

Esempio di configurazione di ISE Version 1.3 Self Registered Guest Portal

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Topologia e flusso](#)

[Configurazione](#)

[WLC](#)

[ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Configurazione opzionale](#)

[Impostazioni registrazione automatica](#)

[Impostazioni guest di accesso](#)

[Impostazioni registrazione dispositivo](#)

[Impostazioni conformità dispositivo guest](#)

[Impostazioni BYOD](#)

[Account approvati dallo sponsor](#)

[Consegna credenziali tramite SMS](#)

[Registrazione dispositivo](#)

[Postura](#)

[BYOD](#)

[Modifica della VLAN](#)

[Informazioni correlate](#)

Introduzione

Cisco Identity Services Engine (ISE) versione 1.3 dispone di un nuovo tipo di portale per utenti guest, denominato Self Registered Guest Portal, che consente agli utenti guest di eseguire la registrazione automatica quando ottengono l'accesso alle risorse di rete. Questo portale consente di configurare e personalizzare più funzionalità. In questo documento viene descritto come configurare questa funzionalità e come risolverne i problemi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione ISE e delle conoscenze base sui seguenti argomenti:

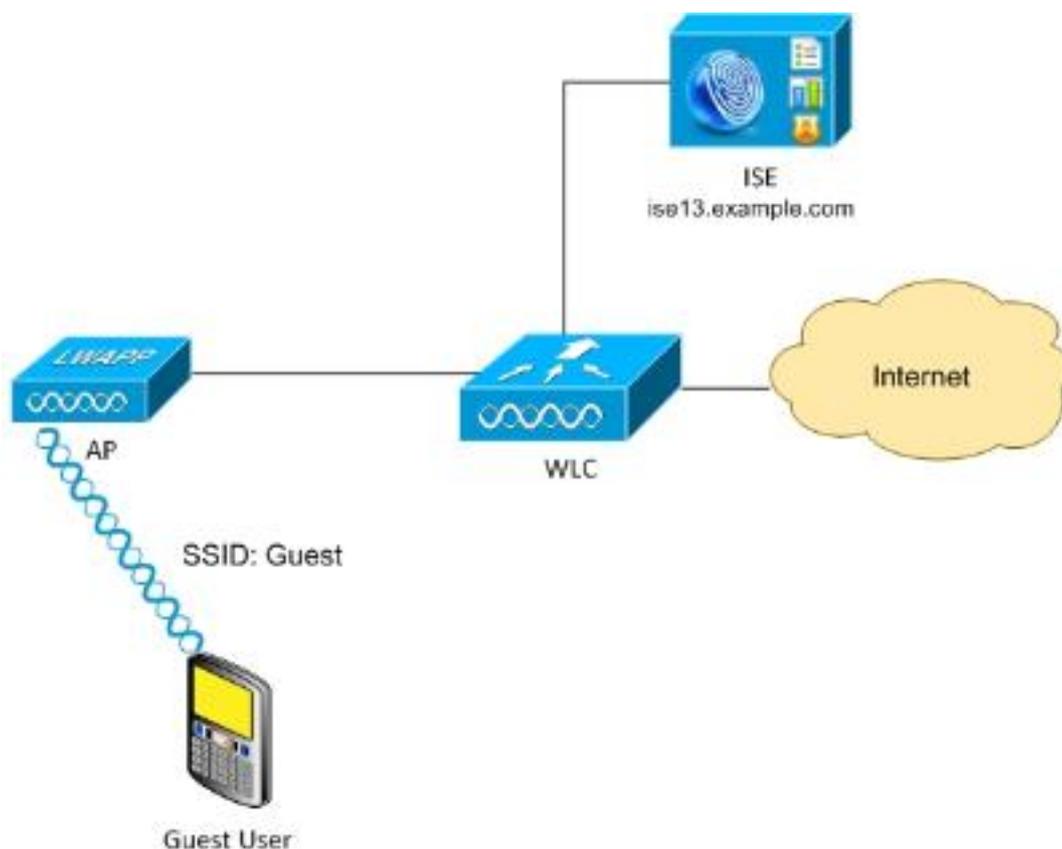
- Implementazioni ISE e flussi guest
- Configurazione dei controller WLC

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7
- Cisco WLC versione 7.6 e successive
- Software ISE, versione 3.1 e successive

Topologia e flusso



In questo scenario vengono presentate diverse opzioni disponibili per gli utenti guest quando eseguono la registrazione automatica.

Di seguito è riportato il flusso generale:

Passaggio 1. L'utente guest viene associato a SSID (Service Set Identifier): Guest Questa è una rete aperta con filtro MAC e ISE per l'autenticazione. Questa autenticazione corrisponde alla seconda regola di autorizzazione su ISE e il profilo di autorizzazione reindirizza al portale Guest Self Registered. ISE restituisce un elemento RADIUS Access-Accept con due coppie cisco-av:

- url-redirect-acl (il traffico deve essere reindirizzato e il nome dell'elenco di controllo di accesso (ACL) definito localmente sul WLC)
- url-redirect (dove reindirizzare il traffico all'ISE)

Passaggio 2. L'utente guest viene reindirizzato ad ISE. Aniché fornire le credenziali per l'accesso, l'utente fa clic su "Non ha un account". L'utente viene reindirizzato a una pagina in cui è possibile creare l'account. È possibile attivare un codice di registrazione segreto facoltativo per limitare il privilegio di autoregistrazione agli utenti che conoscono tale valore segreto. Dopo la creazione dell'account, all'utente vengono fornite le credenziali (nome utente e password) e consente di eseguire l'accesso con tali credenziali.

