

ISE自己登録型ゲストポータルの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トポロジとフロー](#)

[設定](#)

[WLC](#)

[ISE](#)

[確認](#)

[トラブルシューティング](#)

[オプションの設定](#)

[自己登録設定](#)

[ログインゲストの設定](#)

[デバイス登録の設定](#)

[ゲストデバイスのコンプライアンス設定](#)

[BYODの設定](#)

[スポンサー承認アカウント](#)

[SMS経由で資格情報を配信する](#)

[デバイスの登録](#)

[ポスチャ](#)

[BYOD](#)

[VLANの変更](#)

[関連情報](#)

はじめに

このドキュメントでは、ISE自己登録型ゲストポータル機能の設定およびトラブルシューティング方法について説明します。

前提条件

要件

ISE 構成の経験と、次のトピックに関する基本的な知識があることが推奨されます。

- ISE の導入およびゲスト フロー
- ワイヤレスLANコントローラ(WLC)の設定

使用するコンポーネント

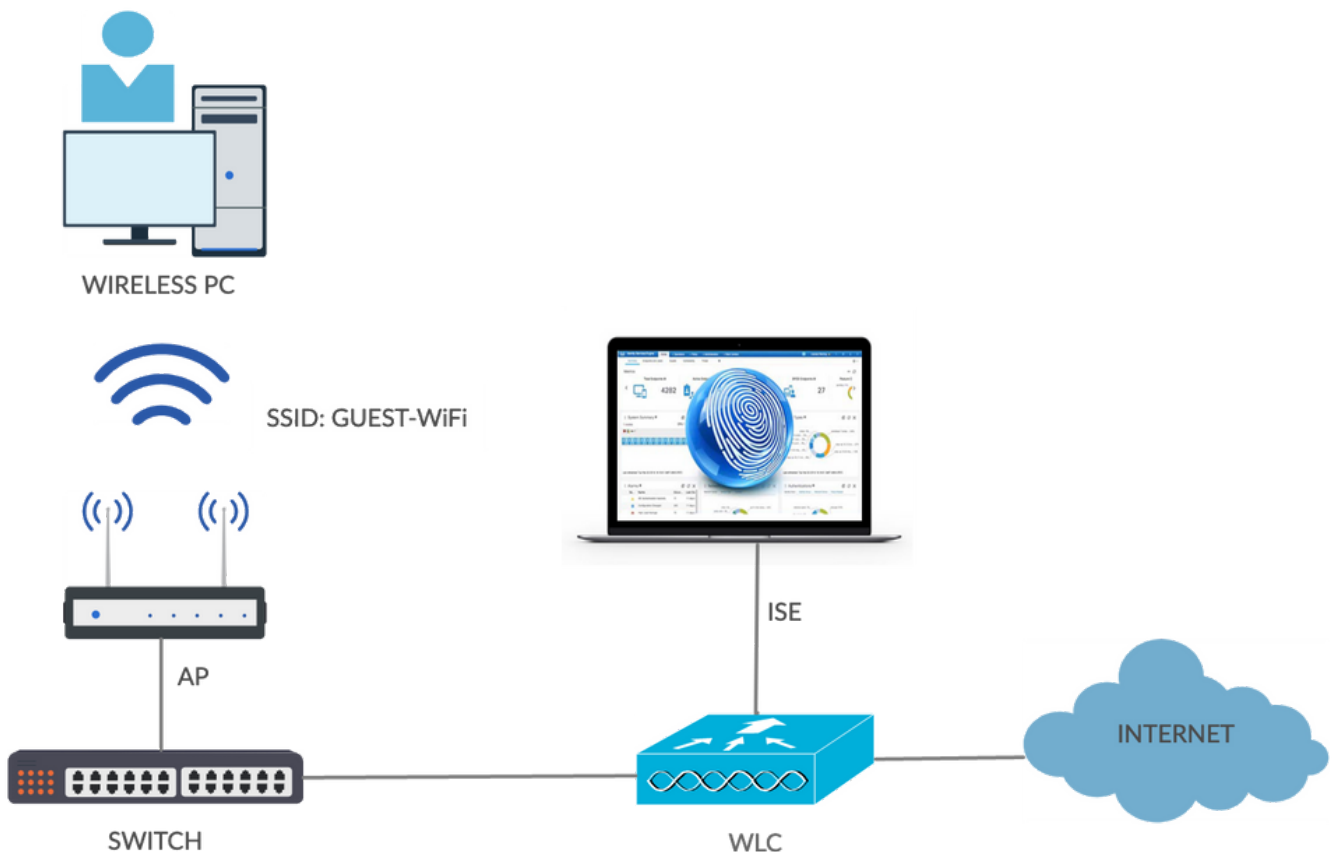
自己登録型ゲストポータル：ゲストユーザは従業員とともに自己登録し、ADクレデンシャルを使用してネットワークリソースにアクセスできます。このポータルでは、複数の機能を設定およびカスタマイズできます。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft Windows 10 Pro
- バージョン8.5.135.0のCisco WLC 5508
- ISEソフトウェアバージョン3.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トポロジとフロー



このシナリオでは、ゲストユーザが自己登録を実行するときに使用できる複数のオプションを示します。


一般的なフローを次に示します。

ステップ 1 : ゲストユーザはService Set Identifier(SSID):Guest-WiFiに関連付けられます。これは、認証に ISE を使用する MAC フィルタリングが設定されたオープン ネットワークです。この認証はISEの2番目の認可ルールと一致し、認可プロファイルはゲストの自己登録ポータルにリダイレクトされます。ISE から、2 つの cisco-av-pairs を使用した RADIUS Access-Accept が返されます。

- url-redirect-acl(どのトラフィックをリダイレクトする必要があるか、およびWLCでローカルに定義されているアクセスコントロールリスト(ACL)の名前)
- url-redirect (そのトラフィックのリダイレクト先 - ISE)

ステップ 2 : ゲストユーザはISEにリダイレクトされます。ログインするためのクレデンシャルを入力する代わりに、ユーザはRegister for Guest Accessをクリックします。ユーザは、そのアカウントを作成できるページにリダイレクトされます。オプションの秘密登録コードを有効にすると、自己登録権限をその秘密値を知っているユーザに制限できます。アカウントが作成されると、ユーザにはクレデンシャル (ユーザ名とパスワード) が提供され、これらのクレデンシャルでログインします。

ステップ 3 : ISEがRADIUS認可変更(CoA)再認証をWLCに送信します。WLCは、Authorize-Only属性を使用してRADIUSアクセス要求を送信するときに、ユーザを再認証します。ISEはWLCでローカルに定義されたAccess-AcceptおよびAirespace ACLで応答し、インターネットへのアクセスのみを提供します (ゲストユーザの最終的なアクセスは認可ポリシーによって異なります) 。

 注:EAPセッションはサブリカントとISEの間で行われるため、再認証をトリガーするにはISEがCoA Terminateを送信する必要があります。ただし、MAB (MACフィルタリング) の場合は、CoA再認証で十分です。ワイヤレスクライアントの関連付け/認証解除は必要ありません。

ステップ 4 : ゲストユーザがネットワークへの望ましいアクセス権を持っている。

ポスチャや個人所有デバイス持ち込み(BYOD)など、複数の追加機能を有効にできます (後述) 。

設定

WLC

1. 認証とアカウントिंगのために新しい RADIUS サーバを追加します。RADIUS CoA (RFC 3576) を有効にするため、[Security] > [AAA] > [Radius] > [Authentication] に移動します。

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The left sidebar shows the navigation menu with 'Security' expanded and 'RADIUS Authentication' selected. The main content area is titled 'RADIUS Authentication Servers > Edit' and contains the following settings:

- Server Index: 2
- Server Address(Ipv4/Ipv6): 10.106.32.25
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for CoA: Enabled
- Server Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- Management Retransmit Timeout: 2 seconds
- Tunnel Proxy: Enable
- IPSec: Enable

アカウントリングでも同様の設定があります。また、[Called Station ID] 属性で SSID を送信するように WLC を設定することが推奨されます。これにより、ISE は SSID に基づいて柔軟なルールを設定できます。

