

ISE Version 1.3 Self Registered Guest Portal Configuration Example



Document ID: 118742

Contributed by Michal Garcarz and Nicolas Darchis, Cisco TAC Engineers.

Feb 13, 2015

Contents

Introduction

Prerequisites

Requirements

Components Used

Topology and Flow

Configure

WLC

ISE

Verify

Troubleshoot

Optional Configuration

Self-Registration Settings

Login Guest Settings

Device Registration Settings

Guest Device Compliance Settings

BYOD Settings

Sponsor-Approved Accounts

Deliver Credentials via SMS

Device Registration

Posture

BYOD

VLAN Change

Related Information

Introduction

Cisco Identity Services Engine (ISE) Version 1.3 has a new type of Guest Portal called the Self Registered Guest Portal, which allows guest users to self-register when they gain access to network resources. This Portal allows you to configure and customize multiple features. This document describes how to configure and troubleshoot this functionality.

Prerequisites

Requirements

Cisco recommends that you have experience with ISE configuration and basic knowledge of these topics:

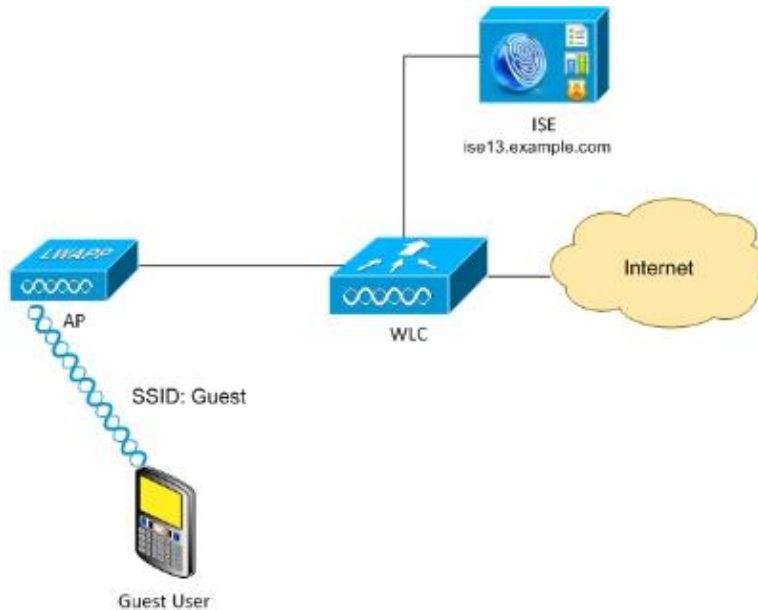
- ISE deployments and Guest flows
- Configuration of Wireless LAN Controllers (WLC)

Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows 7
- Cisco WLC Version 7.6 and Later
- ISE Software, Version 3.1 and Later

Topology and Flow



This scenario presents multiple options available for guest users when they perform self-registration.

Here is the general flow:

Step 1. Guest user associates to Service Set Identifier (SSID): Guest. This is an open network with MAC filtering with ISE for authentication. This authentication matches the second authorization rule on the ISE and the authorization profile redirects to the Guest Self Registered Portal. ISE returns a RADIUS Access-Accept with two cisco-av-pairs:

- url-redirect-acl (which traffic should be redirected, and the name of Access Control List (ACL) defined locally on the WLC)
- url-redirect (where to redirect that traffic- to ISE)

Step 2. The guest user is redirected to ISE. Rather than provide credentials in order to log in, the user clicks "Don't have a account". The user is redirected to a page where that account can be created. An optional secret registration code might be enabled in order to limit the self-registration privilege to people who know that secret value. After the account is created, the user is provided credentials (username and password) and logs in with those credentials.

Step 3. ISE sends a RADIUS Change of Authorization (CoA) Reauthenticate to the WLC. The WLC re-authenticates the user when it sends the RADIUS Access-Request with the Authorize-Only attribute. ISE responds with Access-Accept and Airespace ACL defined locally on the WLC, which provides access to the Internet only (final access for guest user depends on the authorization policy).

Note that for Extensible Authentication Protocol (EAP) sessions, ISE must send a CoA Terminate in order to trigger re-authentication because the EAP session is between the supplicant and the ISE. But for MAB (MAC filtering), CoA Reauthenticate is enough; there is no need to de-associate/de-authenticate the wireless client.

Step 4. The guest user has desired access to the network.

Multiple additional features like posture and Bring Your Own Device (BYOD) can be enabled (discussed later).

