ISE
Sponsored BYOD

Craig Hyps, SAMPG TME
March 2013

Sponsored BYOD

What Is It?

- Sponsored BYOD allows an administrator or other authorized employee to generate temporary credentials on behalf of another employee. These short-term credentials permit the select employee to register their personal device and optionally configure the native supplicant and provision certificates to that personal device for secure access to the corporate network using 802.1X.

Sponsored BYOD

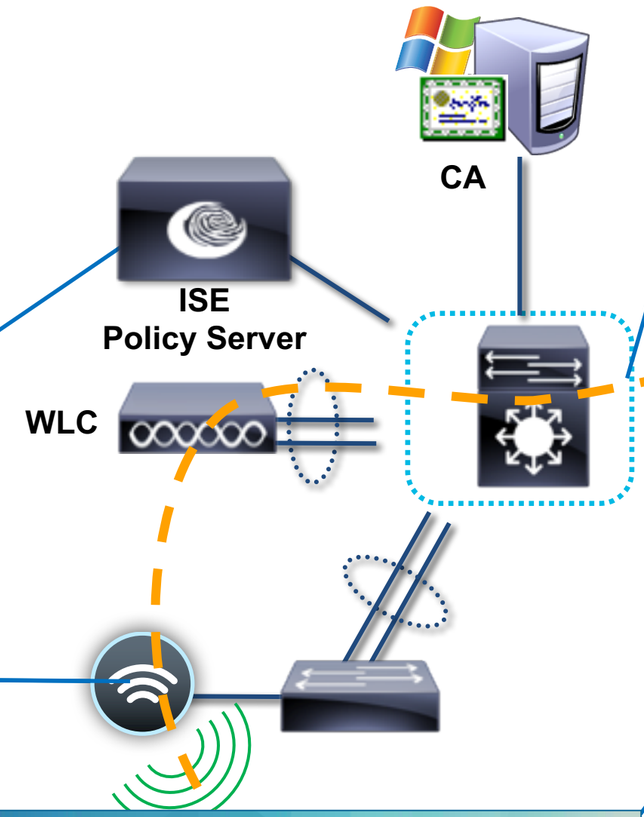
Process Flow

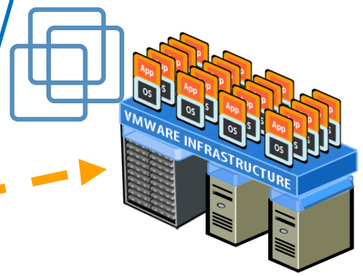
One-time redirect of the employee web session to ISE portal for auth and device onboarding

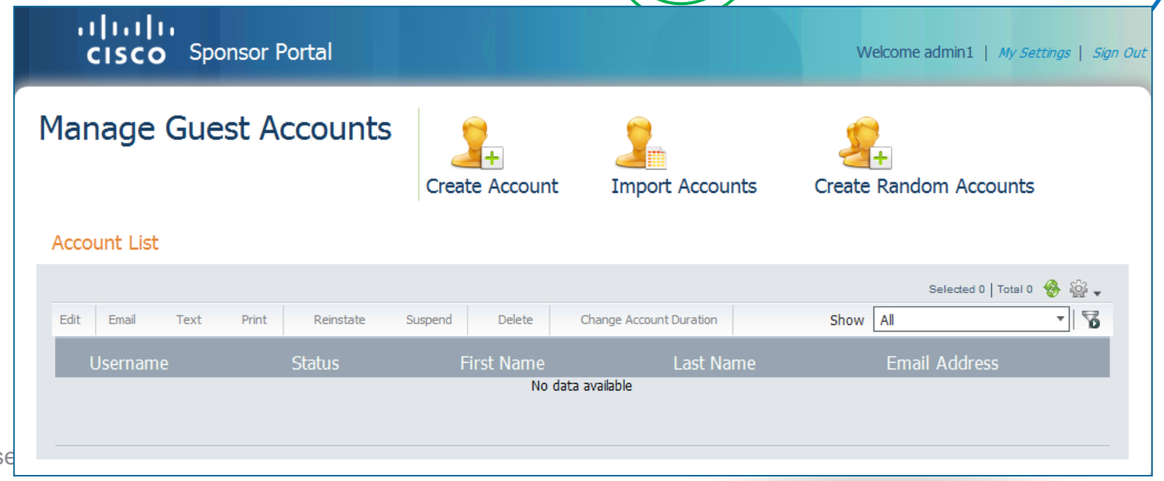
Employee auth using cert with 802.1X; access granted to corporate resources.

