

ISE 2.1 Guest Enhancements

Key Highlights

- Proxy support for HTTP API (SMS)
- Bring Back from 1.2 – From First Login
- NIC Teaming
- Integration with more SAML providers for web portals
- Guest Portal allows credential and SAML SSO login option
- Sponsor Approval Pending accounts filtered view

Proxy support for http api (SMS message transmission)

Administration > System > Settings > Proxy

Proxy Settings

Proxy host server : port :

Bypass proxy for these hosts and domains

Notes

The following functionalities are impacted by the proxy settings

- Partner Mobile Management
- Endpoint Profiler Feed Service Update
- Endpoint Posture Update
- Endpoint Posture Agent Resources Download
- CRL (Certificate Revocation List) Download
- SMS Message Transmission

From First-Login Guest Type

Work Centers > Guest > Configure > Guest Type

- **Hasn't been supported since ISE 1.2**
- Release support in 2.1
- Accounts will be maintained on an upgrade
- Cannot extend an account from first login until the user first logs in
- Benefits
 - Allows creation of an account that may only be used for X amount of hrs
 - Sponsors can pre-print vouchers with credentials ahead of time
 - No reliance on location (time zones) unless using time based restrictions

The screenshot shows the 'Guest Type' configuration page. The 'Guest type name' field is set to 'FirstLoginGuestType'. The 'Description' field is empty. The 'Language File' dropdown is set to 'Language File'. The 'Collect Additional Data' button is 'Custom Fields...'. The 'Maximum Access Time' section is visible. Under 'Account duration starts', the 'From first login' radio button is selected and highlighted with a red box, while the 'From sponsor-specified date (or date of self-registration, if applicable)' radio button is unselected.

From First-Login Guest Type

Account Creation

- Sponsor portal > Create accounts
- Select from first login guest type
- Notice no start stop time, instead you enter how many days (or hours)

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

Create, manage, and approve guest accounts.

Guest type:
FirstLoginGuestType
Maximum devices that can be connected: 5 | Maximum access duration: 5 days

Guest Information
Known | Random | Import

First name:
FFLGuest

Last name:

Access Information
Duration:*
1 Days (Maximum: 5)
FromFirst Login

Create

From First-Login Guest Type

Account Creation - Account Information

- start/end time stamp not set until after first login (account is activated)
- The time left number is the time the account will be inactive before its moved to expired state and then purged by normal purge policy
- Account duration (how long it was created for ex: 8hrs or 1 day) - missing

| Account Information | |
|-------------------------------|---------------------|
| Username: | F0000001 |
| Password: | Nv4@- . gQ |
| First name: | FFLGuest |
| Last name: | |
| Email address: | |
| Company: | |
| Phone number: | |
| Person being visited (email): | |
| Reason for visit: | |
| Guest type: | FirstLoginGuestType |
| SMS provider: | Global Default |
| State: | Created |
| From date (yyyy-mm-dd): | |
| To date (yyyy-mm-dd): | |
| From | First Login |
| Location: | San Jose |
| SSID: | |
| Language: | English |
| Group tag: | |
| Time left: | 90 days |

From First-Login Guest Type

List display behaviour > sponsor portal managed accounts list

- The expiration column is empty until user logs in
- The time left number is the time the account will be inactive before its moved to expired state and then purged by normal purge policy

After the user logs in

- Account will be set with an expiration and will behave exactly like a regular guest
- All gui indications of the guest user will be the same as a regular guest (except for the guest type)



| <input type="checkbox"/> | User... | State | First Na... | Location | Sponsor | Guest T... | Expirati... | Time Left |
|--------------------------|--------------------------|---------|--------------|----------|---------|----------------------|------------------|-------------|
| <input type="checkbox"/> | f0000001 | Created | FFLGuest | San Jose | sponsor | FirstLogin... | | 90 days |
| <input type="checkbox"/> | r0000001 | Created | RegularGu... | San Jose | sponsor | Contractor (default) | 2016-06-06 00:09 | 88D 13H 57M |

From First-Login Guest Type

Workcenters > Guest Access Settings > Guest Account Purge Policy

- First Login Guest accounts move to Expired after N days as configured (90 days)
- Purge of these expired guests occurs as per Scheduled purge policy specified for any Expired guest accounts (every 15 days)

Guest Account Purge Policy

Perform an immediate purge or schedule when to delete expired accounts.

Date of last purge: Not scheduled
Date of next purge: Wed Mar 23 01:00:00 IST 2016

Schedule purge of expired guest accounts

Purge occurs every: * days (1-365)

Purge occurs every: * weeks (1-52)

Day of week: *

Time of purge: *

Expire portal-user information after: * 1-365 days Applies to:

- Inactive LDAP/AD users ⓘ
- Unused guest accounts (where access period starts from first login)

Once expired, accounts will be purged according to the purge policy specified above.

NIC Interface Teaming (Bonding)

- Used for redundancy, no aggregation of bandwidth
- Simple Primary Backup config
- Each PSN will have its own configuration (via the CLI)
- Portal selects the ports it will use across all PSNs (depending on PSN config)

▼ **Portal Settings**

HTTPS port: * (8000 - 8999)

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

| If bonding is not configured on a PSN, use: ⓘ | If bonding is configured on a PSN, use: ⓘ |
|--|--|
| <input checked="" type="checkbox"/> Gigabit Ethernet 0 | <input type="checkbox"/> Bond 0 ⓘ <i>Uses Gigabit Ethernet 0 as primary, 1 as backup.</i> |
| <input type="checkbox"/> Gigabit Ethernet 1 | <input type="checkbox"/> Bond 1 ⓘ <i>Uses Gigabit Ethernet 2 as primary, 3 as backup.</i> |
| <input type="checkbox"/> Gigabit Ethernet 2 | <input type="checkbox"/> Bond 2 ⓘ <i>Uses Gigabit Ethernet 4 as primary, 5 as backup.</i> |
| <input type="checkbox"/> Gigabit Ethernet 3 | |
| <input type="checkbox"/> Gigabit Ethernet 4 | |
| <input type="checkbox"/> Gigabit Ethernet 5 | |

Certificate group tag: * ▼

Configure certificates at:
[Administration](#) > [System](#) > [Certificates](#) > [System Certificates](#)

NIC Interface Teaming (Bonding)

- *Understand*: interface selections for a portal apply to all PSNs in a deployment.

HTTPS port: * 8443 (8000 - 8999)

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

If bonding is not configured on a PSN, use:

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3

If bonding is configured on a PSN, use:

- Bond 0 Uses Gigabit Ethernet 0 as p...
- Bond 1 Uses Gigabit Ethernet 2 as p...

This selection applies to PSNs where Eth0 and Eth1 are not bonded.

This selection applies to PSNs where Eth0 and Eth1 are bonded.

- So, it is perfectly valid to select Eth0/Eth1 and Bond0.
- When a physical interface pair is bonded, the portal listens only on the IP address of the even-numbered interface, i.e., Eth0, Eth2, or Eth4.
- On a PSN where Eth0/Eth1 are bonded, the settings shown above indicate that the PSN will not listen on the Eth0 IP address, since Bond0 is not selected. The selection of Eth0 alone has no effect when Eth0 is part of a bonded pair.

NIC Interface Teaming (Bonding)

- To help debug the assignment of interfaces to a portal on individual PSNs, detailed log messages are written to `/opt/CSCOcpm/logs/guest.log` on each node.
- Example (for settings on previous slide):

```
DEBUG [localhost-startStop-1][ ] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces specified in the portal settings: [eth0]
DEBUG [localhost-startStop-1][ ] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces on this node: [bond0, eth2, eth3]
DEBUG [localhost-startStop-1][ ] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces from portal settings that are available on
this node: [ ]
INFO [localhost-startStop-1][ ] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interface eth0 is selected for portal 'Hotspot Guest
Portal (default)', but eth0 and eth1 are bonded together as interface bond0, so the portal cannot listen on eth0 alone. However, since bond0 is not
selected for this portal, the bonded interface will not be used.
```

- Another example:

```
DEBUG [localhost-startStop-1][ ] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces specified in the portal settings: [eth0,
bond0]
DEBUG [localhost-startStop-1][ ] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces on this node: [bond0, eth2, eth3]
DEBUG [localhost-startStop-1][ ] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interfaces from portal settings that are available on
this node: [bond0]
INFO [localhost-startStop-1][ ] cisco.cpm.guestaccess.portmanager.BondedInterfaceUtils -::- Interface eth0 is selected for portal 'Hotspot Guest
Portal (default)', but eth0 and eth1 are bonded together as interface bond0, so the portal cannot listen on eth0 alone. Since bond0 is also selected for
this portal, the bonded interface will be used instead.
```

Updated SAML Support

Integration with more providers and more generic support

Guest, Sponsor and My Devices Portals

- Oracle (supported since 1.4)
- SAML SSO with PingOne (Cloud), PingFederate (CPE), Azure AD, SecureAuth
- Support Generic SAML SSO as a standard (SAML2)

SAML SSO can be used across the following portals:

- guest, sponsor, my devices, and certificate provisioning
- ISE 2.1 allows external groups to be used in mapping (no longer requires AD/LDAP)

