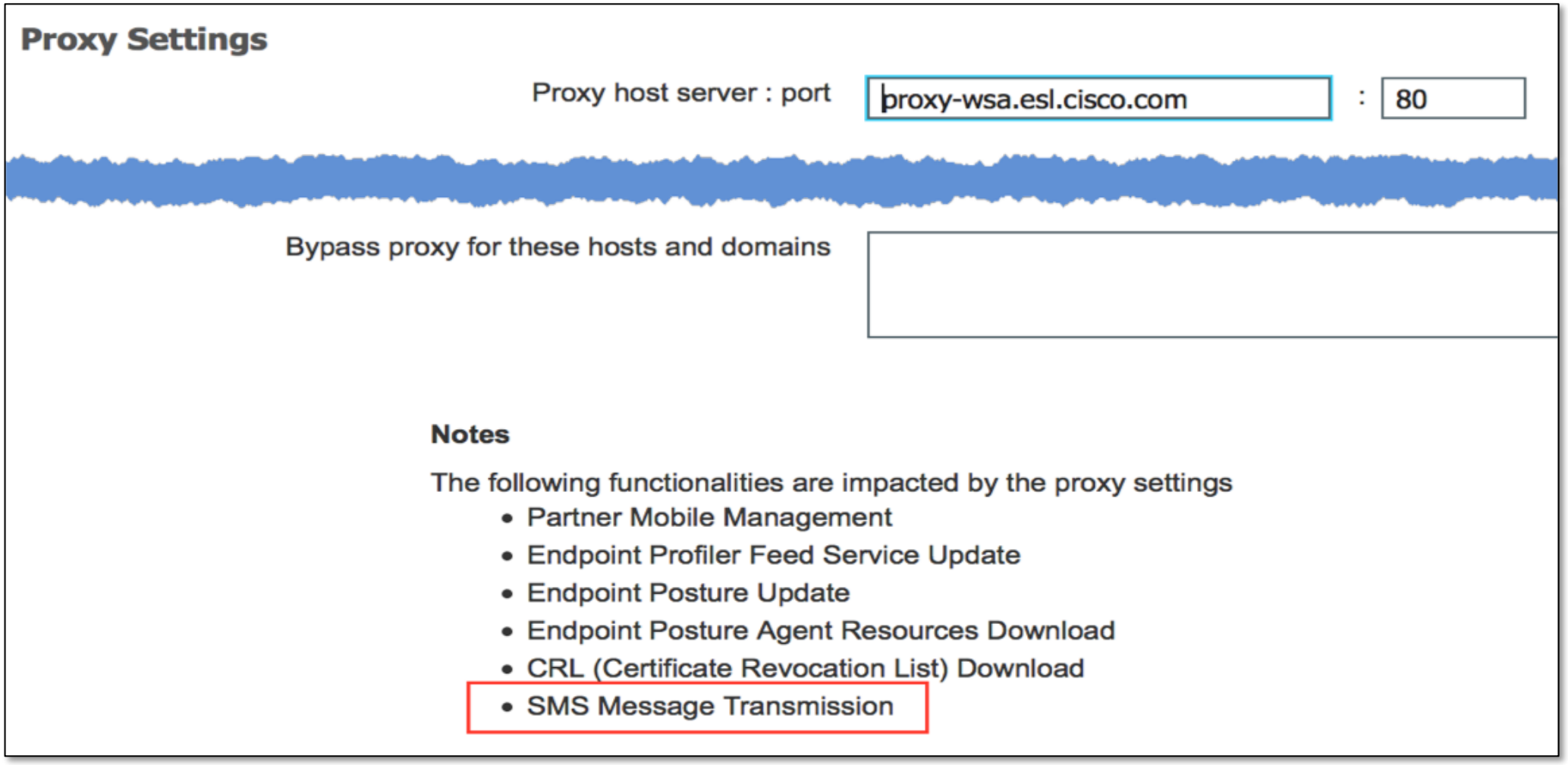
ISE 2.1 Guest Enhancements

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)

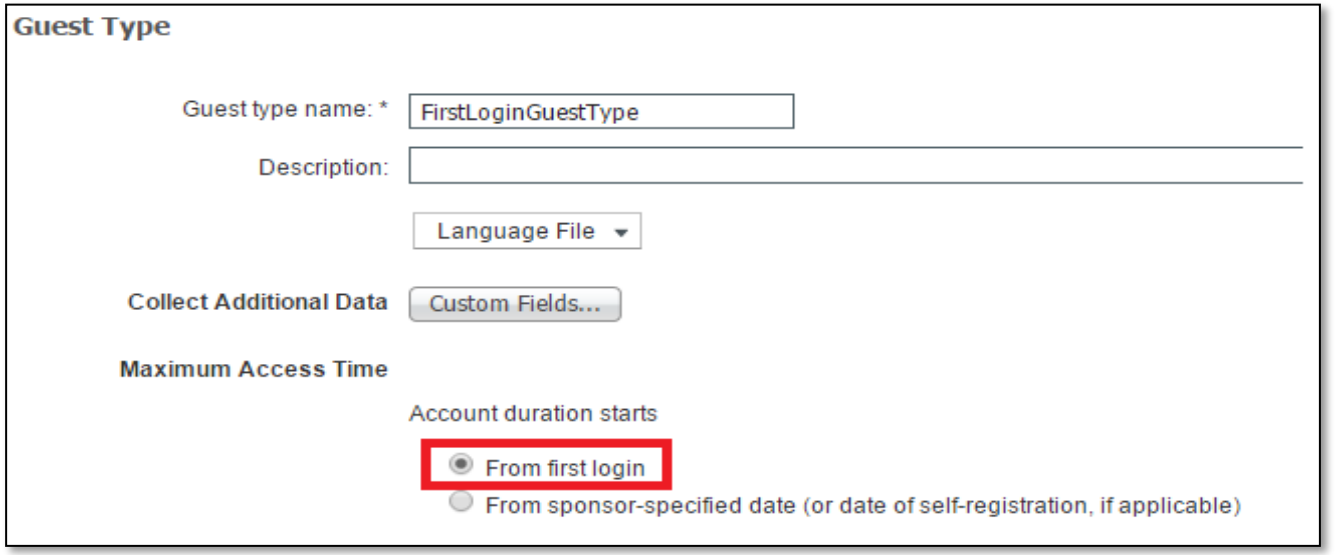
Administration > System > Settings > Proxy



From First-Login Guest Type

Work Centers > Guest > Configure > Guest Type

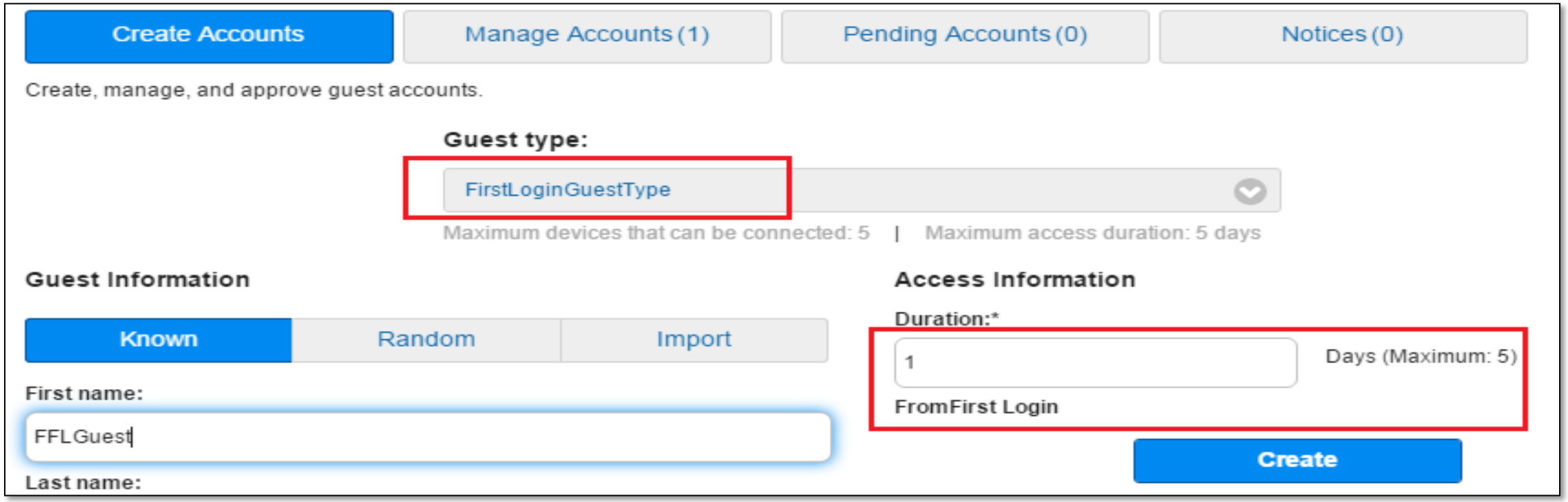
- **Hasn't been supported since ISE 1.2**
- Release support in 2.1
- Accounts will be maintained on an upgrade
- Cannot extend an account from first login until the user first logs in
- Benefits
  - Allows creation of an account that may only be used for X amount of hrs
  - Sponsors can pre-print vouchers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



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)



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

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

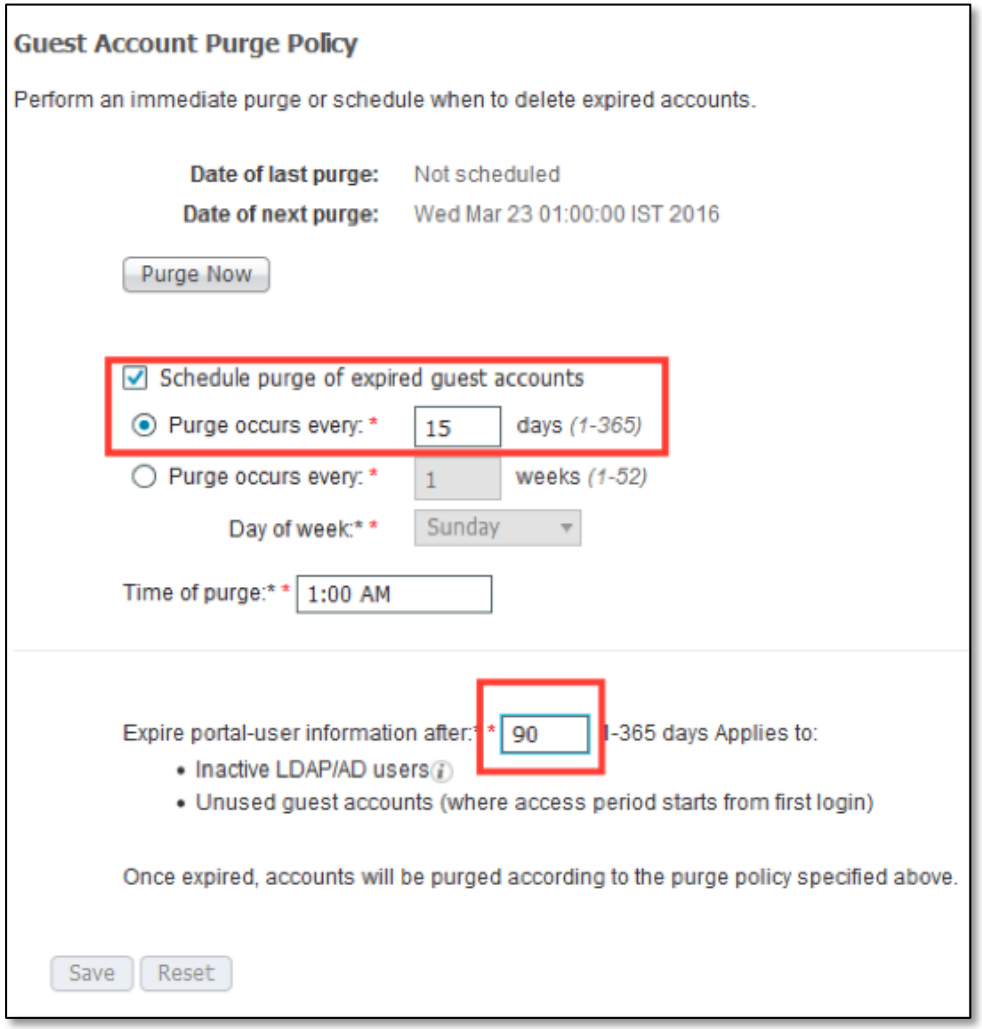
After the user logs in

- 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)

From First-Login Guest Type

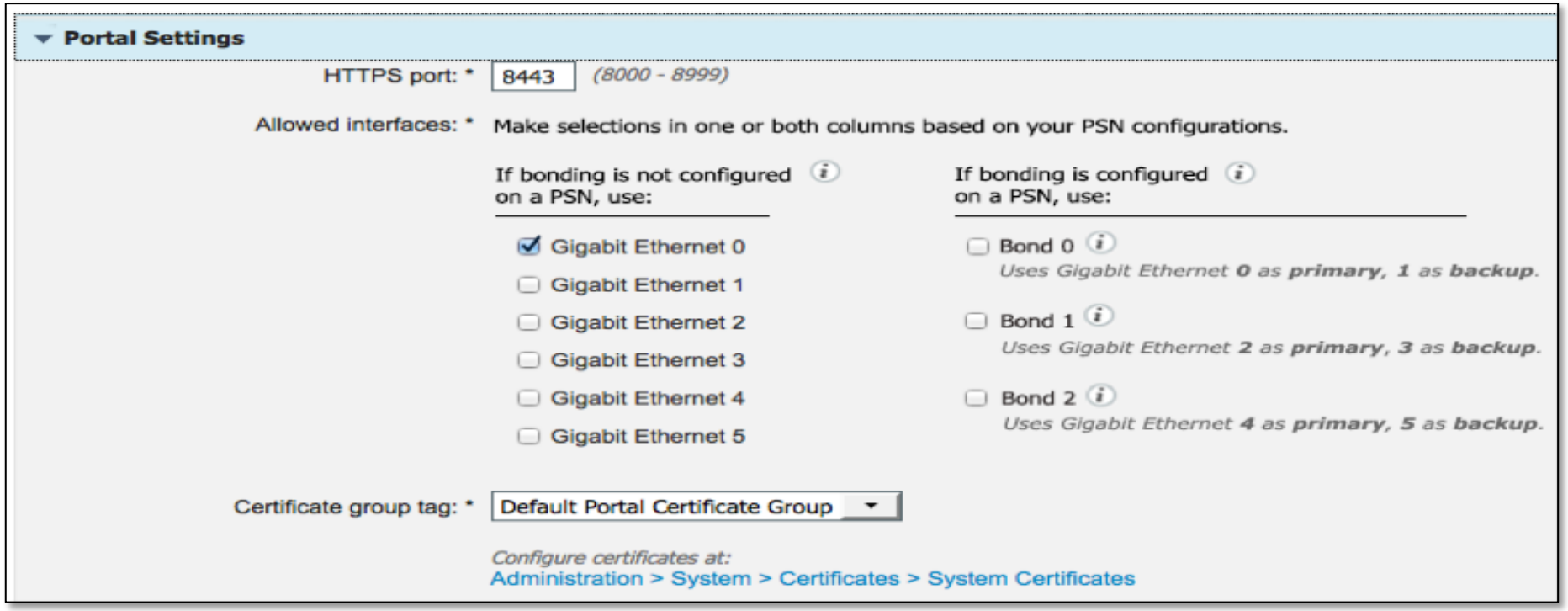
Workcenters > Guest Access Settings > Guest Account Purge Policy

