

# Single Credentialed Portal with Hotspot Button

Device/user flow

Embedded hotspot button on Credentialed portal

1. Device redirected to Sponsored Guest Portal
2. User clicks hotspot to auto-login with embedded creds
  - Can also login with a different type of account (sponsored)
3. Device is registered and COA reauth authorizes by endpoint group
4. Device gets access for 24hrs (configured under guest type for Xdays) before purged
  - Alternate flow can be used to differentiate access using no device reg

# Single Credentialed Portal with Hotspot Button Configuration

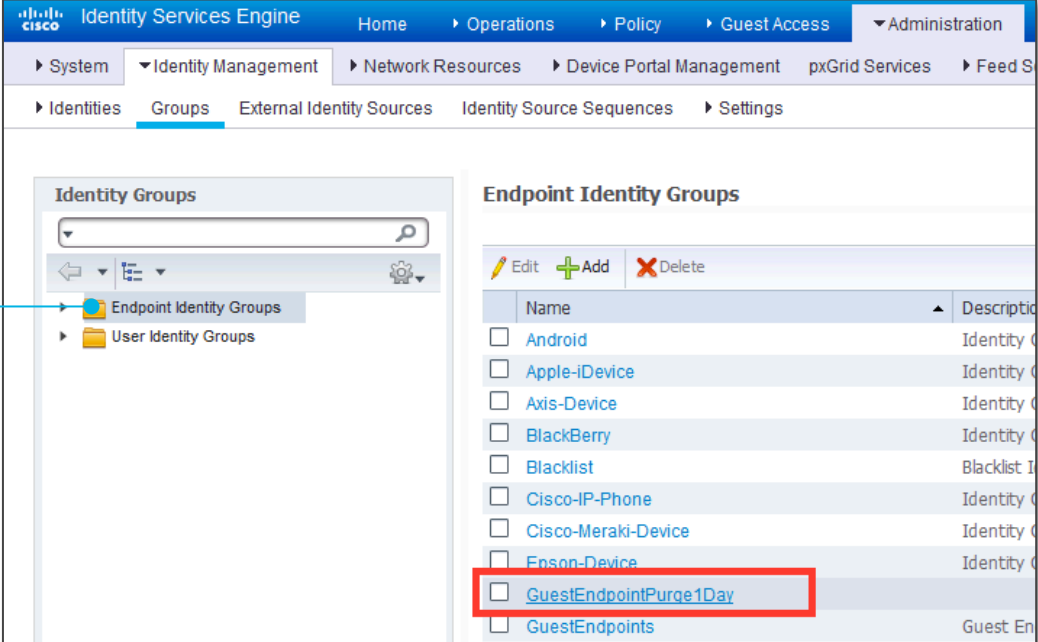
1. Create a special endpoint group (unique group)
  2. Create GuestType for HotSpotCreds
  3. Create a static internal account using HotSpotCreds group
  4. Create new Sponsored Guest portal
  5. Inject Javascript to Embed Creds into portal login page
  6. Create Authz profiles and rules
- Watch! – guest account can only register up to 999 endpoints
  - Added bonus! 1 SSID to handle different access type, requires more authz profiles and rules

# Single Credentialed Portal with Hotspot Button

Create separate Endpoint Group

## Add New Group

Administration > Identity Management > Groups



The screenshot displays the Cisco Identity Services Engine Administration interface. The navigation path is Administration > Identity Management > Groups. The main content area shows a list of Endpoint Identity Groups. The group 'GuestEndpointPurge1Day' is highlighted with a red box.

Name	Description
<input type="checkbox"/> Android	Identity G
<input type="checkbox"/> Apple-iDevice	Identity G
<input type="checkbox"/> Axis-Device	Identity G
<input type="checkbox"/> BlackBerry	Identity G
<input type="checkbox"/> Blacklist	Blacklist I
<input type="checkbox"/> Cisco-IP-Phone	Identity G
<input type="checkbox"/> Cisco-Meraki-Device	Identity G
<input type="checkbox"/> Epsom-Device	Identity G
<input type="checkbox"/> GuestEndpointPurge1Day	
<input type="checkbox"/> GuestEndpoints	Guest En

# Single Credentialed Portal with Hotspot Button

Create separate Guest Type

## Guest Type Changes

Guest Access > Configure > Guest Types

- Uncheck Max Logins
- Set Max devices to 999
- Pick correct endpoint group
- Default Purge is 1 day

**Guest Type**

Guest type name: \*

Description:

**Login Options**

Maximum simultaneous logins  (1-999)

Maximum devices guests can register:  (1-999)

Endpoint identity group for guest device registration:  ⓘ

*Configure endpoint identity groups at: [Administration > Identity > Management > Groups > En](#)*

Purge endpoints in this identity group:  days old ⓘ

The screenshot shows a configuration page for a 'Guest Type'. The name is 'HotSpotEmbedCreds' and the description is 'Special Guest Type for embedded hotspot creds'. Under 'Login Options', the 'Maximum simultaneous logins' checkbox is unchecked and the value is 3. The 'Maximum devices guests can register' is set to 999. The 'Endpoint identity group for guest device registration' is set to 'GuestEndpointPurge1Day'. The 'Purge endpoints in this identity group' is set to 1 day. Red arrows point to the 'Maximum simultaneous logins' checkbox, the 'Maximum devices guests can register' input, the 'Endpoint identity group' dropdown, and the 'Purge endpoints' input.