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The left sidebar shows the navigation menu with 'Security' expanded and 'RADIUS Authentication' selected. The main content area is titled 'RADIUS Authentication Servers' and contains the following settings:

- Auth Called Station ID Type: AP MAC Address:SSID
- Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

The screenshot shows the Cisco WLC configuration interface for RADIUS Accounting Servers. The left sidebar shows the navigation menu with 'Security' expanded and 'RADIUS Accounting' selected. The main content area is titled 'RADIUS Accounting Servers' and contains the following settings:

- Acct Called Station ID Type: IP Address
- MAC Delimiter: Hyphen

Network User	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	* 10.106.32.25

- WLANsタブで、ワイヤレスLAN(WLAN)Guest-WiFiを作成し、正しいインターフェイスを設定します。MAC フィルタリングで Layer2 セキュリティを [None] に設定します。Security/Authentication, Authorization, and Accounting(AAA)Serversで、認証とアカウントリングの両方にISE IPアドレスを選択します。Advancedタブで、AAA Overrideを有効にし、Network Admission Control(NAC)StateをISE NAC(CoA support)に設定します。

3. [Security] > [Access Control Lists] > [Access Control Lists] の順に移動し、2 つのアクセスリストを作成します。

- GuestRedirect : リダイレクトしてはならないトラフィックを許可し、他のすべてのトラフィックをリダイレクトします。
- Internet : 社内ネットワークについては拒否され、その他のすべてのネットワークについては許可されます。

GuestRedirect ACLの例を次に示します (ISEとの間のトラフィックをリダイレクトから除外する必要があります)。

Security

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

Access Control Lists > Edit

General

Access List Name: GuestRedirect

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.106.32.25 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	10.106.32.25 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

ISE

1. Work Centers > Guest Access > Network Devicesの順に選択し、WLCをネットワークアクセスデバイスとして追加します。
2. エンドポイントIDグループを作成します。Work Centers > Guest Access > Identity Groups > Endpoint Identity Groupsの順に移動します。

Cisco ISE

Work Centers · Guest Access

Overview Identities **Identity Groups** Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements

Identity Groups

Endpoint Identity Group List > New Endpoint Group

Endpoint Identity Group

* Name: Cisco_GuestEndpoints

Description:

Parent Group:

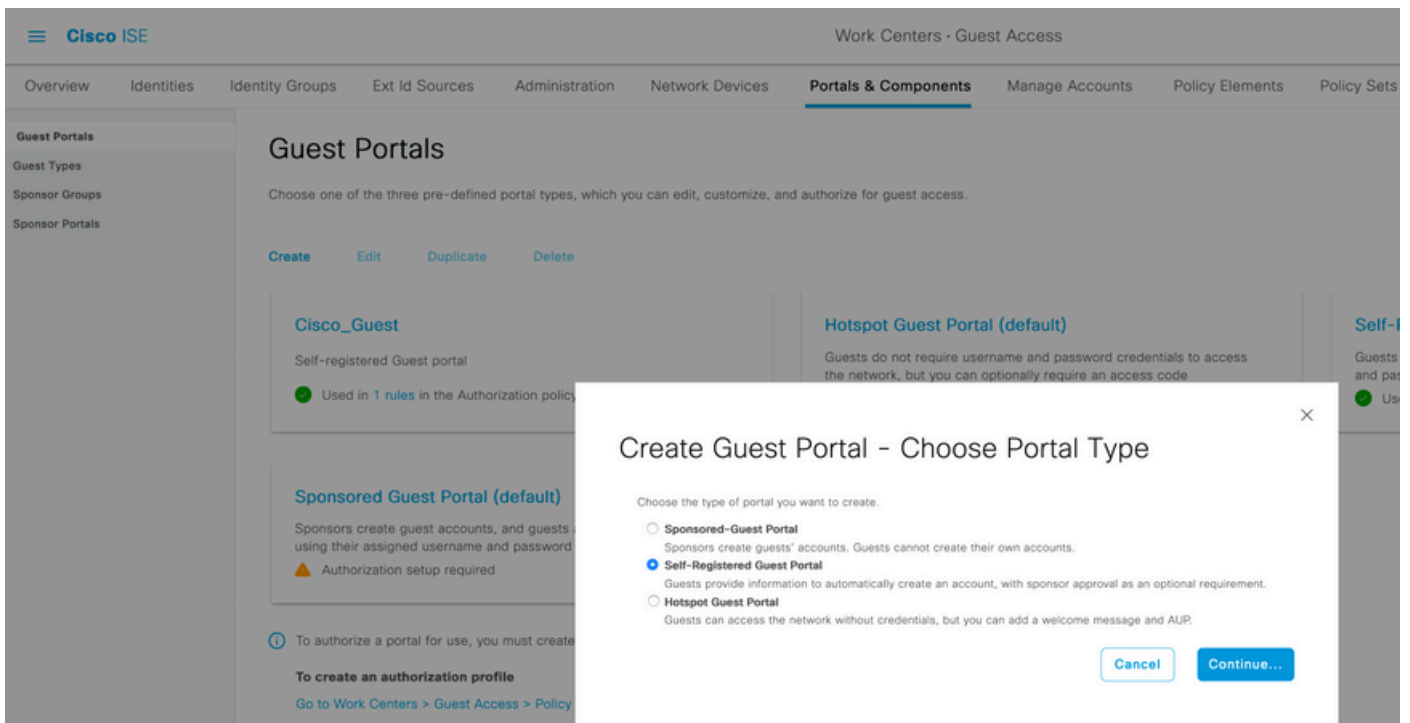
Submit Cancel

3. 「ワーク・センター」>「ゲスト・アクセス」>「ポータルとコンポーネント」>「ゲスト・タイプ」に移動して、ゲスト・タイプを作成します。この新しいゲストタイプで以前作成したエンドポイントIDグループを参照して保存します。

The screenshot shows the configuration page for a new Guest Type in the Cisco Guest Access interface. The page is titled "Portals & Components" and includes a sidebar with navigation options: Guest Portals, Guest Types (selected), Sponsor Groups, and Sponsor Portals. The main content area is divided into several sections:

- Guest type name: ***: A text input field containing "Guest-Daily".
- Description:**: A text area containing "Guest account access for 30 days".
- Language File**: A dropdown menu.
- Collect Additional Data**: A link for "Custom Fields...".
- Maximum Access Time**:
 - Account duration starts**: Radio buttons for "From first login" and "From sponsor-specified date (or date of self-registration, if applicable)". The second option is selected.
 - Maximum account duration**: A text input field showing "5 days" and a range of "1 (1-999)".
 - Allow access only on these days and times:
 - From**: 9:00 AM **To**: 5:00 PM. Days of the week are checked: Sun, Mon, Tue, Wed, Thu, Fri, Sat.
- Configure guest Account Purge Policy at:** A link to "Work Centers > Guest Access > Settings > Guest Account Purge Policy".
- Login Options**:
 - Maximum simultaneous logins: 3 (1-999).
 - When guest exceeds limit:**
 - Disconnect the oldest connection.
 - Disconnect the newest connection.
 - Redirect user to a portal page showing an error message (with an information icon).
 - This requires the creation of an authorization policy rule
 - Maximum devices guests can register: 5 (1-999).
- Endpoint identity group for guest device registration:** A dropdown menu showing "Cisco_GuestEndpoints".

