TOMORROW
starts here.

Advanced ISE Services, Tips and Tricks

BRKSEC-3697

Jason A. Kunst

Technical Marketing Engineer, Secure Access and Mobility

#clmel

Cisco live!

Important: Hidden Slide Alert

Look for this “For Your Reference” Symbol in your PDF’s

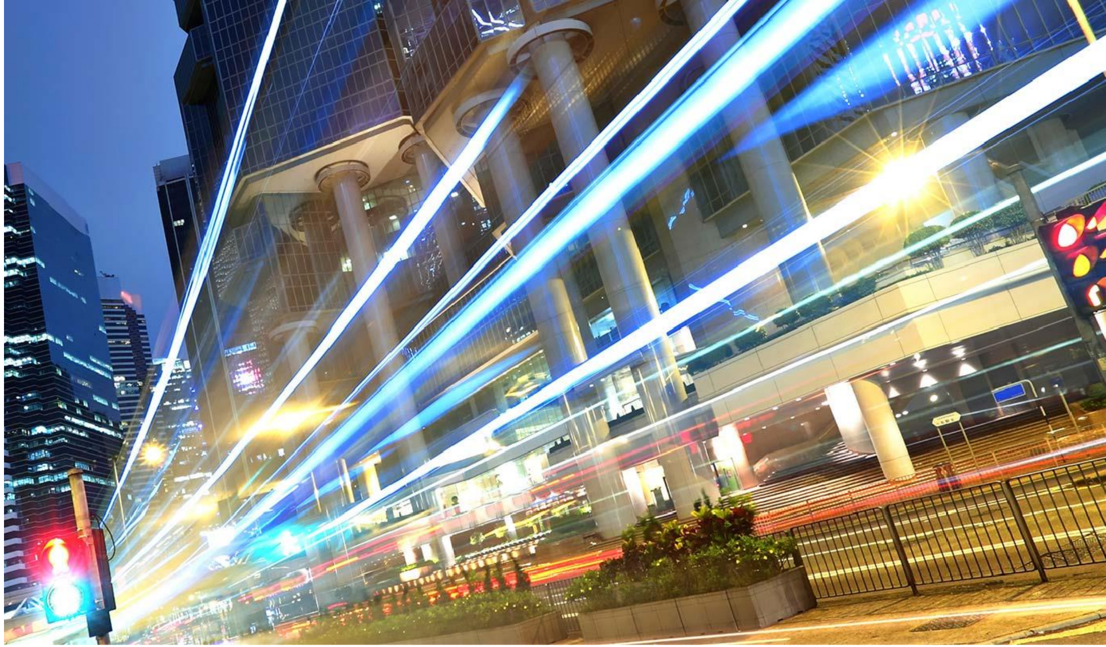
There is a tremendous amount of hidden content, for you to use later!

For Your Reference

**200 +/- Slides in PDF

Agenda

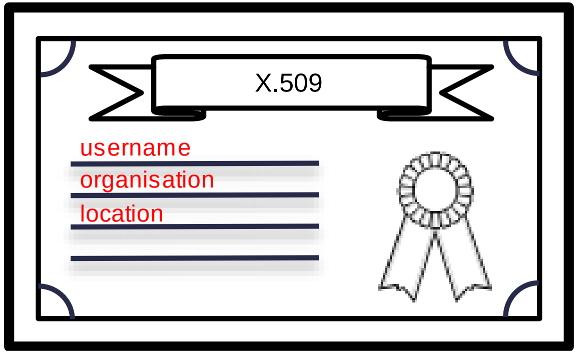
- Introduction
- Certificates, Certificates, Certificates
- BYOD Best Practices
- Integrating with Cisco and Non-Cisco
- ISE in a Security EcoSystem
- Serviceability & Troubleshooting
- Staged Deployments (Time Permitting)
- Conclusion



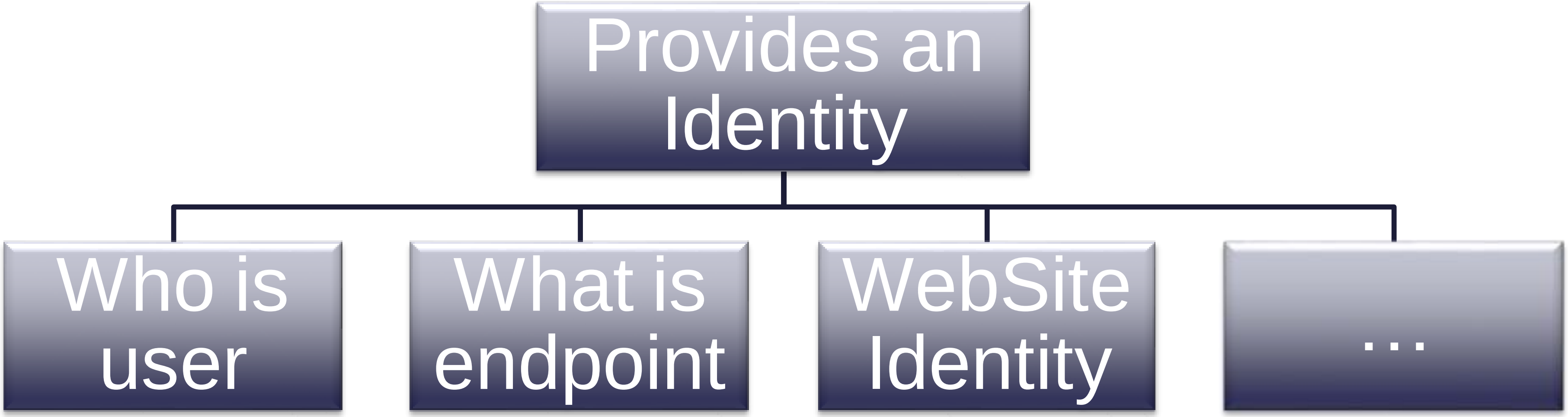
ISE and Certificate Usage

What is an X.509 Certificate

- A Certificate is a signed document…
  - Think of it like a government form of identity



What is the Purpose of an X.509 Certificate?



Provides an Identity

Who is user

What is endpoint

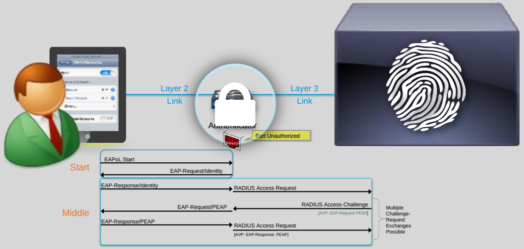
WebSite Identity

…

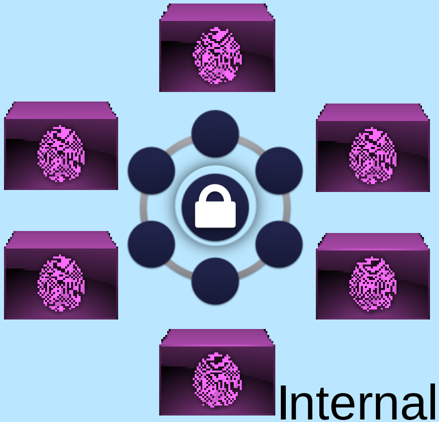
Acts as a seed value for encryption

ISE and Certificates: Multiple Identities

Authentication Server



Secure
Web Server

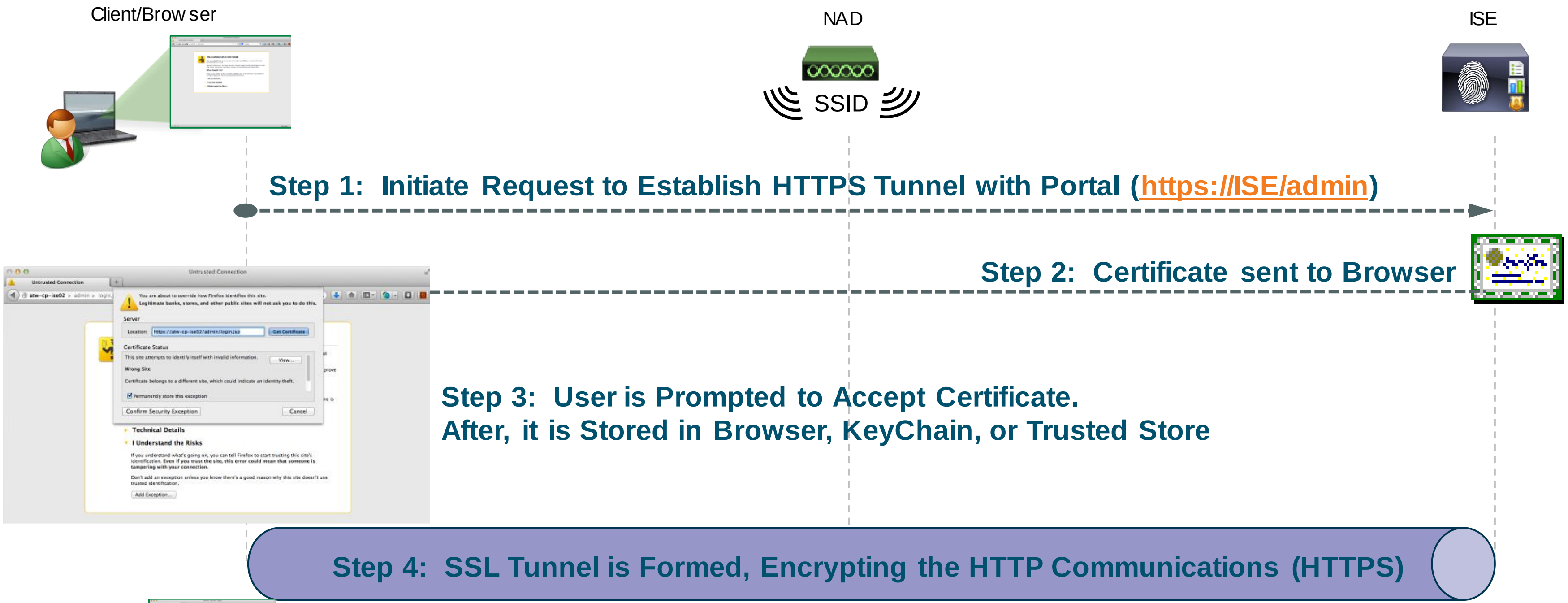


Internal
Communications

Root CA

Certificates and Web Portals

- All Web Portals (Admin, WebAuth, MyDevices, Sponsor, CPP, etc.)



Step 1: Initiate Request to Establish HTTPS Tunnel with Portal (https://ISE/admin)

Step 2: Certificate sent to Browser

Untrusted Connection

Untrusted Connection

atw-cp-ise02 › admin › login.

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://atw-cp-ise02/admin/login.jsp [Get Certificate]

Certificate Status

This site attempts to identify itself with invalid information. [View...]

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

☑ Permanently store this exception

[Confirm Security Exception] [Cancel]

Technical Details

I Understand the Risks

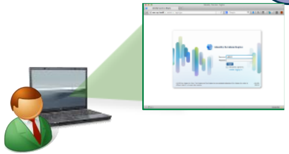
If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

[Add Exception...]

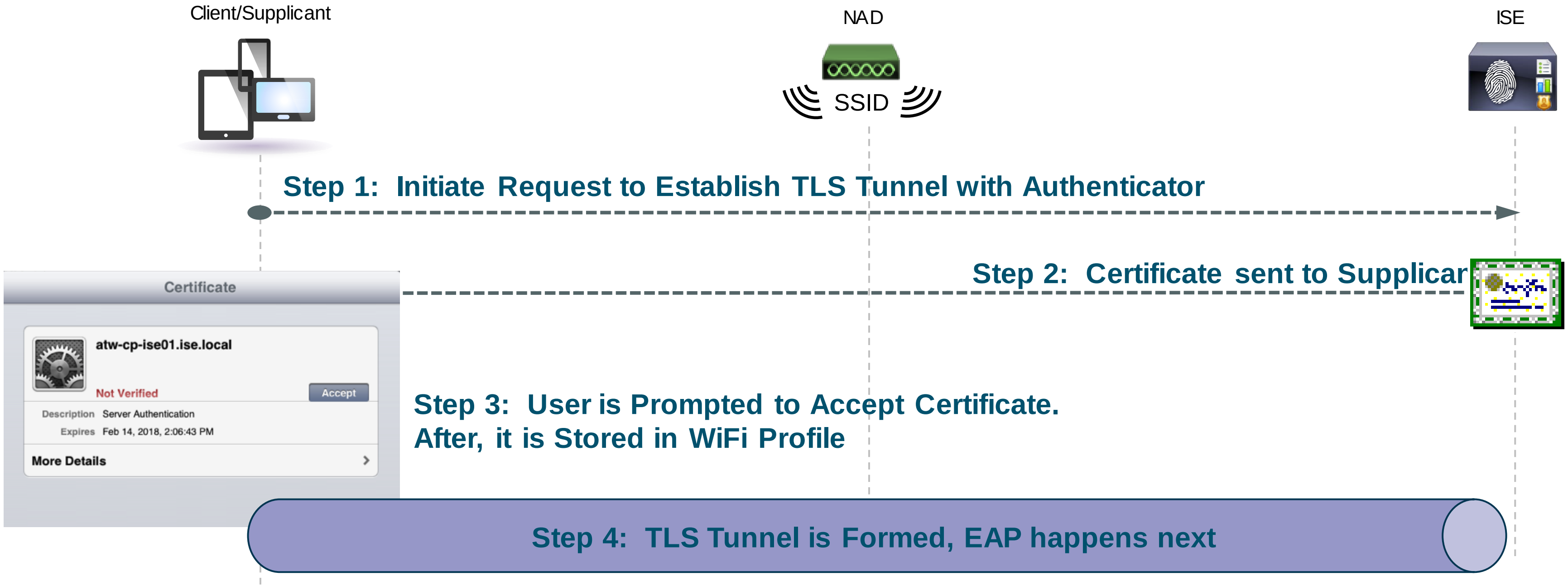
Step 3: User is Prompted to Accept Certificate.
After, it is Stored in Browser, KeyChain, or Trusted Store

Step 4: SSL Tunnel is Formed, Encrypting the HTTP Communications (HTTPS)



Certificates and EAP Communication

- EAP Connections (PEAP, FAST, EAP-TLS)



Step 1: Initiate Request to Establish TLS Tunnel with Authenticator

Step 2: Certificate sent to Supplicar

Certificate

atw-cp-ise01.ise.local

Not Verified

Accept

Description Server Authentication

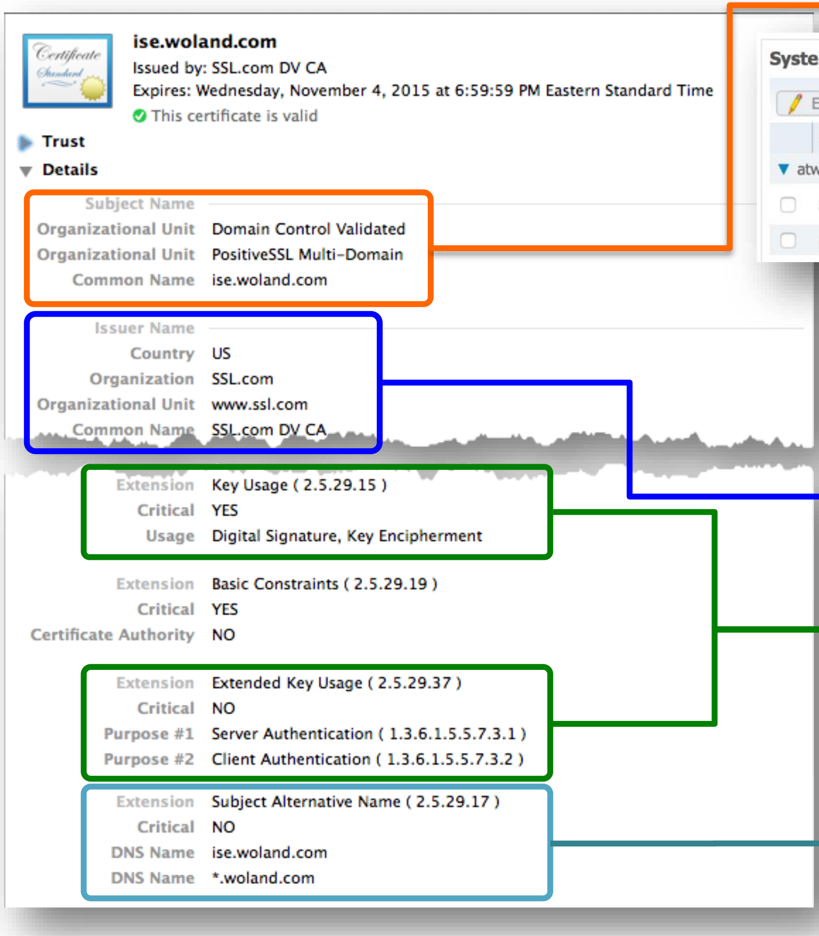
Expires Feb 14, 2018, 2:06:43 PM

More Details >

Step 3: User is Prompted to Accept Certificate. After, it is Stored in WiFi Profile

Step 4: TLS Tunnel is Formed, EAP happens next

ISE Admin/EAP/Portal Certificate Examination

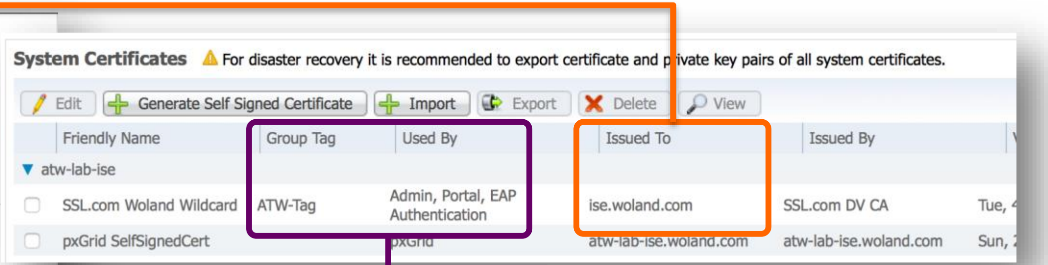


ise.woland.com
Issued by: SSL.com DV CA
Expires: Wednesday, November 4, 2015 at 6:59:59 PM Eastern Standard Time
✓ This certificate is valid

▶ **Trust**

▼ **Details**

Subject Name	
Organizational Unit	Domain Control Validated
Organizational Unit	PositiveSSL Multi-Domain
Common Name	ise.woland.com
Issuer Name	
Country	US
Organization	SSL.com
Organizational Unit	www.ssl.com
Common Name	SSL.com DV CA
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Digital Signature, Key Encipherment
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	ise.woland.com
DNS Name	*.woland.com



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Group Tag	Used By	Issued To	Issued By	
▼ atw-lab-ise						
□	SSL.com Woland Wildcard	ATW-Tag	Admin, Portal, EAP Authentication	ise.woland.com	SSL.com DV CA	Tue, 4
□	pxGrid SelfSignedCert		pxGrid	atw-lab-ise.woland.com	atw-lab-ise.woland.com	Sun, 2

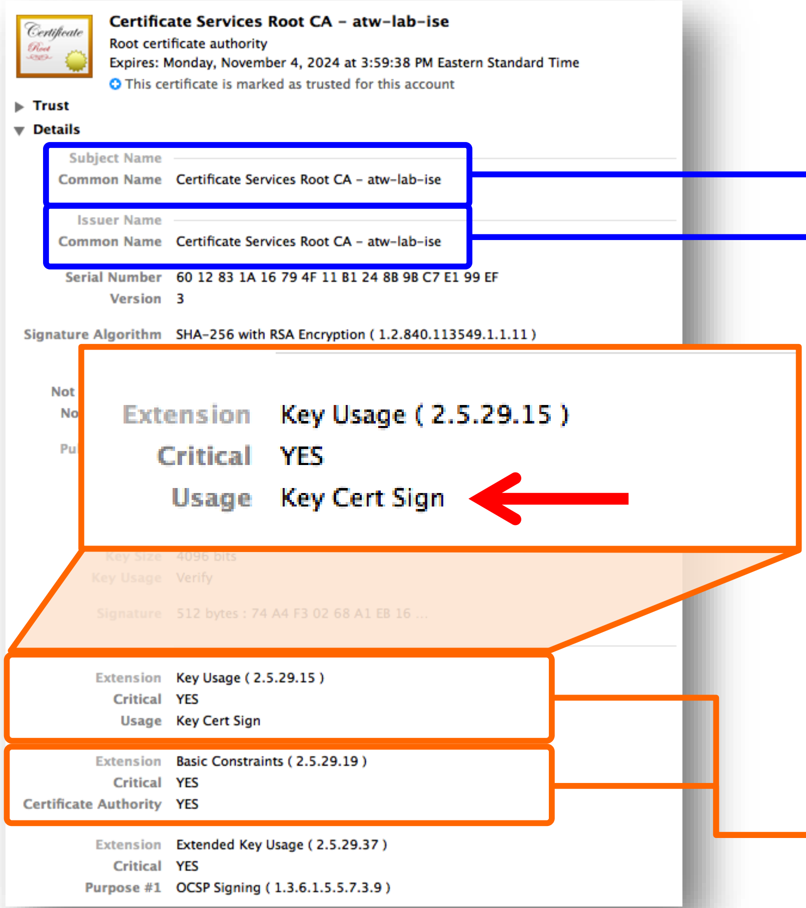
Used for Admin, Portal and EAP.
Any Portal using ATW-Tag uses Cert.

Publically Signed Certificate

Purpose is for Client and Server Auth

SAN includes Wildcard and the CN

ISE Root Certificate Examination

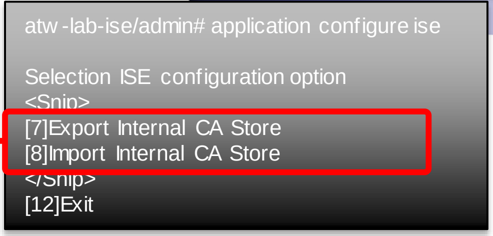


Certificate Services Root CA – atw-lab-ise
Root certificate authority
Expires: Monday, November 4, 2024 at 3:59:38 PM Eastern Standard Time
This certificate is marked as trusted for this account

▶ Trust
▼ Details

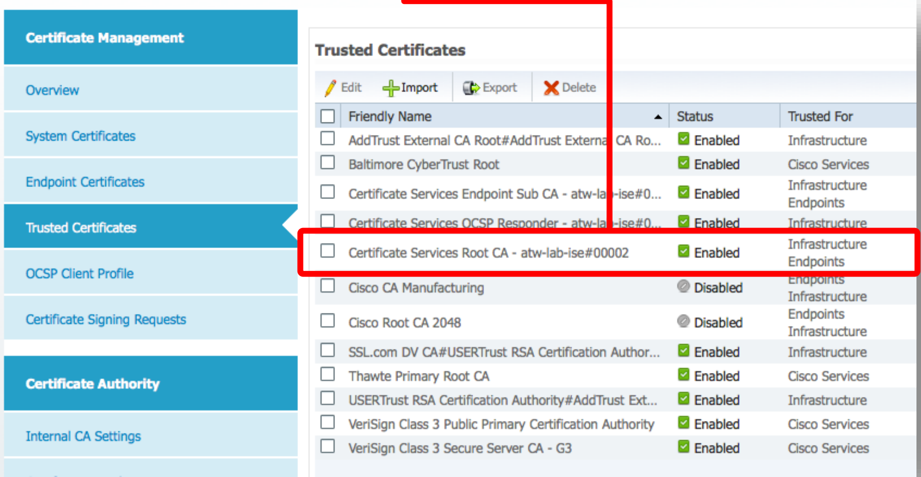
Subject Name	
Common Name	Certificate Services Root CA – atw-lab-ise
Issuer Name	
Common Name	Certificate Services Root CA – atw-lab-ise
Serial Number	60 12 83 1A 16 79 4F 11 B1 24 8B 9B C7 E1 99 EF
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Key Size	4096 bits
Key Usage	Verify
Signature	512 bytes : 74 A4 F3 02 68 A1 EB 16 ...
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Extended Key Usage (2.5.29.37)
Critical	YES
Purpose #1	OCSP Signing (1.3.6.1.5.5.7.3.9)

Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign



```
atw -lab-ise/admin# application configure ise

Selection ISE configuration option
<Snip>
[7]Export Internal CA Store
[8]Import Internal CA Store
</Snip>
[12]Exit
```

Only way to Access The Root Certificate



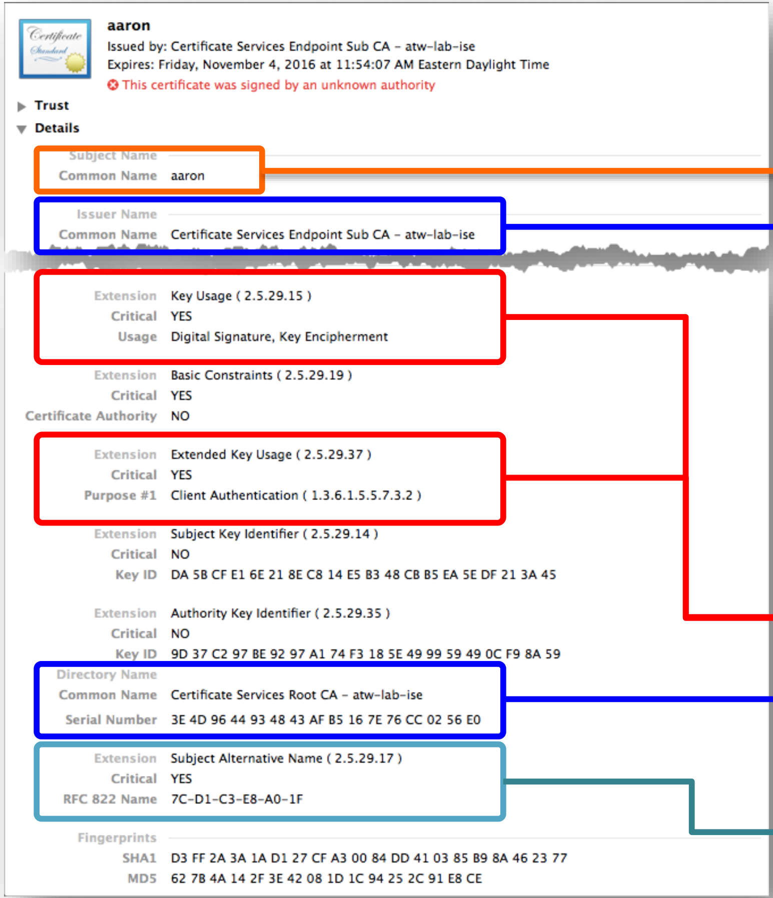
Trusted Certificates

□	Friendly Name	Status	Trusted For
□	AddTrust External CA Root#AddTrust External CA Ro...	✓ Enabled	Infrastructure
□	Baltimore CyberTrust Root	✓ Enabled	Cisco Services
□	Certificate Services Endpoint Sub CA - atw-lab-ise#0...	✓ Enabled	Infrastructure Endpoints
□	Certificate Services OCSP Responder - atw-lab-ise#0...	✓ Enabled	Infrastructure
□	Certificate Services Root CA - atw-lab-ise#00002	✓ Enabled	Infrastructure Endpoints
□	Cisco CA Manufacturing	⊘ Disabled	Endpoints Infrastructure
□	Cisco Root CA 2048	⊘ Disabled	Endpoints Infrastructure
□	SSL.com DV CA#USERTrust RSA Certification Author...	✓ Enabled	Infrastructure
□	Thawte Primary Root CA	✓ Enabled	Cisco Services
□	USERTrust RSA Certification Authority#AddTrust Ext...	✓ Enabled	Infrastructure
□	VeriSign Class 3 Public Primary Certification Authority	✓ Enabled	Cisco Services
□	VeriSign Class 3 Secure Server CA - G3	✓ Enabled	Cisco Services

Self Signed Certificate (It's a Root Cert)

Purpose is for Cert Signing / It is a CA

Endpoint Certificate Examination



aaron
Issued by: Certificate Services Endpoint Sub CA – atw-lab-ise
Expires: Friday, November 4, 2016 at 11:54:07 AM Eastern Daylight Time
This certificate was signed by an unknown authority

▶ Trust
▼ Details

Subject Name
Common Name aaron

Issuer Name
Common Name Certificate Services Endpoint Sub CA – atw-lab-ise

Extension Key Usage (2.5.29.15)
Critical YES
Usage Digital Signature, Key Encipherment

Extension Basic Constraints (2.5.29.19)
Critical YES
Certificate Authority NO

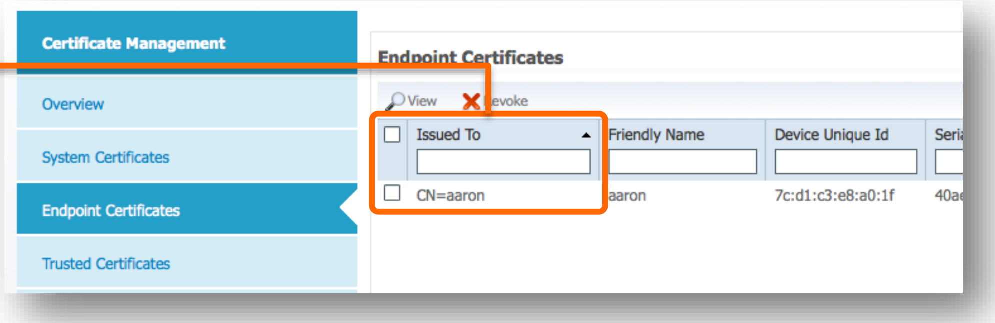
Extension Extended Key Usage (2.5.29.37)
Critical YES
Purpose #1 Client Authentication (1.3.6.1.5.5.7.3.2)

Extension Subject Key Identifier (2.5.29.14)
Critical NO
Key ID DA 5B CF E1 6E 21 8E C8 14 E5 B3 48 CB B5 EA 5E DF 21 3A 45

Extension Authority Key Identifier (2.5.29.35)
Critical NO
Key ID 9D 37 C2 97 BE 92 97 A1 74 F3 18 5E 49 99 59 49 0C F9 8A 59
Directory Name
Common Name Certificate Services Root CA – atw-lab-ise
Serial Number 3E 4D 96 44 93 48 43 AF B5 16 7E 76 CC 02 56 E0

Extension Subject Alternative Name (2.5.29.17)
Critical YES
RFC 822 Name 7C-D1-C3-E8-A0-1F

Fingerprints
SHA1 D3 FF 2A 3A 1A D1 27 CF A3 00 84 DD 41 03 85 B9 8A 46 23 77
MD5 62 7B 4A 14 2F 3E 42 08 1D 1C 94 25 2C 91 E8 CE



□	Issued To	Friendly Name	Device Unique Id	Seri
□	CN=aaron	aaron	7c:d1:c3:e8:a0:1f	40ae

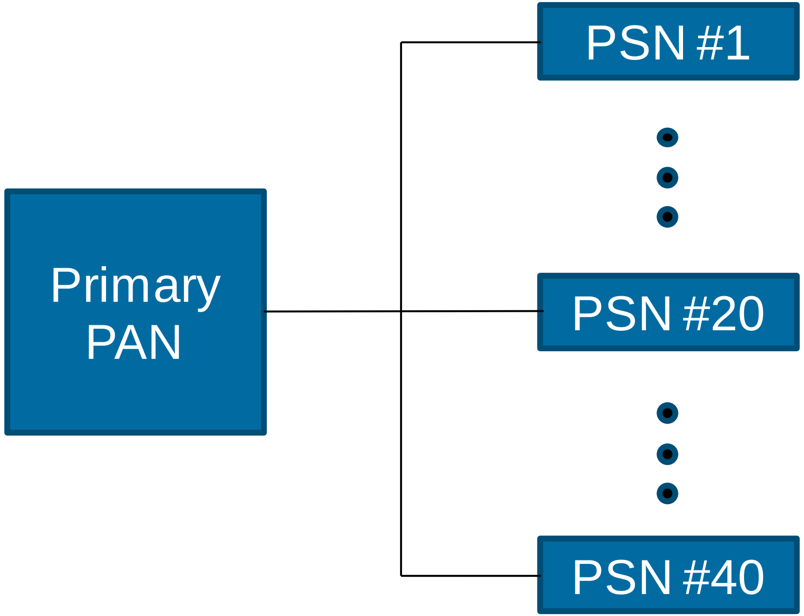
Signed by ISE Sub-CA

Purpose is for Client Auth

SAN includes MAC Address

Certificate Provisioning User Experience in ISE 1.0 – 1.2

- Generate CSR for Primary PAN
- Bind CA-signed cert for Primary PAN



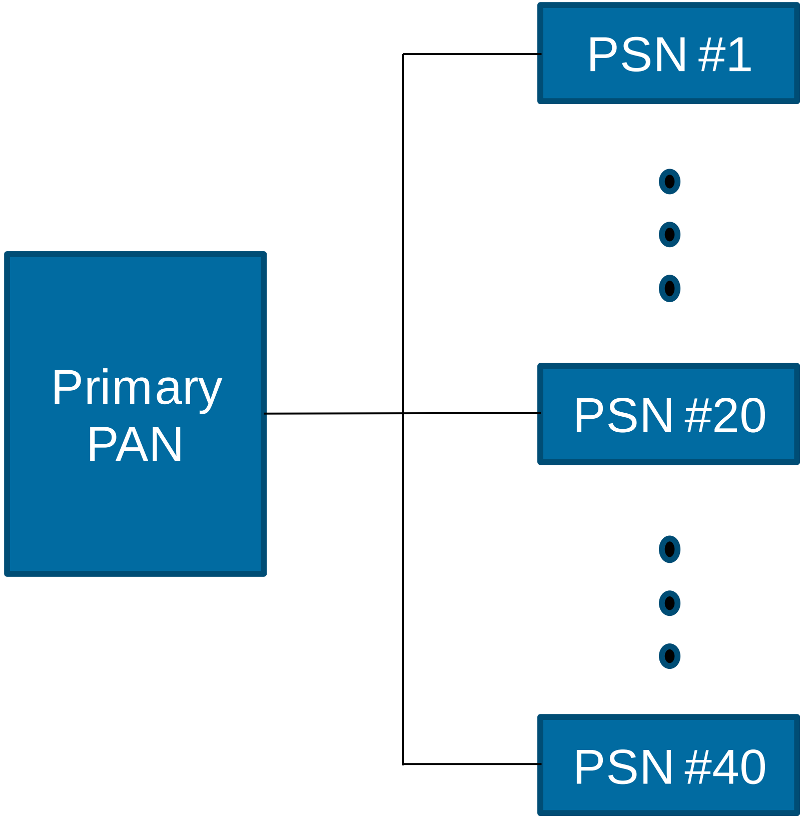
- Generate CSR for PSN #1
- Bind CA-signed cert for PSN #1

- Generate CSR for PSN #20
- Bind CA-signed cert for PSN #20

- Generate CSR for PSN #40
- Bind CA-signed cert for PSN #40

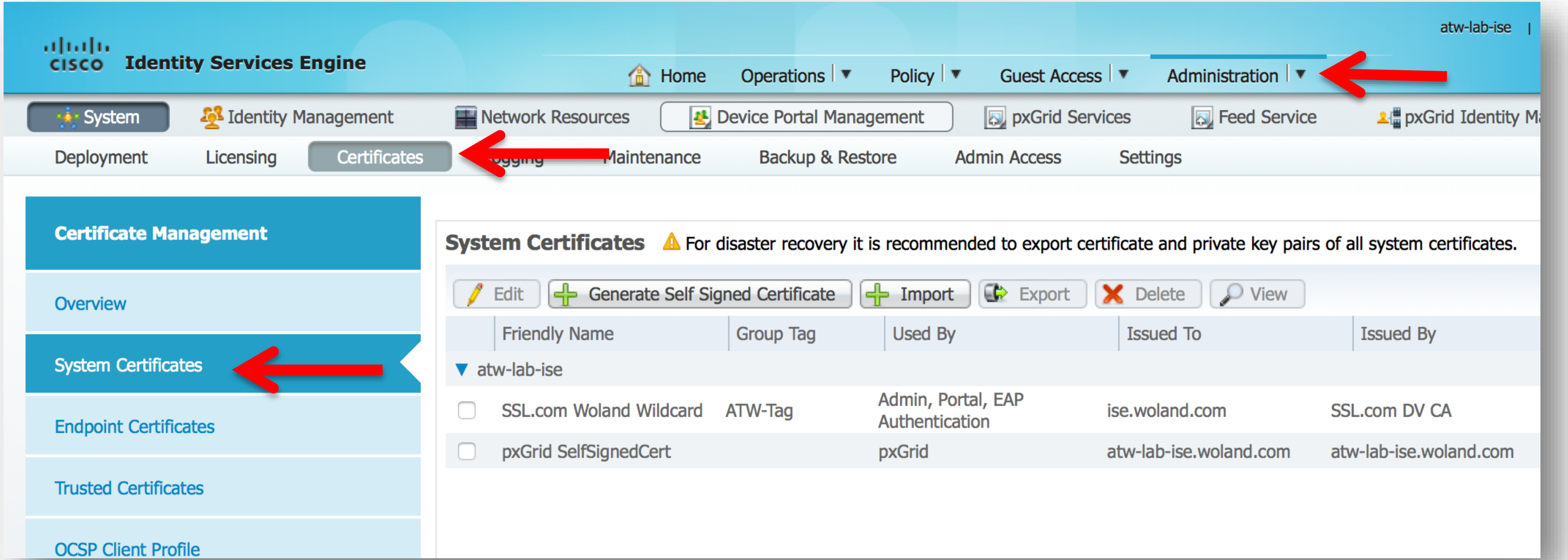
Centralised Certificate Management in 1.3

- Generate CSRs for **ALL NODES** at Primary PAN
- Bind CA-signed certs for **ALL NODES** at Primary PAN
- Manage System (Local) certs for **ALL NODES** at primary PAN



Manage System Certificates

- Certificates used by: Admin, HTTPS Portals, pxGrid, EAP
- These are Private/Public Key Pairs – i.e.: They Identify ISE Personalities

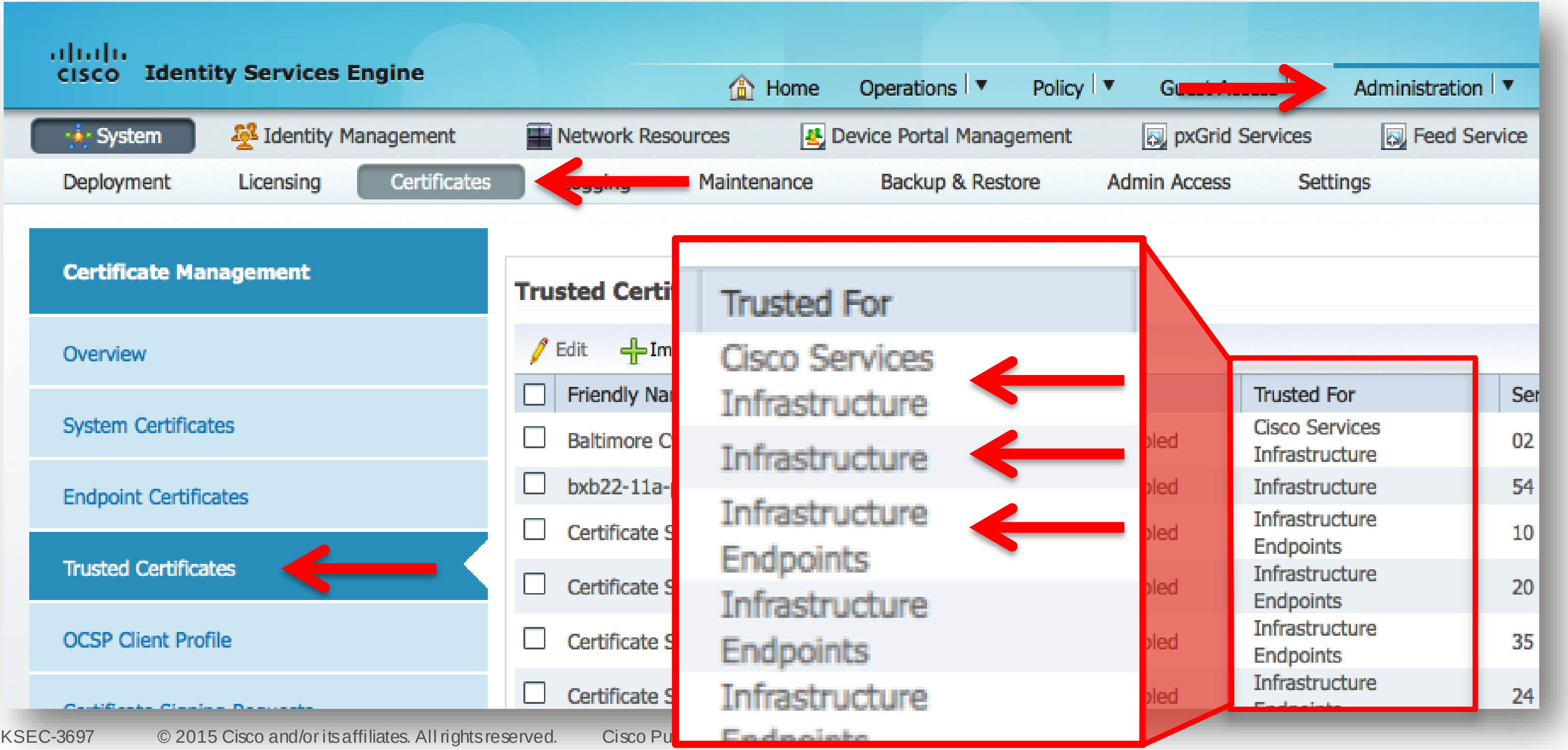


System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Group Tag	Used By	Issued To	Issued By
▼ atw-lab-ise					
□	SSL.com Woland Wildcard	ATW-Tag	Admin, Portal, EAP Authentication	ise.woland.com	SSL.com DV CA
□	pxGrid SelfSignedCert		pxGrid	atw-lab-ise.woland.com	atw-lab-ise.woland.com

Certificates Your ISE Cube will “Trust”

- Trust for EAP, MDM, etc.
- These are copies of their Public Certs. I.e.: They Identify Other Systems

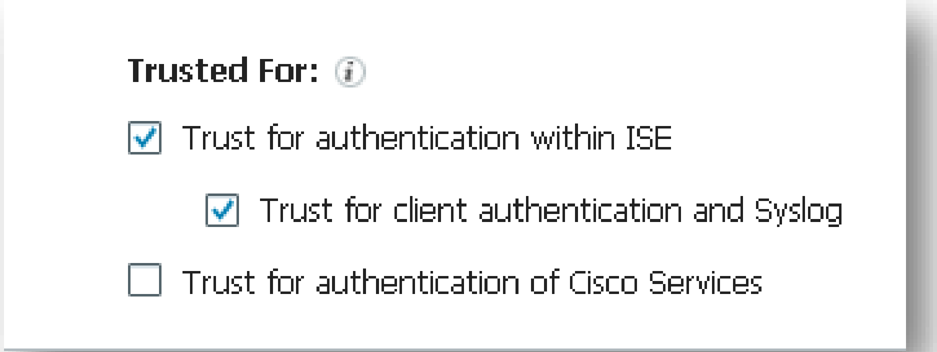


Trusted Certi

Friendly Na		Trusted For	Ser
Baltimore C	bled	Cisco Services Infrastructure	02
bxb22-11a-	bled	Infrastructure	54
Certificate S	bled	Infrastructure Endpoints	10
Certificate S	bled	Infrastructure Endpoints	20
Certificate S	bled	Infrastructure Endpoints	35
Certificate S	bled	Infrastructure Endpoints	24

Trusted Certificates

- In 1.3, trusted certificates have a new “Trusted For” attribute.
  - Security Goal: to prevent the public certificates used for Cisco Services from being used internally.
- When importing a trust certificate, the user must specify what the certificate is trusted for.
- It is important to select at least one category, or the cert will not be used in any trust store.