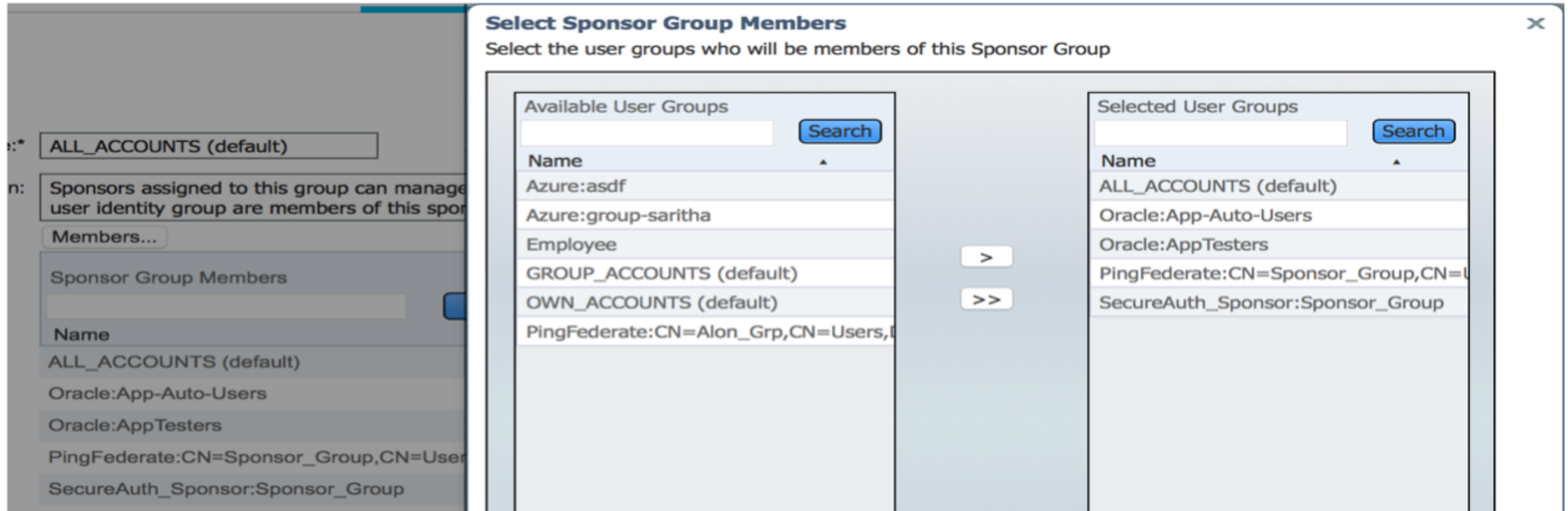
Benefit:

- Gives access to ISE SSO integration benefits to a wider range of customers.

Updated SAML Support

Workcenters > Guest Access > Configure > Sponsor Groups > Choose Group

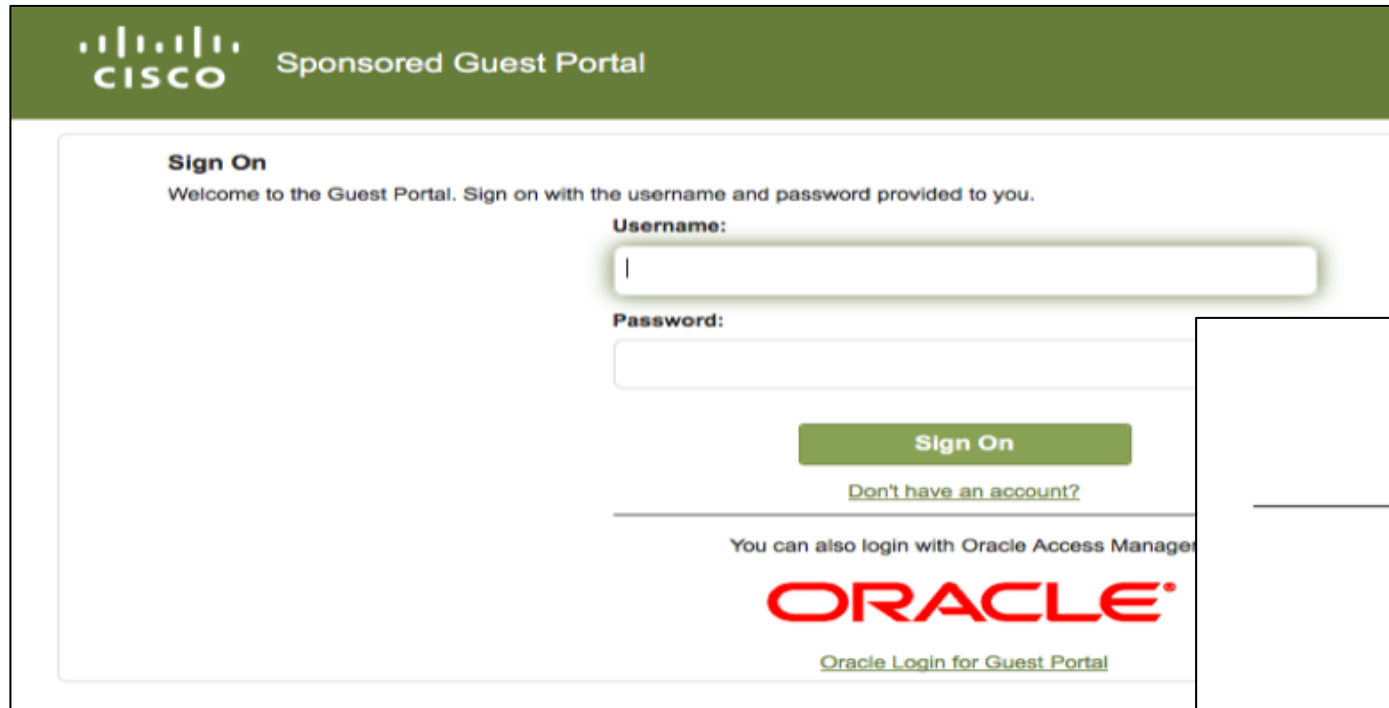
- Integration with external provider requires you to choose the external groups that can access the portal
- ISE now supports receiving group information from the provider (doesn't require ad/ldap)



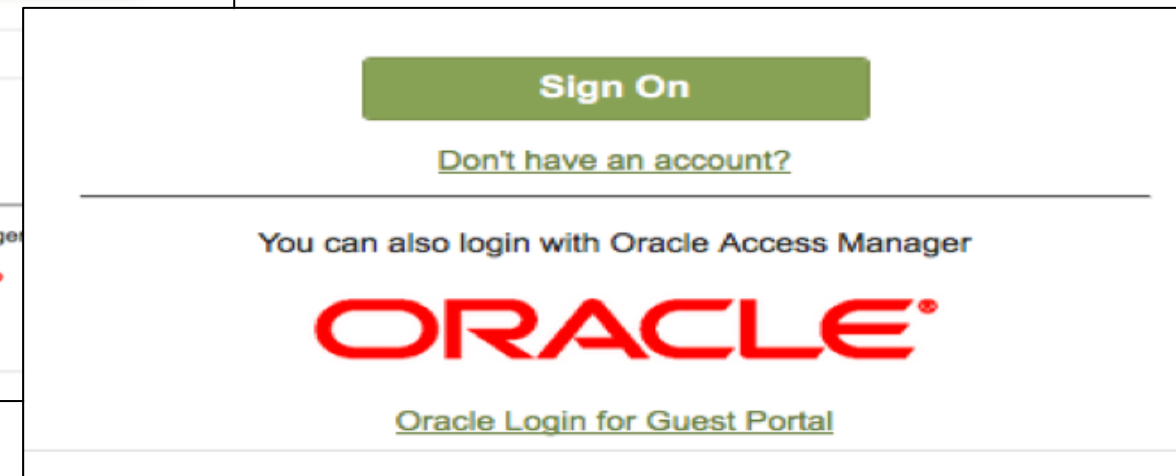
Single portal for credential and SAML SSO login

Allow guests and external provider login (employees/contractors) using single portal

- Extends on ISE 1.4 capability of allowing guest portals to point to SAML provider
- Supports 1 external provider per portal
- Benefits of having single WLAN (SSID) and portal to handle guests and other type users



The screenshot shows the Cisco Sponsored Guest Portal sign-on interface. At the top, there is a green header with the Cisco logo and the text "Sponsored Guest Portal". Below the header, the page 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:" and "Password:". Below the password field is a green "Sign On" button. Underneath the button is a link: "Don't have an account?". At the bottom of the sign-on section, there is a horizontal line, followed by the text "You can also login with Oracle Access Manager", the Oracle logo, and a link "Oracle Login for Guest Portal".



This is a close-up view of the Oracle Access Manager login section from the previous screenshot. It features a green "Sign On" button at the top. Below the button is a link: "Don't have an account?". A horizontal line separates this section from the text "You can also login with Oracle Access Manager". Below this text is the Oracle logo, and at the bottom is a link: "Oracle Login for Guest Portal".