4.新しいゲストポータルタイプとしてSelf-Registered Guest Portalを作成します。Work Centers > Guest Access > Guest Portalsに移動します。

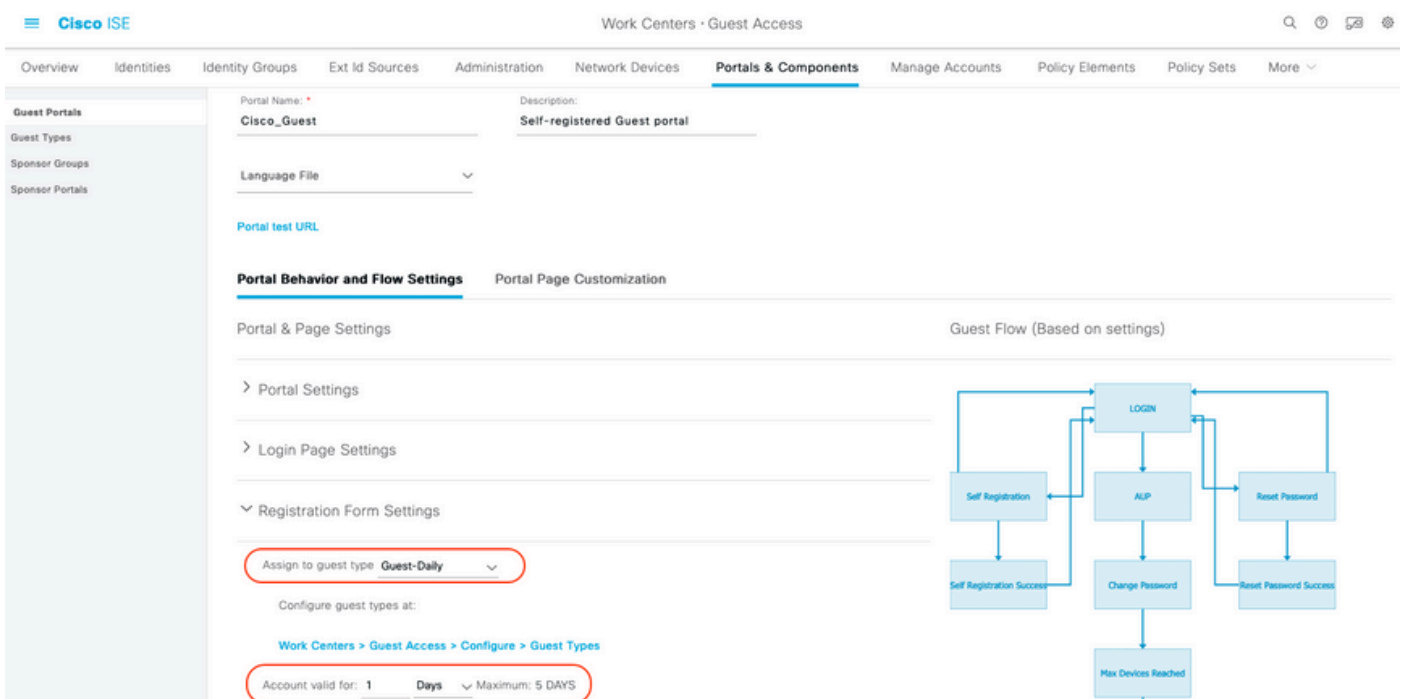


5.ポータル名を選択し、前に作成したゲストタイプを参照し、登録フォーム設定の下でクレデンシャル通知設定を送信して、クレデンシャルを電子メールで送信します。

ISEでSMTPサーバを設定する方法については、次のドキュメントを参照してください。

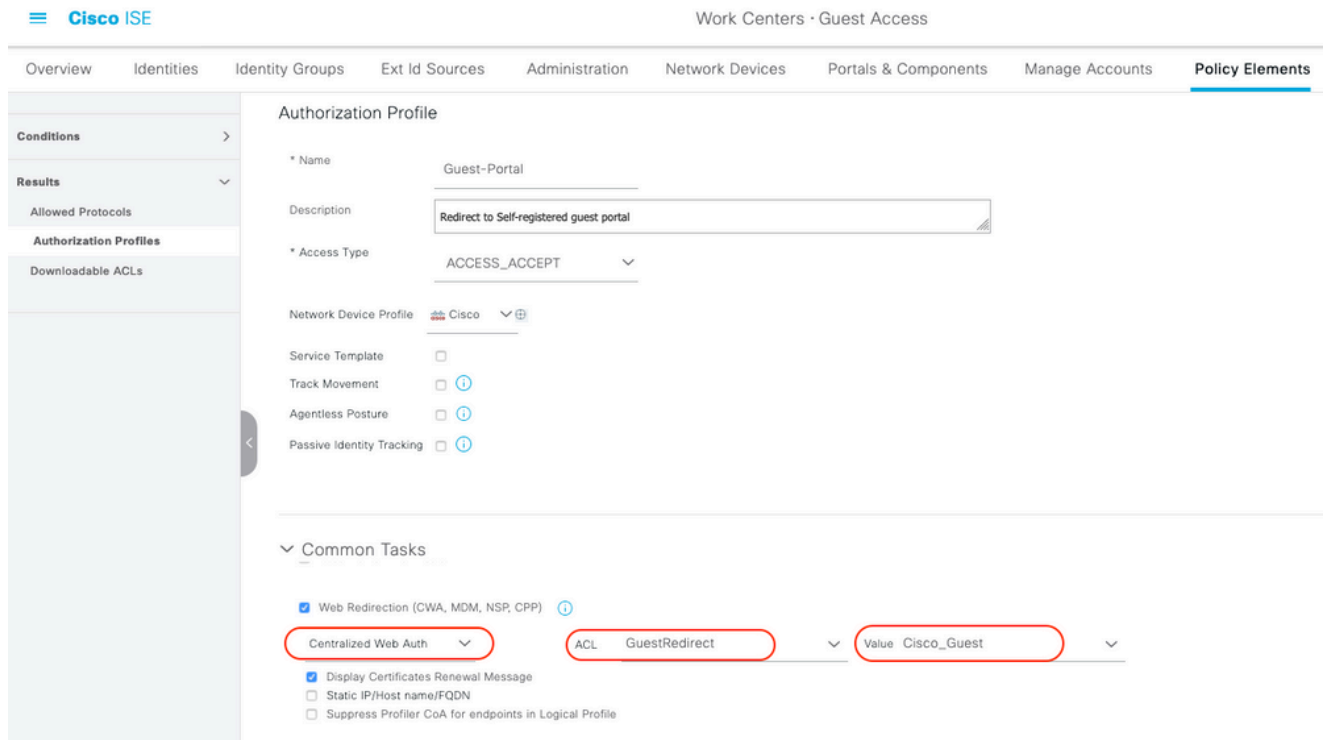
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216187-configure-secure-smtp-server-on-ise.html>

その他の設定はすべてデフォルトのままにします。ポータルページのカスタマイズでは、表示されるすべてのページをカスタマイズできます。デフォルトでは、Guestアカウントは1日間有効で、特定のGuest Typeで設定された日数まで延長できます。



6. Work Centers > Guest Access > Policy Elements > Results > Authorization Profilesの順に移動して、これら2つの認可プロファイルを設定します。

- ゲストポータル(ゲストポータルCisco_Guestへのリダイレクト、およびGuestRedirectという名前のリダイレクトACLを使用)このGuestRedirect ACLは、WLCで以前に作成されました。



- Permit_Internet (Airespace ACLとInternetは同じ)

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components

Authorization Profiles > Permit_internet

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

Airespace ACL Name

Airespace IPv6 ACL Name

ASA VPN

7. Defaultという名前のポリシーセットを変更します。デフォルトのポリシーセットは、ゲストポータルアクセス用に事前に設定されています。MABという名前の認証ポリシーが存在します。このポリシーにより、MAC認証バイパス(MAB)認証を未知のMACアドレスに対して継続（拒否ではなく）できます。

Cisco ISE Work Centers · Guest Access

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements **Policy Sets** More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	Wired_MAB OR Wireless_MAB	Internal Endpoints Options If Auth fail REJECT If User not found CONTINUE If Process fail DROP	0	

8.同じページでAuthorization policyに移動します。次の図に示すように、この認可ルールを作成します。

Authorization Policy (15)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Wifi_Guest_Access	IdentityGroup-Name EQUALS Endpoint Identity Groups: Cisco_GuestEndpoints AND Wireless_MAB	Permit_internet	Select from list	0	
●	Wifi_Redirect_to_Guest_Portal	Radius-Called-Station-ID CONTAINS Guest AND Wireless_MAB	Guest-Portal	Select from list	0	


