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

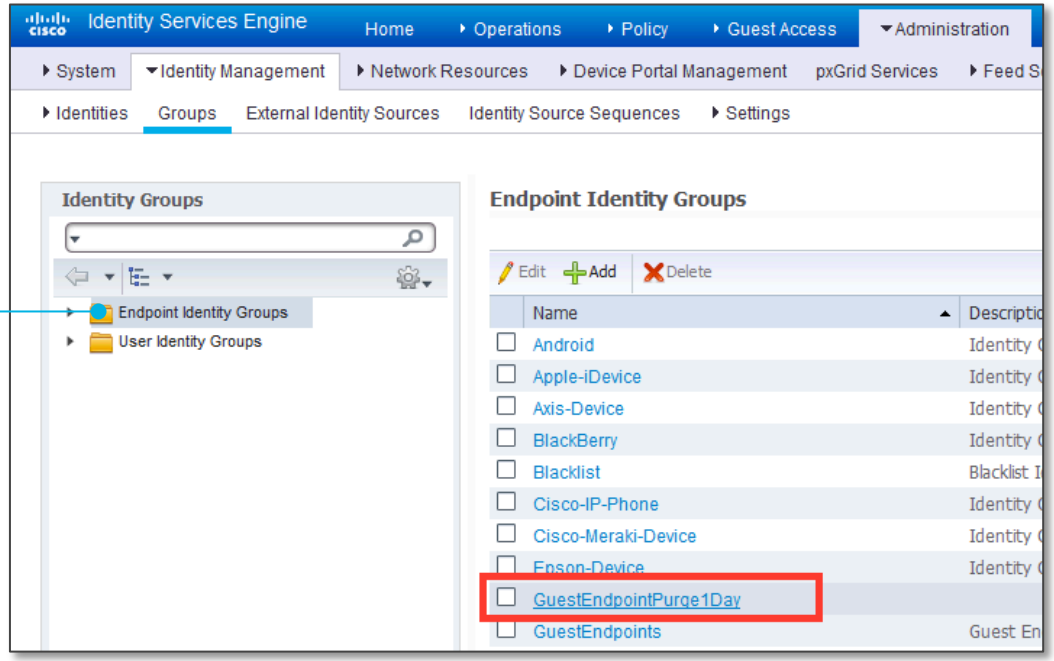
- Watch! – guest account can only register up to 999 endpoints
- Added bonus! 1 SSID to handle different access type, requires more authz profiles and rules

Single Credentialed Portal with Hotspot Button

Create separate Endpoint Group

Add New Group

Administration > Identity Management > Groups



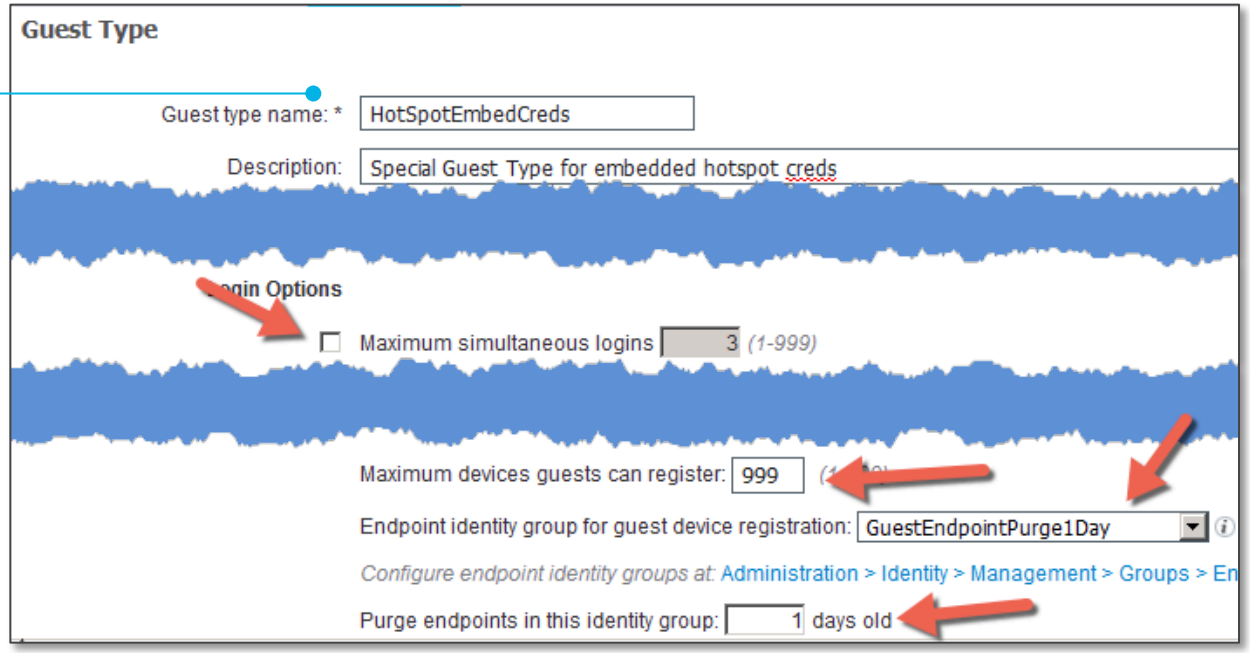
Single Credentialed Portal with Hotspot Button