Single portal for credential and SAML SSO login

Work Centers > Guest Access > Configure > Guest Portals

2 portals required:

- Main Portal has link to sub-portal for external IDP integration
- Authorization Policy points to the main portal

Guest Portals

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

Create Edit Duplicate Delete

| | |
|---|---|
| MyPortalMain ✓ Used in 1 rules in the Authorization policy | Allow login using : MyPortalSSOSub |
| MyPortalSSOSub ✓ Used by another portal for alternate login | Used as alternate login option by : MyPortalMain |

Single portal for credential and SAML SSO login

Work Centers > Guest Access > Configure > Guest Portals > Sub Portal (IDP)

sub-portal – portal page login settings – configured for IDP

The image shows a configuration page for a sub-portal. The main content is a form titled "Portal Settings" with the following fields:

- HTTPS port: * 8443 (8000 - 8999)
- Allowed interfaces: * For PSNs Using Physical Interfaces
 - Gigabit Ethernet 0
 - Gigabit Ethernet 1
 - Gigabit Ethernet 2
 - Gigabit Ethernet 3
 - Gigabit Ethernet 4
 - Gigabit Ethernet 5
- For PSNs with Bonded Interfaces
 - Bond 0 (i) Uses Gigabit Ethernet 0 as primary, Gigabit Ethernet 1 as backup
 - Bond 1 (i) Uses Gigabit Ethernet 2 as primary, Gigabit Ethernet 3 as backup
 - Bond 2 (i) Uses Gigabit Ethernet 4 as primary, Gigabit Ethernet 5 as backup
- Certificate group tag: * Default Portal Certificate Group
- Authentication method: * Oracle (i)

Below the form is a flowchart with four steps connected by downward arrows:

- SSO Login (highlighted with a red box)
- AUP
- Max Devices Reached
- URL (in an oval)

Additional text in the form includes links for configuring certificates and authentication methods.

Single portal for credential and SAML SSO login

Work Centers > Guest Access > Configure > Guest Portals > Sub Portal (IDP)

Users using the SAML SSO portal are mapped to: Employees using this portal as guests inherit login options from

Authentication method: * ⓘ

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

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

Display language:

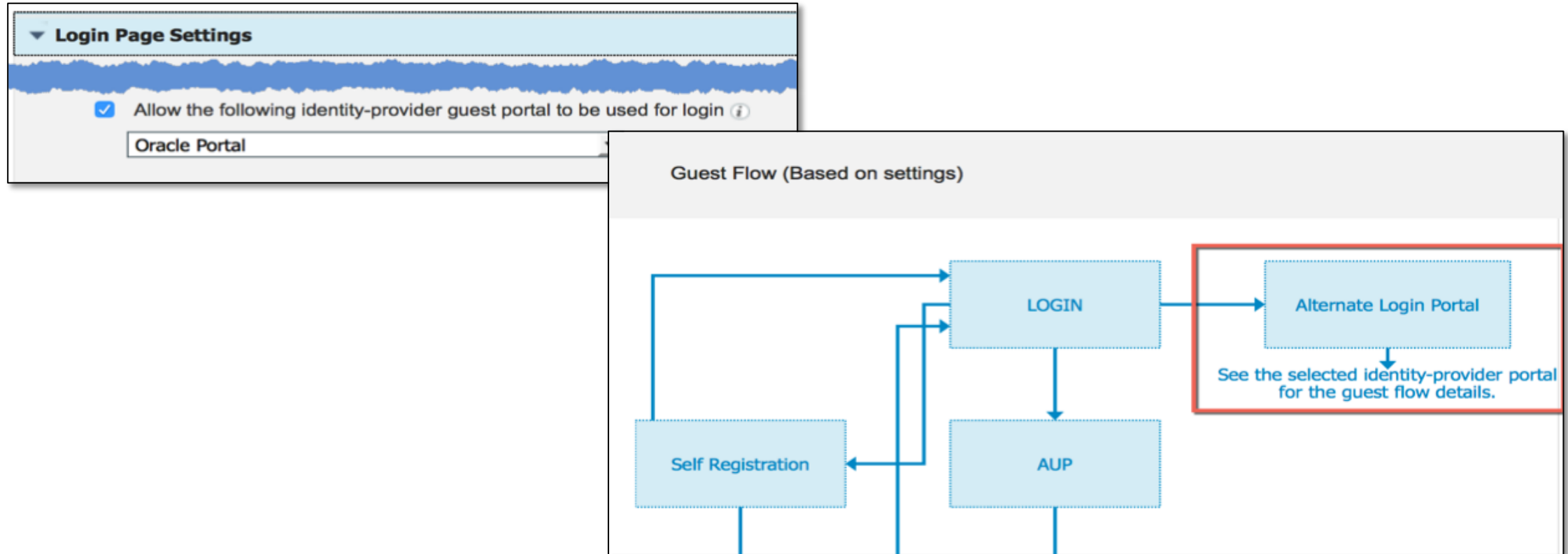
Fallback language:

Always use:

Single portal for credential and SAML SSO login

Work Centers > Guest Access > Configure > Guest Portals > Main Portal

Main Portal config points to sub-portal using IDP – portal page settings login page settings and flow diagram



Single portal for credential and SAML SSO login

Work Centers > Guest Access > Configure > Guest Portals > Main Portal

Main Portal Portal page customization for login page:

- configures options to display logo & text

The screenshot shows a configuration window for the Main Portal. It includes the following elements:

- Alternative login:** A text input field containing "You can also login with Oracle Access Manager" and a "(static text)" label.
- Alternative login access portal:** A dropdown menu set to "Oracle Portal".
- Use this text:** A text input field containing "Oracle Login for Guest Portal".
- as icon tooltip:** A label for the text input field.
- as link:** A checkbox that is checked, with a "✓" icon.
- Icon ...:** A button to select an icon, currently showing the Oracle logo.
- Close and Refresh:** A grey "X" button and a blue circular refresh button.
- Footer note:** "If both link and icon are provided, link will display beneath the icon."

Sponsor Approval Pending accounts filtered view

Workcenters > Guest Access > Configure > Sponsor Groups > Choose Group

- Filters pending accounts list to only show requests for specific sponsor
- Mapped to person being visited email (sponsor's email address) attribute
- Current support for internal user or SAML IdP accounts (AD/LDAP coming in later release)
- Benefits Sponsor Usability & Addresses organizations' privacy requirements by limiting guest data visibility to the relevant sponsor.

Sponsor Can

- View guests' passwords
 - Reset guests' account passwords
- Extend guest accounts
- Send SMS notifications with guests' credentials
- Delete guests' accounts
- Suspend guests' accounts
 - Require sponsor to provide a reason
- Reinstate suspended guests' accounts
- Approve and view requests from self-registering guests
 - Any pending accounts
 - Only pending accounts assigned to this sponsor ?
 - Access Cisco ISE guest accounts using the programmatic

You can only limit the viewing/approving of pending accounts to the sponsor who is associated with the request if the sponsor belongs to an ISE-internal or a SAML identity provider. For AD/LDAP please choose the first option

Sponsor Approval Pending accounts filtered view

Email address mapping for internal users acting as sponsors

- Administration > Identity Management > Identities > Users

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path is Administration > Identity Management > Identities > Users. The left sidebar shows a navigation menu with 'Identities' selected. The main content area shows the configuration for a 'Network Access User' named 'sponsor'. The 'Email' field is highlighted with a red box and contains the value 'sponsor@domain.com'. Other visible fields include 'Name' (sponsor) and 'Status' (Enabled).

Identity Services Engine Home Context Directory Operations Policy Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Services

Identities Groups External Identity Sources Identity Source Sequences Settings

Network Access Users List > saritha

Network Access User

* Name sponsor

Status Enabled

Email sponsor@domain.com

Passwords

Sponsor Approval Pending accounts filtered view

Email address mapping for SAML IDP Sponsors

- Administration > Identity Management > External Identity Sources > SAML Id Providers > IdP > Attributes & Advanced
- Attributes > Name in Assertion is SAML attribute configured to return email address, mapped to Name in ISE
- Advanced > mapped to Name in ISE email attribute

Identity Provider List > PingFederate

SAML Identity Provider

General Identity Provider Config. Service Provider Info. Groups **Attributes**

Attributes

+ Add Edit X Delete

| <input type="checkbox"/> | Name in Assertion* | Type | Default value | Name in ISE* |
|--------------------------|--------------------|--------|---------------|--------------|
| <input type="checkbox"/> | Email | STRING | | Email |

Identity Provider List > PingFederate

SAML Identity Provider

General Identity Provider Config. Service Provider Info. Groups Attributes **Advanced Settings**

Advanced Settings

Identity Attribute ⓘ

Subject Name

Attribute ⓘ

Email attribute ⓘ

Multi-value attributes ⓘ

Each value in a separate XML element

Multiple values in a single XML element separated by:

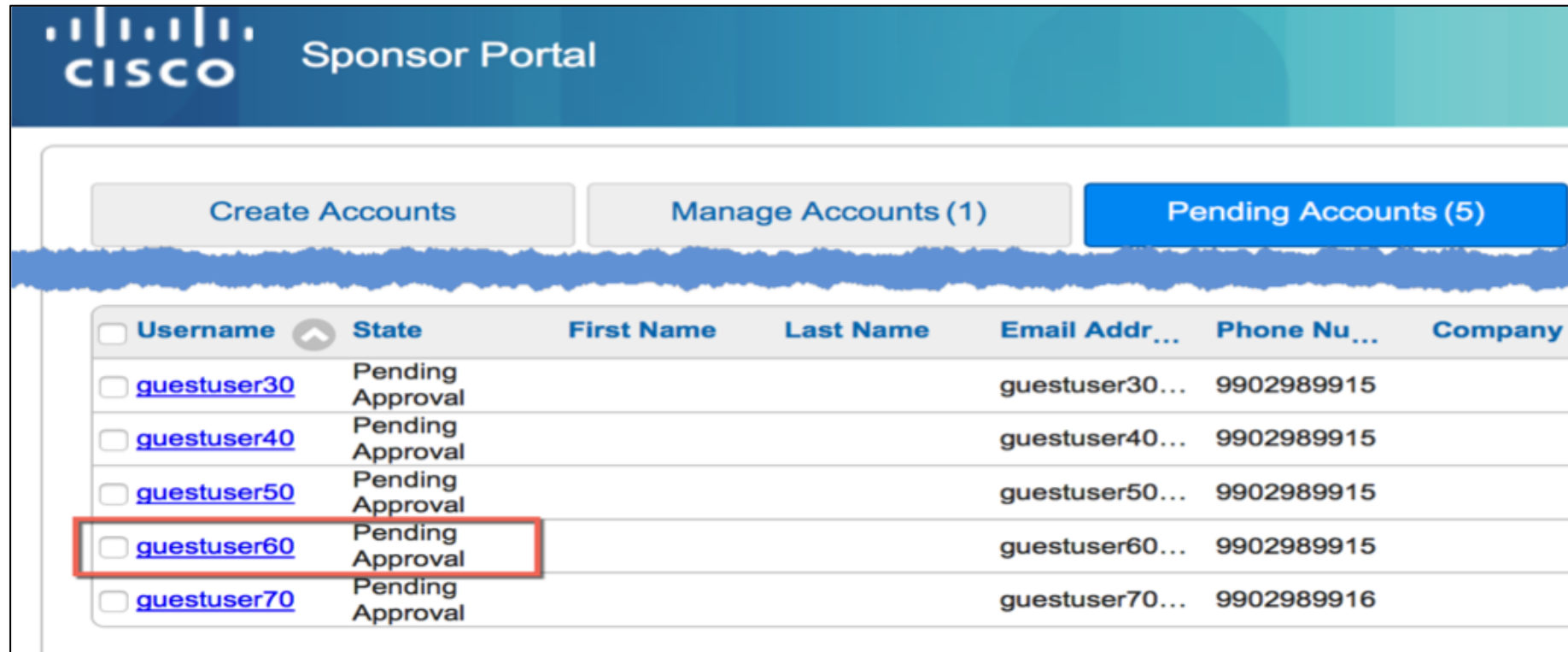
Logout Settings

Sign logout request ⓘ

Sponsor Approval Pending accounts filtered view

Unfiltered view

- Filters pending accounts list to only show requests for specific sponsor
- Mapped to person being visited email (sponsor's email address)

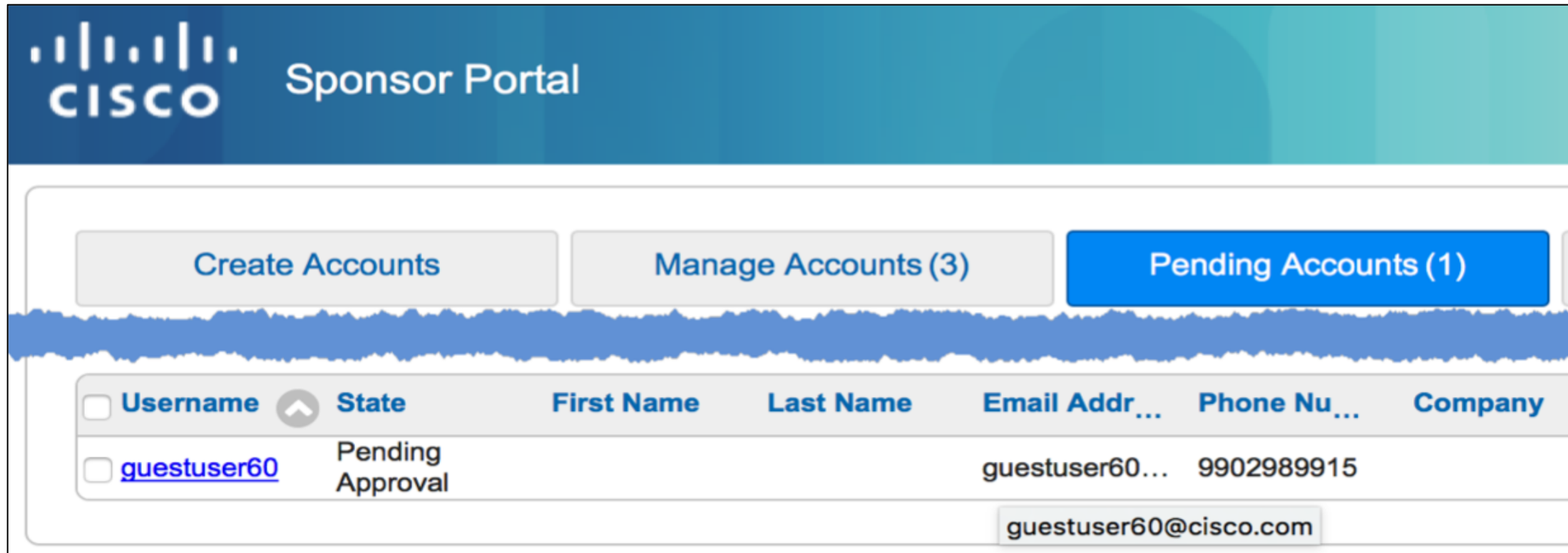


| <input type="checkbox"/> | Username | State | First Name | Last Name | Email Addr... | Phone Nu... | Company |
|--------------------------|-----------------------------|------------------|------------|-----------|----------------|-------------|---------|
| <input type="checkbox"/> | questuser30 | Pending Approval | | | questuser30... | 9902989915 | |
| <input type="checkbox"/> | questuser40 | Pending Approval | | | questuser40... | 9902989915 | |
| <input type="checkbox"/> | questuser50 | Pending Approval | | | questuser50... | 9902989915 | |
| <input type="checkbox"/> | questuser60 | Pending Approval | | | questuser60... | 9902989915 | |
| <input type="checkbox"/> | questuser70 | Pending Approval | | | questuser70... | 9902989916 | |

Sponsor Approval Pending accounts filtered view

Filtered View

- Filters pending accounts list to only show requests for specific sponsor
- Mapped to person being visited email (sponsor's email address)



The screenshot displays the Cisco Sponsor Portal interface. At the top left is the Cisco logo and the text "Sponsor Portal". Below this are three buttons: "Create Accounts", "Manage Accounts (3)", and "Pending Accounts (1)". The "Pending Accounts (1)" button is highlighted in blue. Below the buttons is a table with the following columns: Username, State, First Name, Last Name, Email Addr..., Phone Nu..., and Company. A single row is visible in the table, representing a pending account for "questuser60". The "State" column for this row contains the text "Pending Approval". The "Email Addr..." column contains the email address "questuser60@cisco.com", which is also displayed in a separate text box below the table.

| <input type="checkbox"/> Username | State | First Name | Last Name | Email Addr... | Phone Nu... | Company |
|--|------------------|------------|-----------|----------------|-------------|---------|
| <input type="checkbox"/> questuser60 | Pending Approval | | | questuser60... | 9902989915 | |

questuser60@cisco.com



Guest Enhancements

Identity Services Engine 2.2

Policy & Access

Jason Kunst, TME

January 2017

Guest Enhancements

- Single click guest account approvals
 - Sponsor approval email includes approve/deny links
- Pending Approval Filtering off person being visited
 - Added support for AD/LDAP (ISE 2.1 SAML/internal already supported)
- Sponsor Portal enhancements
 - auto-timezone
 - Column add/remove/resize and reorder
 - Search on phone number
 - Ability to notify guest even though sponsor can't see password
 - Creation date column

