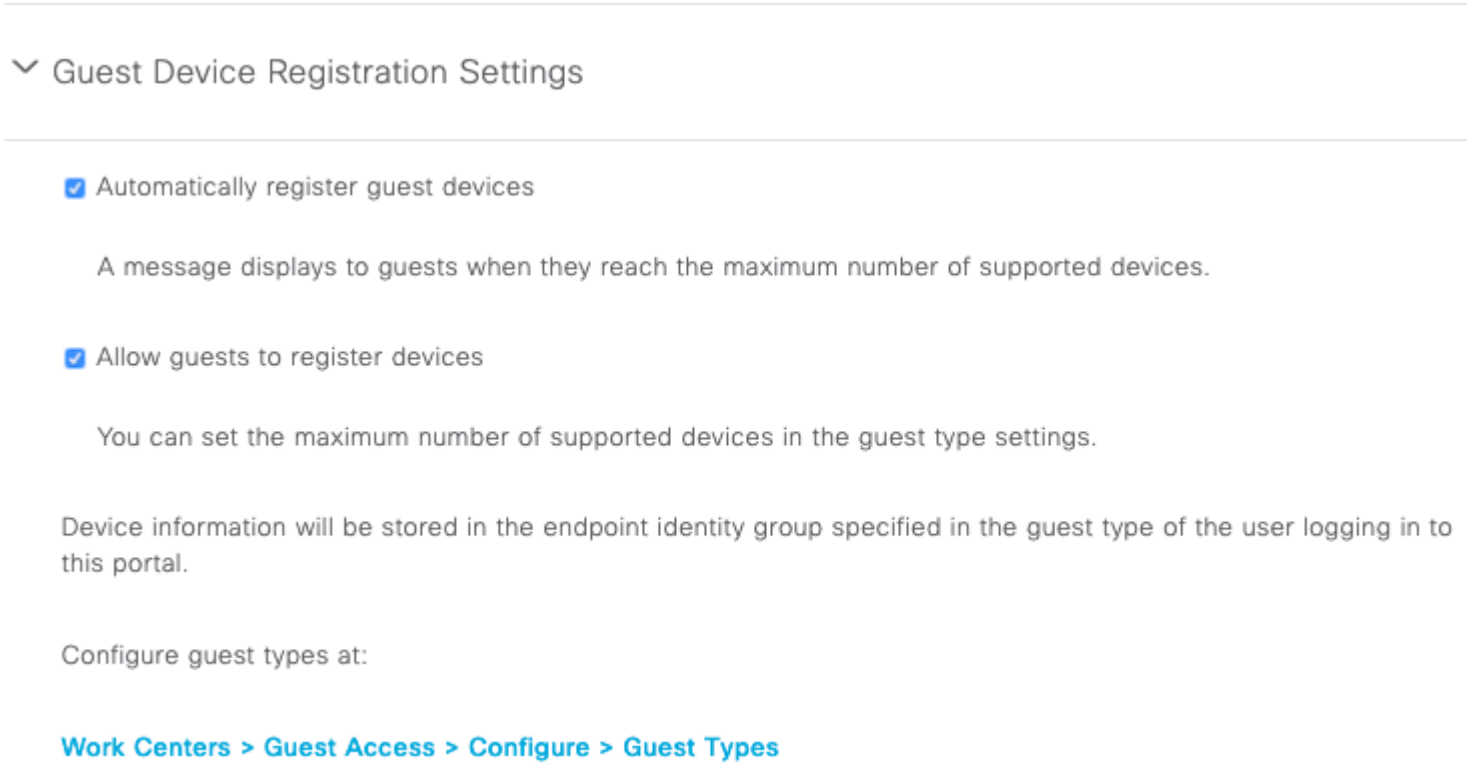
4. Eine SMS wird mit dem gewählten Anbieter und der gewählten Telefonnummer zugestellt:

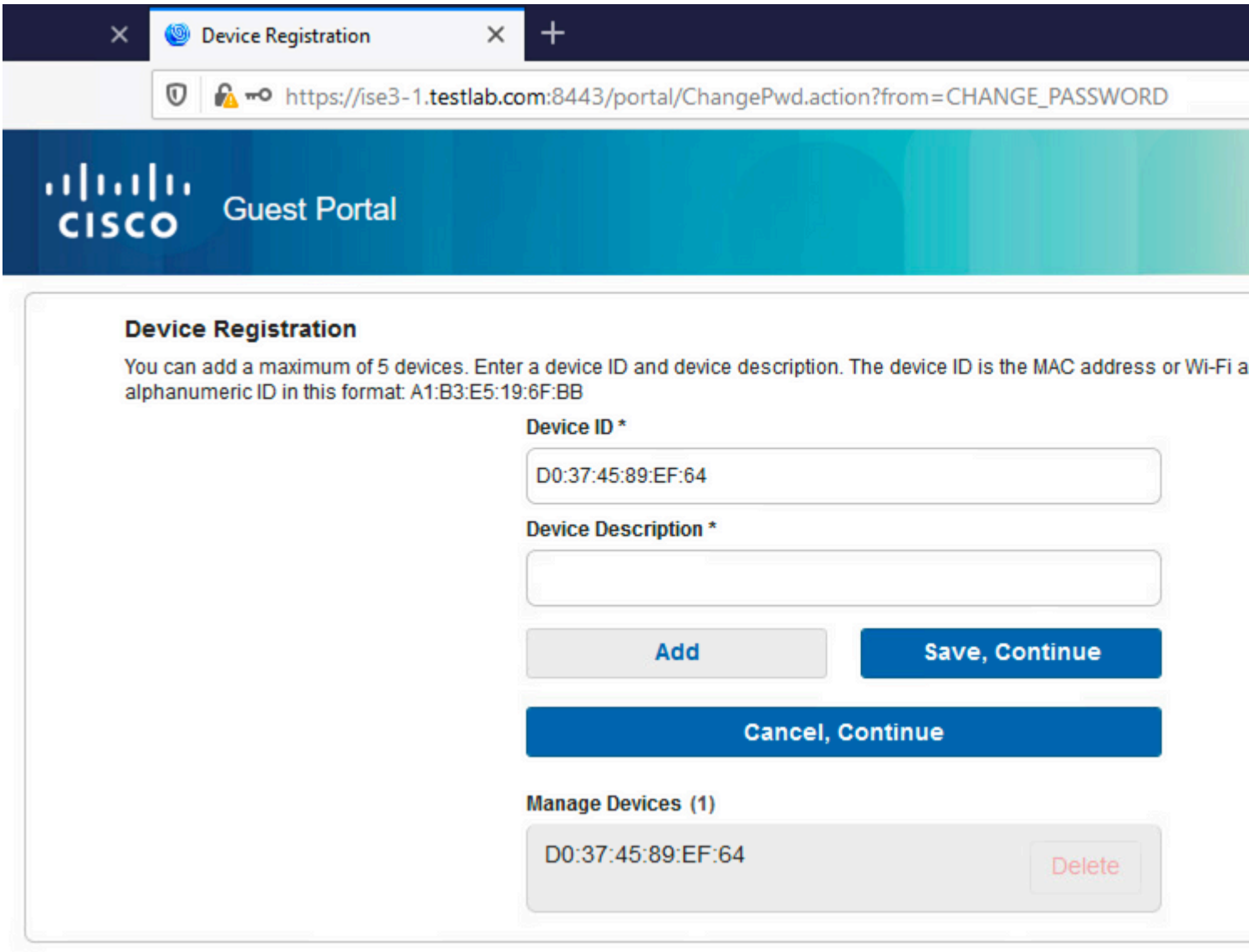


5. Sie können SMS-Anbieter konfigurieren unter **Administration > System > Settings > SMS Gateway**.

Registrierung von Geräten

Wenn die Option **Gäste zur Geräteregistrierung zulassen** aktiviert ist, nachdem sich ein Gastbenutzer angemeldet hat und die AUP akzeptiert, können Sie Geräte registrieren:



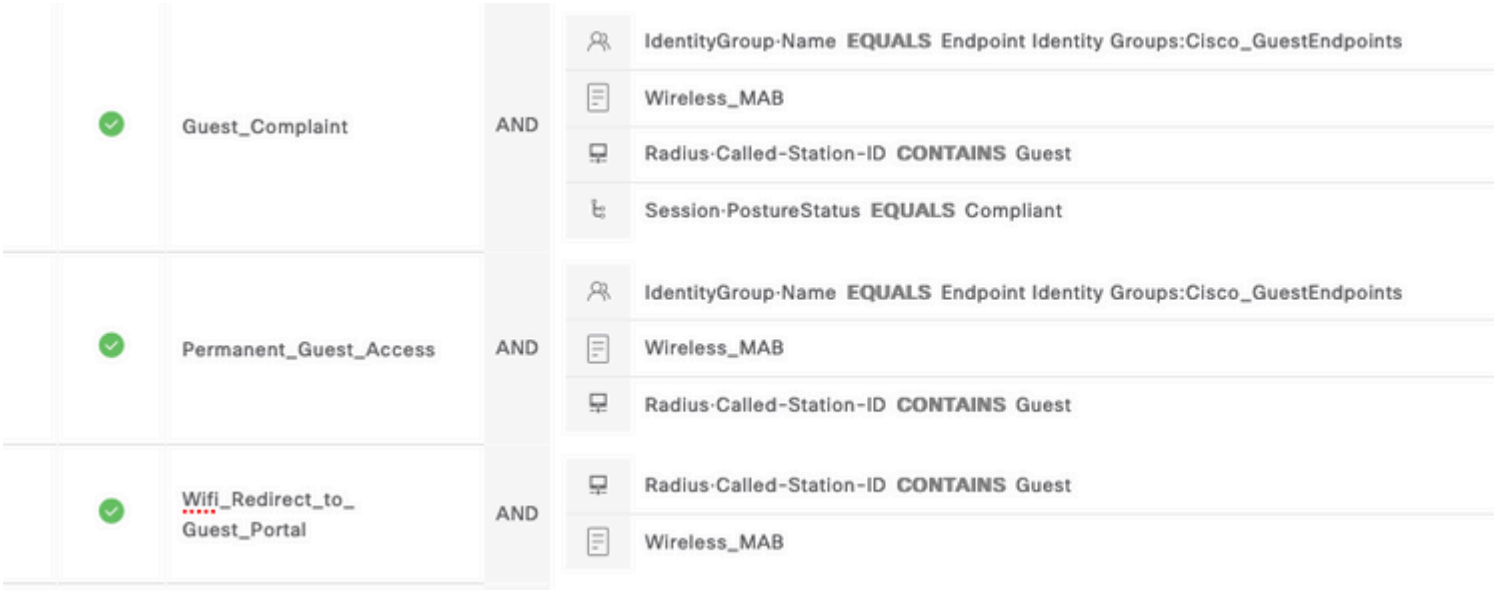


Das Gerät wurde bereits automatisch hinzugefügt (in der Liste "Geräte verwalten"). Dies liegt daran, dass **Gastgeräte automatisch registrieren** ausgewählt wurden.

