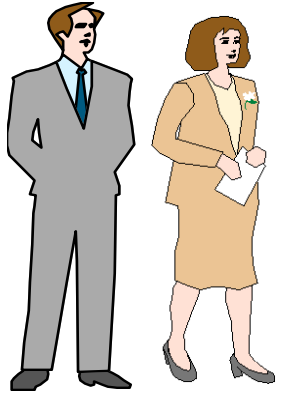
Overview of ISE vs ACS policy model

by: Krishnan Thiruvengadam

Date: 11/10/2017

What is Access Control?



APPROVED

Access control policy plan

Policy

High level business requirement with Identity, context and level of access

Model

Role Based Access control
and/or
Rule Based Access control

Mechanism

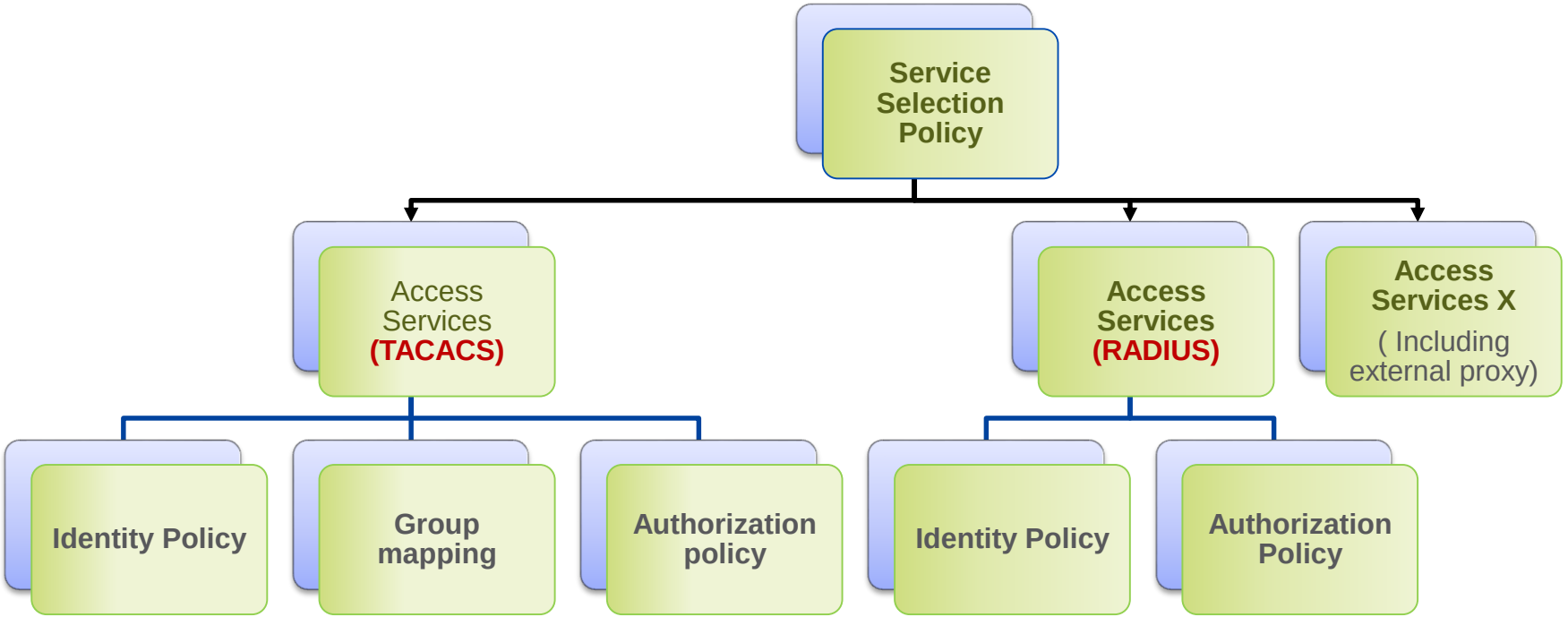
VLAN, ACL, SGT

Identity	Context	Access Level
		Full Access
		Internet only

Policy example

Identity	Context (who, what, when, where, how, posture/threat)	Level of Access
Guest (including contractors)	WiFi, Weekly, verify MAC	Internet
Personal devices	WiFi, employee	Limited Access after onboarding
Device Administrators	Network operators, WLC Help desk, WLC	Full Access Monitoring access

ACS Policy model – Service selection rules



ACS Service Selection Policy

AAA Request

Service Selection

Access Service 1

Access Service 2

Access Service 3

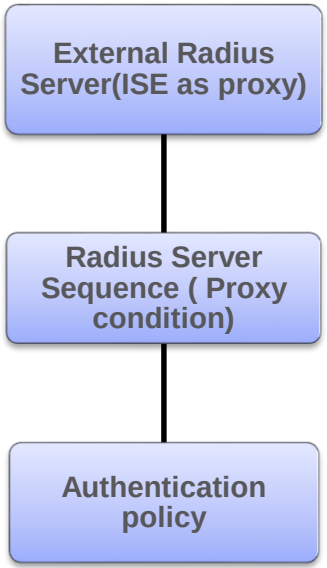
AAA Response

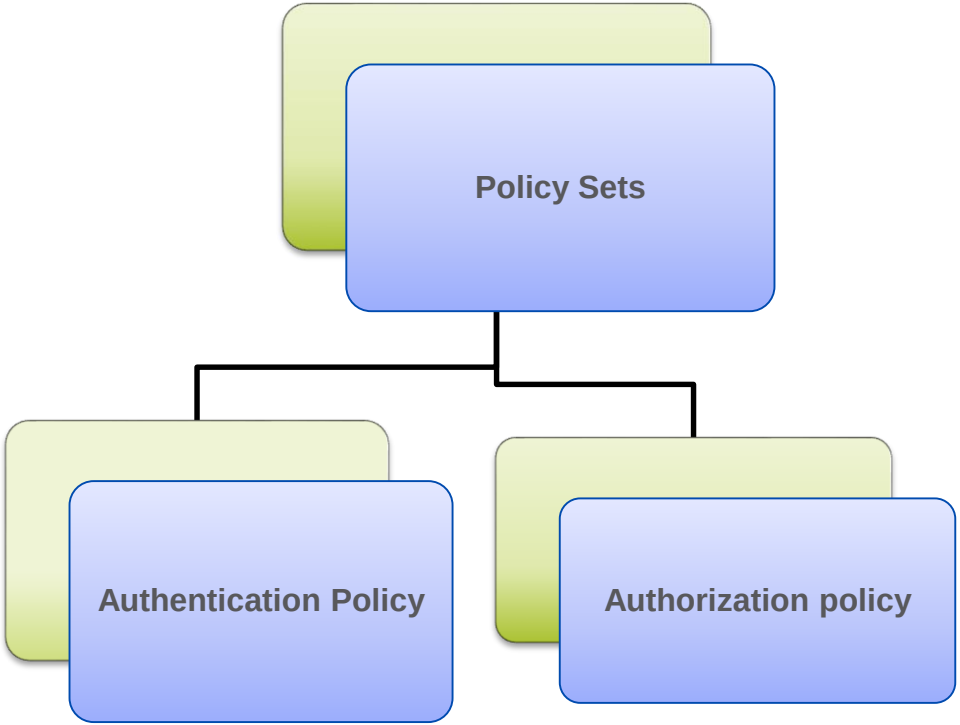
AAA Service with Identity and Authorization policy

