

Overview

Note: This has only been tested on ISE 2.1. This may or may not work with older or newer versions.

This custom Guest portal configuration has 3 Use cases.

- 1) Pure Guest Access with Email Required for Registration
- 2) Employee Guest Access with AD Credentials to Authenticate
- 3) Employee BYOD Access with Device Provisioning for EAP-TLS authentication

Welcome

When the Guest or Employee connects to the Guest SSID, they are re-directed to this Self Registered Guest Portal. Using the Script, we are hiding the regular content of this Login page and presenting a new Message title and 2 buttons.



Welcome

Welcome to the the Guest Wireless Portal. Please choose from the options below to gain access to the Guest Wireless.

[Guest Access](#)

[Employee Access](#)

Guest Access

If the user is a Pure Guest and clicks on Guest Access, they are then presented with the Self Registration page that only requires an email address to be supplied.



Register Device

To gain access to the Guest wireless network, you must supply a valid email address. Any information you provide will not be used for other commercial purposes and will not be sold, rented, leased or forwarded to any third party.

Email address*

[Register](#)

[Cancel](#)

After entering their email address and clicking Register, they are then taken to the Acceptable Use Policy Page where they must scroll down to click Accept.



Acceptable Use Policy

Please read the Acceptable Use Policy

terminated at any time for any reason including, but not limited to, violation of this Agreement, actions that may lead to liability for the Company, disruption of access to other users or networks, and violation of applicable laws or regulations. The Company reserves the right to monitor and collect information while you are connected to the Service and that the collected information can be used at discretion of the Company, including sharing the information with any law enforcement agencies, the Company partners and/or the Company vendors.

The Company may revise this Agreement at any time. You must accept this Agreement each time you use the Service and it is your responsibility to review it for any changes each time.

We reserve the right at all times to withdraw the Service, change the specifications or manner of use of the Service, to change access codes, usernames, passwords or other security information necessary to access the service.

IF YOU DO NOT AGREE WITH THESE TERMS, INCLUDING CHANGES THERETO, DO NOT ACCESS OR USE THE SERVICE.

Accept

Decline

Once they press Accept, behind the scene we are taking them to the Success Page where we have allowed them to Login Directly from the Success Page, but are hiding that page from them and automatically click the Login Button. Once that button has been programmatically pressed, they are then redirected to the URL of our choice based on the Portal Configuration. The endpoint is then put into the GuestEndpoints1DayPurge

Employee Access

If the user is an Employee, they click Employee Access. The button executes a function that then hides the content of the first screen and un-hides the original content of the Username, Password and Sign On Button with the original Welcome text configured in the Portal Settings.



Employee Access

Please sign into the Guest Portal with your Domain Credentials.

Username:

Password:

Sign On

[Not an Employee?](#)

After the employee uses their AD Credentials and successfully authenticates, we present them with the BYOD Welcome page with the option to select Guest Access Only.

1

2

3

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](#)

If the employee selected to Start the BYOD process, they are taken through the normal BYOD provisioning process and their device is provisioned for 802.1X Authentication utilizing the internal ISE CA (this can use External if you like) and put into the EmployeeBYODEndpoints Identity Group for use in the Authorization Policy. Once their device is provisioned, they will be reconnected or will need to manually reconnect to the 802.1X network and granted whatever access is provided based on the authorization profile.

If the employee selects “I want guest access only”, then the device is automatically put into the EmployeeEndpoints Identity Group and the CoA happens and the device is reauthorized based on the results of the Authorization Policy and access is granted per the Authorization Profile configured.

ISE Configuration


Here are all the critical ISE configuration steps required to setup this guest portal. This document does not go into detail about the Client Provisioning for BYOD devices.


Endpoint Identity Groups


Administration -> Identity Management -> Groups

Create the 3 Endpoint Identity Groups shown below for each use Case

Endpoint Identity Groups

 Edit

 Add

 Delete

Name	Description
<div>Endpoints</div>	<div>endpoint group</div>
<input type="checkbox"/> EmployeeBYODEndpoints	Endpoint group for Employee BYOD Devices once successful device Provisioning ...
<input type="checkbox"/> EmployeeEndpoints	Endpoint group for Employee Devices only using Guest Internet Access
<input type="checkbox"/> GuestEndpointsPurge1Day	Endpoint Group for Self Registering Guest Automatic Account Creation

Endpoint Purge Policies

Administration -> Identity Management -> Settings -> Endpoint Purge

Create 3 Endpoint Purge Policies shown below

- 1) EmployeeBYODEndpoints never Purge if Device Registration Status is Registered
- 2) GuestEndpointsPurge1Day purge when Elapsed Days is greater than 1
- 3) EmployeeEndpoints purge when Elapsed Days is greater than 90

