



ISE 1.3-2.0 Sponsor/My Devices Authentication

Using Secondary Attributes to Authorize Sponsors and My Devices Portal Users

Craig Hyps
TME

February 2016

Pre-ISE 1.3 Sponsor Auth

- Prior to ISE 1.3, Sponsor Group Policy used to assign users to Sponsor Groups and assign sponsor privileges
- Multiple conditions supported in addition to group membership.

Sponsor Group Policy

Define the Sponsor Group Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

Status	Policy Name	Identity Groups	Other Conditions	Sponsor Groups
<input checked="" type="checkbox"/>	Manage All Accounts_Admin	If Any	AD1:ExternalGroups EQUALS cts.io...	ManagerSponsorGroup
<input checked="" type="checkbox"/>	Manage Group Accounts_Staff	If Any	AD1:ExternalGroups EQUALS cts.io...	LobbyAmbassador
<input checked="" type="checkbox"/>	Manage Own Accounts_Employ	If Any	AD1:ExternalGroups EQUALS cts.io...	EmployeeSponsorGroup

1.3+ Sponsor/My Devices Auth

- Starting in ISE 1.3, Sponsor Group and My Devices configuration is greatly simplified but limits assignment to group membership only.

Cisco Identity Services Engine

Home Operations | Policy | Guest Access |

Configure Manage Accounts Settings

Sponsor Group

☐ Disable Sponsor Group

Sponsor group name:*

Description:

Sponsor Group Members

AD1:cts.local/Users/employees

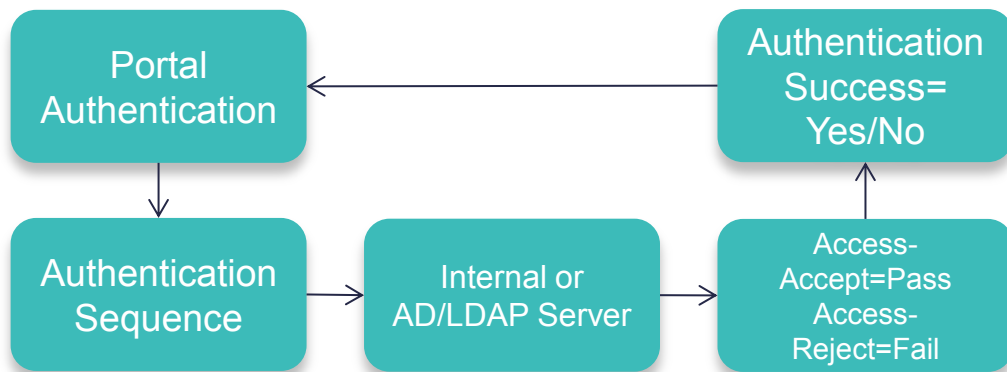
OWN_ACCOUNTS (default)

Challenge #1: How Limit Sponsor/My Devices Access Based on Secondary Attributes?

- Solution: Configure ISE as an Authentication Source for Sponsors/My Devices Portals and define custom conditions that will either permit or deny access.
- Configuration Steps:
 - Define Local ISE PSN(s) as RADIUS Token Server
 - Add ISE RADIUS Server to Sponsor/My Devices Auth Sequence
 - Add ISE PSN(s) as RADIUS Clients
 - Add Authorization Policy Rules for Sponsor/My Devices Auth