Passaggio 3. ISE invia al WLC un messaggio CoA (Change of Authorization) RADIUS autenticato nuovamente. Il WLC autentica nuovamente l'utente quando invia la richiesta di accesso RADIUS con l'attributo Authorize-Only. ISE risponde con ACL Access-Accept e Airespace definiti localmente sul WLC, che fornisce accesso solo a Internet (l'accesso finale per gli utenti guest dipende dalla policy di autorizzazione).

Notare che per le sessioni EAP (Extensible Authentication Protocol), ISE deve inviare un messaggio CoA Terminate per attivare la riautenticazione, in quanto la sessione EAP è tra il richiedente e l'ISE. Ma per MAB (filtro MAC), il riautenticazione CoA è sufficiente; non è necessario annullare l'associazione o l'autenticazione del client wireless.

Passaggio 4. L'utente guest ha desiderato accedere alla rete.

È possibile abilitare diverse funzioni aggiuntive, ad esempio la postura e il BYOD (Bring Your Own Device), illustrate più avanti.

Configurazione

WLC

1. Aggiungere il nuovo server RADIUS per Authentication and Accounting. Selezionare **Security > AAA > Radius > Authentication** (Sicurezza > AAA > Radius > Autenticazione) per abilitare RADIUS CoA (RFC 3576).

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar is titled 'Security' and contains a tree view with 'AAA' expanded to show 'RADIUS' and its sub-items: 'Authentication', 'Accounting', 'Fallback', and 'DNS'. Other items include 'TACACS+', 'LDAP', 'Local Net Users', 'MAC Filtering', 'Disabled Clients', 'User Login Policies', 'AP Policies', and 'Password Policies'. Below these are 'Local EAP', 'Priority Order', 'Certificate', and 'Access Control Lists'. The main content area is titled 'RADIUS Authentication Servers > Edit' and displays the following configuration:

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 customer)
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

Esiste una configurazione simile per l'accounting. Si consiglia inoltre di configurare il WLC in modo che invii un SSID nell'attributo ID della stazione chiamata, che consente all'ISE di configurare regole flessibili basate su SSID:

This screenshot shows the 'RADIUS Authentication Servers' configuration page. The left sidebar is similar to the previous one, but 'Authentication' is highlighted with a dashed box. The main content area shows the following settings:

Acct Call Station ID Type	IP Address
Auth Call Station ID Type	AP MAC Address:SSID

- Nella scheda WLAN, creare il guest WLAN (Wireless LAN) e configurare l'interfaccia corretta. Impostare la sicurezza di layer 2 su **None** con il filtro MAC. In Server di sicurezza/autenticazione, autorizzazione e accounting (AAA), selezionare l'indirizzo IP ISE per l'autenticazione e l'accounting. Nella scheda Advanced (Avanzate), abilitare l'opzione **AAA Override** e impostare lo stato di Network Admission Control (NAC) su RADIUS NAC (supporto CoA).
- Passare a **Sicurezza > Liste di controllo dell'accesso > Liste di controllo dell'accesso** e creare due elenchi di accesso:

GuestRedirect, che consente il traffico che non deve essere reindirizzato e reindirizza tutto il resto del traffico Internet, negata per le reti aziendali e permessa per tutte le altre

Di seguito è riportato un esempio di ACL GuestRedirect (è necessario escludere il traffico

da/verso ISE dal reindirizzamento):

The screenshot shows the Cisco ISE Security configuration interface. The left sidebar contains a navigation menu with categories like AAA, RADIUS, TACACS+, Local EAP, and Priority Order. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab for an 'Access List Name' of 'GuestRedirect'. It displays 'Deny Counters' as 0 and a table of rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	10.62.97.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
2	Permit	0.0.0.0 / 0.0.0.0	10.62.97.21 / 255.255.255.255	Any	Any	Any	Any	Any

ISE

1. Passare ad **Accesso guest > Configura > Portali guest** e creare un nuovo tipo di portale, Portale guest con registrazione automatica:

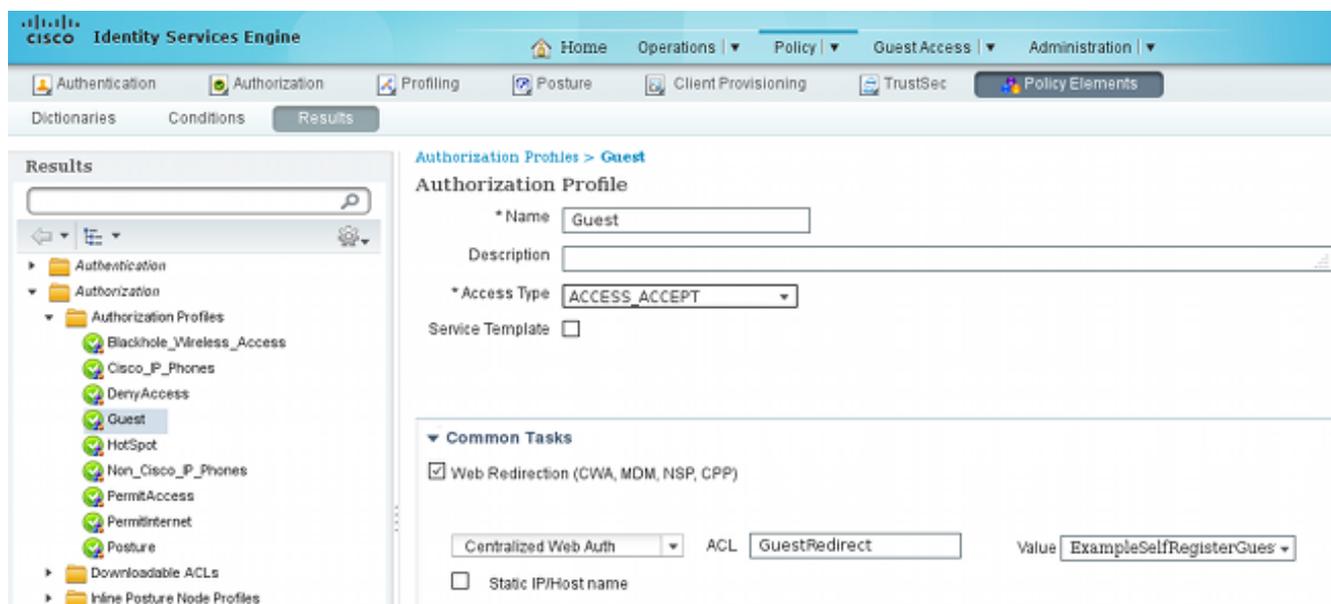
The screenshot shows the Cisco ISE Identity Services Engine configuration page for 'Configure Guest Access and Sponsor Setup'. A modal dialog titled 'Create Guest Portal - Choose Portal Type' is open, allowing the user to select a portal type. The options are:

- Sponsored-Guest Portal: Sponsors create guests' accounts. Guests cannot create their own accounts.
- Self-Registered Guest Portal: Guests provide information to automatically create an account, with sponsor approval as an optional requirement.
- Hotspot Guest Portal: Guests can access the network without credentials, but you can add a welcome message and AUP.

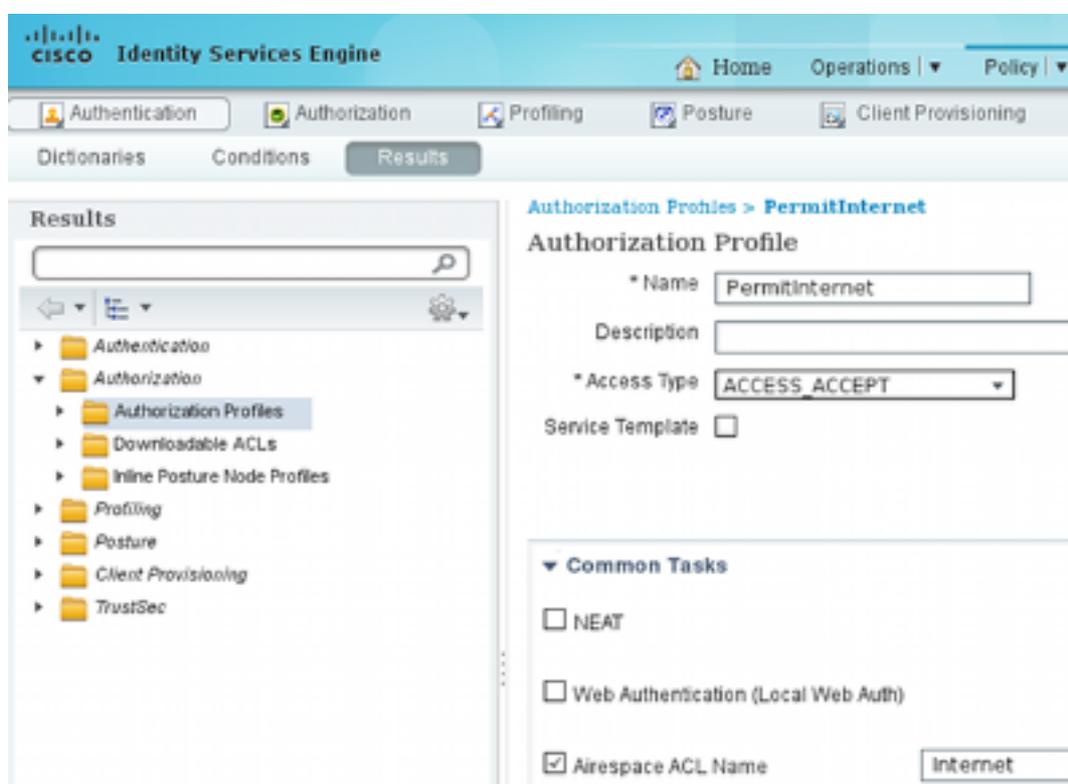
Buttons for 'Continue...' and 'Cancel' are visible at the bottom of the dialog. A note at the bottom of the page states: 'To authorize a portal for use, you must create an Authorization profile for it and then reference that profile in a rule in the Authorization policy.'

2. Scegliere il nome del portale a cui verrà fatto riferimento nel profilo di autorizzazione. Impostare tutte le altre impostazioni sui valori predefiniti. In Personalizzazione pagine portale è possibile personalizzare tutte le pagine presentate.
3. Configura profili di autorizzazione:

Guest (con reindirizzamento al nome del portale Guest e ACL GuestRedirect)



PermitInternet (con ACL Airespace uguale a Internet)



- Per verificare le regole di autorizzazione, passare a **Criterio > Autorizzazione**. In ISE versione 1.3, per impostazione predefinita, l'autenticazione MAB (MAC Authentication Bypass) non riuscita (indirizzo MAC non trovato) continua (non rifiutata). Questa opzione è molto utile per i portali guest poiché non è necessario modificare le regole di autenticazione predefinite.