Endpoint Purge

Define the EndPoint Purge Policy by configuration rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▼ Never Purge			
Status	Rule Name	Conditions (identity groups and/or other conditions)	
	EnrolledRule	if DeviceRegistrationStatus Equals Registered	Edit ▼
	EmployeeBYODEndpoints	if EmployeeBYODEndpoints AND ENDPOINTPURGE DeviceRegistrationStatus EQUALS Registered	Edit ▼

▼ Purge			
Status	Rule Name	Conditions (identity groups and/or other conditions)	
	GuestEndpointsPurgeRule	if GuestEndpoints AND ElapsedDays Greater than 30	Edit ▼
	RegisteredEndpointsPurgeRule	if RegisteredDevices AND ElapsedDays Greater than 30	Edit ▼
	GuestEndpoints1DayPurgeRule	if GuestEndpointPurge1Day AND ENDPOINTPURGE ElapsedDays GREATER THAN 1	Edit ▼
	EmployeeEndpoints90DayPurge Rule	if EmployeeEndpoints AND ENDPOINTPURGE ElapsedDays GREATER THAN 90	Edit ▼

Guest Types

Work Centers -> Guest Access -> Configure -> Guest Types

Create the 2 Guest Types shown below with the given criteria. You can modify this to your environment.

- 1) Employee – Settings to allow Account to be active for 90 Days with 3 devices max registered and 3 simultaneous logins.
- 2) Guest – Settings to allow account to be active for only 1 day with 1 device max registered and 1 simultaneous login.

Guest Types

You can edit and customize the default guest types and create additional ones.

[Create](#) [Edit](#) [Duplicate](#) [Delete](#)

Employee
Guest type for Employees good for 90 days with Maximum logins of 3 and Maximum Registered Devices of 3.

Guest
Guest type for Guest good for 1 day with Maximum logins of 1 and Maximum Registered Devices of 1.

Guest Username Policy

Work Centers -> Guest Access -> Settings -> Guest Username Policy

Setup the Guest Username Policy to utilize the Email Address.

Username Criteria for Known Guests

If data is available, base username on:

- ☐ First name and last name
- ☒ Email address

Guest Portal

Work Centers -> Guest Access -> Configure -> Guest Portals

Create a new Self Registered Guest Portal (name it whatever) and apply the following settings

Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

CreateEditDuplicateDelete

GuestEmployeePortal

✔

Used in 1 rules in the Authorization policy

Portal Behavior and Flow Settings

- Portal Settings
 - Set “Employees using this portal as guests inherit login options from:” to **Employee**

▼ Portal Settings

HTTPS port: *

8443

(8000 - 8999)

Allowed

Make selections in one or both columns based on your PSN configurations.

interfaces: *

If bonding **is not** configured ⓘ
on a PSN, use:

☒ Gigabit Ethernet 0

☐ Gigabit Ethernet 1

☐ Gigabit Ethernet 2

☐ Gigabit Ethernet 3

☐ Gigabit Ethernet 4

☐ Gigabit Ethernet 5

If bonding **is** configured ⓘ
on a PSN, use:

☒ Bond 0
Uses Gigabit Ethernet 0 as primary

☐ Bond 1
Uses Gigabit Ethernet 2 as primary

☐ Bond 2
Uses Gigabit Ethernet 4 as primary

Certificate

Default Portal Certificate Group

group tag: *

Configure certificates at:
[Work Centers > Guest Access > Administration > System Certificates](#)

Authentication

Guest_Portal_Sequence ⓘ

method: *

Configure authentication methods at:
[Work Centers > Guest Access > Identities > Identity Source Sequences](#)
[Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers](#)

Employees

using this

portal as

guests inherit

login options

from: *

Employee

- Login Page Settings
 - Uncheck everything except “Allow guests to create their own accounts”

▼ Login Page Settings

☐ Require an access code:

Maximum failed login attempts before rate limiting: (1 - 999)

Time between login attempts when rate limiting: minutes (1 - 999)

☐ Include an AUP

☐ Require acceptance

☒ Allow guests to create their own accounts

☐ Allow guests to change password after login

☐ Allow the following identity-provider guest portal to be used for login ⓘ

There are no guest portals configured to use a SAML Id Provider as the Authenticator

- Self-Registration Page Settings
 - Set “Assign self-registered guests to guest type” to **Guest**
 - Set “Account valid for” to 1 Days and Uncheck all options except “Email Address” for Fields to include and Required

▼ Self-Registration Page Settings

Assign self-registered guests to guest type:

Configure guest types at:
[Work Centers > Guest Access > Configure > Guest Types](#)

Account valid for: Maximum: 1 DAYS

☐ Require a registration code for self registration:

Fields to include	Required
<input type="checkbox"/> User name	<input type="checkbox"/>
<input type="checkbox"/> First name	<input type="checkbox"/>
<input type="checkbox"/> Last name	<input type="checkbox"/>
<input checked="" type="checkbox"/> Email address	<input checked="" type="checkbox"/>

- Set the “After registration submission, direct guest to” to **Self-Registration Success Page**

After registration submission, direct guest to

☒ Self-Registration Success page

☐ Login page with instructions about how to obtain login credentials

- Self-Registration Success Page
 - Uncheck everything except the following: **User name, Password & Allow guests to log in directly from the Self-Registration Success page**

▼ Self-Registration Success Settings

Include this information on the Self-Registration Success page:

- ☒ User name
- ☒ Password
- ☐ First name
- ☐ Last name
- ☐ Email address
- ☐ Phone number
- ☐ Company
- ☐ Location
- ☐ SMS Service Provider
- ☐ Person being visited
- ☐ Reason for visit

Allow guest to send information to self using:

- ☐ Print
- ☐ Email
- ☐ SMS
- ☐ Include an AUP on page ▼
- ☐ Require acceptance
 - ☐ Require scrolling to end of AUP

Self-Registration Success Page continues to Login page by default.

- ☒ Allow guests to log in directly from the Self-Registration Success page

- Acceptable Use Policy (AUP) Page Settings
 - Check “Include an AUP page”
 - Do not Check “Use different AUP for employees”
 - Check “Skip AUP for employees”
 - Check “Require scrolling to end of AUP”
 - Show AUP
 - Select “On first login only”

Acceptable Use Policy (AUP) Page Settings

☒ Include an AUP page

☐ Use different AUP for employees
☒ Skip AUP for employees
☒ Require scrolling to end of AUP

Show AUP

☒ On first login only
☐ On every login
☐ Every days (starting at first login)

- Guest Device Registration Settings
 - Check "Automatically register guest devices"

Guest Device Registration Settings

☒ Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

☐ Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

[Work Centers > Guest Access > Configure > Guest Types](#)

- BYOD Settings
 - Check "Allow employees to use personal devices on the network"
 - Set "Endpoint identity group:" to **EmployeeBYODEndpoints**
 - Check "Allow employees to choose to guest access only"
 - Set "After successful device configuration take employee to" the URL of your choice

▼ BYOD Settings

☒ Allow employees to use personal devices on the network

Endpoint identity group:

Configure endpoint identity groups at
[Administration > Identity Management > Groups > Endpoint Identity Groups](#)

The endpoints in this group will be purged according to the policies defined in:
[Administration > Identity Management > Settings > Endpoint purge](#)

☒ Allow employees to choose to guest access only

☐ Display Device ID field during registration

Configure employee registered devices at
[Work Centers > BYOD > Settings > Employee Registered Devices](#)

After successful device configuration take employee to:

☐ Originating URL ⓘ

☐ Success page

☒ URL:

- Authentication Success Settings
 - Set “Once authenticated, take guest to:” a URL of your choice

▼ Authentication Success Settings

Once authenticated, take guest to:

☐ Originating URL ⓘ

☐ Authentication Success page

☒ URL:

e.g. cisco.com, www.cisco.com or http://www.cisco.com

Portal Page Customization

- Login
 - Content Title: Employee Access
 - Instructional Text: Please sign into the Guest Portal with your Domain Credentials.
 - Change Create New Account link to “Not an Employee?”

- In Optional Content 2, Click the “Toggle HTML Source” icon and paste the entire content between the lines below starting with <script> and ending with </script>. When Finished, make sure to click the “Toggle HTML Source” button again and Save the Portal.