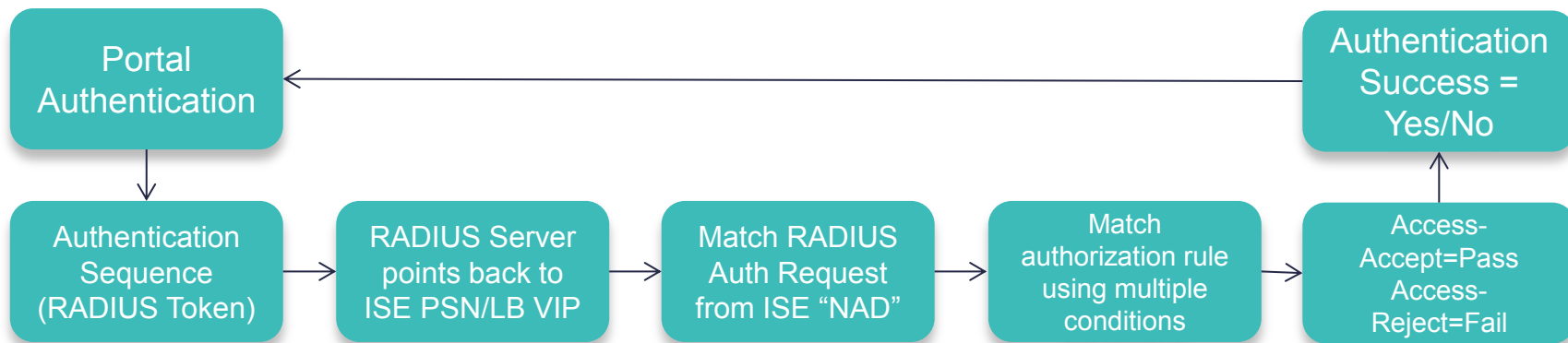
Traditional Sponsor/My Devices Portal Auth Flow

- ISE 1.3–2.1 logic is to determine Pass/Fail (Access-Accept / Access-Reject) response based on Authentication only
- Sponsor/My Devices Portal also includes Authorization based on group membership



Modified Sponsor/My Devices Portal Auth Flow

- Define local ISE as an external RADIUS Token Server to perform a separate Authorization policy lookup before responding with Pass/Fail
- Pass/Fail response based on multiple AuthZ conditions, not just AuthC.



Define Local ISE PSN(s) as RADIUS Token Server

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes links for Home, Operations, Policy, Guest Access, and Administration. Below this, a secondary navigation bar shows System, Identity Management (selected), Network Resources, Device Portal Management, pxGrid Services, Feed Service, and pxGrid Identity. The main content area is divided into tabs: Identities, Groups, External Identity Sources (selected), Identity Source Sequences, and Settings.

On the left, the 'External Identity Sources' sidebar lists various authentication methods: Certificate Authentication Profile, Active Directory (with AD1 sub-item), LDAP, **RADIUS Token** (highlighted with a red box), and RSA SecurID.

The main panel shows the 'RADIUS Token Identity Sources' configuration page, with tabs for General, Connection (selected), Authentication, and Authorization. The 'Server Connection' section includes options for Safeword Server, Enable Secondary Server, and a radio button selection for 'Always Access Primary Server First' (selected) and 'Failback to Primary Server after' (set to 5 minutes). The 'Primary Server' section contains fields for Host IP (10.1.100.2, highlighted with a red box), Shared Secret (masked with dots and a 'Show' button), Authentication Port (1812), Server Timeout (5 seconds), and Connection Attempts (3). The 'Secondary Server' section has corresponding empty fields for Host IP, Shared Secret, Authentication Port, Server Timeout, and Connection Attempts.

Add ISE RADIUS Server to Sponsor/My Devices Auth Seq.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes the Cisco logo, the text 'Identity Services Engine', and a menu with 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, a secondary navigation bar shows 'System', 'Identity Management' (selected), 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Serv'. The main content area is titled 'Identity Source Sequences List > Sponsor_Portal_Sequence'. Under the 'Identity Source Sequence' section, the 'Name' field is set to 'Sponsor_Portal_Sequence' and the 'Description' is 'A built-in Identity Sequence for the Sponsor Portal'. The 'Certificate Based Authentication' section has an unchecked checkbox for 'Select Certificate Authentication Profile'. The 'Authentication Search List' section includes a description: 'A set of identity sources that will be accessed in sequence until first authentication succeeds'. It features two lists: 'Available' (containing 'Internal Endpoints' and 'Guest Users') and 'Selected' (containing 'ISE_Loopback', 'Internal Users', 'All_AD_Join_Points', and 'AD1'). A red box highlights 'ISE_Loopback' in the 'Selected' list, and a blue box highlights the 'Name' field.