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 GuestEndpoints AND Radius:Called-Station-ID CONTAINS Guest	then PermitInternet
✓	Guest_Authenticate	if Radius:Called-Station-ID CONTAINS Guest	then Guest

I nuovi utenti associati al SSID guest non fanno ancora parte di alcun gruppo di identità. Per questo motivo soddisfano la seconda regola, che utilizza il profilo di autorizzazione Guest per reindirizzarli al portale Guest corretto.

Dopo che un utente ha creato un account e ha eseguito l'accesso, ISE invia una richiesta RADIUS CoA e il WLC esegue la riautenticazione. Questa volta, la prima regola viene soddisfatta insieme al profilo di autorizzazione PermitInternet e restituisce il nome ACL applicato sul WLC.

5. Aggiungere il WLC come dispositivo di accesso alla rete da **Amministrazione > Risorse di rete > Dispositivi di rete**.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

1. Dopo aver eseguito l'associazione con il SSID guest e aver digitato un URL, si viene reindirizzati alla pagina di accesso:

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:

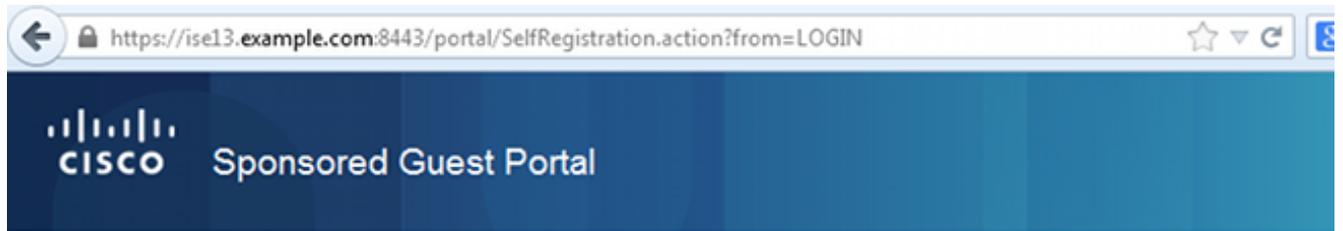
Passcode:

Sign On

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

[Contact Support](#)

2. Poiché non si dispone ancora di credenziali, è necessario scegliere **Non si dispone di un account?** opzione. Viene visualizzata una nuova pagina che consente la creazione di account. Se l'opzione Codice di registrazione è stata attivata nella configurazione del portale guest, il valore segreto è obbligatorio (in questo modo viene garantita la registrazione automatica solo agli utenti con autorizzazioni corrette).



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. In caso di problemi relativi alla password o ai criteri utente, selezionare **Accesso guest > Impostazioni > Criteri password guest** o **Accesso guest > Impostazioni > Criteri nome utente guest** per modificare le impostazioni. Di seguito è riportato un esempio:

▶ **Guest Email Settings** Identify the SMTP server and specify the email domain.

▶ **Guest Locations and SSIDs** Specify the locations where you want to offer guest access.

▶ **Guest Password Policy** Specify the policy settings that will be enforced for guest passwords.

▼ **Guest Username Policy** Specify the policy settings that will be enforced for guest usernames.
 Configure username requirements that will be enforced for guest usernames. Username requirements include:

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)

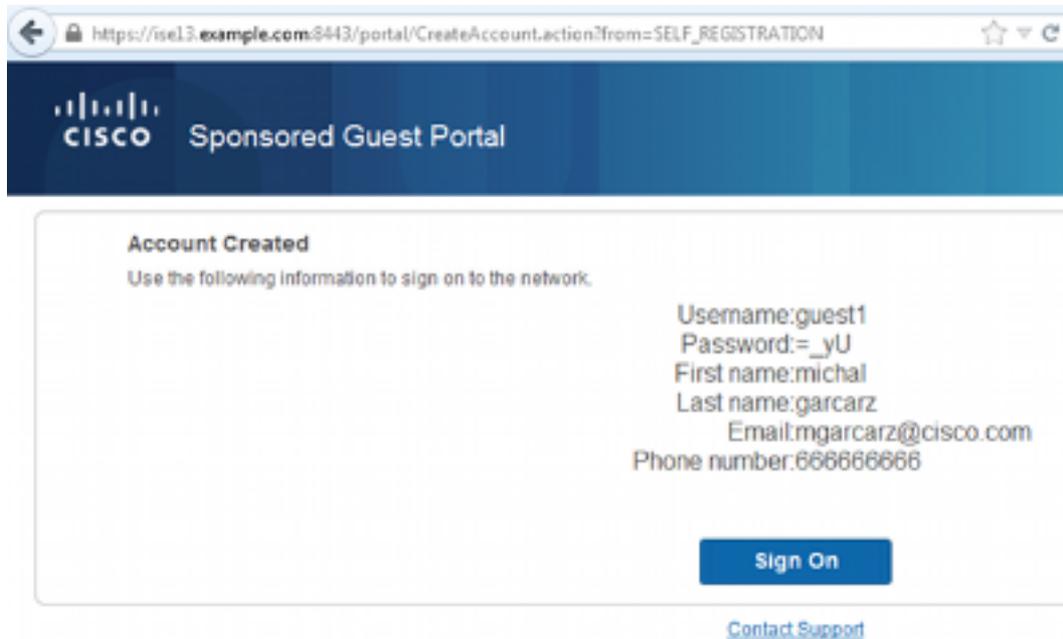
Numeric:

Minimum numeric: (0-64)

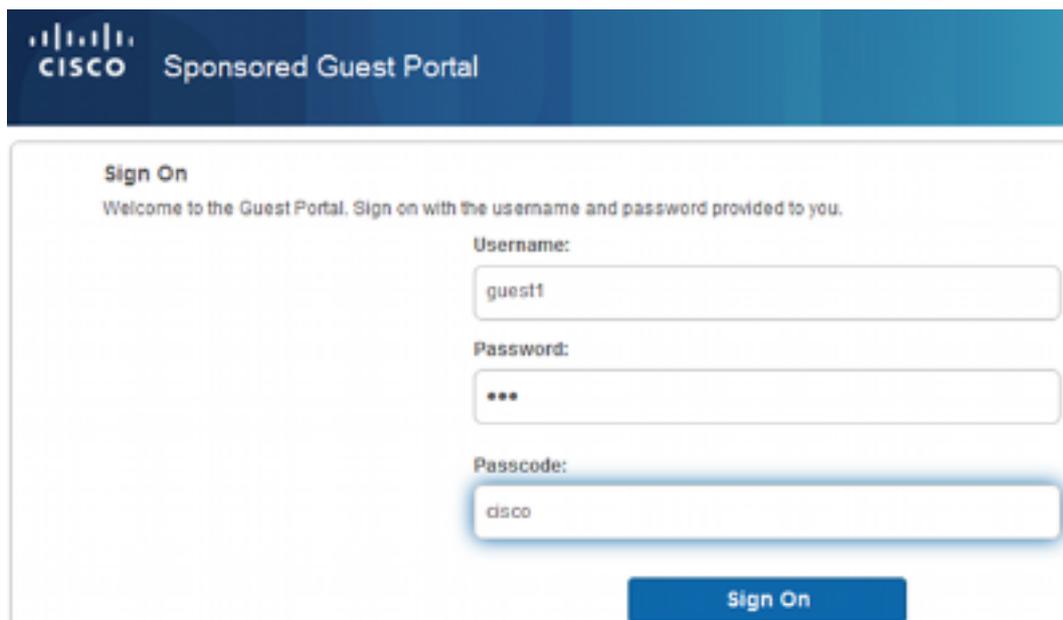
Special:

Minimum special: (0-64)

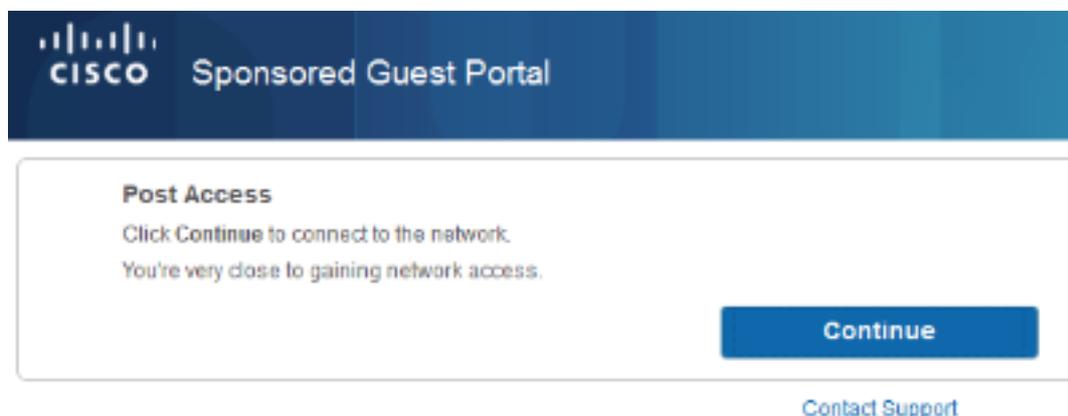
4. Dopo la creazione dell'account, vengono visualizzate le credenziali (password generata in base ai criteri password guest):



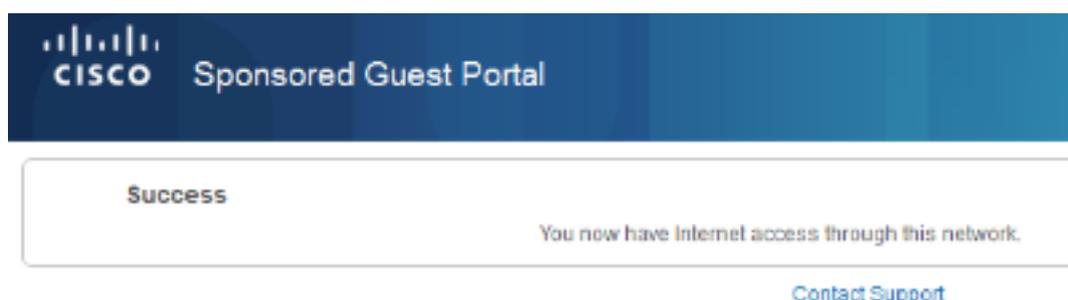
5. Fare clic su **Sign On** (Accedi) e fornire le credenziali (potrebbe essere necessario un passcode di accesso aggiuntivo se configurato in Guest Portal; si tratta di un altro meccanismo di sicurezza che consente l'accesso solo a coloro che conoscono la password).