# Single Credentialed Portal with Hotspot Button

Create internal Guest account

## Add Internal Account

Admin > Identity Mgmt >  
Identities > Users  
Use new GuestType

The screenshot displays the Cisco Identity Services Engine (ISE) administration interface. The breadcrumb navigation path is: Home > Operations > Policy > Guest Access > Administration > Identity Management > Network Resources > Device Portal Management > Network Access Users List > New Network Access User. The main form is titled 'New Network Access User' and contains the following fields:

- Name:** hotspotembed
- Status:** Enabled (checked)
- User Groups:** A dropdown menu is open, showing 'GuestType\_HotSpotEmbedCre...' as the selected option. A red arrow points to this dropdown.

At the bottom of the form, there are 'Submit' and 'Cancel' buttons.

# Single Credentialed Portal with Hotspot Button

Inject into new Sponsored Guest Portal

Select Portal > Page customization > Login Page > Optional Content 2

```
<script>
  //adding hotspot btn to form-buttons block
  jQuery('.cisco-ise-form-buttons:first').append("<div class='ui-submit ui-btn ui-shadow'><input type='submit'
value='Hotspot' class='hotspot-btn'/></div>");
  //handling hotspot button click event
  jQuery('.hotspot-btn').on('click', function(evt){
    evt.preventDefault();
    //adding predefined values to login form inputs
    jQuery("input[name='user.username']").val("guest");
    jQuery("input[name='user.password']").val("ISEisC00L");
    //clicking on submit button
    jQuery("#ui_login_signon_button").trigger('click');
  });
</script>
```

Add this line if you want to prevent browser from storing the credentials:

```
jQuery("input[name='user.password']").attr('type', 'text');
```

# Single Credentialed Portal with Hotspot Button

Inject into new Sponsored Guest Portal

Use this code if needing multiple accounts to scale above 999

```
<script>
  //adding hotspot btn to form-buttons block
  jQuery('.cisco-ise-form-buttons:first').append("<div class='ui-submit ui-btn ui-shadow'><input type='submit'
value='Hotspot' class='hotspot-btn'/></div>");
  //handling hotspot button click event
  jQuery('.hotspot-btn').on('click', function(evt){
    evt.preventDefault();
    //adding predefined values to login form inputs
    var accounts=["guest1","guest2","guest3"];
    Var username=accounts[parseInt(Math.random*3)];
    jQuery("input[name='user.username']").val(username);
    jQuery("input[name='user.password']").val("PASSWORD_GOES_HERE");
    jQuery("#ui_login_signon_button").trigger('click');
    //clicking on submit button
    jQuery("#ui_login_signon_button").trigger('click');
  });
</script>
```

# Single Credentialed Portal with Hotspot Button

portal login options

## Use other credentials

Allow guest to enter sponsored credentials for longer or better access (TOS depending on Guest Type and Authz Rules)

## Embedded Credentials

Button auto-submit and sign-on

The screenshot displays a mobile interface for a Cisco Guest Portal. At the top, there are tabs for 'Preview' and 'Settings'. Below this is a header with the Cisco logo and the text 'Sponsored Guest ...'. The main content area is titled 'Sign On' and includes a welcome message: 'Welcome to the Guest Portal. Sign on with the username and password provided to you.' There are two input fields: 'Username:' with the value 'guest' and 'Password:' with a masked password of ten dots. Below the password field is a blue 'Sign On' button and a grey 'Hotspot' button. At the bottom of the screen, there is a 'Refresh Preview' button. Two blue lines with circular endpoints point from the text on the left to the 'Sign On' button and the 'Hotspot' button.



# Single Credentialed Portal with Hotspot Button

authorization rules showing differentiated access

## Guest\_type TOS

Use different accounts to grant with different Type of Service based on web-auth flow (no remember me)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	UnknownDeviceGuestRedirect	if Wireless_MAB	then GuestRedirect
<input checked="" type="checkbox"/>	PermitGuest_Gold	if GuestType_Weekly (default) AND Wireless_MAB	then GuestPermit_GOLD
<input checked="" type="checkbox"/>	PermitGuest_Silver	if GuestType_Daily (default) AND Wireless_MAB	then GuestPermit_SILVER

## Endpoint TOS

Use different endpoint groups to grant with different Type of Service based on web-auth + registration flow (remember me)

<input checked="" type="checkbox"/>	PermitGuest_Gold	if Guest_Gold AND Wireless_MAB	then GuestPermit_GOLD
<input checked="" type="checkbox"/>	PermitGuest_Silver	if Guest_Silver AND Wireless_MAB	then GuestPermit_SILVER