Guest Enhancements

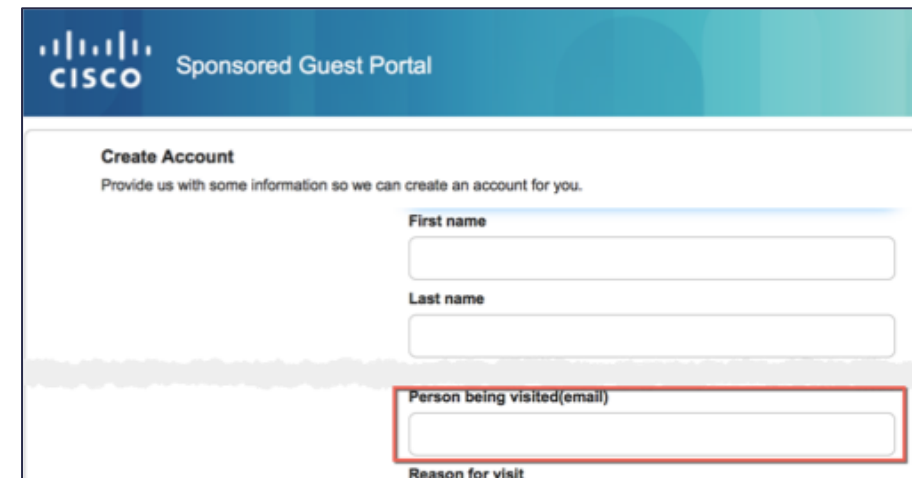
- Bring Back from 1.2
 - Custom Portal Files (replaces need for file remediation)
 - Mini-editor choose custom file
 - Support of video, images, javascript, .JSON
 - Sponsor group LDAP attributes
 - Auto send notification to guest if email address present

Guest Enhancements

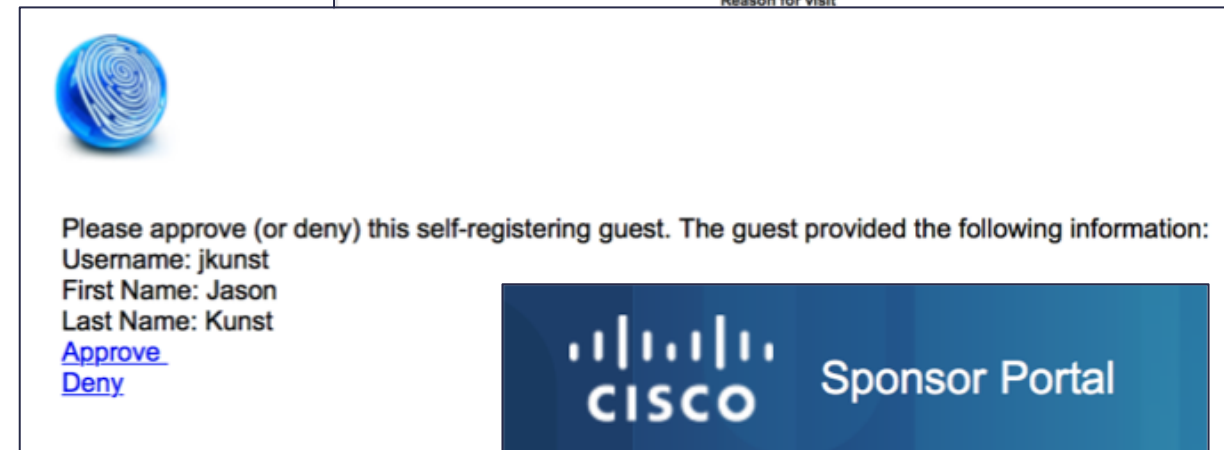
- Set guest password via CSV and API
- Background Image support
- Hotspot COA (Change of Authorization)
 - re-auth vs terminate (fixes hotspot reconnect delays of 10–30 sec)
- Sponsor Portal guest import allows sponsor to set the password
- ERS API updates
 - Set guest password
 - Create guest types and sponsor groups

Single click sponsor approval Overview

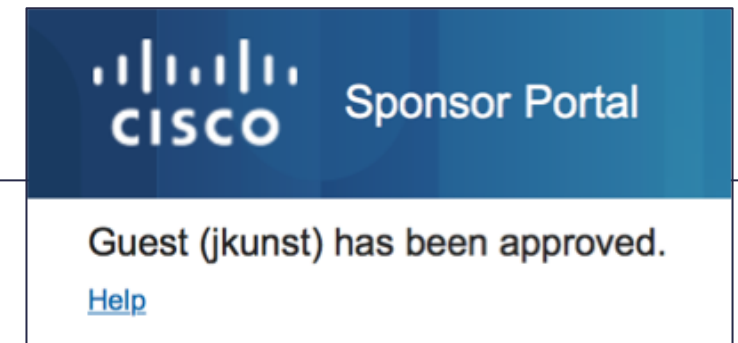
- Self-registered accounts can be approved with a single click from the notification emails
- Relies on the person being visited (sponsor) email address or can be sent to list of sponsors
- Supported with ad/ldap email addresses



The screenshot shows the 'Create Account' form in the Cisco Sponsored Guest Portal. The form includes input fields for 'First name', 'Last name', and 'Person being visited(email)'. The 'Person being visited(email)' field is highlighted with a red border. Below the form, there is a 'Reason for visit' label.



The screenshot shows an approval notification email from the Cisco Sponsor Portal. It features a blue fingerprint icon and the following text: 'Please approve (or deny) this self-registering guest. The guest provided the following information: Username: jkunst, First Name: Jason, Last Name: Kunst'. Below the information are two links: 'Approve' and 'Deny'.



The screenshot shows the confirmation message in the Cisco Sponsor Portal. It displays the Cisco logo and the text: 'Guest (jkunst) has been approved.' Below the message is a 'Help' link.

Single click sponsor approval person being visited

- allows direct approval (with optional authentication)
- Links valid for minutes, day, hours
- Sponsor is validated against List of sponsor portals upon self-registration
- Customization from 1st Portal matched

Require self-registered guests to be approved
Email approval request to: **person being visited** ⓘ

Enter a comma-separated list of email addresses

[Work Centers > Guest Access > Settings > Guest Email Settings](#)

Approve/Deny Links

(Approval request email includes Approve & Deny links by default.)

Links are valid for (1-2 days)

Require sponsor to provide credentials for authentication

Sponsor is matched to a Sponsor Portal to verify approval privileges
[< Hide Details](#)

The following list of sponsor portals is used to verify approval privileges ⓘ

Sponsor Portal (default)

Single click sponsor approval

sponsor email addresses listed below

- Requires authentication as the person being visited is unknown
- Sponsor validated during login to approval portal

Require self-registered guests to be approved

Email approval request to: sponsor email addresses listed below ⓘ

Enter a comma-separated list of email addresses

[Work Centers](#) > [Guest Access](#) > [Settings](#) > [Guest Email Settings](#)

Approve/Deny Links

(Approval request email includes Approve & Deny links by default.)

Links are valid for (1-2 days)

Sponsor is matched to a Sponsor Portal to verify approval privileges

[< Hide Details](#)

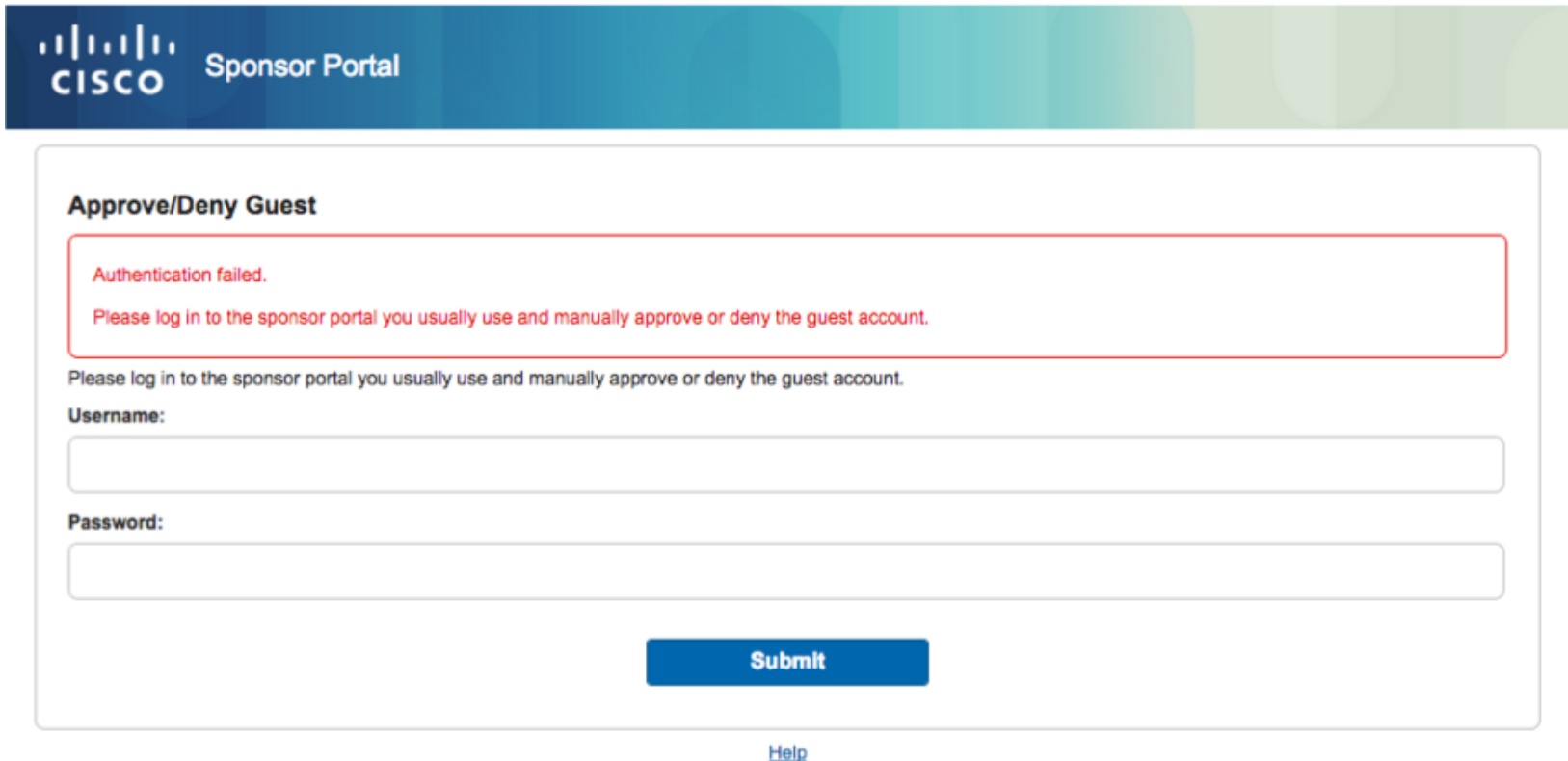
The following list of sponsor portals is used to verify approval privileges ⓘ