6. Se l'operazione ha esito positivo, è possibile che venga presentato un criterio di utilizzo accettabile opzionale (se configurato nel portale guest). Potrebbe essere visualizzata anche la pagina Post Access (configurabile anche in Guest Portal).



L'ultima pagina conferma che l'accesso è stato concesso:



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

In questa fase, ISE presenta i seguenti log:

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding
0	0	82	0

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

Ecco il flusso:

- L'utente guest incontra la seconda regola di autorizzazione (Guest_Authenticate) e viene reindirizzato a Guest ("Autenticazione completata").
- L'ospite viene reindirizzato per la registrazione automatica. Dopo aver eseguito correttamente l'accesso (con l'account appena creato), ISE invia il messaggio di autenticazione CoA, che viene confermato dal WLC ("Autorizzazione dinamica riuscita").

- Il WLC esegue la riautenticazione con l'attributo Authorize-Only e viene restituito il nome ACL ("Authorize-Only success"). Al guest viene fornito l'accesso alla rete corretto.

I rapporti (**Operazioni > Rapporti > Rapporti ISE > Rapporti Accesso guest > Rapporto Guest principale**) confermano anche che:

Master Guest Report								Favorite
From 08/01/2014 12:00:00 AM to 08/01/2014 02:42:34 PM								Page << 1 >>
Logged At	Guest User Name	MAC Address	IP Address	Operation	User Name	Message	AUP Acceptance	
2014-08-01 13:18:49.9	quest1	64-66-83-08-23-A3	10.221.0.218				Guest user has accepted the use policy	
2014-08-01 13:18:08.7	quest1	64-66-83-08-23-A3	10.221.0.218	Add	SelfRegistration			

Un utente sponsor (con privilegi corretti) è in grado di verificare lo stato corrente di un utente guest.

In questo esempio viene confermata la creazione dell'account, ma l'utente non ha mai eseguito l'accesso ("In attesa dell'accesso iniziale"):

The screenshot shows the Cisco Sponsor Portal interface. At the top, there is a navigation bar with the Cisco logo and the text "Sponsor Portal". Below the navigation bar, there are several tabs: "Create Accounts", "Manage Accounts (1)", "Pending Accounts (0)", and "Notices (0)". Underneath the tabs, there are buttons for "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:	quest1
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

Configurazione opzionale

Per ogni fase del flusso è possibile configurare diverse opzioni. Tutto questo è configurato per il portale guest in **Accesso guest > Configura > Portali guest > NomePortale > Modifica > Impostazioni comportamento e flusso del portale**. Le impostazioni più importanti includono:

Impostazioni registrazione automatica

- Tipo di ospite: descrive il periodo di attività dell'account, le opzioni di scadenza della password, le ore di accesso e le opzioni (una combinazione di profilo temporale e ruolo di ospite di ISE versione 1.2)
- Codice di registrazione: se questa opzione è abilitata, solo gli utenti che conoscono il codice segreto possono eseguire la registrazione automatica (devono fornire la password al momento della creazione dell'account)
- AUP - Accetta criteri d'uso durante la registrazione automatica
- Obbligo per lo sponsor di approvare/attivare l'account guest

Impostazioni guest di accesso

- Codice di accesso: se abilitato, solo gli utenti guest che conoscono il codice segreto possono accedere
- AUP - Accetta criteri d'uso durante la registrazione automatica
- Opzione modifica password

Impostazioni registrazione dispositivo

- Per impostazione predefinita, il dispositivo viene registrato automaticamente

Impostazioni conformità dispositivo guest

- Consente una postura all'interno del flusso

Impostazioni BYOD

- Consente agli utenti aziendali che utilizzano il portale come utenti guest di registrare i propri dispositivi personali

Account approvati dallo sponsor

Se è selezionata l'opzione **Richiedi approvazione ospiti registrati automaticamente**, l'account creato dall'ospite deve essere approvato da uno sponsor. Questa funzionalità potrebbe utilizzare la posta elettronica per inviare la notifica allo sponsor (per l'approvazione dell'account guest):

Se il server SMTP (Simple Mail Transfer Protocol) o il server predefinito per la notifica da posta elettronica non è configurato, l'account non verrà creato:

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

Il log di guest.log conferma che l'indirizzo iniziale globale utilizzato per la notifica è mancante:

```
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.
```

Se la configurazione e-mail è corretta, l'account viene creato:

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. Under the "Settings" menu, 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

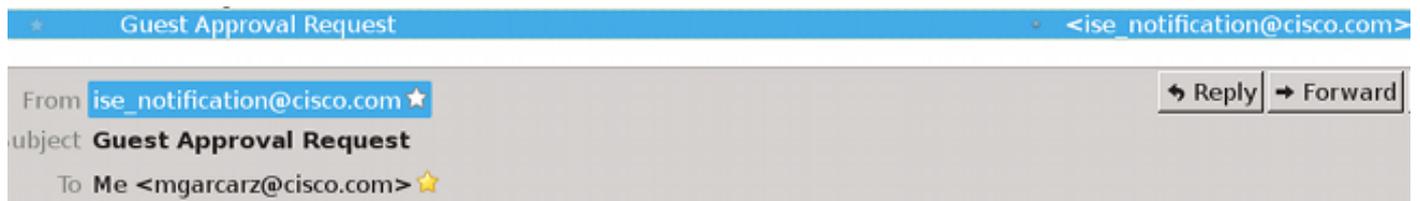
Use the following information to sign on to the network.