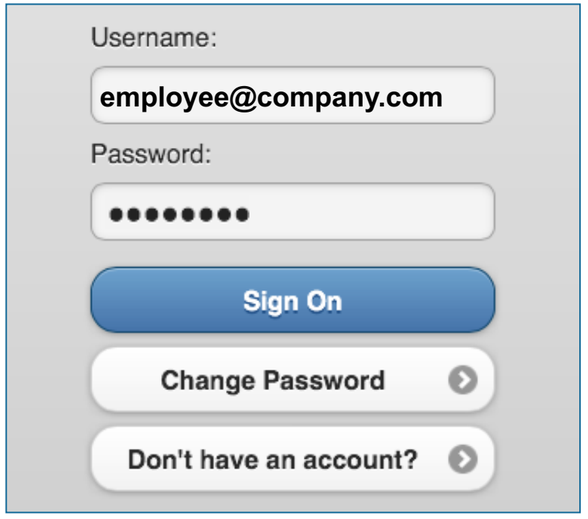
Secure SSID « BYOD-8021X » with EAP-TLS

Sponsor generates temp credentials for employee









Sponsored BYOD

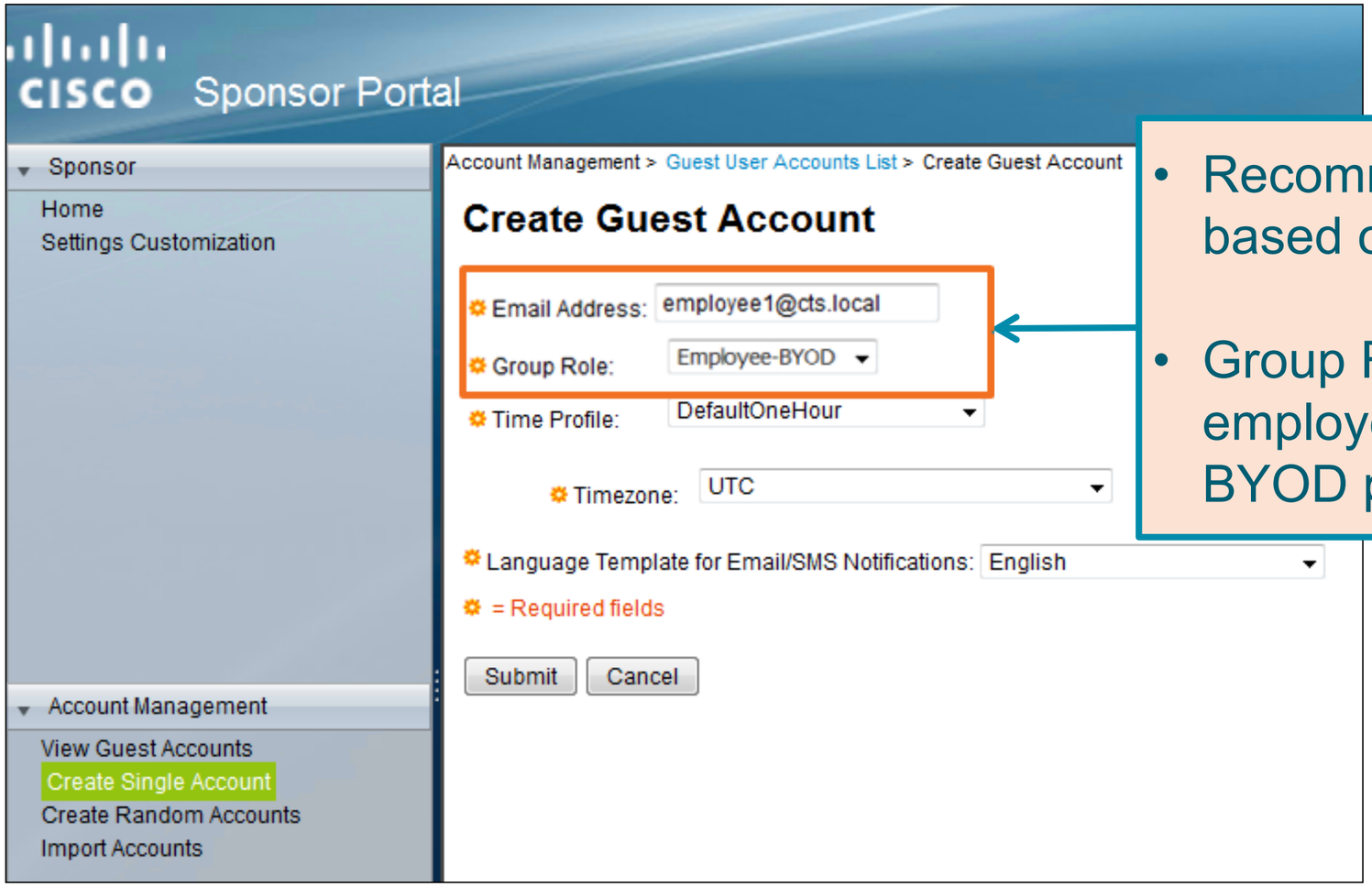
Challenges and Solution

- Current ISE limitations:
  - Sponsor portal is intended to generate guest accounts only.
  - ISE Device Registration and Native Supplicant Provisioning is intended for employees or other non-guest accounts.
  - Default ISE policy bypasses Device Registration and NSP for all guest users.

- Solution:
  - Manager uses ISE sponsor portal to create a guest account *for an employee*
  - Guest username policy is set to match employee user ID, example email address.
  - Manager assigns “guest” account to specific ID group, example “EmployeeNSP”
  - New Authorization Policy rule matches ID group and applies NSP authorization.

Sponsored BYOD Configuration

Sponsor Creates Temporary Employee Credentials

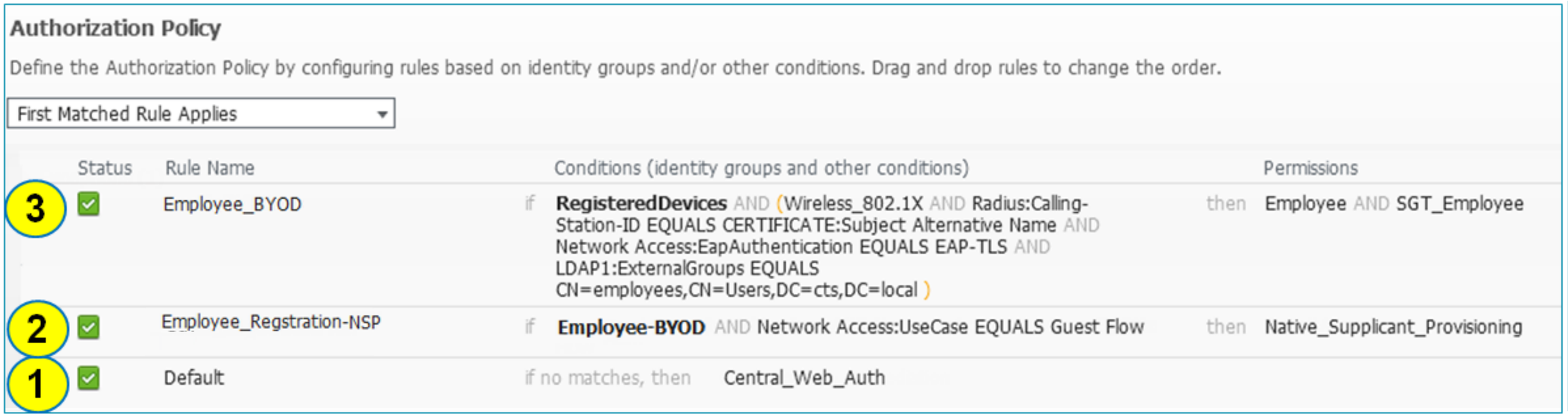


- Recommend guest username be based on employee name or ID.
- Group Role assignment identifies employees that will be directed to BYOD process upon login.