Trusted For:

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

□ Trust for authentication of Cisco Services

System Certificate Roles – ISE 1.3

1.2 Role Name	1.3 Role Name	How Many	May Use Wildcard (*) in SAN	May use Wildcard (*) in Subject
HTTPS	Admin	1	Yes	Yes
EAP	EAP Authentication	1	Yes	No[1]
-	pxGrid	1	No	No
-	Portal	Many	Yes	Yes

- ‘Admin’ cert is the server cert for the Admin Console
- ‘pxGrid’ cert is the server cert for authenticating the ISE node to pxGrid clients
- ‘Portal’ cert is a server cert associated with a particular ISE portal (Guest, Sponsor, My Devices, …)
- In a freshly installed node, the default self-signed cert has all four roles

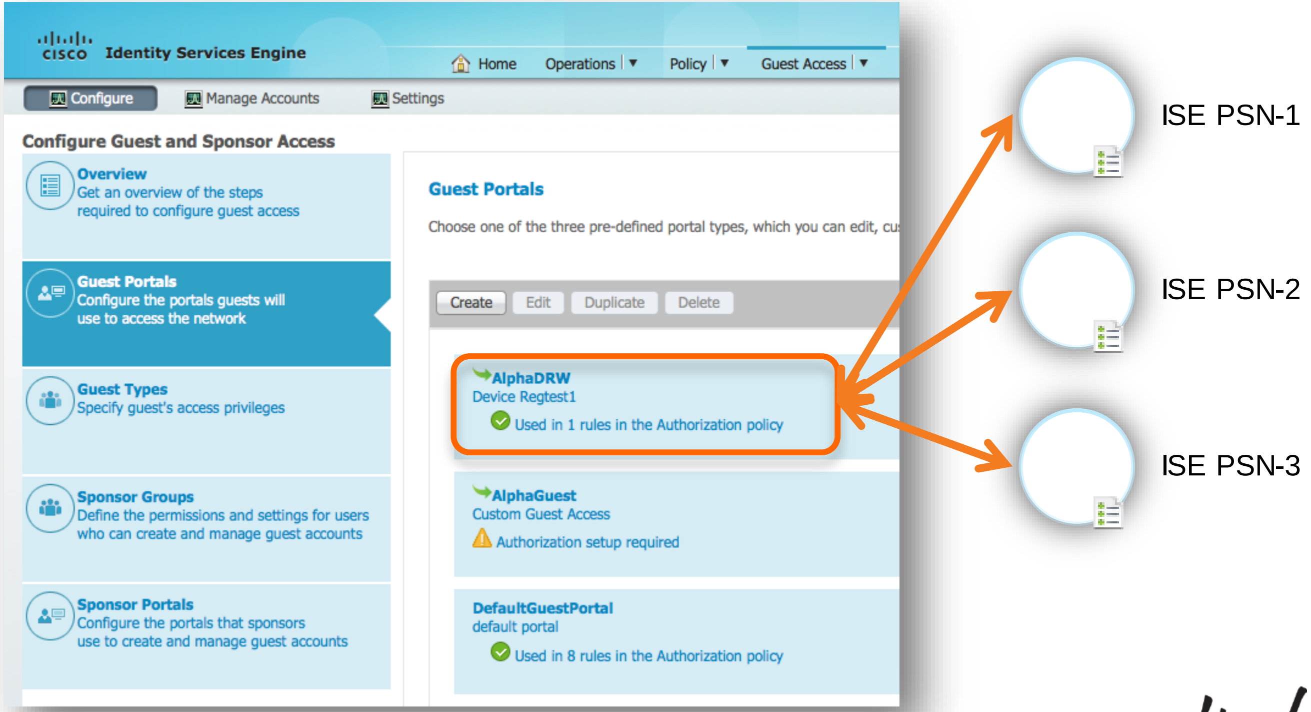
Certificates for <u>all</u> roles are managed from the Primary PAN node.

[1] While ISE technically allows wildcard in the CN, Microsoft supplicants will reject, so never recommended

ISE 1.3: Multiple Web Portals

Each Portal Could Use A Different Certificate

- Each Portal Exists on ALL PSN’s
- Each Portal Requires a Certificate
- One Certificate per Interface > IP:Port
- Each PSN Could Have Unique Certificates (Identity)



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

Guest Portals

Choose one of the three pre-defined portal types, which you can edit, cu

AlphaDRW
Device Regtest1
✓ Used in 1 rules in the Authorization policy

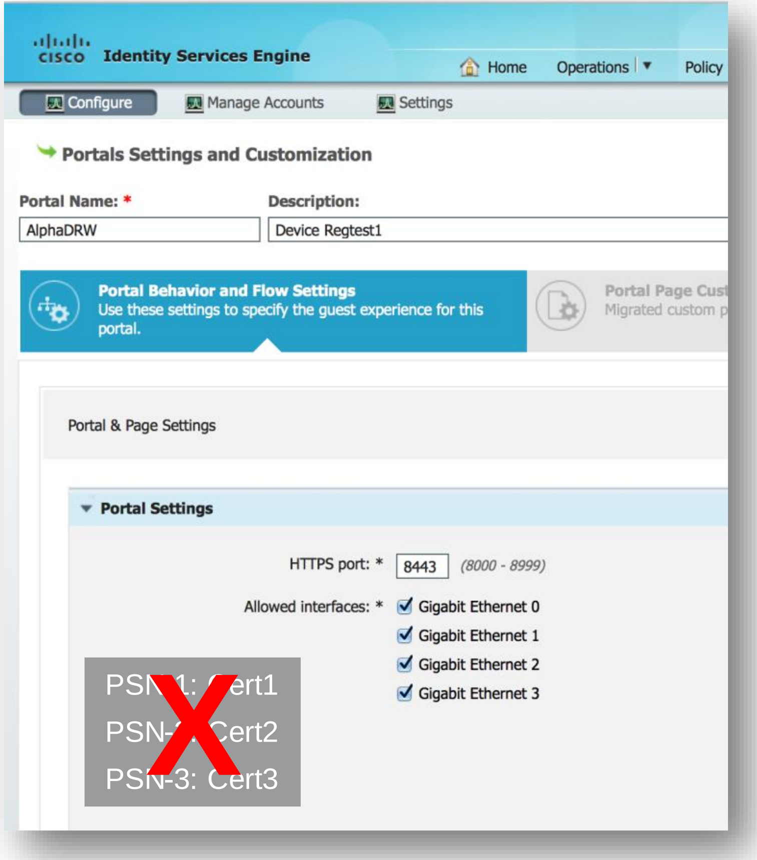
AlphaGuest
Custom Guest Access
⚠ Authorization setup required

DefaultGuestPortal
default portal
✓ Used in 8 rules in the Authorization policy

Problem: Assign Certificate on All PSNs to Portal?

How To Assign "At Scale"

- New UI Paradigm with ISE 1.3 is to Keep All Portal Configuration Together.
- Options:
  - Add complexity to the Portal Configuration Page by Choosing Certificates on Each Node?
    - What about Large Deployments (40 PSNs)?
  - Configure it entirely outside of the Portal Configuration screen?
  - Some way to combine?



Portals Settings and Customization

Portal Name: * AlphaDRW

Description: Device Regtest1

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

▾ Portal Settings

HTTPS port: * 8443 (8000 - 8999)

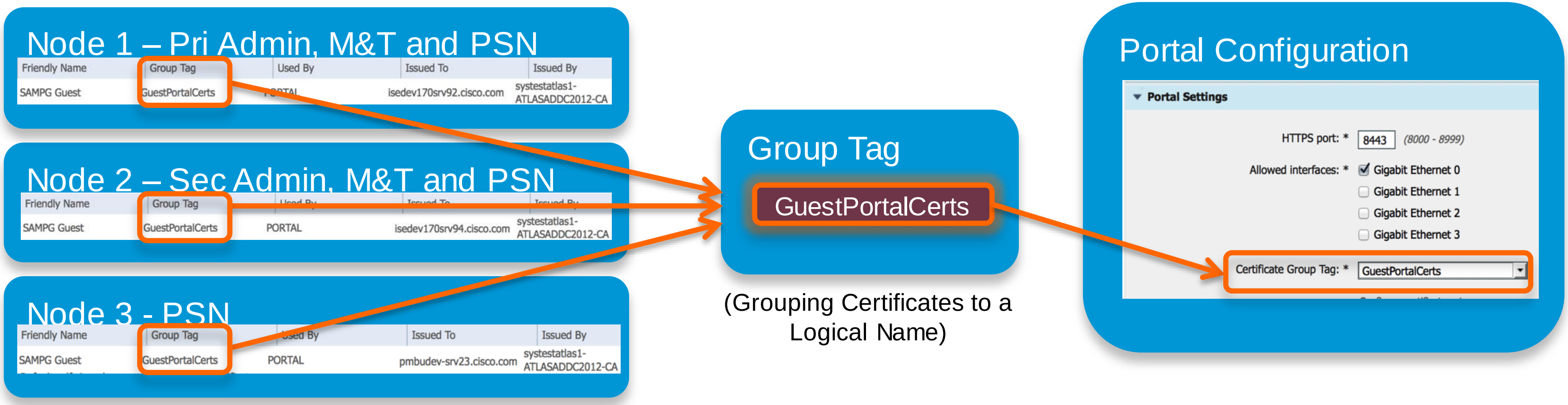
Allowed interfaces: *
☑ Gigabit Ethernet 0
☑ Gigabit Ethernet 1
☑ Gigabit Ethernet 2
☑ Gigabit Ethernet 3

PSN-1: Cert1
PSN-2: Cert2
PSN-3: Cert3

X

Solution: Portal Certificate Group Tag

- **Portal Certificate Group Tag** provides a solution to configure node-specific certificates for Portal configuration by associating node certificates to a logical name.



Node 1 – Pri Admin, M&T and PSN

Friendly Name	Group Tag	Used By	Issued To	Issued By
SAMPG Guest	GuestPortalCerts	PORTAL	isedev170srv92.cisco.com	systestatlas1-ATLASADDC2012-CA

Node 2 – Sec Admin, M&T and PSN

Friendly Name	Group Tag	Used By	Issued To	Issued By
SAMPG Guest	GuestPortalCerts	PORTAL	isedev170srv94.cisco.com	systestatlas1-ATLASADDC2012-CA

Node 3 - PSN

Friendly Name	Group Tag	Used By	Issued To	Issued By
SAMPG Guest	GuestPortalCerts	PORTAL	pmbudev-srv23.cisco.com	systestatlas1-ATLASADDC2012-CA

Group Tag

GuestPortalCerts

(Grouping Certificates to a Logical Name)

Portal Configuration

▼ Portal Settings

HTTPS port: * 8443 (8000 - 8999)

Allowed interfaces: * ☑ Gigabit Ethernet 0

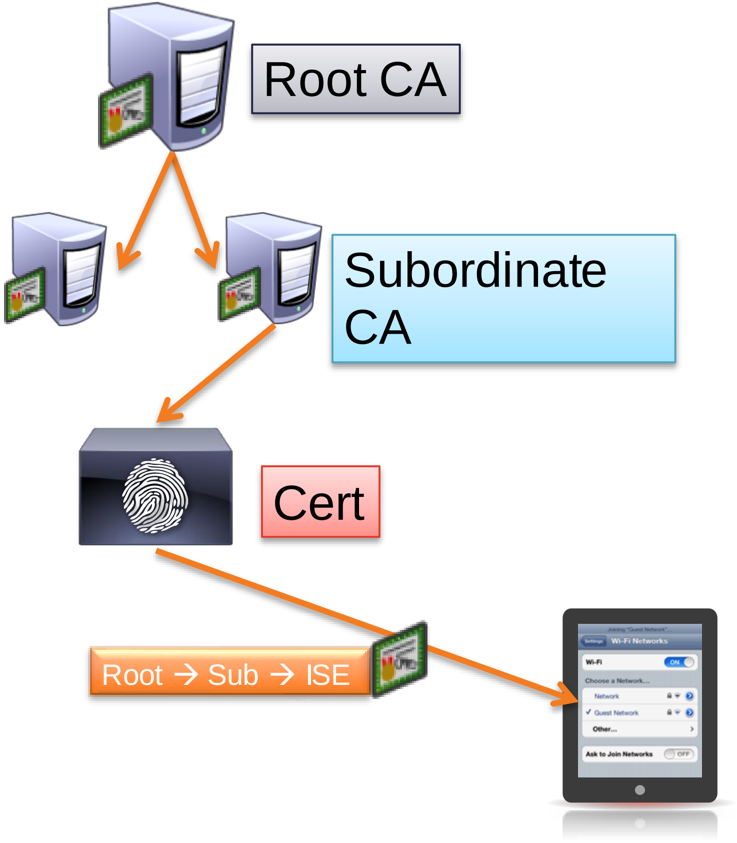
☐ Gigabit Ethernet 1

☐ Gigabit Ethernet 2

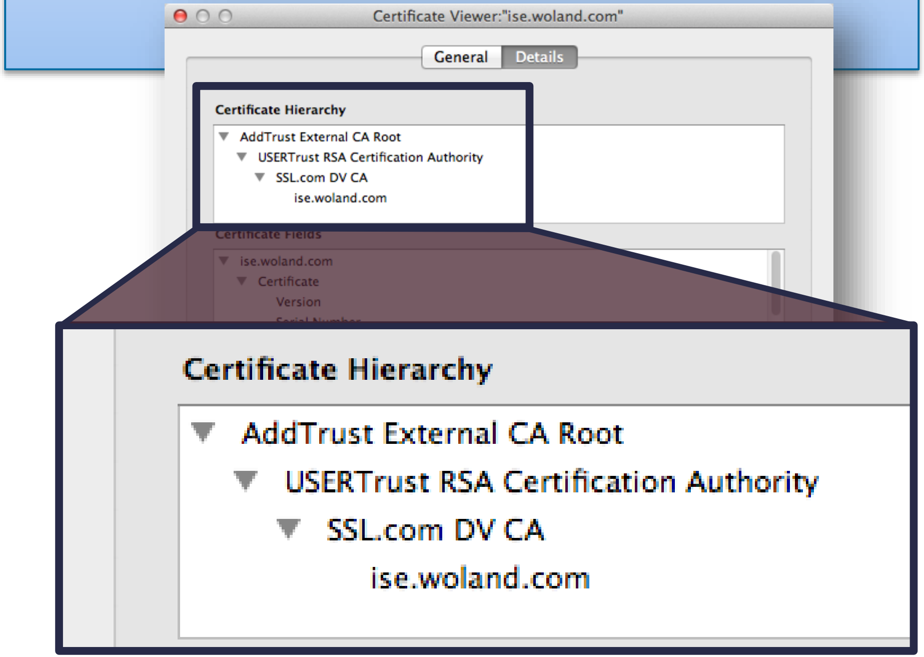
☐ Gigabit Ethernet 3

Certificate Group Tag: * GuestPortalCerts

Certificate Chains



- For Scalability, X.509 Certificate Authorities may have hierarchy
- ISE will present full signing chain to client during authentication
  - Client must trust each CA within the chain



Certificate Hierarchy

- AddTrust External CA Root
  - USERTrust RSA Certification Authority
    - SSL.com DV CA
      - ise.woland.com

Certificate Fields

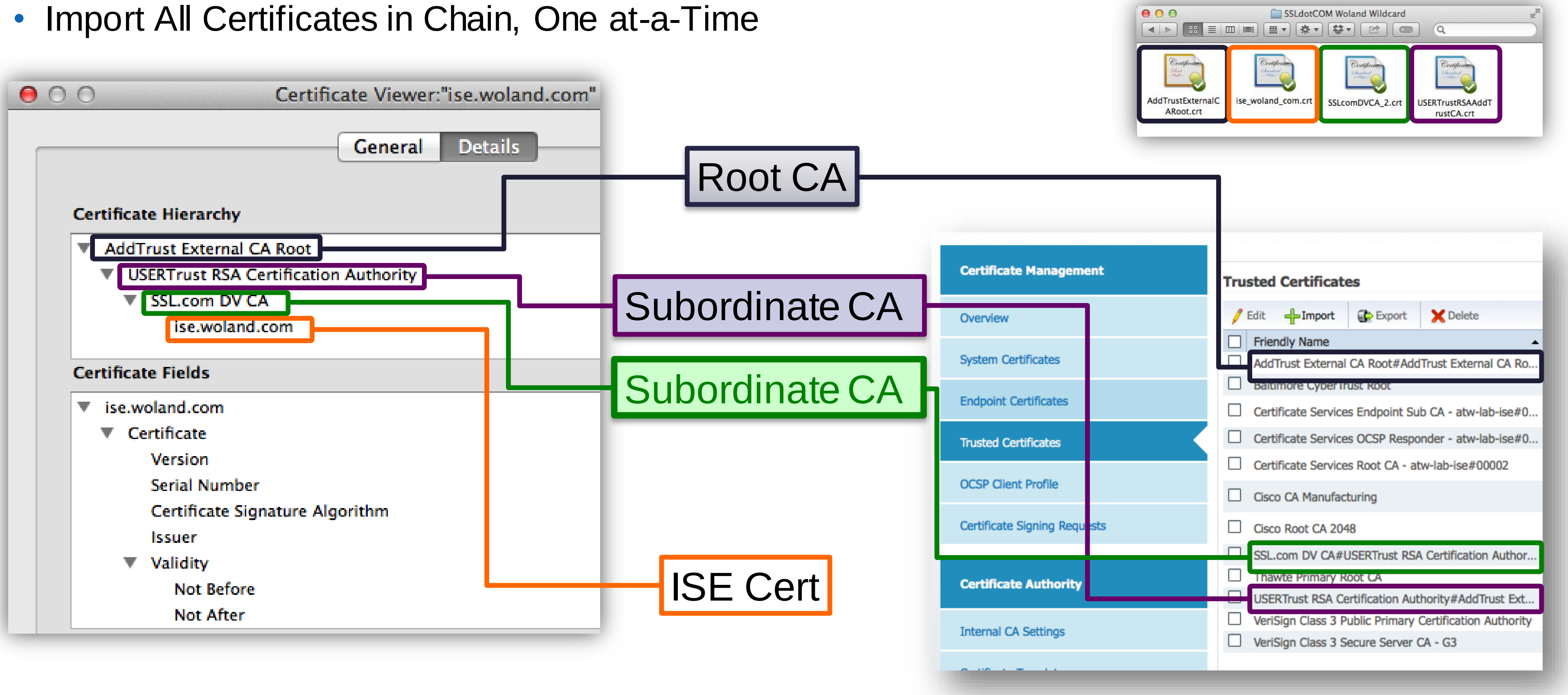
- ise.woland.com
  - Certificate
    - Version
    - Serial Number

Certificate Hierarchy

- AddTrust External CA Root
  - USERTrust RSA Certification Authority
    - SSL.com DV CA
      - ise.woland.com

Always Add the Root and Subordinate CA's

- Import All Certificates in Chain, One at-a-Time



Certificate Hierarchy

- AddTrust External CA Root
  - USERTrust RSA Certification Authority
    - SSL.com DV CA
      - ise.woland.com

Certificate Fields

- ise.woland.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before
      - Not After

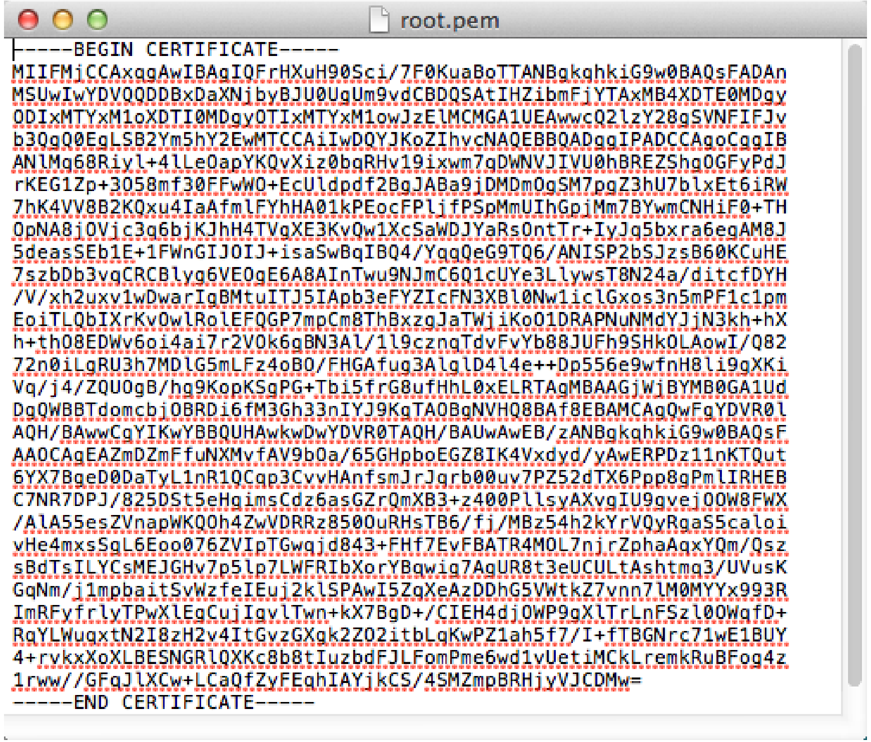
Trusted Certificates

□	Friendly Name
□	AddTrust External CA Root#AddTrust External CA Ro...
□	Baltimore CyberTrust Root
□	Certificate Services Endpoint Sub CA - atw-lab-ise#0...
□	Certificate Services OCSP Responder - atw-lab-ise#0...
□	Certificate Services Root CA - atw-lab-ise#00002
□	Cisco CA Manufacturing
□	Cisco Root CA 2048
□	SSL.com DV CA#USERTrust RSA Certification Author...
□	Thawte Primary Root CA
□	USERTrust RSA Certification Authority#AddTrust Ext...
□	VeriSign Class 3 Public Primary Certification Authority
□	VeriSign Class 3 Secure Server CA - G3

If you must use a PKCS chain, it needs to be in PEM format (not DER)

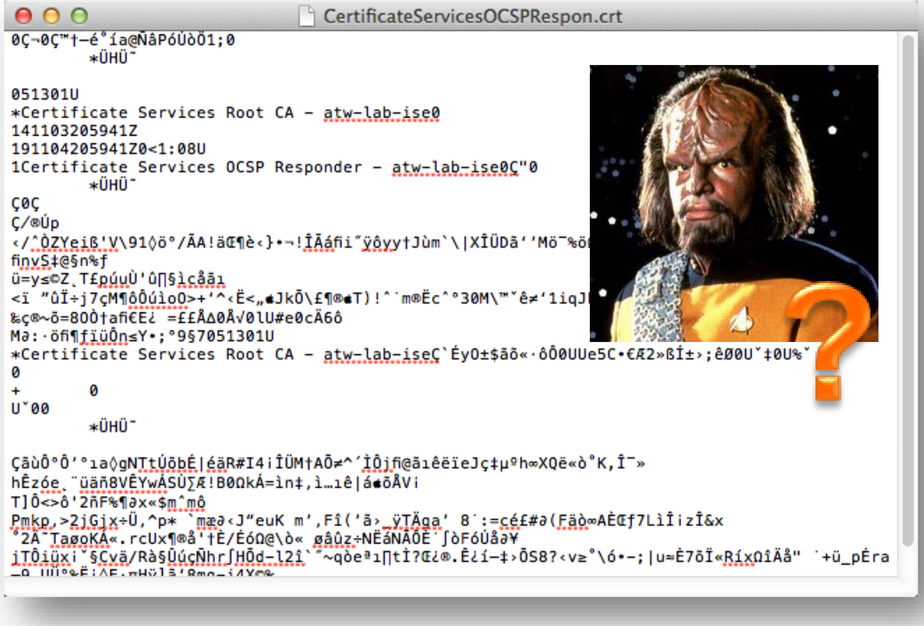
PEM versus DER

PEM



```
-----BEGIN CERTIFICATE-----
MIIFMjCCAxqgAwIBAgIQFrHXuH90Sci/7F0KuaBoTTANBgkqhkiG9w0BAQsFADAn
MSUwIwYDVQQDDBxDaXNjbyBJU0UgUm9vdCBDQSAtIHZibmFjYTAxMB4XDTE0MDgy
ODIxMTYxM1oXDTI0MDgyOTIxMTYxM1owJzElMCMGA1UEAwwcQ2lzY28gSVNFIFJv
b3QgQ0EgLSB2Ym5hY2EwMTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIB
ANlMq68Riyl+4lLeOapYKQvXiz0bqRHv19ixwm7qDWNVJIVU0hBREZShgOGFyPdJ
rKEG1Zp+3O58mf30FFwWO+EcUldpdf2BgJABa9jDMDmOgSM7pgZ3hU7blxEt6iRW
7hK4VV8B2KQxu4IaAfmlFYhHA01kPEocFPljfPSpMmUIhGpjMm7BYwmCNHiF0+TH
OpNA8jOVjc3q6bjKJhH4TVgXE3KvQw1XcSaWDJYaRsOntTr+IyJq5bxra6egAM8J
5deasSEb1E+1FWnGIJOIJ+isaSwBqIBQ4/YqqQeG9TQ6/ANISP2bSJzsB60KCuHE
7szbDb3vqCRCBlyg6VEOgE6A8AInTwu9NJmC6Q1cUYe3LlywsT8N24a/ditcfDYH
/V/xh2uxv1wDwarIgBMtuITJ5IApb3eFYZIcFN3XBl0Nw1iclGxos3n5mPF1c1pm
EoiTLQbIXrKvOwlRolEFQGP7mpCm8ThBxzgJaTWjiKoO1DRAPNuNMdYJjN3kh+hX
h+thO8EDWv6oi4ai7r2VOk6gBN3Al/1l9cznqTdvFvYb88JUFh9SHkOLAowI/Q82
72n0iLgRU3h7MDlG5mLFz4oBO/FHGAfug3AlglD4l4e++Dp556e9wfnH8li9gXKi
Vq/j4/ZQUOgB/hg9KopKSgPG+Tbi5frG8ufHhL0xELRTAgMBAAGjWjBYMB0GA1Ud
DgQWBBTdomcbjOBRDi6fM3Gh33nIYJ9KqTAOBgNVHQ8BAf8EBAMCAgQwFgYDVR0l
AQH/BAwwCgYIKwYBBQUHAwkwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsF
AAOCAgEAZmDZmFfuNXMvfAV9bOa/65GHpboEGZ8IK4Vxdyd/yAwERPDz11nKTQut
6YX7BgeD0DaTyL1nR1QCqp3CvvHAnfsmJrJqrb00uv7PZ52dTX6Ppp8gPmlIRHEB
C7NR7DPJ/825DSt5eHgimsCdz6asGZrQmXB3+z400PllsyAXvgIU9gvejOOW8FWX
/AlA55esZVnapWKQOh4ZwVDRRz850OuRHsTB6/fj/MBz54h2kYrVQyRgaS5caloi
vHe4mxsSgL6Eoo076ZVIpTGwqjd843+FHf7EvFBATR4MOL7njrZphaAqxYQm/Qsz
sBdTsILYCsMEJGHv7p5lp7LWFRIbXorYBqwig7AgUR8t3eUCULtAshtmq3/UVusK
GqNm/j1mpbaitSvWzfeIEuj2klSPAwI5ZqXeAzDDhG5VWtkZ7vnn7lM0MYYx993R
ImRFyfrlyTPwXlEgCujIgvlTwn+kX7BgD+/CIEH4djOWP9gXlTrLnFSzl0OWqfD+
RqYLWuqxtN2I8zH2v4ItGvzGXgk2ZO2itbLqKwPZ1ah5f7/I+fTBGNrc71wE1BUY
4+rvkxXoXLBESNGRlQXKc8b8tIuzbdFJLFomPme6wd1vUetiMCkLremkRuBFog4z
1rww//GFqJlXCw+LCaQfZyFEqhIAYjkCS/4SMZmpBRHjyVJCDMw=
-----END CERTIFICATE-----
```

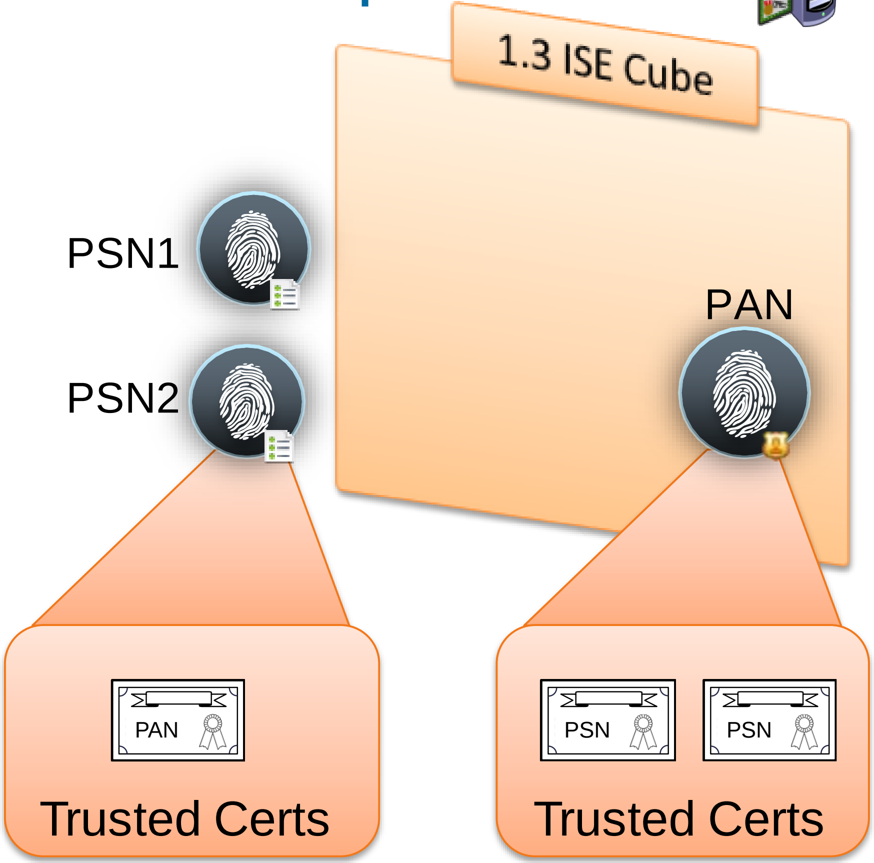
DER



```
0Ç¬0Ç™†–é˚ía@ÑâPóÙòÖ1;0
        *ÜHÜ˜

051301U
*Certificate Services Root CA - atw-lab-ise0
141103205941Z
191104205941Z0<1:08U
1Certificate Services OCSP Responder - atw-lab-ise0Ç"0
        *ÜHÜ˜
Ç0Ç
Ç/®Úp
</˚ÒZYeiß'V\91◊ö°/ÃA!äŒ¶è‹}•¬!ÎÃáfi˝ÿôyy†Jùm`\|XÎÜDã‘'Mö¯%ö
finvS‡@§n%ƒ
ü=y≤©Z˛T£púuÙ'û∏§ìcåãı
<ï "ûÏ÷j7çM¶ôÔúìoO>+'^‹Ë<„JkÕ\£¶®T)!ˆ˙m®Ëc˚°30M\™ˇê≠'1iqJ
&ç®~õ=8OÒ†afi€E¿ =££ÅΔ0Å√0lU#e0cÄ6ô
Mə:·öfi¶fïüÔn≤Y•;°9§7051301U
*Certificate Services Root CA - atw-lab-iseÇ`ÉyO±$ãõ«·ôÔ0UUe5C•€Æ2»ßİ±›;êØ0Uˇ‡0U%ˇ
0
+       0
Uˇ00
        *ÜHÜ˜

ÇãùÔ°Ô'°ıa◊gNTtÚõbÉ|éäR#I4¡ÎÜM†AÕ≠^´ÌÔjfi@ãıêëïeJç‡µºh∞XQë«ò˚K,Î¯»
hÊzóe˛¨üäñ8VÊYwÁSÙ∑Æ!B0ΩkÁ=ìn‡,ì…ıê|áõÅV¡
T]Ô<>ô'2ñF%¶əx«$mˆmô
Pmkp,>2jGjx÷Ü,^p* `mæə‹J"euK m',Fî('ã›_ÿTÄga' 8˙:=cé£#ə(Fäò∞AÈŒƒ7LìÎ¡zÎ&x
˚2Á˜TaøoKÁ«.rcUx¶®å'†È/ÉóΩ@\ò« øâûz÷NËáNÄÖÈ˙∫òFóÚåə¥
jTÔiüxi˘§Cvä/Rà§ÛúçÑhr∫HÕd–l2î`˝~qòeªı∏tÌ?Œ¿®.Ê¿í–‡›ÕS8?‹v≥˚\ó•–;|u≈È7õÏ«RíxΩîÄå" ˙+ü_pÉra
```

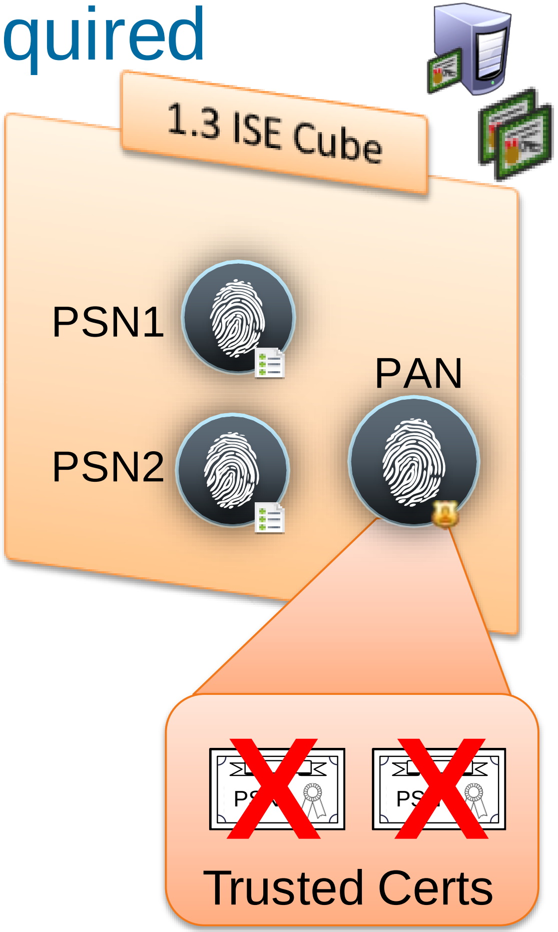
Joining an ISE Cube: Mutual Trust Required

- In order to join an ISE node to an existing ISE Cube:
  - You must trust the PAN Cert on the 2ndary node(s)
  - And vice-versa.



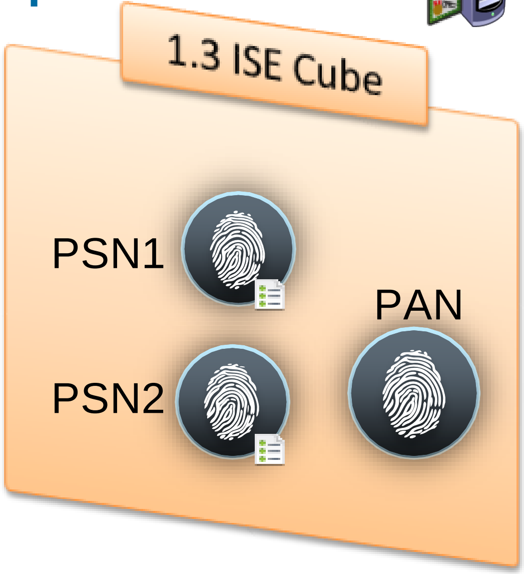
Joining an ISE Cube: Mutual Trust Required

- In order to join an ISE node to an existing ISE Cube:
  - You must trust the PAN Cert on the 2ndary node(s)
  - And vice-versa.
- Then you upgrade all Certs
  - Delete the old Self-Signed Certificates from the System Certs
  - Delete the old Self-Signed Certs from the Trusted Cert Store



Joining an ISE Cube: Mutual Trust Required

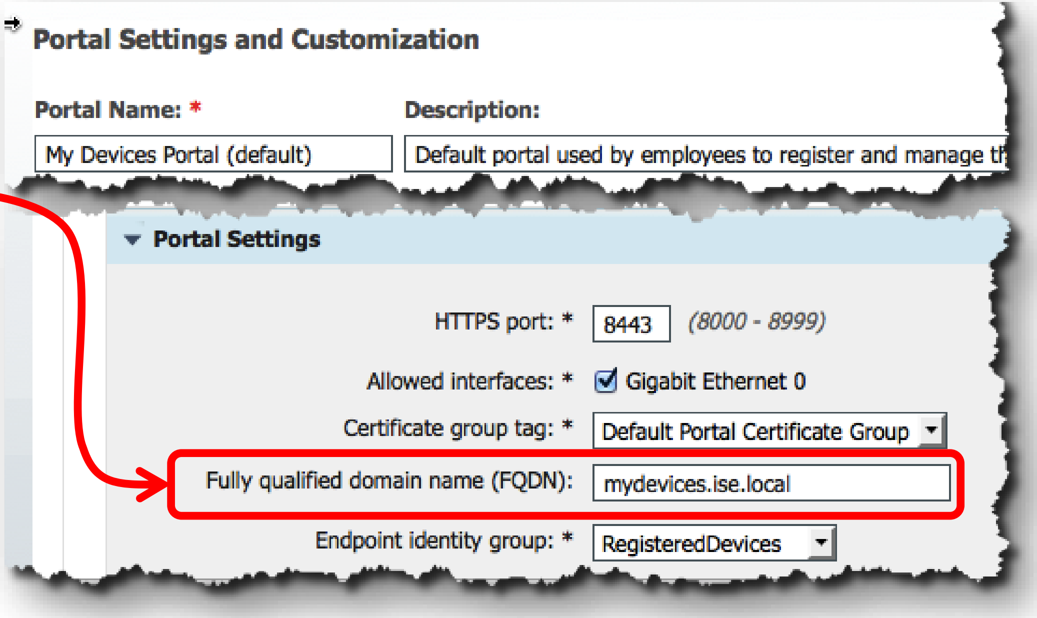
- In order to join an ISE node to an existing ISE Cube:
  - You must trust the PAN Cert on the 2ndary node(s)
  - And vice-versa.
- Then you upgrade all Certs
  - Delete the old Self-Signed Certificates from the System Certs
  - Delete the old Self-Signed Certs from the Trusted Cert Store
- So, it’s often easiest to upgrade to a CA-Signed & Trusted Cert Before Joining the Cube.