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

Sign On

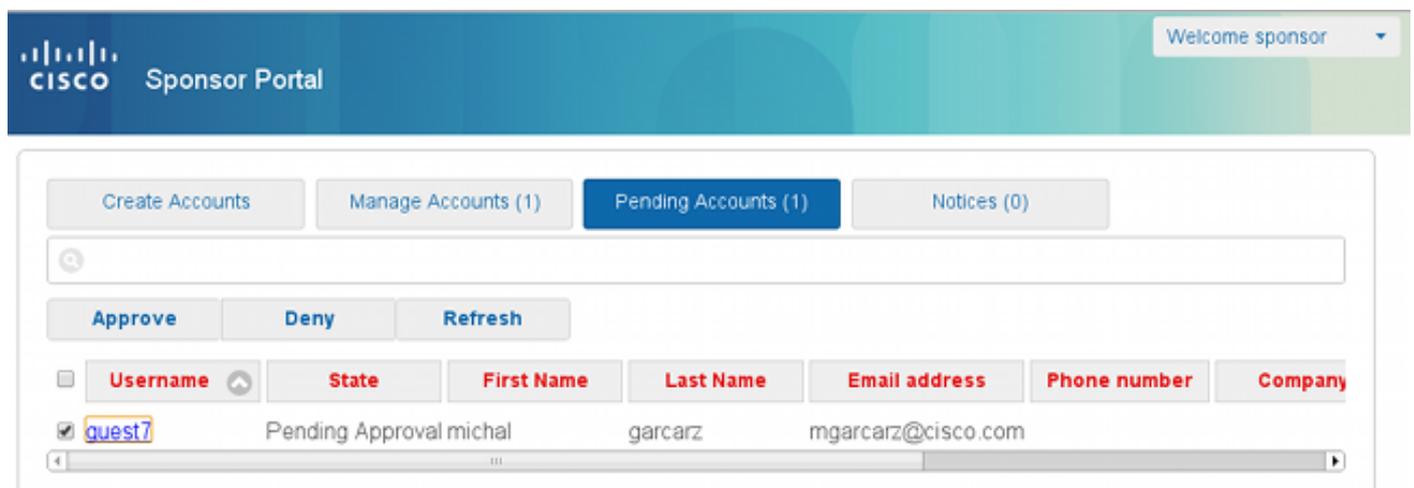
Dopo aver abilitato l'opzione **Richiedi approvazione ospiti registrati automaticamente**, i campi nome utente e password vengono automaticamente rimossi dalla sezione **Includi queste informazioni nella pagina Registrazione automatica riuscita**. Per questo motivo, quando è necessaria l'approvazione dello sponsor, le credenziali per gli utenti guest non vengono visualizzate per impostazione predefinita nella pagina Web che presenta informazioni che mostrano che l'account è stato creato. Devono invece essere recapitati tramite SMS o e-mail. Questa opzione deve essere abilitata nella sezione **Invia notifica credenziali all'approvazione tramite** (contrassegna e-mail/SMS).

Allo sponsor viene inviato un messaggio di posta elettronica di notifica:



Please approve (or deny) this self-registering guest. The guest provided the following information:
Username: guest7
First Name: michal
Last Name: garcarz

Lo sponsor accede al portale e approva l'account:



Da questo momento in poi, l'utente guest può eseguire l'accesso (con le credenziali ricevute tramite e-mail o SMS).

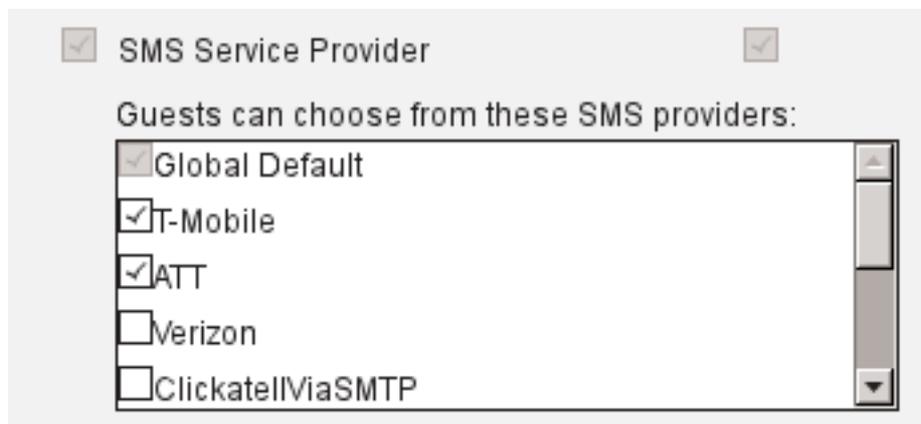
In sintesi, in questo flusso vengono utilizzati tre indirizzi e-mail:

- Indirizzo di notifica "Da". Questo valore viene definito in modo statico o prelevato dall'account dello sponsor e utilizzato come indirizzo Da per entrambi: notifica allo sponsor (per l'approvazione) e dettagli sulle credenziali all'ospite. Questa impostazione è configurata in **Accesso guest > Configura > Impostazioni > Impostazioni e-mail guest**.
- Indirizzo di notifica "A". Questa opzione viene utilizzata per notificare allo sponsor che ha ricevuto un account per l'approvazione. Questa opzione è configurata nel portale guest in **Accesso guest > Configura > Portali guest > Nome portale > Richiedi l'approvazione degli ospiti registrati automaticamente > Invia richiesta di approvazione tramite posta elettronica a**.
- Indirizzo Guest "To". Questo viene fornito dall'utente guest durante la registrazione. Se è selezionata l'opzione **Invia notifica delle credenziali all'approvazione tramite posta elettronica**, l'e-mail con i dettagli delle credenziali (nome utente e password) viene recapitata al guest.