Sponsor Portal (default)

Single click sponsor approval

sponsor email addresses listed below


- Failure message for no matching identity source sequence



The screenshot shows the Cisco Sponsor Portal interface. At the top left is the Cisco logo and the text 'Sponsor Portal'. The main content area is titled 'Approve/Deny Guest'. A red-bordered box contains the following text: 'Authentication failed.' and 'Please log in to the sponsor portal you usually use and manually approve or deny the guest account.' Below this box, the same instruction is repeated. There are two input fields: 'Username:' and 'Password:'. A blue 'Submit' button is located at the bottom of the form. A 'Help' link is positioned below the 'Submit' button.

Sponsor Portal Enhancements

Search on phone number!

 Sponsor Portal Welcome sponsor ▾

[Create Accounts](#) [Manage Accounts \(2\)](#) [Pending Accounts \(0\)](#) [Notices \(0\)](#)

Create, manage, and approve guest accounts.

(**1 accounts found**)

[Edit](#) [Resend](#) [Extend](#) [Suspend](#) [Delete](#) [Reset Password](#) [Reinstate](#) [Refresh](#)

| User... | State | First Na... | Last Name | Phone N... | Location | Sponsor | Guest T... | Creation... | Expirati... | Time Left |
|---|---------|-------------|-----------|--------------|----------|---------|----------------------|------------------|------------------|-------------|
| <input type="checkbox"/> i001 | Created | john | | 508-555-1212 | San Jose | sponsor | Contractor (default) | 2016-09-13 00:49 | 2016-12-10 19:49 | 88D 23H 00M |

...

Sponsor Portal Enhancements


Reorder, Resize, Add/Remove Columns plus a new one creation date!

The screenshot displays the Cisco Sponsor Portal interface. At the top, there is a navigation bar with the Cisco logo and the text "Sponsor Portal". Below this, there are several buttons: "Create Accounts", "Manage Accounts (2)", "Pending Accounts (0)", and "Notice". A search bar is present below the buttons. A table of accounts is shown with columns: First Name, Last Name, Email Address, Group Tag, Phone Number, Location, and Creation Date. A dropdown menu is open on the right side, showing a list of columns that can be selected or deselected: Username, State, First Name, Last Name, Email Address, Phone Number, Group Tag, Location, Sponsor, Guest Type, and Creation Date. A red arrow points from the "Group Tag" column in the top table to the "Group Tag" column in the bottom table. A red box highlights the "Creation Date" and "Expiration Date" columns in the bottom table.

| First Na... | Last Name | Email A... | Group Tag | Phone N... | Location | Creation... | Expiration... |
|--------------------------------|-----------|------------|-----------|--------------|----------|-----------------------------------|------------------|
| <input type="checkbox"/> john | | | | 508-555-1212 | San Jose | 2016-09-13 00:49 2016-12-10 19:49 | 2016-12-10 19:49 |
| <input type="checkbox"/> jason | | | | 617-555-1212 | San Jose | 2016-09-13 00:50 2016-12-10 19:49 | 2016-12-10 19:49 |

Sponsor Portal Enhancements

Browser Auto-Timezone

 Sponsor Portal Welcome sponsor

[Create Accounts](#) [Manage Accounts \(2\)](#) [Pending Accounts \(0\)](#) [Notices \(0\)](#)

Create, manage, and approve guest accounts.

Guest type:
Contractor (default)
Maximum devices that can be connected: 5 | Maximum access duration: 365 days

Guest Information

[Known](#) [Random](#) [Import](#)

First name:

Last name:

Email address:

Phone number:

Access Information

Duration:* Days (Maximum: 365)

From Date (yyyy-mm-dd) * From Time *

To Date (yyyy-mm-dd) * To Time *

Location:
Zulu

[Create](#)

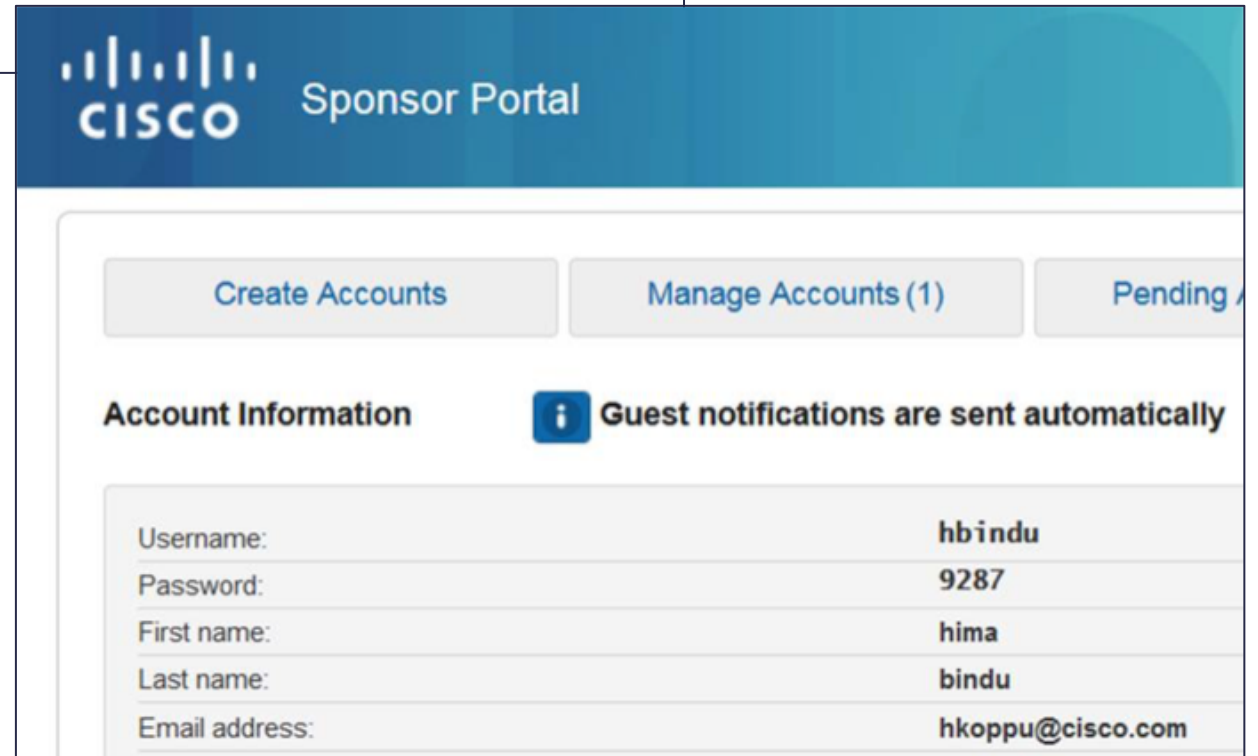
Sponsor Portal Enhancements

Auto notify guest if email address is present

Automatic guest notification:

Automatically email guests upon account creation if email address is available.