Identity Source Sequence

* Name: Sponsor_Portal_Sequence

Description: A built-in Identity Sequence for the Sponsor Portal

▼ Certificate Based Authentication

☐ Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
Internal Endpoints	>	ISE_Loopback
Guest Users	<	Internal Users
		All_AD_Join_Points
		AD1



Add ISE PSN(s) as RADIUS Clients

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The left sidebar shows the 'Network Devices' section. The main content area, titled 'Network Devices', contains a table of configured devices. The first row, 'ISE_Self', is highlighted with a red box. The table columns are Name, IP/Mask, Location, and Type.

	Name	IP/Mask	Location	Type
<input type="checkbox"/>	ISE_Self	10.1.100.2/32	All Locations	All Device Types
<input type="checkbox"/>	admin-pc	10.1.100.200...	All Locations	All Device Types
<input type="checkbox"/>	cat3750x	10.1.50.2/32	All Locations	All Device Types
<input type="checkbox"/>	cat6500	10.1.100.1/32	All Locations	All Device Types

Add Authorization Policy Rules for Sponsor/My Devices -- Sponsor Example














- Define specific conditions to allow / deny sponsor access.
 - Permit_Access authorization will allow sponsor to successfully authenticate to Sponsor Portal
 - Deny_Access authorization will return Access-Reject and cause sponsor to fail portal authentication

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	Sponsor_Allowed	if (Network Access:Device IP Address EQUALS 10.1.100.2 AND AD1:l EQUALS Cleveland)	then PermitAccess
	Sponsor_Not_Allowed	if (Network Access:Device IP Address EQUALS 10.1.100.2 AND AD1:l EQUALS San Jose)	then DenyAccess

- Policy example matches requests where:
 - ISE is the RADIUS client
 - AD locale attribute matches City location defined under AD user properties.