Consegna credenziali tramite SMS

Le credenziali guest possono essere recapitate anche tramite SMS. È necessario configurare le seguenti opzioni:

1. Scegliere il provider di servizi SMS:



2. Controllare la **notifica Invia credenziali all'approvazione utilizzando**: Casella di controllo **SMS**.
3. Quindi, all'utente guest viene chiesto di scegliere il provider disponibile quando crea un account:

← <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. Viene inviato un SMS con il provider e il numero di telefono scelti:

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. È possibile configurare i provider SMS in **Amministrazione > Sistema > Impostazioni > Gateway SMS**.

Registrazione dispositivo

Se l'opzione **Consenti agli utenti guest di registrare i dispositivi** è selezionata dopo che un utente guest ha eseguito l'accesso e ha accettato le CDS, è possibile registrare i dispositivi:

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"/>
-------------------	---------------------------------------

Si noti che il dispositivo è già stato aggiunto automaticamente (si trova nell'elenco Gestione dispositivi). Ciò si verifica perché è stata selezionata la **registrazione automatica dei dispositivi guest**.

Postura

Se l'opzione **Richiedi conformità dispositivo guest** è selezionata, agli utenti guest viene assegnato un agente che esegue la postura (NAC/Web Agent) dopo l'accesso e l'accettazione dell'AUP (e facoltativamente la registrazione del dispositivo). ISE elabora le regole di provisioning client per decidere quale agente deve essere sottoposto a provisioning. L'agente in esecuzione sulla stazione esegue quindi la postura (in base alle regole di postura) e invia i risultati all'ISE, che invia la nuova autenticazione CoA per modificare lo stato di autorizzazione, se necessario.

Le regole di autorizzazione possibili potrebbero avere un aspetto simile al seguente:

▶ Exceptions (0)

Standard

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

I primi nuovi utenti che incontrano la regola Guest_Authenticate reindirizzano al portale Guest con registrazione automatica. Dopo che l'utente si è registrato e ha effettuato l'accesso, CoA cambia lo stato di autorizzazione e dispone di accesso limitato per eseguire la postura e la risoluzione dei problemi. Solo dopo il provisioning dell'agente NAC e la conformità della stazione, CoA cambia nuovamente lo stato di autorizzazione per fornire l'accesso a Internet.

I problemi tipici della postura includono la mancanza di regole di provisioning client corrette:

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](#)

Ciò può essere confermato anche esaminando il file guest.log (nuovo in ISE versione 1.3):

```
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

Se l'opzione **Consenti ai dipendenti di utilizzare i dispositivi personali in rete** è selezionata, gli utenti aziendali che utilizzano questo portale possono passare attraverso il flusso BYOD e registrare i dispositivi personali. Per gli utenti guest, questa impostazione non modifica nulla.

Cosa significa "dipendenti che utilizzano il portale come guest"?

Per impostazione predefinita, i portali guest sono configurati con l'archivio identità **Guest_Portal_Sequence**:

▼ 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](#)

Questa è la sequenza di memorizzazione interna che tenta prima gli utenti interni (prima degli utenti guest):

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

Quando in questa fase sul portale guest, l'utente fornisce le credenziali definite nell'archivio Utenti interni e si verifica il reindirizzamento BYOD:

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

In questo modo gli utenti aziendali possono eseguire BYOD per i dispositivi personali.

Quando invece delle credenziali degli utenti interni, vengono fornite le credenziali degli utenti guest, il flusso normale continua (senza BYOD).

Modifica della VLAN

Questa opzione è simile alla modifica della VLAN configurata per il portale guest in ISE versione 1.2. Permette di eseguire activeX o un'applet Java, che attiva DHCP per il rilascio e il rinnovo. Questa operazione è necessaria quando la funzione CoA attiva la modifica della VLAN per l'endpoint. Quando si usa il protocollo MAB, l'endpoint non rileva una modifica della VLAN. Una soluzione possibile è modificare la VLAN (rilascio/rinnovo DHCP) con l'agente NAC. In alternativa è possibile richiedere un nuovo indirizzo IP tramite l'applet restituito sulla pagina Web. È possibile configurare un ritardo tra rilascio/CoA/rinnovo. Questa opzione non è supportata per i dispositivi mobili.

Informazioni correlate

- [Guida alla configurazione dei servizi di postura di Cisco ISE](#)
- [BYOD wireless con Identity Services Engine](#)
- [Esempio di configurazione del supporto ISE SCEP per BYOD](#)
- [Guida per l'amministratore di Cisco ISE 1.3](#)
- [Esempio di autenticazione Web centralizzata su WLC e ISE](#)
- [Esempio di autenticazione Web centrale con punti di accesso FlexConnect su un WLC con configurazione ISE](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)