Sponsor Permissions



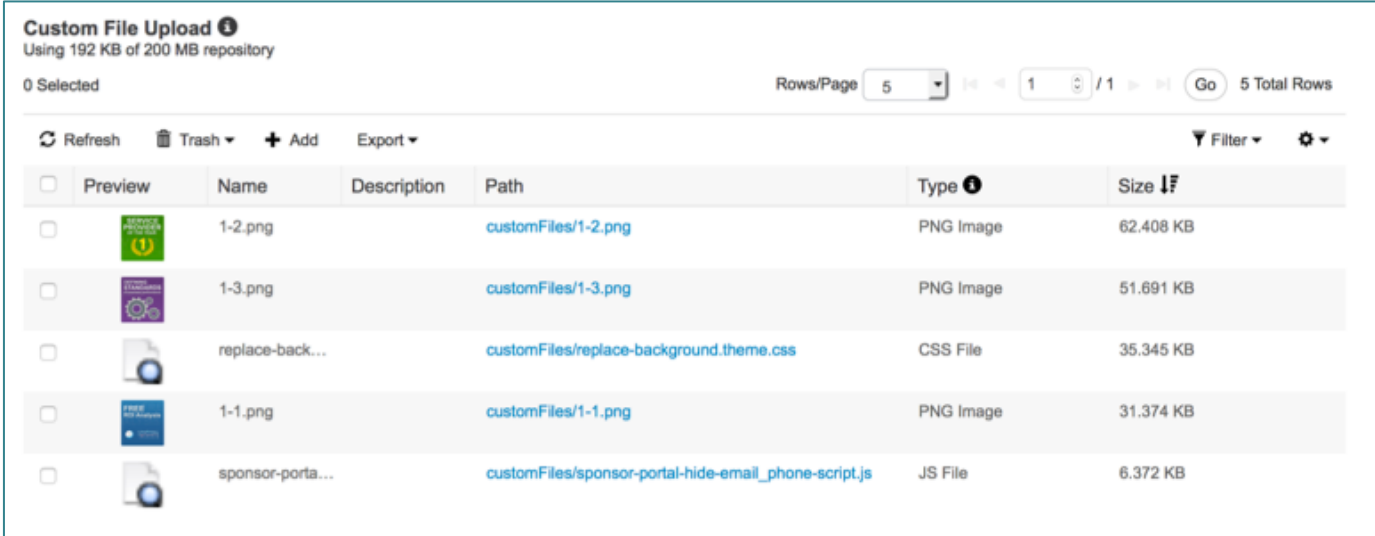
The screenshot shows the Cisco Sponsor Portal interface. At the top, there is a blue header with the Cisco logo and the text "Sponsor Portal". Below the header, there are three buttons: "Create Accounts", "Manage Accounts (1)", and "Pending". Underneath the buttons, there is a section titled "Account Information" with a blue information icon and the text "Guest notifications are sent automatically". Below this, there is a table with account details.

| | |
|----------------|------------------|
| Username: | hbindu |
| Password: | 9287 |
| First name: | hima |
| Last name: | bindu |
| Email address: | hkoppu@cisco.com |

Custom Portal Files

Bring Back from 1.2 - host needed portal files for customization






- .JSON, .JS, Images (.gif, .jpg, .png), Videos (.mp4)
- Remove need for YAWS - Yet another web server 😊
- Remove need for file remediation hosting of files (Apex licenseing)



Custom File Upload
Using 192 KB of 200 MB repository

0 Selected Rows/Page 5 1 / 1 Go 5 Total Rows

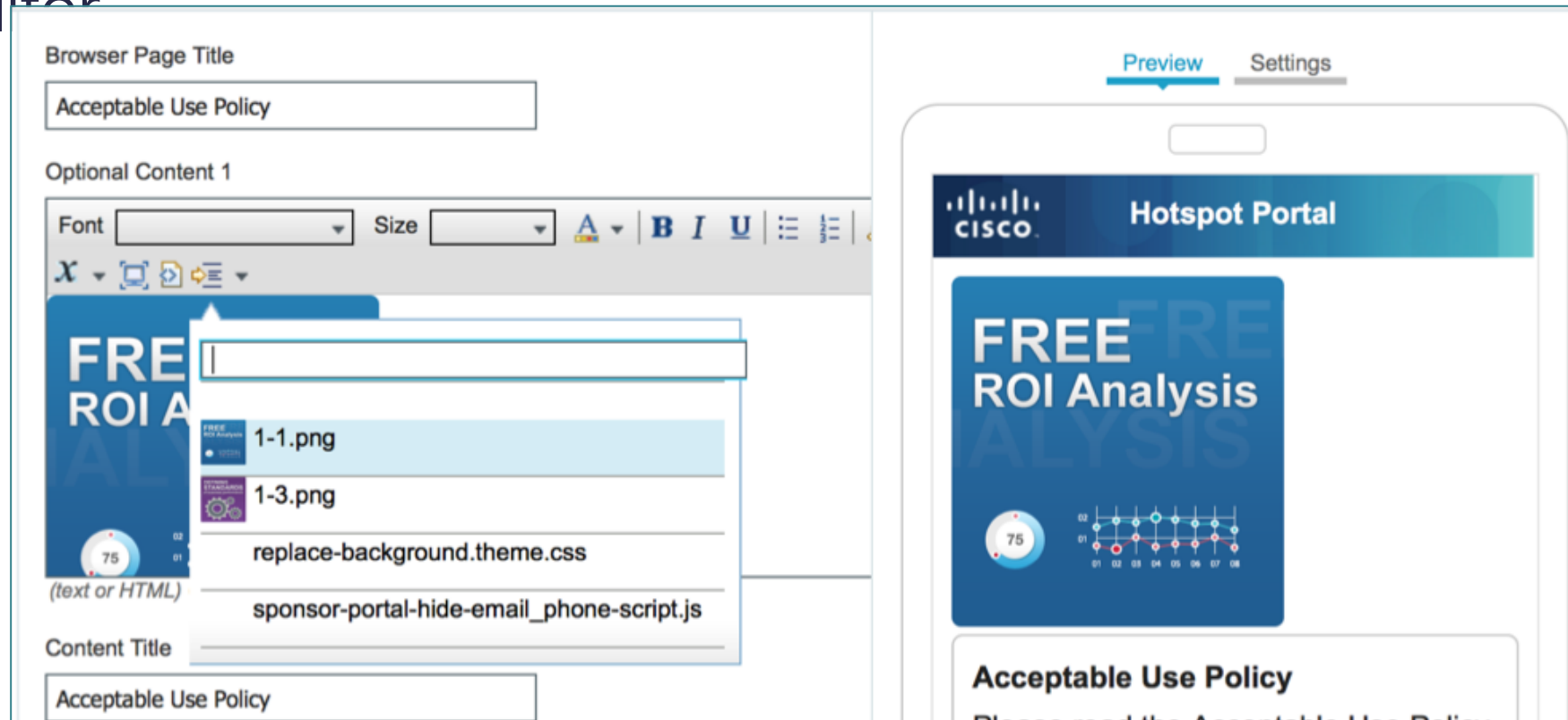
Refresh Trash Add Export Filter

| Preview | Name | Description | Path | Type | Size |
|---|------------------|-------------|---|-----------|-----------|
|  | 1-2.png | | customFiles/1-2.png | PNG Image | 62.408 KB |
|  | 1-3.png | | customFiles/1-3.png | PNG Image | 51.691 KB |
|  | replace-back... | | customFiles/replace-background.theme.css | CSS File | 35.345 KB |
|  | 1-1.png | | customFiles/1-1.png | PNG Image | 31.374 KB |
|  | sponsor-porta... | | customFiles/sponsor-portal-hide-email_phone-script.js | JS File | 6.372 KB |

Custom Portal Files

mini-editor insert file easiness

- Direct access to the custom portal files from the mini-editor



Custom Portal Files

Upload HTML to use as a message portal for quarantine or other flows

- **File path:**
<https://iseip:port/portal/customFiles/mymessage.html>
- **Replaces hotspot as a message portal**
<https://communities.cisco.com/message/212221#212221>

Authorization Profiles > Remediation_Message

Authorization Profile

* Name

Description

* Access Type

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = url-redirect-acl=REDIRECT_ACL

Cisco:cisco-av-pair = 43/portal/customFiles/mymessage.html

▼ **Attributes Details**

Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=REDIRECT_ACL
cisco-av-pair = url-redirect=https://10.86.118.26:8443/portal/customFiles/mymessage.html

Custom Portal Files



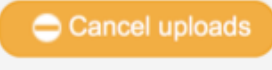
Uploading

- Upload multiple files at a time
- Supports up to 200mb
- Max file size is 50mb

Add files

Upload files

| | | |
|---|------------|-------|
| sponsor-portal-hide-email_phone-script.js | ✓ Uploaded | Clear |
| replace-background.theme.css | ✓ Uploaded | Clear |
| 1-1.png | ✓ Uploaded | Clear |
| 1-2.png | ✓ Uploaded | Clear |
| 1-3.png | ✓ Uploaded | Clear |

 Add files...  Start uploads  Cancel uploads


Custom Portal Files

Export all or select files

Custom File Upload ⓘ
Using 128 KB of 200 MB repository


0 Selected

Refresh Trash Add Export

| <input type="checkbox"/> | Preview | Name |
|--------------------------|--|---------|
| <input type="checkbox"/> |  | 1-3.png |

Opening allCustomFiles_export.zip

You have chosen to open:

 allCustomFiles_export.zip
which is: ZIP archive
from: <https://10.86.118.26>

What should Firefox do with this file?