Simple URL for My Devices & Sponsor Portals

- In 1.3: Sponsor Portal and My Devices Portal must be accessed via a user-friendly URL and selectable port.
- Ex: http://mydevices.company.com

  Automatic redirect to https://fqdn:port
- FQDN for URL must be added to DNS and resolve to the Policy Service node(s) used for Guest Services.
- *Recommend populating Subject Alternative Name (SAN) field of PSN local cert with this alternative FQDN or Wildcard to avoid SSL cert warnings due to name mismatch.*



Portal Settings and Customization

Portal Name: * My Devices Portal (default)

Description: Default portal used by employees to register and manage th

Portal Settings

HTTPS port: * 8443 (8000 - 8999)

Allowed interfaces: * ☑ Gigabit Ethernet 0

Certificate group tag: * Default Portal Certificate Group

Fully qualified domain name (FQDN): mydevices.ise.local

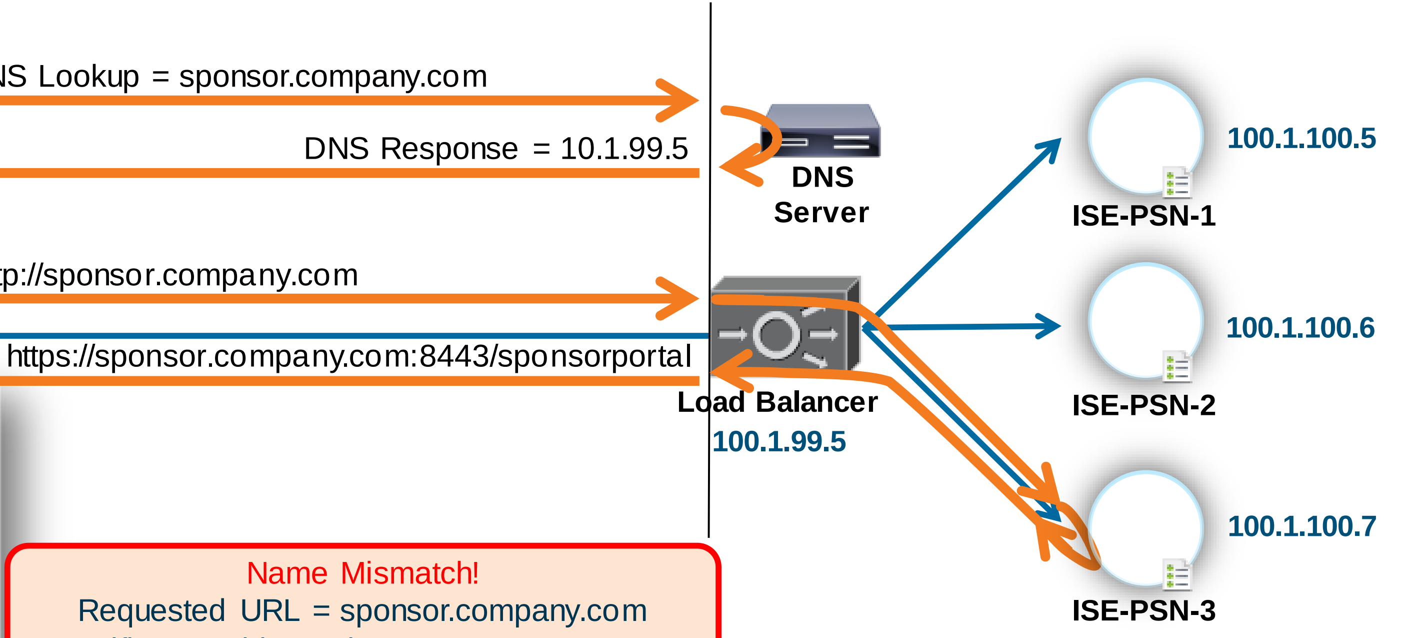
Endpoint identity group: * RegisteredDevices

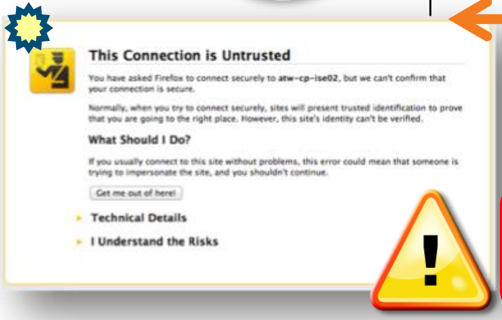
ISE Certificate without SAN

- Certificate Warning - Name Mismatch

http://sponsor.cts.local

SPONSOR





This Connection is Untrusted

You have asked Firefox to connect securely to **atw-cp-ise02**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

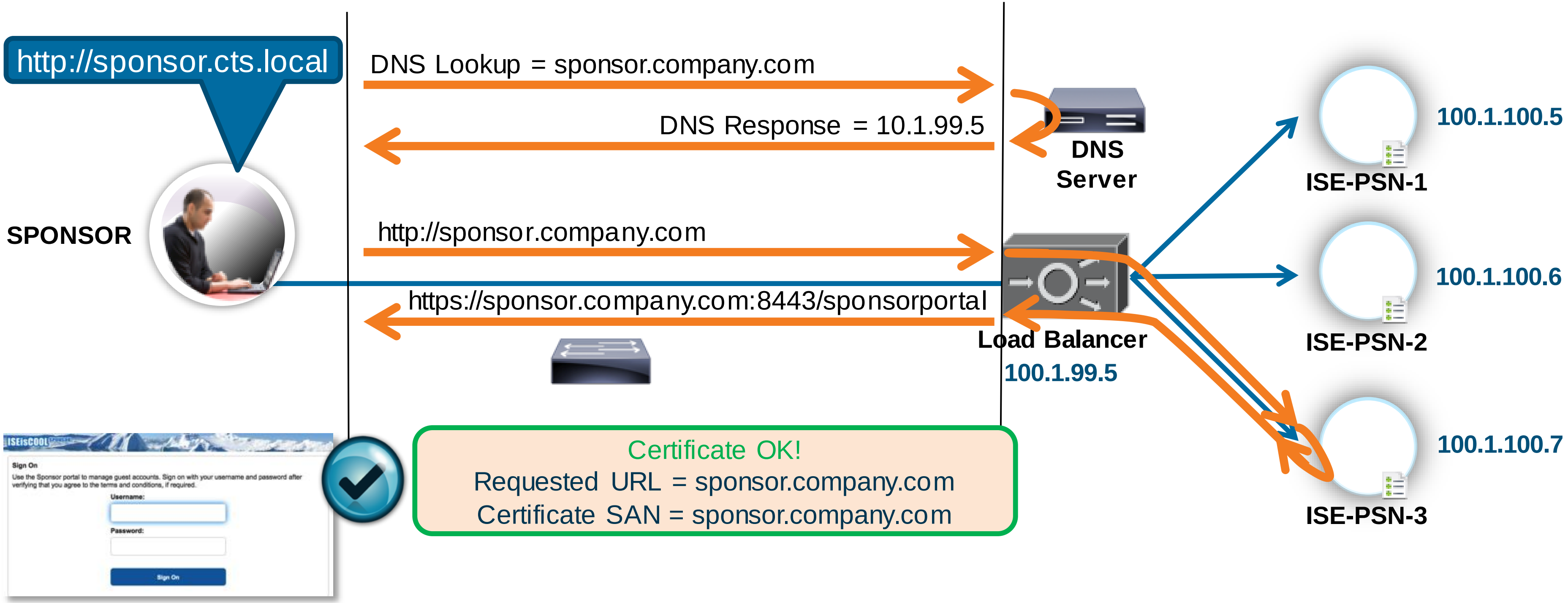
Get me out of here!

- **Technical Details**
- **I Understand the Risks**

Name Mismatch!
Requested URL = sponsor.company.com
Certificate Subject = ise-psn-3.company.com

ISE Certificate with SAN

- No Certificate Warning



Sign On

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.

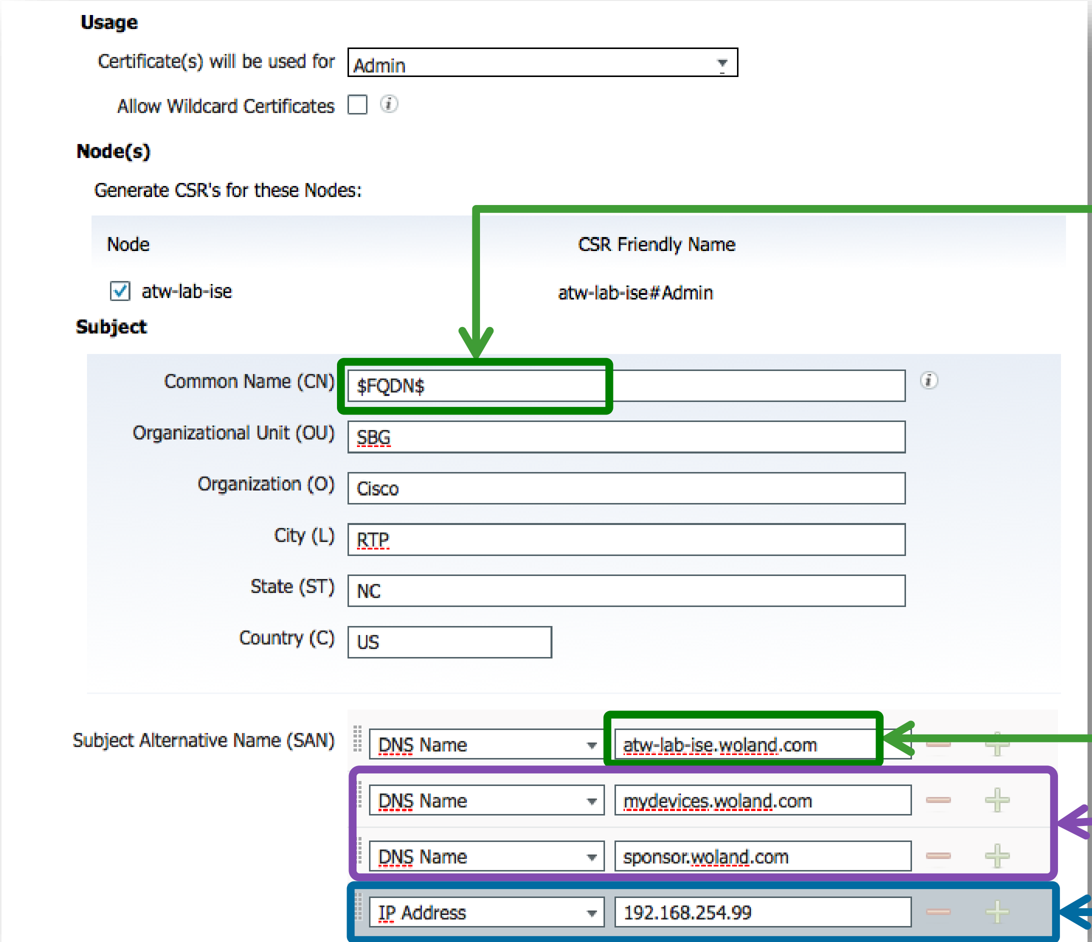
Username:

Password:

Sign On

Certificate OK!
Requested URL = sponsor.company.com
Certificate SAN = sponsor.company.com

ISE Certificate with SAN



Usage

Certificate(s) will be used for: Admin

Allow Wildcard Certificates □

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ atw-lab-ise	atw-lab-ise#Admin

Subject

Common Name (CN)	$FQDN$
Organizational Unit (OU)	SBG
Organization (O)	Cisco
City (L)	RTP
State (ST)	NC
Country (C)	US

Subject Alternative Name (SAN)

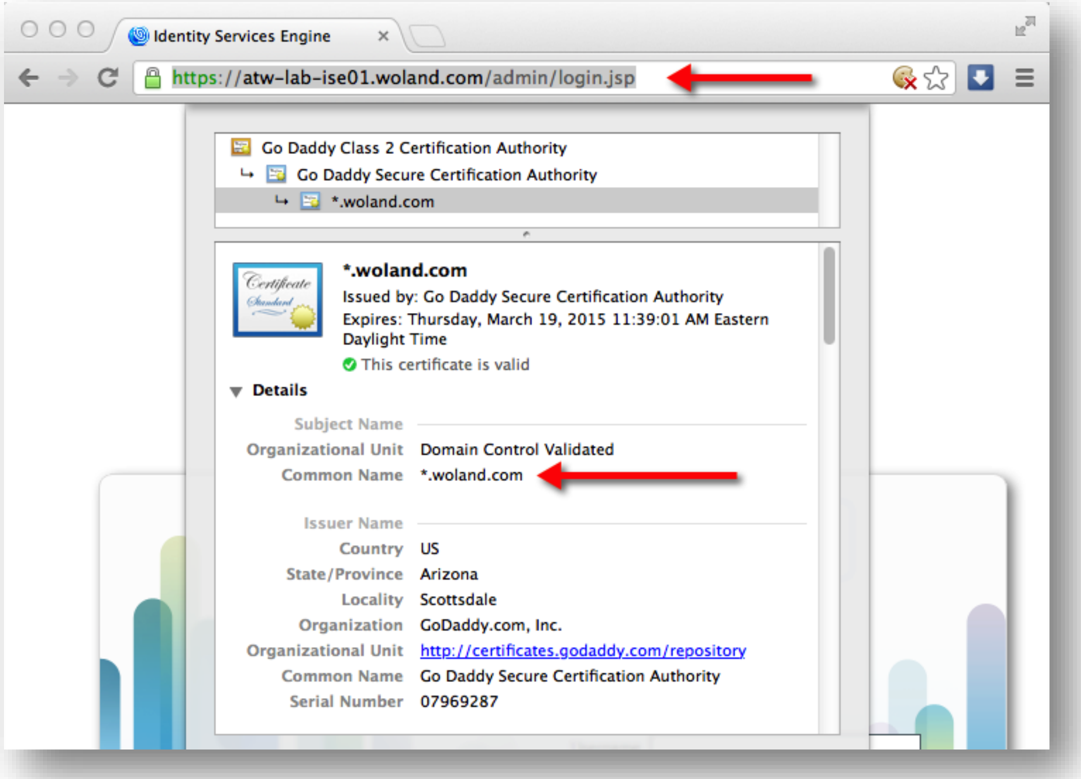
DNS Name	atw-lab-ise.woland.com
DNS Name	mydevices.woland.com
DNS Name	sponsor.woland.com
IP Address	192.168.254.99

CN must also exist in SAN

Other FQDNs as "DNS Names"

IP Address is also option

“Traditional” Wildcard Certificates



Go Daddy Class 2 Certification Authority
↳ Go Daddy Secure Certification Authority
↳ *.woland.com

***.woland.com**
Issued by: Go Daddy Secure Certification Authority
Expires: Thursday, March 19, 2015 11:39:01 AM Eastern Daylight Time
✓ This certificate is valid

▼ **Details**

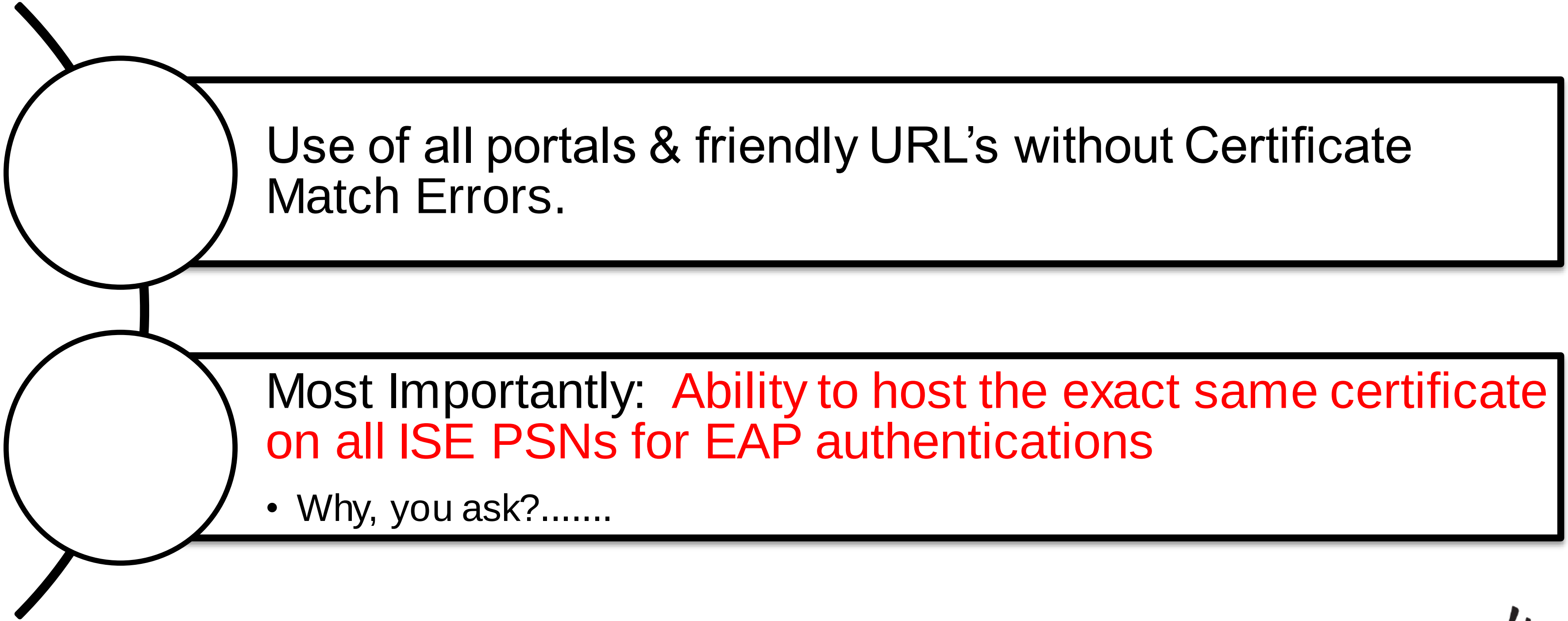
Subject Name	
Organizational Unit	Domain Control Validated
Common Name	*.woland.com
Issuer Name	
Country	US
State/Province	Arizona
Locality	Scottsdale
Organization	GoDaddy.com, Inc.
Organizational Unit	http://certificates.godaddy.com/repository
Common Name	Go Daddy Secure Certification Authority
Serial Number	07969287

- Wildcard Certificates are used to identify any secure web site that is part of the domain:
  - e.g.: *.woland.com works for:
    - www.woland.com
    - mydevices.woland.com
    - sponsor.woland.com
    - AnyThingIWant.woland.com

!= psn.[ise].woland.com

Position in FQDN is fixed

Wildcard Certificates – Why use with ISE?



Use of all portals & friendly URL’s without Certificate Match Errors.

Most Importantly: Ability to host the exact same certificate on all ISE PSNs for EAP authentications

- Why, you ask?.......

Clients Misbehave!

- Example education customer:
  - ONLY 6,000 Endpoints (all BYOD style)
  - 10M Auths / 9M Failures in a 24 hours!
  - 42 Different Failure Scenarios – all related to clients dropping TLS (both PEAP & EAP-TLS).
- Supplicant List:
  - Kyocera, Asustek, Murata, Huawei, Motorola, HTC, Samsung, ZTE, RIM, SonyEric, ChiMeiCo, Apple, Intel, Cybertan, Liteon, Nokia, HonHaiPr, Palm, Pantech, LgElectr, TaiyoYud, Barnes&N
- 5411 No response received during 120 seconds on last EAP message sent to the client
  - This error has been seen at a number of Escalation customers
  - Typically the result of a misconfigured or misbehaving supplicant not completing the EAP process.

Recreating the Issue

Yes, my Wife was Absolutely THRILLED That this was completed In the kitchen!! ☺

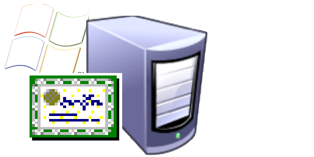
Recreating the Issue

Cisco Cius	Android 2.2.2 / Kernel 2.6.31.6-mrst
Galaxy Player	Android 2.3.5 / Kernel 2.6.35.7
Galaxy TAB 10.1	Android 4.0.4 / Kernel 3.1.10
Galaxy Tab 2	Android 4.1.1 / Kernel 3.0.31
Acer A110 Tab	Android 4.1.2 / Kernel 3.1.10
Google Nexus7	Android 4.2.2 / Kernel 3.1.10-g05b777c
iPod Touch 1Gen	iOS 3.1.3 (7E18)

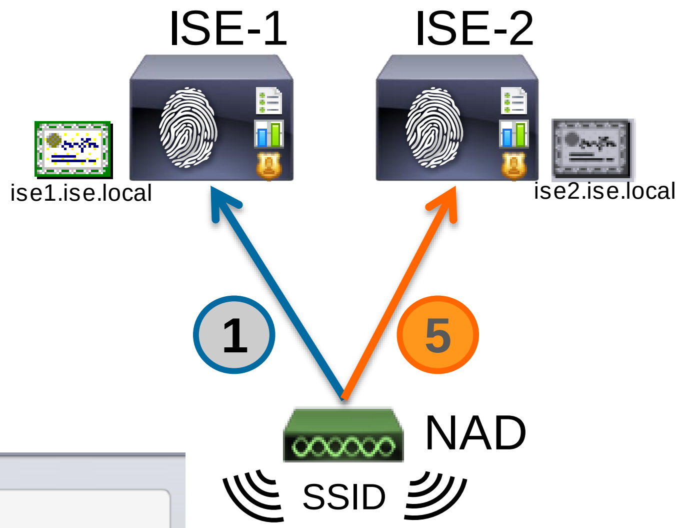
iPad1	iOS 5.1.1 (9B206)
iPad2	iOS 6.0.1 (10A523)
iPad Mini	iOS 6.1.2 (10B146)
iPhone 4	iOS 6.0 (10A403)
iPhone 5	iOS 6.1.3 (10B329)
Nook HD	Nook 2.1.0

MacBook Pro 17	OSX 10.7.5
MacBook Air	OSX 10.8.2 (12C30006)
Kindle Fire HD	Version 7.3.0_user_3013320
Microsoft Surface	WindowsRT
Win7 Native	Windows7 Ultimate ServicePack1
WinXP Native	WindowsXP SP3
Windows 8 Native	Windows 8 Native Supplicant

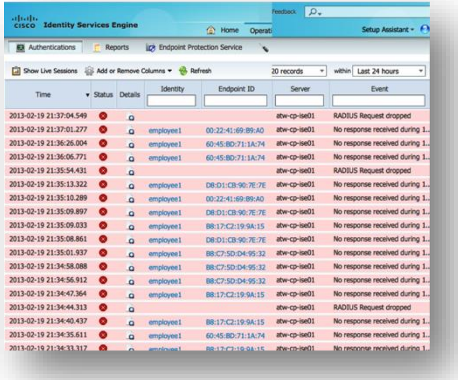
Clients Misbehave: Apple Example



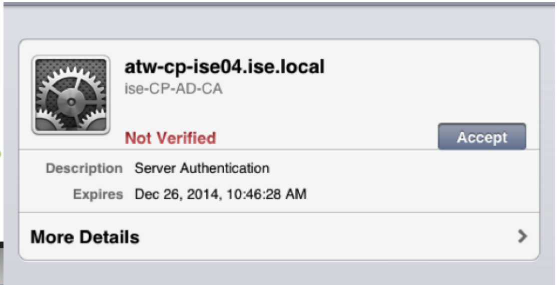
Cert Authority



- Multiple PSNs
- Each Cert signed by Trusted Root
- Apple Requires Accept on all certs!
  - Results in 5411 / 30sec retry



Time	Status	Details	Identity	Endpoint ID	Server	Event
2013-02-19 21:37:04.549	✖	🔍			atw-cp-ise01	RADIUS Request dropped
2013-02-19 21:37:01.277	✖	🔍	employee1	00:22:41:69:B9:A0	atw-cp-ise01	No response received during 1...
2013-02-19 21:36:26.004	✖	🔍	employee1	60:45:BD:71:1A:74	atw-cp-ise01	No response received during 1...
2013-02-19 21:36:06.771	✖	🔍	employee1	60:45:BD:71:1A:74	atw-cp-ise01	No response received during 1...
2013-02-19 21:35:54.431	✖	🔍			atw-cp-ise01	RADIUS Request dropped
2013-02-19 21:35:13.322	✖	🔍	employee1	D8:D1:CB:90:7E:7E	atw-cp-ise01	No response received during 1...
2013-02-19 21:35:10.289	✖	🔍	employee1	00:22:41:69:B9:A0	atw-cp-ise01	No response received during 1...
2013-02-19 21:35:09.897	✖	🔍	employee1	D8:D1:CB:90:7E:7E	atw-cp-ise01	No response received during 1...
2013-02-19 21:35:09.033	✖	🔍	employee1	B8:17:C2:19:9A:15	atw-cp-ise01	No response received during 1...
2013-02-19 21:35:08.861	✖	🔍	employee1	D8:D1:CB:90:7E:7E	atw-cp-ise01	No response received during 1...
2013-02-19 21:35:01.937	✖	🔍	employee1	B8:C7:5D:D4:95:32	atw-cp-ise01	No response received during 1...
2013-02-19 21:34:58.088	✖	🔍	employee1	B8:C7:5D:D4:95:32	atw-cp-ise01	No response received during 1...
2013-02-19 21:34:56.912	✖	🔍	employee1	B8:C7:5D:D4:95:32	atw-cp-ise01	No response received during 1...
2013-02-19 21:34:47.364	✖	🔍	employee1	B8:17:C2:19:9A:15	atw-cp-ise01	No response received during 1...
2013-02-19 21:34:44.313	✖	🔍			atw-cp-ise01	RADIUS Request dropped
2013-02-19 21:34:40.437	✖	🔍	employee1	B8:17:C2:19:9A:15	atw-cp-ise01	No response received during 1...
2013-02-19 21:34:35.611	✖	🔍	employee1	60:45:BD:71:1A:74	atw-cp-ise01	No response received during 1...
2013-02-19 21:34:33.317	✖	🔍	employee1	B8:17:C2:19:9A:15	atw-cp-ise01	No response received during 1...



atw-cp-ise04.ise.local

ise-CP-AD-CA

Not Verified

Description Server Authentication

Expires Dec 26, 2014, 10:46:28 AM

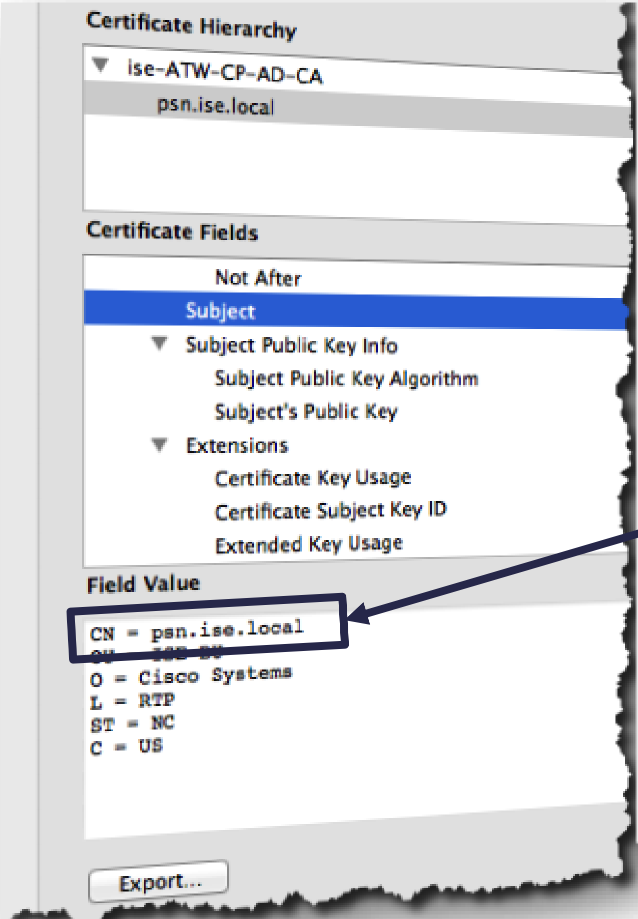
More Details

Apple iOS & MacOS

WiFi Profile

1. Authentication goes to ISE-1
2. ISE-1 sends certificate
3. Client trusts ISE-1
4. Client Roams
5. Authentication goes to ISE-2
6. Client Prompts for Accept

Solution: Common Cert, Wildcard in SAN



Certificate Hierarchy

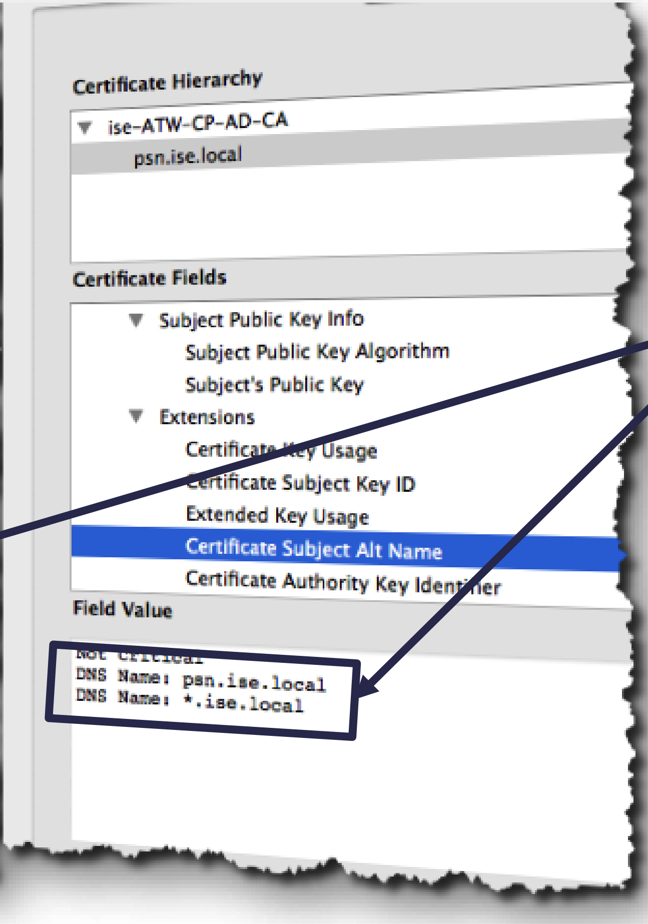
- ise-ATW-CP-AD-CA
  - psn.ise.local

Certificate Fields

- Not After
- Subject
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Extensions
  - Certificate Key Usage
  - Certificate Subject Key ID
  - Extended Key Usage

Field Value

```
CN = psn.ise.local
OU = ISE BU
O = Cisco Systems
L = RTP
ST = NC
C = US
```



Certificate Hierarchy

- ise-ATW-CP-AD-CA
  - psn.ise.local

Certificate Fields

- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Extensions
  - Certificate Key Usage
  - Certificate Subject Key ID
  - Extended Key Usage
  - Certificate Subject Alt Name
  - Certificate Authority Key Identifier

Field Value

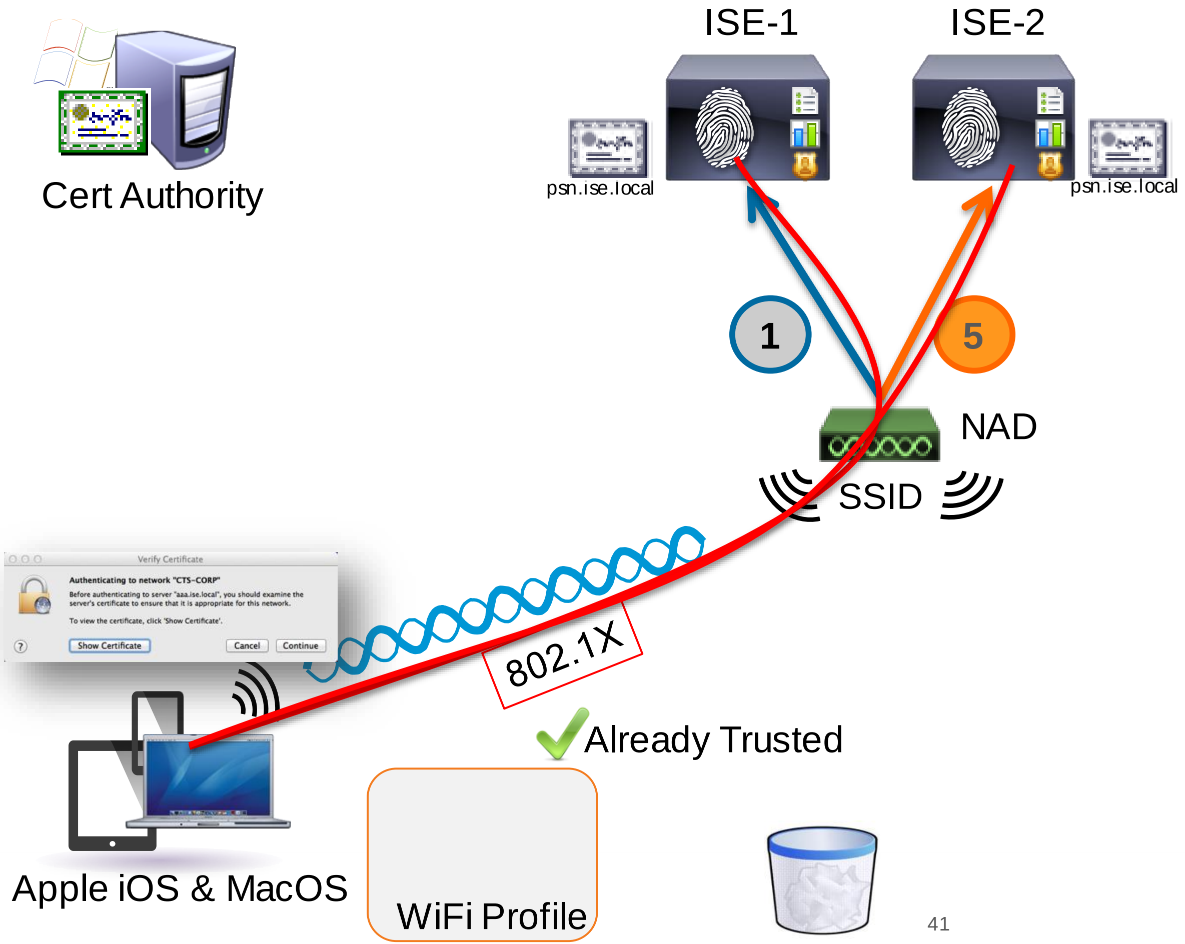
```
Not Critical
DNS Name: psn.ise.local
DNS Name: *.ise.local
```

Allows anything ending with The Domain Name.

-

Same EXACT Priv / Pub Key May be installed on all PSNs

Solution: Common Cert, Wildcard in SAN



Verify Certificate

Authenticating to network "CTS-CORP"

Before authenticating to server "aaa.ise.local", you should examine the server's certificate to ensure that it is appropriate for this network.

To view the certificate, click 'Show Certificate'.

? Show Certificate Cancel Continue

- CN= psn.ise.local
- SAN contains all PSN FQDNs
  - psn.ise.local
  - *.ise.local
- Tested and works with:
  comodo.com CA
  SSL.com CA
  Microsoft 2008 CA
- Failed with: GoDaddy CA
  -- they don’t like * in SAN
  -- they don’t like non-* in CN

1. Authentication goes to ISE-1
2. ISE-1 sends certificate
3. Client trusts ISE-1
4. Client Roams
5. Authentication goes to ISE-2
6. Client Already Trusts Cert

Internal CA Details

Internal Certificate Authority

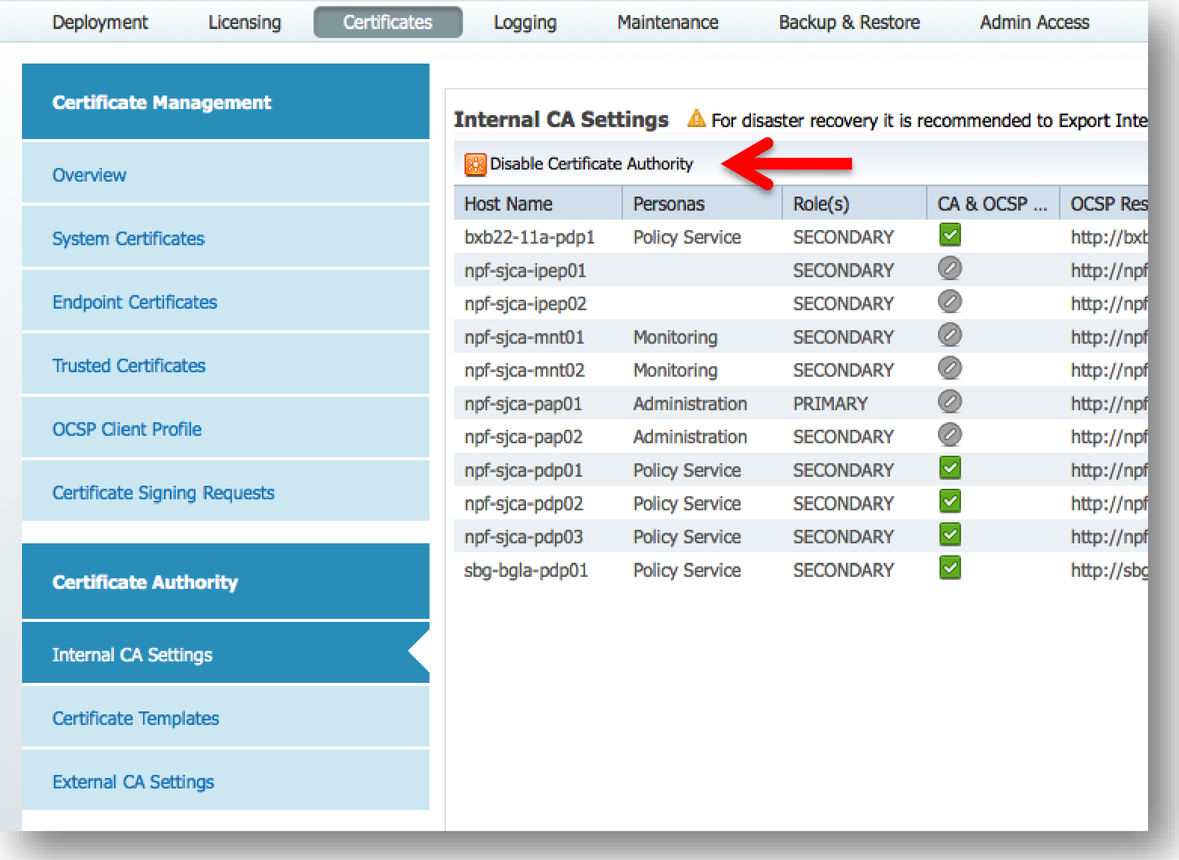
Why use ISE as a Certificate Authority?

- Microsoft Public Key Infrastructure via a 2003/2008 Enterprise Server can add significant complexity and expense to an ISE deployment.

Benefits of internal CA:

- Internal CA simplifies ISE deployment
- ISE can deliver certificates directly to endpoints
- No need to rely on integrating ISE to PKI for BYOD Cert provisioning
- Internal CA can still work with existing PKI Infrastructure
- Closed Loop BYOD Solution
- Focused on BYOD and MDM use-cases only, not a general purpose CA

Configuring the Native Certificate Authority



Internal CA Settings ⚠ For disaster recovery it is recommended to Export Inte

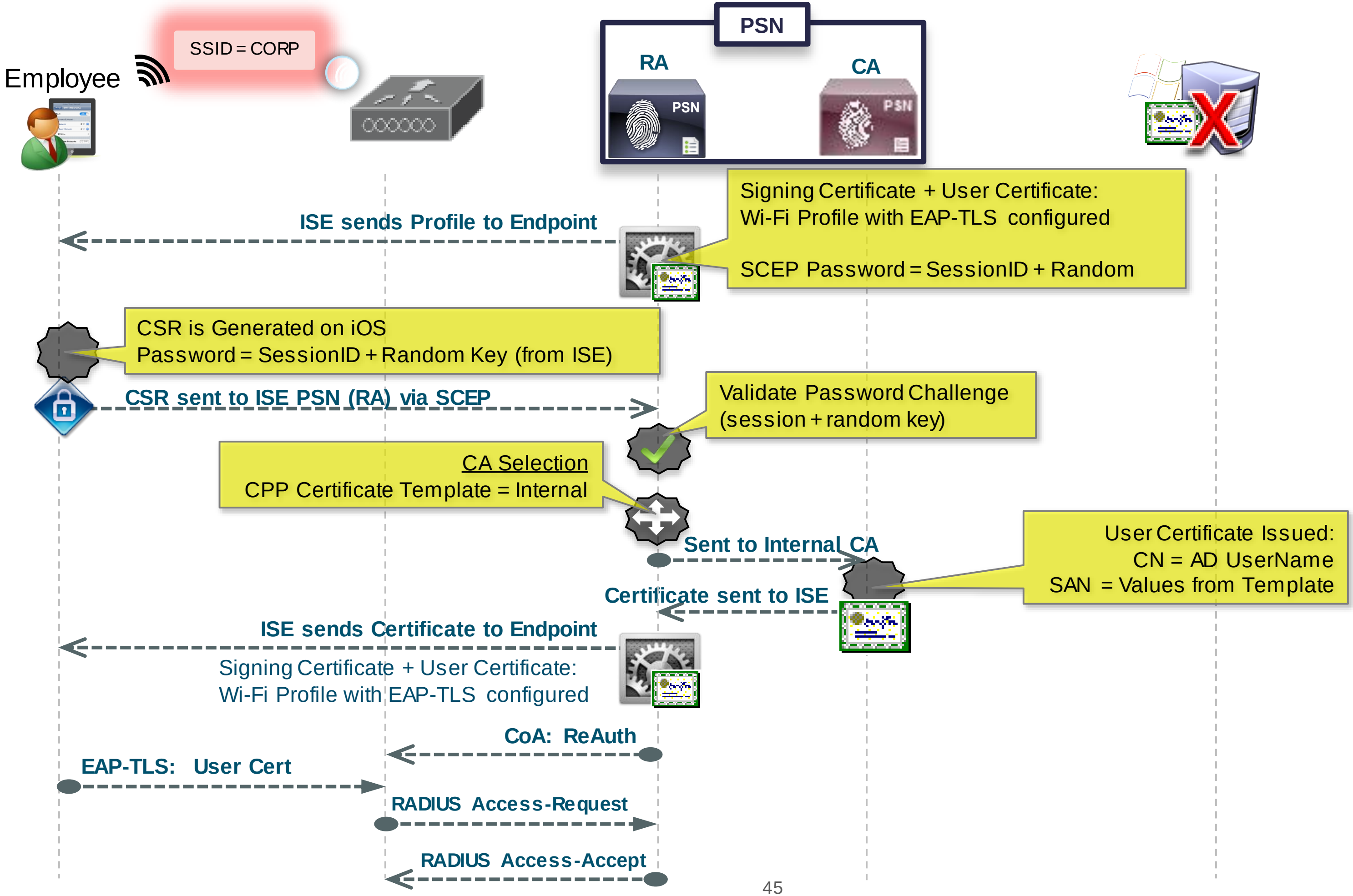
Host Name	Personas	Role(s)	CA & OCSP ...	OCSP Res
bxb22-11a-pdp1	Policy Service	SECONDARY	☑	http://bxb
npf-sjca-ipep01		SECONDARY	⊘	http://npf
npf-sjca-ipep02		SECONDARY	⊘	http://npf
npf-sjca-mnt01	Monitoring	SECONDARY	⊘	http://npf
npf-sjca-mnt02	Monitoring	SECONDARY	⊘	http://npf
npf-sjca-pap01	Administration	PRIMARY	⊘	http://npf
npf-sjca-pap02	Administration	SECONDARY	⊘	http://npf
npf-sjca-pdp01	Policy Service	SECONDARY	☑	http://npf
npf-sjca-pdp02	Policy Service	SECONDARY	☑	http://npf
npf-sjca-pdp03	Policy Service	SECONDARY	☑	http://npf
sbg-bgla-pdp01	Policy Service	SECONDARY	☑	http://sbg

- Yes, that’s really it!