Service Selection policy filters and chooses Access Services

ACS Service Selection Criteria
AAA protocol
Network device group
ACS server
Request attributes
Date and time
AAA client

ISE Policy model – Policy sets





Policy Sets

Policy set conditions/ criteria

Device type / OS/

Nexus

ASA/Firewall

Layer 3 switch

WLC

Medium/ 3rd party device profile and attributes

Wired

Wireless

VPN

Cisco Prime

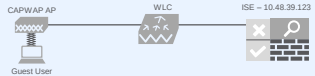
3rd Party devices

Authentication Type (pre-defined conditions)

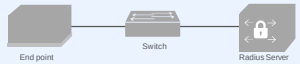
Easy Connect

802.1x

Web Auth



White Listing



Network Device Location

Corporate headquarters

Branch

Campus

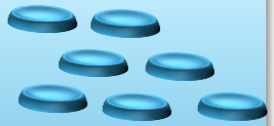
Across Geographies

Refer to the Cisco ISE Compatibility Matrix  http://cs.co/ise-compatibility

Conditions supported in ISE Policy sets

Policy Set Conditions (Network Access)

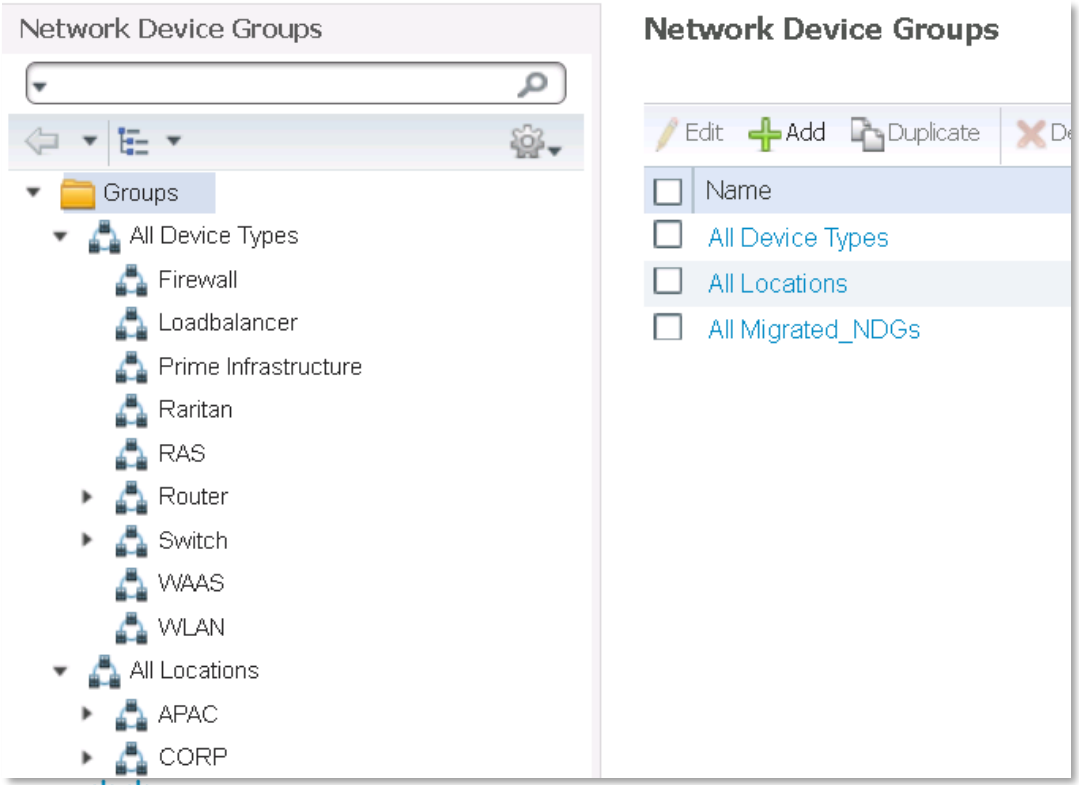
- Network devices
- Basic Network access
- 3rd party NAD
- Network device profiles
- Radius/ TACACS+ attribute
- Pre-defined conditions



Policy Set Conditions (Device Administration)

- Network devices
- Basic Network access
- TACACS+ attribute
- Pre-defined conditions