- 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)



NIC Interface Teaming (Bonding)

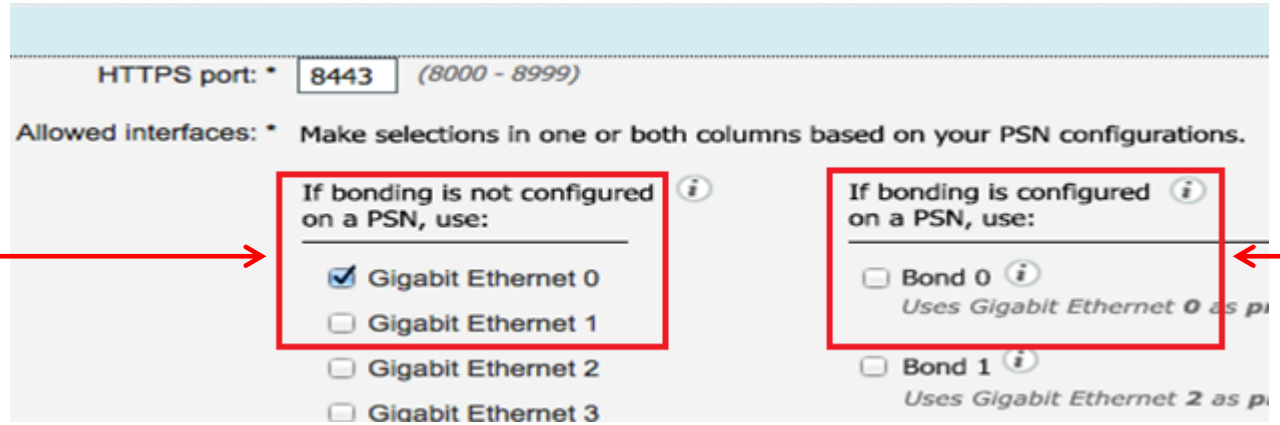
- Used for redundancy, no aggregation of bandwidth
- Simple Primary Backup config
- Each PSN will have its own configuration (via the CLI)
- Portal selects the ports it will use across all PSNs (depending on PSN config)



NIC Interface Teaming (Bonding)

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

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)

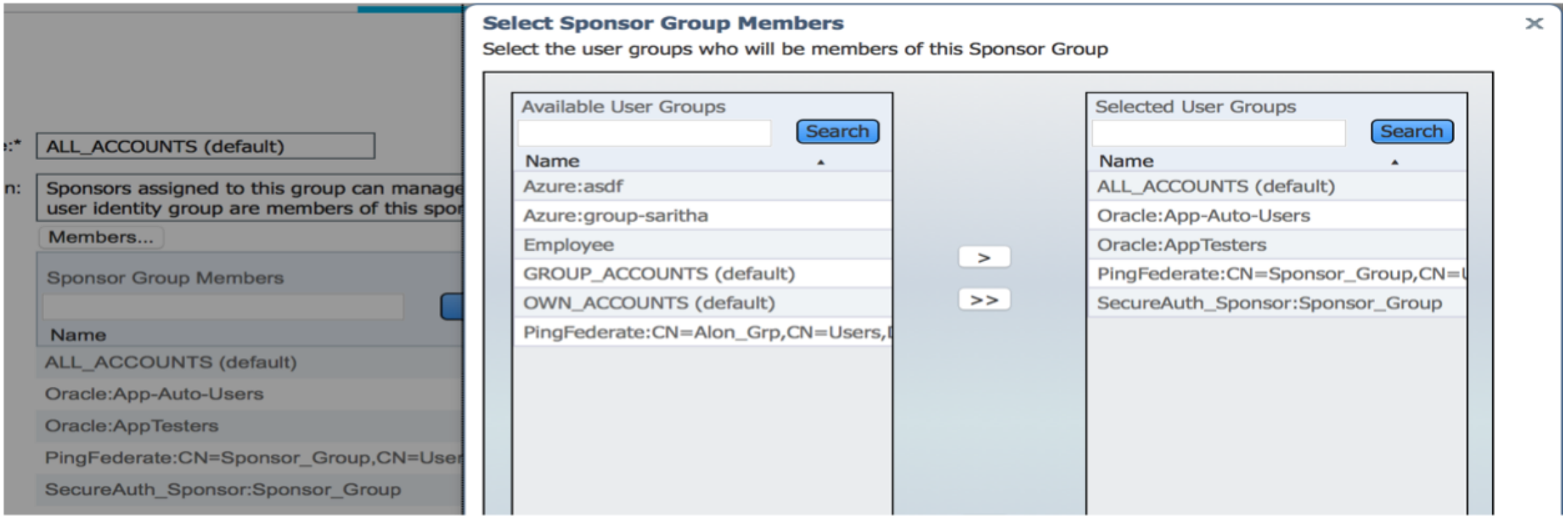
Benefit:

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

Updated SAML Support

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

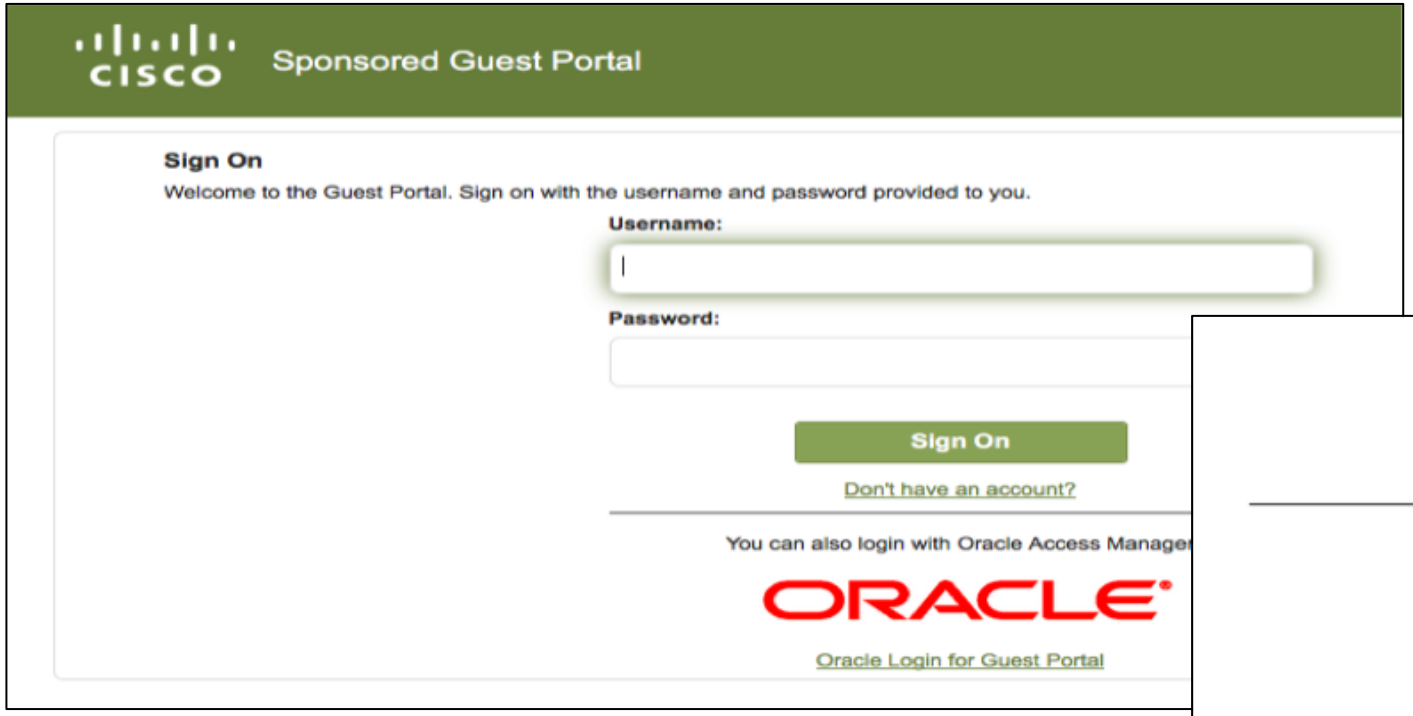
- Integration with external provider requires you to choose the external groups that can access the portal
- ISE now supports receiving group information from the provider (doesn't require ad/ldap)

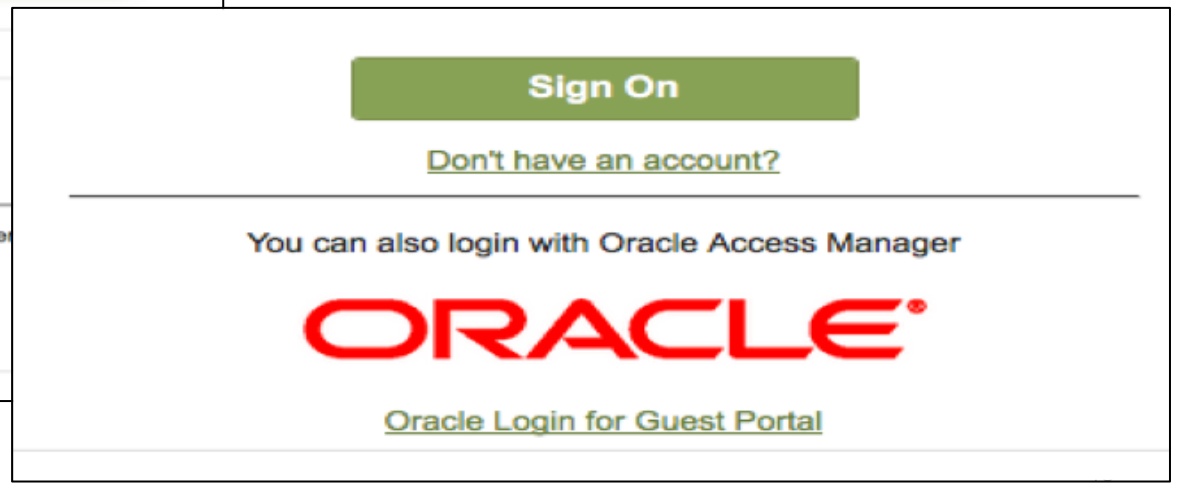


Single portal for credential and SAML SSO login

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



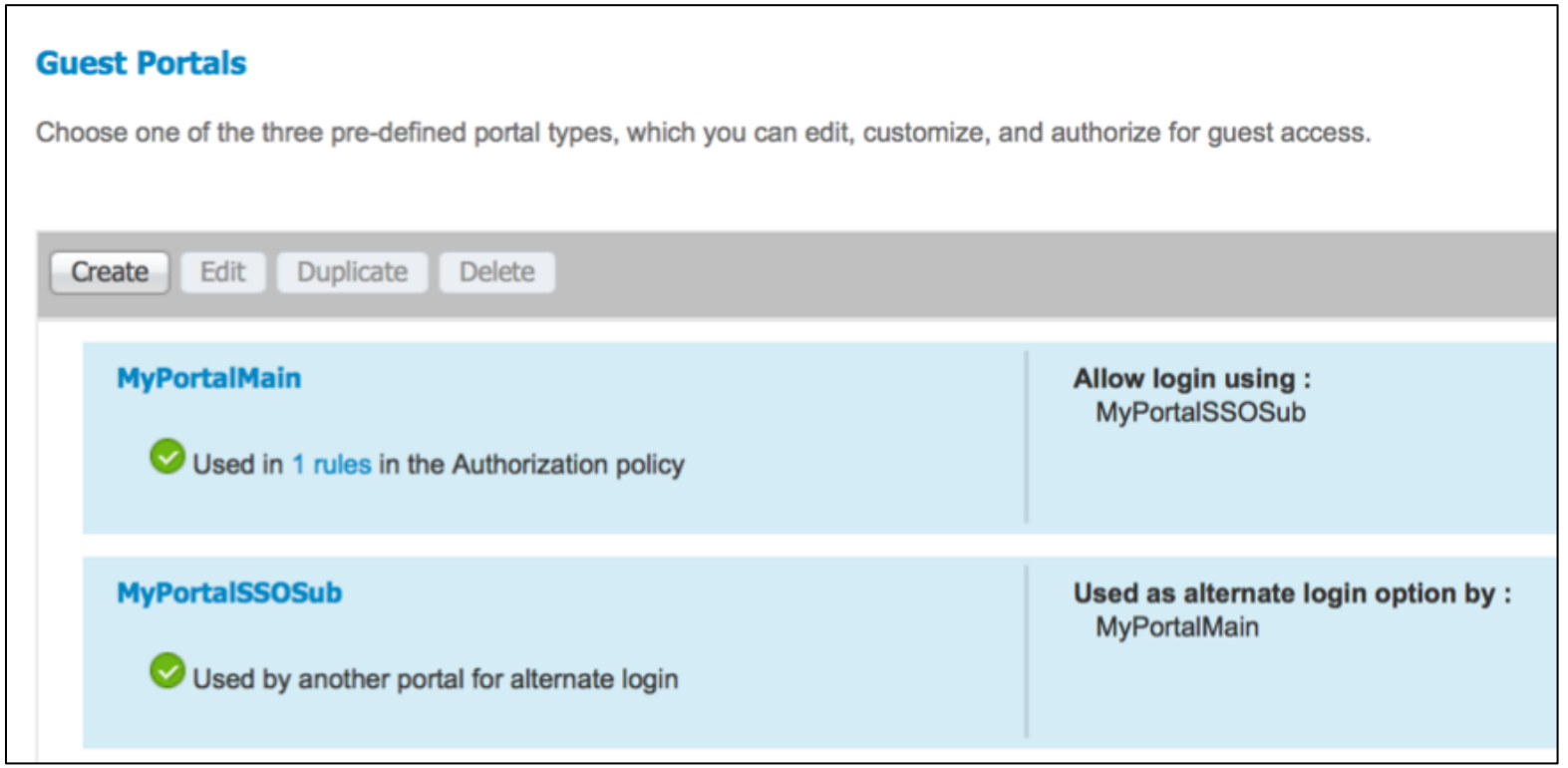


Single portal for credential and SAML SSO login

Work Centers > Guest Access > Configure > Guest Portals

2 portals required:

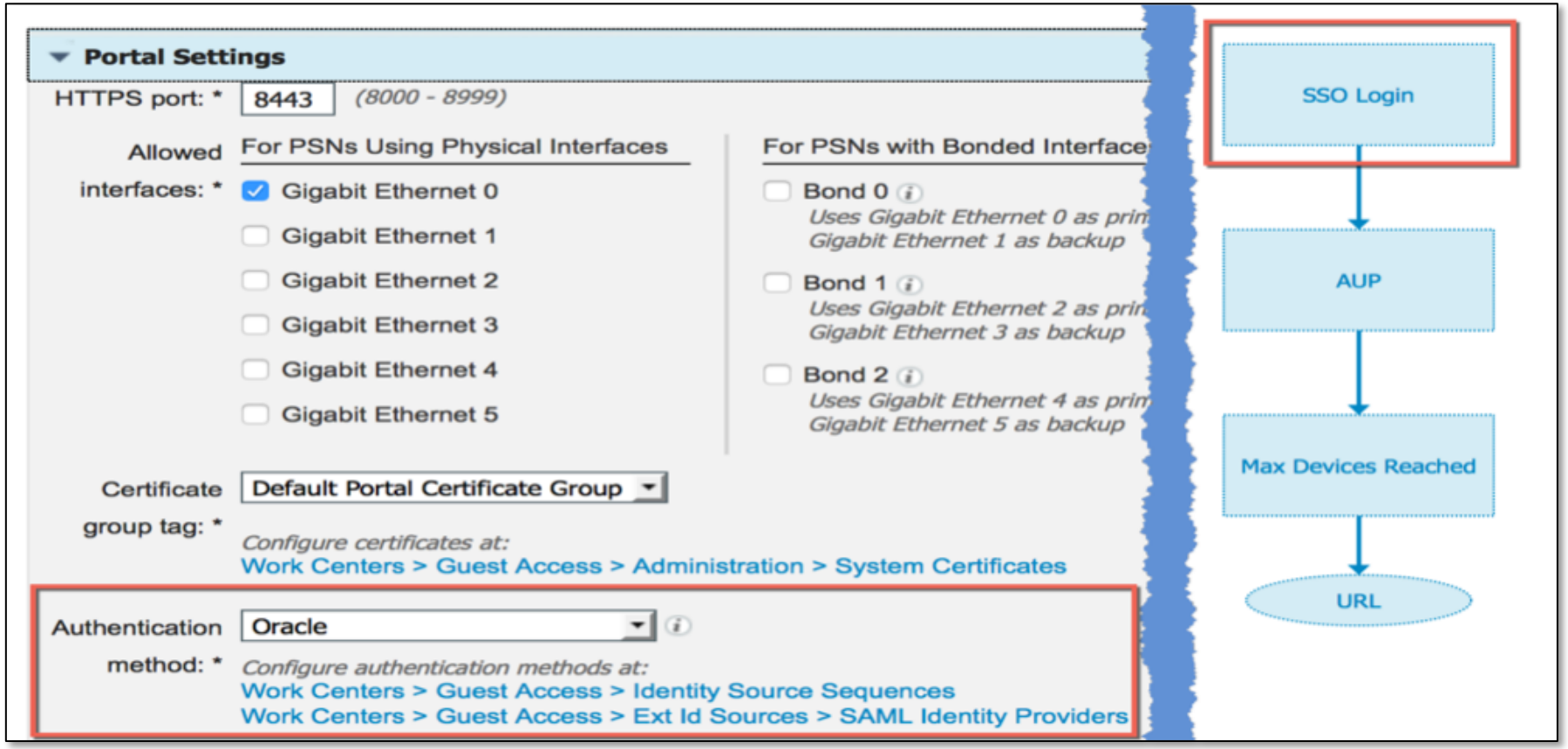
- Main Portal has link to sub-portal for external IDP integration
- Authorization Policy points to the main portal



Single portal for credential and SAML SSO login

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

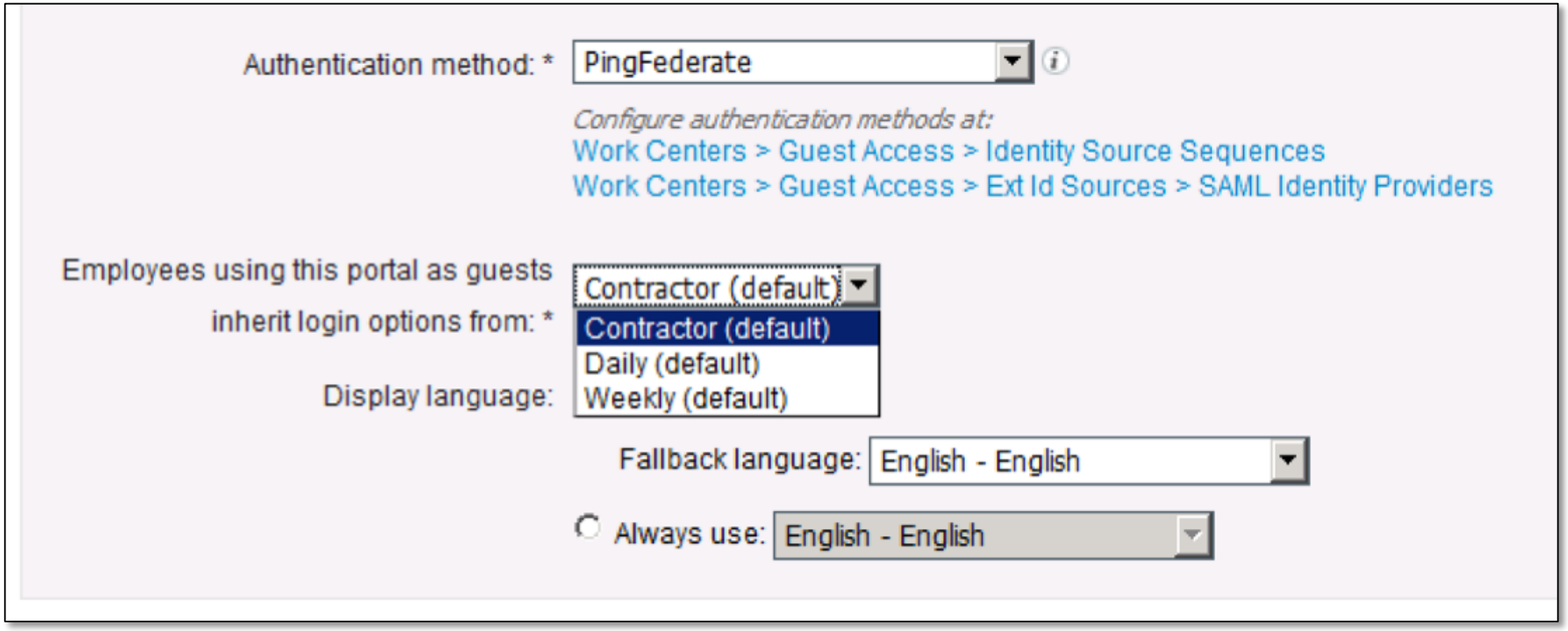
sub-portal – portal page login settings – configured for IDP



Single portal for credential and SAML SSO login

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

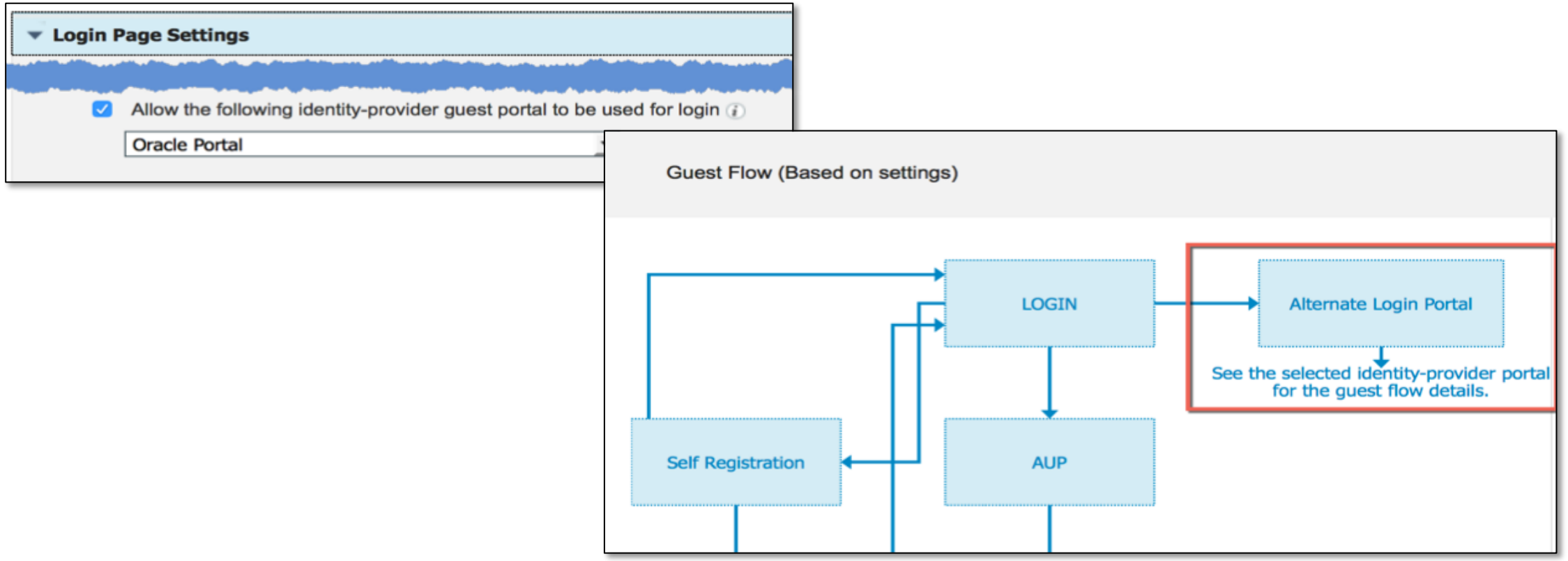
Users using the SAML SSO portal are mapped to: Employees using this portal as guests inherit login options from



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

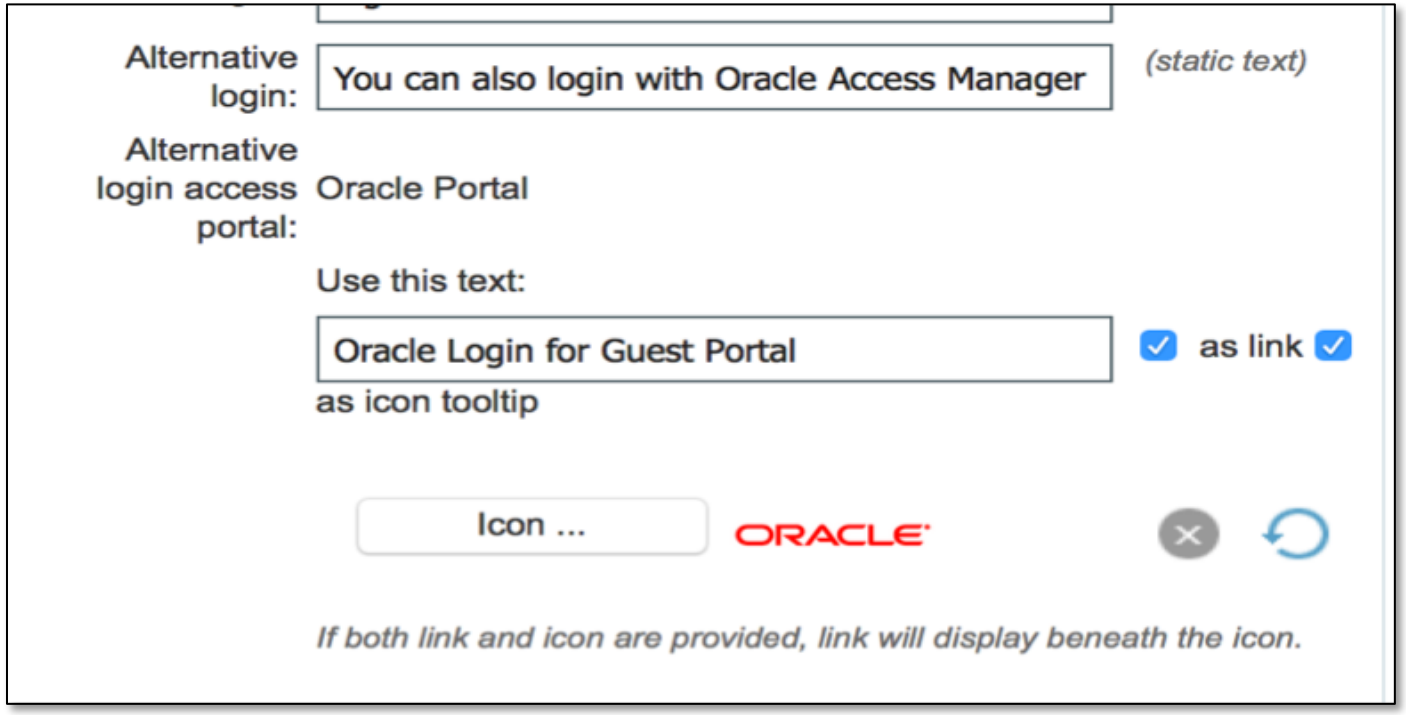


Single portal for credential and SAML SSO login

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

Main Portal Portal page customization for login page:

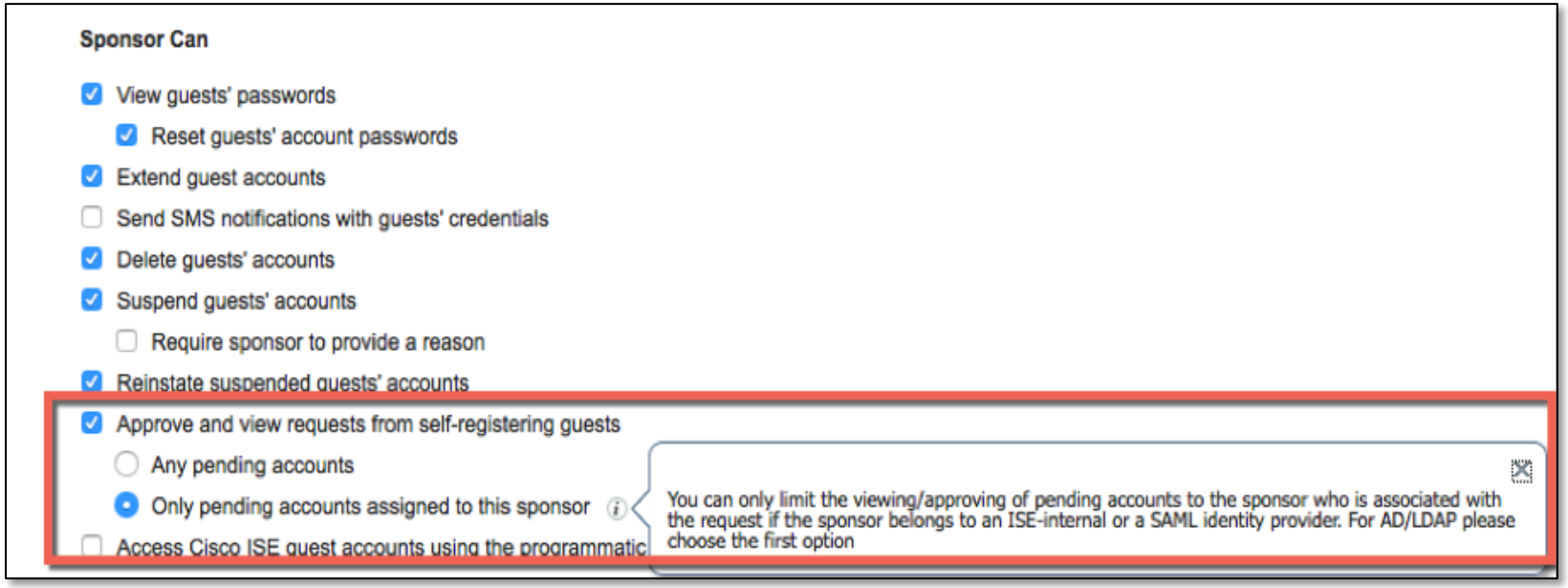
- configures options to display logo & text



Sponsor Approval Pending accounts filtered view

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

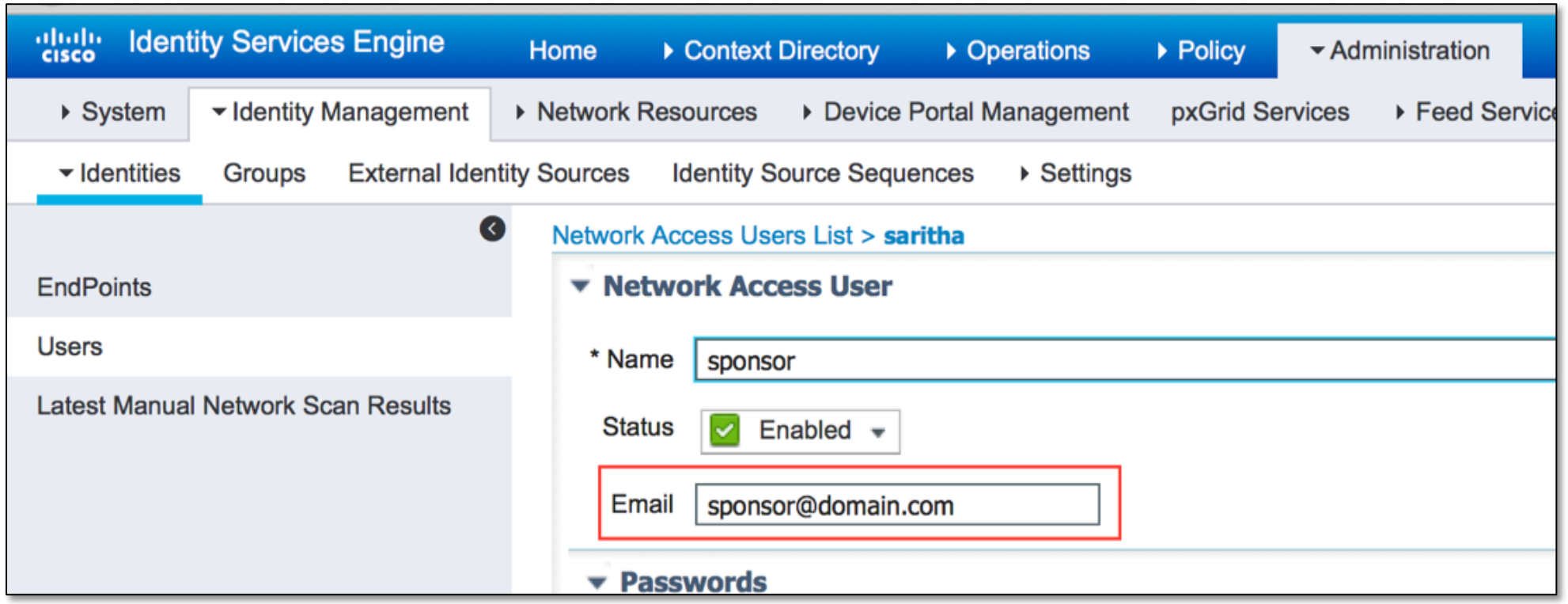
- Filters pending accounts list to only show requests for specific sponsor
- Mapped to person being visited email (sponsor's email address) attribute
- Current support for internal user or SAML IdP accounts (AD/LDAP coming in later release)
- Benefits Sponsor Usability & Addresses organizations' privacy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



Sponsor Approval Pending accounts filtered view

Email address mapping for internal users acting as sponsors

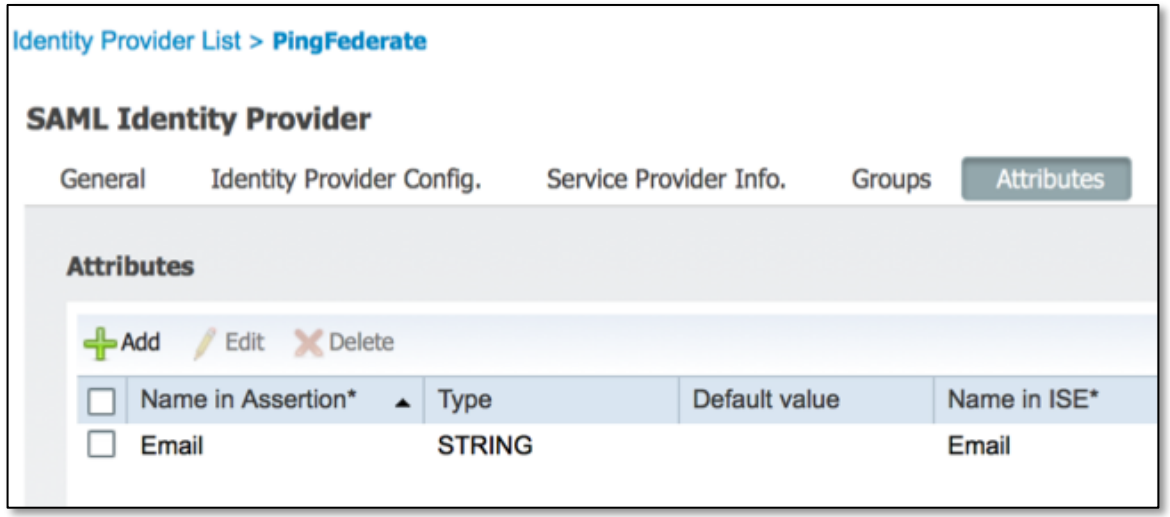
- Administration > Identity Management > Identities > Users