☺ So easy

Enabled by Default

NSP Flow – Internal CA



ISE sends Profile to Endpoint

Signing Certificate + User Certificate:
Wi-Fi Profile with EAP-TLS configured

SCEP Password = SessionID + Random

CSR is Generated on iOS
Password = SessionID + Random Key (from ISE)

CSR sent to ISE PSN (RA) via SCEP

Validate Password Challenge
(session + random key)

CA Selection
CPP Certificate Template = Internal

Sent to Internal CA

User Certificate Issued:
CN = AD UserName
SAN = Values from Template

Certificate sent to ISE

ISE sends Certificate to Endpoint

Signing Certificate + User Certificate:
Wi-Fi Profile with EAP-TLS configured

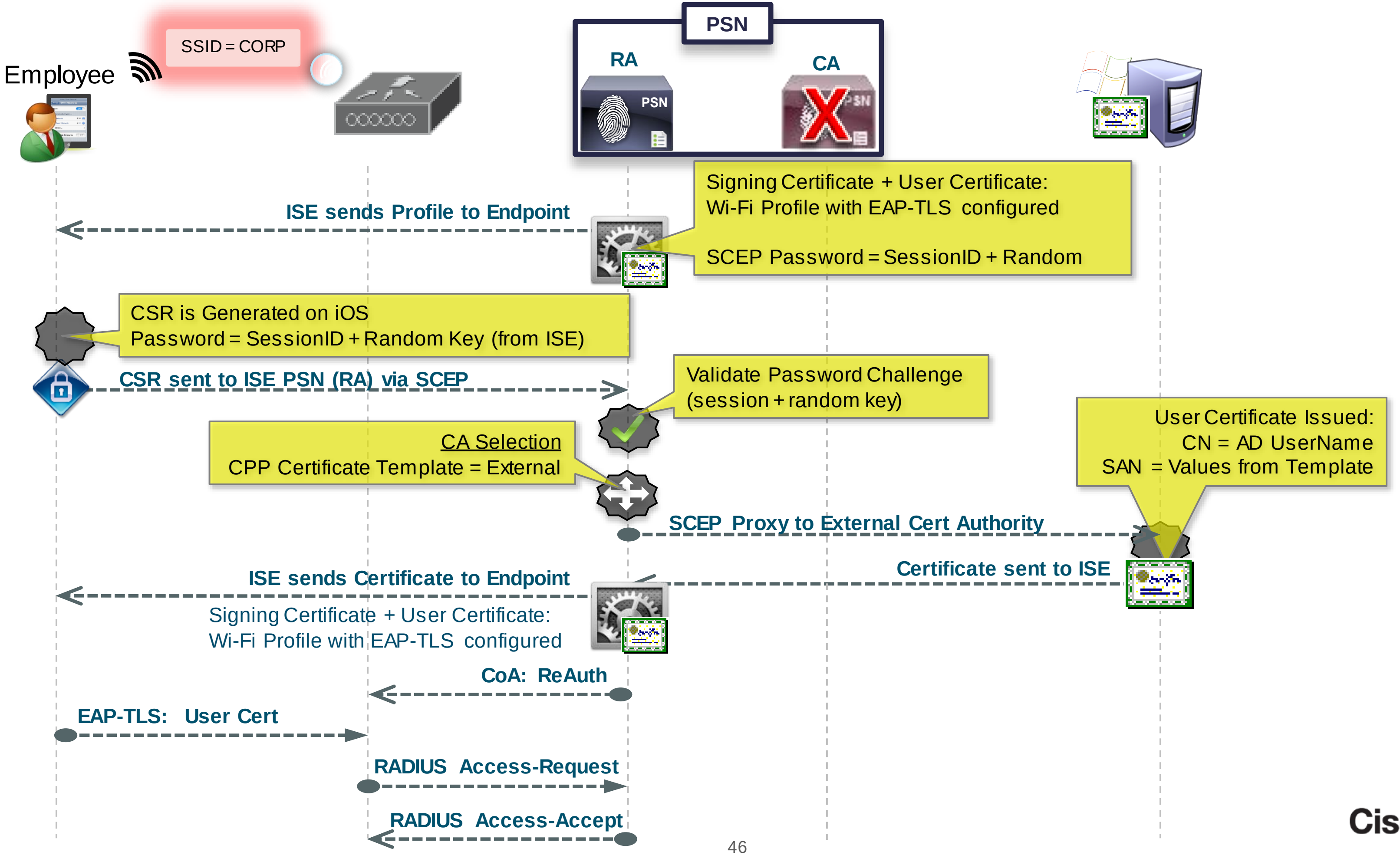
CoA: ReAuth

EAP-TLS: User Cert

RADIUS Access-Request

RADIUS Access-Accept

NSP Flow – External CA



Employee

SSID = CORP

PSN

RA

CA

ISE sends Profile to Endpoint

Signing Certificate + User Certificate:
Wi-Fi Profile with EAP-TLS configured

SCEP Password = SessionID + Random

CSR is Generated on iOS
Password = SessionID + Random Key (from ISE)

CSR sent to ISE PSN (RA) via SCEP

Validate Password Challenge
(session + random key)

CA Selection
CPP Certificate Template = External

User Certificate Issued:
CN = AD UserName
SAN = Values from Template

SCEP Proxy to External Cert Authority

Certificate sent to ISE

ISE sends Certificate to Endpoint

Signing Certificate + User Certificate:
Wi-Fi Profile with EAP-TLS configured

CoA: ReAuth

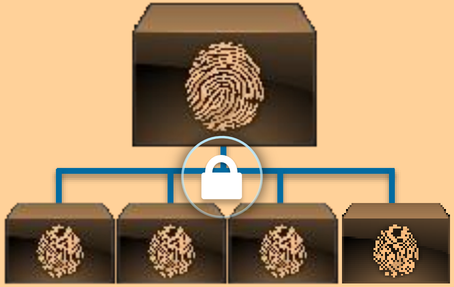
EAP-TLS: User Cert

RADIUS Access-Request

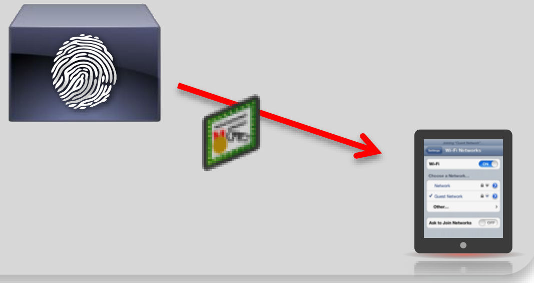
RADIUS Access-Accept

ISE CA: Multiple Personalities/Identities

Root CA

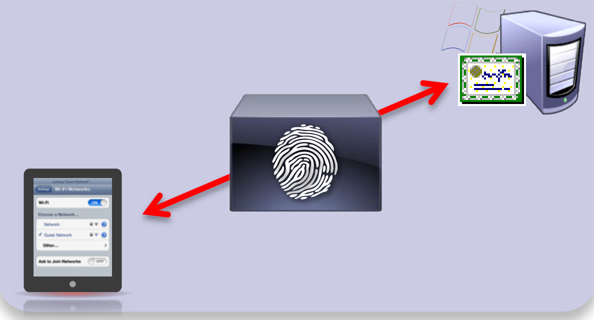


Subordinate CA

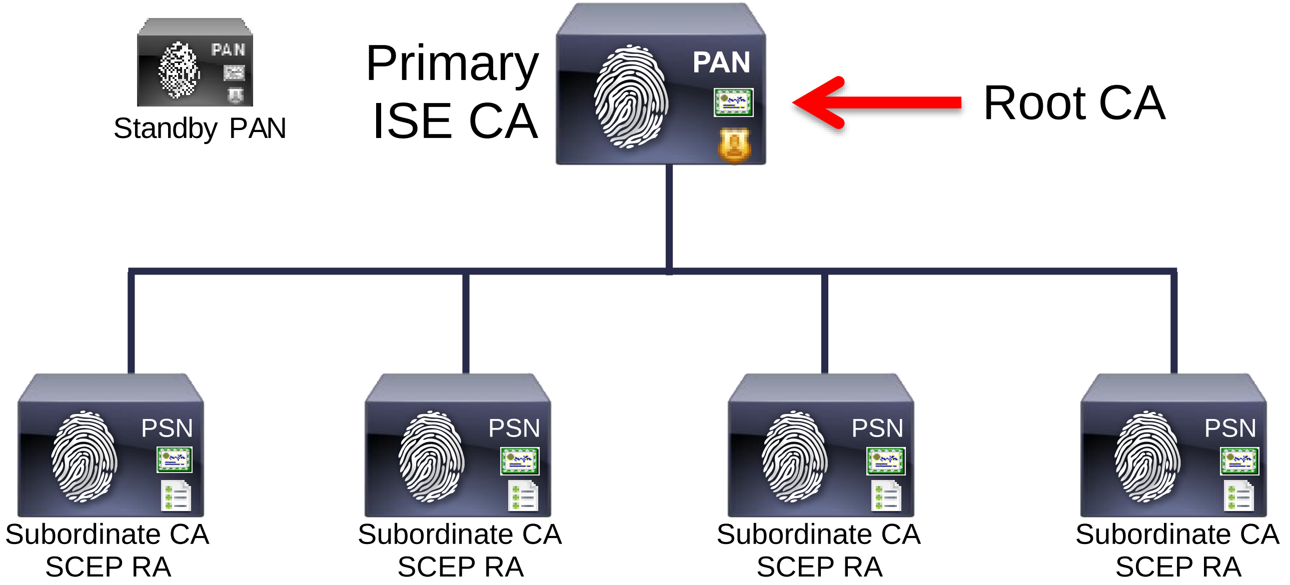


OCSP Server

Registration Authority



ISE Certificate Authority Architecture



Root CA is Used to Sign the certificates for the Subordinate CA's.

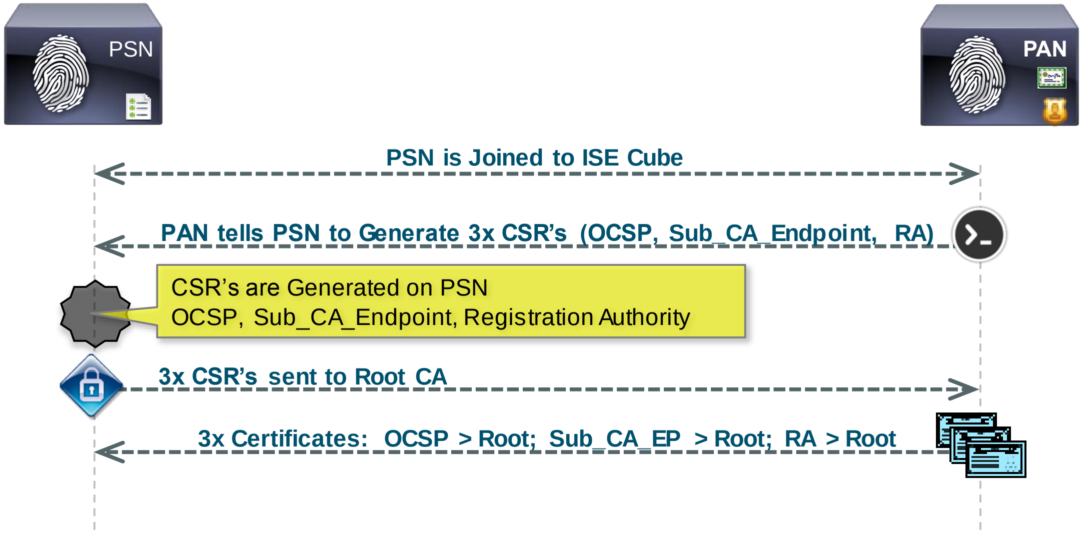
Subordinate CA signs the Actual Endpoint Certs

Secondary PAN is another Root CA! Ensure you export Primary PAN and import on Secondary

Node Registration Process Overview

Each PSN will get three certificates for CA functions:

- Subordinate CA – To sign endpoint certificates
- OCSP – To identify node with OCSP service
- Registration Authority (RA) – To identify sub-ca when requesting certificates for endpoints.



PSN
PAN
PSN is Joined to ISE Cube
PAN tells PSN to Generate 3x CSR's (OCSP, Sub_CA_Endpoint, RA)
CSR's are Generated on PSN
OCSP, Sub_CA_Endpoint, Registration Authority
3x CSR's sent to Root CA
3x Certificates: OCSP > Root; Sub_CA_EP > Root; RA > Root

Certificate Authority

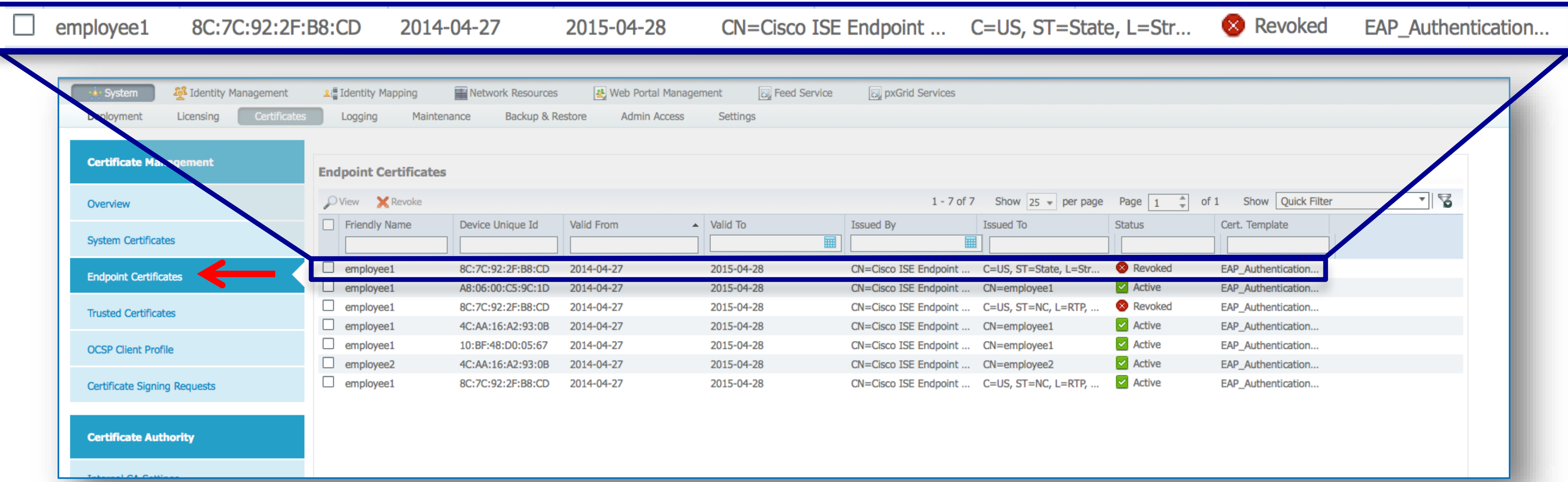
All PSNs are instructed by PAN to Generate the CSR's

PAN (Root CA) signs all three certs per-node

Secondary PAN does not generate CSR's to Root CA

MnT does not generate any CSRs to Root CA

Issue & Revoke Endpoint Certificates

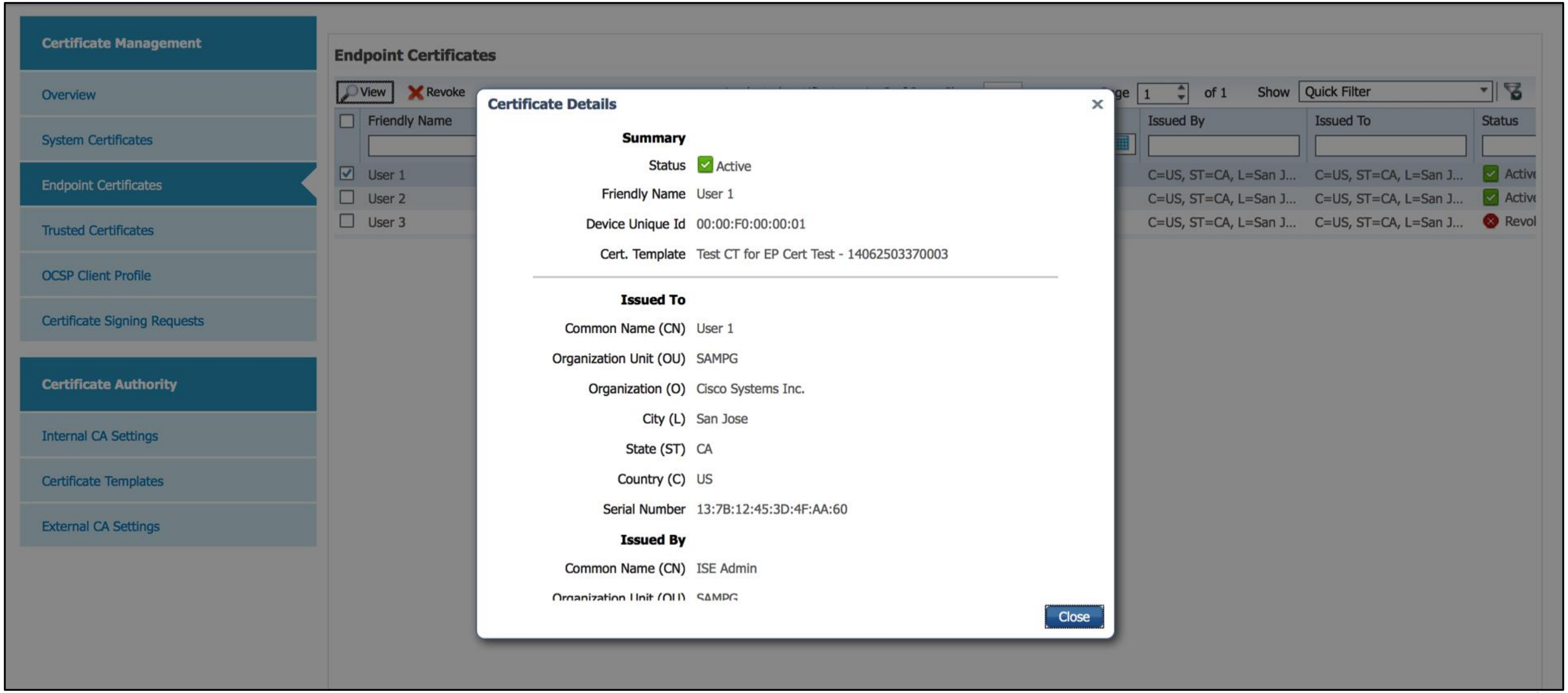


Endpoint Certificates

□	Friendly Name	Device Unique Id	Valid From	Valid To	Issued By	Issued To	Status	Cert. Template
□	employee1	8C:7C:92:2F:B8:CD	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	C=US, ST=State, L=Str...	Revoked	EAP_Authentication...
□	employee1	A8:06:00:C5:9C:1D	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	CN=employee1	Active	EAP_Authentication...
□	employee1	8C:7C:92:2F:B8:CD	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	C=US, ST=NC, L=RTP, ...	Revoked	EAP_Authentication...
□	employee1	4C:AA:16:A2:93:0B	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	CN=employee1	Active	EAP_Authentication...
□	employee1	10:BF:48:D0:05:67	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	CN=employee1	Active	EAP_Authentication...
□	employee2	4C:AA:16:A2:93:0B	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	CN=employee2	Active	EAP_Authentication...
□	employee1	8C:7C:92:2F:B8:CD	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	C=US, ST=NC, L=RTP, ...	Active	EAP_Authentication...

- Lists all the endpoint certificates issued by the Internal CA.
- Status – Active, Revoked, Expired
- Quick Overview of certificate details, Including the Template Used
- Automatically Revoked when an Endpoint is marked as “Lost”
- Certificates may be Manually Revoked

View Endpoint Certificate Contents



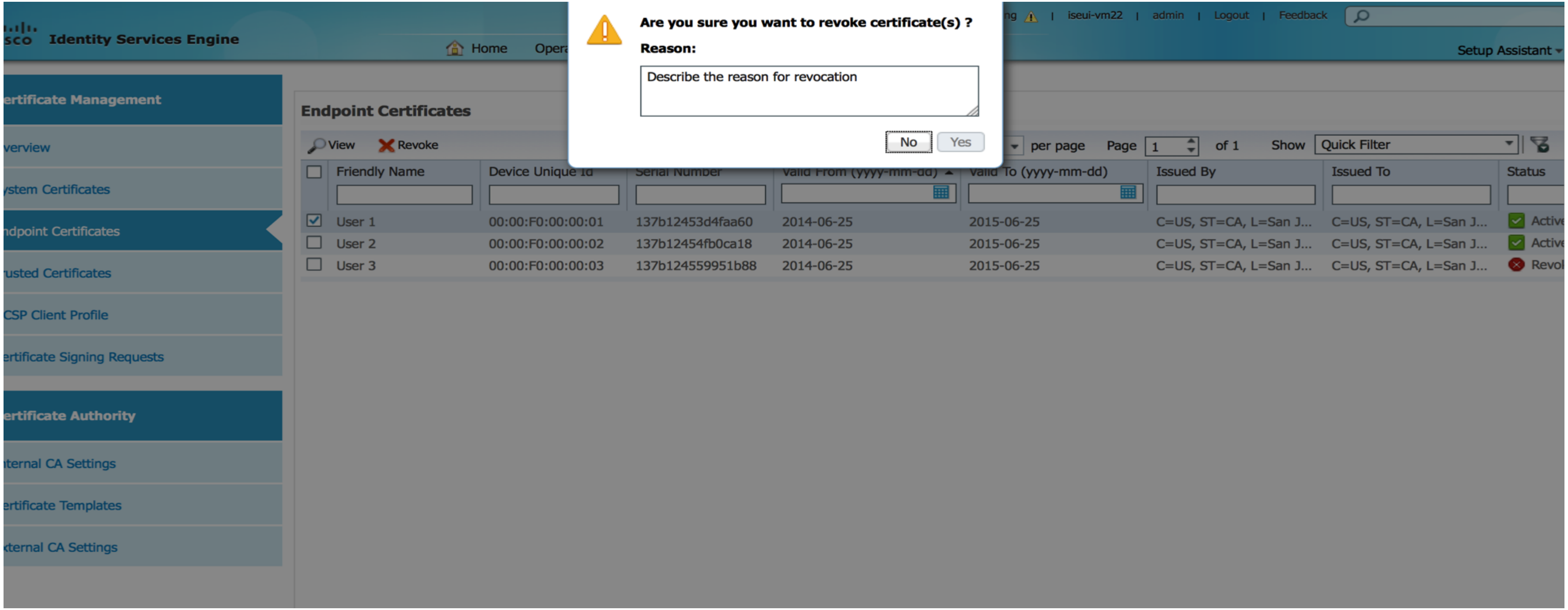
Endpoint Certificates

	Friendly Name	Issued By	Issued To	Status
☑	User 1	C=US, ST=CA, L=San J...	C=US, ST=CA, L=San J...	✓ Activ
□	User 2	C=US, ST=CA, L=San J...	C=US, ST=CA, L=San J...	✓ Activ
□	User 3	C=US, ST=CA, L=San J...	C=US, ST=CA, L=San J...	⊗ Revol

Certificate Details ×

Summary	
Status	✓ Active
Friendly Name	User 1
Device Unique Id	00:00:F0:00:00:01
Cert. Template	Test CT for EP Cert Test - 14062503370003
Issued To	
Common Name (CN)	User 1
Organization Unit (OU)	SAMPG
Organization (O)	Cisco Systems Inc.
City (L)	San Jose
State (ST)	CA
Country (C)	US
Serial Number	13:7B:12:45:3D:4F:AA:60
Issued By	
Common Name (CN)	ISE Admin
Organization Unit (OU)	SAMPG

Revoke Certificates



Are you sure you want to revoke certificate(s) ?

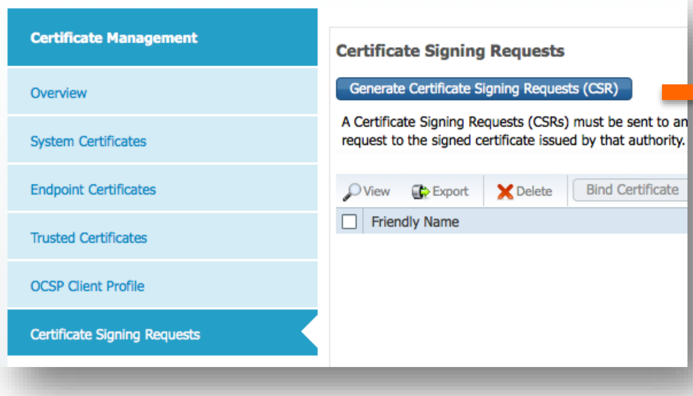
Reason:

Describe the reason for revocation

Endpoint Certificates

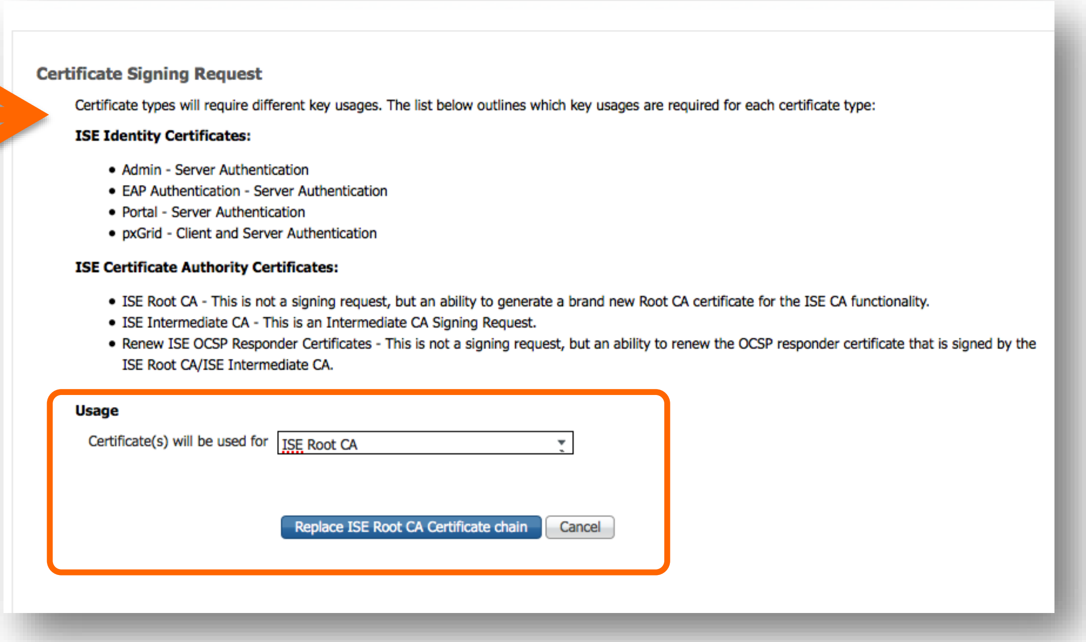
□	Friendly Name	Device Unique Id	Serial Number	Valid From (yyyy-mm-dd)	Valid To (yyyy-mm-dd)	Issued By	Issued To	Status
☑	User 1	00:00:F0:00:00:01	137b12453d4faa60	2014-06-25	2015-06-25	C=US, ST=CA, L=San J...	C=US, ST=CA, L=San J...	✓ Active
□	User 2	00:00:F0:00:00:02	137b12454fb0ca18	2014-06-25	2015-06-25	C=US, ST=CA, L=San J...	C=US, ST=CA, L=San J...	✓ Active
□	User 3	00:00:F0:00:00:03	137b124559951b88	2014-06-25	2015-06-25	C=US, ST=CA, L=San J...	C=US, ST=CA, L=San J...	✖ Revol

Re-generate the Root CA



Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to an
request to the signed certificate issued by that authority.



Certificate Signing Request

Certificate types will require different key usages. The list below outlines which key usages are required for each certificate type:

ISE Identity Certificates:

- Admin - Server Authentication
- EAP Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication

ISE Certificate Authority Certificates:

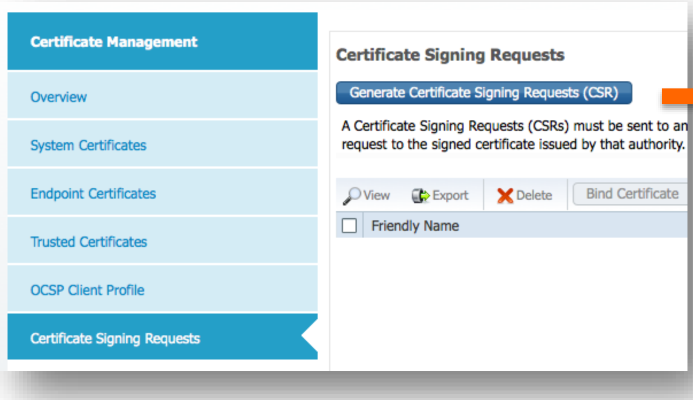
- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: ISE Root CA

- The Entire certificate chain can be re-generated if needed.
- Old CA certificates remain in the Trust store to ensure authentication of previously provisioned endpoints work successfully.

ISE as an Intermediate CA



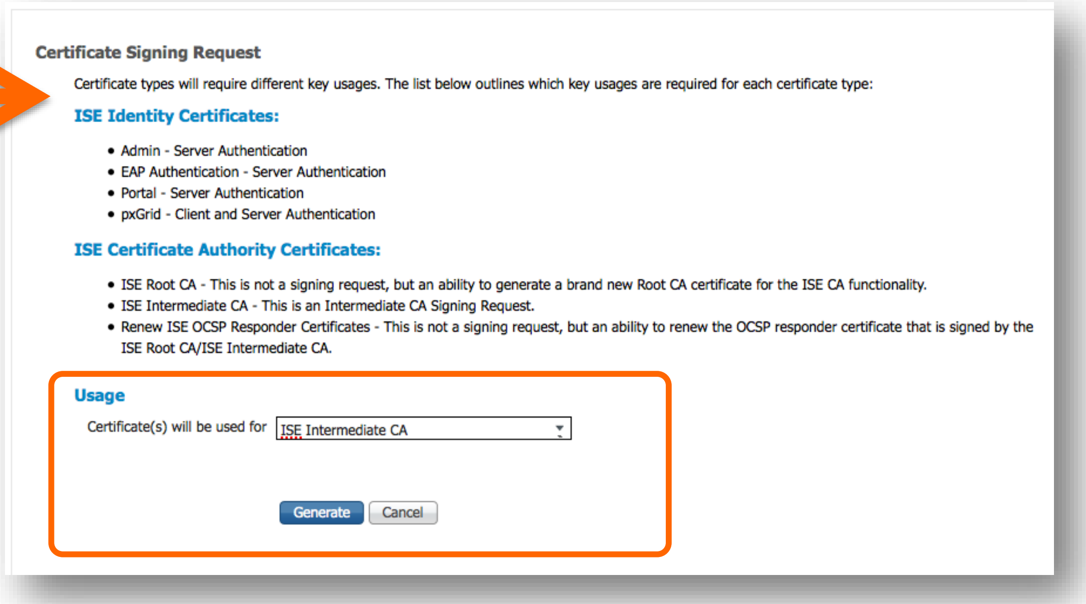
Certificate Management

- Overview
- System Certificates
- Endpoint Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to an
request to the signed certificate issued by that authority.



Certificate Signing Request

Certificate types will require different key usages. The list below outlines which key usages are required for each certificate type:

ISE Identity Certificates:

- Admin - Server Authentication
- EAP Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication

ISE Certificate Authority Certificates:

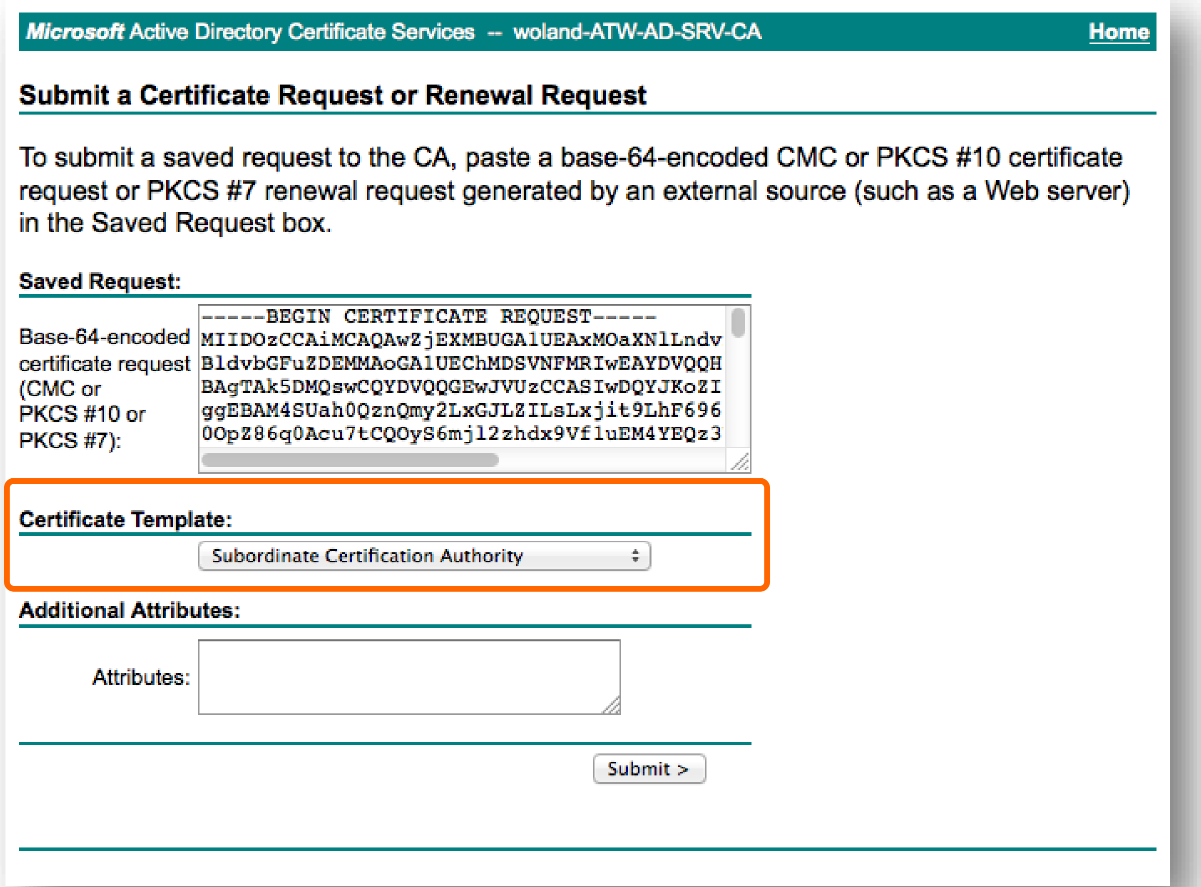
- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: ISE Intermediate CA

- ISE’s internal CA can work seamlessly with an existing CA in your deployment.
- Just make it an intermediate CA (sub-ordinate CA) to your existing CA.
  - Create a CSR for the ISE node and get a certificate issued by the existing CA.