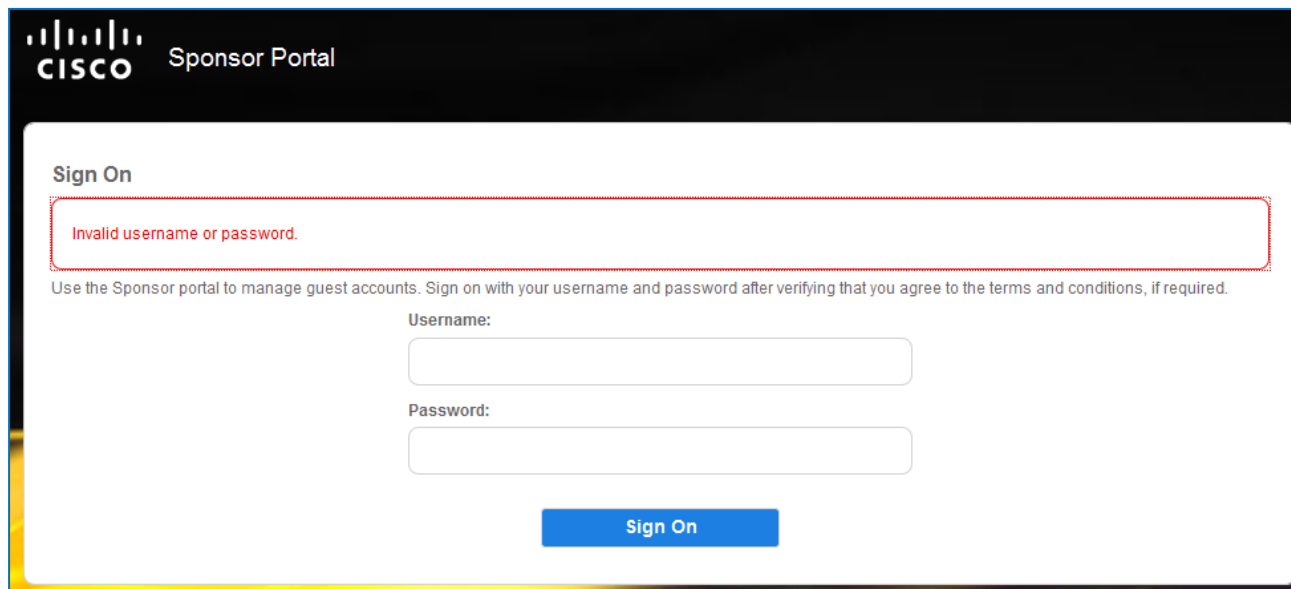
Example Live Authentications Log

- Employee1 is AD user where City = Cleveland
- Employee2 is AD user where City = San Jose

 Show Live Sessions  Add or Remove Columns  Refresh  Reset Repeat Counts Refresh Ev							
Time	Status	Details	Identity 	Authentication Policy 	Authorization Policy 	Authorization Profiles 	Network Device 
2014-11-20 12:22:25.442			employee2	Default >> Default >>...	Default >> Sponsor_...	DenyAccess	ISE_Self
2014-11-20 12:22:03.750			employee1	Default >> Default >>...	Default >> Sponsor_...	PermitAccess	ISE_Self

Portal User Experience – Sponsor Example

- Employee1 is allowed access to Sponsor Portal
- Employee2 receives error regarding invalid credentials for portal access



The screenshot displays the Cisco Sponsor Portal interface. At the top left, the Cisco logo is followed by the text "Sponsor Portal". Below this, the "Sign On" section is visible. A red-bordered box contains the error message "Invalid username or password." in red text. Below the error message, a line of text reads: "Use the Sponsor portal to manage guest accounts. Sign on with your username and password after verifying that you agree to the terms and conditions, if required." Underneath this text are two input fields: "Username:" and "Password:". At the bottom center of the form is a blue "Sign On" button.

Challenge #2: How to Map Sponsor Groups Based on Secondary Attributes?

- Solution: Configure a separate LDAP ID Store that maps Group Names to secondary attributes rather than AD/LDAP Group membership.
- Configuration Steps:
 - Define new LDAP Identity Store in ISE with Custom Schema
 - Add new Groups in ISE LDAP Store as “Pointer” objects
 - Update AD/LDAP user accounts with custom attribute values that map to new group pointer objects
 - Add New LDAP Store Pointer groups to ISE Sponsor Group configuration

Add New Group Attribute Values under AD/LDAP User

The screenshot shows the Active Directory Users and Computers console. The left pane displays the tree structure, with 'Users' under 'cts.local' selected. The right pane shows a list of 48 objects, with 'employee1' (User) highlighted. The 'employee1 Properties' dialog box is open, showing the 'General' tab. The 'City' field is highlighted with a red box and contains the value 'Cleveland'.

Server Manager (AD)

- Roles
 - Active Directory Certificate Services
 - Active Directory Domain Services
 - Active Directory Users and Computers
 - cts.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - LostAndFound
 - MAB
 - Managed Service Accounts
 - Program Data
 - System
 - Users
 - NTDS Quotas
- Active Directory Sites and Services
- DHCP Server
- DNS Server
- File Services
- Web Server (IIS)

Users 48 objects [Filter Activated]