Configure

WLC

1. Add the new RADIUS server for Authentication and Accounting. Navigate to **Security > AAA > RADIUS > Authentication** in order to enable 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 shows the 'Security' menu with 'AAA' expanded to 'RADIUS' > 'Authentication'. The main content area is titled 'RADIUS Authentication Servers > Edit' and displays the following configuration details:

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

There is a similar configuration for Accounting. It is also advised to configure the WLC to send SSID in the Called Station ID attribute, which allows the ISE to configure flexible rules based on SSID:

This screenshot shows the 'RADIUS Authentication Servers' configuration page. The left sidebar shows 'Security' > 'AAA' > 'RADIUS' > 'Authentication'. The main content area shows the following settings:

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

2. Under the WLANs tab, create the Wireless LAN (WLAN) Guest and configure the Correct Interface. Set Layer2 security to *None* with MAC filtering. In Security/Authentication, Authorization, and Accounting (AAA) Servers, select the ISE IP address for both Authentication and Accounting. On the Advanced tab, enable *AAA Override* and set the Network Admission Control (NAC) State to RADIUS NAC (CoA support).

3. Navigate to *Security > Access Control Lists > Access Control Lists* and create two access lists:

- ◆ GuestRedirect, which permits traffic that should not be redirected and redirects all other traffic
- ◆ Internet, which is denied for corporate networks and permitted for all others

Here is an example for GuestRedirect ACL (need to exclude traffic to/from ISE from redirection):

Security

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Access Control Lists > Edit

General

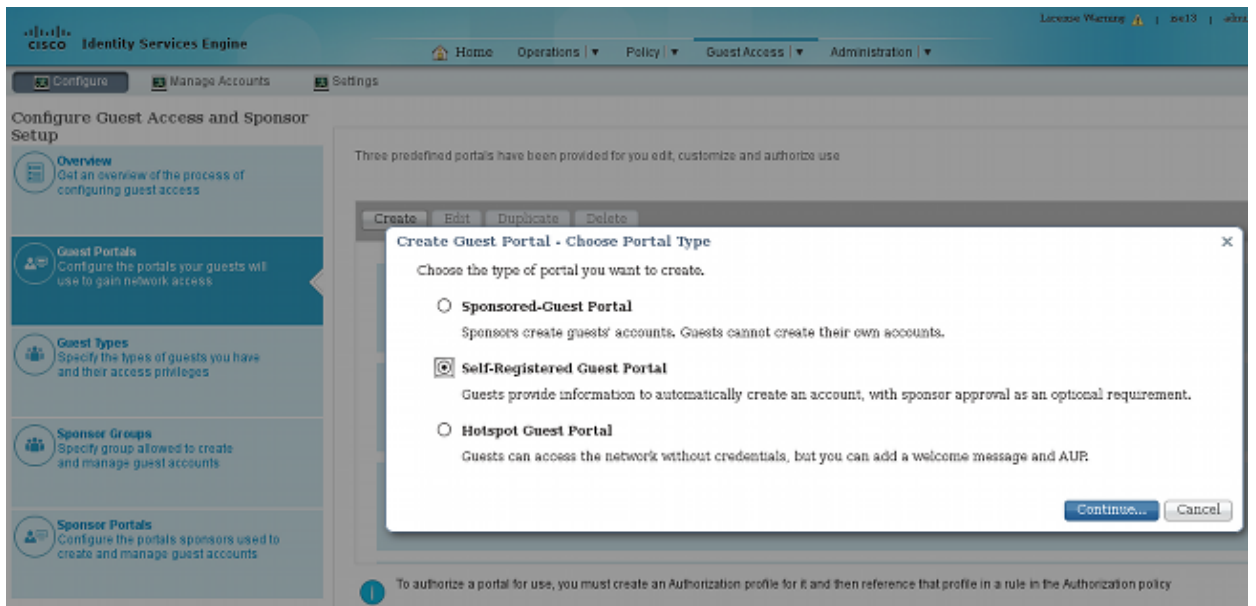
Access List Name GuestRedirect

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
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

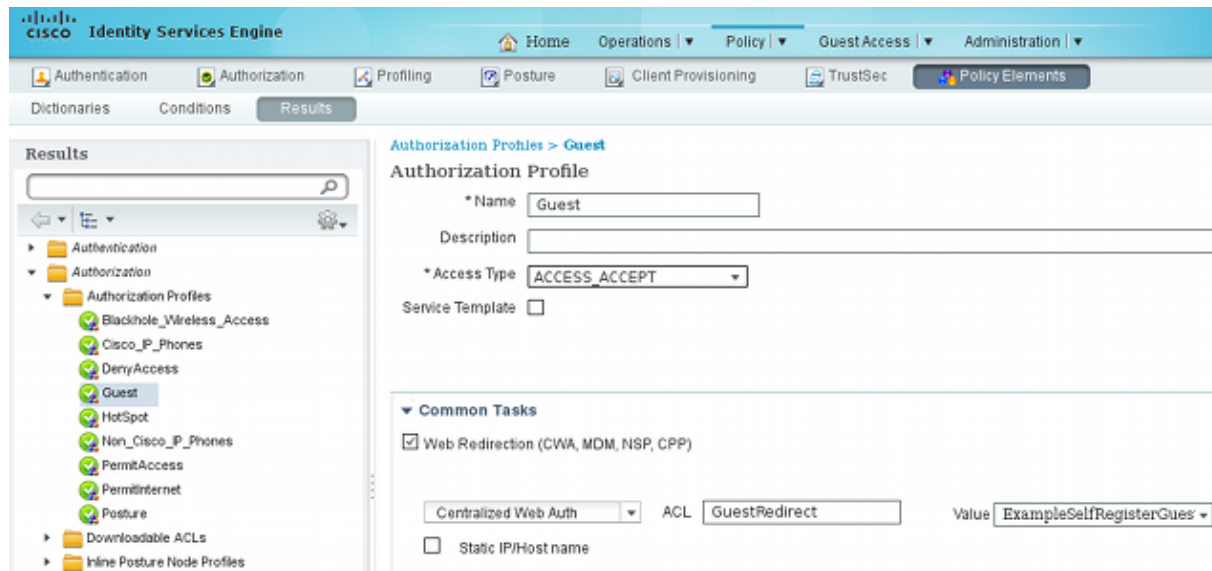
1. Navigate to *Guest Access > Configure > Guest Portals*, and create a new portal type, Self Registered Guest Portal:



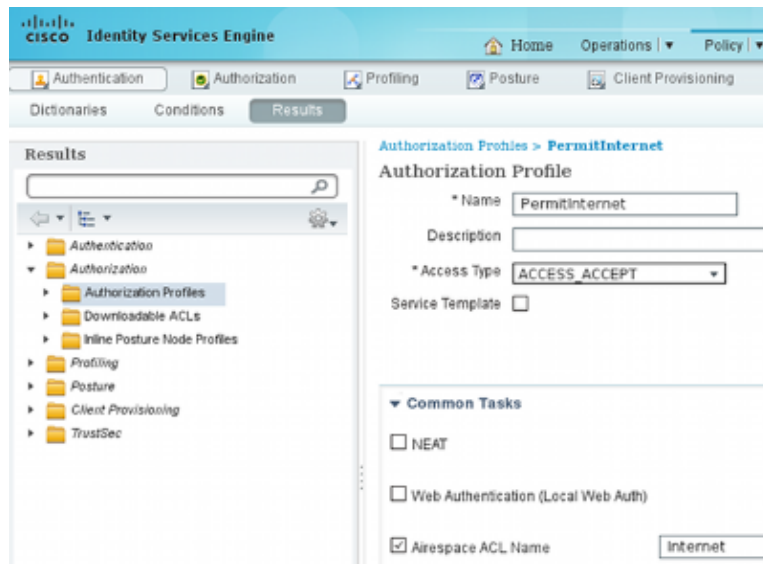
2. Choose the portal name that will be referenced in the authorization profile. Set all of the other settings to default. Under Portal Page Customization, all pages presented can be customized.

3. Configure Authorization profiles:

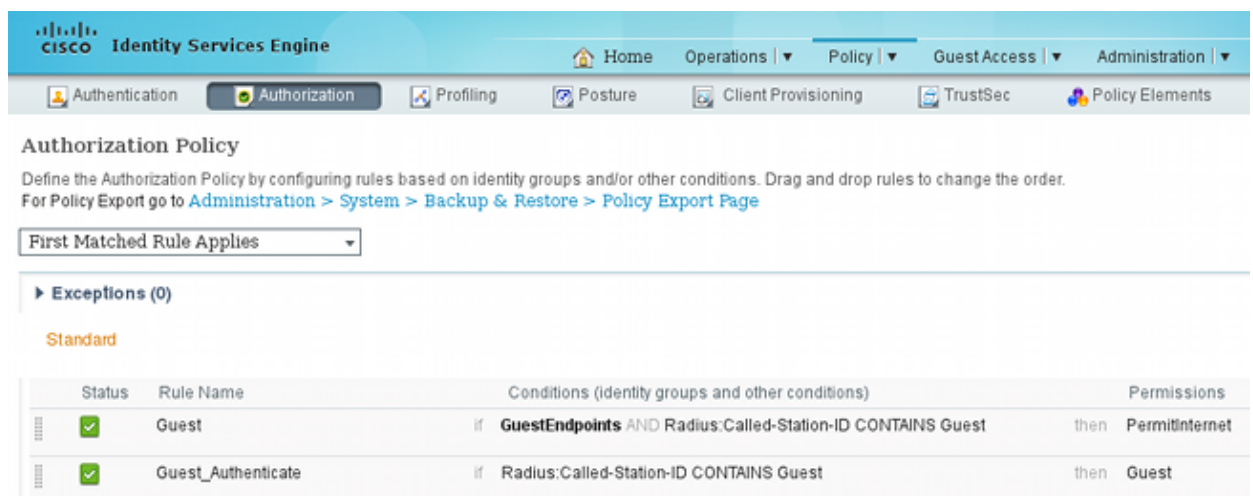
- ◆ Guest (with redirection to Guest portal name and ACL GuestRedirect)



- ◆ PermiInternet (with Airespace ACL equal Internet)



4. In order to verify the authorization rules, navigate to **Policy > Authorization**. In ISE Version 1.3 by default for failed MAC Authentication Bypass (MAB) access (MAC address not found) authentication is continued (not rejected). This is very useful for Guest Portals because there is no need to change anything in default authentication rules.