Status

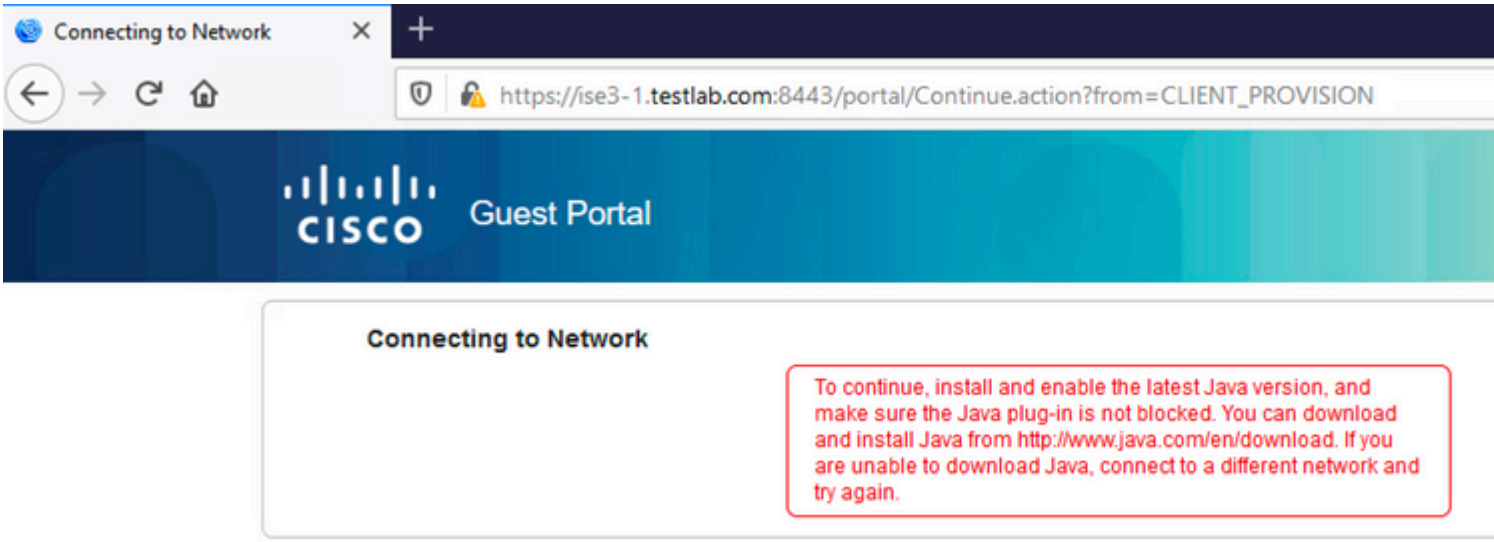
Wenn die Option **Erfüllung von Gastgeräteanforderungen erfordern** ausgewählt ist, wird Gastbenutzern ein Agent bereitgestellt, der den Status (NAC/Web-Agent) durchführt, nachdem sie sich angemeldet und die AUP akzeptiert haben (und optional eine Geräteregistrierung durchführen). Die ISE verarbeitet Client-Bereitstellungsregeln, um zu entscheiden, welcher Agent bereitgestellt werden muss. Anschließend führt der auf der Station ausgeführte Agent den Status aus (gemäß den Statusregeln) und sendet die Ergebnisse an die ISE, die die CoA erneut authentifiziert, um ggf. den Autorisierungsstatus zu ändern.

Mögliche Autorisierungsregeln können wie folgt aussehen:



Die ersten neuen Benutzer, bei denen eine Guest_Authenticate-Regel auftritt, werden zum Portal "Self Register Guest" umgeleitet. Wenn sich der Benutzer selbst registriert und anmeldet, ändert der CoA-Status den Autorisierungsstatus, und der Benutzer erhält eingeschränkten Zugriff für die Durchführung von Status- und Sanierungsmaßnahmen. Erst nachdem der NAC Agent bereitgestellt wurde und die Station die Vorgaben erfüllt, ändert CoA den Autorisierungsstatus erneut, um den Zugriff auf das Internet zu ermöglichen.

Zu den typischen Problemen mit dem Status gehören die fehlenden korrekten Client-Bereitstellungsregeln:



Dies kann auch bestätigt werden, wenn Sie die Datei **guest.log** untersuchen:

<#root>

```
2020-11-09 09:23:32,157 ERROR [https-jsse-nio-10.106.32.25-8443-exec-7][] guestaccess.flowmanager.step.g
```