ゲストSSIDに関連付けられた新しいユーザは、まだIDグループに属していないため、2番目のルールに一致し、ゲストポータルにリダイレクトされます。

ユーザが正常にログインした後、ISEがRADIUS CoAを送信し、WLCが再認証を実行します。今回は、最初の認可ルールが照合され（エンドポイントが定義済みのエンドポイントアイデンティティグループの一部になるため）、ユーザはPermit_internet認可プロファイルを取得します。

9.また、条件ゲストフローを使用して、ゲストへの一時的なアクセスを提供することもできます。この条件はISE上のアクティブセッションをチェックしており、属性が設定されています。そのセッションに、以前にゲストユーザが正常に認証されたことを示す属性がある場合は、条件が一致します。ISEがNetwork Access Device(NAD)からRadius Accounting Stopメッセージを受信すると、セッションは終了し、後で削除されます。その段階で、Network Access:UseCase = Guest Flowの条件が満たされなくなっています。その結果、そのエンドポイントに対する後続のすべての認証が、ゲスト認証のためにリダイレクトされる一般的なルールにヒットします。

Authorization Policy (15)

Status	Rule Name	Conditions	Results		
			Profiles	Security Groups	Hits
●	Temporary_Guest_Access	AND Network Access-UseCase EQUALS Guest Flow Wireless_MAB	Permit_internet x	Select from list	1
○	Permanent_Guest_Access	AND IdentityGroup Name EQUALS Endpoint Identity Groups: Cisco_GuestEndpoints Wireless_MAB	Permit_internet x	Select from list	2
●	Wifi_Redirect_to_Guest_Portal	AND Radius-Called-Station-ID CONTAINS Guest Wireless_MAB	Guest-Portal x	Select from list	3

 注：一時ゲストアクセスまたは固定ゲストアクセスのいずれかを使用できますが、両方は使用できません。

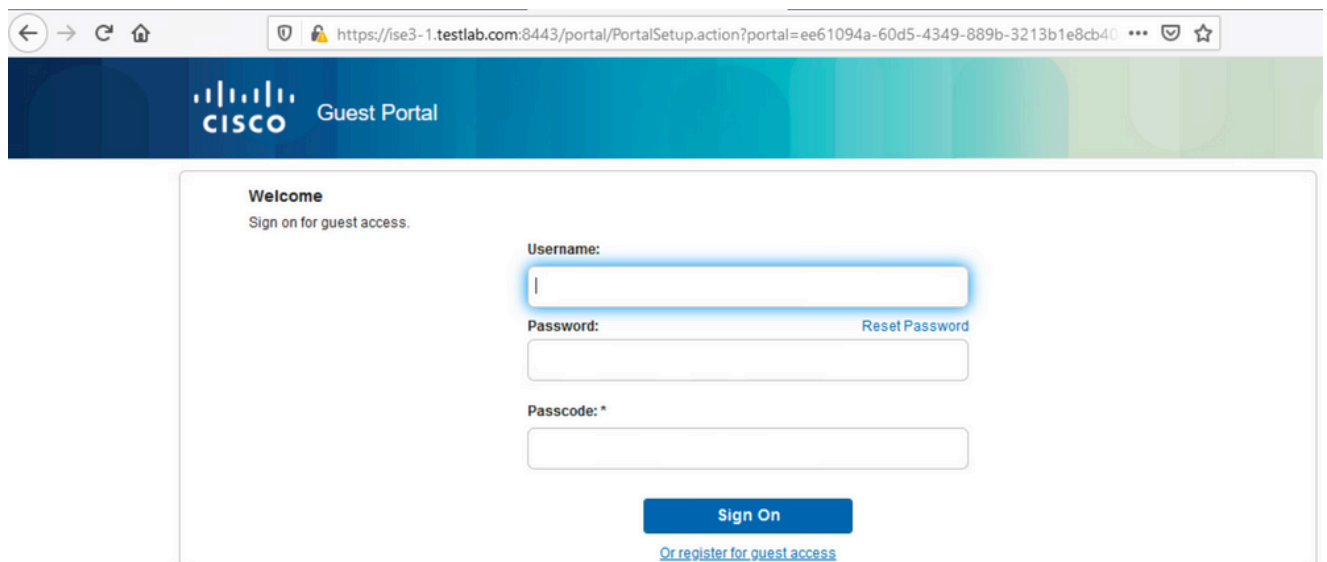
ISEゲストの一時のおよび永続的なアクセスの設定の詳細については、このドキュメントを参照してください。

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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. ゲストSSIDと関連付けてURLを入力すると、図に示すように、ゲストポータルページにリダイレクトされます。



Guest Portal

Welcome
Sign on for guest access.

Username:

Password: [Reset Password](#)

Passcode: *

[Sign On](#)

[Or register for guest access](#)

2. まだクレデンシャルを持っていないため、Register for Guest accessオプションを選択する必要があります。アカウントを作成するための登録フォームが表示されます。ゲストポータル設定でRegistration Codeオプションが有効になっている場合は、このシークレット値が必要です（これにより、正しい権限を持つユーザだけが自己登録を許可されるようになります）。

https://ise3-1.testlab.com:8443/portal/SelfRegistration.action?from=LOGIN 80%

CISCO Guest Portal

Registration
Please complete this registration form:

Registration Code*
8015

Username
guest1

First name
Poonam

Last name
Garg

Email address*
poongarg@cisco.com

Mobile number
+91 0000000000

Company
Cisco

Person being visited(email)
abc@cisco.com

Reason for visit
Personal

Register Cancel

Activat
Go to Set

3.パスワードまたはユーザポリシーに問題がある場合は、[Work Centers] > [Guest Access] > [Settings] > [Guest Username Policy] に移動して設定を変更します。ランダム データの例は次のとおりです。

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements **More** ▾

Guest Account Purge Policy
Custom Fields
Guest Email Settings
Guest Locations and SSIDs
Guest Username Policy
Guest Password Policy
DHCP & DNS Services
Logging

Guest Username Policy

Configure username requirements that will be enforced for guest usernames. Usernames are not case sensitive.

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: ▾ ABCDEFGHIJKLMNOPQRSTUVWXYZ

Minimum alphabetic: (0-64)

Numeric: ▾ 23456789

Minimum numeric: (0-64)

Special: ▾

Minimum special: (0-64)

4.アカウントが正常に作成されると、クレデンシャル (ゲストパスワードポリシーに従って生成されたパスワード) が表示されます。また、ゲストユーザが設定されている場合は、電子メール通知が受信されます。

https://ise3-1.testlab.com:8443/portal/CreateAccount.action?from=SELF_REGISTRATION

CISCO Guest Portal guest1 ⓘ

Account Created

Choose how to receive your login information, by text or email. Email Me attempts left:5

You can only click the button 5 times.

Username: guest1
Password: 3154
First name: Poonam
Last name: Garg
Email: poongarg@cisco.com
Mobile number: +910000000000
Company: Cisco
Location: India
SMS provider: Global Default
Person being visited (email): abc@cisco.com
Reason being visited: Personal

Your Guest Account Credentials



ise@testlab.com <ise@testlab.com>

Today at 9:47 AM

To: Poonam Garg (poongarg)



Hello Poonam,
Your guest account details:
Username: guest1
Password: 3154
First Name: Poonam
Last Name: Garg
Mobile Number:+910000000000
Valid From: 2020-11-07 09:43:50
Valid To: 2020-11-08 09:43:50
Person being visited: abc@cisco.com
Reason for visit: Personal

5. Sign Onをクリックして、クレデンシャルを入力します (ゲストポータルで設定する場合は、アクセスパスコードを追加する必要があります。これは、パスワードを知っている人だけがログインできるようにする別のセキュリティメカニズムです)。

https://ise3-1.testlab.com:8443/portal/SelfRegistrationSuccess.action?from=SELF_REGISTRATION_SUCCESS

CISCO Guest Portal

Welcome
Sign on for guest access.

Username:
guest1

Password: [Reset Password](#)
.....