New users who associate to the Guest SSID are not yet part of any identity group. This is why they match the second rule, which uses the Guest authorization profile to redirect them to the correct Guest Portal.

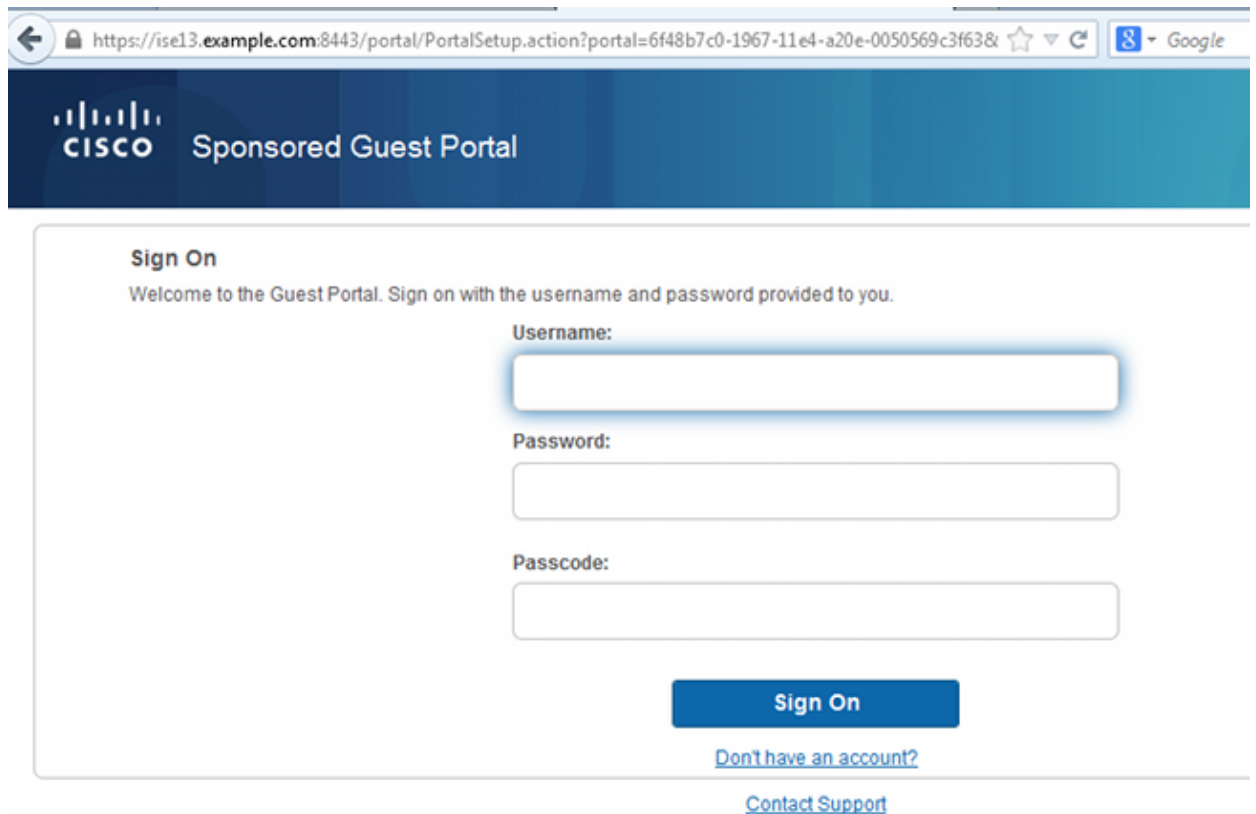
After a user creates an account and logs in successfully, ISE sends a RADIUS CoA and the WLC performs re-authentication. This time, the first rule is matched along with authorization profile PermitInternet and returns the ACL name that is applied on the WLC.

5. Add the WLC as a Network Access Device from **Administration > Network Resources > Network Devices**.

Verify

Use this section in order to confirm that your configuration works properly.

1. After you associate with the Guest SSID and type a URL, then you are redirected to the login page:



The screenshot shows a web browser window with the URL <https://ise13.example.com:8443/portal/PortalSetup.action?portal=6f48b7c0-1967-11e4-a20e-0050569c3f63&>. The page header features the Cisco logo and the text "Sponsored Guest Portal". The main content area is titled "Sign On" and includes the following text: "Welcome to the Guest Portal. Sign on with the username and password provided to you." Below this text are three input fields: "Username:", "Password:", and "Passcode:". A blue "Sign On" button is positioned below the input fields. At the bottom of the form, there are two links: "[Don't have an account?](#)" and "[Contact Support](#)".