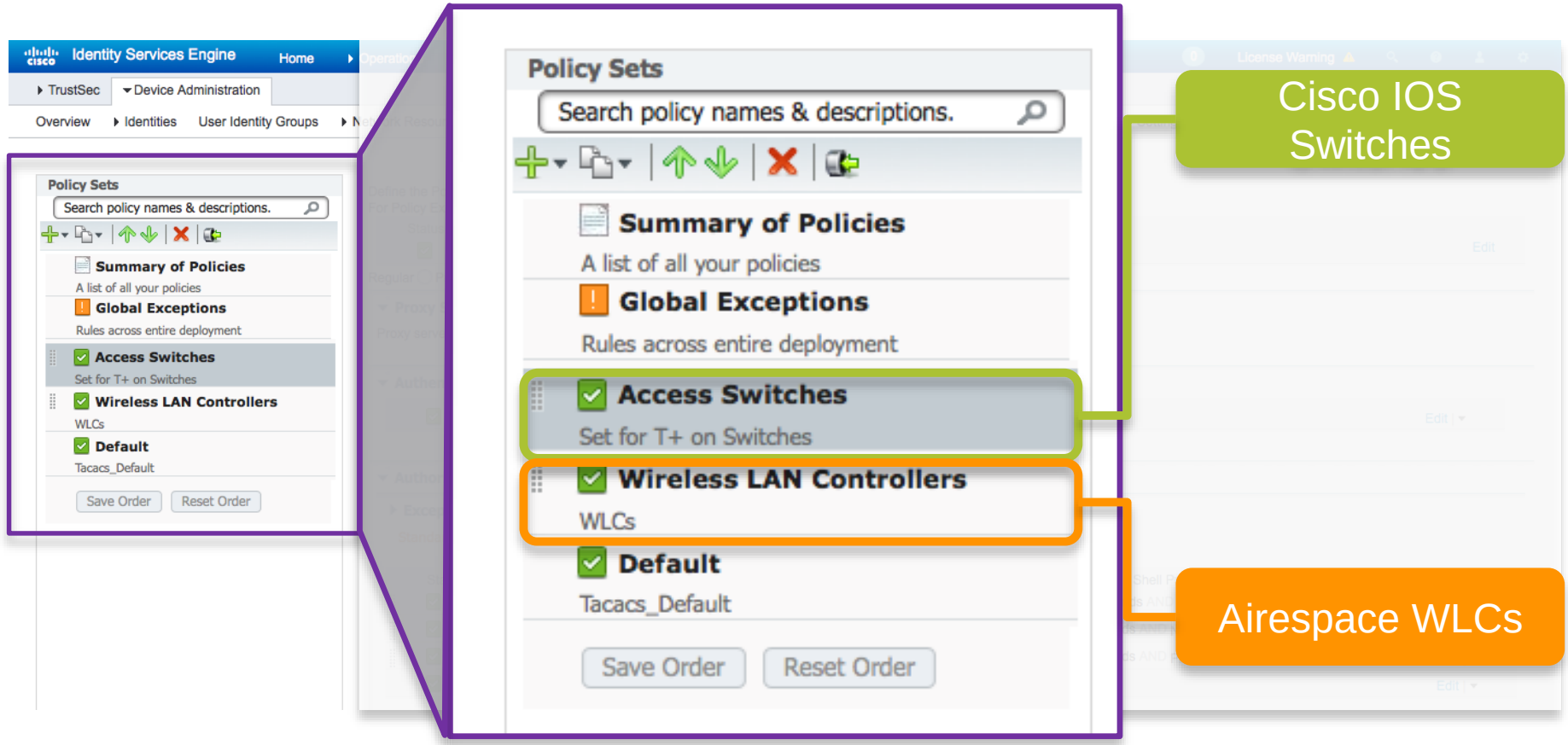
Device Administration Best Practices



USE NDG'S!

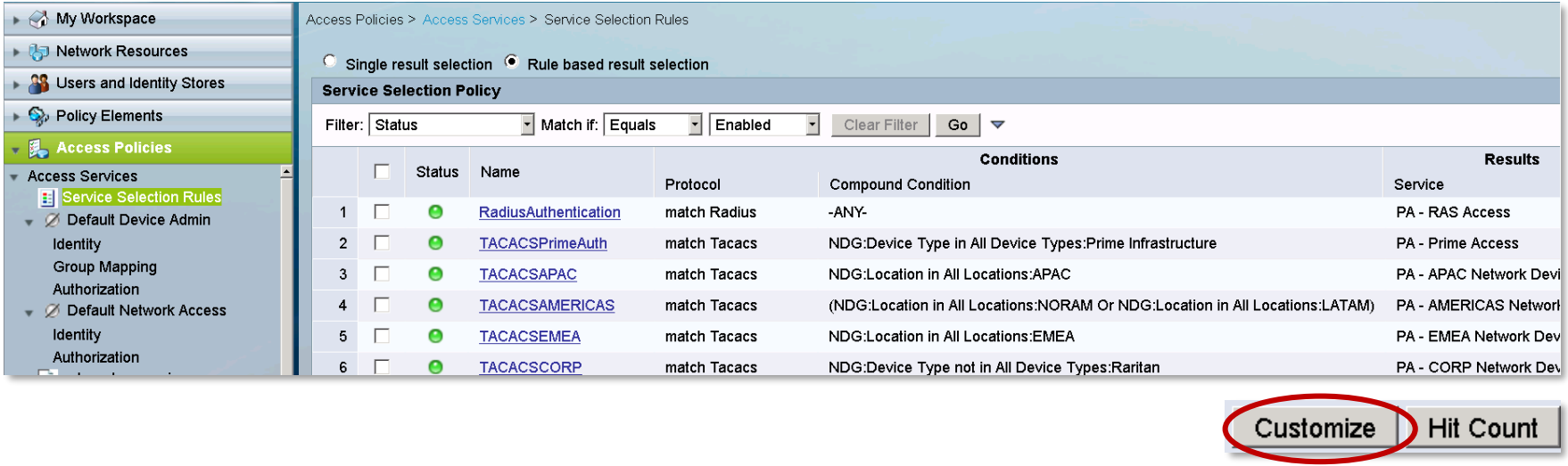
- Different Policy Sets for IOS than AireSpace OS
- Different for Security Apps than Routers
- Different for ASA
- Differentiate based on location of Device

Use Policy Sets Based on Device Type

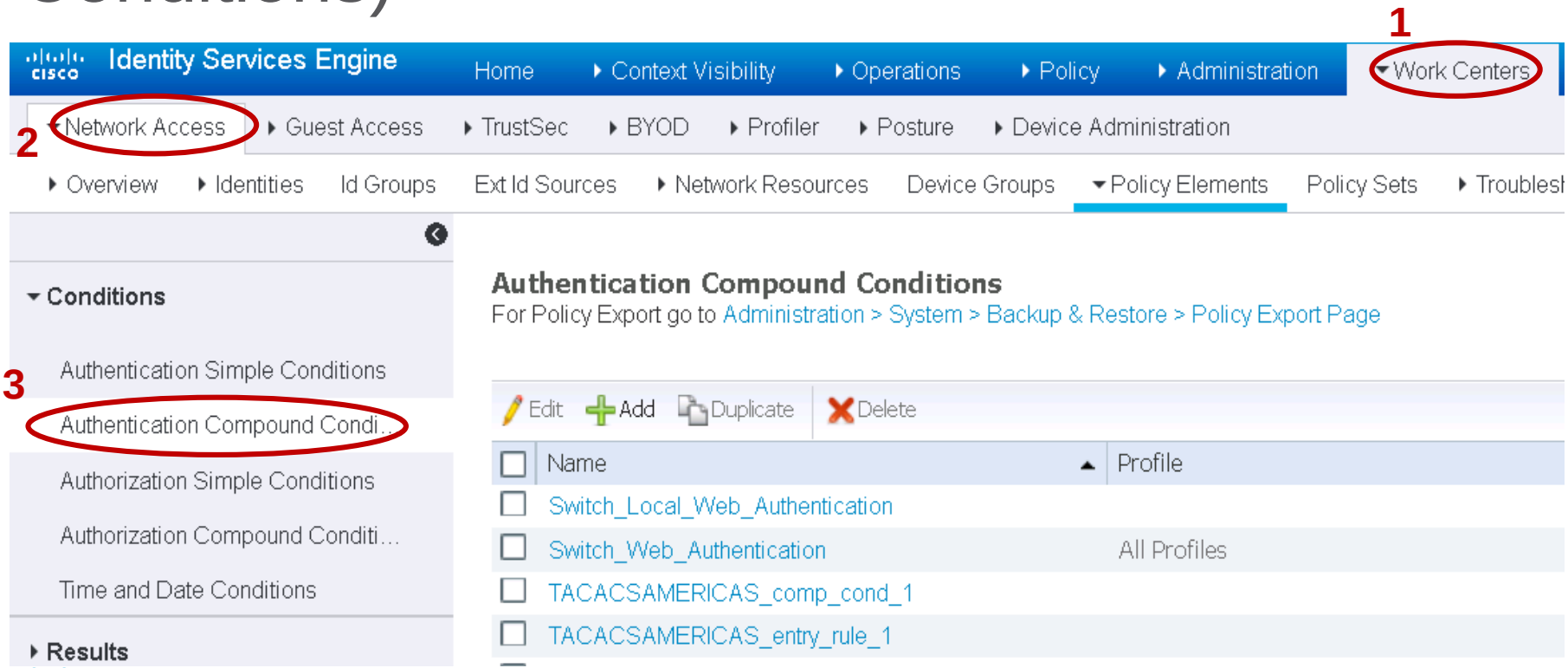


ACS - Service Selection rules (custom conditions)