Name	Type
Domain Guests	Security Group - Global
Domain Users	Security Group - Global
employees	Security Group - Global
employees-con...	Security Group - Global
Group Policy Cr...	Security Group - Global
PC-group	Security Group - Global
Read-only Dom...	Security Group - Global
San Jose	Security Group - Global
staff	Security Group - Global
students	Security Group - Global
VIP	Security Group - Global
Enterprise Admins	Security Group - Univ...
Enterprise Rea...	Security Group - Univ...
Schema Admins	Security Group - Univ...
admin1	User
admin2	User
Administrator	User
contractor1	User
contractor2	User
doctor1	User
doctor2	User
employee1	User
employee2	User
Guest	User

employee1 Properties

Published Certificates | Member Of | Password Replication | Dial-in | Object

Security | Environment | Sessions

Remote control | Remote Desktop Services Profile

Personal Virtual Desktop | COM+ | Attribute Editor

General | Address | Account | Profile | Telephones | Organization

Street:

P.O. Box:

City:

State/province:

Zip/Postal Code:

Country/region:

OK Cancel Apply Help

Add New Group Attribute Values under AD/LDAP User

The screenshot shows the Windows Server Manager (AD) console on the left and the 'employee2 Properties' dialog box on the right.

Server Manager (AD) Console:

- Roles
 - Active Directory Certificate Services
 - Active Directory Domain Services
 - Active Directory Users and Computers
 - cts.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - LostAndFound
 - MAB
 - Managed Service Accounts
 - Program Data
 - System
 - Users
 - NTDS Quotas
 - Active Directory Sites and Services
- Features
 - DHCP Server
 - DNS Server
 - File Services
 - Web Server (IIS)
- Diagnostics
- Configuration
- Storage

Users 48 objects [Filter Activated] Table:

Name	Type
Domain Guests	Security Group - Global
Domain Users	Security Group - Global
employees	Security Group - Global
employees-con...	Security Group - Global
Group Policy Cr...	Security Group - Global
PC-group	Security Group - Global
Read-only Dom...	Security Group - Global
San Jose	Security Group - Global
staff	Security Group - Global
students	Security Group - Global
VIP	Security Group - Global
Enterprise Admins	Security Group - Univ...
Enterprise Rea...	Security Group - Univ...
Schema Admins	Security Group - Univ...
admin1	User
admin2	User
Administrator	User
contractor1	User
contractor2	User
doctor1	User
doctor2	User
employee1	User
employee2	User
Guest	User

employee2 Properties Dialog Box:

The 'General' tab is selected. The 'City' field is highlighted with a red box and contains the text 'San Jose'.

Fields visible in the General tab:

- Street:
- P.O. Box:
- City: San Jose
- State/province:
- Zip/Postal Code:
- Country/region:

Buttons at the bottom: OK, Cancel, Apply, Help.

Verify New User Attributes in AD/LDAP from LDAP Browser

The screenshot displays the LDAP browser interface with three main panels. The left panel shows a tree view of the directory structure, with 'CN=employee1' and 'CN=employee2' highlighted. The top-right panel shows the attributes for 'CN=employee1', with the 'cn' attribute value 'Cleveland' highlighted by a red box. The bottom-right panel shows the attributes for 'CN=employee2', with the 'cn' attribute value 'San Jose' highlighted by a red box. A blue callout box points to these two entries with the text: 'employee1 mapped to Cleveland' and 'employee2 mapped to San Jose'.

employee1 mapped to Cleveland
employee2 mapped to San Jose

Name	Value
objectClass	top
objectClass	person
objectClass	organizationalPerson
objectClass	user
cn	employee1
l	Cleveland
description	cts:security-group-tag=0002-0
physicalDeliveryOffice	
distinguishedName	
instanceType	
whenCreated	
whenChanged	
displayName	
uSNCreated	
memberOf	
uSNChanged	
name	
userAccountControl	
badPwdCount	
codePage	
countryCode	
badPasswordTime	
lastLogoff	
lastLogon	
pwdLastSet	
primaryGroupID	

cn	employee2
l	San Jose
distinguishedName	CN=employee2,CN=Users,DC=cts,DC=local
instanceType	[Writable]
whenCreated	3/21/2012 3:57:53 AM
whenChanged	4/14/2015 8:55:52 PM
displayName	employee2
uSNCreated	32904
memberOf	CN=employees,CN=Users,DC=cts,DC=local
uSNChanged	837133
name	employee2
userAccountControl	[NormalAccount, NoPasswordExpiration]
badPwdCount	0
codePage	0
countryCode	0
badPasswordTime	9/23/2013 3:17:57 PM
lastLogoff	unspecified
lastLogon	2/27/2015 1:52:02 AM
pwdLastSet	3/21/2012 3:57:53 AM
primaryGroupID	513
accountExpires	never