2. Since you do not have any credentials yet, you must choose the *Don't have an account?* option. A new page that allows account creation displays. If the Registration Code option was enabled under the Guest Portal configuration, that secret value is required (this ensures that only people with correct permissions are allowed to self-register).

The image shows a web browser window with the URL `https://ise13.example.com:8443/portal/SelfRegistration.action?from=LOGIN`. The page header features the Cisco logo and the text "Sponsored Guest Portal". The main content area is titled "Create Account" and includes the instruction: "Please provide us with some information so we can create an account for you." The form contains the following fields:

- Registration Code***: cisco
- Username**: guest1
- First name**: michal
- Last name**: garcarz
- Email address**: mgarcarz@cisco.com
- Phone number**: 666666666

3. If there are any problems with the password or the user policy, navigate to **Guest Access > Settings > Guest Password Policy** or **Guest Access > Settings > Guest Username Policy** in order to change settings. Here is an example:

CISCO Identity Services Engine Home

Configure Manage Accounts **Settings**

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

▶ **Guest Locations and SSIDs** Specify the locations where you want to allow 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 length:**

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

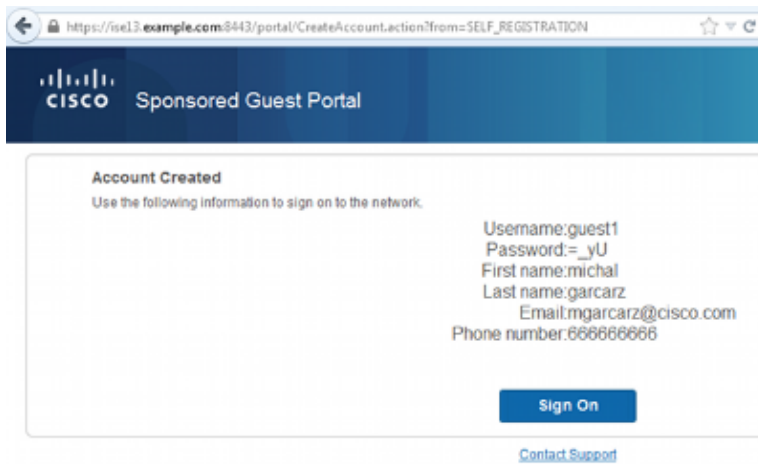
Characters Allowed in Randomly-Generated Usernames

Alphabetic: (0-64)
Minimum alphabetic: (0-64)

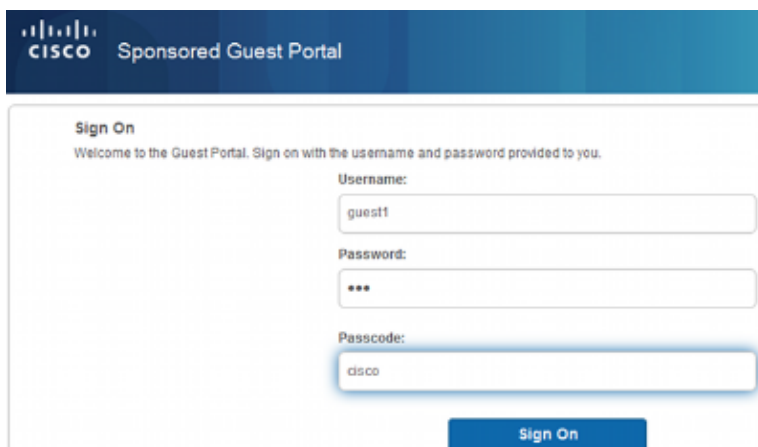
Numeric: (0-64)
Minimum numeric: (0-64)

Special: (0-64)
Minimum special: (0-64)

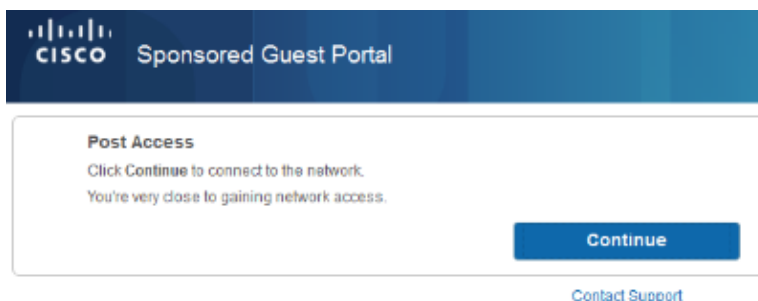
4. After successful account creation, you are presented with credentials (password generated as per guest password policies):



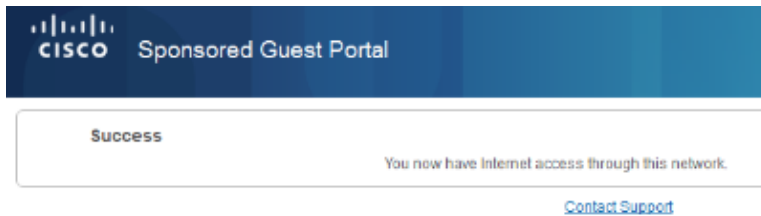
5. Click **Sign On** and provide credentials (additional Access Passcode might be required if configured under the Guest Portal; this is another security mechanism that allows only those who know the password to log in).