Passcode: *
8015

Sign On

[Or register for guest access](#)

6.成功すると、オプションのアクセプタブルユースポリシー(AUP)を表示できます (ゲストポータルで設定されている場合)。ユーザにはパスワードの変更オプションが表示され、ログイン後のバナー (ゲストポータルでも設定可能) も表示されます。



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 if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco Systems website and



Change Password

You are required to change your password now. Please enter a new password.

Current password:

New password:

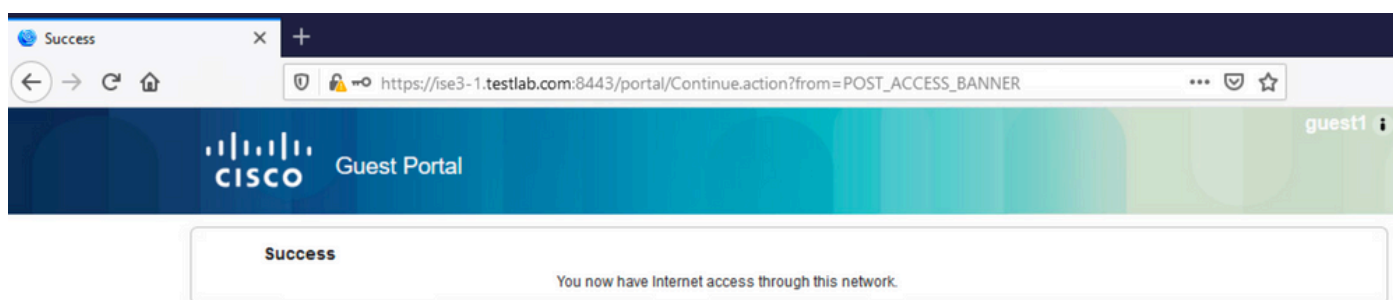
Confirm password:



Welcome Message

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

7.最後のページ (ログイン後のバナー) で、アクセスが許可されたことを確認します。



トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

この段階で、ISEは図に示すように、Operations > RADIUS > Live Logsの下にこれらのログを表示します。

Time	Status	Details	Identity	Endpoint ID	Authenticat...	Authorization Policy	Authorization P...	IP Address	Identity Group	Event
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...		Session State is Started
Nov 07, 2020 04:17:32.42...	■	🔍	guest1	D0-37-45-89-EF-64	Default	Default >> Permanent_Guest_Access	Permit_Internet		User Identity Groups:GuestType_Guest-Daily	Authorize-Only succeeded
Nov 07, 2020 04:17:32.39...	■	🔍		D0-37-45-89-EF-64						Dynamic Authorization succeeded
Nov 07, 2020 04:16:14.85...	■	🔍	guest1	D0-37-45-89-EF-64				10.106.32.2...	GuestType_Guest-Daily	Guest Authentication Passed
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		Profiled	Authentication succeeded

ここで、フローを示します。

- ゲストユーザは2番目の許可ルール(Wifi_Redirect_to_Guest_Portal)に遭遇し、ゲストポータルにリダイレクトされます(認証に成功しました)。
- ゲストは自己登録のためにリダイレクトされます。(新しく作成されたアカウントで)ログインに成功すると、ISEはCoA再認証を送信し、WLCによって確認されます(Dynamic Authorization succeeded)。
- WLCはAuthorize-Only属性で再認証を実行し、ACL名が返されます(Authorize-Only succeeded)。ゲストには、正しいネットワークアクセスが提供されます。

レポート(「操作」>「レポート」>「ゲスト」>「マスター・ゲスト・レポート」)では、次の確認も行います。

Master Guest Report

From 2020-11-07 00:00:00.0 To 2020-11-07 04:38:26.0

Reports exported in last 7 days 0

My Reports Export To Schedule

Filter Refresh

Logged At	Guest User Name	MAC Address	IP Address	Operation	Sponsor User Name
× Today x	Guest User Name	MAC Address	IP Address	Operation	Sponsor User Name
2020-11-07 04:17:01.1...	guest1	D0:37:45:89:EF:64	10.106.32.254	Password Change	guest1
2020-11-07 04:16:33.9...	guest1	D0:37:45:89:EF:64	10.106.32.254	AUP	
2020-11-07 04:13:51.0...	guest1	D0:37:45:89:EF:64	10.106.32.254	Add	SelfRegistration

スポンサーユーザ (正しい権限を持つ) は、ゲストユーザの現在のステータスを確認できます。

この例では、アカウントが作成され、ユーザがポータルにログインしたことを確認します。

CISCO Sponsor Portal Welcome test123

Create Accounts Manage Accounts (1) Pending Accounts (0) Notices (0)

Resend Extend Edit Suspend Reinstate Delete Reset Password Print

Username:	guest1
Password:
First name:	Poonam
Last name:	Garg
Email address:	poongarg@cisco.com
Company:	Cisco
Mobile number:	+910000000000
Person being visited (email):	abc@cisco.com
Reason for visit:	Personal
Guest type:	Guest-Daily
SMS provider:	Global Default
From date (yyyy-mm-dd):	2020-11-07 09:43
To date (yyyy-mm-dd):	2020-11-08 09:43
Location:	India
SSID:	
Language:	English
Group tag:	
Time left:	0D 22H 48M
State:	Active

Done

オプションの設定

このフローの各段階で、異なるオプションを設定できます。これらはすべて、ゲストポータルごとWork Centers > Guest Access > Portals & Components > Guest Portals > Portal Name > Edit > Portal Behavior and Flow Settingsで設定します。さらに重要な設定は次のとおりです。

自己登録設定

- Guest Type (ゲストタイプ) : アカウントがアクティブである期間、パスワードの有効期限オプション、ログオン時間、およびオプション (時間プロファイルとゲストロールが混在) について説明します。
- 登録コード : 有効にすると、シークレットコードを知っているユーザだけが自己登録を許可されます (アカウントの作成時にパスワードを入力する必要があります) 。
- AUP : 自己登録時に使用ポリシーを受け入れる
- スポンサーがゲストアカウントを承認またはアクティブ化するための要件。

ログインゲストの設定

- アクセスコード : 有効にすると、シークレットコードを知っているゲストユーザだけがログインを許可されます。
- AUP : 自己登録時に使用ポリシーを受け入れます。
- パスワード変更オプション。