Create New LDAP Identity Store for Sponsor Auth in ISE

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The left sidebar displays the 'External Identity Sources' tree, with 'LDAP_Sponsor' selected. The main content area shows the configuration for 'LDAP Identity Source' under the 'General' tab. The configuration includes fields for Name, Description, Schema, Subject Objectclass, Subject Name Attribute, Certificate Attribute, Group Objectclass, and Group Map Attribute. A red box highlights the 'Subject Objectclass', 'Subject Name Attribute', 'Certificate Attribute', 'Group Objectclass', 'Group Map Attribute', and the radio button options. A blue callout box points to the 'Group Map Attribute' field, stating: 'Group Map Attribute is user attribute which contains group reference, I = locale in this example'. The radio button 'Subject Objects Contain Reference To Groups' is selected.

External Identity Sources

- Certificate Authentication Profile
- Active Directory
 - AD 1
- LDAP
 - AD_LDAP
 - LDAP 1
 - LDAP_Sponsor**
- RADIUS Token
- RSA SecurID

LDAP Identity Source

General | Connection | Directory Organization | Groups | Attributes

* Name: LDAP_Sponsor

Description:

Schema: Custom

* Subject Objectclass: person

* Subject Name Attribute: cn

Certificate Attribute: userCertificate

* Group Objectclass: group

* Group Map Attribute: I

☒ Subject Objects Contain Reference To Groups

☐ Group Objects Contain Reference To Subjects

Subjects In Groups Are Stored In Member Attribute As: Distinguished Name

Add New LDAP “Pointer” Groups to ISE LDAP Store

- Manually enter names (not fetch) to match desired user attribute values
- Groups do NOT need to exist in AD/LDAP—They are “pointers” only!

LDAP Identity Sources List > LDAP_Sponsor

LDAP Identity Source

General Connection Directory Organization **Groups** Attributes

Edit Add Delete Group

☐ Name Select Groups From Directory

Add Group

Group Names can be virtually any value to match directory attributes. Examples: Yes/No or True/False

Add Directory Group ✕

Please enter name for new Group:

Cleveland

OK Cancel

LDAP Identity Sources List > LDAP_Sponsor

LDAP Identity Source

General Connection Directory Organization **Groups** Attributes

Edit Add Delete Group

☐ Name

☐ Cleveland

☐ San Jose

Add/Edit Sponsor Groups using New LDAP Group Names

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes the Cisco logo, the product name 'Identity Services Engine', and a menu with 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, a secondary bar contains 'Configure', 'Manage Accounts', and 'Settings' tabs. The left sidebar, titled 'Configure Guest and Sponsor Access', lists five options: 'Overview', 'Guest Portals', 'Guest Types', 'Sponsor Groups' (which is highlighted in blue), and 'Sponsor Portals'. The main content area is titled 'Sponsor Groups' and includes a descriptive sentence: 'You can edit and customize the default sponsor groups and create additional ones.' Below this text is a toolbar with 'Create', 'Edit', 'Duplicate', and 'Delete' buttons. A list of three sponsor groups follows: 'ALL_ACCOUNTS (San Jose)', 'GROUP_ACCOUNTS (default)', and 'OWN_ACCOUNTS (Cleveland)'. The first and third groups are highlighted with red rectangular boxes. Each group entry shows its name in bold, its location in parentheses, and a brief description of its permissions.