6. When successful, an optional Acceptable Use Policy (AUP) might be presented (if configured under the Guest Portal). The Post Access page (also configurable under Guest Portal) might also display.



The last page confirms that access has been granted:



Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

At this stage, ISE presents these logs:

Time	Status	Det...	Repeat Count	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2014-08-01 13:19:52...	!			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

Here is the flow:

- The guest user encounters the second authorization rule (Guest_Authenticate) and is redirected to Guest ("Authentication succeeded").
- The guest is redirected for self-registration. After successfully login (with the newly-created account), ISE sends the CoA Reauthenticate, which is confirmed by the WLC ("Dynamic Authorization succeeded").
- The WLC performs re-authentication with the Authorize-Only attribute and the ACL name is returned ("Authorize-Only succeeded"). The guest is provided the correct network access.

Reports (*Operations > Reports > ISE Reports > Guest Access Reports > Master Guest Report*) also confirms that:

Logged At	Guest User Name	MAC Address	IP Address	Operation	User Name	Message	AUP Acceptance
2014-08-01 13:18:49.9	guest1	64-66-B3-08-23-A3	10.221.0.218				Guest user has accepted the use policy
2014-08-01 13:18:08.7	guest1	64-66-B3-08-23-A3	10.221.0.218	Add	SelfRegistration		

A sponsor user (with correct privileges) is able to verify the current status of a guest user.

This example confirms that the account is created, but the user has never logged in ("Awaiting Initial Login"):

https://sponsor.example.com:8443/sponsorportal/LoginSubmit.action?from=LOGIN#manageAccountSummary

Welcome sponsor

CISCO Sponsor Portal

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

Resend Extend Edit Suspend

Reinstate Delete Reset Password Print

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

Optional Configuration

For every stage of this flow, different options can be configured. All of this is configured per the Guest Portal at **Guest Access > Configure > Guest Portals > PortalName > Edit > Portal Behavior and flow settings**. More important settings include:

Self-Registration Settings

- Guest Type – Describes how long the account is active, password expiry options, logon hours and options (this is mixture of Time Profile and Guest Role from ISE Version 1.2)
- Registration code – If enabled, only users who know the secret code are allowed to self-register (must provide the password when account is created)
- AUP – Accept Use Policy during self-registration
- Requirement for sponsor to approve/activate guest account

Login Guest Settings

- Access code – If enabled, only guest users who know the secret code are allowed to log in
- AUP – Accept Use Policy during self-registration
- Password change option

Device Registration Settings

- By default, the device is registered automatically

Guest Device Compliance Settings

- Allows for a posture within the flow

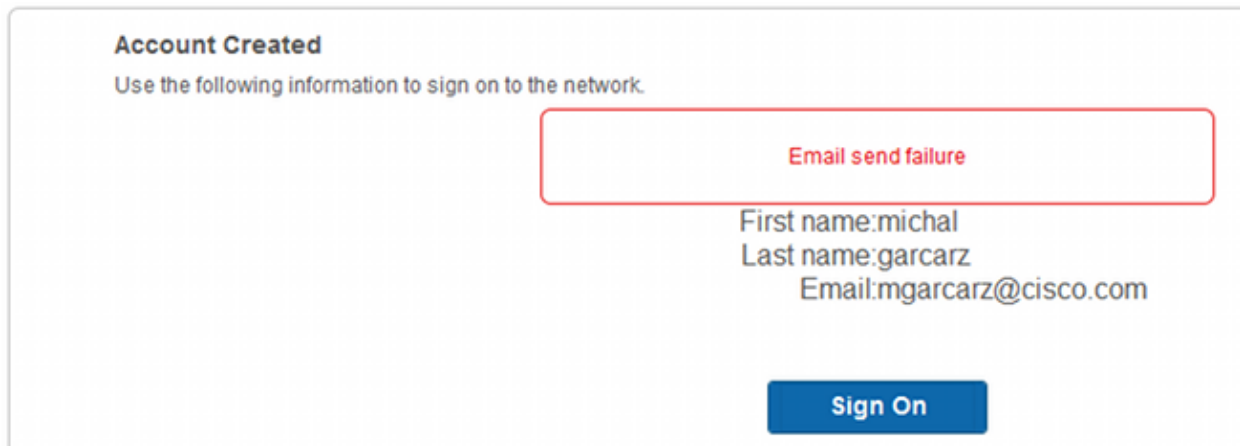
BYOD Settings

- Allows corporate users who use the portal as guests to register their personal devices