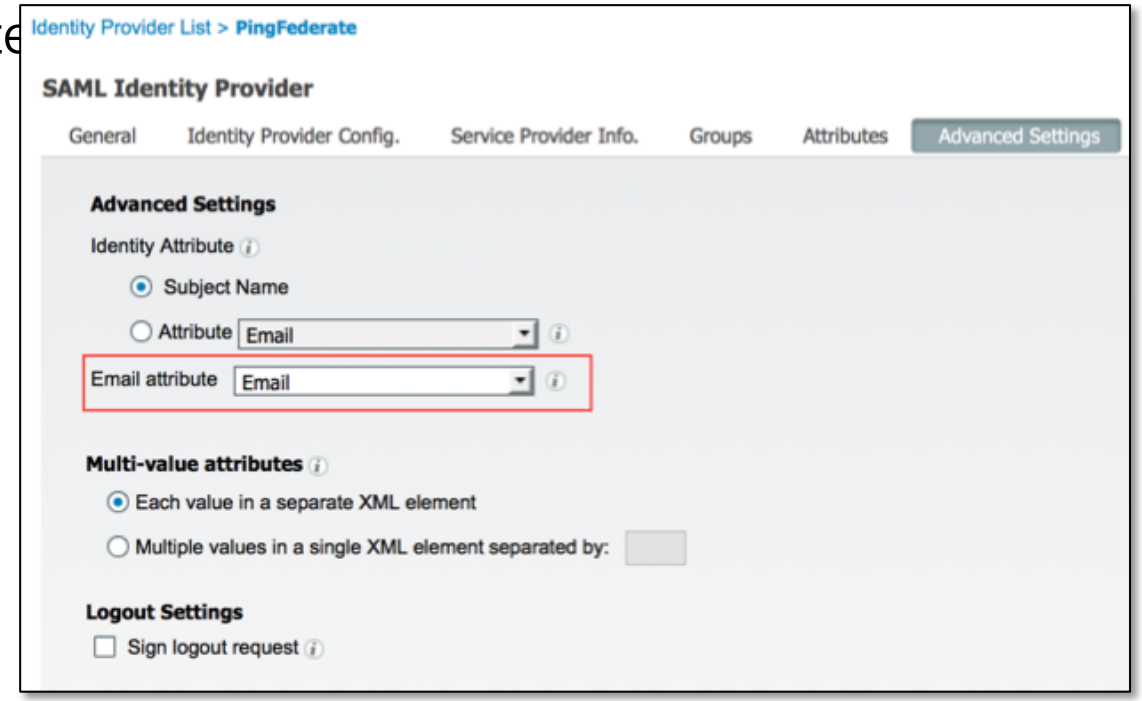


Sponsor Approval Pending accounts filtered view

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

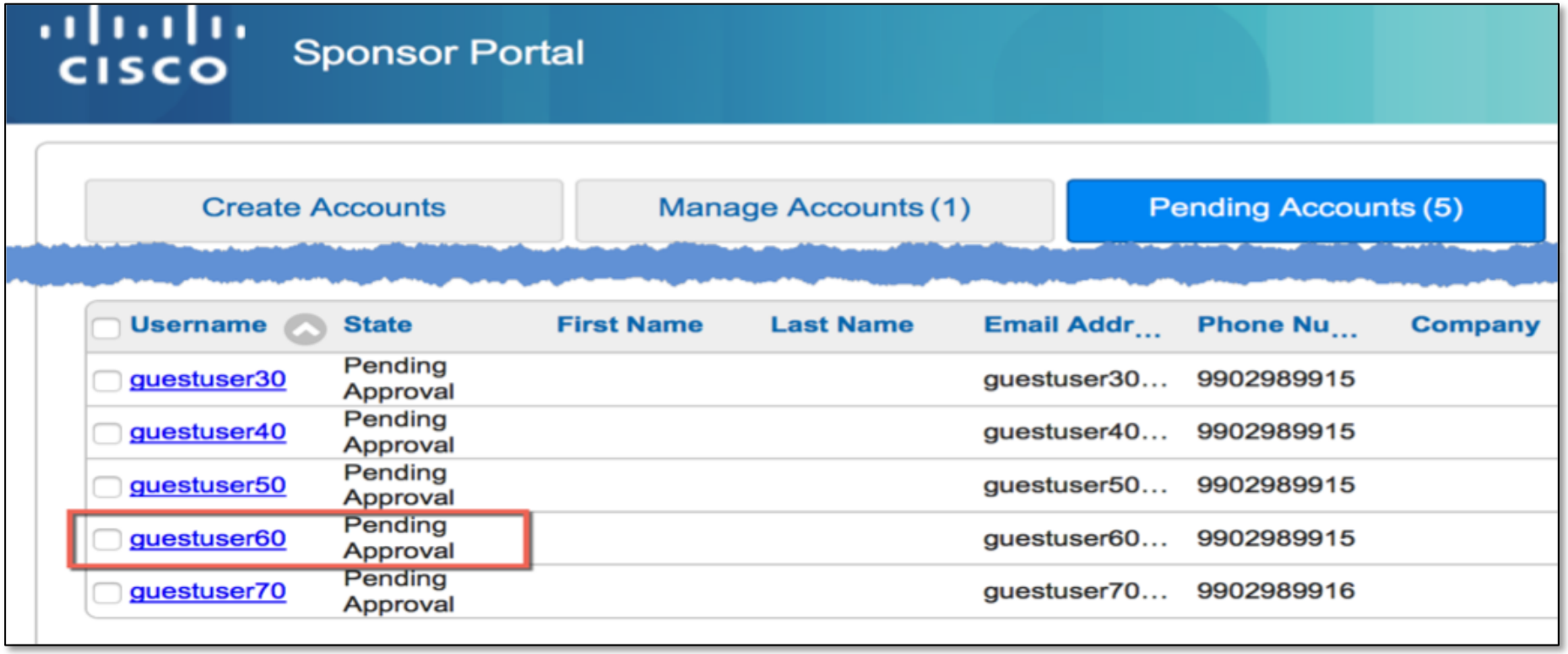




Sponsor Approval Pending accounts filtered view

Unfiltered view

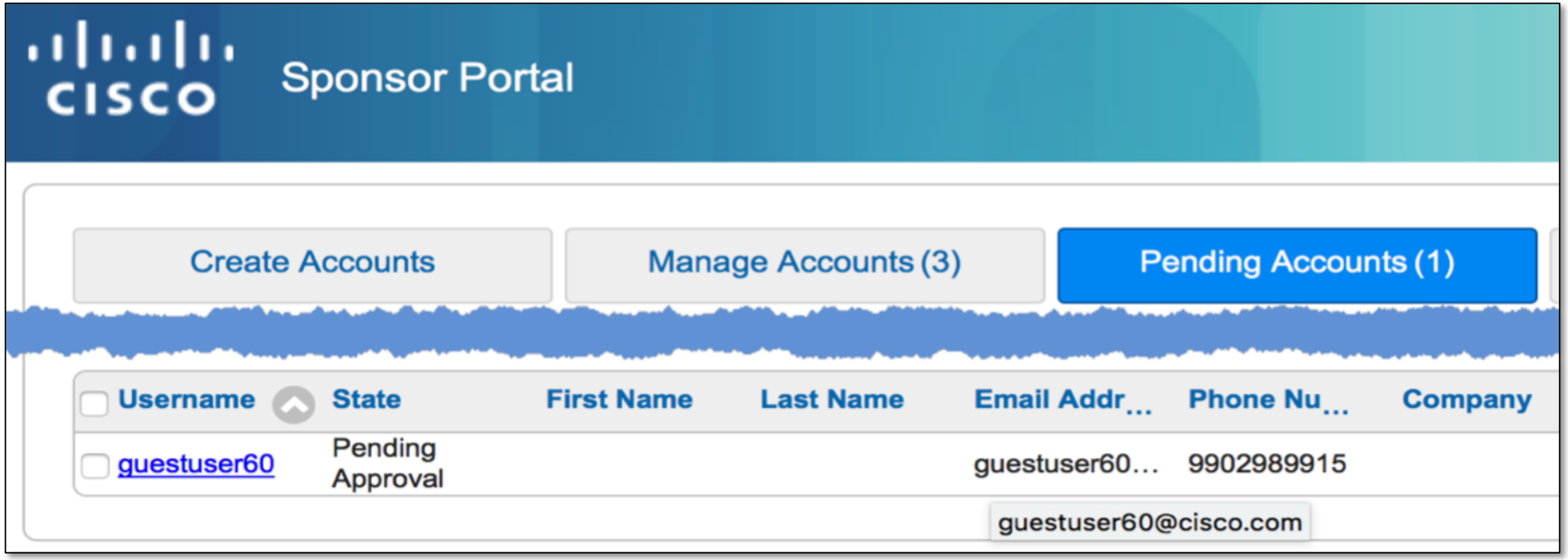
- Filters pending accounts list to only show requests for specific sponsor
- Mapped to person being visited email (sponsor's email address)



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)



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

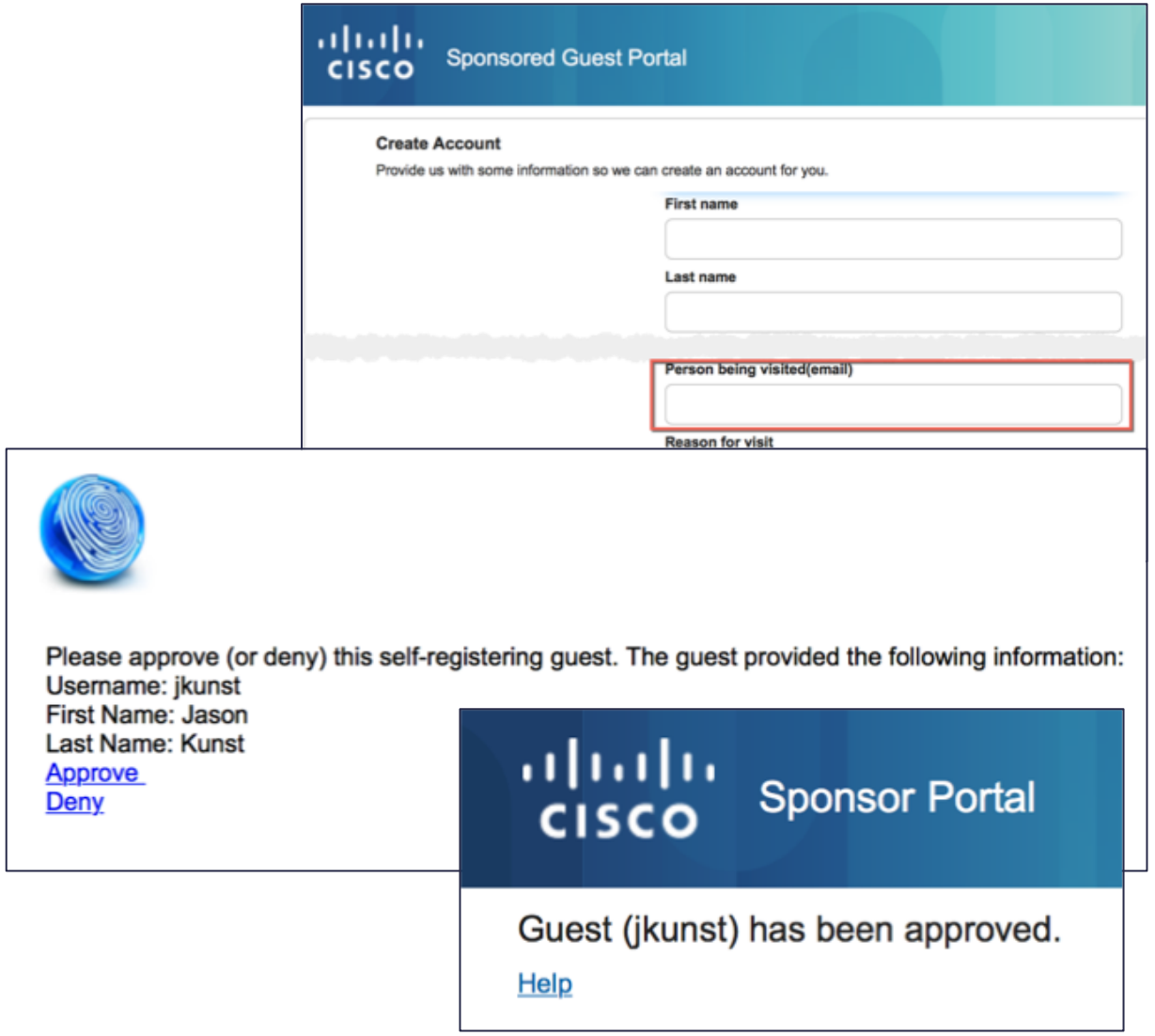
- Bring Back from 1.2
  - Custom Portal Files (replaces need for file remediation)
    - Mini-editor choose custom file
    - Support of video, images, javascript, .JSON
  - Sponsor group LDAP attributes
  - Auto send notification to guest if email address present

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

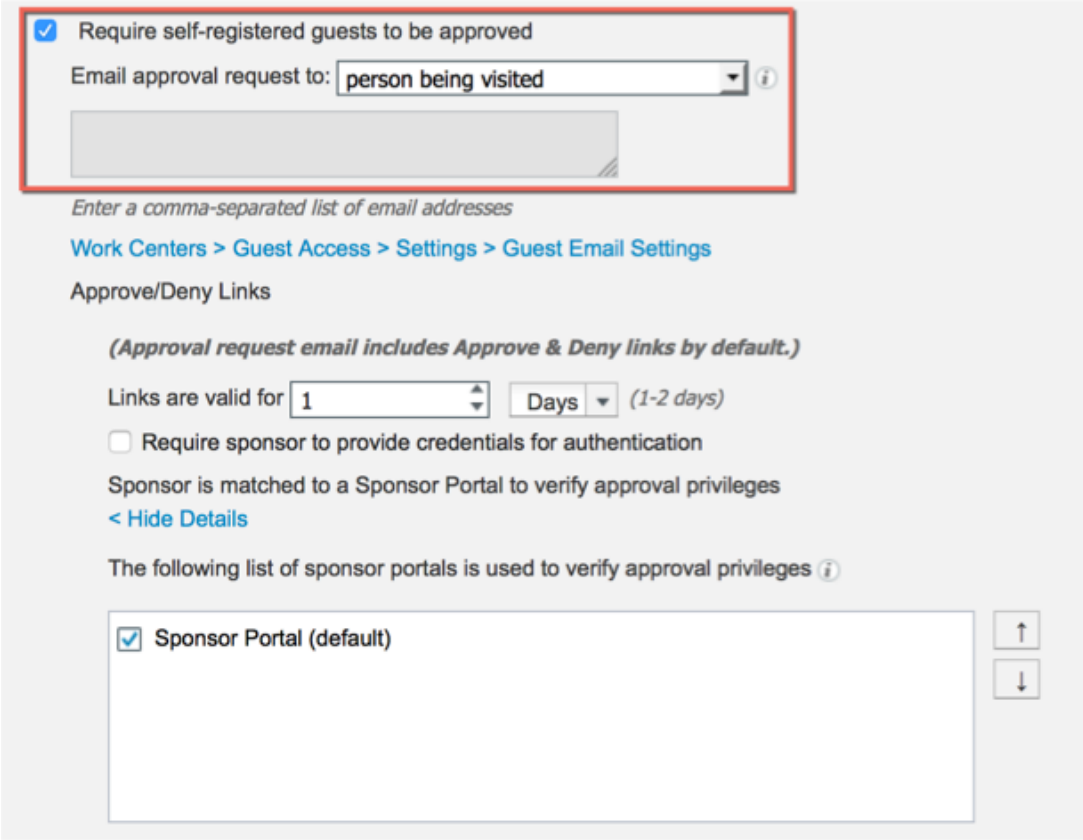
Single click sponsor approval
Overview

- 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



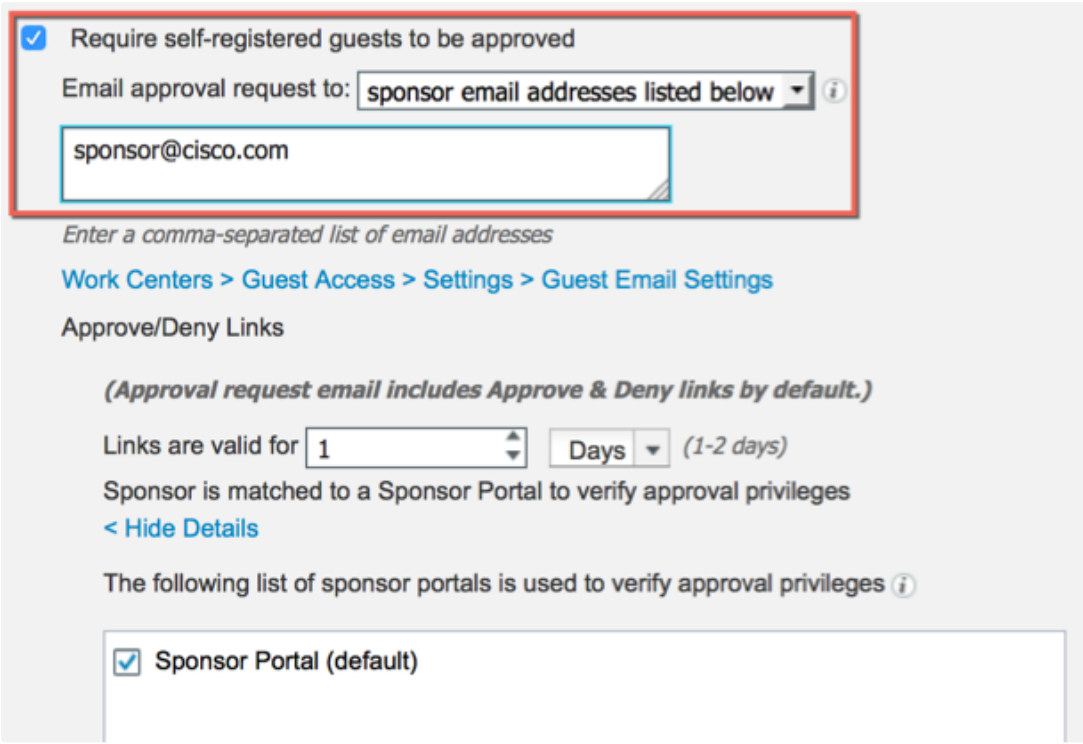
Single click sponsor approval
person being visited

- 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



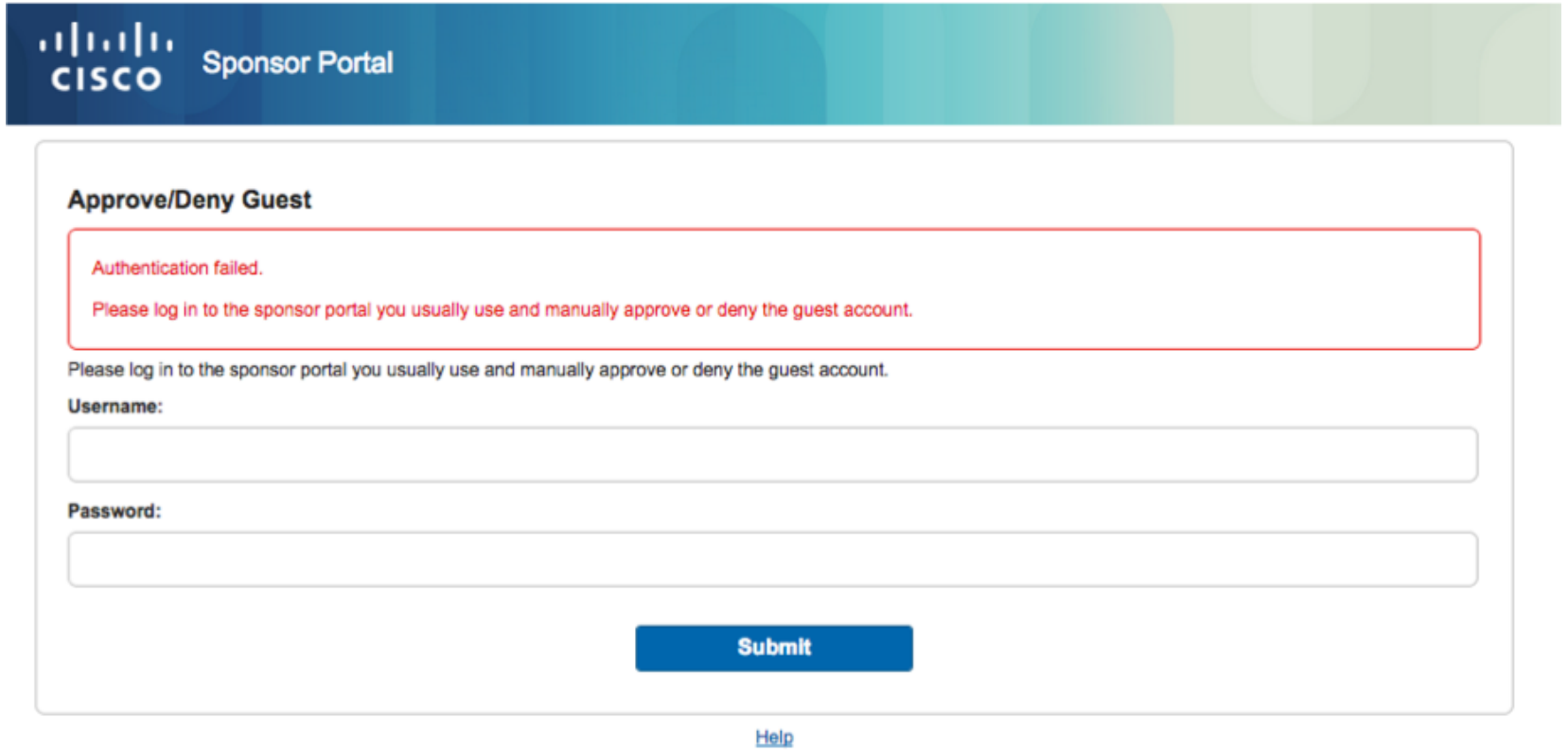
Single click sponsor approval
sponsor email addresses listed below