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

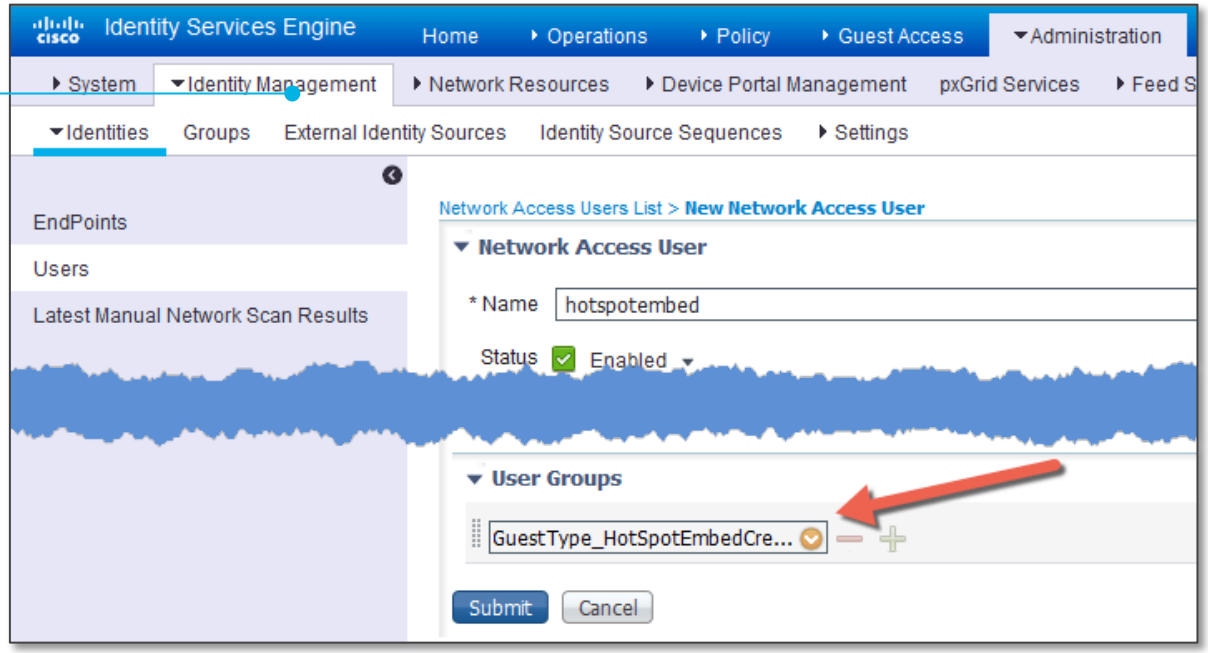


Single Credentialed Portal with Hotspot Button

Create internal Guest account

Add Internal Account

Admin > Identity Mgmt > Identities > Users
Use new GuestType



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

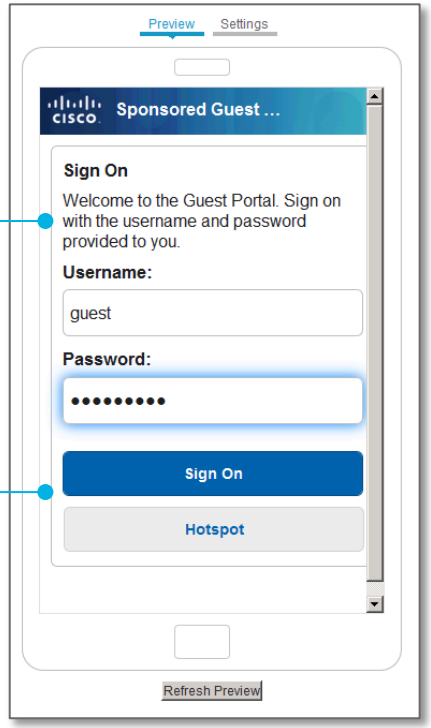
portal login options

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

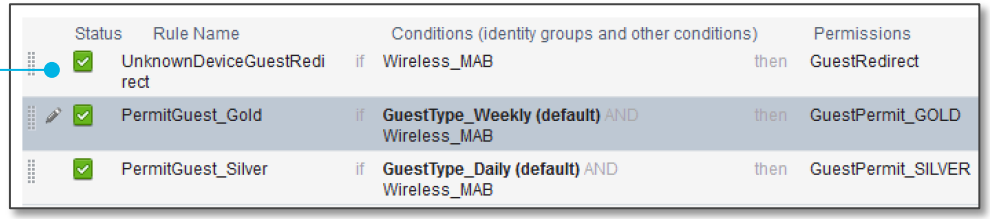


Single Credentialed Portal with Hotspot Button

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
✓	UnknownDeviceGuestRedirect	if Wireless_MAB	then GuestRedirect
✓	PermitGuest_Gold	if **GuestType_Weekly (default)** AND Wireless_MAB	then GuestPermit_GOLD
✓	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)

✓	PermitGuest_Gold	if **Guest_Gold** AND Wireless_MAB	then GuestPermit_GOLD
✓	PermitGuest_Silver	if **Guest_Silver** AND Wireless_MAB	then GuestPermit_SILVER