ACS UI: Access Policies → Access Services → Service Selection rules → Customize

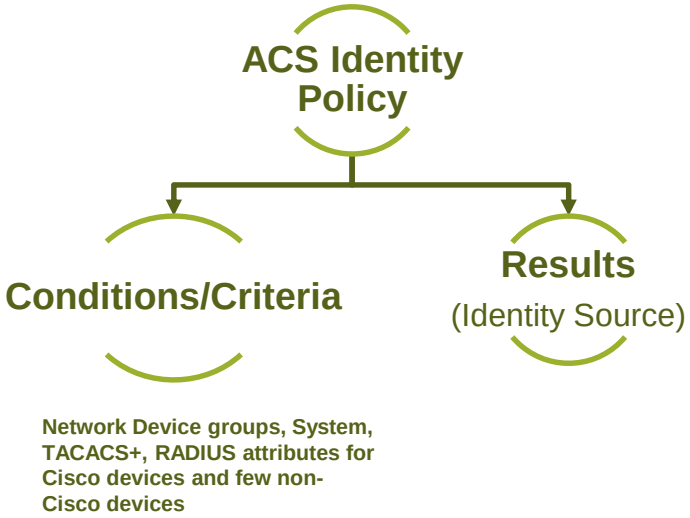


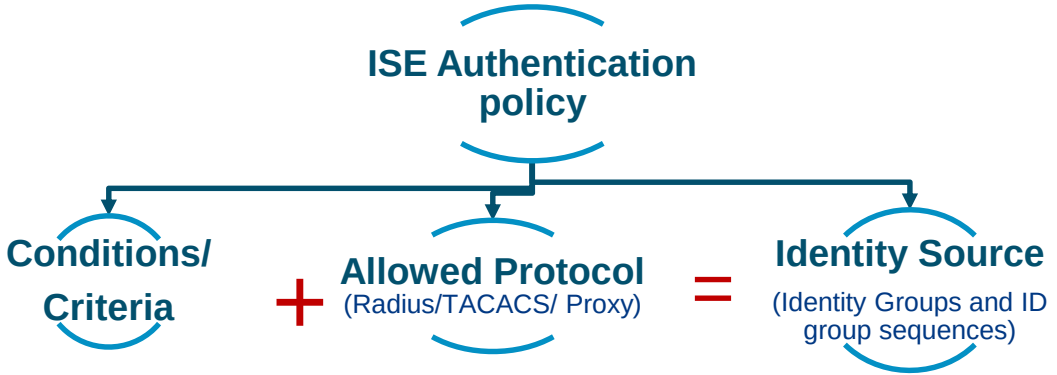
ISE - Policy set criteria (Compound Conditions)