デバイス登録の設定

- デフォルトでは、デバイスは自動的に登録されます。

ゲストデバイスのコンプライアンス設定

- フロー内のポスチャを許可します。

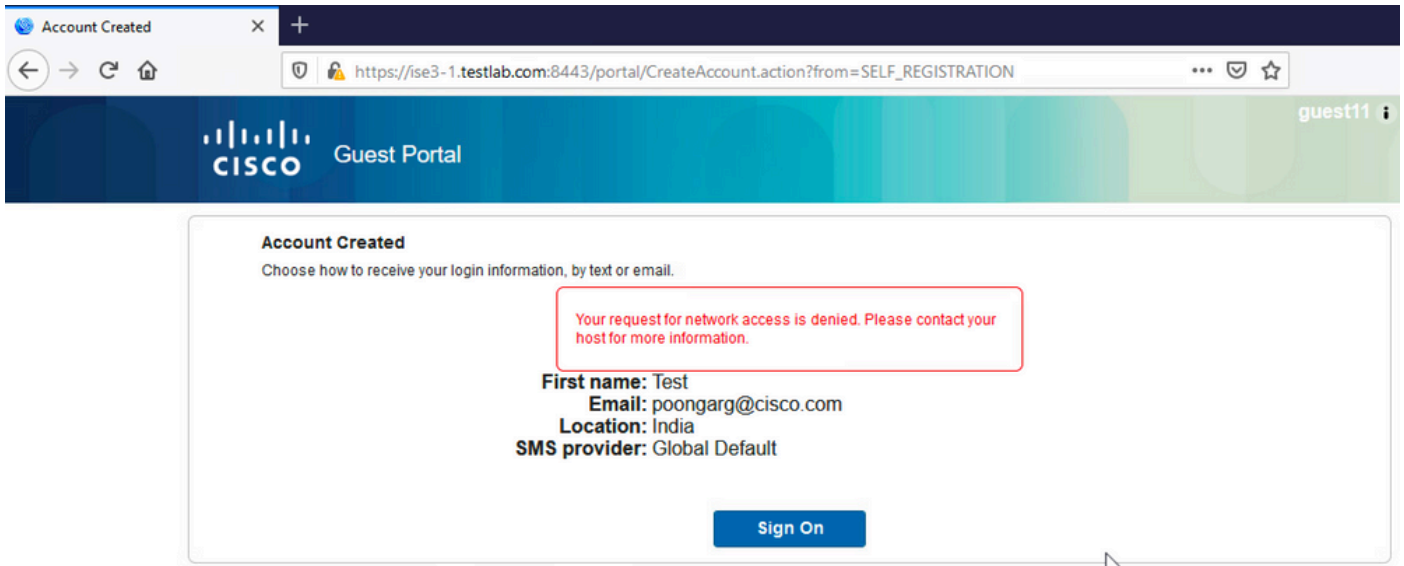
BYODの設定

- ポータルをゲストとして使用する企業ユーザが個人デバイスを登録できるようにします。

スポンサー承認アカウント

Registration Form SettingsでRequire guests to be approvedオプションが選択されている場合、ゲストによって作成されたアカウントはスポンサーによって承認される必要があります。この機能では、電子メールを使用してスポンサーに通知を送信できます (ゲストアカウントの承認のため) 。

Simple Mail Transfer Protocol(SMTP)サーバの設定に誤りがある場合、アカウントは作成されません。



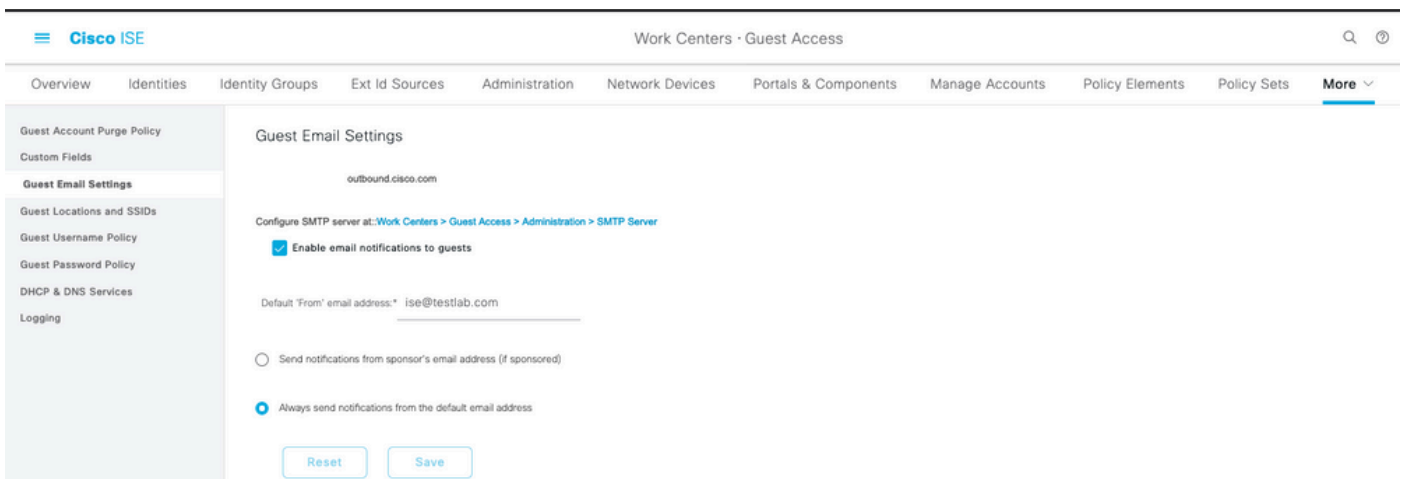
guest.logからのログは、SMTPサーバの設定が誤っているためにスポンサー電子メールに承認通知を送信する際に問題が発生していることを示しています。

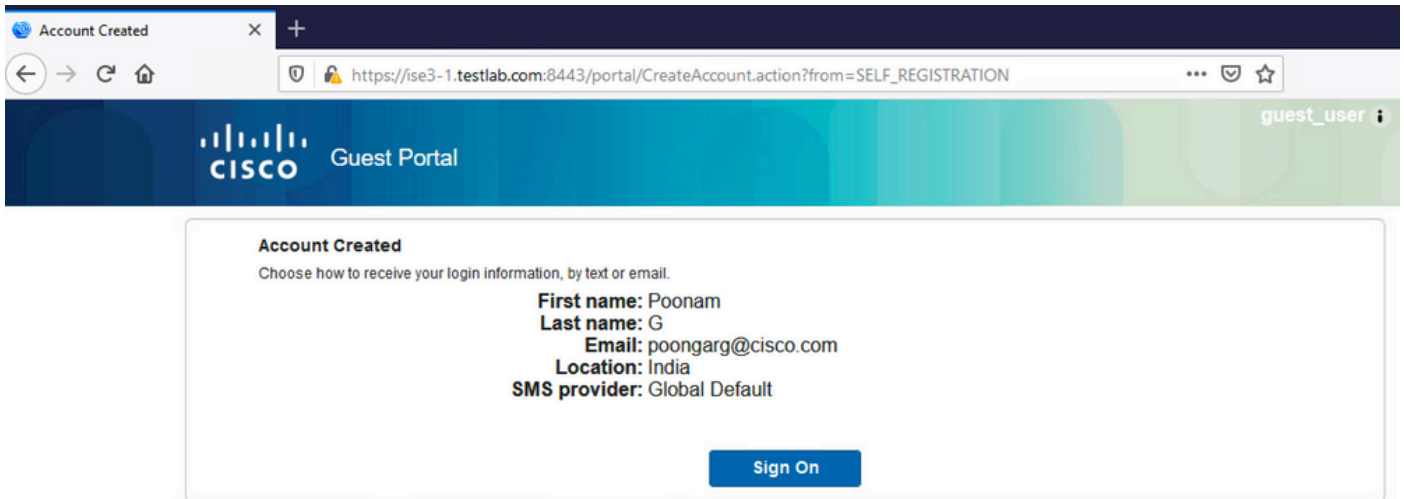
<#root>

```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTP_RETRY_THREAD][ ] cpm.guestaccess.apiservices.util.SmtptM  
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
```