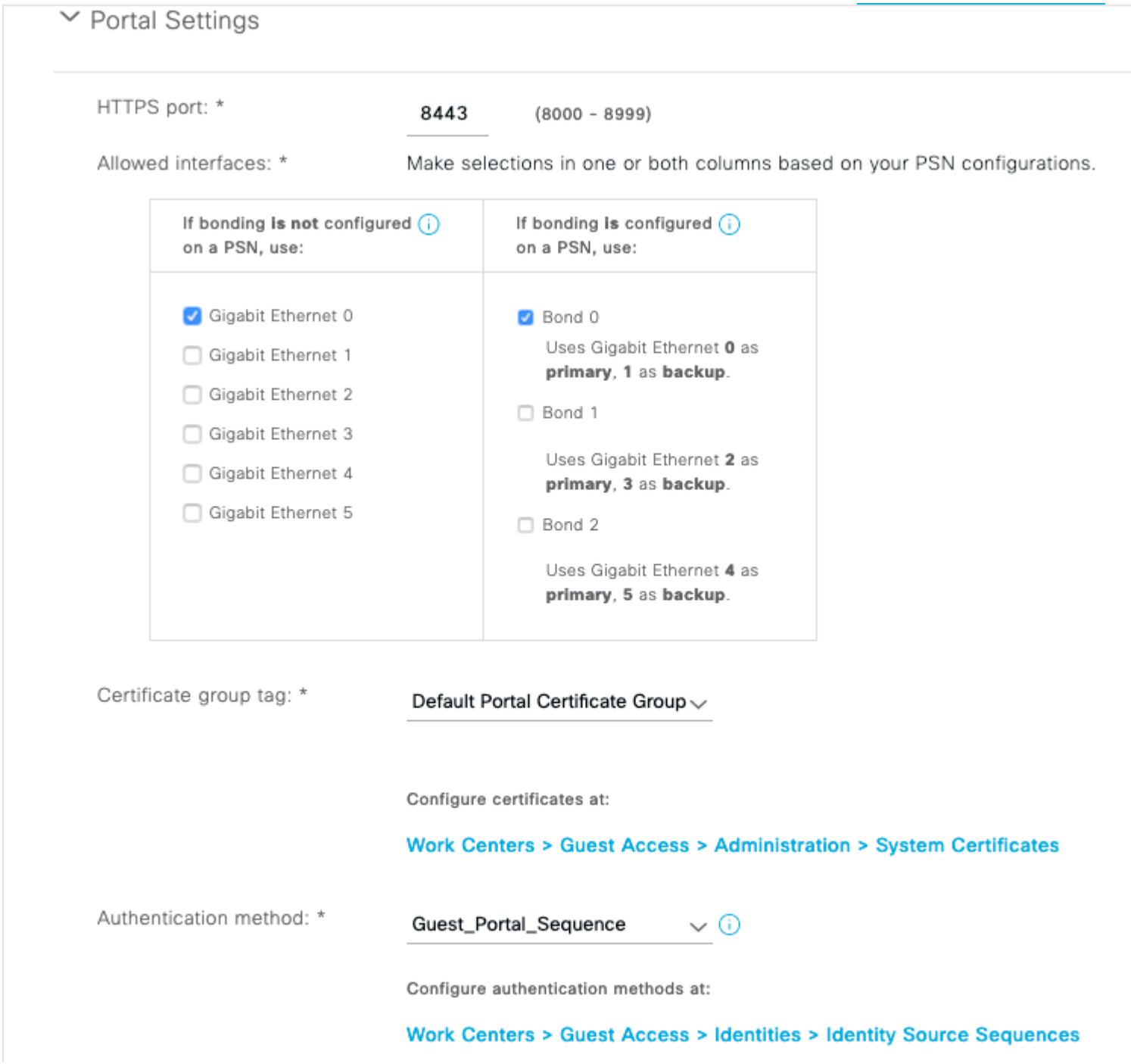
BYOD

Wenn die Option **Allow employee to use personal devices on the network** (**Verwendung privater Geräte**