Sponsored BYOD Configuration

Authorization Policy

1. Sponsored employee logs in first time via CWA (Default rule) using “guest” credentials.
2. CoA re-auth sent upon successful web authentication; employee now hits NSP rule based on matching ID group and Guest Flow conditions.
3. When NSP completes, user reconnects on secure WLAN using EAP-TLS with newly provisioned certificate. Optional matching of client MAC (Calling-Station-ID) to certificate SAN and AD/LDAP lookups based on user name found in certificate Subject—inserted as part of NSP process.



Sponsored BYOD Configuration

Authorization Details (Post Provisioning)

Authentication Details	
Logged At:	March 2,2013 1:43:30.245 AM
Occurred At:	March 2,2013 1:43:32.988 AM
Server:	ise-psn-2
Authentication Method:	dot1x
EAP Authentication Method :	EAP-TLS
EAP Tunnel Method :	
Username:	employee1@cts.local
RADIUS Username :	employee1@cts.local
Calling Station ID:	7C:6D:62:E3:D5:05
Framed IP Address:	
Use Case:	
Network Device:	wlc5508
Network Device Groups:	Device Type#All Device Types#Wireless,Location#All Locations#North_America#RTP
NAS IP Address:	10.1.44.90
NAS Identifier:	Cisco_0c:99:a4
NAS Port:	1
NAS Port ID:	
NAS Port Type:	Wireless - IEEE 802.11
Allowed Protocol:	Default Network Access
Service Type:	Framed
Identity Store:	
Authorization Profiles:	Employee,SGT_Employee
Active Directory Domain:	
Identity Group:	RegisteredDevices
Allowed Protocol Selection Matched Rule:	Dot1X
Identity Policy Matched Rule:	Default
Selected Identity Stores:	
Authorization Policy Matched Rule:	Employee_BYOD
SGA Security Group:	SGT_Employee
AAA Session ID:	ise-psn-2/151542177/524
Audit Session ID:	0a012c5a000005a651315921
Tunnel Details:	Tunnel-Type=(tag=0) VLAN,Tunnel-Medium-Type=(tag=0) 802,Tunnel-Private-Group-ID=(tag=0) 40
Cisco-AVPairs:	audit-session-id=0a012c5a000005a651315921
Other Attributes:	ConfigVersionId=5,DestinationPort=1812,Protocol=Radius,Framed-MTU=1300,State=37CPMSessionID=0a012c5a000005a651315921;33SessionID=ise-psn-2/151542177/524;,Airespace-Wlan-Id=8,ExternalGroups=cn=employees,cn=users,dc=cts,dc=local,CPMSessionID=0a012c5a000005a651315921,EndPointMACAddress=7C-6D-62-E3-D5-05,EndPointMatchedProfile=Apple-iPad,HostIdentityGroup=Endpoint Identity Groups:RegisteredDevices,Device Type=Device Type#All Device Types#Wireless,Location=Location#All Locations#North_America#RTP,Device IP Address=10.1.44.90,Called-Station-ID=f0-25-72-12-6f-a0:BYOD-8021X

Authentication Method:	dot1x
EAP Authentication Method :	EAP-TLS
EAP Tunnel Method :	
Username:	employee1@cts.local
RADIUS Username :	employee1@cts.local
Calling Station ID:	7C:6D:62:E3:D5:05

Matched Rule = Employee_BYOD
WLAN = BYOD-8021X
Endpoint Identity Group = RegisteredDevices
ExternalGroups = cn=employees,cn=users,dc=cts,dc=local
Profile=Apple-iPad

Sponsored BYOD

Demonstration VoD

- 11-minute VoD demonstrates the entire process of creating a guest account, the user provisioning experience, as well as review of the authentication logs and Authorization Policy rules:

https://cisco.webex.com/ciscosales/lsr.php?RCID=8990f752b80f41ae29e2adb0f5f98ca1


CISCO