

ISE Guest portal with optional AD login for BYOD

This document details how to modify a standard hotspot guest wireless portal (hosted via ISE) to include and allow differentiated access for internal employees and vendors (BYOD scenario) as follows:

Guests – access for one day

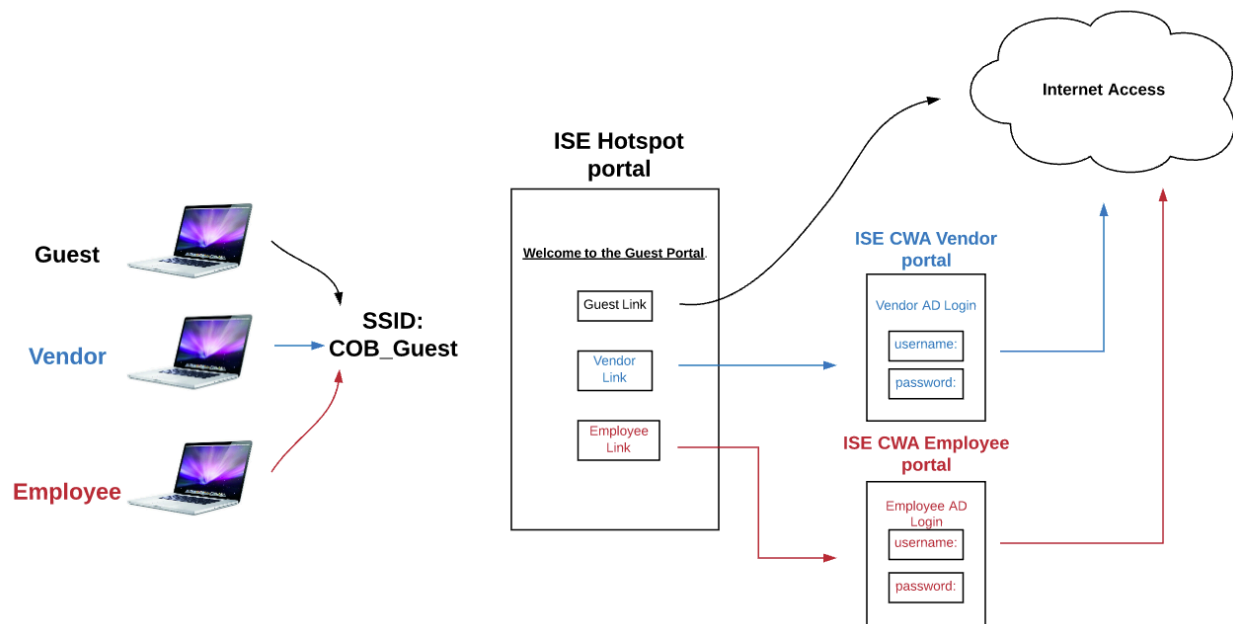
Vendors – access for 1 week

Employees – access for 1 month

The initial guest hotspot page should include an AUP and “accept” link that allows guest direct access to the internet. The page also has links for Vendors and Employees that take them to separate CWA portals where they can login with AD credentials, with the benefit of extended access as described above.

Devices are registered in individual Endpoint Identity Groups (IG) with associated purge policies.

There are 3 portals created for this configuration. The overall flow is illustrated below.



The initial Guest portal is a hotspot portal. Custom code is added to the “Optional Content 1” box located under the Guest Portals/your Guest portal/Portal Page Customization configuration section. This code captures the device session ID to maintain the vendor and employee sessions through the additional portal links, see in the image below as Employee Portal and Vendor Portal.



Employee portal Vendor portal

Acceptable Use Policy

Please read the Acceptable Use Policy.

COB Guests, please accept the policy for one-day access.

Accept

Decline

COB Employees and Vendors, use the links below for extended access.

Employee Portal

Vendor Portal

The Employee and Vendor CWA portals are not tied to Authorization policies and resulting conditions. They are needed as portals for the vendor and employee AD groups to login through, however. The portal login process authenticates them and adds their device MAC to the corresponding IG.