Configure Guest and Sponsor Access

- Overview**
Get an overview of the steps required to configure guest access
- Guest Portals**
Configure the portals guests will use to access the network
- Guest Types**
Specify guest's access privileges
- Sponsor Groups**
Define the permissions and settings for users who can create and manage guest accounts
- Sponsor Portals**
Configure the portals that sponsors use to create and manage guest accounts

Sponsor Groups

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

Create Edit Duplicate Delete

- ALL_ACCOUNTS (San Jose)**
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
- 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
- OWN_ACCOUNTS (Cleveland)**
Sponsors assigned to this group can manage only the guest accounts that they have created. By default, users in the OWN_ACCOUNTS user identity group are members of this sponsor group

Add the LDAP “Pointer” Groups as Members

- Guest Access > Configure > Sponsor Groups

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The main page is titled 'Sponsor Group' and includes a 'Configure' tab. A red box highlights the 'Sponsor group name:*' field, which contains the text 'ALL_ACCOUNTS (San Jose)'. Below this, the 'Description' field contains the text: 'Sponsors assigned to this group can manage all guest user identity group are members of this group'. A 'Members...' button is visible. To the right, a modal window titled 'Select Sponsor Group Members' is open. It contains two lists: 'Available User Groups' and 'Selected User Groups'. The 'Available User Groups' list includes 'AD1:cts.local/Users/contractors', 'AD1:cts.local/Users/doctors', 'AD1:cts.local/Users/Domain Admins', 'AD1:cts.local/Users/Domain Computers', 'AD1:cts.local/Users/Domain Users', 'AD1:cts.local/Users/employees', 'AD1:cts.local/Users/employees-cont', 'AD1:cts.local/Users/Enterprise Admins', and 'AD1:cts.local/Users/PC-group'. The 'Selected User Groups' list includes 'ALL_ACCOUNTS (default)' and 'LDAP_Sponsor:San Jose', which is highlighted with a red box. A 'Search' button is present in both lists. Navigation buttons '>' and '>>' are located between the lists.

Add the LDAP “Pointer” Groups as Members

Sponsor group name:* ALL_ACCOUNTS (San Jose)

Description: 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

Members...