ISE as an Intermediate CA



Microsoft Active Directory Certificate Services -- woland-ATW-AD-SRV-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDOzCCAiMCAQAwZjEXMBUGA1UEAxMOaXN1Lndv
BldvbGFuZDEMMAoGA1UEChMDSVNFMRIwEAYDVQQH
BAgTAk5DMQswCQYDVQQGEwJVUzCCASIwDQYJKoZI
ggEBAM4SUah0QznQmy2LxGJLZILsLxjit9LhF696
0OpZ86q0Acu7tCQOyS6mjl2zhdx9VfluEM4YEQz3
```

Certificate Template:

Subordinate Certification Authority

Additional Attributes:

Attributes:

Ensure that you get a certificate from your existing CA with Key Certificate signing capabilities (Sub_CA Template)

Ensure the Existing Root CA has a Tree Size >= 3
(ISE is 2-tiers)

Certificate Revocation

- Online Certificate Status Protocol (OCSP)
- Certificate Revocation List (CRL)

OCSP

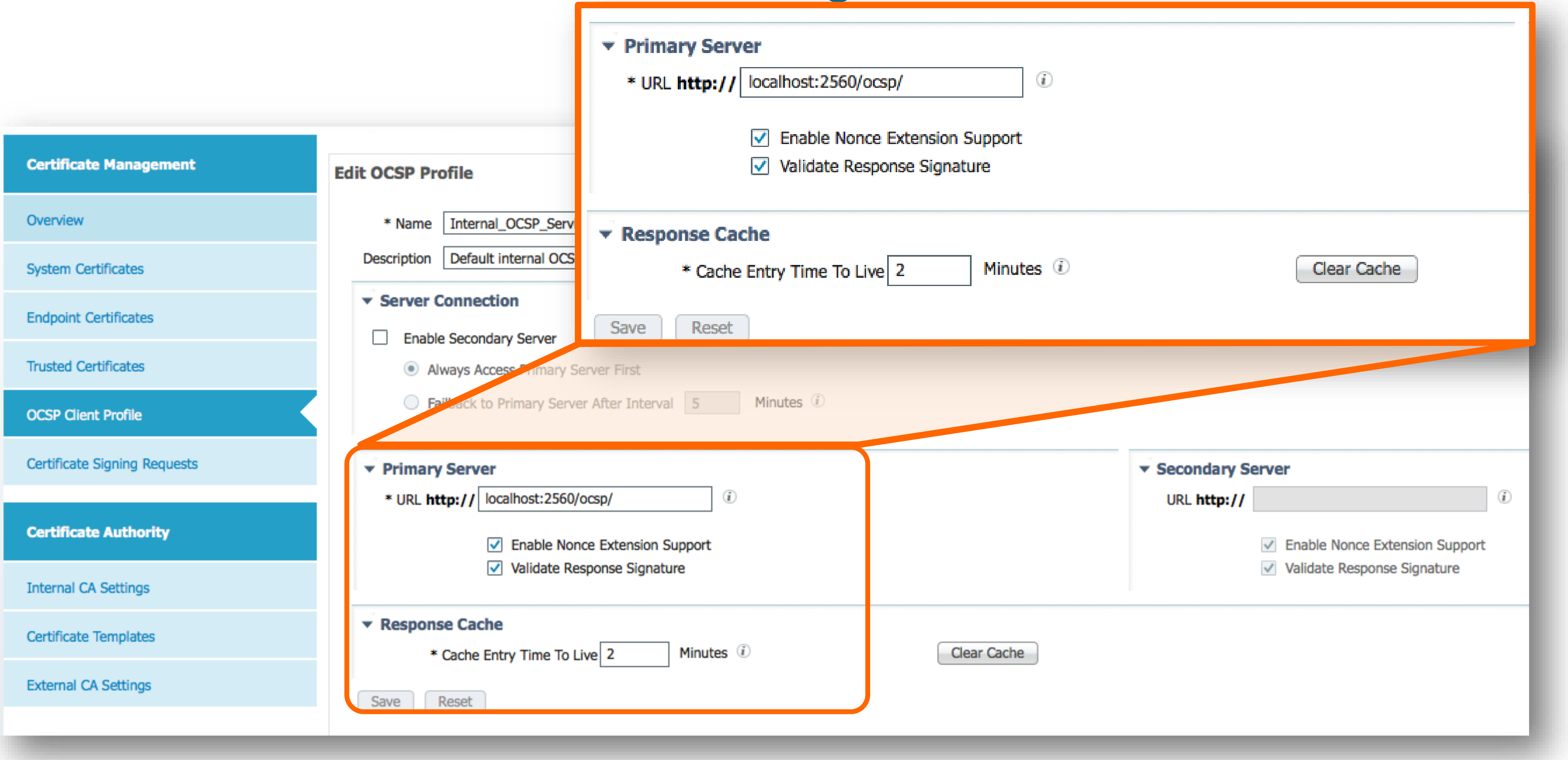
- Preferred method
- Provides near real-time updates
- Allows near real-time request
- Think: Policeman checking from laptop in squad-car, with live query into DMV Database.

CRL

- A signed document published on website
- Periodically downloaded and stored locally
- The server examines the CRL to see if the client's cert was revoked already.
- Think: Policeman having a list of suspended drivers in his squad car.

Note: ISE does not use the CRL field in the cert, only the local configuration.

Default Internal OCSP Configuration



Edit OCSP Profile

* Name Internal_OCSP_Serv

Description Default internal OCS

Server Connection

□ Enable Secondary Server

● Always Access Primary Server First

○ Fallback to Primary Server After Interval 5 Minutes

Primary Server

* URL **http://** localhost:2560/ocsp/

☑ Enable Nonce Extension Support

☑ Validate Response Signature

Secondary Server

URL **http://**

☑ Enable Nonce Extension Support

☑ Validate Response Signature

Response Cache

* Cache Entry Time To Live 2 Minutes

Primary Server

* URL **http://** localhost:2560/ocsp/

☑ Enable Nonce Extension Support

☑ Validate Response Signature

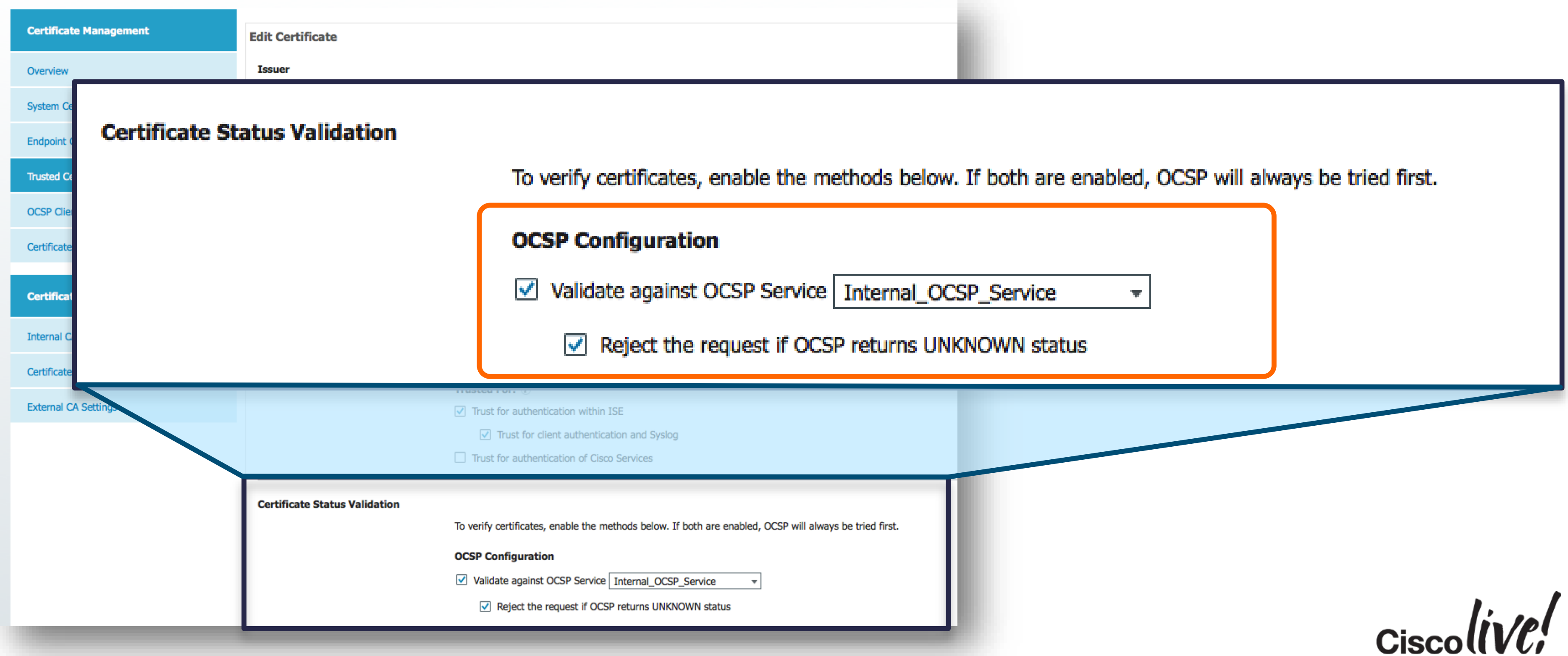
Response Cache

* Cache Entry Time To Live 2 Minutes

Clear Cache

Save Reset

OCSP Check



Edit Certificate

Issuer

Certificate Status Validation

To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first.

OCSP Configuration

☑ Validate against OCSP Service Internal_OCSP_Service ▾

☑ Reject the request if OCSP returns UNKNOWN status

Trusted For:

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

Certificate Status Validation

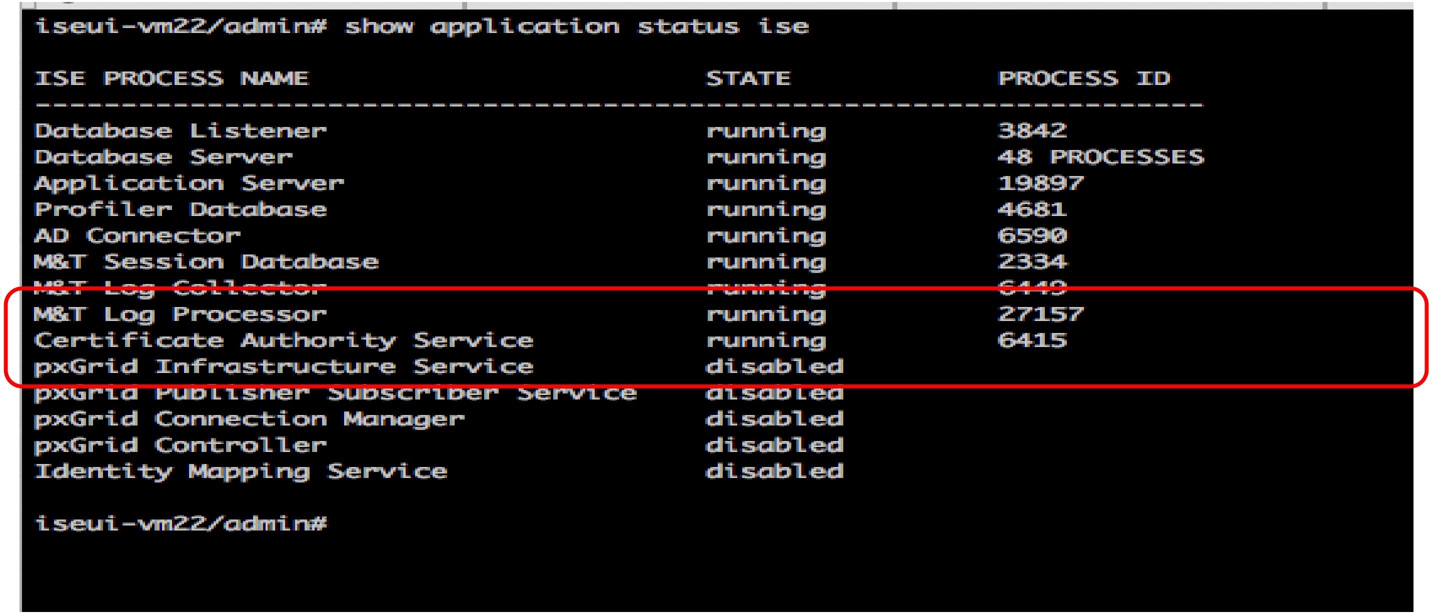
To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first.

OCSP Configuration

☑ Validate against OCSP Service Internal_OCSP_Service ▾

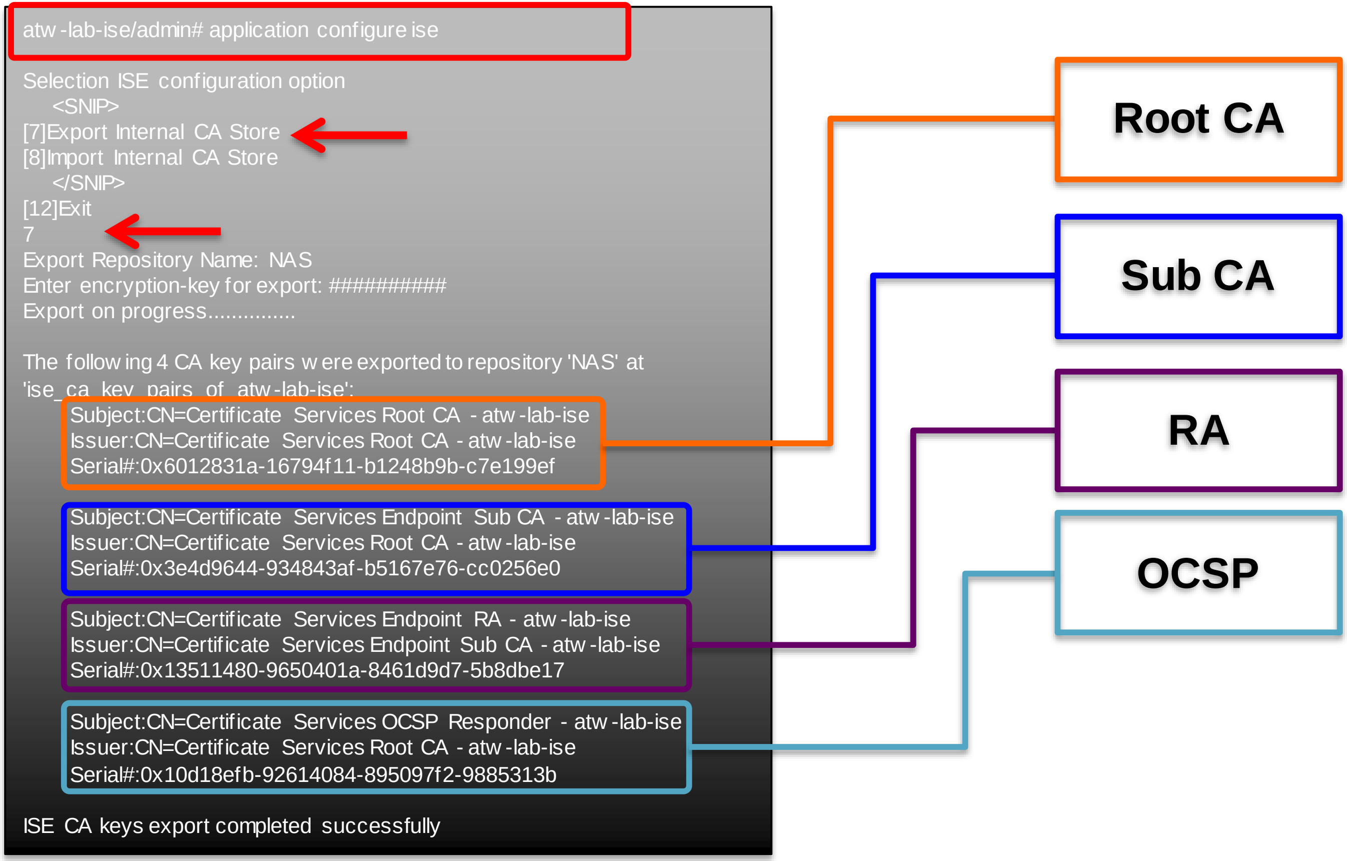
☑ Reject the request if OCSP returns UNKNOWN status

CA Server Status



```
iseui-vm22/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          3842
Database Server                        running          48 PROCESSES
Application Server                     running          19897
Profiler Database                      running          4681
AD Connector                           running          6590
M&T Session Database                   running          2334
M&T Log Collector                      running          6449
M&T Log Processor                      running          27157
Certificate Authority Service          running          6415
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
Identity Mapping Service               disabled

iseui-vm22/admin#
```

Export CA Certs



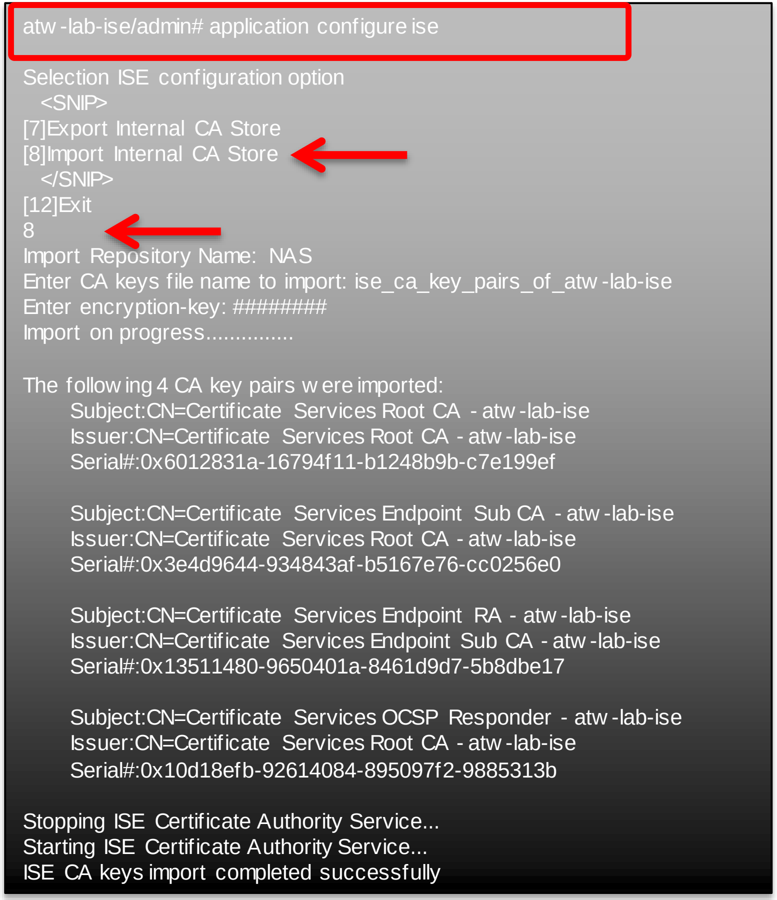
```
atw-lab-ise/admin# application configure ise

Selection ISE configuration option
    <SNIP>
[7]Export Internal CA Store
[8]Import Internal CA Store
    </SNIP>
[12]Exit
7
Export Repository Name: NAS
Enter encryption-key for export: ##########
Export on progress...............

The following 4 CA key pairs were exported to repository 'NAS' at
'ise_ca_key_pairs_of_atw-lab-ise':
      Subject:CN=Certificate Services Root CA - atw-lab-ise
      Issuer:CN=Certificate Services Root CA - atw-lab-ise
      Serial#:0x6012831a-16794f11-b1248b9b-c7e199ef

      Subject:CN=Certificate Services Endpoint Sub CA - atw-lab-ise
      Issuer:CN=Certificate Services Root CA - atw-lab-ise
      Serial#:0x3e4d9644-934843af-b5167e76-cc0256e0

      Subject:CN=Certificate Services Endpoint RA - atw-lab-ise
      Issuer:CN=Certificate Services Endpoint Sub CA - atw-lab-ise
      Serial#:0x13511480-9650401a-8461d9d7-5b8dbe17

      Subject:CN=Certificate Services OCSP Responder - atw-lab-ise
      Issuer:CN=Certificate Services Root CA - atw-lab-ise
      Serial#:0x10d18efb-92614084-895097f2-9885313b

ISE CA keys export completed successfully
```

Exporting the CA Certs to a Repository

Will be an Encrypted GPG Bundle

Four Key Pairs

Import of CA Certs

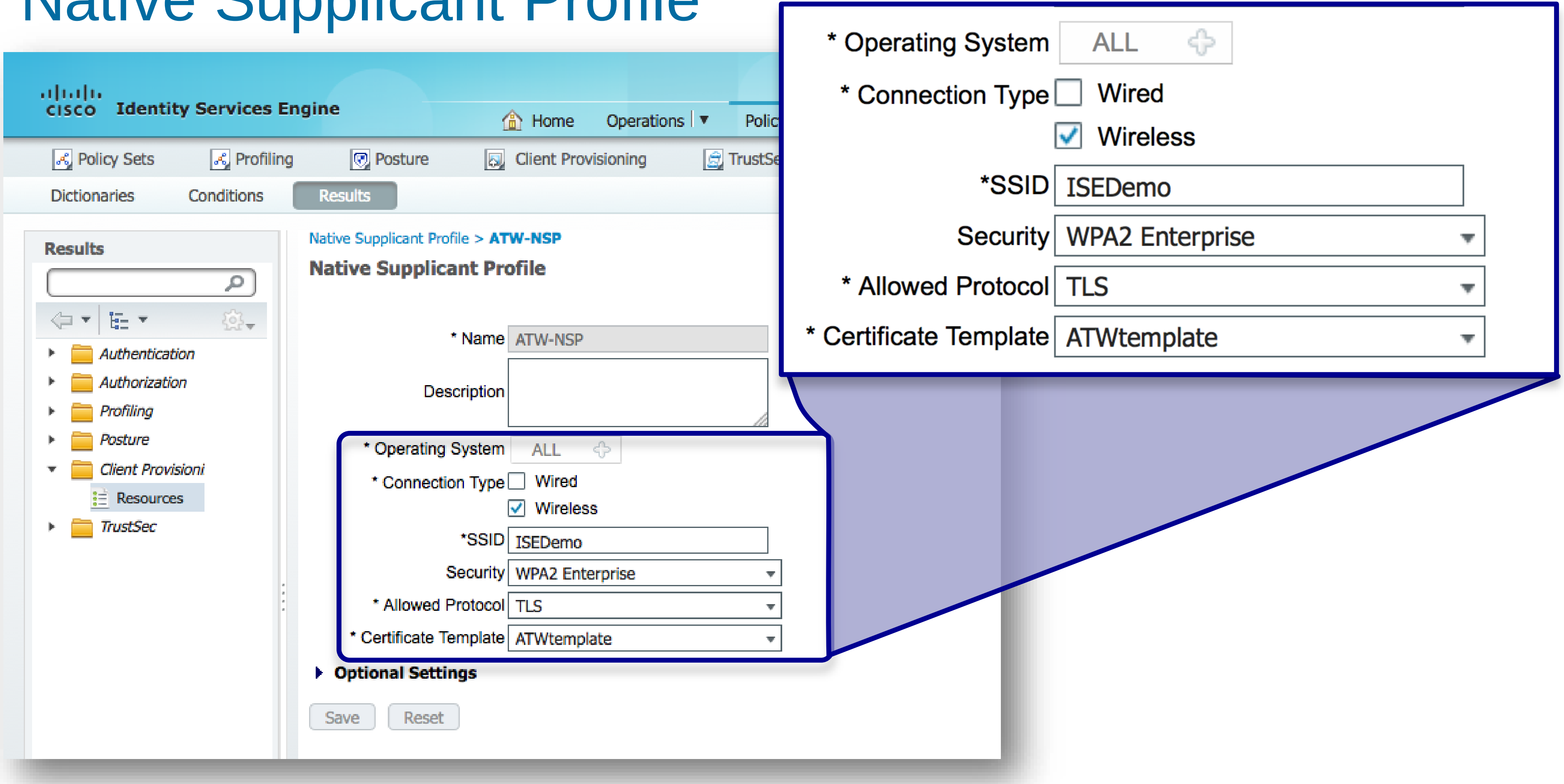


```
atw-lab-ise/admin# application configure ise

Selection ISE configuration option
  <SNIP>
[7]Export Internal CA Store
[8]Import Internal CA Store
  </SNIP>
[12]Exit
8
Import Repository Name: NAS
Enter CA keys file name to import: ise_ca_key_pairs_of_atw-lab-ise
Enter encryption-key: ########
Import on progress...............

The following 4 CA key pairs were imported:
      Subject:CN=Certificate Services Root CA - atw-lab-ise
      Issuer:CN=Certificate Services Root CA - atw-lab-ise
      Serial#:0x6012831a-16794f11-b1248b9b-c7e199ef

      Subject:CN=Certificate Services Endpoint Sub CA - atw-lab-ise
      Issuer:CN=Certificate Services Root CA - atw-lab-ise
      Serial#:0x3e4d9644-934843af-b5167e76-cc0256e0

      Subject:CN=Certificate Services Endpoint RA - atw-lab-ise
      Issuer:CN=Certificate Services Endpoint Sub CA - atw-lab-ise
      Serial#:0x13511480-9650401a-8461d9d7-5b8dbe17

      Subject:CN=Certificate Services OCSP Responder - atw-lab-ise
      Issuer:CN=Certificate Services Root CA - atw-lab-ise
      Serial#:0x10d18efb-92614084-895097f2-9885313b

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

Always perform the certificate import to the secondary PAN

Ensures that the same PKI Tree is always used

Native Supplicant Profile



Native Supplicant Profile > **ATW-NSP**

Native Supplicant Profile

* Name	ATW-NSP
Description	
* Operating System	ALL
* Connection Type	□ Wired ☑ Wireless
*SSID	ISEDemo
Security	WPA2 Enterprise
* Allowed Protocol	TLS
* Certificate Template	ATWtemplate

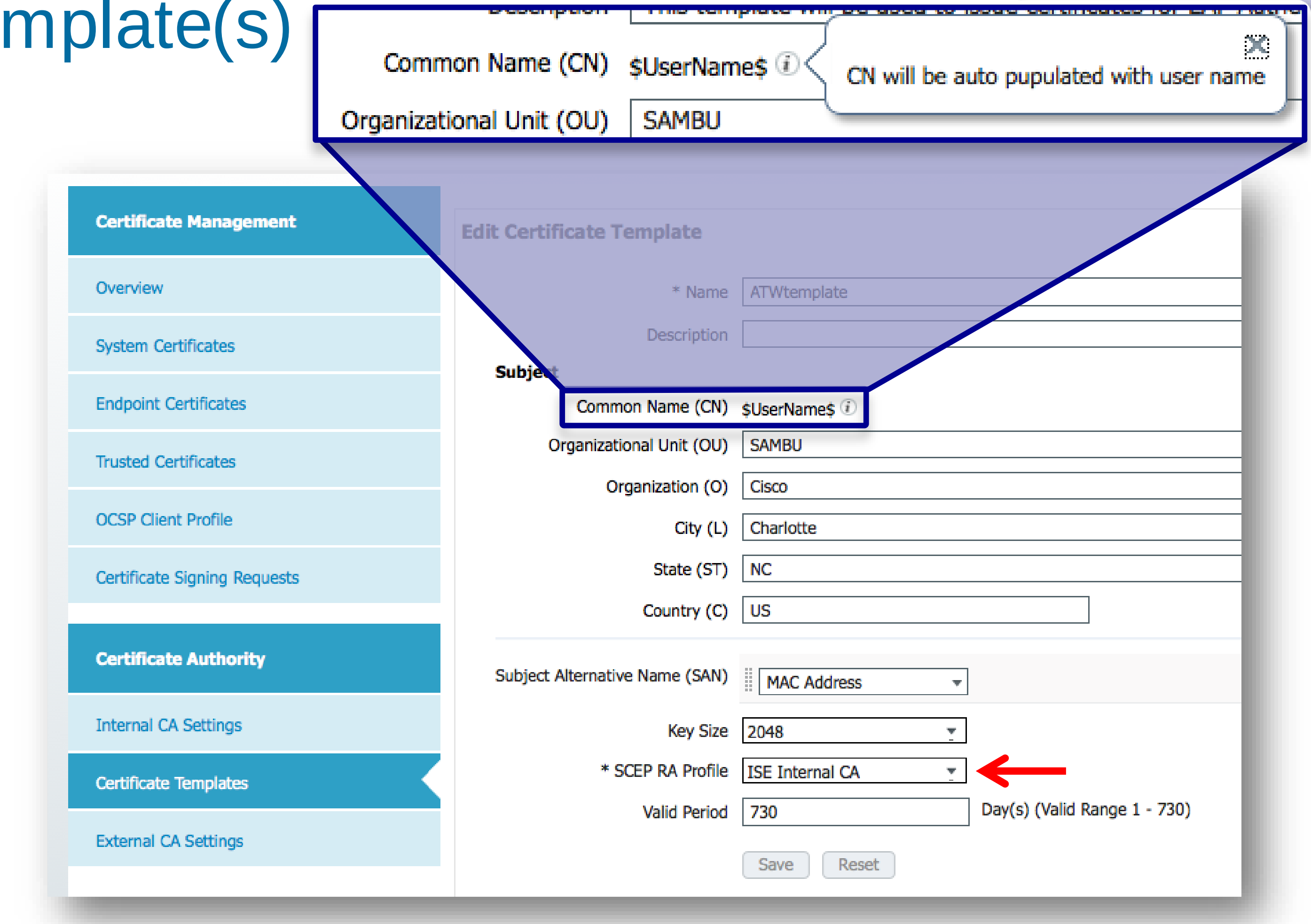
Optional Settings

Save Reset

* Operating System ALL
* Connection Type □ Wired ☑ Wireless
*SSID ISEDemo
Security WPA2 Enterprise
* Allowed Protocol TLS
* Certificate Template ATWtemplate

Certificate Template(s)

- Define Internal or External CA
- Set the Key Sizes
- SAN Field Options:
  - MAC Address
  - No Free-Form Adds..
- Set length of validity



Common Name (CN)	$UserName$
Organizational Unit (OU)	SAMBU

CN will be auto pupulated with user name

Edit Certificate Template

* Name	ATWtemplate
Description	

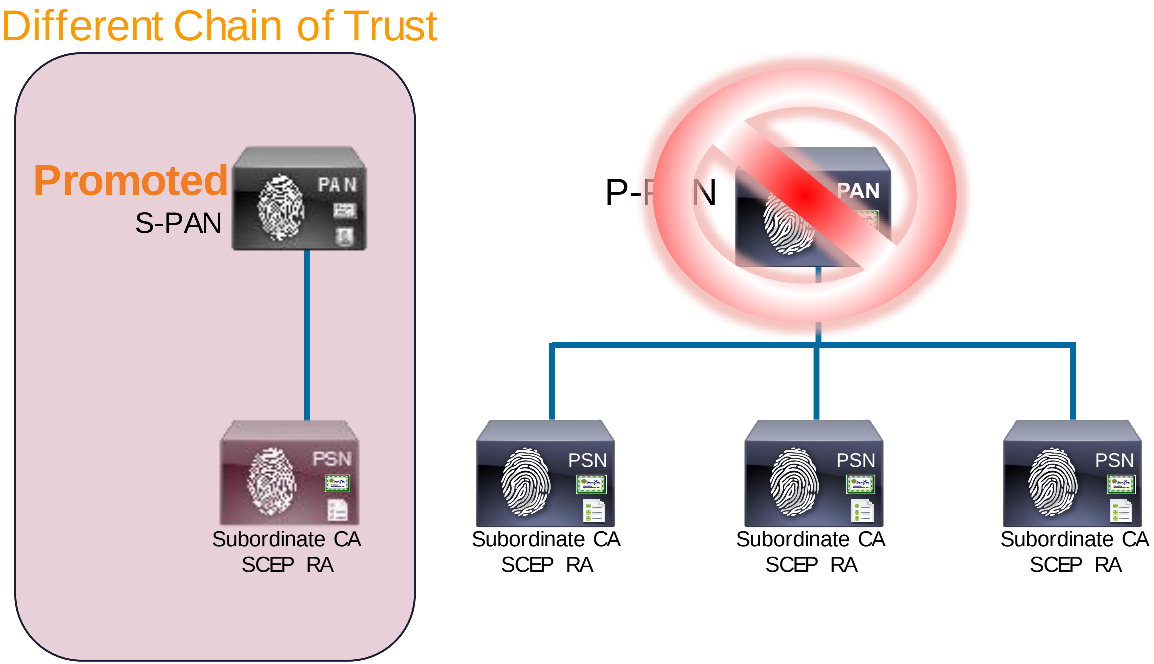
Subject

Common Name (CN)	$UserName$
Organizational Unit (OU)	SAMBU
Organization (O)	Cisco
City (L)	Charlotte
State (ST)	NC
Country (C)	US
Subject Alternative Name (SAN)	MAC Address
Key Size	2048
* SCEP RA Profile	ISE Internal CA
Valid Period	730 Day(s) (Valid Range 1 - 730)

Other Factoids

- No temporary revocations (cannot un-revoke)
  - Use Blacklist instead
- ISE does not publish a CRL, OCSP only
- ISE does not use the CRL distributions listed in endpoint Certs, it uses the manual configured CRL distribution point
- Cannot selectively enable/disable CA service on PSNs. All or nothing.
- When issuing cert from PSN, it will be subordinate to the PAN

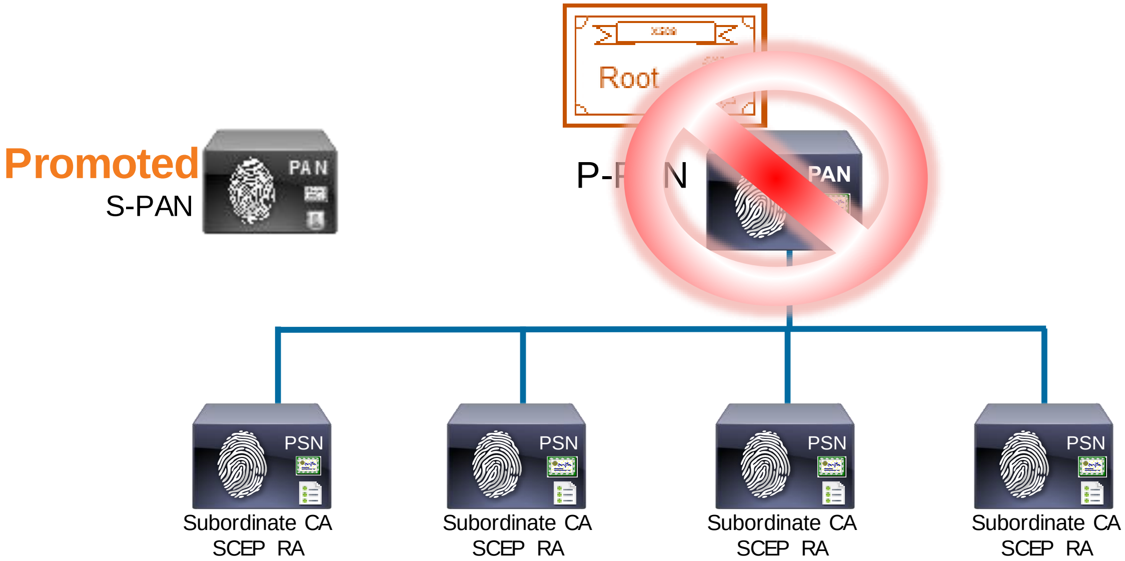
ISE CA: Dual Root Phenomenon



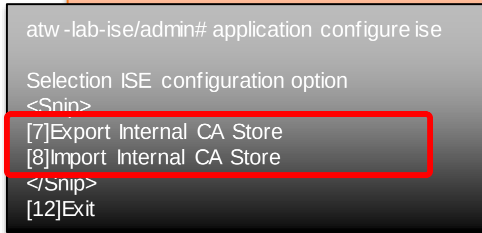
- The 4th PSN added to Cube while S-PAN temporarily the root.
- Now is a different chain of trust!

ISE CA: Dual Root Phenomenon

Single Chain of Trust



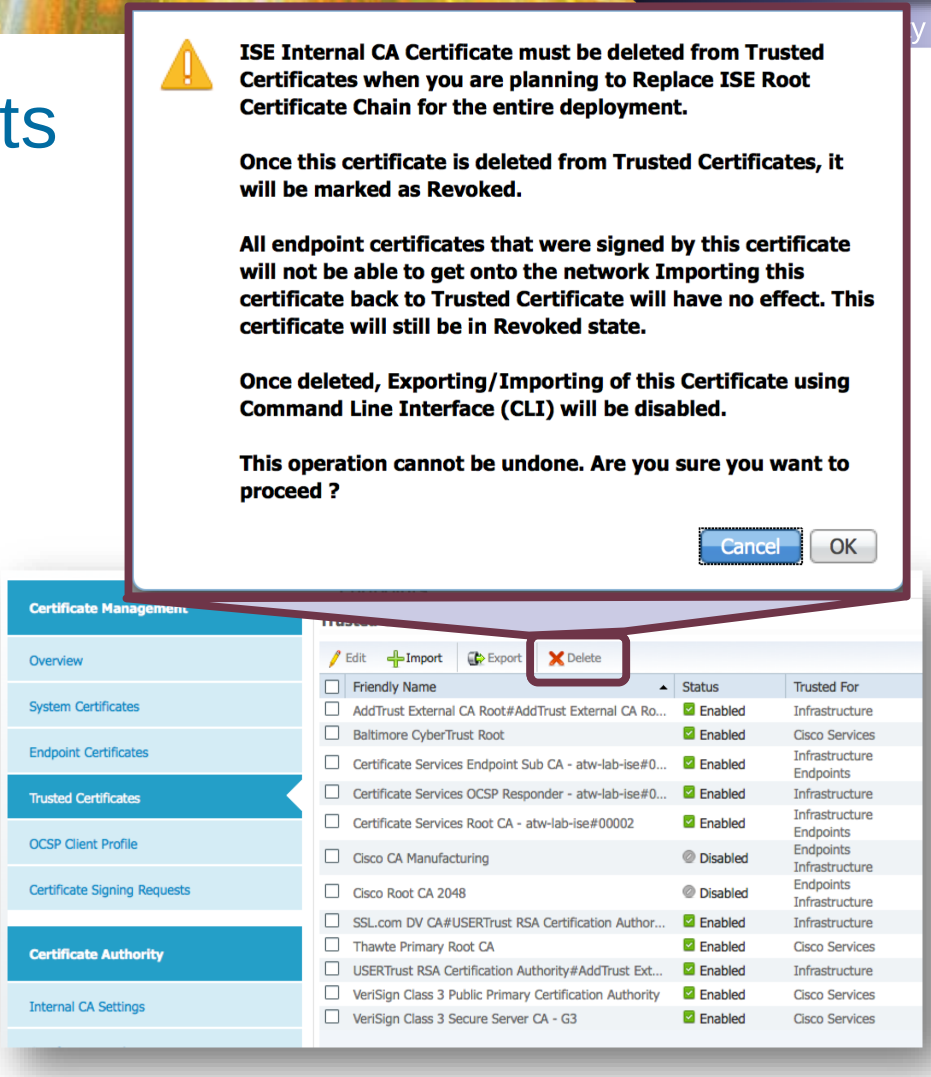
- Export Root CA & Import into S-PAN
- The 4th PSN added to Cube while S-PAN temporarily the root.
- S-PAN has same Chain of Trust



```
atw-lab-ise/admin# application configure ise

Selection ISE configuration option
<Snip>
[7]Export Internal CA Store
[8]Import Internal CA Store
</Snip>
[12]Exit
```

Do Not Delete ISE CA Certs

- Will Revoke the Certificate from CA
  - All Endpoint Certificates will now be Invalid & Rejected
  - Cannot Undo



ISE Internal CA Certificate must be deleted from Trusted Certificates when you are planning to Replace ISE Root Certificate Chain for the entire deployment.

Once this certificate is deleted from Trusted Certificates, it will be marked as Revoked.

All endpoint certificates that were signed by this certificate will not be able to get onto the network Importing this certificate back to Trusted Certificate will have no effect. This certificate will still be in Revoked state.

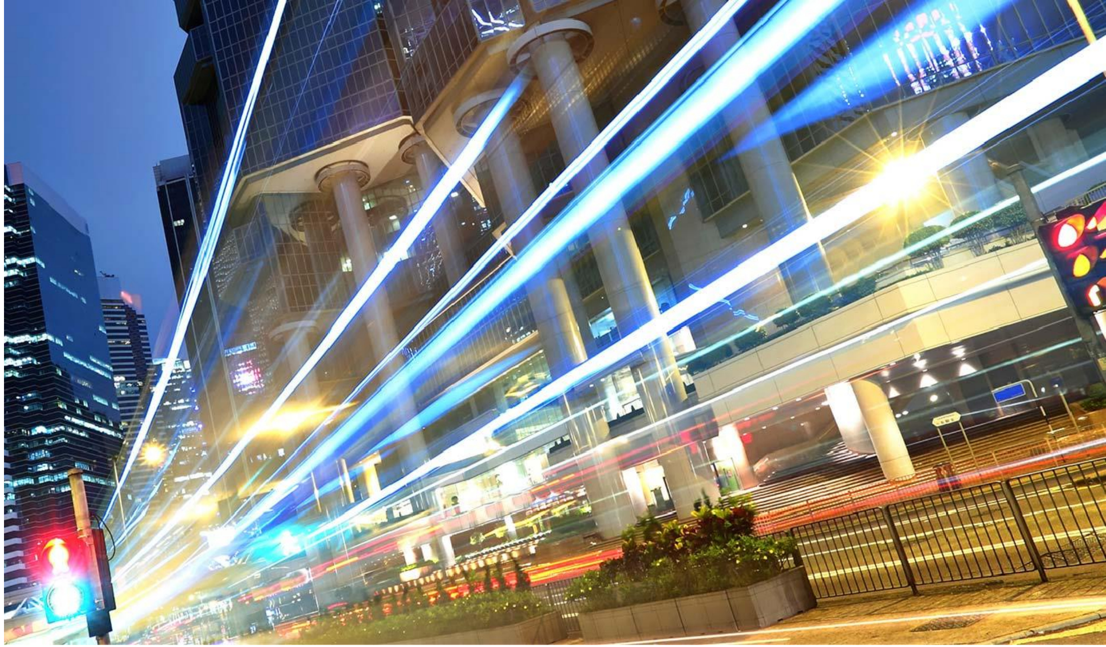
Once deleted, Exporting/Importing of this Certificate using Command Line Interface (CLI) will be disabled.

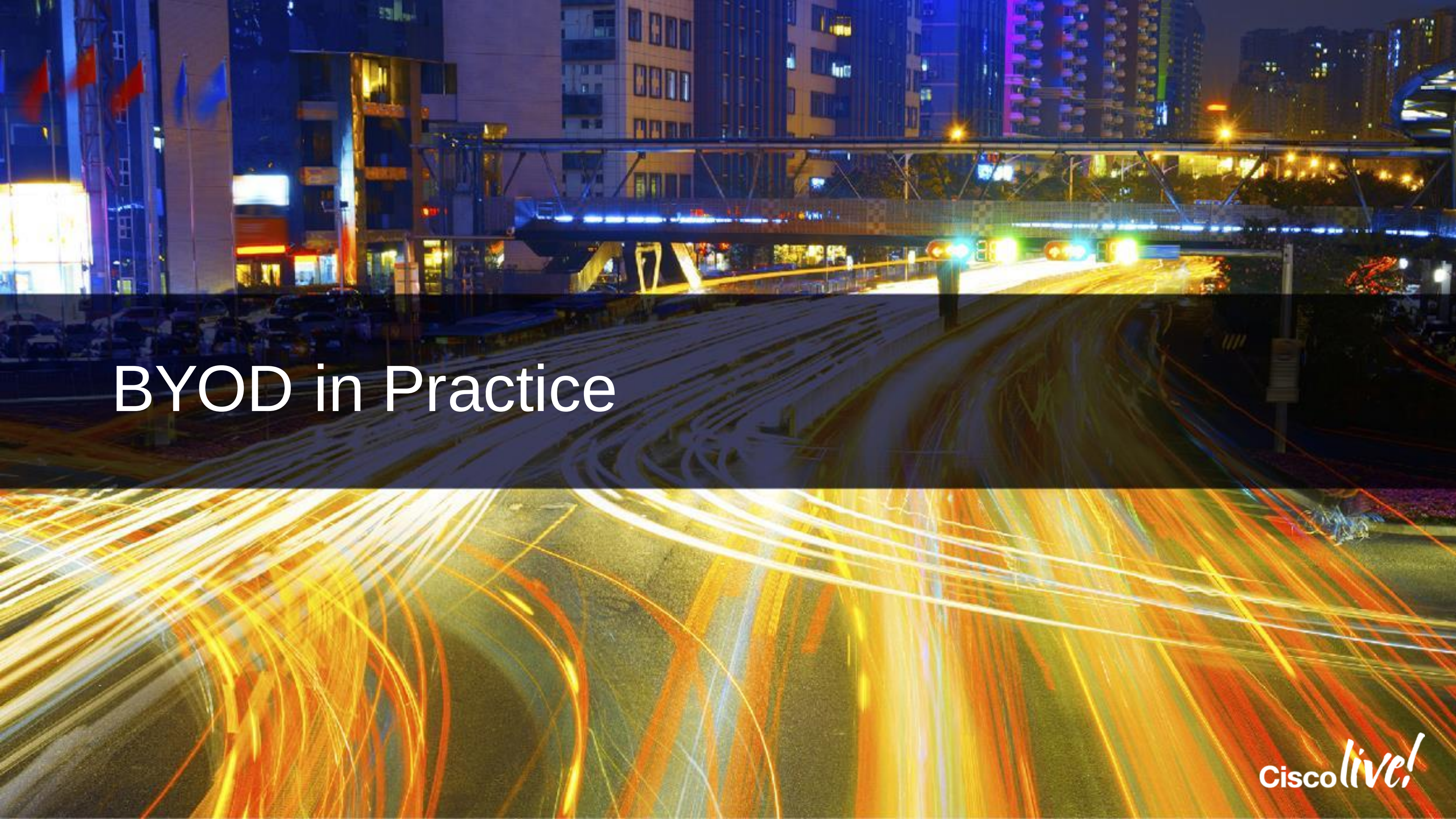
This operation cannot be undone. Are you sure you want to proceed ?