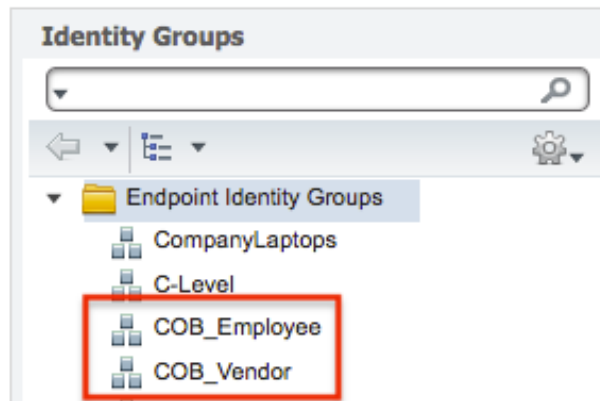
Groups, Containers and Settings

First, create/determine the AD groups you'll reference for Employees and Vendors. Add them to ISE as you would any AD group.

[External Identity Sources](#) [Identity Source Sequences](#) [Settings](#)

Sources		Connection	Whitelisted Domains	PassiveID	Groups
Authentication Profile		Edit Add Delete Group Update SID Values			
<input type="checkbox"/>	Name				SID
<input type="checkbox"/>	cnetpdx.lab/CNETPDX_Groups/C-Level				S-1-5-21-56268
<input type="checkbox"/>	cnetpdx.lab/CNETPDX_Groups/COB_Employees				S-1-5-21-56268
<input type="checkbox"/>	cnetpdx.lab/CNETPDX_Groups/COB_Vendors				S-1-5-21-56268

Next, create two new IGs in ISE for Vendors and Employees. We'll assign these IGs to each portal respectively.



Create an Identity Source Sequence to lookup AD logins against. We'll select this for the two CWA portals.

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

Available		Selected
Internal Endpoints	>	cnetpdx.lab
Internal Users	<	
Guest Users		
LDAP_cnetpdx_lab		
All_AD_Join_Points		

Create Vendor and Employee guest types and select the IGs under Login Options you created above for each, and any other options you need. Below is an example from the Employee guest type.

Guest Portals

Guest Types

Sponsor Groups

Sponsor Portals

Guest Types

You can edit and customize the default guest types.

Create

Edit

Duplicate

Delete

AD Domain Users
AD user group - 30 days before re-authentication

C Level Users
members of C-Level AD group and n

COB_Employee

Login Options

☒ Maximum simultaneous logins (1-999)

When guest exceeds limit:

☒ Disconnect the oldest connection

☐ Disconnect the newest connection

☐ Redirect user to a portal page showing an error message ⓘ

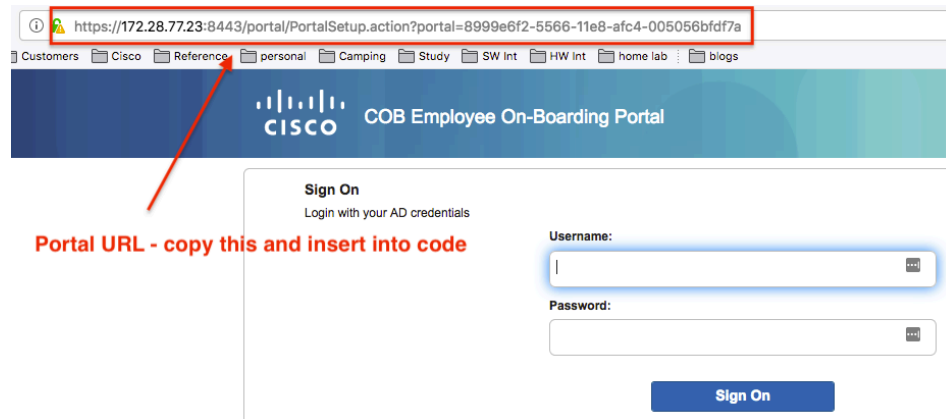
This requires the creation of an authorization policy rule

Maximum devices guests can register: (1-999)

Endpoint identity group for guest device registration: ⓘ

Portals

Create two CWA portals, one each for Employees and Vendors then use the test URL feature to grab the URLs. Below is the Employee portal, for example.