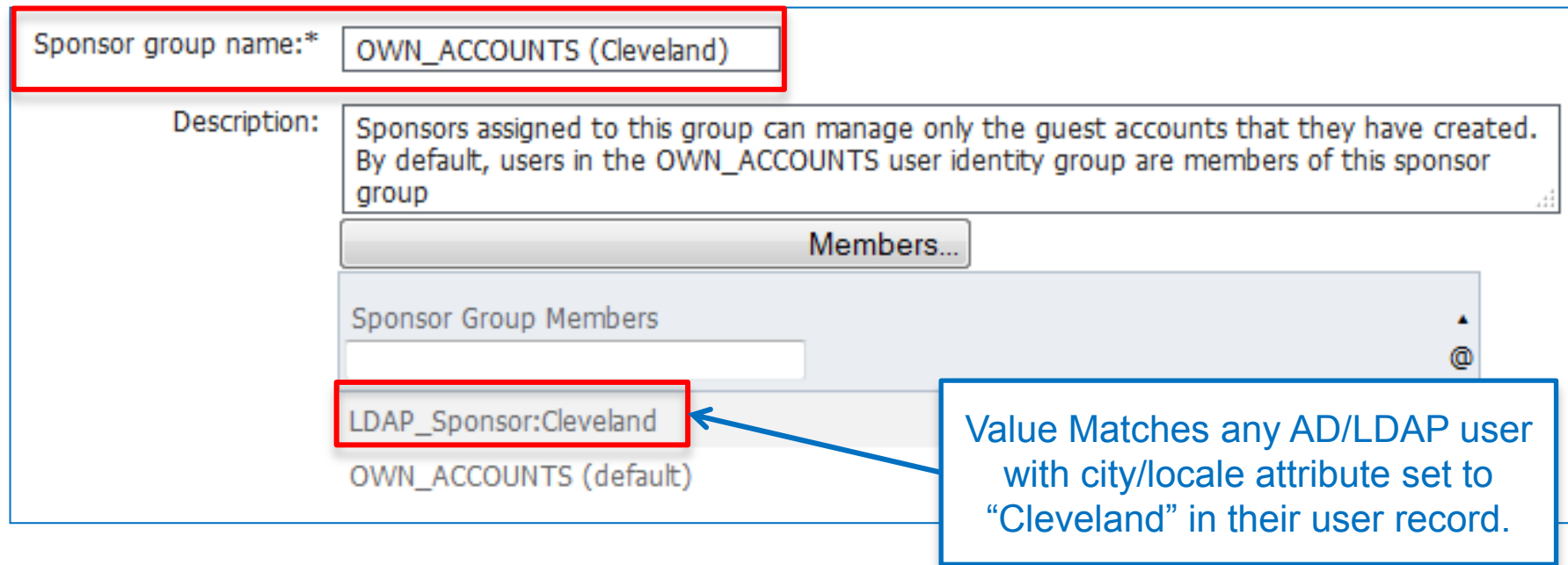
Sponsor Group Members

ALL_ACCOUNTS (default)

LDAP_Sponsor:San Jose

Value Matches any AD/LDAP user with city/locale attribute set to “San Jose” in their user record.

Add the LDAP “Pointer” Groups as Members



Sponsor group name:*

Description: Sponsors assigned to this group can manage only the guest accounts that they have created. By default, users in the OWN_ACCOUNTS user identity group are members of this sponsor group

Members...

Sponsor Group Members

-
- OWN_ACCOUNTS (default)

Value Matches any AD/LDAP user with city/locale attribute set to “Cleveland” in their user record.

Sponsor Portal User Experience

- Employee1 (mapped to Cleveland) only sees Guests they created (Currently 0)

CISCO Sponsor Portal

Welcome employee1 ▾

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

Guest type:

Contractor (default) ▾

Maximum devices that can be connected: 5
Maximum access duration: 365 days

Guest Information

Known Random Import

Access Information

Duration:*
89 Days (Maximum:365)

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

First name:

Sponsor Portal User Experience

- Employee2 (mapped to San Jose) is able to manage ALL Accounts including those created by other Sponsors

The screenshot displays the Cisco Sponsor Portal interface. At the top left is the Cisco logo and the text "Sponsor Portal". At the top right, a welcome message "Welcome employee2" is shown in a dropdown menu, highlighted with a red box. Below this, there are four buttons: "Create Accounts", "Manage Accounts (12)" (highlighted with a red box), "Pending Accounts (0)", and "Notices (0)". A search bar is located below the buttons. Below the search bar, there are seven buttons: "Edit", "Resend", "Extend", "Suspend", "Delete", "Reset Password", and "Reinstate", followed by a "Refresh" button. Below these buttons is a table with the following columns: "User...", "State", "First Name", "Last Name", "Email Ad...", "Phone N...", "Group Tag", "Location", "Sponsor", "Guest Ty...", "Expirati...", and "Time Left". The table contains three rows of data:

User...	State	First Name	Last Name	Email Ad...	Phone N...	Group Tag	Location	Sponsor	Guest Ty...	Expirati...	Time Left
flintstone	Created	Fred	Flintstone	cmhyps@y...	2162330155	API	Denver	admin1	Contractor (default)	2015-04-17 20:01	2D 10H 17M
jstevenson	Created	Jill	Stevenson	jstevens@...	555-111-2...	red	New York	admin1	Weekly (default)	2015-04-19 20:16	4D 08H 32M
newquest...	Created					red	New York	admin1	Weekly (default)	2015-04-19 20:16	4D 08H 32M