☐	Friendly Name	Status	Trusted For
☐	AddTrust External CA Root#AddTrust External CA Ro...	☑ Enabled	Infrastructure
☐	Baltimore CyberTrust Root	☑ Enabled	Cisco Services
☐	Certificate Services Endpoint Sub CA - atw-lab-ise#0...	☑ Enabled	Infrastructure Endpoints
☐	Certificate Services OCSP Responder - atw-lab-ise#0...	☑ Enabled	Infrastructure
☐	Certificate Services Root CA - atw-lab-ise#00002	☑ Enabled	Infrastructure Endpoints
☐	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure
☐	Cisco Root CA 2048	Disabled	Endpoints Infrastructure
☐	SSL.com DV CA#USERTrust RSA Certification Author...	☑ Enabled	Infrastructure
☐	Thawte Primary Root CA	☑ Enabled	Cisco Services
☐	USERTrust RSA Certification Authority#AddTrust Ext...	☑ Enabled	Infrastructure
☐	VeriSign Class 3 Public Primary Certification Authority	☑ Enabled	Cisco Services
☐	VeriSign Class 3 Secure Server CA - G3	☑ Enabled	Cisco Services

Agenda

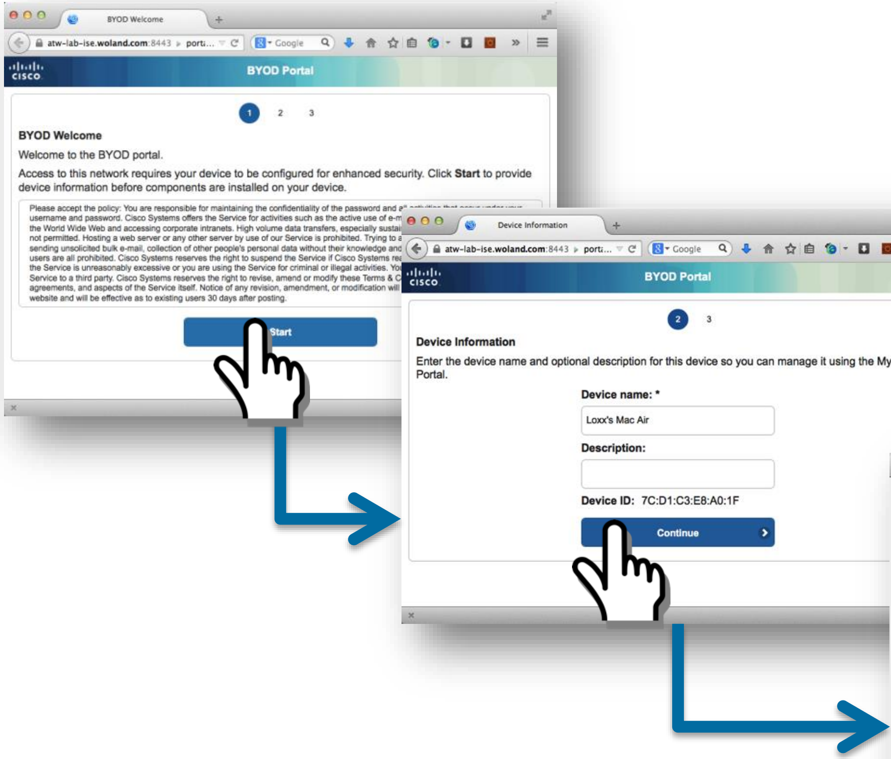
- Introduction
- Certificates, Certificates, Certificates
- BYOD Best Practices
- Integrating with Cisco and Non-Cisco
- ISE in a Security EcoSystem
- Serviceability & Troubleshooting
- Staged Deployments (Time Permitting)
- Conclusion





BYOD in Practice

Java-Less Provisioning



BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and a[illegible] username and password. Cisco Systems offers the Service for activities such as the active use of e-m[illegible] the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustai[illegible] not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to a[illegible] sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and[illegible] users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems rea[illegible] the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You[illegible] Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & C[illegible] agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will [illegible] website and will be effective as to existing users 30 days after posting.

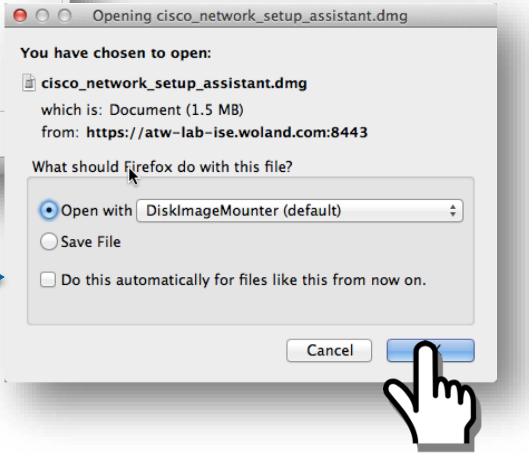
Device Information

Enter the device name and optional description for this device so you can manage it using the My Devices Portal.

Device name: * Loxx's Mac Air

Description:

Device ID: 7C:D1:C3:E8:A0:1F



Opening cisco_network_setup_assistant.dmg

You have chosen to open:

cisco_network_setup_assistant.dmg

which is: Document (1.5 MB)

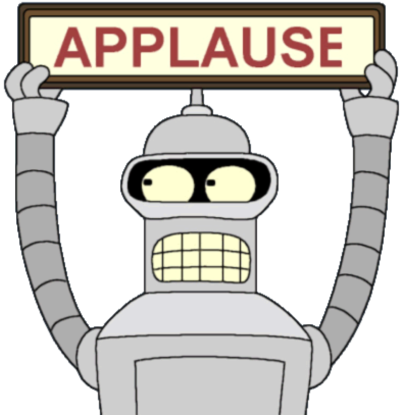
from: **https://atw-lab-ise.woland.com:8443**

What should Firefox do with this file?

● Open with DiskImageMounter (default)

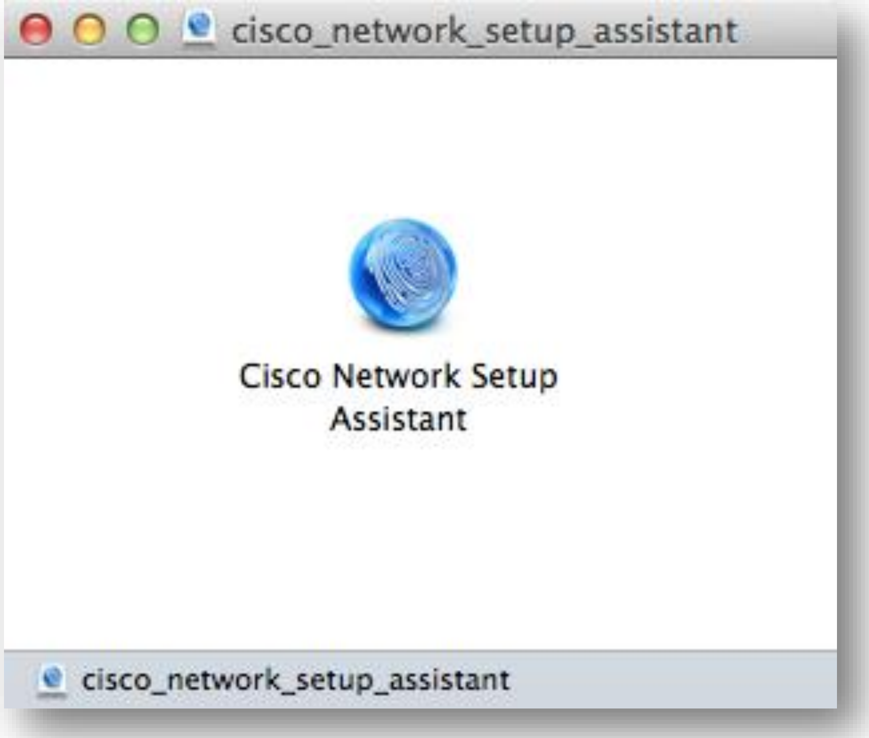
○ Save File

□ Do this automatically for files like this from now on.



Java-Less Provisioning

- Downloads as DMG
- Double-Click to Run App



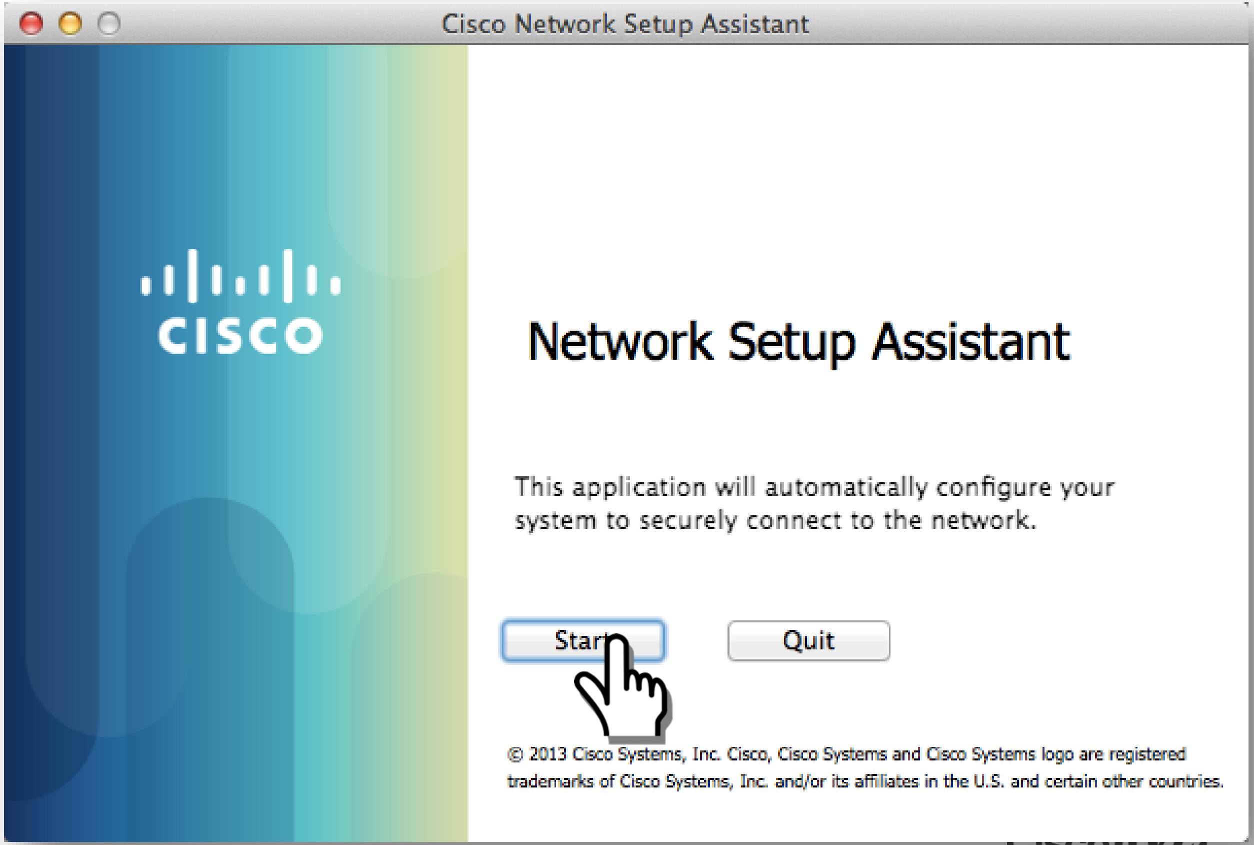
cisco_network_setup_assistant

Cisco Network Setup Assistant

cisco_network_setup_assistant

Java-Less Provisioning

- Downloads as DMG
- Double-Click to Run App



Cisco Network Setup Assistant

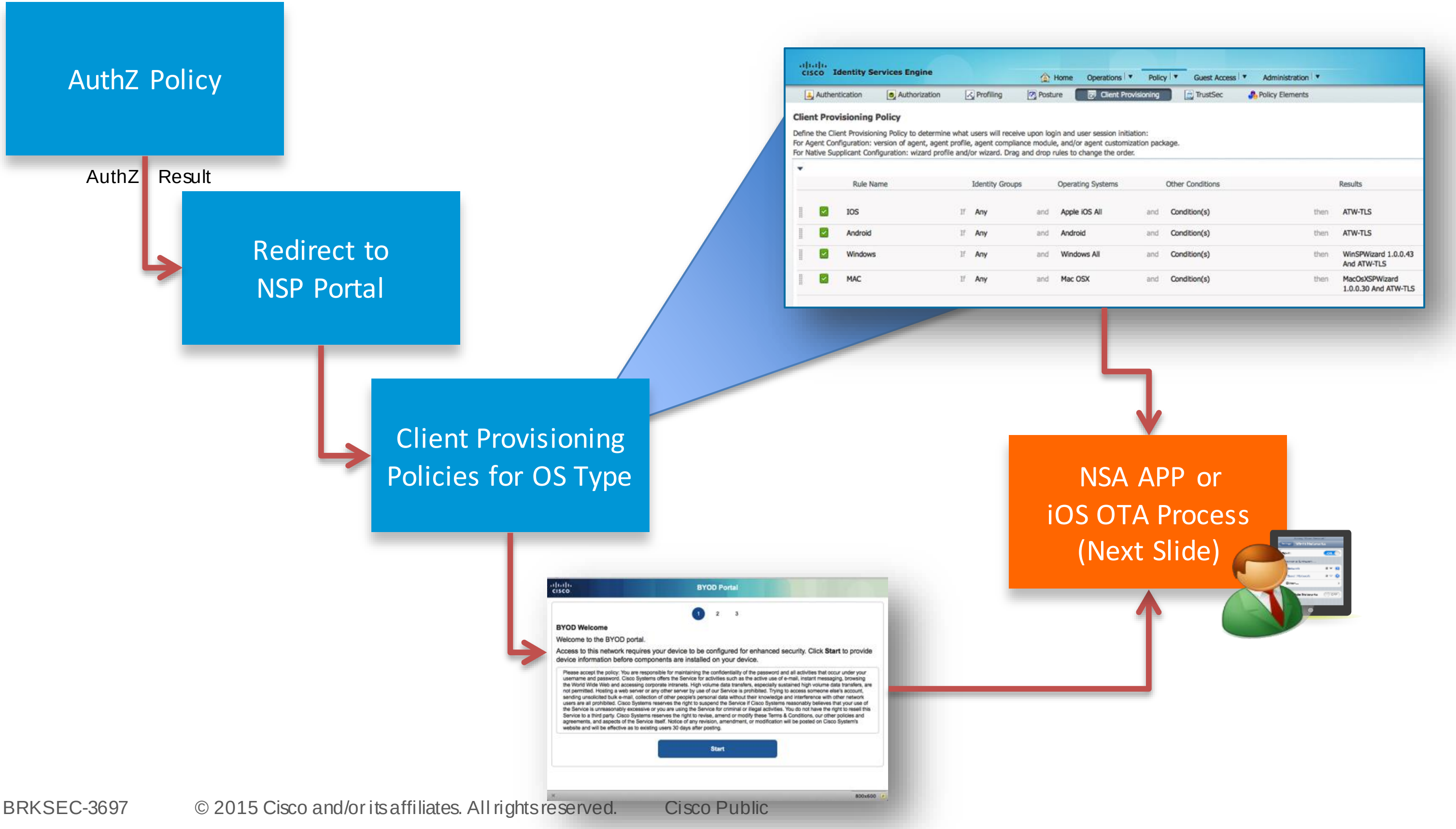
Network Setup Assistant

This application will automatically configure your system to securely connect to the network.

© 2013 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Refresher: Native Supplicant Provisioning Flow

Single-SSID Flow


AuthZ Policy
AuthZ Result
Redirect to NSP Portal
Client Provisioning Policies for OS Type
NSA APP or iOS OTA Process (Next Slide)

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	ATW-TLS
☑	Android	If	Any	and	Android	and	Condition(s)	then	ATW-TLS
☑	Windows	If	Any	and	Windows All	and	Condition(s)	then	WinSPWizard 1.0.0.43 And ATW-TLS
☑	MAC	If	Any	and	Mac OSX	and	Condition(s)	then	MacOsXSPWizard 1.0.0.30 And ATW-TLS

BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Refresher: Native Supplicant Provisioning Flow

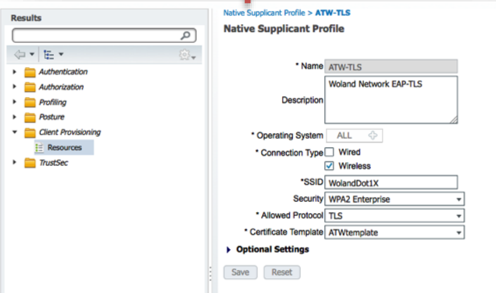
NSA App Or Apple OTA

Native Supplicant Profile

Certificate Template

SCEP Certificate Provisioning & Native Supplicant Profile

CoA



Native Supplicant Profile > **ATW-TLS**

Native Supplicant Profile

* Name: ATW-TLS

Description: Woland Network EAP-TLS

* Operating System: ALL

* Connection Type: □ Wired ☑ Wireless

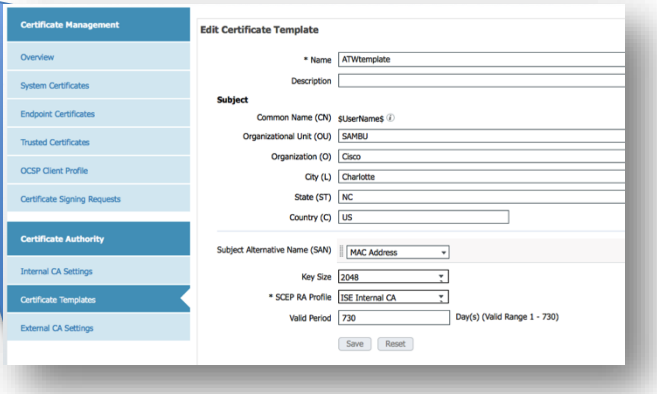
*SSID: WolandDot1X

Security: WPA2 Enterprise

* Allowed Protocol: TLS

* Certificate Template: ATWtemplate

Optional Settings



Edit Certificate Template

* Name: ATWtemplate

Description:

Subject

Common Name (CN): $UserName$

Organizational Unit (OU): SAMBU

Organization (O): Cisco

City (L): Charlotte

State (ST): NC

Country (C): US

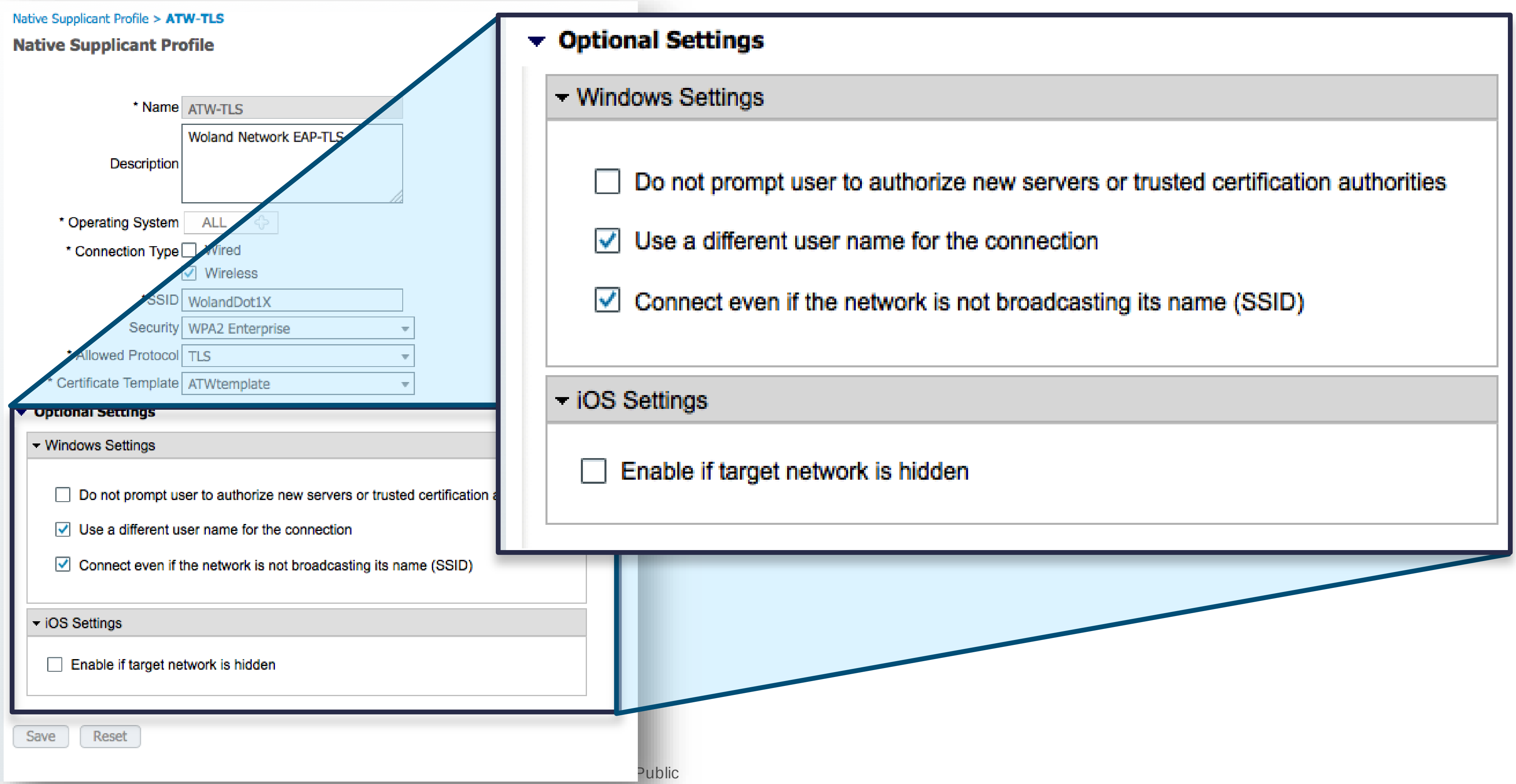
Subject Alternative Name (SAN): MAC Address

Key Size: 2048

* SCEP RA Profile: ISE Internal CA

Valid Period: 730 Day(s) (Valid Range 1 - 730)

New: Windows & iOS Settings in NSP



Native Supplicant Profile > **ATW-TLS**

Native Supplicant Profile

* Name	ATW-TLS
Description	Woland Network EAP-TLS
* Operating System	ALL
* Connection Type	□ Wired ☑ Wireless
* SSID	WolandDot1X
Security	WPA2 Enterprise
* Allowed Protocol	TLS
* Certificate Template	ATWtemplate

Optional Settings

Windows Settings

- □ Do not prompt user to authorize new servers or trusted certification a
- ☑ Use a different user name for the connection
- ☑ Connect even if the network is not broadcasting its name (SSID)

iOS Settings

- □ Enable if target network is hidden

Optional Settings

Windows Settings

- □ Do not prompt user to authorize new servers or trusted certification authorities
- ☑ Use a different user name for the connection
- ☑ Connect even if the network is not broadcasting its name (SSID)

iOS Settings

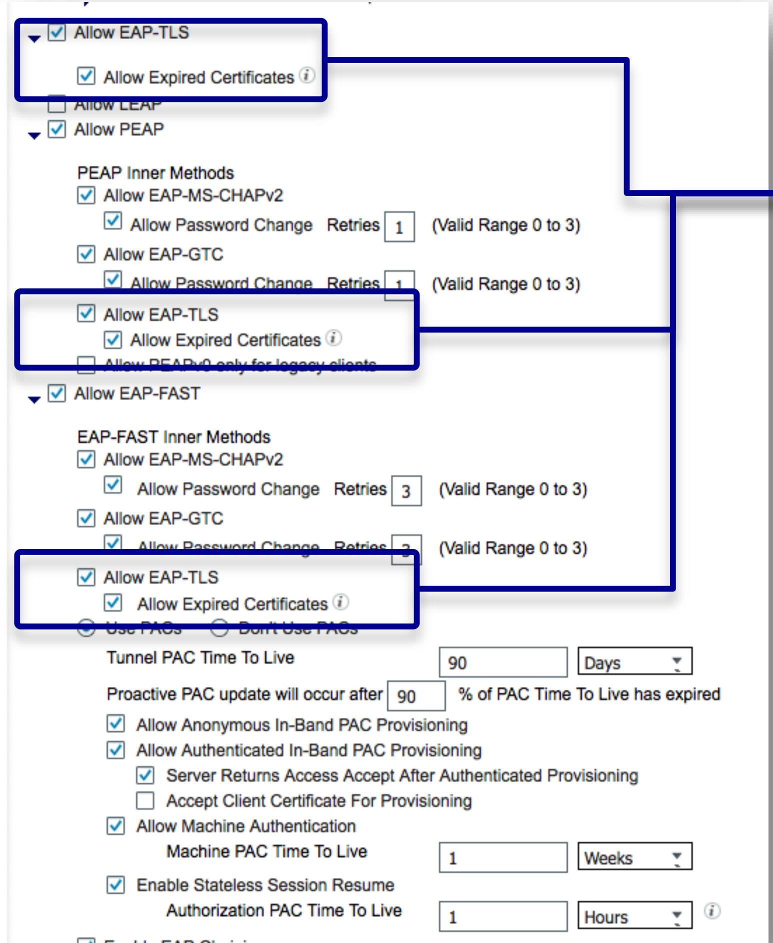
- □ Enable if target network is hidden

Renewing Certificates

1.2.1

	Works	Comments
Before Expiry		
iOS	✓	
Android	✓	
Windows	✓	
MAC-OSX	✓	
After Expiry		
iOS	✓	
Android	✓	
Windows	✗	Supplicant will not use an expired cert
MAC-OSX	✓	

Allowing Expired Certificates



☑ Allow EAP-TLS

☑ Allow Expired Certificates ⓘ

□ Allow LEAP

☑ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-GTC

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-TLS

☑ Allow Expired Certificates ⓘ

□ Allow PEAPv0 only for legacy clients

☑ Allow EAP-FAST

EAP-FAST Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 3 (Valid Range 0 to 3)

☑ Allow EAP-GTC

☑ Allow Password Change Retries 3 (Valid Range 0 to 3)

☑ Allow EAP-TLS

☑ Allow Expired Certificates ⓘ

● Use PACs ○ Don't Use PACs

Tunnel PAC Time To Live 90 Days

Proactive PAC update will occur after 90 % of PAC Time To Live has expired

☑ Allow Anonymous In-Band PAC Provisioning

☑ Allow Authenticated In-Band PAC Provisioning

☑ Server Returns Access Accept After Authenticated Provisioning

□ Accept Client Certificate For Provisioning

☑ Allow Machine Authentication

Machine PAC Time To Live 1 Weeks

☑ Enable Stateless Session Resume

Authorization PAC Time To Live 1 Hours ⓘ

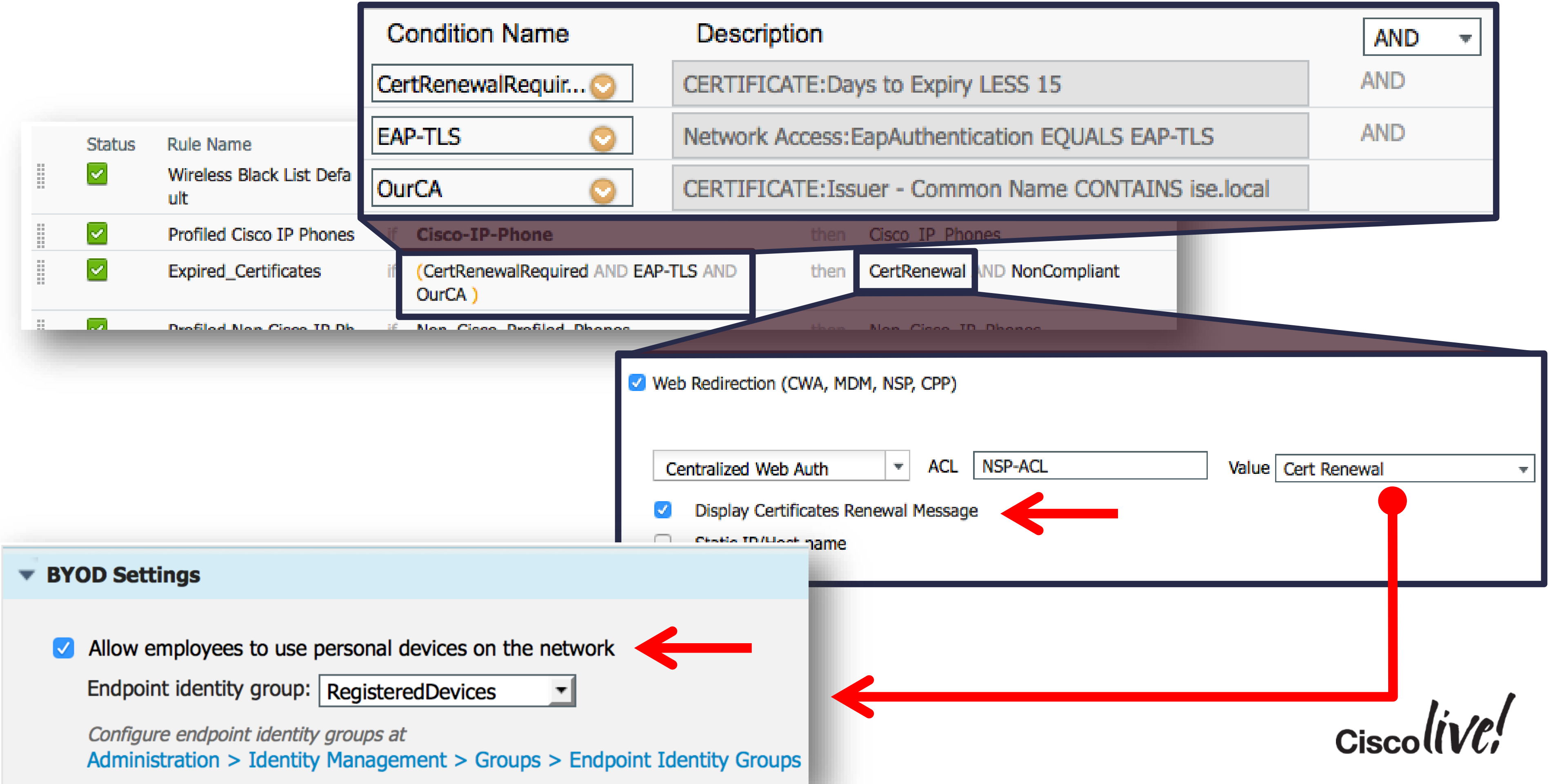
☑ Enable EAP Chaining

Policy > Policy Elements > Results > Authentication > Allowed Protocols

May allow expired certs for EAP-TLS

- Pure EAP-TLS
- EAP-TLS as an Inner Method

Redirect Expired Certs



Condition Name	Description	AND
CertRenewalRequir...	CERTIFICATE:Days to Expiry LESS 15	AND
EAP-TLS	Network Access:EapAuthentication EQUALS EAP-TLS	AND
OurCA	CERTIFICATE:Issuer - Common Name CONTAINS ise.local	

	Status	Rule Name		Conditions		Permissions
	☑	Wireless Black List Default				
	☑	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
	☑	Expired_Certificates	if	(CertRenewalRequired AND EAP-TLS AND OurCA)	then	CertRenewal AND NonCompliant
	☑	Profiled Non Cisco IP Ph	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones

☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth ACL NSP-ACL Value Cert Renewal

☑ Display Certificates Renewal Message

□ Static IP/Host name

BYOD Settings

☑ Allow employees to use personal devices on the network

Endpoint identity group: RegisteredDevices

Configure endpoint identity groups at
Administration > Identity Management > Groups > Endpoint Identity Groups

BYOD Security Practices from the Field

If you can, Create an Identity Group for your Corporate Owned Devices.

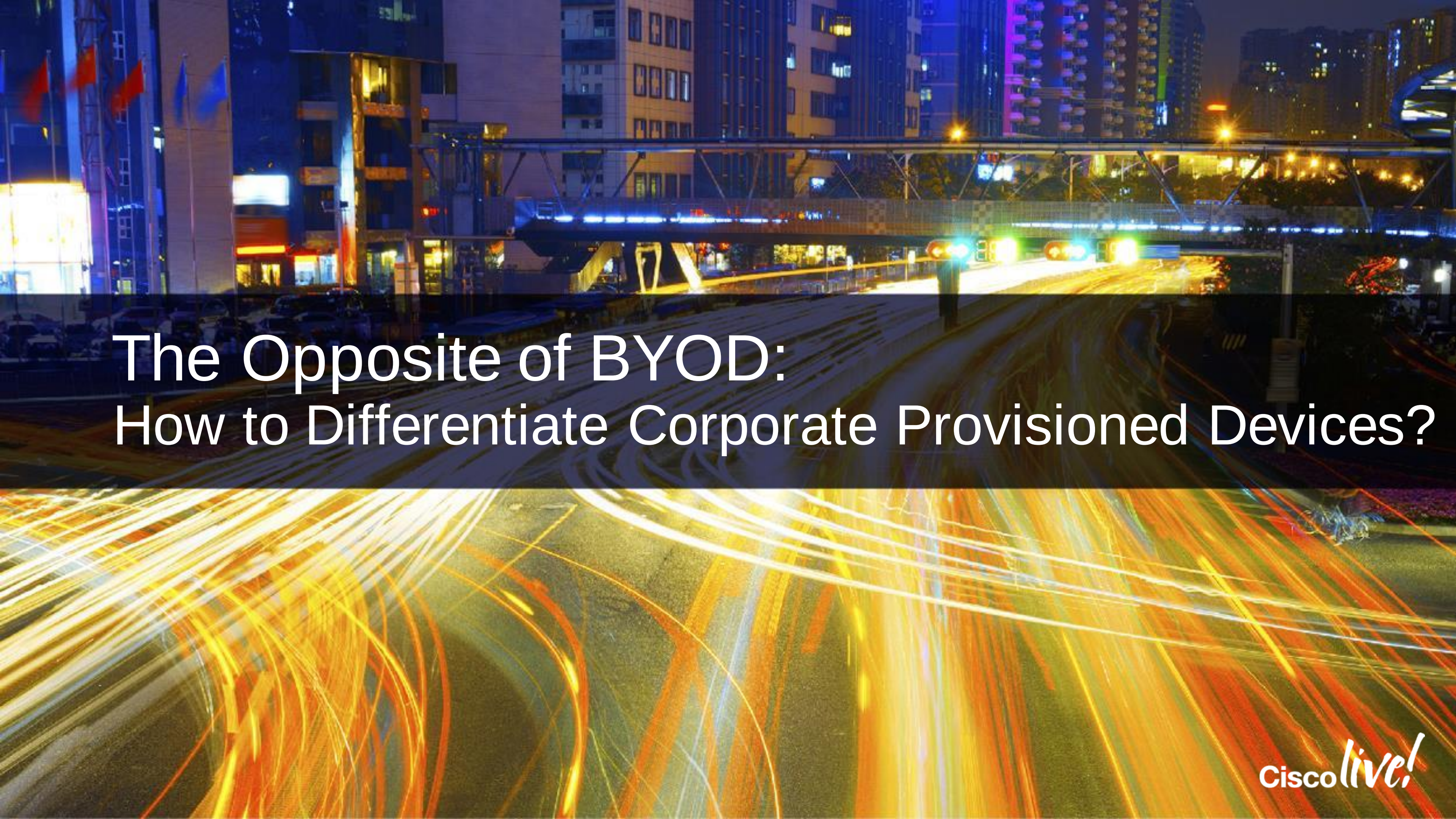
- May be populated by .CSV import, or REST API
- Uses the Endpoint ID Group for what it was designed to do: MAC Address Management

Provision Different Certificates for Corporate Owned Assets

- Available 1.3+, or if you use MDM to distribute the certificates

Don’t Trust ONLY the Certificate

- That is technically only authenticating the device, not the user

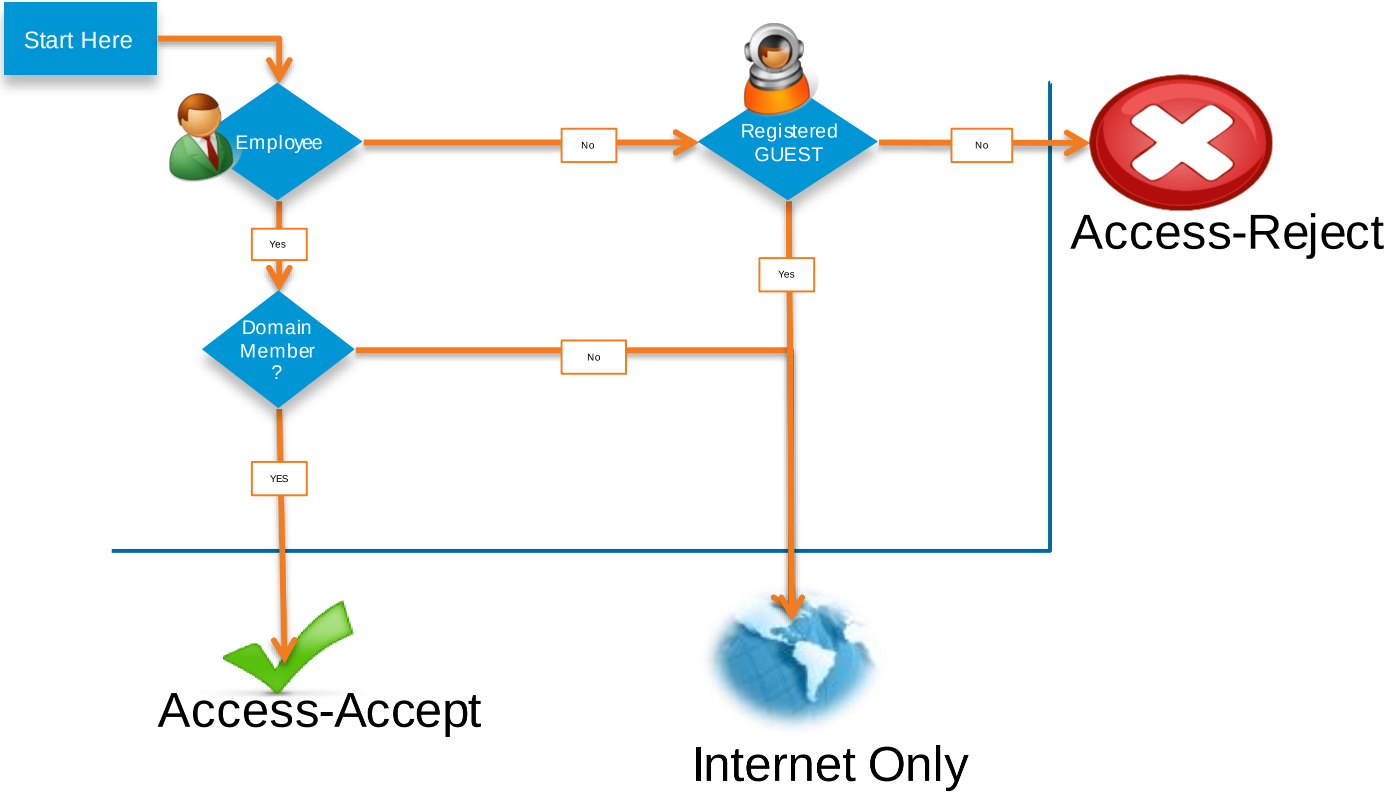


The Opposite of BYOD:

How to Differentiate Corporate Provisioned Devices?

Corporate Assets

Provide differentiated access for IT-managed systems.



Identifying the Machine AND the USER

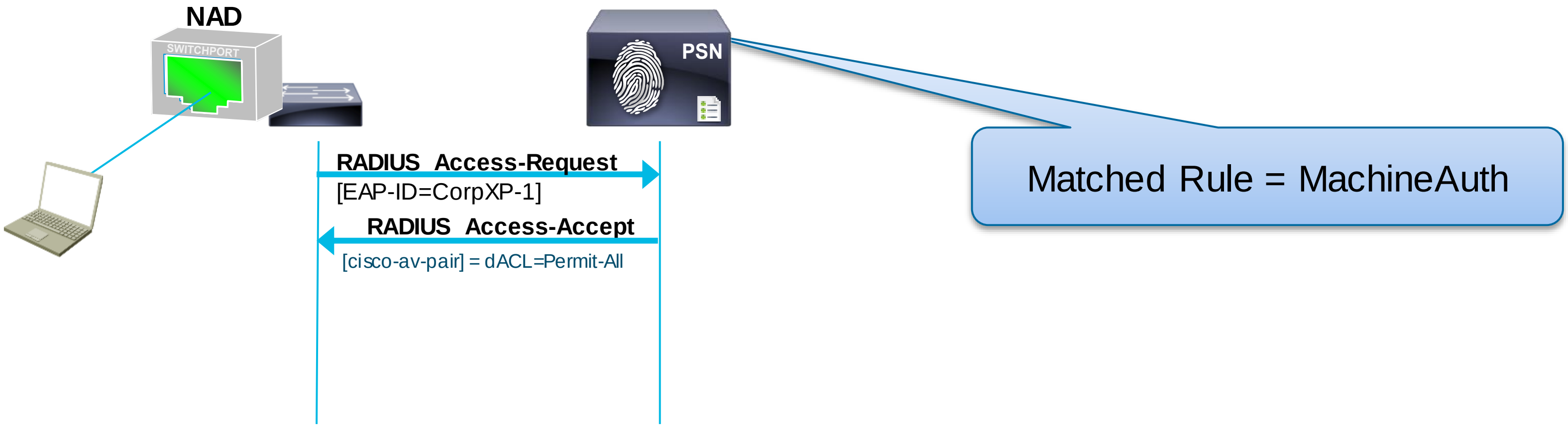
- Machine Access Restrictions (MAR)
- MAR provides a mechanism for the RADIUS server to search the previous authentications and look for a machine-authentication with the same Calling-Station-ID.
- This means the machine must do authenticate before the user.
  - i.e. Must log out, not use hibernate, etc….
- See the reference slides for more possible limitations.