Copy the URL from each portal (vendor and employee) as indicated in the image above and paste into the code like so:

Employee portal

```
<script>
jQuery(window).ready(function() {
var hostname = window.location.hostname;
var WebSessionId =
window.location.href.substr(window.location.href.search("\\?")).split("=")[2];
jQuery('.cisco-ise-body').append(' <center><a
href="https://172.28.77.23:8443/portal/PortalSetup.action?portal=8999e6f2-5566-11e8-afc4-005056bdf7a&sessionId='+WebSessionId+'&action=cwa" style="color: rgb(0,255,0)"><font
color="212121"><button type="submit">Employee Portal</button></font></a></center>');
});
</script>
```

Vendor portal

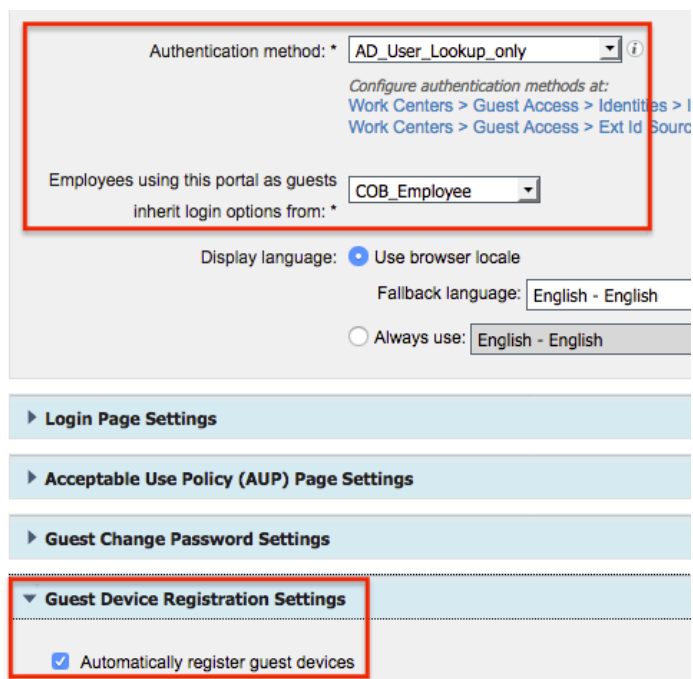
```
<script>
jQuery(window).ready(function() {
var hostname = window.location.hostname;
var WebSessionId =
window.location.href.substr(window.location.href.search("\\?")).split("=")[2];
```

```
jQuery('.cisco-ise-body').append(' <center><a
href="https://172.28.77.23:8443/portal/PortalSetup.action?portal=180f2352-53c8-11e8-afc4-
005056bdfd7a&sessionId='+WebSessionId+'&action=cwa" style="color: rgb(0,255,0)"><font
color="212121"><button type="submit">Vendor Portal</button></font></a></center>');
});
</script>
```

Do not include the underlined Employee Portal and Vendor Portal text as seen above. That is only to describe what you see in the code examples.

Keep this in a text file for use on the guest portal later. Each of these code samples above will create the link buttons on the guest hotspot portal, which we'll do shortly.

Within each of the vendor and employee portals, select the ISS we created for AD lookup, the matching guest type and automatic device registration.



Authentication method: * AD_User_Lookup_only ⓘ

Configure authentication methods at:
[Work Centers > Guest Access > Identities > I](#)
[Work Centers > Guest Access > Ext Id Sourc](#)

Employees using this portal as guests COB_Employee
 inherit login options from: *

Display language: ☒ Use browser locale

Fallback language: English - English

☐ Always use: English - English

▶ Login Page Settings

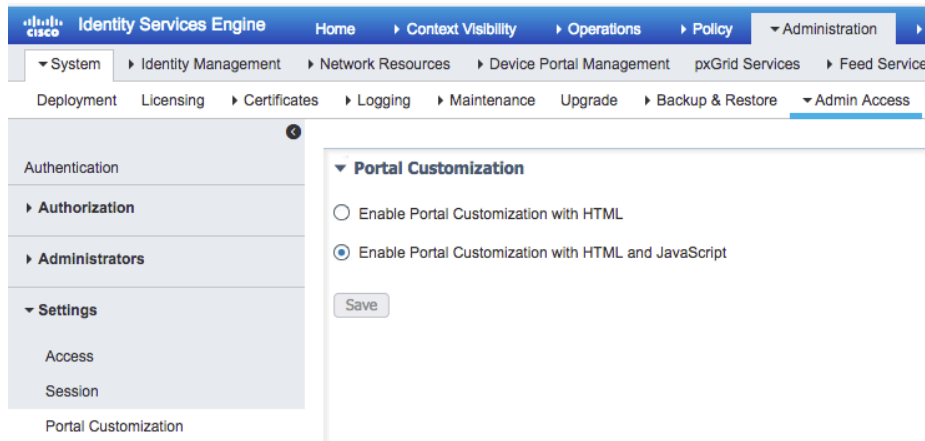
▶ Acceptable Use Policy (AUP) Page Settings