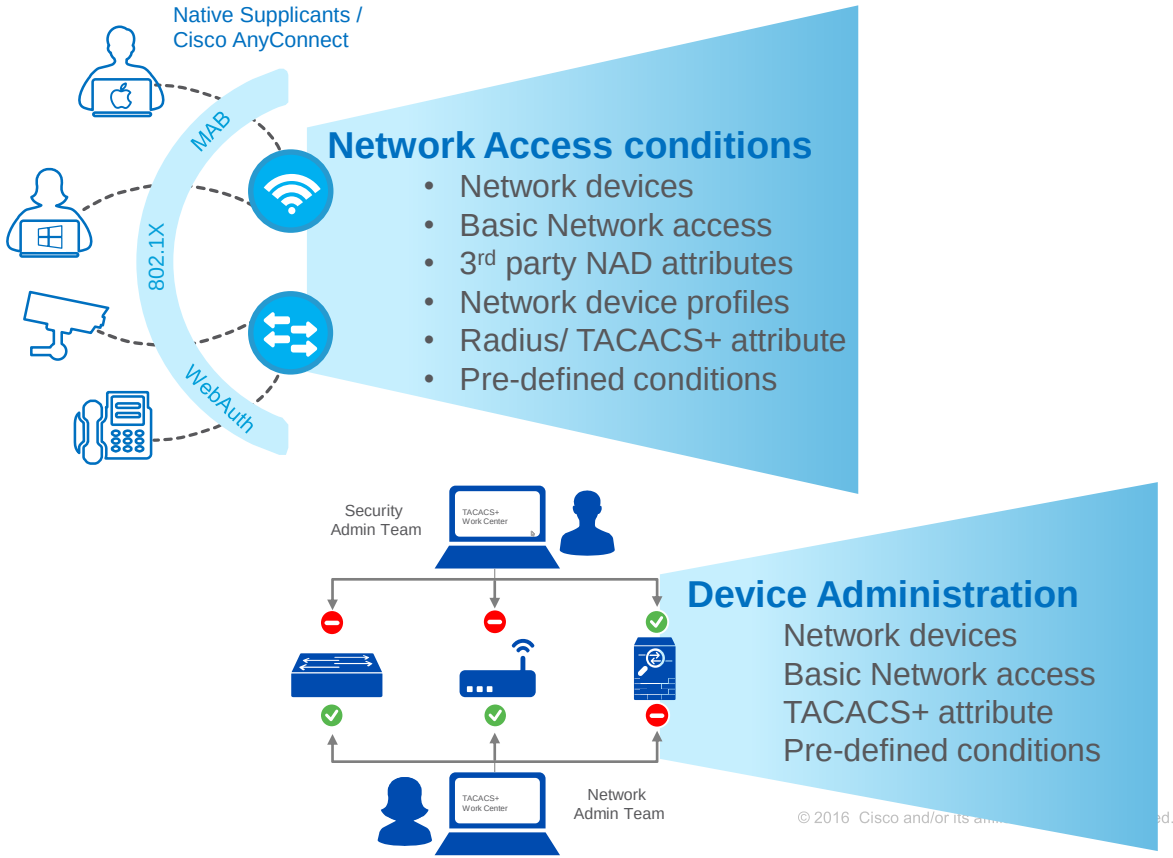
Authentication Policy

ACS vs ISE Authentication policy

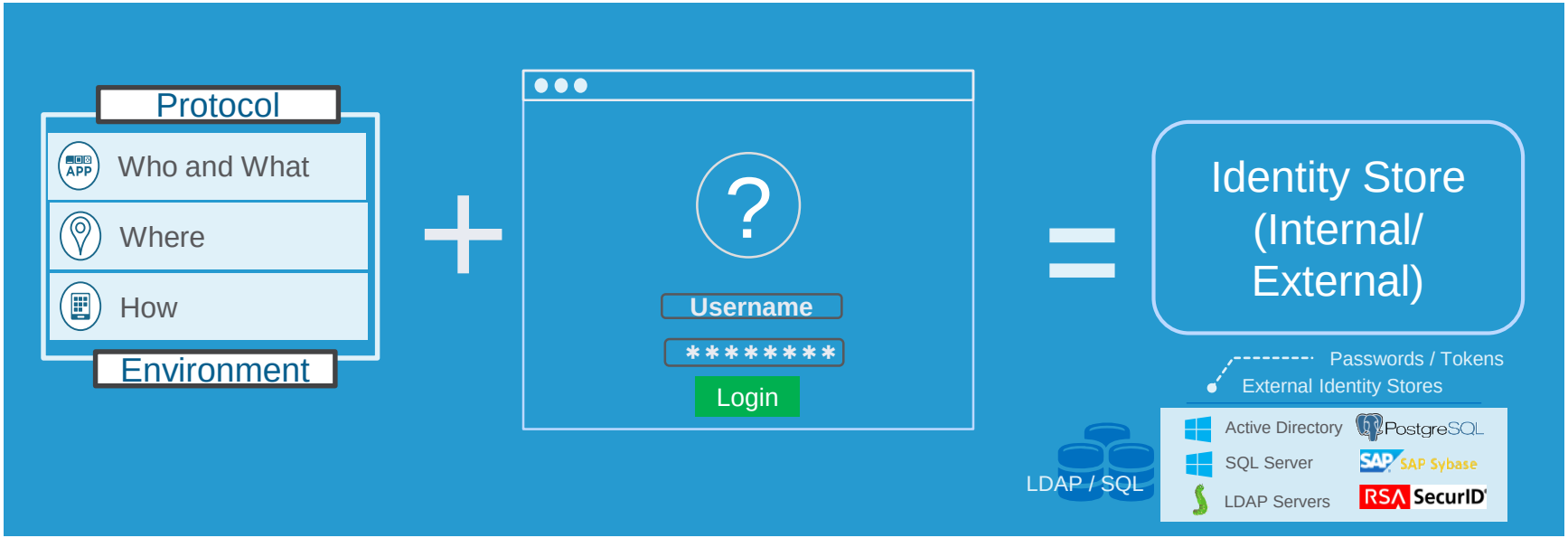




Conditions supported in ISE Authentication policies

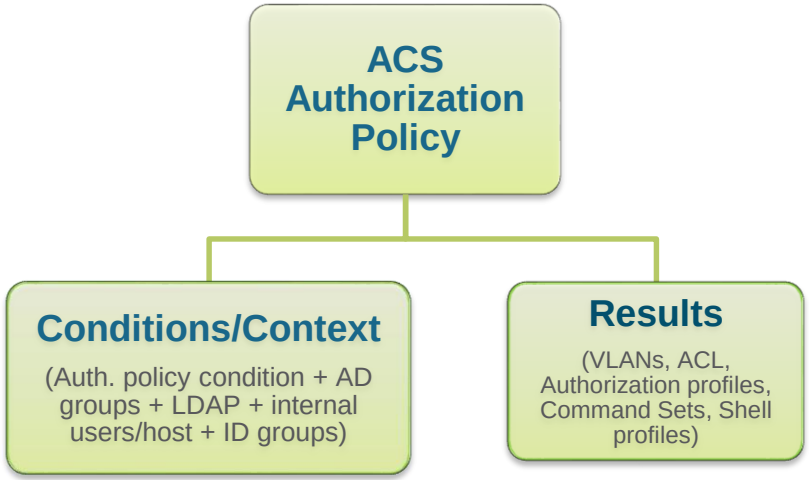


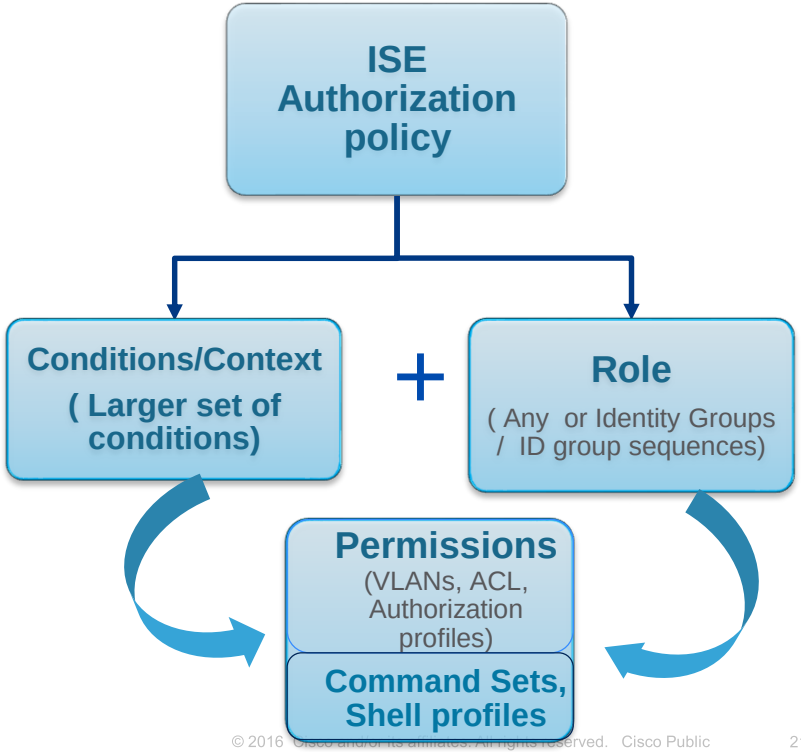
How does ISE authenticate users?



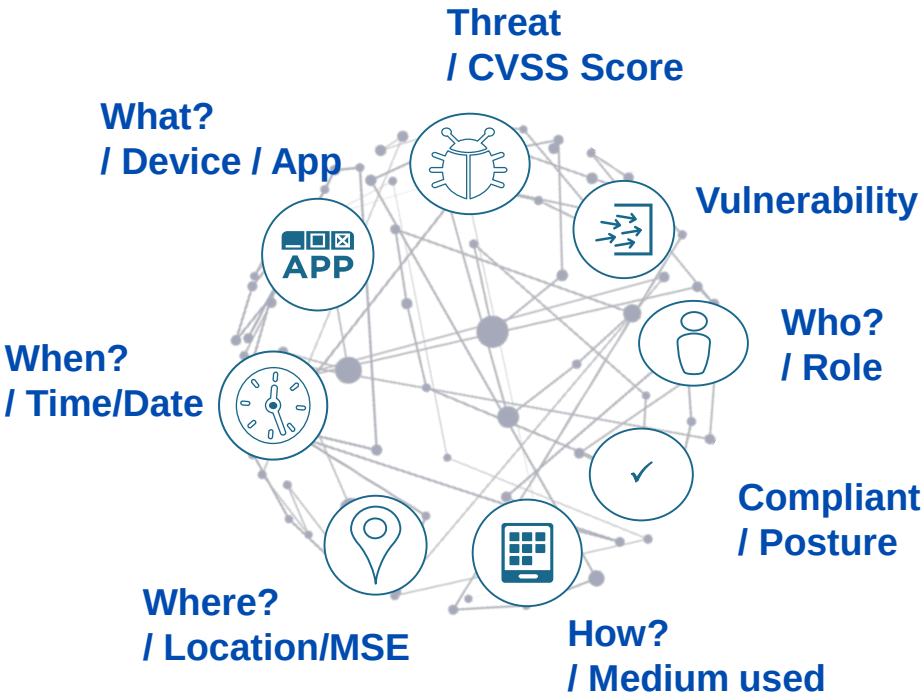
Authorization policy

ACS vs ISE Authorization policy





Authorization Policy Conditions/Context



Context /Conditions

- Network devices
- Basic Network access
- 3rd party NAD
- Network device profiles
- Radius/ TACACS+ attribute
- Pre-defined conditions
  - Time and Date Conditions
- Active Directory
- LDAP
- Endpoints
- Guest
- CWA
- Session
- MSE
- Passive ID
- Internal Users/ Groups