Machine Access Restrictions (MAR)

MAR Cache

Calling-Station-ID 00:11:22:33:44:55 – Passed

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco IP Phone
MachineAuth	if	Domain Computers	then	MachineAuth
Employee	if	Employee & **WasMachineAuthenticated = true**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then	WEBAUTH		



RADIUS Access-Request
[EAP-ID=CorpXP-1]

RADIUS Access-Accept
[cisco-av-pair] = dACL=Permit-All

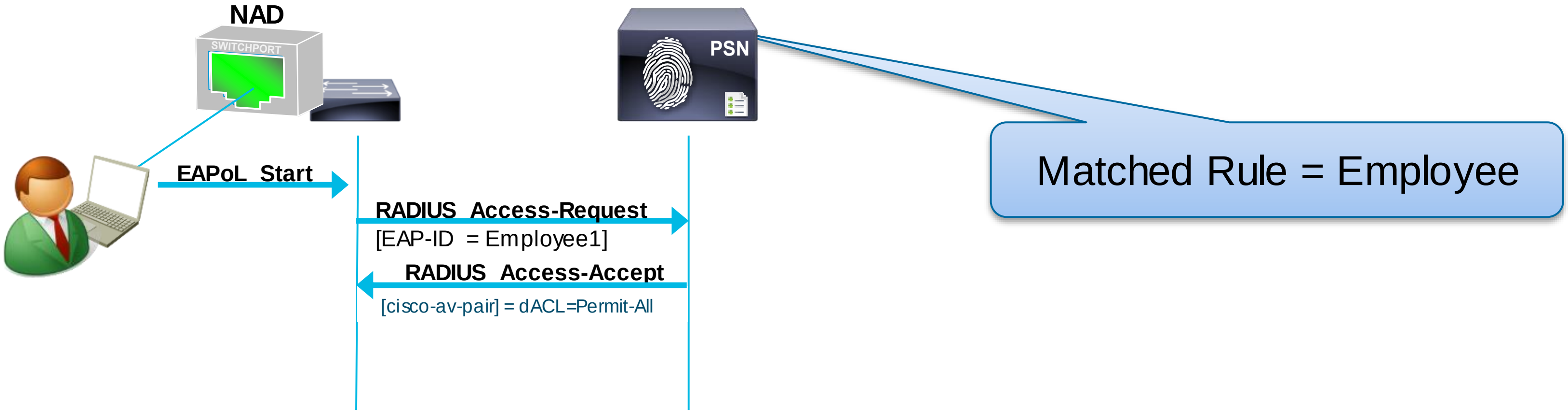
Matched Rule = MachineAuth

Machine Access Restrictions (MAR)

MAR Cache

Calling-Station-ID 00:11:22:33:44:55 – Passed

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAUth
Employee	if	Employee & **WasMachineAuthenticated = true**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	



EAPoL Start

RADIUS Access-Request
[EAP-ID = Employee1]

RADIUS Access-Accept
[cisco-av-pair] = dACL=Permit-All

Matched Rule = Employee

Machine Access Restrictions (MAR)

- Potential Issues with MAR

- Potential Issues with MAR:
  - **Wired/WiFi transitions**: Calling-Station-ID (MAC address) is used to link machine and user authentication; MAC address will change when laptop moves from wired to wireless breaking the MAR linkage.
  - **Machine state caching**: The state cache of previous machine authentications is neither persistent across ACS/ISE reboots nor replicated amongst ACS/ISE instances
  - **Hibernation/Standby**: 802.1X fails when the endpoint enters sleep/hibernate mode and then moves to a different location, or comes back into the office the following day, where machine auth cache is not present in new RADIUS server or has timed out.

Identifying the Machine AND the User

- The next chapter of authentication: EAP-Chaining

- IETF working group has published standard on Tunneled EAP (TEAP).
  - Next-Generation EAP method that provides all benefits of current EAP Types.
  - Also provides EAP-Chaining.
  - RFC-7170 http://www.rfc-editor.org/rfc/rfc7170.txt

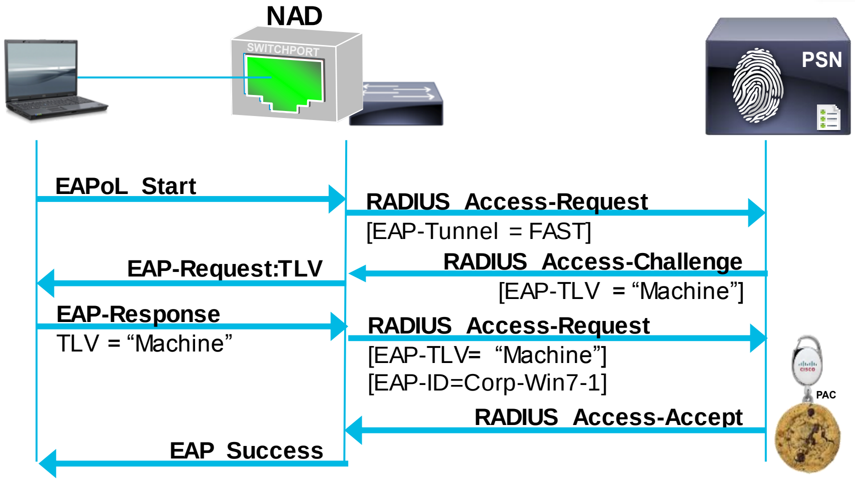
- Cisco has done it before TEAP is ready
  - EAP-FASTv2
  - AnyConnect 3.1
  - Identity Services Engine 1.1.1 (1.1 Minor Release)

EAP-Chaining

With AnyConnect 3.1.1 and ISE 1.1.1

1. Machine Authenticates
2. ISE Issues Machine AuthZ PAC

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco IP Phone
MachineAuth	if	Domain Computers	then	MachineAuth
Employee	if	Employee & **Network Access:EAPChainingResult = User and machine suceeded**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	



EAPoL Start

RADIUS Access-Request
[EAP-Tunnel = FAST]

EAP-Request:TLV

RADIUS Access-Challenge
[EAP-TLV = “Machine”]

EAP-Response
TLV = “Machine”

RADIUS Access-Request
[EAP-TLV= “Machine”]
[EAP-ID=Corp-Win7-1]

RADIUS Access-Accept

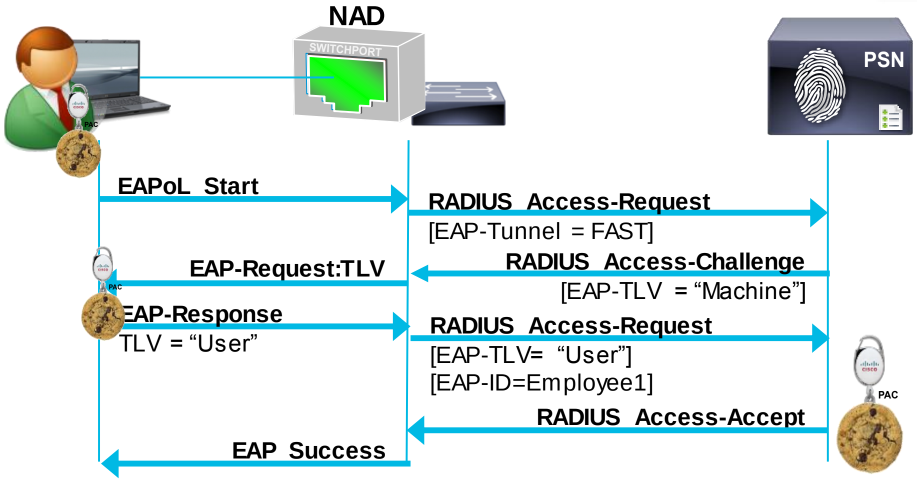
EAP Success

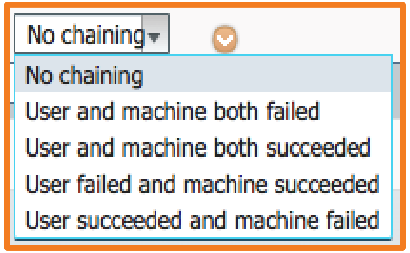
EAP-Chaining

With AnyConnect 3.1.1 and ISE 1.1.1

3. User Authenticates
4. ISE receives Machine PAC
5. ISE issues User AuthZ PAC

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAuth
Employee	if	Employee & **Network Access:EAPChainingResult = User and machine suceeded**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then	WEBAUTH		




No chaining

- No chaining
- User and machine both failed
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

EAP-Chaining FAQ

For Your Reference

Q: I use MSChapV2 today, can I use that with EAP-Chaining?
A: TEAP & EAP-FAST are tunneled EAP methodologies, you may use whichever inner-methods you would like, as long as both the supplicant and RADIUS sever support the protocol(s). I.e.: EAP-TLS, EAP-MSChapV2, EAP-GTC.

Q: What Supplicants Support EAP-Chaining Today?
A: Today, only Cisco AnyConnect NAM has support through EAP-FASTv2.
Please talk to your OS Vendors about supporting TEAP in their native supplicants!

Q: Can I chain certificates with username/pwd's?
A: Yes! You may mix and match the machine and user credential types however you see fit. I.e.: Machine Certificates + User Certificates, or Machine Certificates + Username/PWDs, or Machine Passwords + Username/PWDs, etc.

Identifying the Machine AND the User

What to do when EAP-Chaining is not Available?

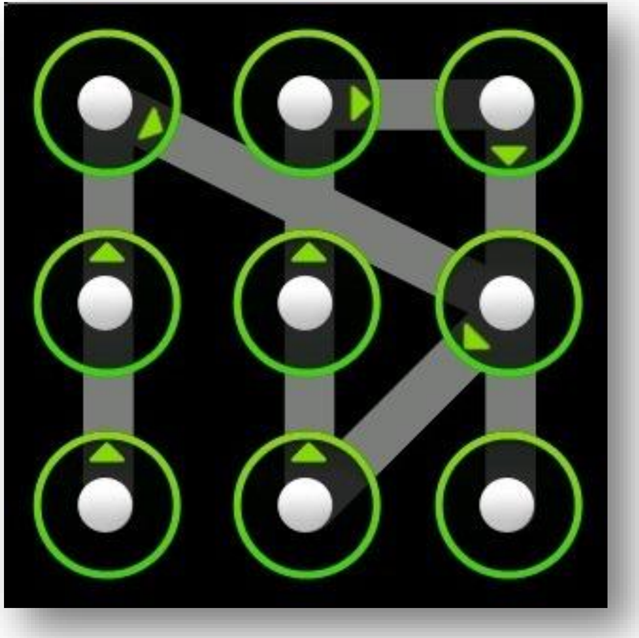
- There are many needs to determine Machine AND the User
  - Windows is the only current OS that can run EAP-Chaining (with AnyConnect)
  - What about iOS or Android based Tablets?

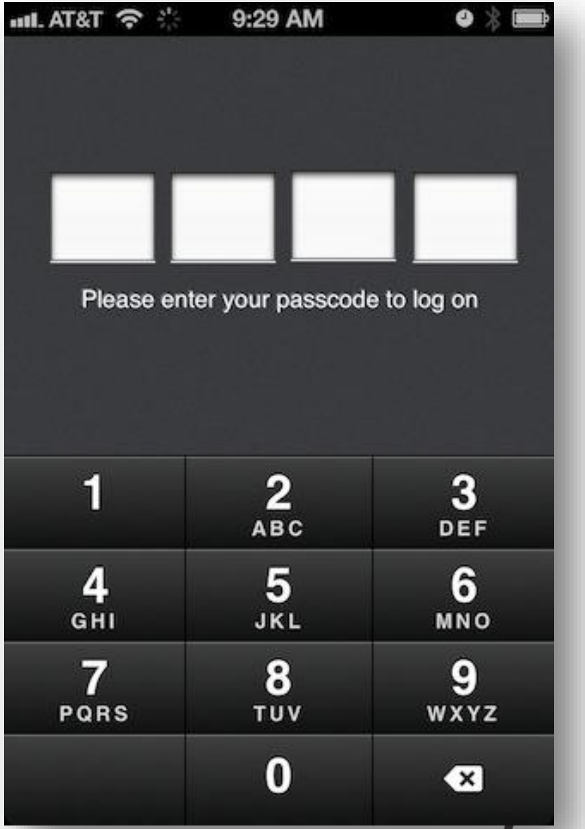
- Chain together 802.1X with Centralised Web Authentication (CWA)
  - Can validate the device using a user-issued certificates
  - Will validate the 'actual user' with username/password or smartcard or other method that validates the user

Mobile Device w/ Certificate

What Identifies the Actual User?

Mobile Device
w/ Certificate



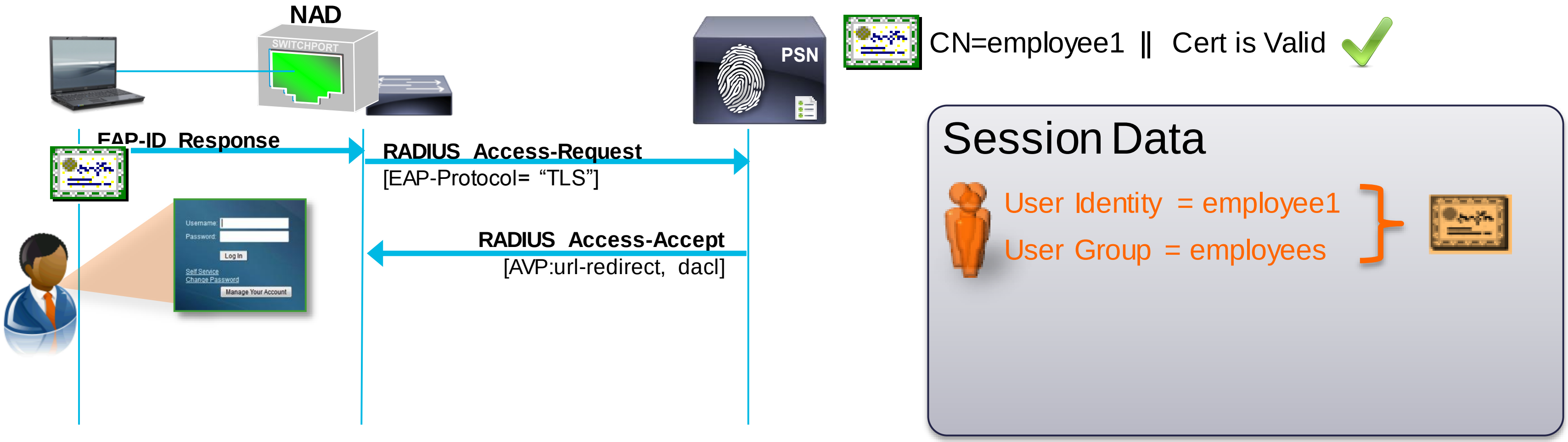


Please enter your passcode to log on

802.1X and CWA Chaining

1. EAP-TLS Authentication
2. ISE Sends Access-Accept w/ URL-Redirect

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
Employee_CWA	if	AD:ExternalGroup=Employees AND CWA:CWA_ExternalGroup=Employees	then	Employee & SGT
Employee_1X	if	Employee & Network Access: EAPAuthentication = EAP-TLS	then	CWAchain
Default	If no matches, then	WEBAUTH		



RADIUS Access-Request
[EAP-Protocol= "TLS"]

RADIUS Access-Accept
[AVP:url-redirect, dacl]

CN=employee1 || Cert is Valid ✓

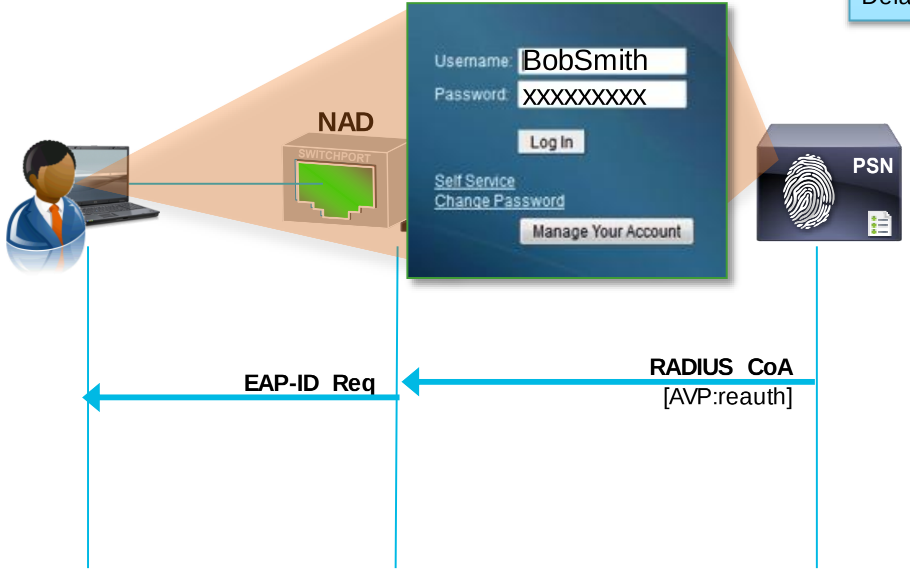
Session Data

User Identity = employee1
User Group = employees

802.1X and CWA Chaining

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
Employee_CWA	if	AD:ExternalGroup=Employees AND CWA:CWA_ExternalGroup= Employees	then	Employee & SGT
Employee_1X	if	Employee & Network Access: EAPAuthentication = EAP-TLS	then	CWAchain
Default	If no matches, then		WEBAUTH	

3. User Enters Uname/PWD
4. ISE Sends CoA-reauth



Username: BobSmith

Password: XXXXXXXXX

Session Data

User Identity = employee1

User Group = employees

+

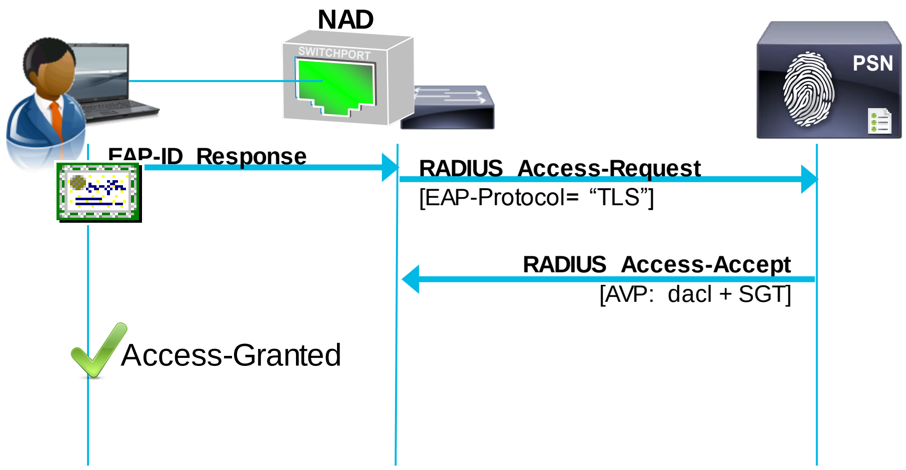
CWA Identity = BobSmith

CWA Group = employees

802.1X and CWA Chaining

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
Employee_CWA	if	**AD:ExternalGroup=Employees AND CWA:CWA_ExternalGroup=Employees**	then	Employee & SGT
Employee_1X	if	Employee & **Network Access: EAPAuthentication = EAP-TLS**	then	CWAchain
Default	If no matches, then		WEBAUTH	

3. User Enters Uname/PWD
4. ISE Sends CoA-reauth
5. Supplicant Responds with Cert
6. ISE sends Accept, dACL & SGT



NAD

PSN

EAP-ID Response

RADIUS Access-Request
[EAP-Protocol= "TLS"]

RADIUS Access-Accept
[AVP: dacl + SGT]

✓ Access-Granted

CN=employee1 || Cert is Valid ✓

Session Data

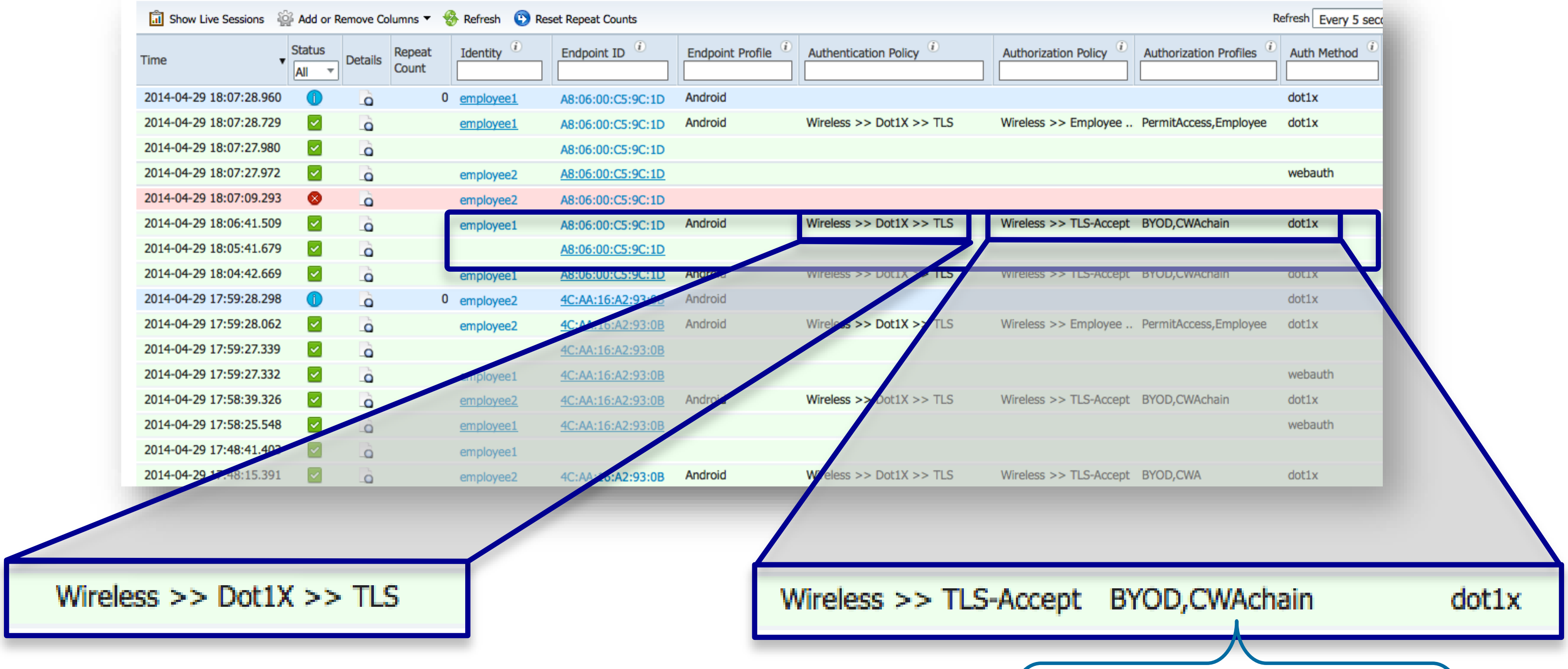
User Identity = employee1
User Group = employees

+

CWA Identity = BobSmith
CWA Group = employees

Following the Flow

1. Initial EAP-TLS Auth



Time ▾	Status All ▾	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Auth Method
2014-04-29 18:07:28.960	ⓘ	🔍	0	employee1	A8:06:00:C5:9C:1D	Android				dot1x
2014-04-29 18:07:28.729	✓	🔍		employee1	A8:06:00:C5:9C:1D	Android	Wireless >> Dot1X >> TLS	Wireless >> Employee ..	PermitAccess,Employee	dot1x
2014-04-29 18:07:27.980	✓	🔍			A8:06:00:C5:9C:1D					
2014-04-29 18:07:27.972	✓	🔍		employee2	A8:06:00:C5:9C:1D					webauth
2014-04-29 18:07:09.293	✗	🔍		employee2	A8:06:00:C5:9C:1D					
2014-04-29 18:06:41.509	✓	🔍		employee1	A8:06:00:C5:9C:1D	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWAchain	dot1x
2014-04-29 18:05:41.679	✓	🔍			A8:06:00:C5:9C:1D					
2014-04-29 18:04:42.669	✓	🔍		employee1	A8:06:00:C5:9C:1D	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWAchain	dot1x
2014-04-29 17:59:28.298	ⓘ	🔍	0	employee2	4C:AA:16:A2:93:0B	Android				dot1x
2014-04-29 17:59:28.062	✓	🔍		employee2	4C:AA:16:A2:93:0B	Android	Wireless >> Dot1X >> TLS	Wireless >> Employee ..	PermitAccess,Employee	dot1x
2014-04-29 17:59:27.339	✓	🔍			4C:AA:16:A2:93:0B					
2014-04-29 17:59:27.332	✓	🔍		employee1	4C:AA:16:A2:93:0B					webauth
2014-04-29 17:58:39.326	✓	🔍		employee2	4C:AA:16:A2:93:0B	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWAchain	dot1x
2014-04-29 17:58:25.548	✓	🔍		employee1	4C:AA:16:A2:93:0B					webauth
2014-04-29 17:48:41.403	✓	🔍		employee1						
2014-04-29 17:48:15.391	✓	🔍		employee2	4C:AA:16:A2:93:0B	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWA	dot1x

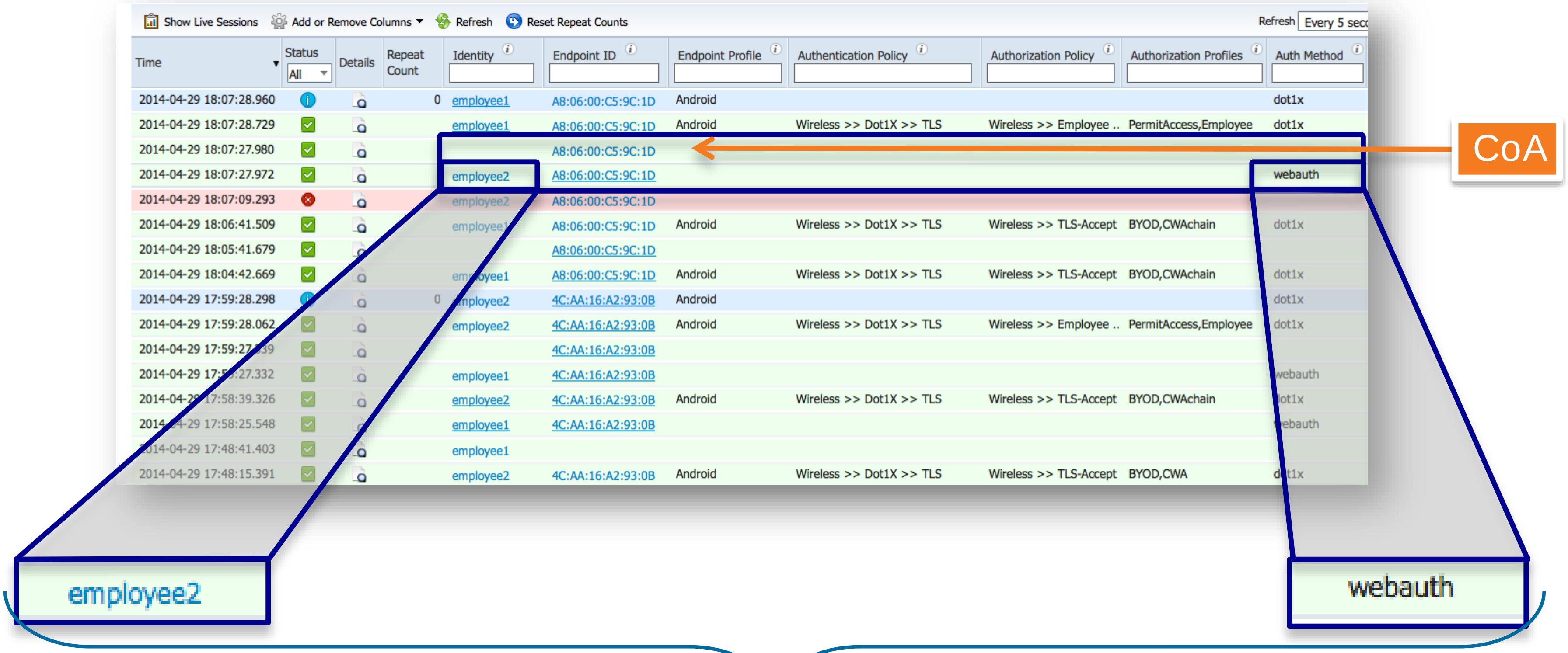
Wireless >> Dot1X >> TLS

Wireless >> TLS-Accept BYOD,CWAchain dot1x

Redirection to CWA Portal

Following the Flow

2. WebAuth from User

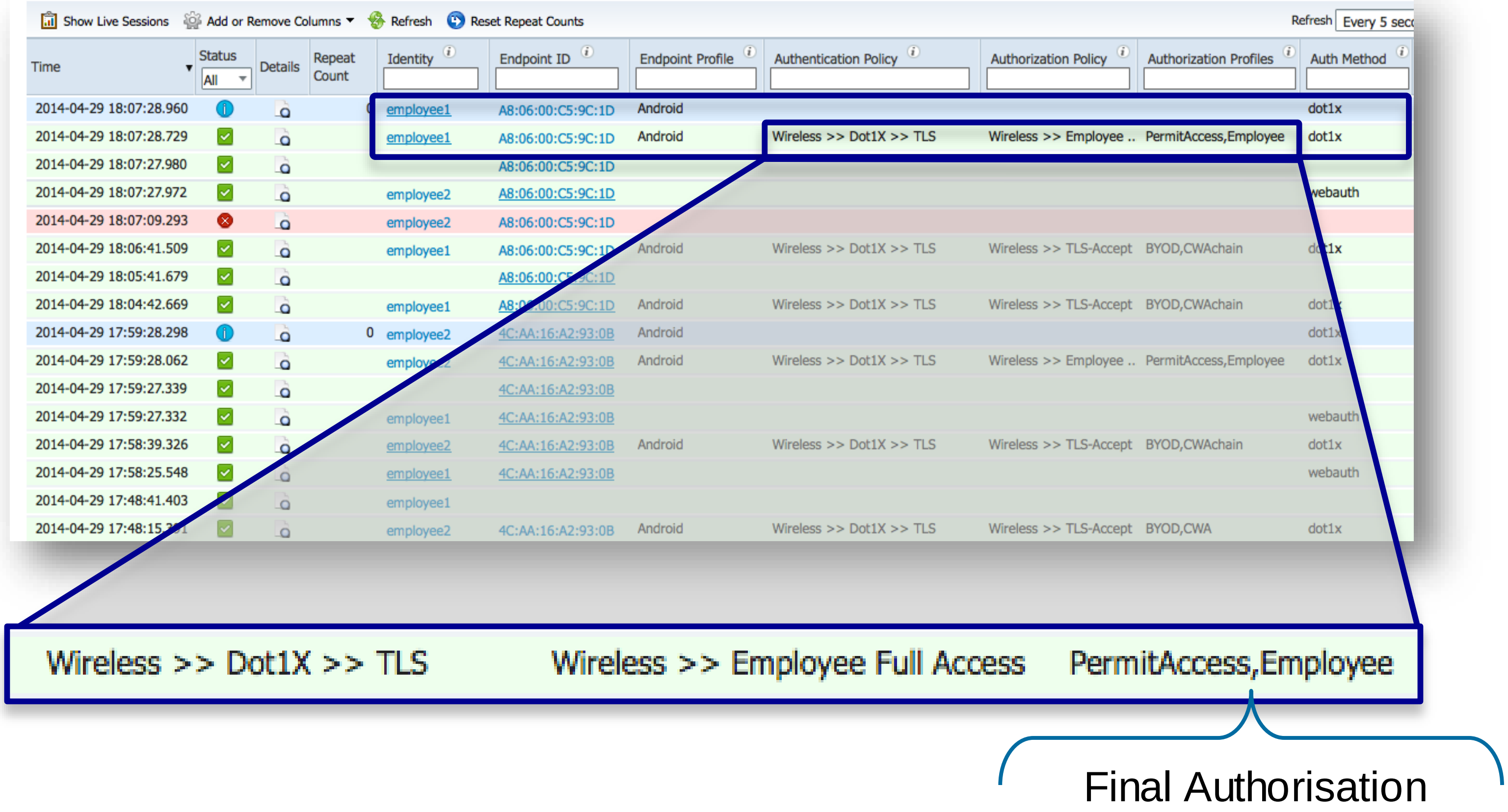


Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Auth Method
2014-04-29 18:07:28.960	ⓘ	🔍	0	employee1	A8:06:00:C5:9C:1D	Android				dot1x
2014-04-29 18:07:28.729	✓	🔍		employee1	A8:06:00:C5:9C:1D	Android	Wireless >> Dot1X >> TLS	Wireless >> Employee ..	PermitAccess,Employee	dot1x
2014-04-29 18:07:27.980	✓	🔍			A8:06:00:C5:9C:1D					
2014-04-29 18:07:27.972	✓	🔍		employee2	A8:06:00:C5:9C:1D					webauth
2014-04-29 18:07:09.293	✗	🔍		employee2	A8:06:00:C5:9C:1D					
2014-04-29 18:06:41.509	✓	🔍		employee1	A8:06:00:C5:9C:1D	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWAchain	dot1x
2014-04-29 18:05:41.679	✓	🔍			A8:06:00:C5:9C:1D					
2014-04-29 18:04:42.669	✓	🔍		employee1	A8:06:00:C5:9C:1D	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWAchain	dot1x
2014-04-29 17:59:28.298	ⓘ	🔍	0	employee2	4C:AA:16:A2:93:0B	Android				dot1x
2014-04-29 17:59:28.062	✓	🔍		employee2	4C:AA:16:A2:93:0B	Android	Wireless >> Dot1X >> TLS	Wireless >> Employee ..	PermitAccess,Employee	dot1x
2014-04-29 17:59:27.339	✓	🔍			4C:AA:16:A2:93:0B					
2014-04-29 17:59:27.332	✓	🔍		employee1	4C:AA:16:A2:93:0B					webauth
2014-04-29 17:58:39.326	✓	🔍		employee2	4C:AA:16:A2:93:0B	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWAchain	dot1x
2014-04-29 17:58:25.548	✓	🔍		employee1	4C:AA:16:A2:93:0B					webauth
2014-04-29 17:48:41.403	✓	🔍		employee1						
2014-04-29 17:48:15.391	✓	🔍		employee2	4C:AA:16:A2:93:0B	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWA	dot1x

Not Required to be Different Username

Following the Flow

3. Final Auth with Full Result



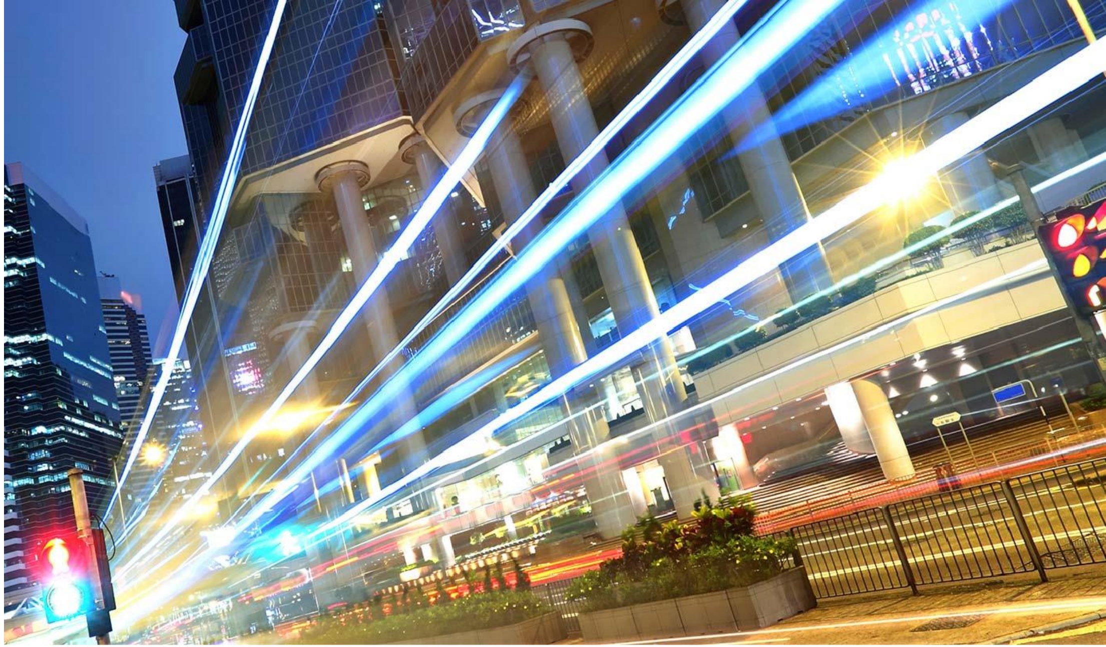
Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Auth Method
2014-04-29 18:07:28.960	ⓘ	🔍	0	employee1	A8:06:00:C5:9C:1D	Android				dot1x
2014-04-29 18:07:28.729	✓	🔍		employee1	A8:06:00:C5:9C:1D	Android	Wireless >> Dot1X >> TLS	Wireless >> Employee ..	PermitAccess,Employee	dot1x
2014-04-29 18:07:27.980	✓	🔍			A8:06:00:C5:9C:1D					
2014-04-29 18:07:27.972	✓	🔍		employee2	A8:06:00:C5:9C:1D					webauth
2014-04-29 18:07:09.293	✗	🔍		employee2	A8:06:00:C5:9C:1D					
2014-04-29 18:06:41.509	✓	🔍		employee1	A8:06:00:C5:9C:1D	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWAchain	dot1x
2014-04-29 18:05:41.679	✓	🔍			A8:06:00:C5:9C:1D					
2014-04-29 18:04:42.669	✓	🔍		employee1	A8:06:00:C5:9C:1D	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWAchain	dot1x
2014-04-29 17:59:28.298	ⓘ	🔍	0	employee2	4C:AA:16:A2:93:0B	Android				dot1x
2014-04-29 17:59:28.062	✓	🔍		employee2	4C:AA:16:A2:93:0B	Android	Wireless >> Dot1X >> TLS	Wireless >> Employee ..	PermitAccess,Employee	dot1x
2014-04-29 17:59:27.339	✓	🔍			4C:AA:16:A2:93:0B					
2014-04-29 17:59:27.332	✓	🔍		employee1	4C:AA:16:A2:93:0B					webauth
2014-04-29 17:58:39.326	✓	🔍		employee2	4C:AA:16:A2:93:0B	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWAchain	dot1x
2014-04-29 17:58:25.548	✓	🔍		employee1	4C:AA:16:A2:93:0B					webauth
2014-04-29 17:48:41.403	✓	🔍		employee1						
2014-04-29 17:48:15.301	✓	🔍		employee2	4C:AA:16:A2:93:0B	Android	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	BYOD,CWA	dot1x

Wireless >> Dot1X >> TLS   Wireless >> Employee Full Access   PermitAccess,Employee

Final Authorisation

Agenda

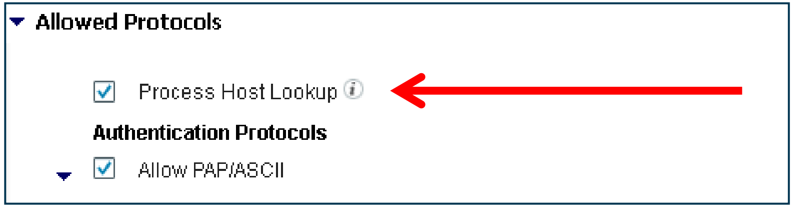
- Introduction
- Certificates, Certificates, Certificates
- BYOD Best Practices
- Integrating with Cisco and Non-Cisco
- ISE in a Security EcoSystem
- Serviceability & Troubleshooting
- Staged Deployments (Time Permitting)
- Conclusion



Non-Cisco NAD Integration

ISE and Endpoint Lookup

- ISE maintains a separate User and Endpoint "store".
  - User store may be queried at any time.
- By default: endpoint store may only be accessed if the incoming request was identified as a MAB. (Service-Type = Call-Check)
  - ISE also ignores the u-name/pwd fields, but uses the calling-station-id (mac-address of the endpoint)
- Why?
  - **Security!** Before this, malicious users would be able to put a mac-address into the username & password fields of WebAuth (or non-Cisco switches even in the supplicant identity).



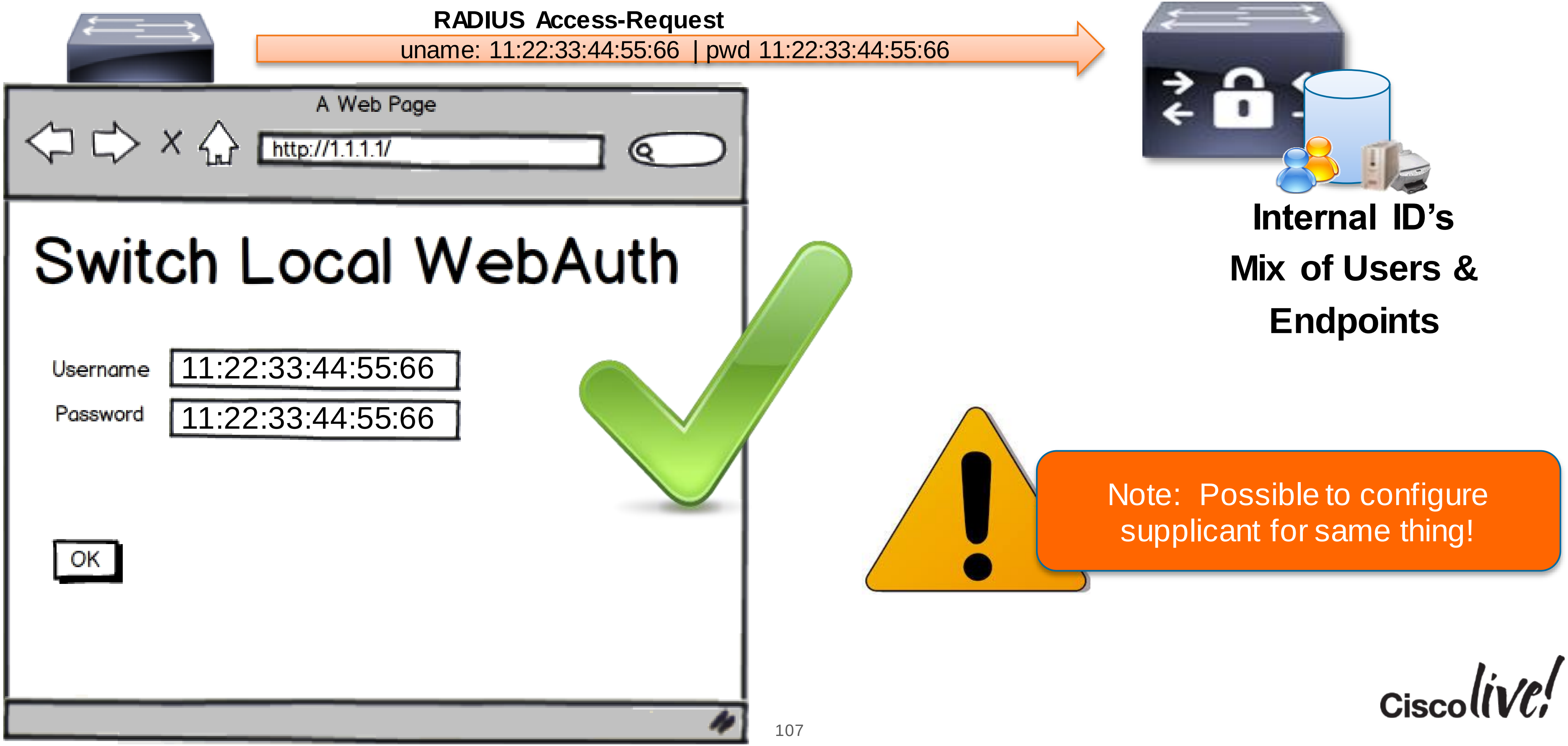
▾ Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII

Why Restrict MAB to Calling-Station-ID?