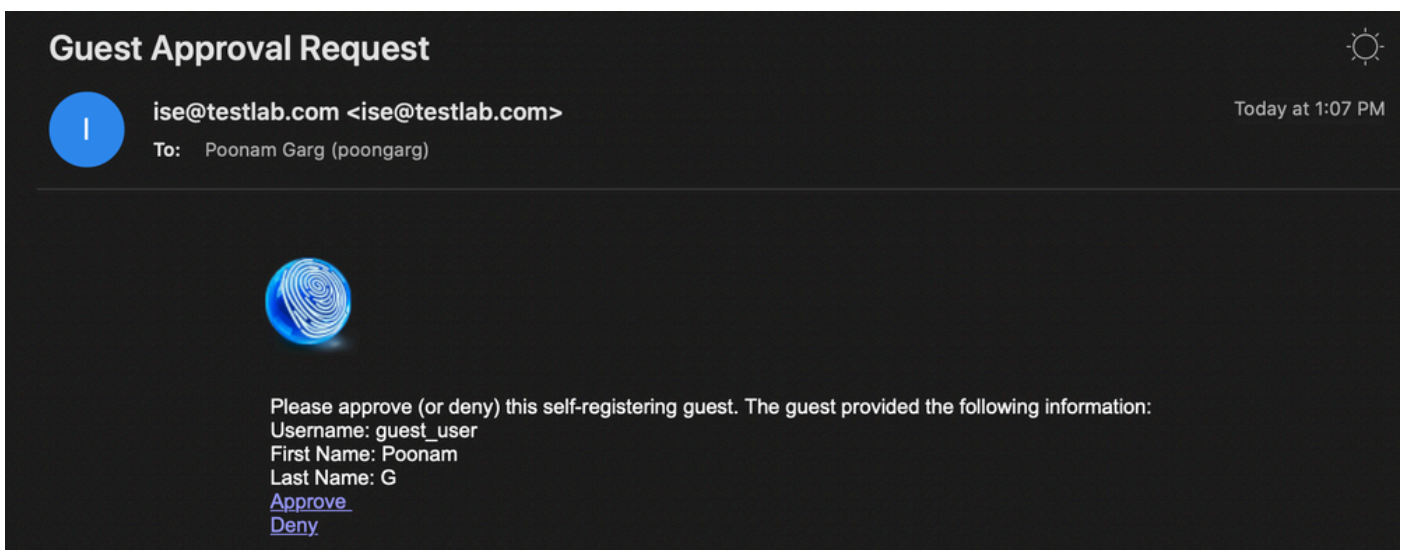
電子メールとSMTPサーバを適切に設定すると、アカウントが作成されます。





Require guests to be approved オプションを有効にすると、ユーザ名フィールドとパスワードフィールドが Include this information on the Self-Registration Success page セクションから自動的に削除されます。このため、スポンサーの承認が必要な場合、アカウントが作成されたことを示す情報を表示する Web ページには、ゲストユーザのクレデンシャルがデフォルトでは表示されません。代わりに、ショートメッセージサービス(SMS)または電子メールで配信する必要があります。このオプションは、Send credential notification upon approval using セクション(mark email/SMS)で有効にする必要があります。

スポンサーに通知メールが送信されます。



スポンサーが承認リンクをクリックし、スポンサーポータルにログインすると、アカウントが承認されます。



この時点から、ゲストユーザはログインを許可されます (電子メールまたはSMSで受信したクレ

デンシヤルを使用)。

要約すると、このフローでは3つの電子メールアドレスが使用されます。

- 通知の「送信元」アドレス。これは静的に定義されるか、またはスポンサーアカウントから取得され、スポンサーへの通知（承認のため）とゲストへのクレデンシヤルの詳細の両方の送信元アドレスとして使用されます。これは、Work Centers > Guest Access > Settings > Guest Email Settingsで設定します。
- 通知の「宛先」アドレス。これは、スポンサーに承認のアカウントを受信したことを通知するために使用されます。これは、ゲストポータルでWork Centers > Guest Access > Guest Portals > Portals and Components > Portal Name > Registration Form Settings > Require guests to be approved > Email approval request toの順に選択することで設定されます。
- ゲストの「宛先」アドレス。これは、登録時にゲストユーザによって提供されます。Send credential notification upon approval using Emailが選択されている場合、クレデンシヤルの詳細（ユーザ名とパスワード）が記載された電子メールがゲストに配信されます。

SMS経由で資格情報を配信する

ゲストクレデンシヤルはSMSでも配信できます。次のオプションを設定する必要があります。

1. Registration Form SettingsでSMSサービスプロバイダーを選択します。

SMS Service Provider

Guests can choose from these SMS providers:

- Global Default
- T-Mobile
- ATT
- Verizon
- ClickatellViaSMTP
- Orange
- Inmobile
- TheRingRingCompany
- Sprint
- NaaS

Guest see providers list only if multiple are selected

Configure SMS providers at:

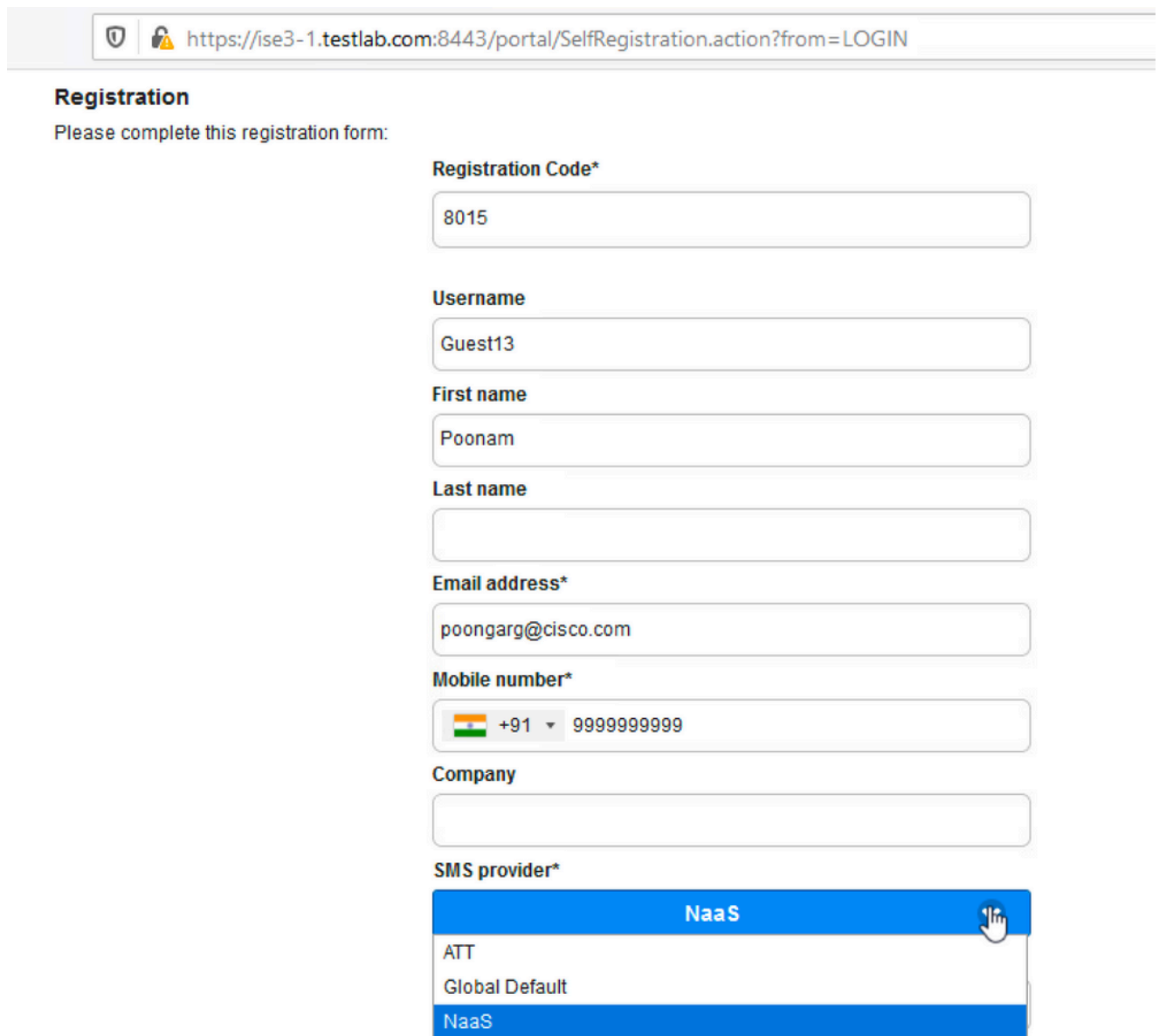
[Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

2. Send credential notification upon approval using: SMSチェックボックスにチェックマークを付けます。

Send credential notification upon approval using:

- Email
- SMS

3. 次に、ゲストユーザがアカウントを作成するときに、使用可能なプロバイダーを選択するように求められます。



Registration
Please complete this registration form:

Registration Code*
8015

Username
Guest13

First name
Poonam

Last name

Email address*
poongarg@cisco.com

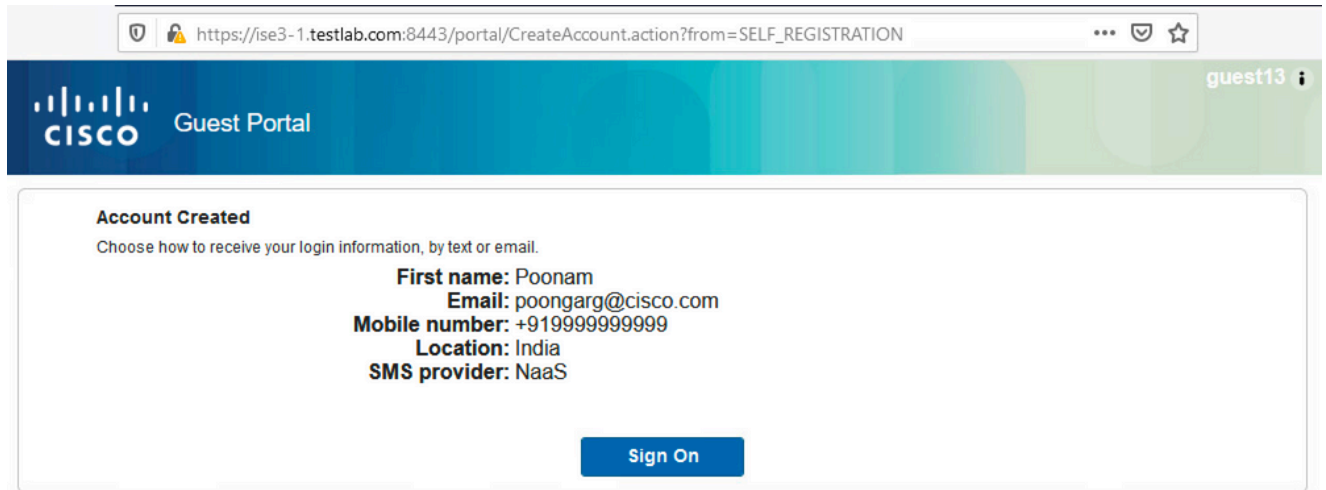
Mobile number*
+91 9999999999

Company

SMS provider*
NaaS

ATT
Global Default
NaaS

4. 選択したプロバイダーと電話番号を含むSMSが配信されます。



5. SMSプロバイダーは、Administration > System > Settings > SMS Gatewayで設定できます。

デバイスの登録

ゲストユーザがログインしてAUPを受け入れた後で、Allow guests to register devicesオプションを選択すると、デバイスを登録できます。

Guest Device Registration Settings

- Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

- Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

[Work Centers > Guest Access > Configure > Guest Types](#)

Device Registration

You can add a maximum of 5 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)

D0:37:45:89:EF:64

デバイスがすでに自動的に追加されている（[デバイスの管理]リストに表示されている）ことに注目してください。これは、「ゲストデバイスを自動的に登録」が選択されているためです。

ポスチャ

Require guest device complianceオプションが選択されている場合、ゲストユーザは、ログインしてAUPを受け入れた（およびオプションでデバイス登録を実行した）後にポスチャ(NAC/Web Agent)を実行するエージェントでプロビジョニングされます。ISEはクライアントプロビジョニングルールを処理して、プロビジョニングする必要があるエージェントを決定します。次に、ステーションで実行されているエージェントが（ポスチャルールに従って）ポスチャを実行し、結果をISEに送信します。ISEは必要に応じてCoA再認証を送信し、認証ステータスを変更します。

許可ルールは次のようになります。

✔	Guest_Complaint	AND	<ul style="list-style-type: none"> IdentityGroup-Name EQUALS Endpoint Identity Groups: Cisco_GuestEndpoints Wireless_MAB Radius-Called-Station-ID CONTAINS Guest Session-PostureStatus EQUALS Compliant 	PermitAccess ×	▼ +
✔	Permanent_Guest_Access	AND	<ul style="list-style-type: none"> IdentityGroup-Name EQUALS Endpoint Identity Groups: Cisco_GuestEndpoints Wireless_MAB Radius-Called-Station-ID CONTAINS Guest 	Limited_Access ×	▼ +
✔	Wifi_Redirect_to_Guest_Portal	AND	<ul style="list-style-type: none"> Radius-Called-Station-ID CONTAINS Guest Wireless_MAB 	Guest-Portal ×	▼ +

Guest_Authenticateルールが発生した最初の新規ユーザは、自己登録ゲストポータルにリダイレクトされます。ユーザが自己登録してログインすると、CoAは認証ステータスを変更し、ユーザ

にはポスチャと修復を実行するための制限付きアクセスが提供されます。NACエージェントがプロビジョニングされ、ステーションが準備した後にのみ、CoAはインターネットへのアクセスを提供するために認可ステータスを再度変更します。

ポスチャの一般的な問題には、正しいクライアントプロビジョニングルールがないことが含まれます。



これは、guest.logファイルを調べる場合にも確認できます。

<#root>

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

BYOD

Allow employees to use personal devices on the networkオプションが選択されている場合、このポータルを使用する企業ユーザはBYODフローを通過して個人デバイスを登録できます。ゲストユーザの場合、この設定は何も変更しません。

「ゲストとしてポータルを使用する従業員」とはどのような意味ですか。

デフォルトでは、ゲストポータルはGuest_Portal_Sequence IDストアで設定されます。

▼ Portal Settings

HTTPS port: * 8443 (8000 - 8999)

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

If bonding is not configured on a PSN, use: ⓘ	If bonding is configured on a PSN, use: ⓘ
<input checked="" type="checkbox"/> Gigabit Ethernet 0 <input type="checkbox"/> Gigabit Ethernet 1 <input type="checkbox"/> Gigabit Ethernet 2 <input type="checkbox"/> Gigabit Ethernet 3 <input type="checkbox"/> Gigabit Ethernet 4 <input type="checkbox"/> Gigabit Ethernet 5	<input checked="" type="checkbox"/> Bond 0 Uses Gigabit Ethernet 0 as primary , 1 as backup . <input type="checkbox"/> Bond 1 Uses Gigabit Ethernet 2 as primary , 3 as backup . <input type="checkbox"/> Bond 2 Uses Gigabit Ethernet 4 as primary , 5 as backup .

Certificate group tag: * Default Portal Certificate Group ▼

Configure certificates at:

[Work Centers > Guest Access > Administration > System Certificates](#)

Authentication method: * Guest_Portal_Sequence ▼ ⓘ

Configure authentication methods at:

[Work Centers > Guest Access > Identities > Identity Source Sequences](#)

これは、最初に（ゲストユーザの前に）内部ユーザを試行し、次にADクレデンシャルを試行する内部ストアシーケンスです。選択したIDストアに認証アクセスできない場合、詳細設定はシーケンス内の次のストアに進むことであるため、内部クレデンシャルまたはADクレデンシャルを持つ従業員はポータルにログインできます。

Overview **Identities** Identity Groups Ext Id Sources Administration Network Devices Portals & Components

Endpoints
Network Access Users
Identity Source Sequences

Identity Source Sequence

* Name Guest_Portal_Sequence

Description
A built-in Identity Sequence for the Guest Portal

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
	Guest Users
	All_AD_Join_Points

ゲストポータルのこの段階では、ユーザは内部ユーザストアまたはActive Directoryで定義されたクレデンシャルを提供し、BYODリダイレクションが発生します。

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.

The following system was detected

Windows

Was your device detected incorrectly?

Select your Device

Windows

Start

このように、企業ユーザは個人所有デバイスに対してBYODを実行できます。

内部ユーザ/ADクレデンシャルの代わりにゲストユーザのクレデンシャルが提供されると、通常のフローが継続されます (BYODなし)。

VLANの変更

これにより、DHCPの解放と更新をトリガーするactiveXまたはJavaアプレットを実行できます。これは、CoAがエンドポイントのVLANの変更をトリガーする場合に必要です。MABが使用されている場合、エンドポイントはVLANの変更を認識しません。考えられる解決策は、NACエージェントでVLAN (DHCPリリース/更新) を変更することです。別のオプションとして、Webページに返されたアプレットを使用して新しいIPアドレスを要求する方法もあります。リリース/CoA/更新間の遅延を設定できます。このオプションは、モバイルデバイスではサポートされていません。

関連情報

- [Cisco ISE コンフィギュレーション ガイドのポスチャ サービス](#)
- [アイデンティティ サービス エンジンのワイヤレス BYOD](#)
- [BYOD 対応 ISE SCEP サポートの設定例](#)
- [WLC と ISE での中央 Web 認証の設定例](#)
- [ISE を搭載した WLC 上で FlexConnect AP を使用した 中央 Web 認証の設定例](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。