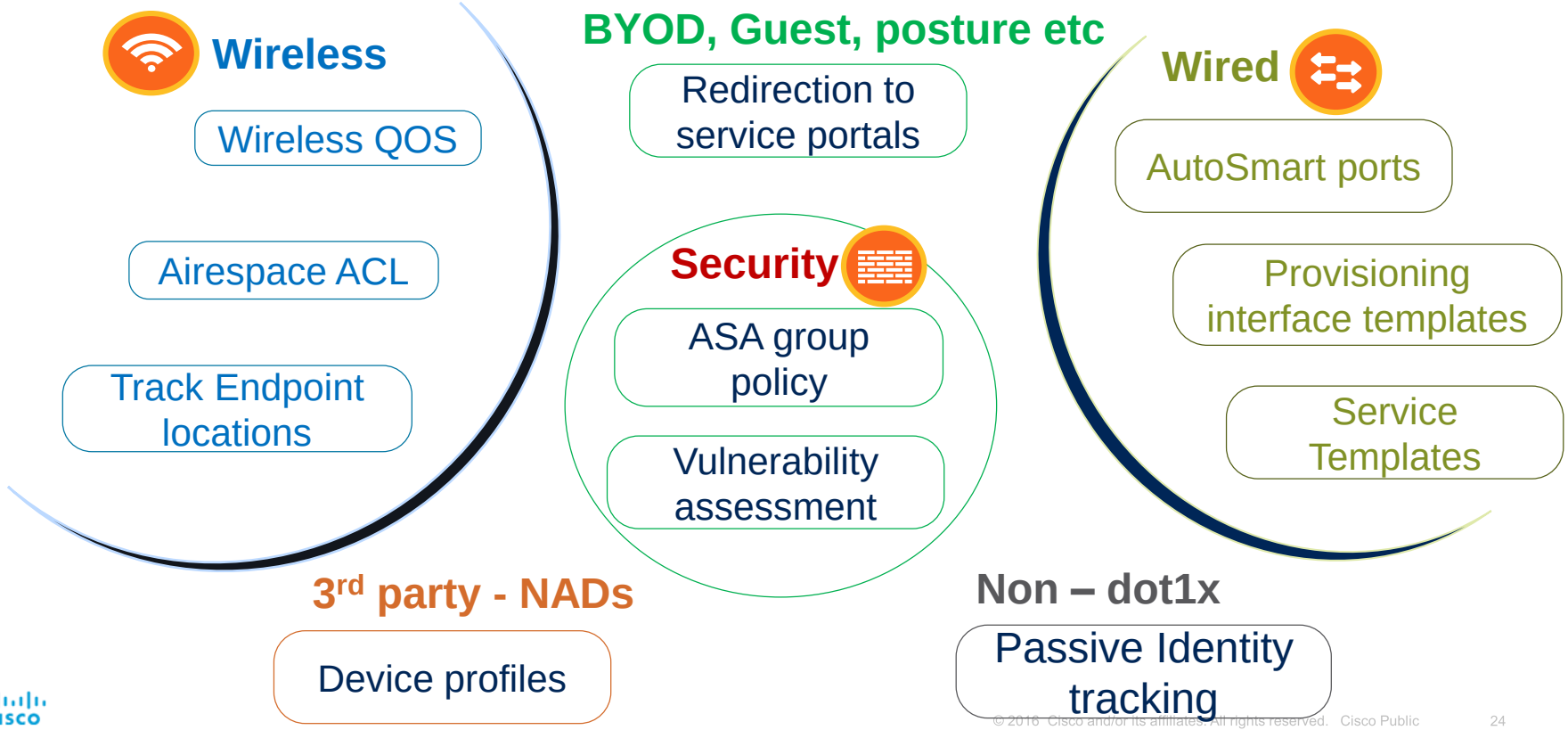
Reference:
https://communities.cisco.com/docs/DOC-67894

Context Rich context Support for 400+ attributes

Authorization policy – Permissions (Network Access)