Be mindful of single quotes and double quotes as well as line breaks.

```
<script>
  //Insert New Headding and Content on first load of page.
  $('.cisco-ise-scriptable').append("<div id='login-
opts'><h1 class='cisco-ise cisco-ise-content-header'
id='ui_welcome_label'>Welcome</h1><p class='cisco-ise
cisco-ise-instruction-message'
id='ui_login_options'>Welcome to the the Guest Wireless
Portal. Please choose from the options below to gain
access to the Guest Wireless.</p></div>");

  //Insert Guest Access Button and Employee Access Button
  $('.cisco-ise-scriptable').append("<div id='login-opts-
btns'><input type='submit' value='Guest Access'
class='guest-btn' /><input type='submit' value='Employee
Access' class='employee-btn' /></div></div>");

  //Hide Username and Password Box
  $('#login_username_password').hide();
  $('.cisco-ise-form-buttons').hide();
  $("#ui_login_content_label").hide();
  $("#ui_login_instruction_message").hide();

  //Create Guest Button Event to Submit form with Predefined
Username and Password
  $('.guest-btn').on('click', function(gstevt){
    gstevt.preventDefault();

    //Don't Have an Account Button to Collect Email Address
    $('#ui_login_self_reg_button').click();
  });

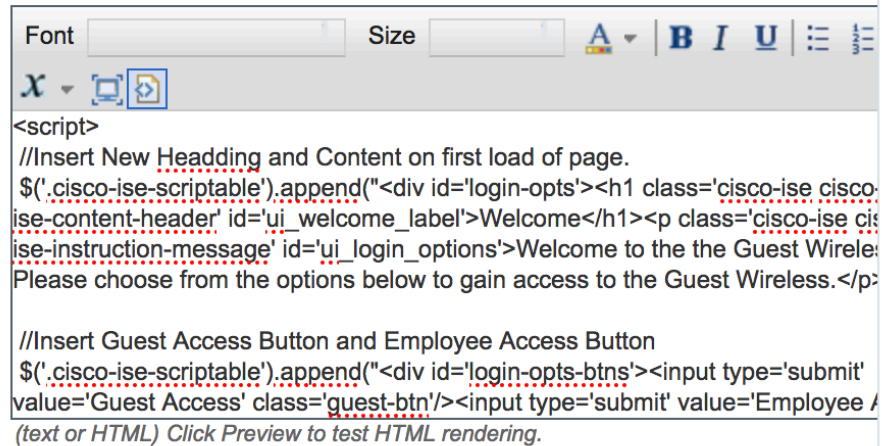
  //Create Employee button click event to remove AUP and
Check AUP box
  $('.employee-btn').on('click', function(empevt){
    empevt.preventDefault();

    //Hide Initial Login Options Content and Buttons
    $("#login-opts").hide();
    $("#login-opts-btns").hide();

    //Showing Login Form and removing AUP
    $("#login_username_password").show();
    $(".cisco-ise-form-buttons").show();
    $("#ui_aup_hotspot_text").hide();
    $("#ui_login_content_label").show();
    $("#ui_login_instruction_message").show();

  });
</script>
```

Optional Content 2



```
<script>
//Insert New Heading and Content on first load of page.
$('.cisco-ise-scriptable').append("<div id='login-opts'><h1 class='cisco-ise cisco-ise-content-header' id='ui_welcome_label'>Welcome</h1><p class='cisco-ise cisco-ise-instruction-message' id='ui_login_options'>Welcome to the the Guest Wireless. Please choose from the options below to gain access to the Guest Wireless.</p>

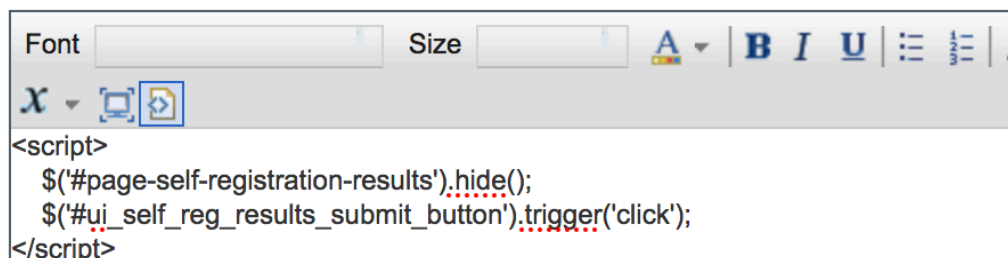
//Insert Guest Access Button and Employee Access Button
$('.cisco-ise-scriptable').append("<div id='login-opts-btns'><input type='submit' value='Guest Access' class='guest-btn'/><input type='submit' value='Employee Access' class='employee-btn'></div>");
</script>
(text or HTML) Click Preview to test HTML rendering.
```

- Self-Registration
 - Content Title: Register Device
 - Instructional Text: To gain access to the Guest wireless network, you must supply a valid email address. Any information you provide will not be used for other commercial purposes and will not be sold, rented, leased or forwarded to any third party.
 - Guest AUP text: Put your AUP here for Guest
- Self-Registration Success
 - Optional Content 2, Click the “Toggle HTML Source” icon and paste the entire content between the lines below starting with `<script>` and ending with `</script>`. When Finished, make sure to click the “Toggle HTML Source” button again and Save the Portal.

Be mindful of single quotes and double quotes as well as line breaks.

```
<script>
//Hide the Entire Page and Click the Submit Button
$('#page-self-registration-results').hide();
$('#ui_self_reg_results_submit_button').trigger('click');
</script>
```

Optional Content 2



```
<script>
$('#page-self-registration-results').hide();
$('#ui_self_reg_results_submit_button').trigger('click');
</script>
```