Sponsor-Approved Accounts

If the *Require self-registered guests to be approved* option is selected, then the account created by the guest must be approved by a sponsor. This feature might use email in order to deliver notification to the sponsor (for guest account approval):

If the Simple Mail Transfer Protocol (SMTP) server or default from notification from email is not configured, then the account will not be created:



The log from guest.log confirms that the global from address used for notification is missing:

```
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.
```

When you have the proper email configuration, the account is created:

CISCO Identity Services Engine Home Operations

Configure Manage Accounts **Settings**

- ▶ **Guest Account Purge Policy** Specify when to delete expired guest accounts :
- ▶ **Custom Fields** Add custom fields that can be used for creating
- ▼ **Guest Email Settings** Identify the SMTP server and specify the email

SMTP server:

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

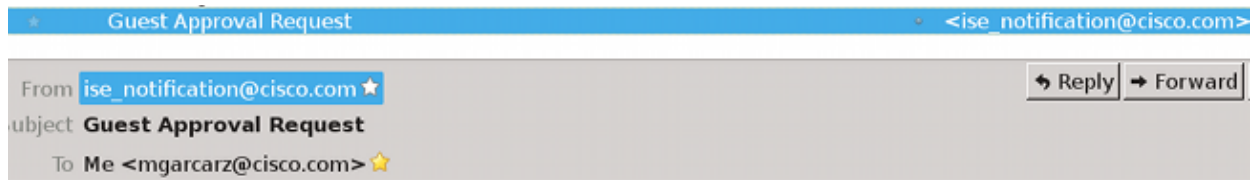
Account Created
Use the following information to sign on to the network.

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

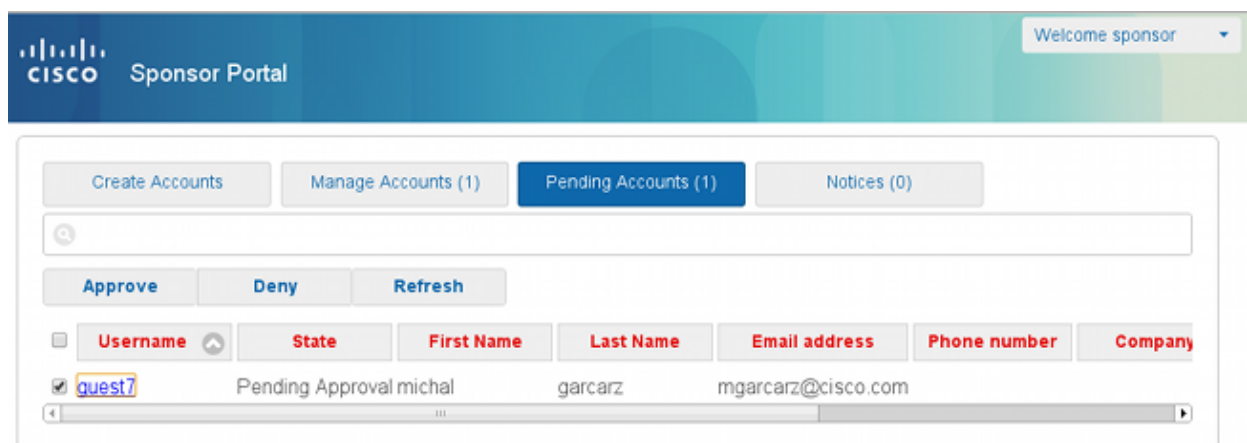
Sign On

After you enable the *Require self-registered guests to be approved* option, the username and password fields are automatically removed from the *Include this information on the Self-Registration Success page* section. This is why, when sponsor approval is needed, credentials for guest users are not displayed by default on the web page that presents information to show that the account has been created. Instead they must be delivered by Short Message Services (SMS) or email. This option must be enabled in the *Send credential notification upon approval using* section (mark email/SMS).

A notification email is delivered to the sponsor:



The sponsor logs into the Sponsor portal and approves the account:



From this point on, the guest user is allowed to log in (with the credentials received by email or SMS).

In summary, there are three email addresses used in this flow:

- Notification "From" address. This is defined statically or taken from the sponsor account and used as the From address for both: notification to sponsor (for approval) and credential details to the guest. This is configured under *Guest Access > Configure > Settings > Guest Email Settings*.
- Notification "To" address. This is used in order to notify the sponsor that it has received an account for approval. This is configured in the Guest Portal under *Guest Access > Configure > Guest Portals > Portal Name > Require self-registered guests to be approved > Email approval request to*.
- Guest "To" address. This is provided by the guest user during registration. If *Send credential notification upon approval using Email* is selected, the email with credential details (username and password) is delivered to the guest.