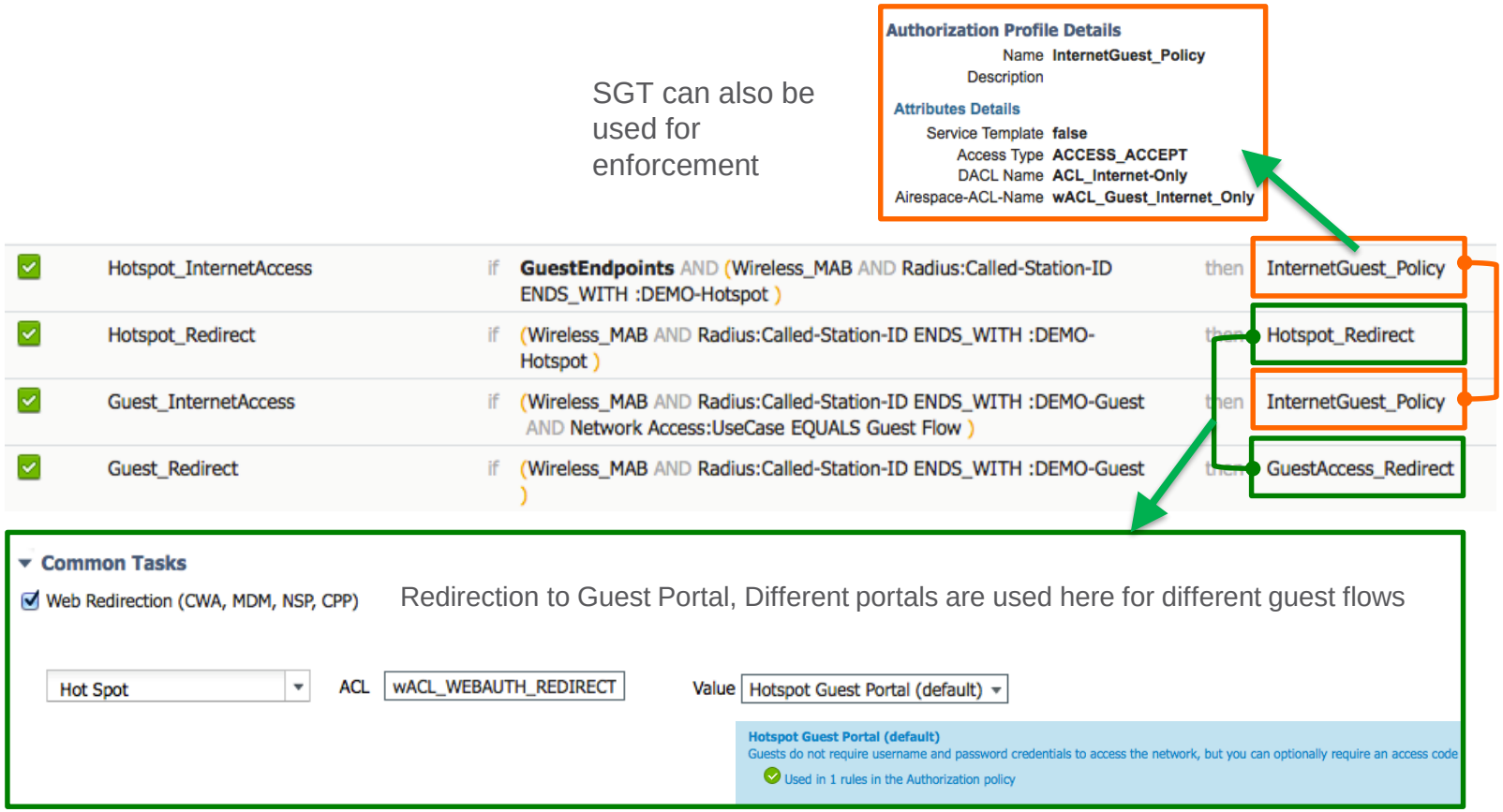
ACS	ISE
Downloadable ACL (Static/Dynamic from AD, Internal users/hosts, LDAP)	**Downloadable ACL** with syntax check(Static / Dynamic supported in ISE 2.1 p 2(internal users/AD)
Authorization profile	
Downloadable ACL **Filter ID ACL** **Proxy ACL**	**Downloadable ACL** **Filter ID ACL**
Linksec Security policy: Should, must, must-not secure	**MACSec policy**: Should, must, must-not secure
Reauthentication timer (Static/Dynamic from AD, Internal users/hosts, LDAP)	**Reauthentication timer**(static) (Use Advanced setting to map it to AD attribute)
VLAN (Static/Dynamic from AD/internal users/host/LDAP) with configurable ID only	**VLAN** (AD support via Advanced setting- create RADIUS attributes for VLAN and map the value to AD attribute)
QOS (Input and Output policy map)	**Not supported**

Authorization policy – Authorization profile (ISE only)



Authorization Policy Example

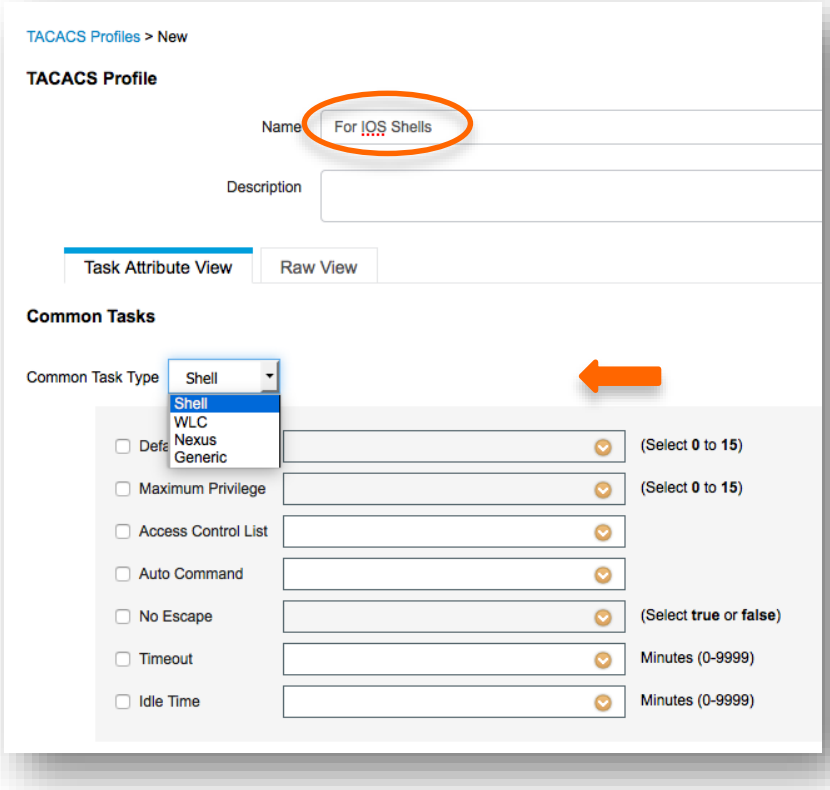
SGT can also be used for enforcement



Authorization policy – Shell Profiles(Device Administration)