▶ Guest Change Password Settings

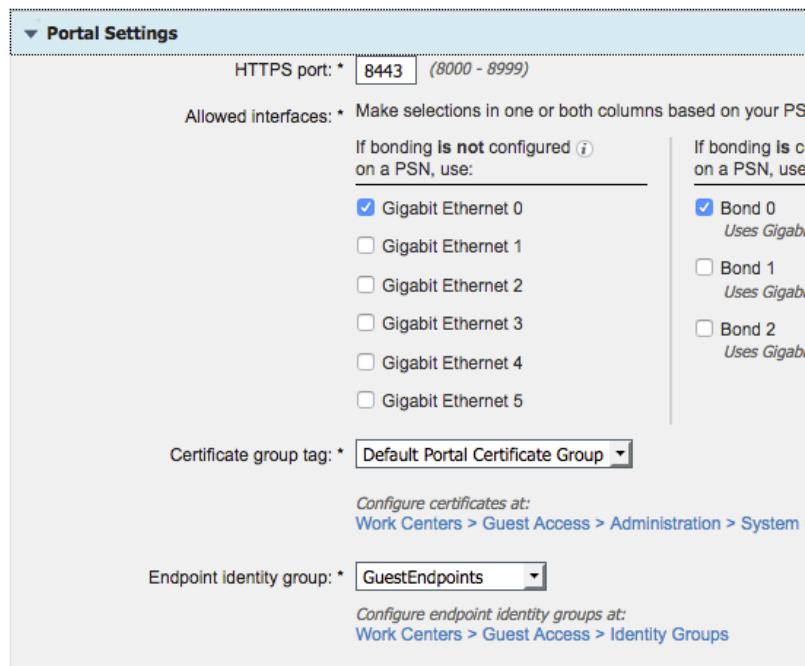
▼ Guest Device Registration Settings

☒ Automatically register guest devices

Enable portal customization under Administration/System/Admin Access/Portal Customization/Enable Portal Customization with HTML and JavaScript



Now we can build a hotspot portal for Guests. Here we're using the built-in GuestEndpoints IG.



To create the link buttons on the guest portal, go to the Portal Page Customization view of your guest portal. Tick the “toggle HTML source” button, paste in the code from your text file, then tick the button again to apply it.

Page Customizations







Browser Page Title




Acceptable Use Policy

Optional Content 1

Font

Size

```
<script>
jQuery(window).ready(function() {
var hostname = window.location.hostname;
var WebSessionId =
window.location.href.substr(window.location.href.search("\?").split("=")[2];
jQuery('.cisco-ise-body').append(' <center><a href="https://172.28.77.23:8443/portal
/PortalSetup.action?portal=8999e6f2-5566-11e8-afc4-005056bdf7a&
sessionId='+WebSessionId+'&action=cwa" style="color: rgb(0,255,0)"><font
color="212121"><button type="submit">Employee Portal</button></font>
</a></center>');
});
</script><script>
jQuery(window).ready(function() {
```

(text or HTML) Click Preview to test HTML rendering.

Content Title






Acceptable Use Policy

Instructional Text











Save and then use the portal test URL at the top to view and test the buttons you just created. If it works it will look like the example image on page 2 of this document and each button will take you to the right portal.

Authorization and Authentication Policies

Below is an example of the authentication and authorization policies used.

	COB_Guest_and_BYOD	AND	 Portland Office
			 Wireless_Access
			 Wireless_MAB
			 Radius·Called-Station-ID ENDS_WITH COB_Gues

Three Authorization policies are required.

Status	Rule Name	Conditions		Profiles
	COB_Guest_Permit		IdentityGroup·Name EQUALS Endpoint Identity Groups:GuestEndpoints	
	COB_BYOD_Permit	AND	<div> Wireless_MAB</div> <div>OR</div> <div> IdentityGroup·Name EQUALS Endpoint Identity Groups:COB_Employee</div> <div> IdentityGroup·Name EQUALS Endpoint Identity Groups:COB_Vendor</div>	
	COB_Guest_BYOD_onboarding		Wireless_MAB	