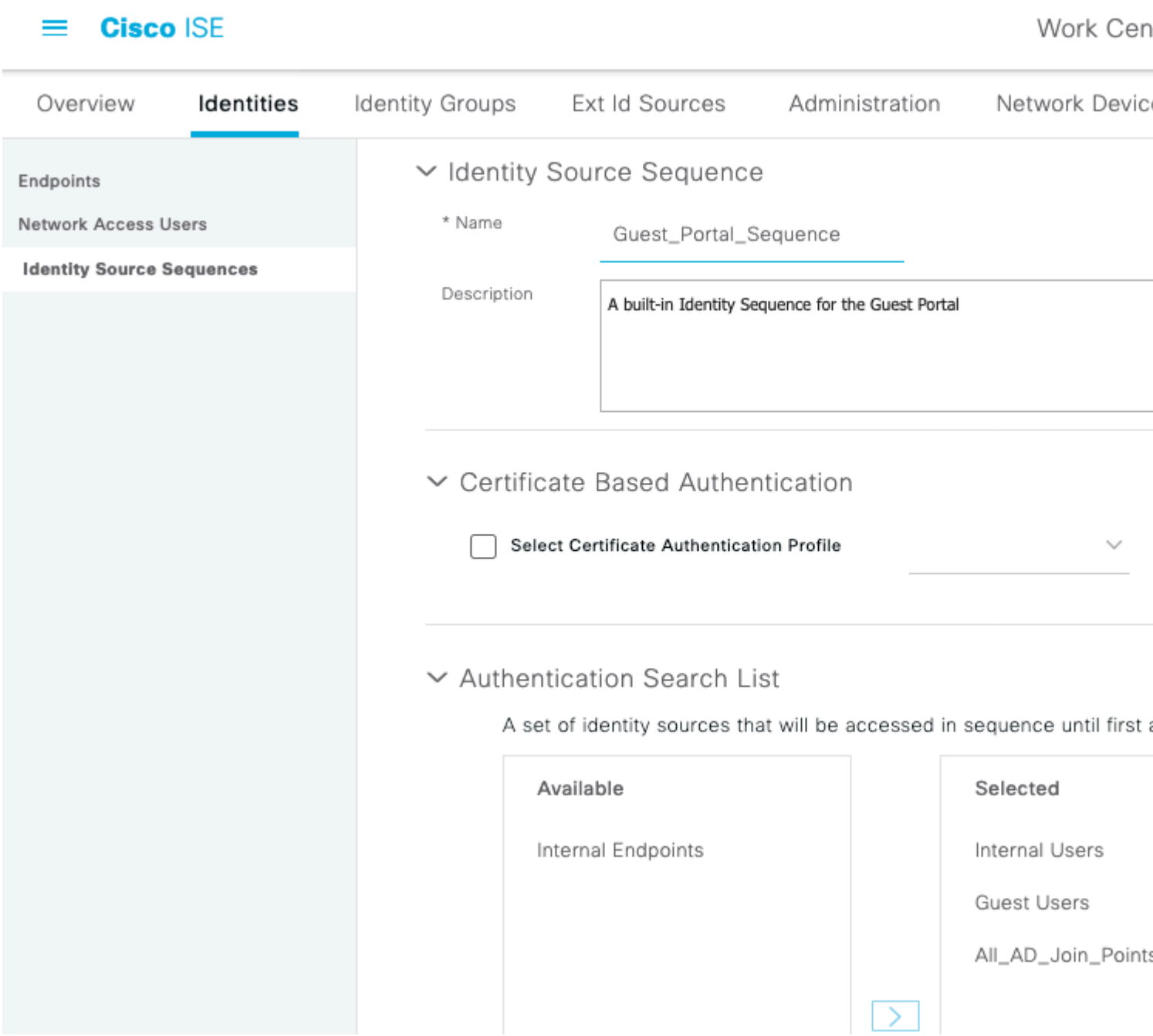
im Netzwerk zulassen) ausgewählt ist, können Benutzer im Unternehmen, die dieses Portal nutzen, den BYOD-Fluss durchlaufen und private Geräte registrieren. Für Gastbenutzer ändert diese Einstellung nichts.