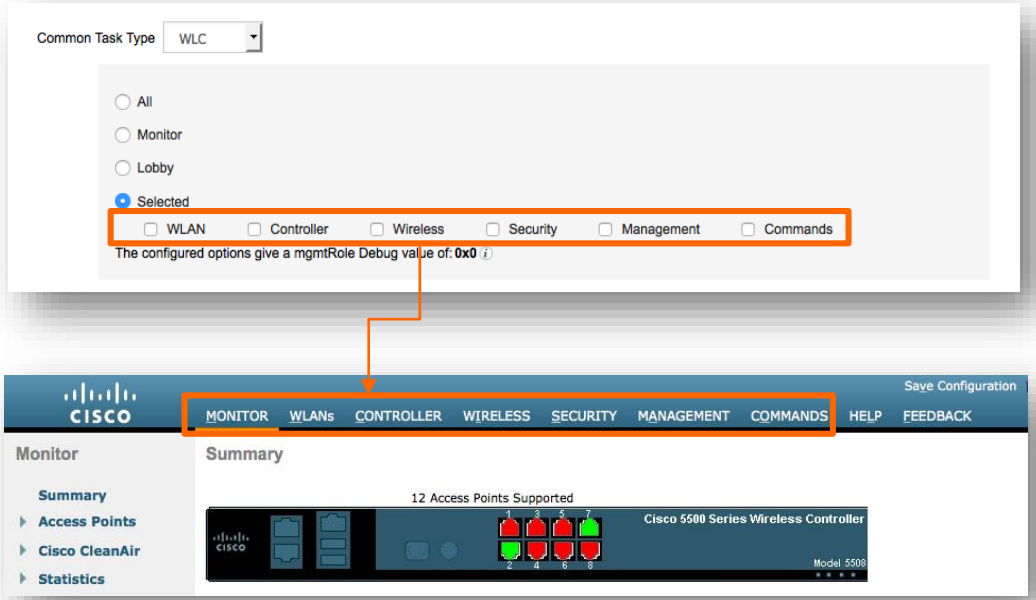
ACS

ISE – IOS devices

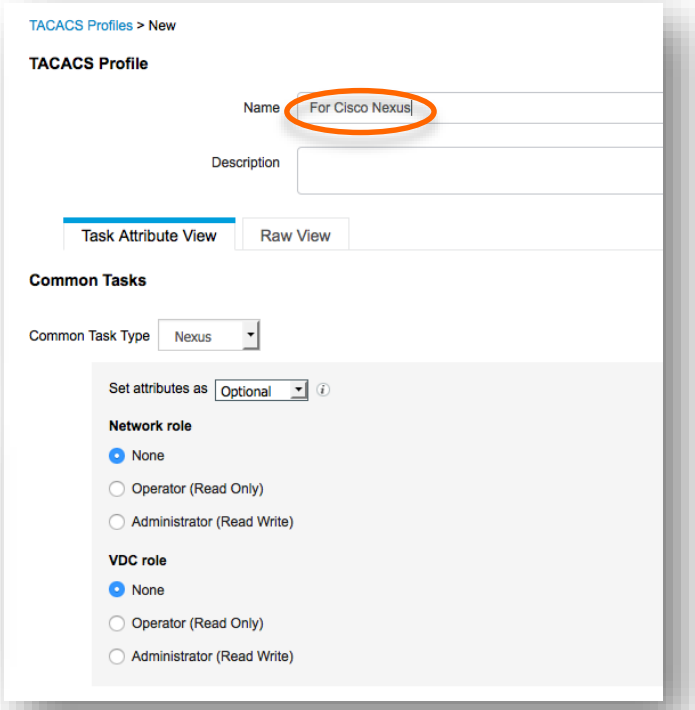


TACACS+ Profile Types (ISE Only)

ISE – WLC devices



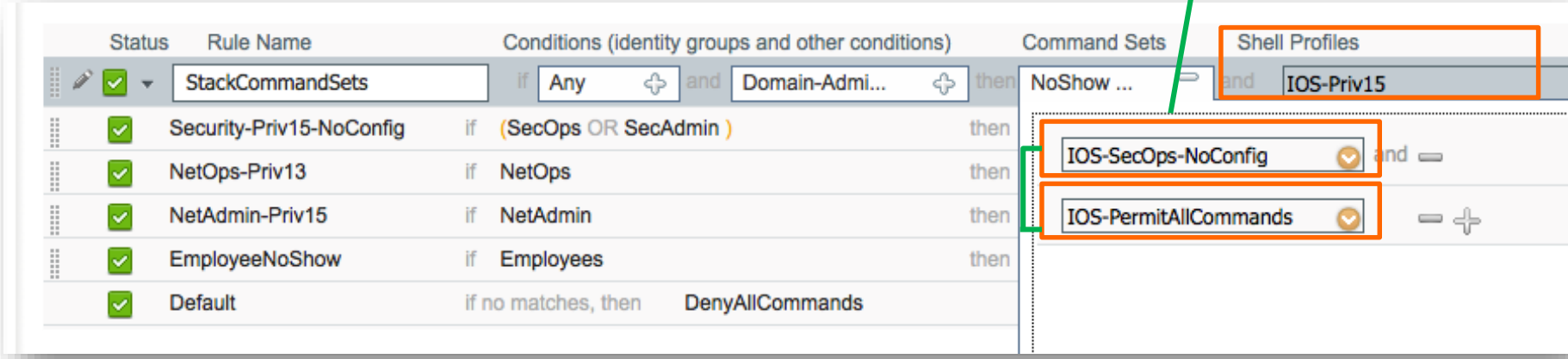
ISE – Nexus devices



Authorization policy Device administration

IOS-SecOps-NoConfig
Deny_Always Config *
Permit Everything Else

IOS-PermitAllCommands
Permit *



ISE Public Resources

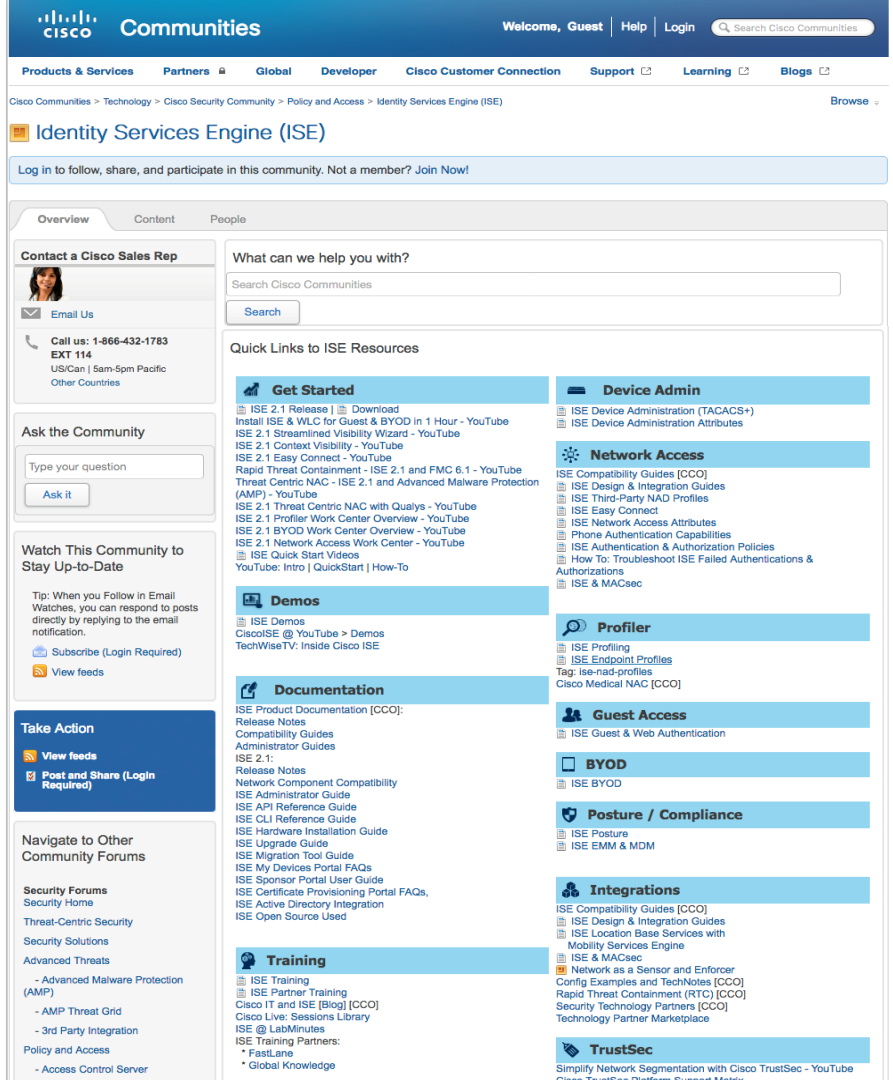
ISE Public Community:
http://cs.co/ise-community

Customer Connection Program:
http://cisco.com/go/ccp > Security

ISE Compatibility Guides:
http://cs.co/ise-compatibility

ISE Design & Integration Guides:
http://cs.co/ise-guides

ISE Licensing / Ordering Guide:
http://cs.co/ise-licensing | http://cs.co/ise-ordering



Thank you.