Deliver Credentials via SMS

Guest credentials can be also delivered by SMS. These options should be configured:

1. Choose the SMS service provider:

SMS Service Provider

Guests can choose from these SMS providers:

- Global Default
- T-Mobile
- ATT
- Verizon
- ClickatelIViaSMTP

2. Check the *Send credential notification upon approval using: SMS* check box.
3. Then, the guest user is asked to choose the available provider when he creates an 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. An SMS is delivered with the chosen provider and phone number:

Account Created
Use the following information to sign on to the network.

First name:michal
 Last name:garcarz
 Email:mgarcarz@cisco.com
 Phone number:6666666666
 SMS Provider:Global Default

[Sign On](#)

5. You can configure SMS Providers under *Administration > System > Settings > SMS Gateway*.

Device Registration

If the *Allow guests to register devices* option is selected after a guest user logs in and accepts the AUP, you can register devices:

The screenshot shows the 'Device Registration' page in the Cisco Sponsored Guest Portal. At the top, there is a header with the Cisco logo and 'Sponsored Guest Portal'. Below the header, the page title is 'Device Registration'. A message states: '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'. There are two input fields: 'Device ID' and 'Device Description'. Below these fields are three buttons: 'Add' (disabled), 'Save, continue' (active), and 'Cancel, continue' (active). At the bottom, there is a 'Manage Devices (1)' section with a table containing one device with the MAC address '64:66:B3:08:23:A3' and a 'Delete' button.

Notice that the device has already been added automatically (it is on Manage Devices list). This is because *Automatically register guest devices* was selected.

Posture

If the *Require guest device compliance* option is selected, then guest users are provisioned with an Agent that performs the posture (NAC/Web Agent) after they log in and accept the AUP (and optionally perform device registration). ISE processes Client Provisioning rules to decide which Agent should be provisioned. Then the Agent that runs on the station performs the posture (as per Posture rules) and sends results to the ISE, which sends the CoA reauthenticate to change authorization status if needed.

Possible authorization rules might look similar to this:

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

The first new users who encounter Guest_Authenticate rule redirect to the Self Register Guest portal. After the user self-registers and logs in, CoA changes authorization status and the user is provided with limited access to perform posture and remediation. Only after the NAC Agent is provisioned and the station is compliant does CoA change authorization status once again in order to provide access to the Internet.

Typical problems with posture include lack of correct Client Provisioning rules:

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](#)

This can also be confirmed if you examine guest.log file (new in ISE Version 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

If the *Allow employees to use personal devices on the network* option is selected, then corporate users who use this portal can go through BYOD flow and register personal devices. For guest users, that setting does not change anything.

What does "employees using portal as guest" mean?

By default, guest portals are configured with the *Guest_Portal_Sequence* identity store:

▼ 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](#)

This is the internal store sequence that tries the Internal Users first (before Guest Users):

The screenshot shows the Cisco ISE configuration interface for the 'Guest_Portal_Sequence' Identity Source Sequence. The 'Name' field is 'Guest_Portal_Sequence' and the 'Description' is 'A built-in Identity Sequence for the Guest Portal'. Under 'Certificate Based Authentication', the 'Select Certificate Authentication Profile' checkbox is unchecked. Under 'Authentication Search List', the 'Available' list contains 'Internal Endpoints' and 'AD1', while the 'Selected' list contains 'Internal Users', 'Guest Users', and 'All_AD_Instances'. Navigation arrows are visible between the lists.

When at this stage on the guest portal, the user provides credentials that are defined in the Internal Users store and the BYOD redirection occurs:

The screenshot shows the 'Cisco Sponsored Guest Portal' user interface. At the top, there is a navigation bar with steps 1, 2, 3, and 4, where step 1 is highlighted. Below the navigation bar, the text reads 'BYOD Welcome' and 'Welcome to the BYOD portal.' A message states: '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.' There are two buttons: a blue 'Start' button and a grey 'I want guest access only' button.

This way corporate users can perform BYOD for personal devices.

When instead of Internal Users credentials, Guest Users credentials are provided, normal flow is continued (no BYOD).

VLAN Change

This is a similar option to the VLAN change configured for the Guest Portal in ISE Version 1.2. It allows you to run activeX or a Java applet, which triggers DHCP to release and renew. This is needed when CoA triggers the change of VLAN for the endpoint. When MAB is used, the endpoint is not aware of a change of VLAN. A possible solution is to change VLAN (DHCP release/renew) with the NAC Agent. Another option is to request a new IP address via the applet returned on the web page. A delay between release/CoA/renew can be configured. This option is not supported for mobile devices.

Related Information

- *Posture services on Cisco ISE Configuration Guide*
- *Wireless BYOD with Identity Services Engine*
- *ISE SCEP support for BYOD Configuration Example*
- *Cisco ISE 1.3 Administrators Guide*
- *Central Web Authentication on the WLC and ISE Configuration Example*
- *Central Web Authentication with FlexConnect APs on a WLC with ISE Configuration Example*
- *Technical Support & Documentation – Cisco Systems*