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

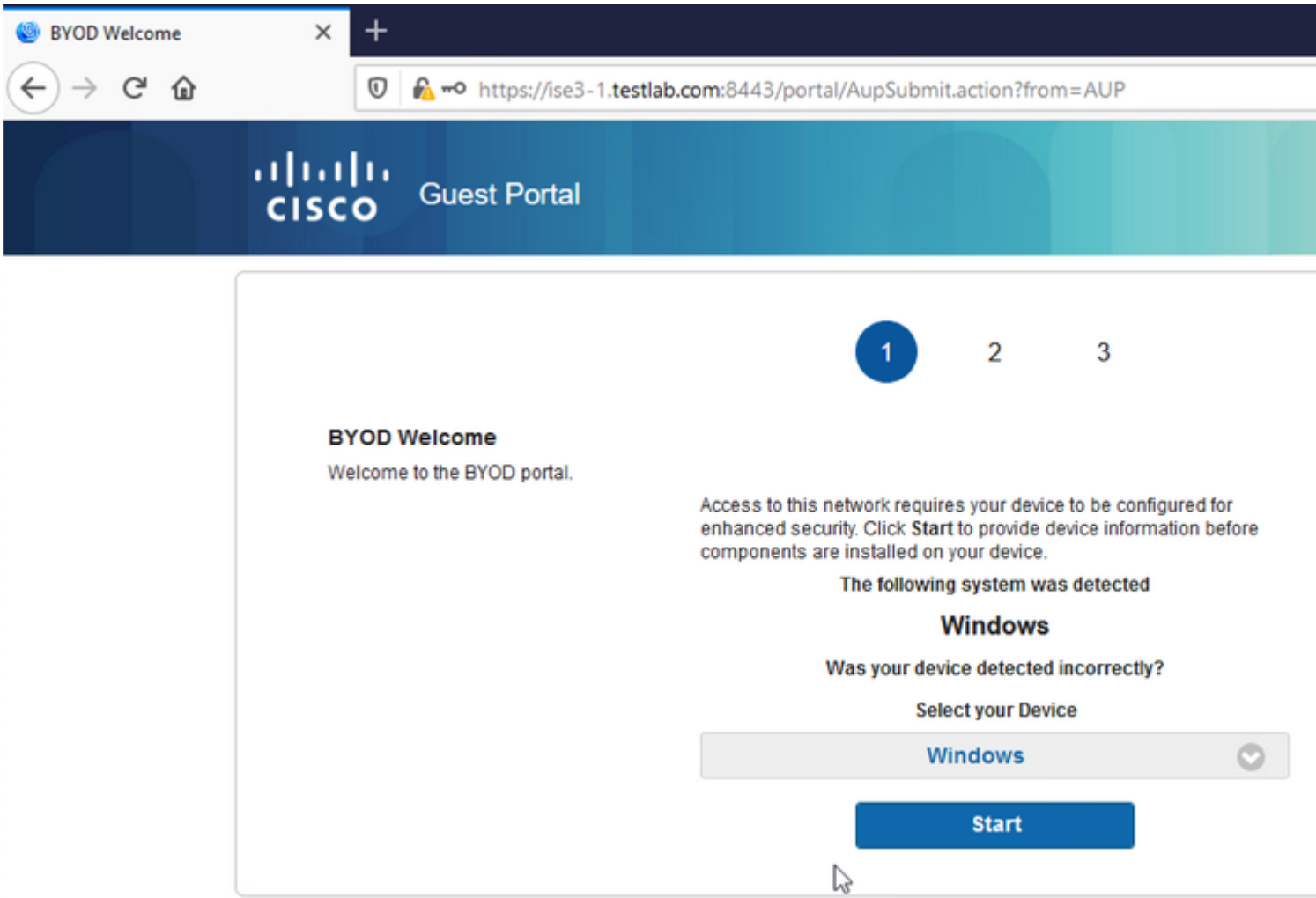
Gastportale werden standardmäßig mit dem Identitätsspeicher **Guest_Portal_Sequence** konfiguriert:



Dies ist die interne Speichersequenz, die zuerst die internen Benutzer (vor Gastbenutzern) und dann die AD-Anmeldeinformationen ausprobiert. Da die erweiterten Einstellungen den nächsten Speicher in der Sequenz verwenden sollen, wenn der Zugriff auf einen ausgewählten Identitätsspeicher zur Authentifizierung nicht möglich ist, kann sich ein Mitarbeiter mit internen Anmeldeinformationen oder AD-Anmeldeinformationen beim Portal anmelden.



In dieser Phase des Gastportals stellt der Benutzer Anmeldeinformationen bereit, die im Speicher für interne Benutzer oder in Active Directory definiert sind, und die BYOD-Umleitung erfolgt:



So können Benutzer im Unternehmen BYOD für private Geräte durchführen.

Wenn anstelle von internen Benutzern/AD-Anmeldeinformationen Anmeldeinformationen für Gastbenutzer bereitgestellt werden, wird der normale Fluss fortgesetzt (kein BYOD).

VLAN-Änderung

Es ermöglicht Ihnen, ActiveX oder ein Java-Applet auszuführen, was DHCP zur Freigabe und Verlängerung veranlasst. Dies ist erforderlich, wenn der CoA die Änderung des VLAN für den Endpunkt auslöst. Wenn MAB verwendet wird, erkennt der Endpunkt keine Änderung des VLAN. Eine mögliche Lösung besteht darin, das VLAN (DHCP-Freigabe/-Verlängerung) mit dem NAC Agent zu ändern. Eine weitere Möglichkeit besteht darin, über das auf der Webseite zurückgegebene Applet eine neue IP-Adresse anzufordern. Eine Verzögerung zwischen Release/CoA/Renew 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 für BYOD - Konfigurationsbeispiel**
- **Zentrale Webauthentifizierung im Konfigurationsbeispiel für WLC und ISE**
- **Zentrale Web-Authentifizierung mit FlexConnect APs auf einem WLC mit ISE - Konfigurationsbeispiel**
- **Technischer Support und Dokumentation für Cisco Systeme**

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.