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

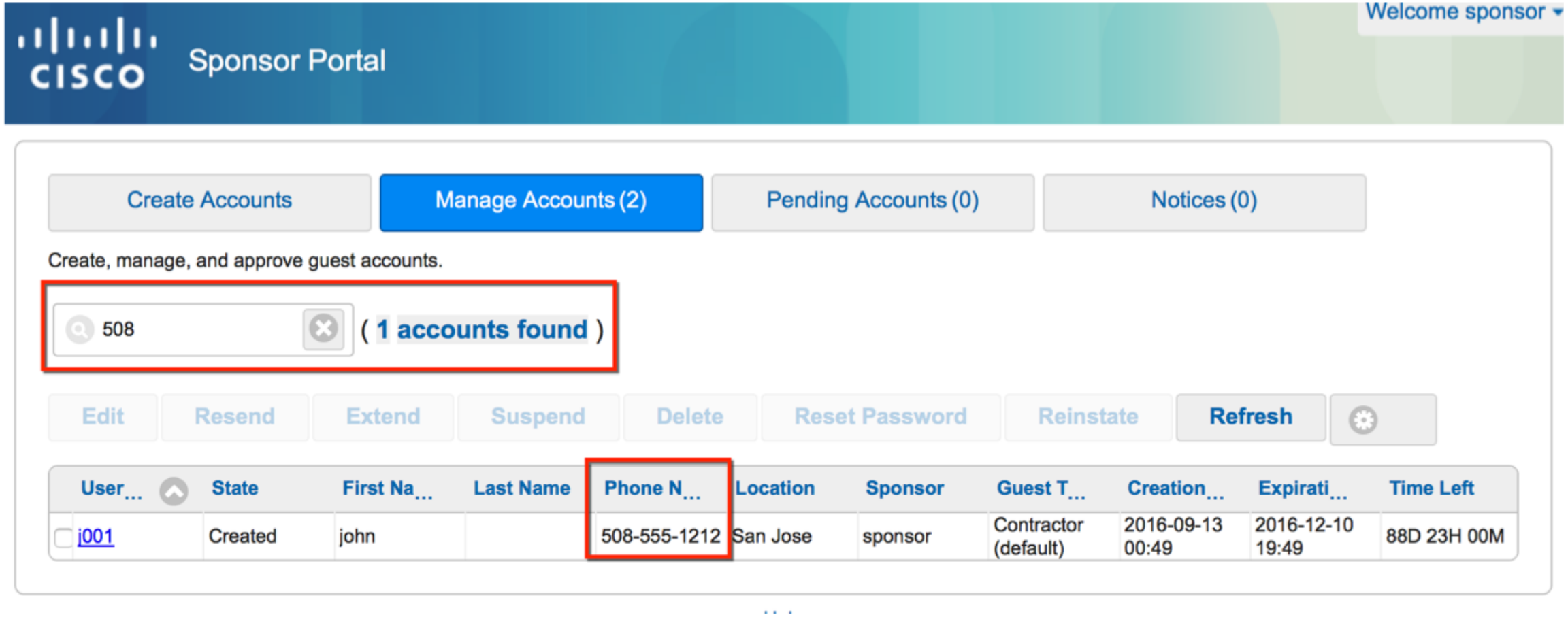


Single click sponsor approval
sponsor email addresses listed below

- Failure message for no matching identity source sequence

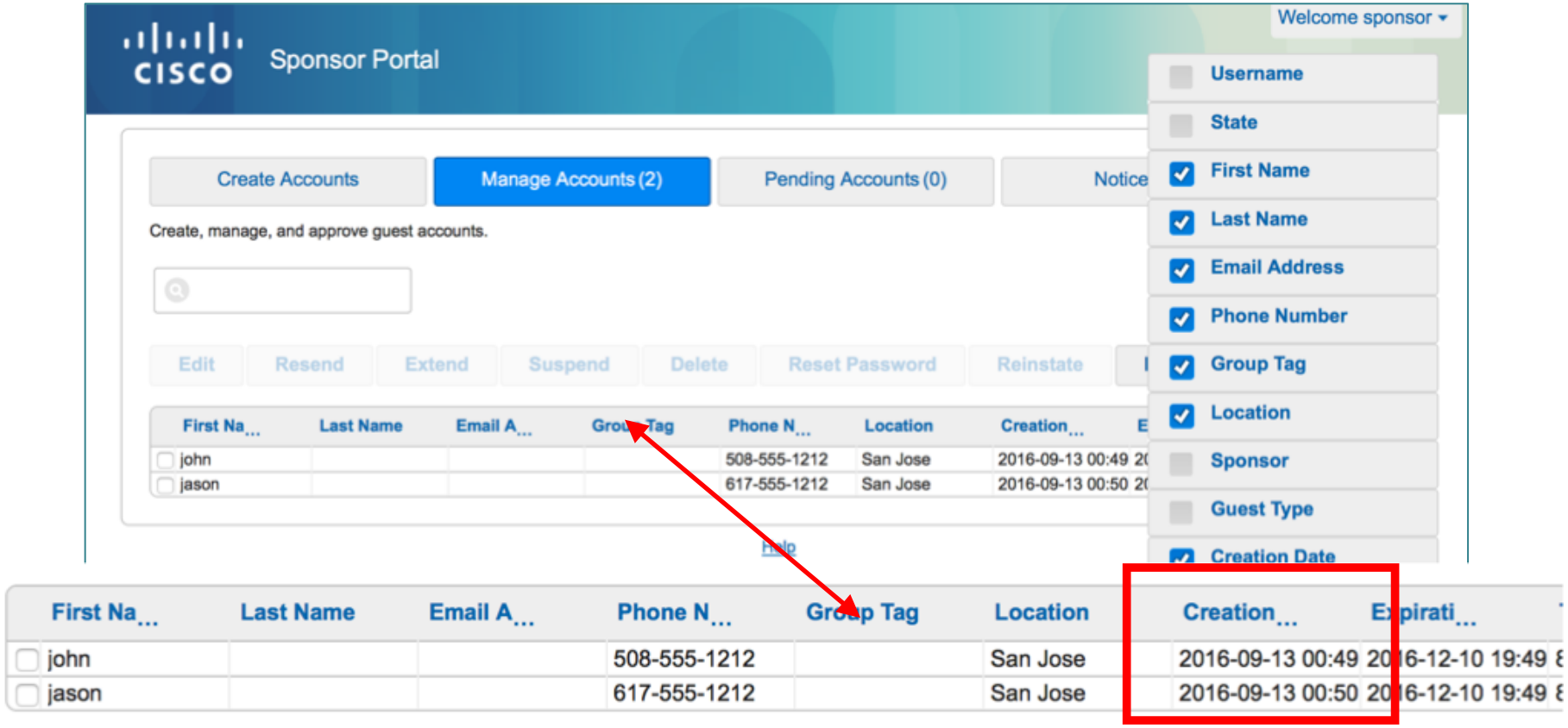


Sponsor Portal Enhancements
Search on phone number!

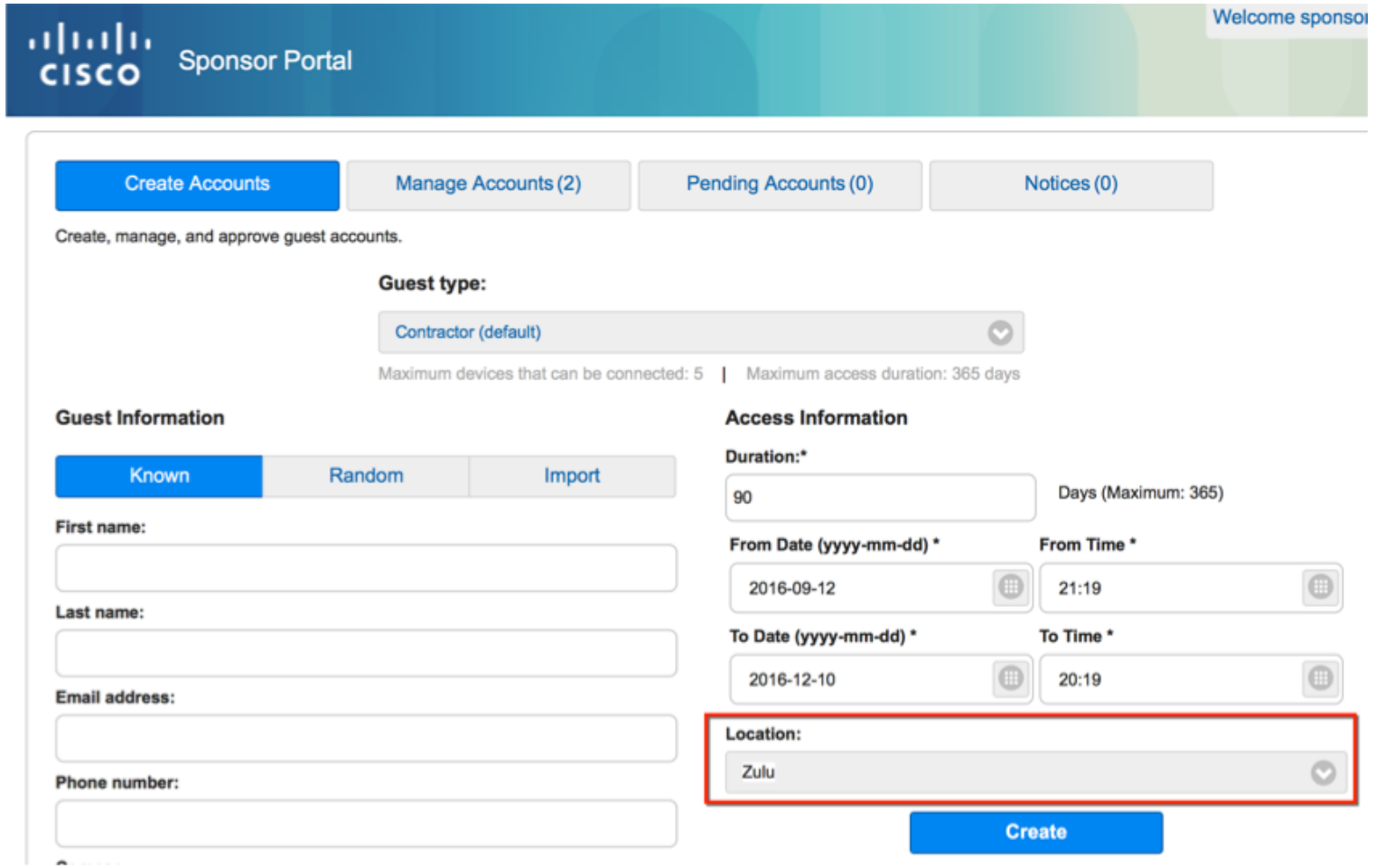


Sponsor Portal Enhancements

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



Sponsor Portal Enhancements
Browser Auto-Timezone

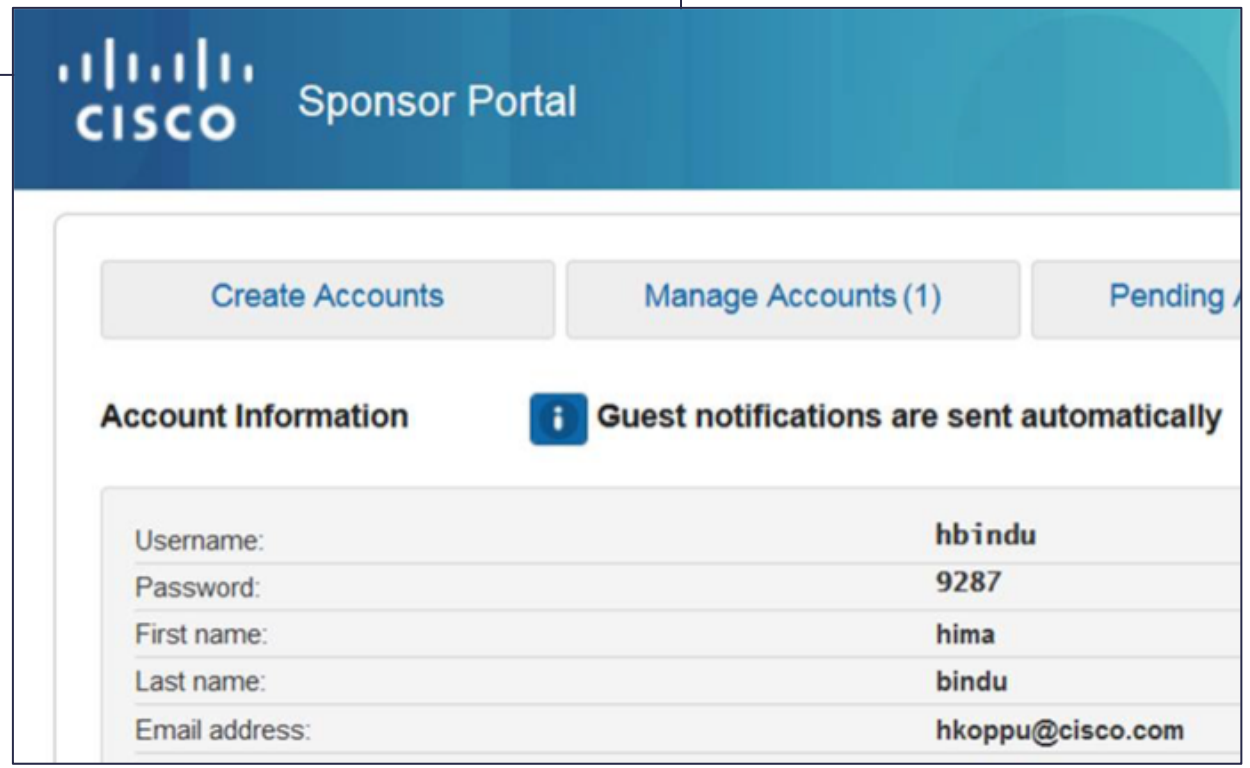


Sponsor Portal Enhancements
Auto notify guest if email address is present

Automatic guest notification:

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

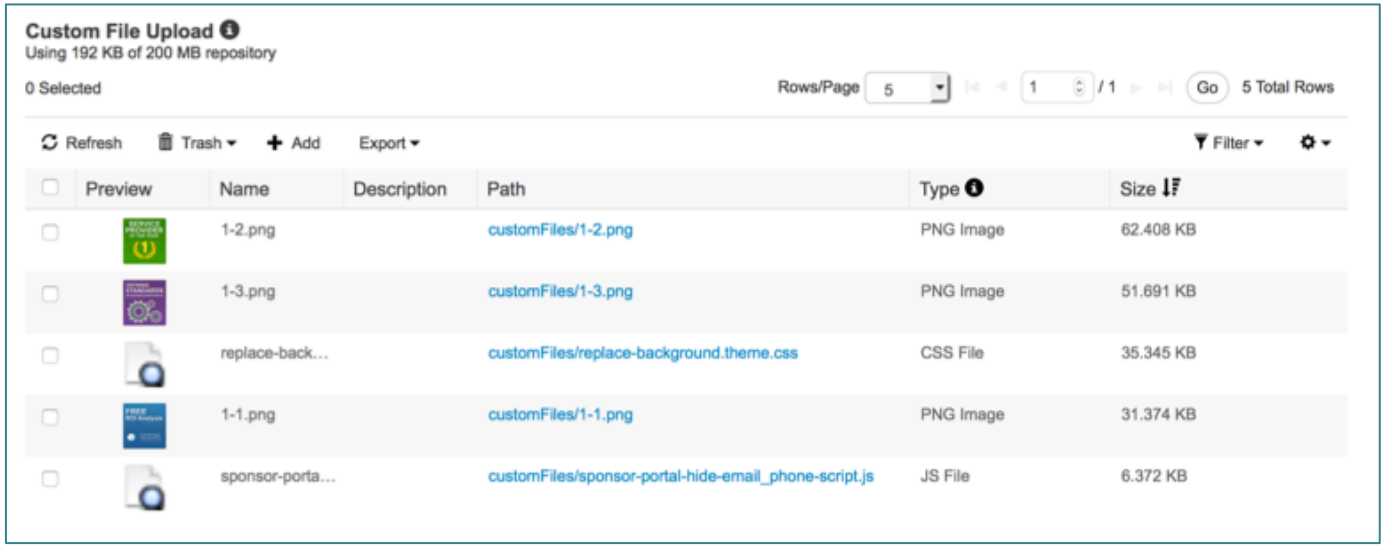
Sponsor Permissions



Custom Portal Files

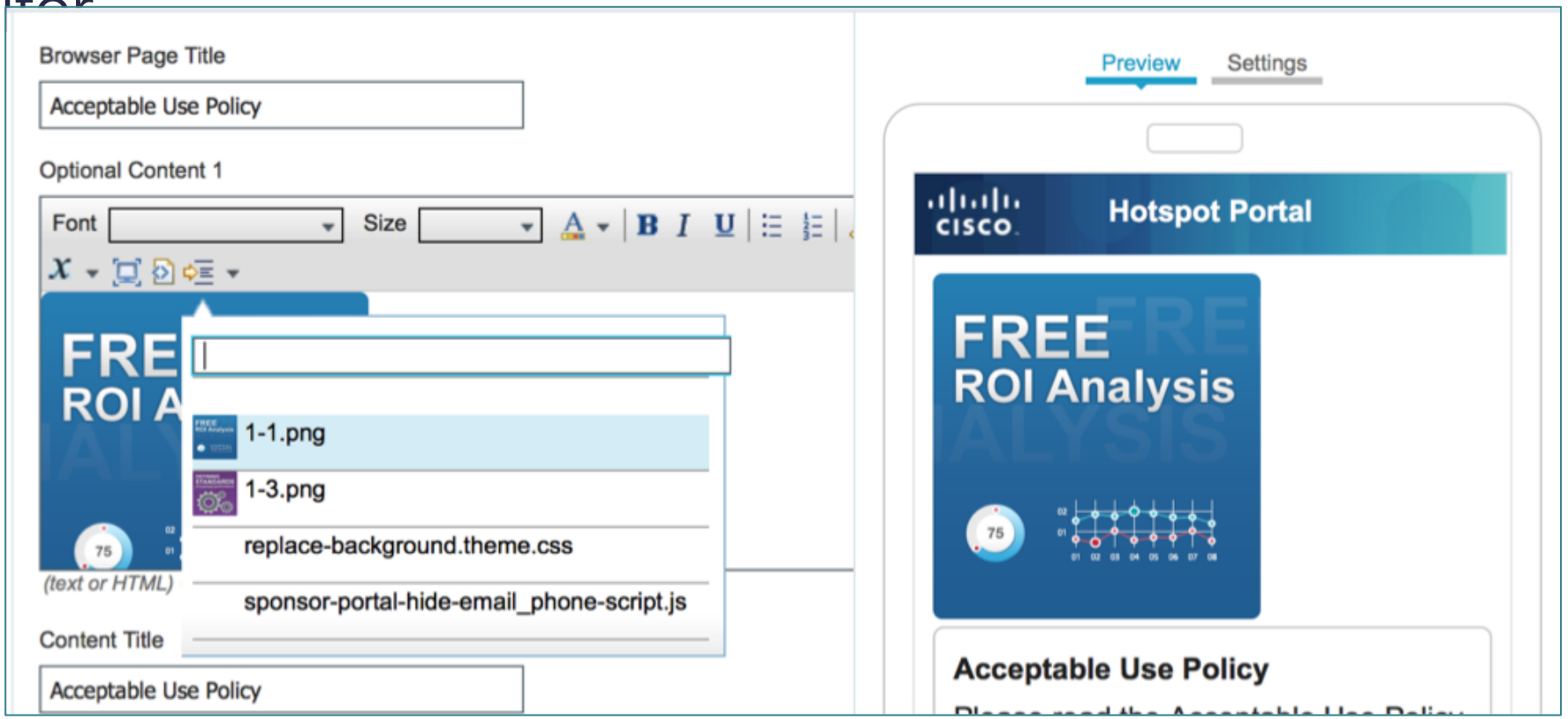
Bring Back from 1.2 – host needed portal files for customization

- .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 Portal Files
mini-editor insert file easiness

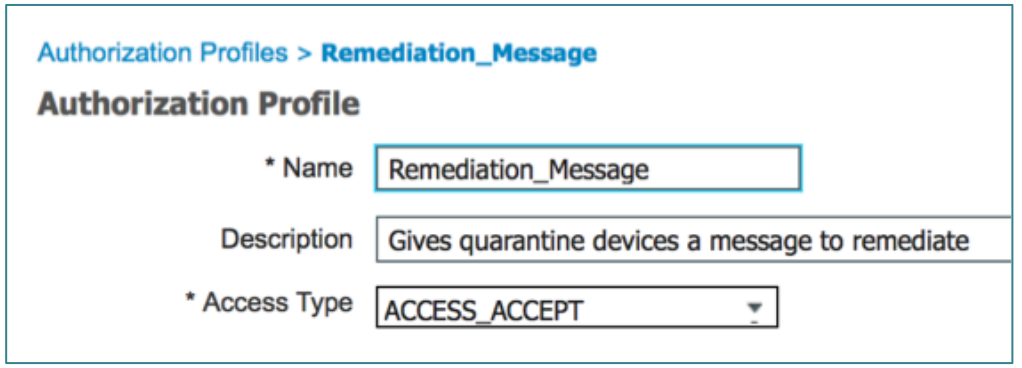
- Direct access to the custom portal files from the mini-editor

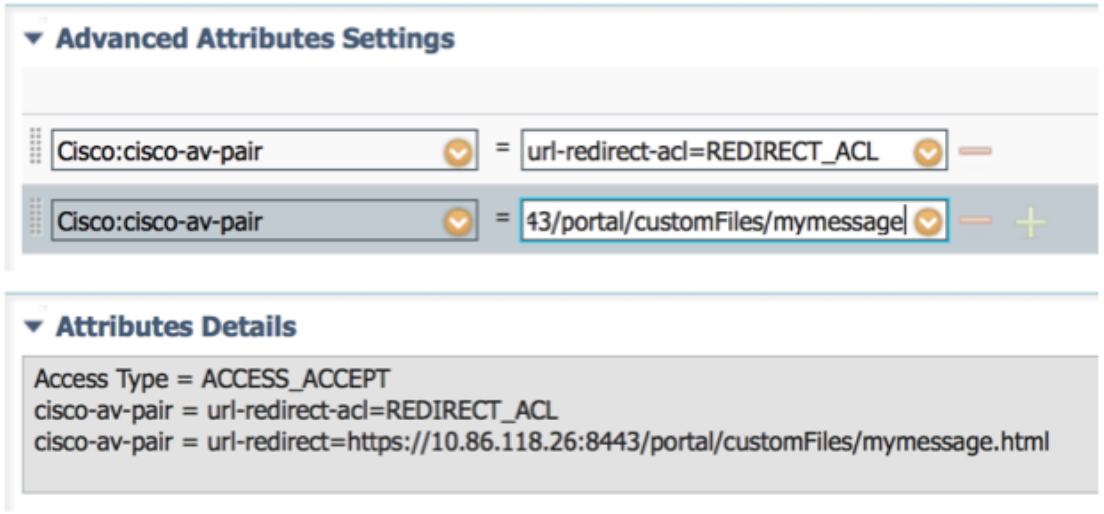


Custom Portal Files

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

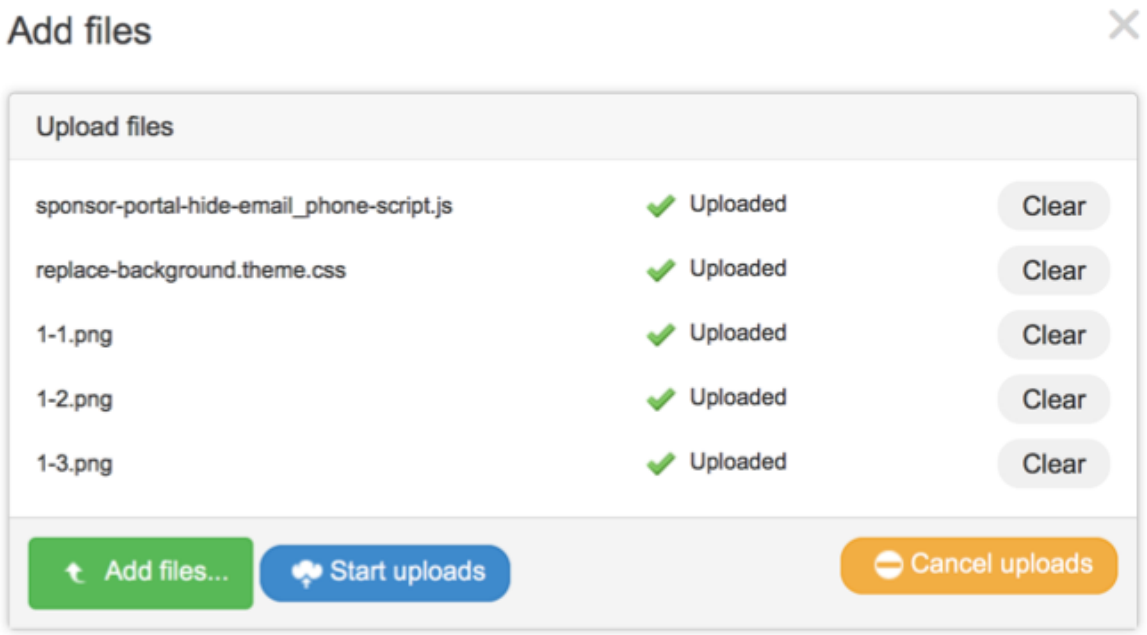
- File path: https://iseip:port/portal/customFiles/mymessage.html
- Replaces hotspot as a message portal https://communities.cisco.com/message/212221#212221