Open with Archive Utility (default)

Save File

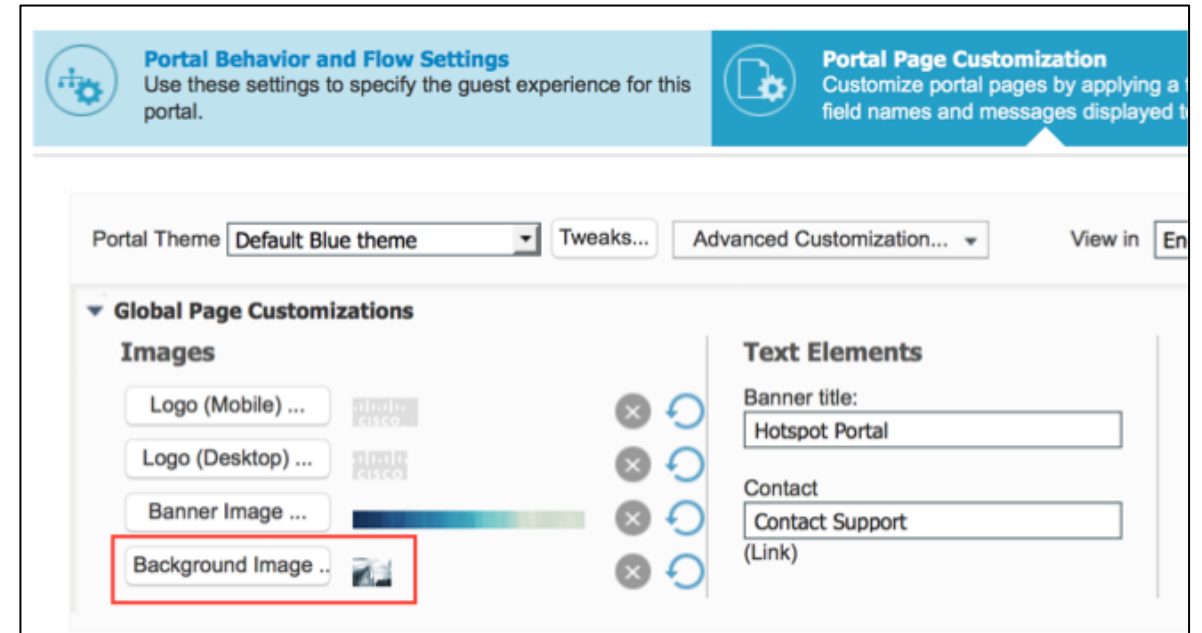
Do this automatically for files like this from now on.

Cancel OK

Background images

background image for your portal

- Built-in mechanism
- No more need to use workaround
- <https://supportforums.cisco.com/discussion/12344731/ise-13-portal-customization-background-image>



Sponsor Group mapping off attributes grant access off AD/LDAP, ODBC SAML Attributes

Bring Back From ISE 1.2!

Removes need for workaround (ISE 1.3-2.1)

<https://communities.cisco.com/docs/DOC-64526>



The screenshot shows the Cisco Communities website interface. At the top, there is a navigation bar with the Cisco logo, the word "Communities", a "50+" badge, and a user profile for "Jason Kunst" with "4,129 points". Below this is a secondary navigation bar with links for "Products & Services", "Partners", "Global", "Developer", "Cisco Customer Connection", and "Support". The main content area displays a document titled "ISE 1.3-2.1 Sponsor Authorization on Secondary Attributes" with a "Version 3" badge. The document is attributed to "chyps" and "Jason Kunst". The text of the document explains that ISE 1.2 supported authorization based on Identity Group membership, while ISE 1.3 introduced enhancements that limit authorization to group membership. The document provides two workarounds for leveraging group membership and secondary attributes for portal authorization in ISE 1.3, 1.4, 2.0, and 2.1. Social sharing buttons for Like, G+, Share, and Tweet are visible on the right side of the document content.

Sponsor Group mapping off attributes

grant access off AD/LDAP, ODBC SAML Attributes

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Identity Management > External Identity Sources > LDAP Identity Sources List > LDAP. The left sidebar shows a tree view of External Identity Sources, with LDAP selected. The main content area displays the 'LDAP Identity Source' configuration page, with the 'Attributes' tab active. Below the tabs, there are buttons for 'Edit', '+ Add', and 'X Delete Attribute'. A table lists the attributes for the LDAP identity source.

| <input type="checkbox"/> | Name | Type | Default | Internal Name |
|--------------------------|-------------|--------|---------|---------------|
| <input type="checkbox"/> | cn | STRING | | cn |
| <input type="checkbox"/> | givenName | STRING | | givenName |
| <input type="checkbox"/> | objectClass | STRING | | objectClass |
| <input type="checkbox"/> | sn | STRING | | sn |
| <input type="checkbox"/> | uid | STRING | | uid |

Sponsor Group mapping off attributes

grant access off AD/LDAP, ODBC SAML Attributes

Sponsor group name:*

Description:

Match Criteria

Member Groups - Sponsor must belong to at least one of the selected groups.

Members...

- ALL_ACCOUNTS (default)
- LDAP:cn=Accounting Managers,ou=groups,dc=ildap,dc=com
- LDAP:cn=Directory Administrators,dc=ildap,dc=com

Other conditions (optional) - sponsor must match all conditions.

| | | | | | | |
|---|---------------------|---|--------|-----------------|-----|----|
| ◇ | LDAP:uid | ⌵ | Equals | svani@ildap.coi | AND | ⚙️ |
| ◇ | LDAP:givenName | ⌵ | Equals | sathya | AND | ⚙️ |
| ◇ | LDAP:cn | ⌵ | Equals | sathya vani | AND | ⚙️ |
| ◇ | LDAP:sn | ⌵ | Equals | Vani | AND | ⚙️ |
| ◇ | LDAP:objectClass | ⌵ | Equals | person | AND | ⚙️ |
| ◇ | LDAP:ExternalGro... | ⌵ | Equals | ap,dc=corr | | ⚙️ |


Verify that these sponsors are included in the identity source sequence associated with the sponsor portal they will use.



Sponsor Group mapping off attributes

grant access off AD/LDAP, ODBC SAML Attributes

Sponsor Groups

You can edit and customize the default sponsor groups and create additional ones.

A sponsor is assigned the permissions from all matching sponsor groups (multiple matches are permitted) 

| Enabled | Name | Member Groups | Other Conditions |
|---|--|--|---|
|  | ALL_ACCOUNTS (default) Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group | LDAP:cn=Directory Administrators, dc=ildap,dc=com LDAP:cn=PD More | LDAP:uid EQUALS svani@ildap.com AND LDAP:givenName EQUALS sathya AND More |
|  | GROUP_ACCOUNTS (default) Sponsors assigned to this group can manage just the guest accounts created by sponsors from the same sponsor group. By default, users in the GROUP_ACCOUNTS user identity group are members of this sponsor group | GROUP_ACCOUNTS (default) | |

Sponsor Group mapping off attributes

grant access off AD/LDAP, ODBC SAML Attributes

| Enabled | Name | Member Groups | Other Conditions |
|---|--|---|---|
|  | ALL_ACCOUNTS (default) Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group | LDAP:cn=Directory Administrators, dc=ildap,dc=com LDAP:cn=PD Managers,ou=groups,dc=i ALL_ACCOUNTS (default) LDAP:cn=Accounting Managers,ou=groups,dc=i LDAP:cn=emailtype_own, dc=ildap,dc=com LDAP:cn=QA Managers,ou=groups,dc=i LDAP:cn=emailtype_grou dc=ildap,dc=com LDAP:cn=lsgroup,ou=Peo dc=ildap,dc=com LDAP:cn=HR Managers,ou=groups,dc=i | LDAP:uid EQUALS svani@ildap.com AND LDAP:givenName EQUALS sathya AND LDAP:cn EQUALS sathya vani AND LDAP:sn EQUALS Vani AND LDAP:objectClass EQUALS person AND LDAP:ExternalGroups EQUALS cn=emailtype_group,ou=People, dc=ildap,dc=com |

Hotspot COA Reauthenticate Option

- Bad user experience if disconnect when roaming open networks, some devices take a while to reconnect (10–30 sec)
- ISE 1.3–2.1 are disconnect (terminate)
- CSCcut93791 – Introduced in 1.4.1 & ISE 2.1 patch 1

The screenshot displays the configuration page for a Hotspot Guest Portal. At the top, the 'Portal Name' is 'Hotspot Guest Portal (default)' and the 'Description' is 'Guests do not require username and password credentials to access the net'. Below this are two tabs: 'Portal Behavior and Flow Settings' and 'Portal Page Customization'. The 'Portal Settings' section is expanded, showing the following configuration:

- HTTPS port: * 8443 (8000 - 8999)
- Allowed interfaces: * Gigabit Ethernet 0, Gigabit Ethernet 1, Gigabit Ethernet 2
- Purge endpoints in this identity group: 30 days
- Configure endpoint purge at: [Administration > Identity Management > Settings > Endpoint purge](#)
- CoA Type: CoA Reauthenticate ⓘ, CoA Terminate

The 'CoA Type' section is highlighted with a red box.

Sponsor Portal CSV import set password

- Either one (or both) of the username / password columns need to be present in the imported file
- The ISE application provides values for the missing column data
- User name and password values in the imported file need not be compliant with the Guest UI settings for username / password policies

Guest Information

| | | |
|-------|--------|--------|
| Known | Random | Import |
|-------|--------|--------|

Click to download the import template file.
[Download Template](#)

Select file:
 No file selected. Maximum: 200

Group tag:

Language:
English - English