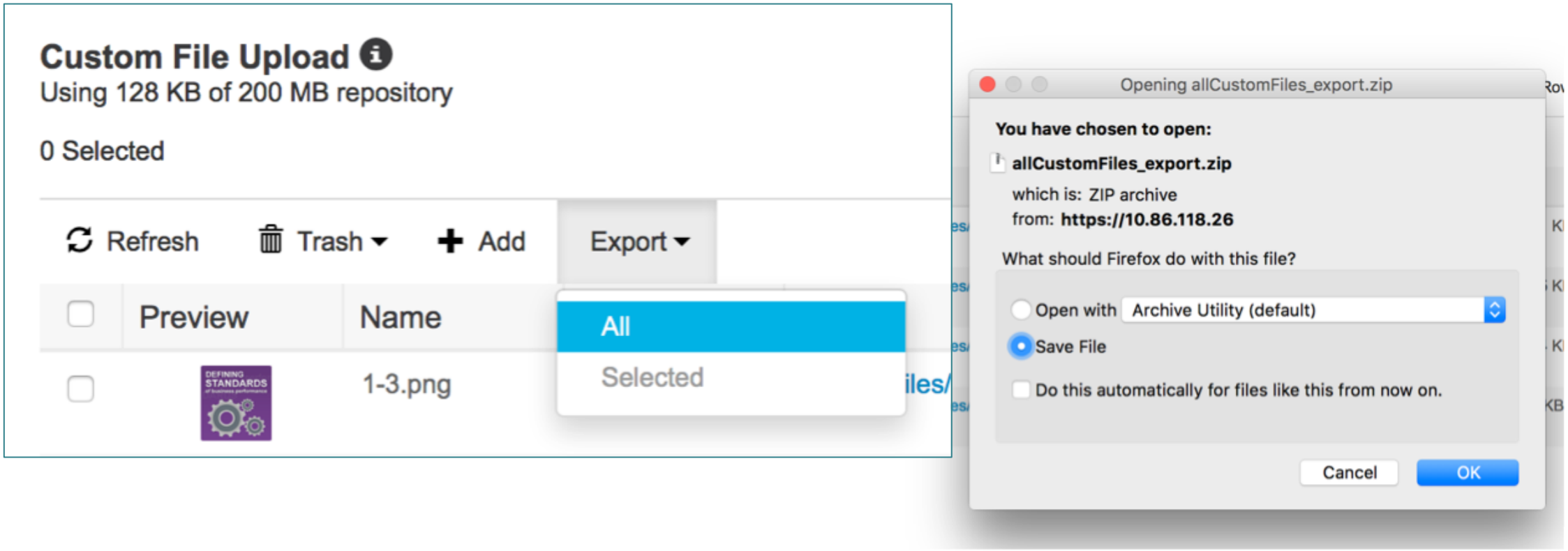


Custom Portal Files
Uploading

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

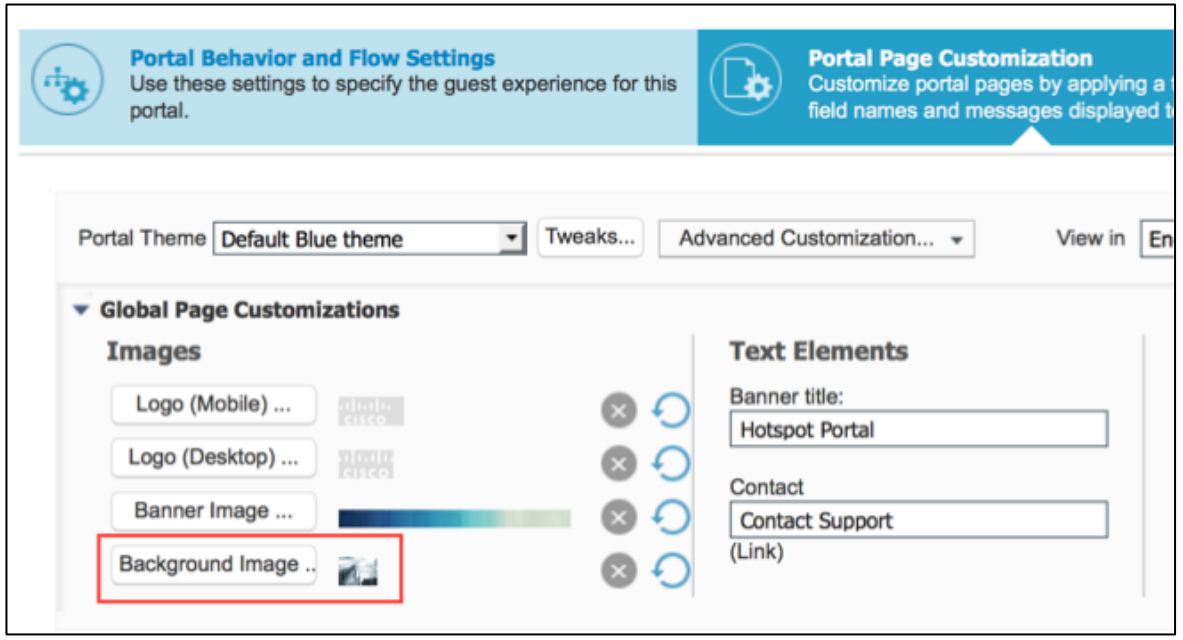


Custom Portal Files
Export all or select files



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



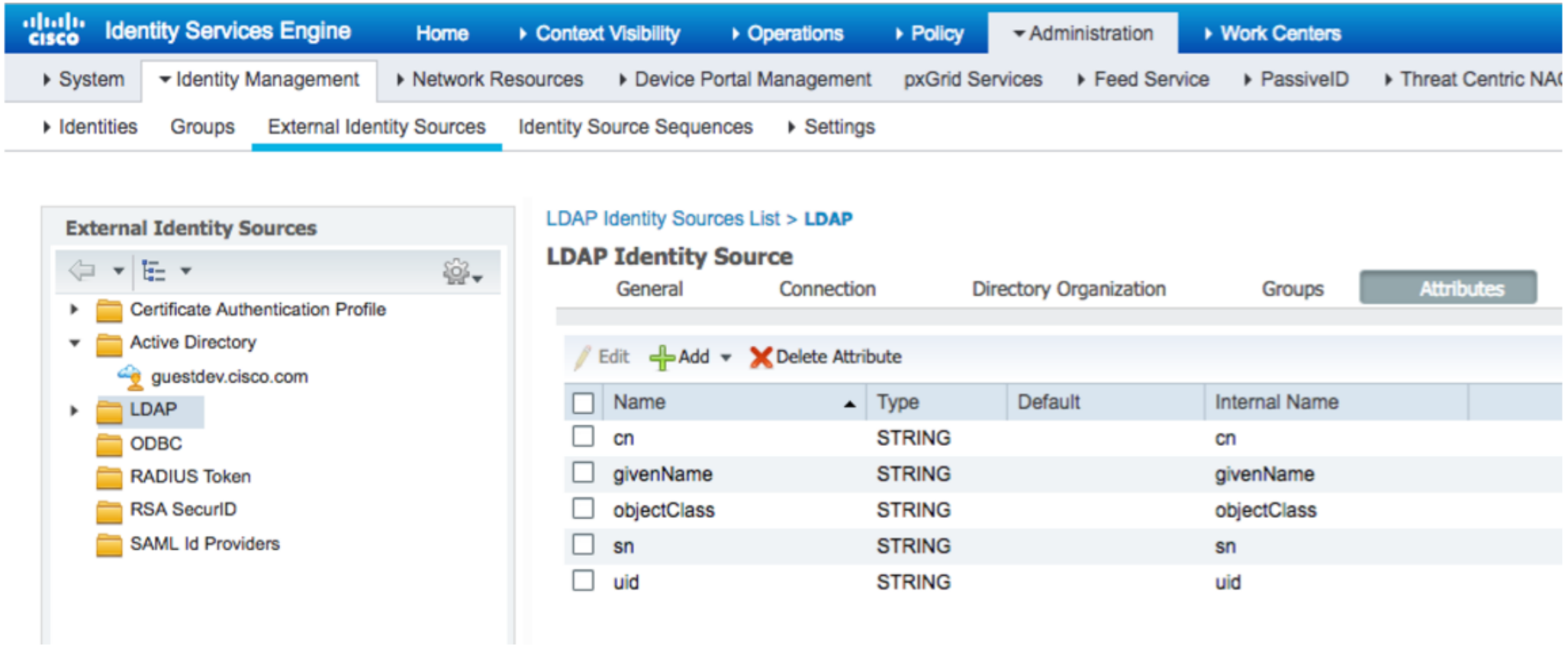
Sponsor Group mapping off attributes
grant access off AD/LDAP, ODBC SAML Attributes

Bring Back From ISE 1.2!

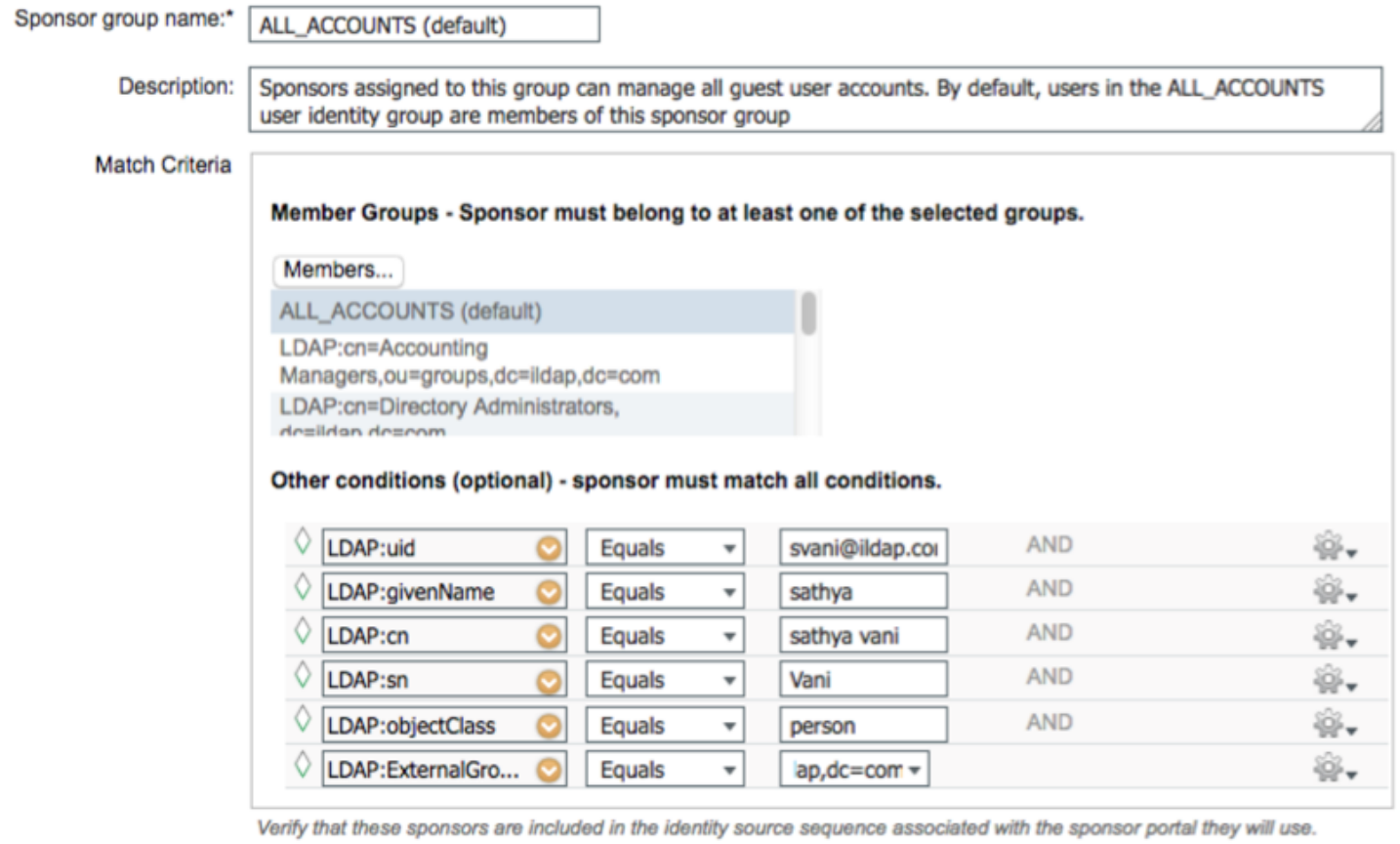
Removes need for workaround (ISE 1.3-2.1)

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

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



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



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)

Create | Edit | Duplicate | Delete

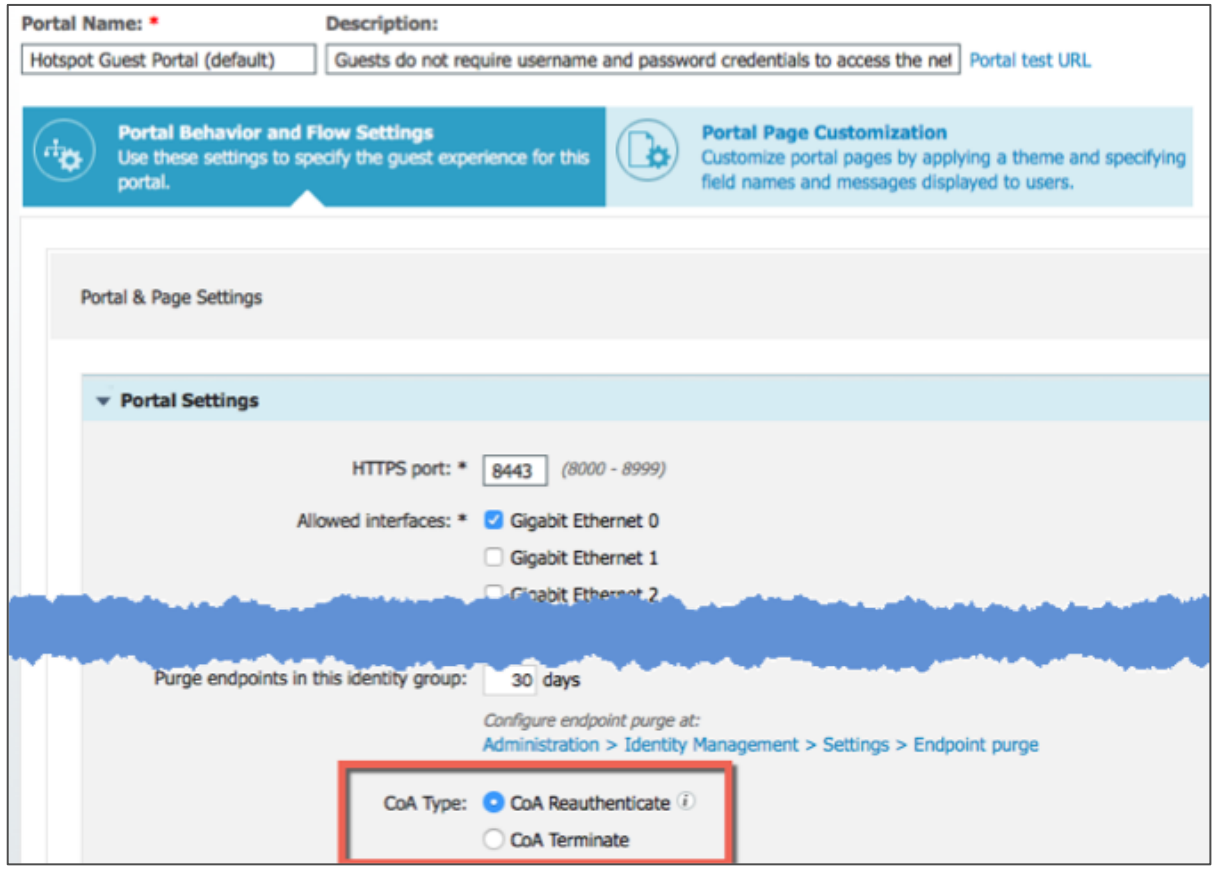
Enabled	Name	Member Groups	Other Conditions
✓	**ALL_ACCOUNTS (default)** Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group	LDAP:cn=Directory Administrators, dc=ildap,dc=com LDAP:cn=PD More	LDAP:uid 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)
- CSCut93791- Introduced in 1.4.1 & ISE 2.1patch1



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