RADIUS Access-Request

uname: 11:22:33:44:55:66 | pwd 11:22:33:44:55:66

Switch Local WebAuth

Username 11:22:33:44:55:66

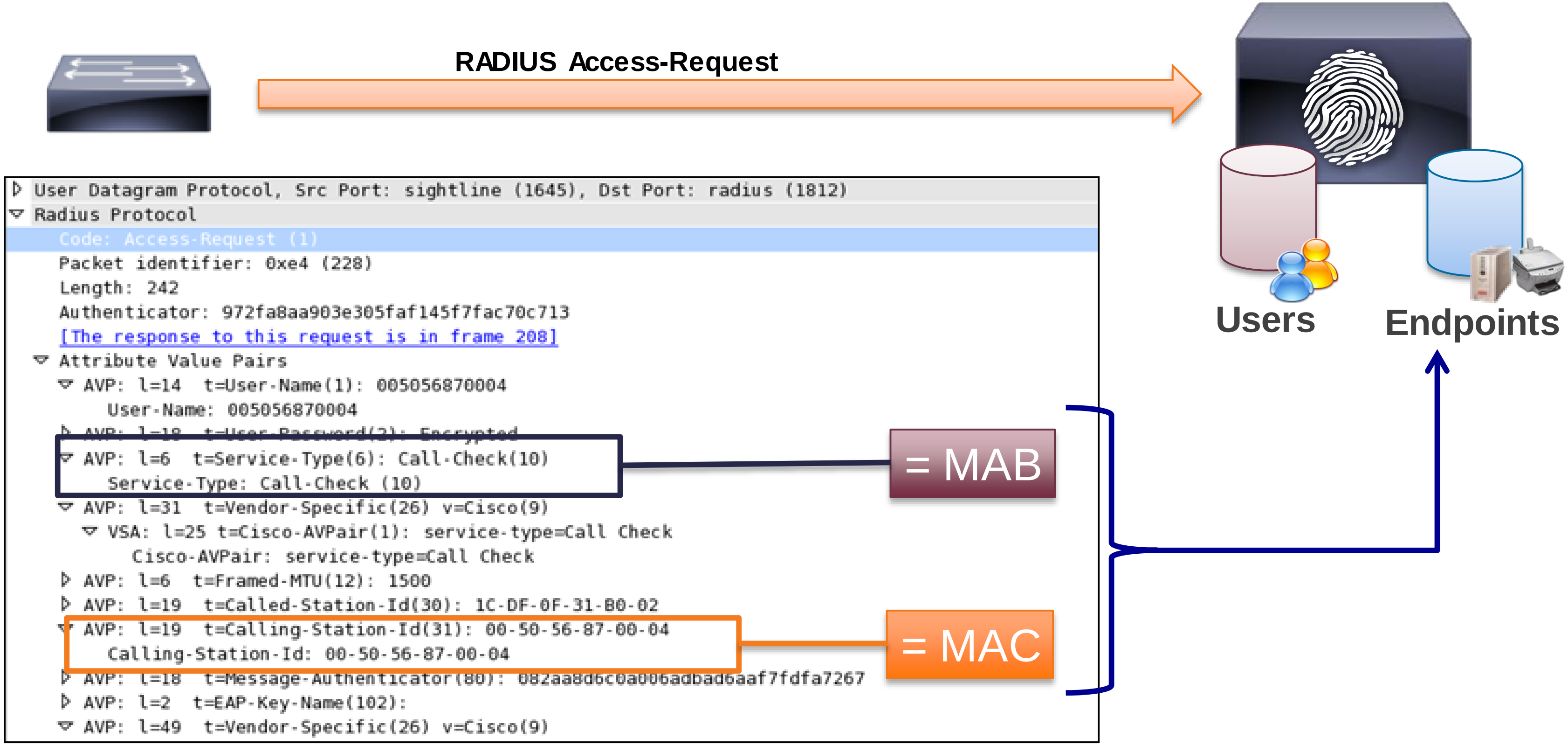
Password 11:22:33:44:55:66

Internal ID's

Mix of Users & Endpoints

Note: Possible to configure supplicant for same thing!

Cisco MAB – MAC Authentication Bypass

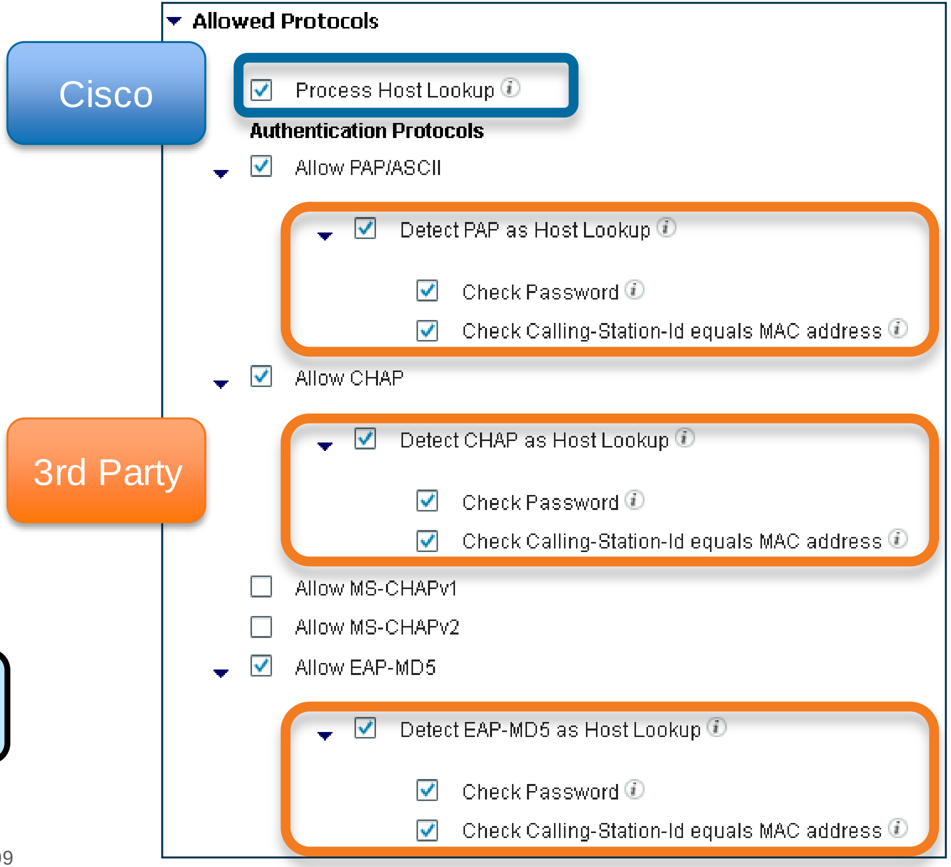


```
▷ User Datagram Protocol, Src Port: sightline (1645), Dst Port: radius (1812)
▽ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0xe4 (228)
    Length: 242
    Authenticator: 972fa8aa903e305faf145f7fac70c713
    [The response to this request is in frame 208]
  ▽ Attribute Value Pairs
    ▽ AVP: l=14  t=User-Name(1): 005056870004
        User-Name: 005056870004
    ▷ AVP: l=18  t=User-Password(2): Encrypted
    ▽ AVP: l=6  t=Service-Type(6): Call-Check(10)
        Service-Type: Call-Check (10)
    ▽ AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
      ▽ VSA: l=25 t=Cisco-AVPair(1): service-type=Call Check
          Cisco-AVPair: service-type=Call Check
    ▷ AVP: l=6  t=Framed-MTU(12): 1500
    ▷ AVP: l=19  t=Called-Station-Id(30): 1C-DF-0F-31-B0-02
    ▽ AVP: l=19  t=Calling-Station-Id(31): 00-50-56-87-00-04
        Calling-Station-Id: 00-50-56-87-00-04
    ▷ AVP: l=18  t=Message-Authenticator(80): 082aa8d6c0a006adbad6aaf7fdfa7267
    ▷ AVP: l=2  t=EAP-Key-Name(102):
    ▽ AVP: l=49  t=Vendor-Specific(26) v=Cisco(9)
```

3rd-Party Devices and MAB

- Many 3rd parties use Service-Type = Login for 802.1X, MAB and WebAuth
- Some 3rd Parties do not populate Calling-Station-ID with MAC address.
- With ISE 1.2, MAB can work with different Service-Type, Calling-Station-ID values, and “password” settings.

Recommendation is to keep as many checkboxes enabled as possible for increased security



Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII
- ☑ Detect PAP as Host Lookup
  - ☑ Check Password
  - ☑ Check Calling-Station-Id equals MAC address

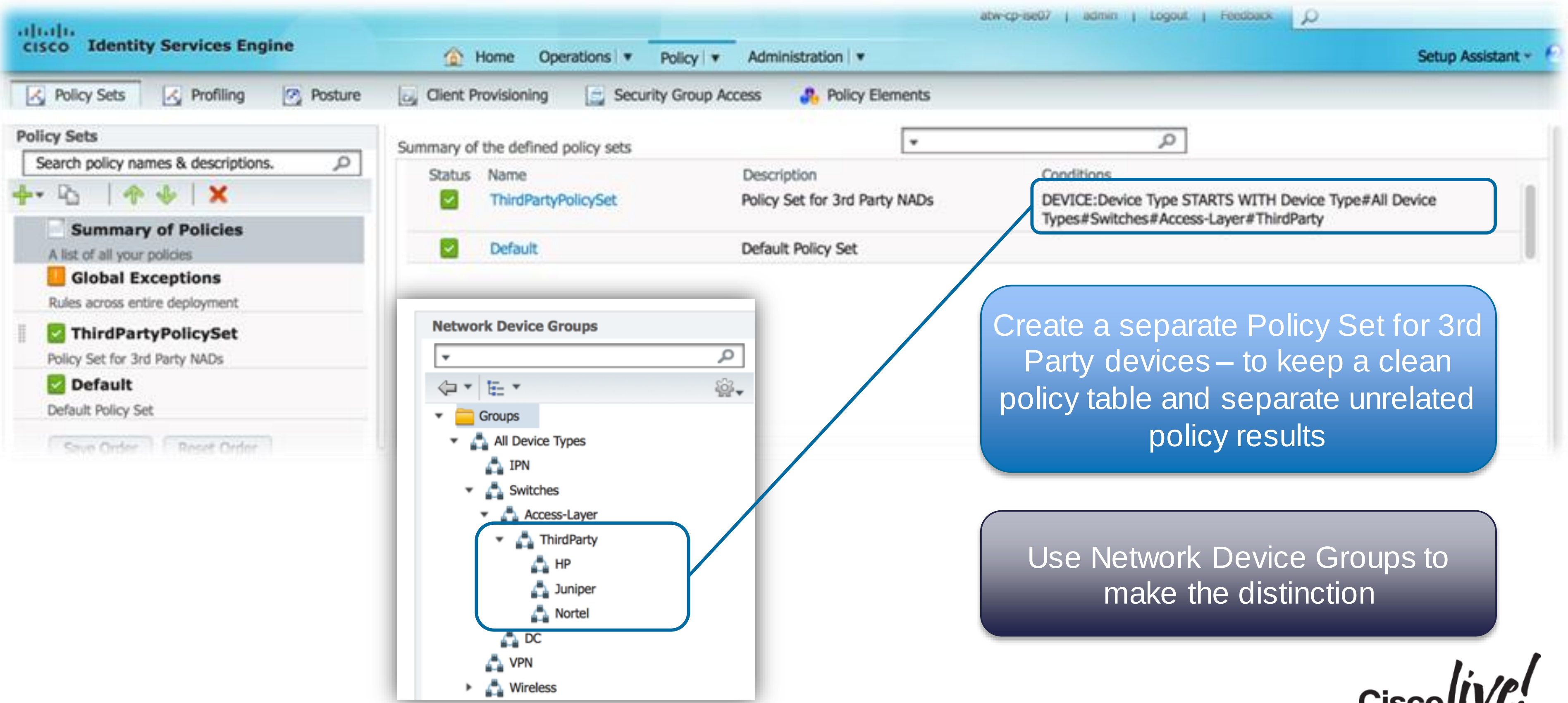
☑ Allow CHAP
- ☑ Detect CHAP as Host Lookup
  - ☑ Check Password
  - ☑ Check Calling-Station-Id equals MAC address

□ Allow MS-CHAPv1

□ Allow MS-CHAPv2

☑ Allow EAP-MD5
- ☑ Detect EAP-MD5 as Host Lookup
  - ☑ Check Password
  - ☑ Check Calling-Station-Id equals MAC address

Setup a Policy Set for 3rd Party NADs



Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

ThirdPartyPolicySet
Policy Set for 3rd Party NADs

Default
Default Policy Set

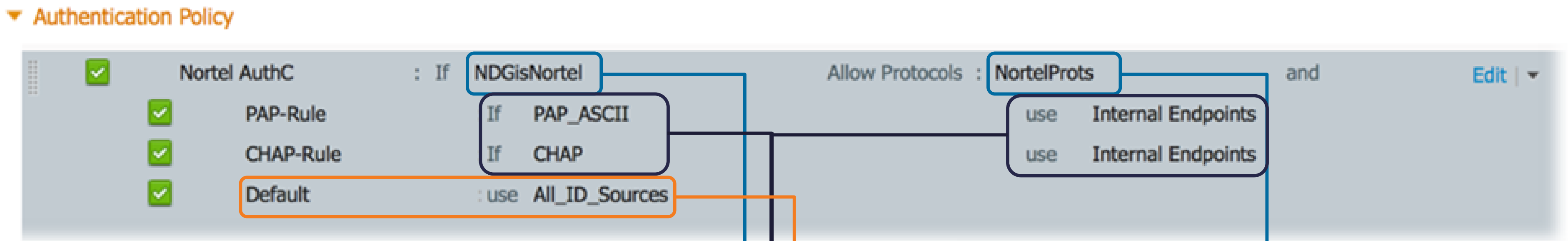
Summary of the defined policy sets

Status	Name	Description	Conditions
✓	ThirdPartyPolicySet	Policy Set for 3rd Party NADs	DEVICE:Device Type STARTS WITH Device Type#All Device Types#Switches#Access-Layer#ThirdParty
✓	Default	Default Policy Set	

Create a separate Policy Set for 3rd Party devices – to keep a clean policy table and separate unrelated policy results

Use Network Device Groups to make the distinction

Example: Nortel & Alcatel Authentication Policy



Authentication Policy

☑ Nortel AuthC : If NDGisNortel Allow Protocols : NortelProts and Edit

☑ PAP-Rule If PAP_ASCII use Internal Endpoints

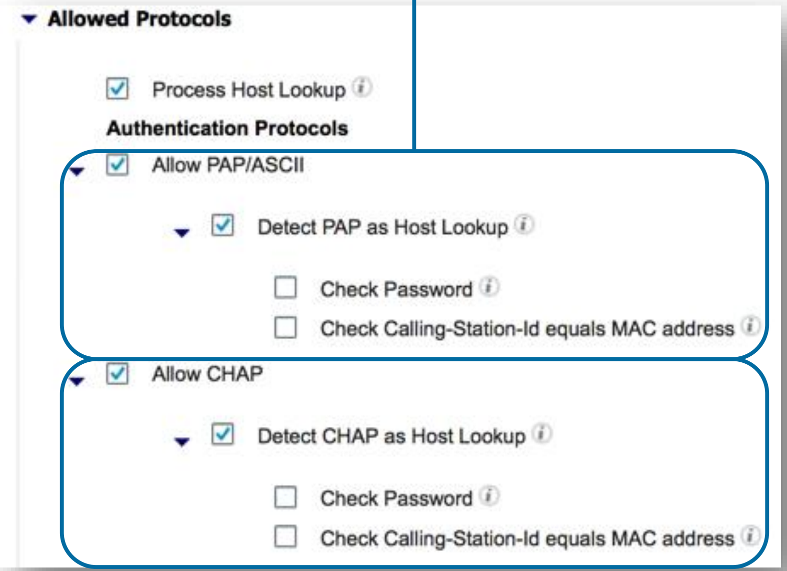
☑ CHAP-Rule If CHAP use Internal Endpoints

☑ Default : use All_ID_Sources

Network Device Group = “Nortel”

For “better” security, lock PAP & CHAP into MAB lookups (Internal Endpoints)

All other authentications are sent to an Identity Sequence (Internal Users > Guest > AD)



Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII

☑ Detect PAP as Host Lookup

□ Check Password

□ Check Calling-Station-Id equals MAC address

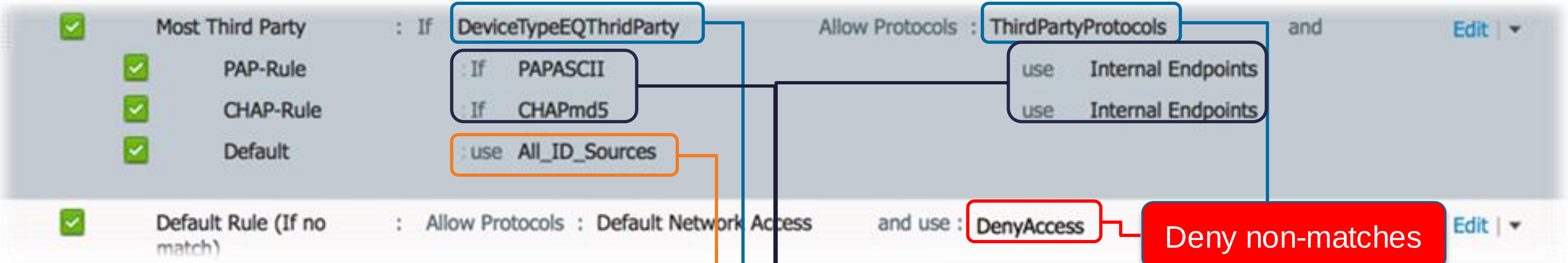
☑ Allow CHAP

☑ Detect CHAP as Host Lookup

□ Check Password

□ Check Calling-Station-Id equals MAC address

Example: Rest of 3rd Party Authentication Policy



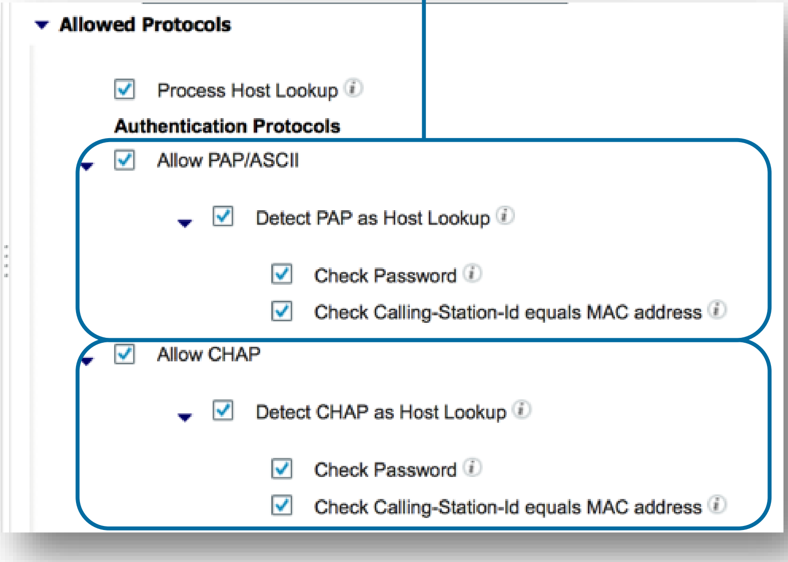
☑	Most Third Party	: If DeviceTypeEQThridParty		Allow Protocols : ThirdPartyProtocols	and	Edit | ▾
☑	PAP-Rule	: If PAPASCII		use Internal Endpoints		
☑	CHAP-Rule	: If CHAPmd5		use Internal Endpoints		
☑	Default	: use All_ID_Sources				
☑	Default Rule (If no match)	: Allow Protocols : Default Network Access		and use : DenyAccess		Edit | ▾

Deny non-matches

Network Device Group = “Third Party”

For “better” security, lock PAP & CHAP into MAB lookups (Internal Endpoints)

All other authentications are sent to an Identity Sequence (Internal Users > Guest > AD)



▾ **Allowed Protocols**

☑ Process Host Lookup ⓘ

Authentication Protocols

▾ ☑ Allow PAP/ASCII

▾ ☑ Detect PAP as Host Lookup ⓘ

☑ Check Password ⓘ

☑ Check Calling-Station-Id equals MAC address ⓘ

▾ ☑ Allow CHAP

▾ ☑ Detect CHAP as Host Lookup ⓘ

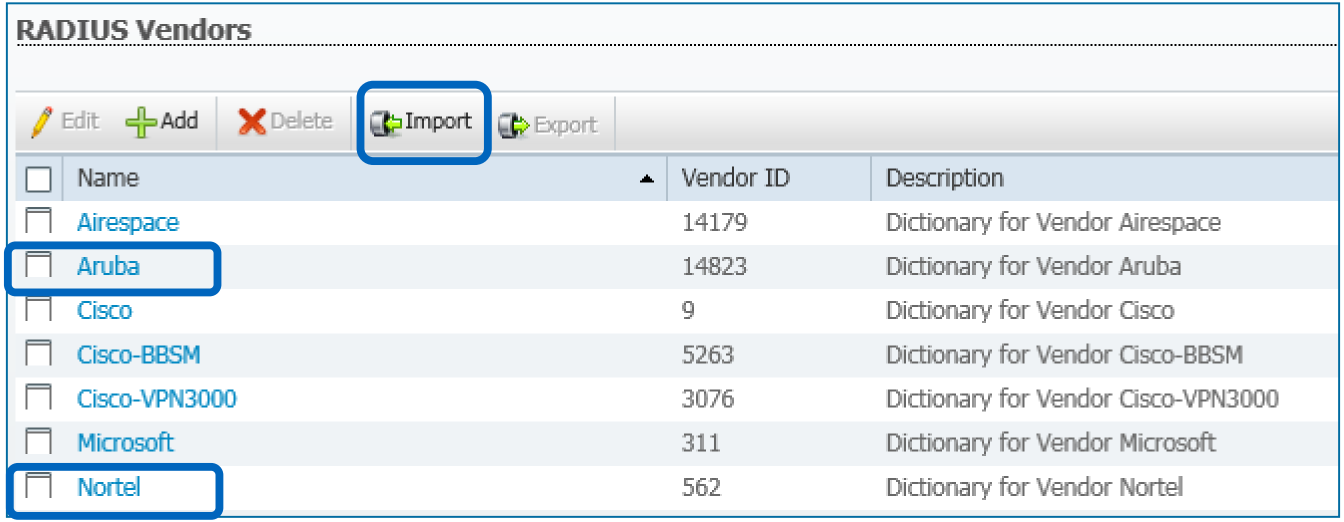
☑ Check Password ⓘ

☑ Check Calling-Station-Id equals MAC address ⓘ

Third Party Vendors VSA Attributes

- You may import other RADIUS Dictionaries into ISE:
  Policy > Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors

Dictionaries for FreeRADIUS will work

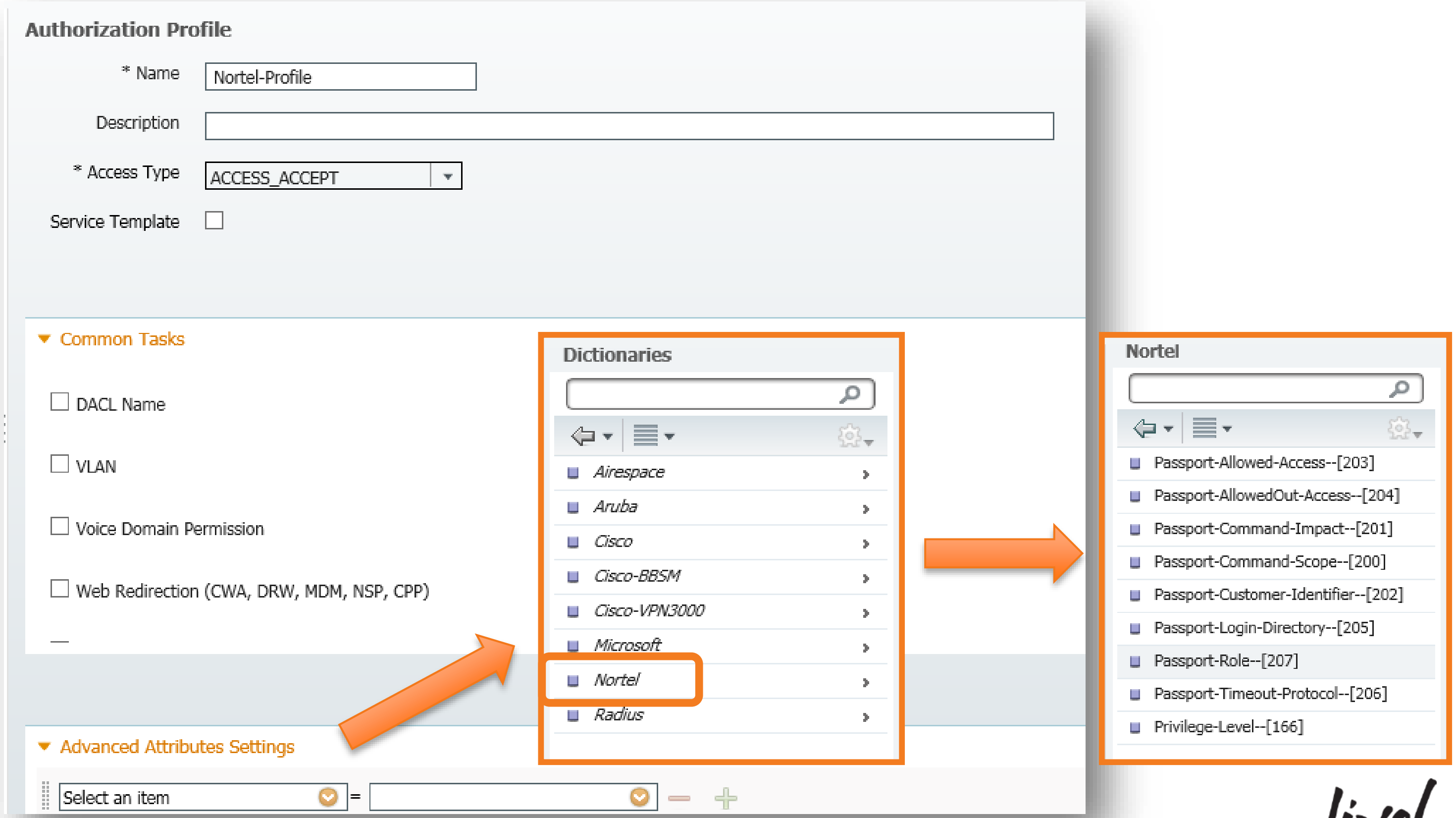


RADIUS Vendors

□	Name	Vendor ID	Description
□	Airespace	14179	Dictionary for Vendor Airespace
□	Aruba	14823	Dictionary for Vendor Aruba
□	Cisco	9	Dictionary for Vendor Cisco
□	Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
□	Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000
□	Microsoft	311	Dictionary for Vendor Microsoft
□	Nortel	562	Dictionary for Vendor Nortel

Authorisation Profiles for Third Party

Go to “Advanced Attribute Settings” to use the 3rd Party Dictionaries



Authorization Profile

* Name	Nortel-Profile
Description	
* Access Type	ACCESS_ACCEPT
Service Template	□

▼ Common Tasks

□ DACL Name

□ VLAN

□ Voice Domain Permission

□ Web Redirection (CWA, DRW, MDM, NSP, CPP)

▼ Advanced Attributes Settings

Select an item =

Dictionaries

- Airespace
- Aruba
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft
- Nortel
- Radius

Nortel

- Passport-Allowed-Access--[203]
- Passport-AllowedOut-Access--[204]
- Passport-Command-Impact--[201]
- Passport-Command-Scope--[200]
- Passport-Customer-Identifier--[202]
- Passport-Login-Directory--[205]
- Passport-Role--[207]
- Passport-Timeout-Protocol--[206]
- Privilege-Level--[166]

Results of my 3rd Party Testing

For Your Reference

Alcatel Switch:

Uncheck both Calling-Station-ID & Password

To set VLAN:

Tunnel-Medium-Type = IEEE-802
Tunnel-Type = VLAN
Tunnel-Private-Group-ID = 100

Avaya (Nortel) Switch:

Uncheck both Calling-Station-ID & Password

Juniper EX Switch:

Leave Calling-Station-ID & Password Checked

HP (H3C) Switch:

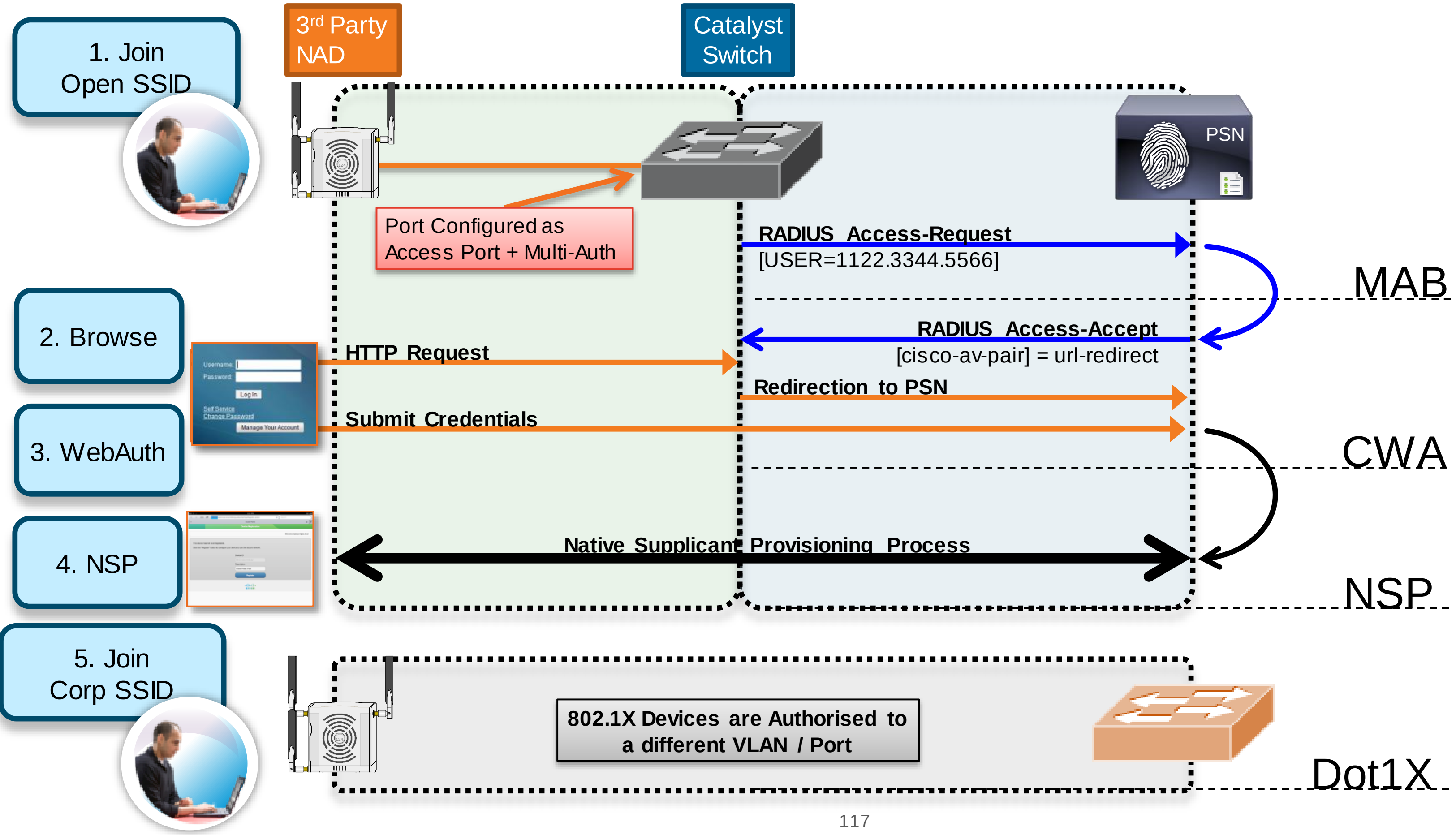
Uncheck Calling-Station-ID, Leave Password Checked

RuggedCom Switch:

Uncheck Calling-Station-ID, Leave Password Checked

BYOD Onboarding for 3rd Party NADs

Using a Cisco Catalyst Switch as Inline PeP



1. Join Open SSID

2. Browse

3. WebAuth

4. NSP

5. Join Corp SSID

3rd Party NAD

Catalyst Switch

PSN

Port Configured as Access Port + Multi-Auth

RADIUS Access-Request [USER=1122.3344.5566]

RADIUS Access-Accept [cisco-av-pair] = url-redirect

HTTP Request

Redirection to PSN

Submit Credentials

Native Supplicant Provisioning Process

802.1X Devices are Authorised to a different VLAN / Port

MAB

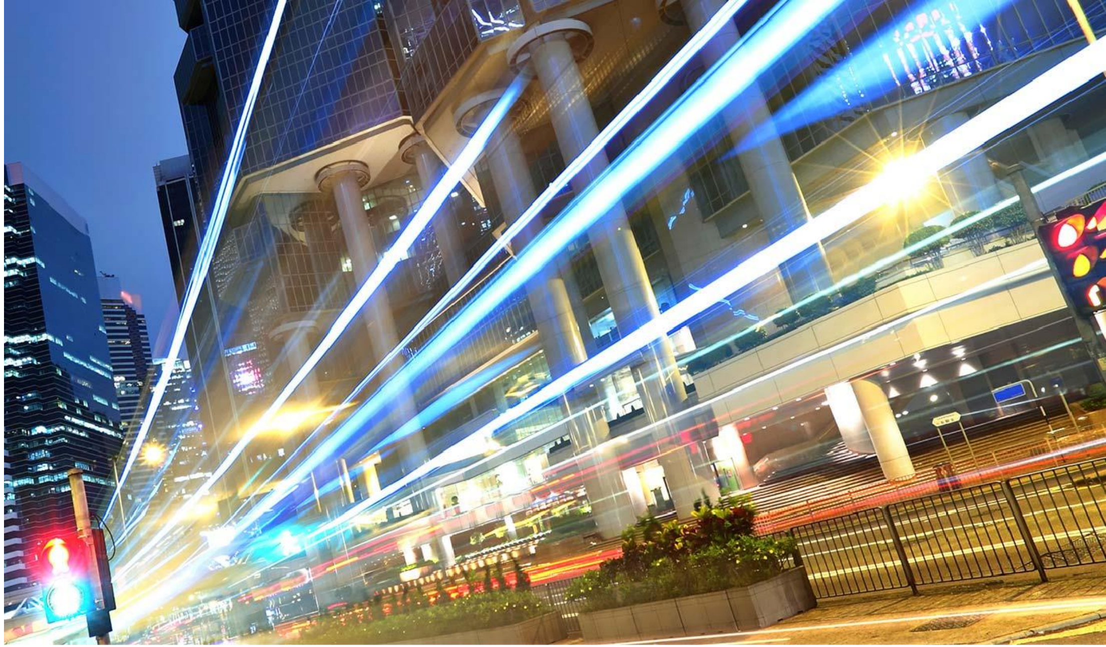
CWA

NSP

Dot1X

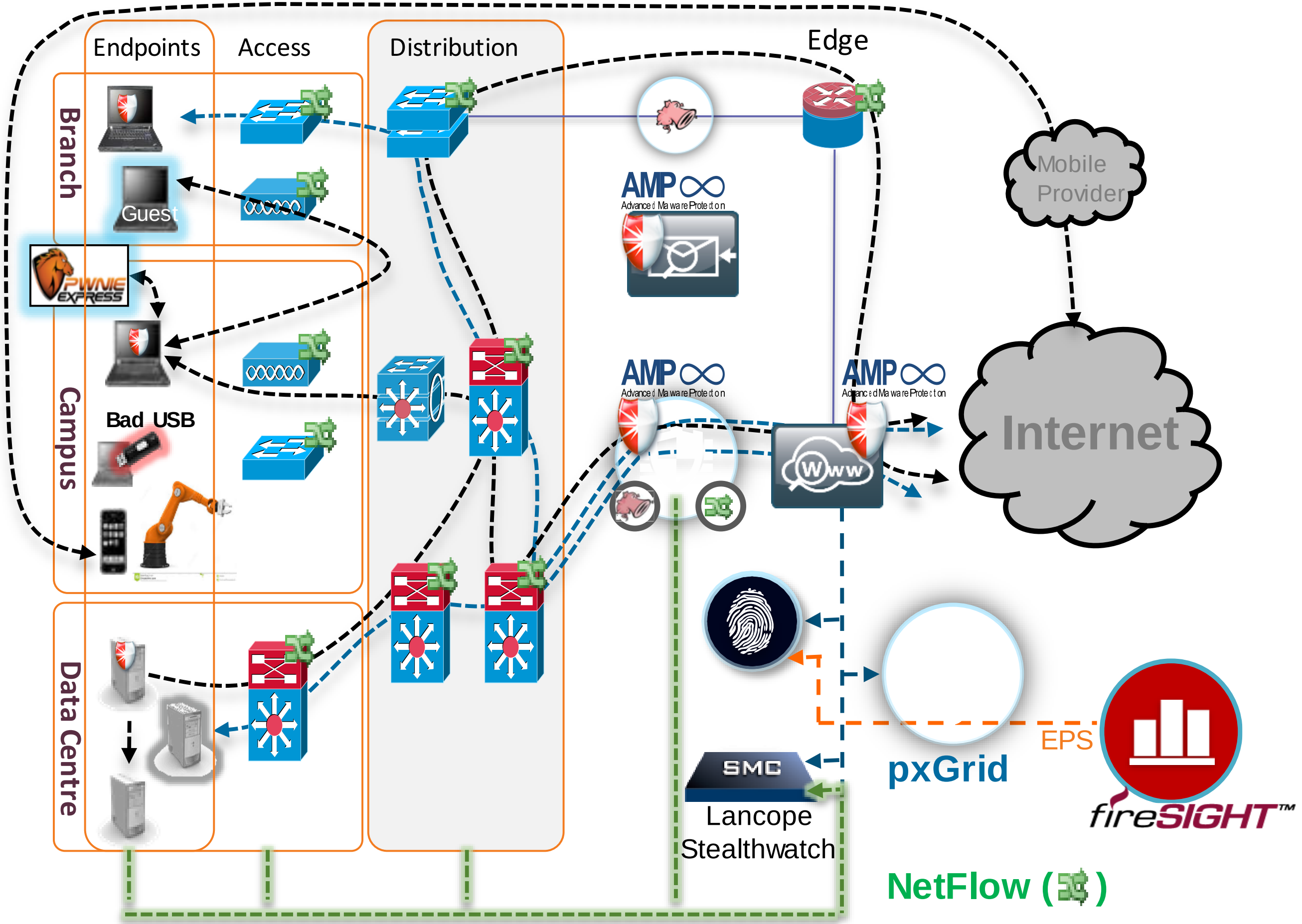
Agenda

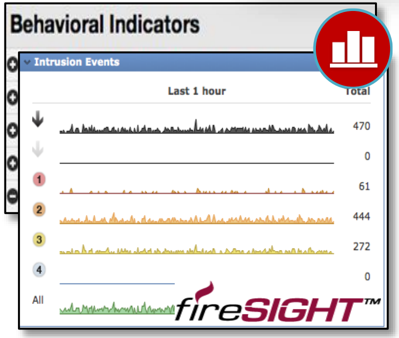
- Introduction
- Certificates, Certificates, Certificates
- BYOD Best Practices
- Integrating with Cisco and Non-Cisco
- ISE in a Security EcoSystem
- Serviceability & Troubleshooting
- Staged Deployments (Time Permitting)
- Conclusion

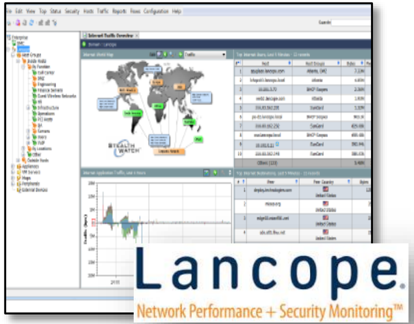


ISE in a Security EcoSystem

Using ISE in a Security EcoSystem

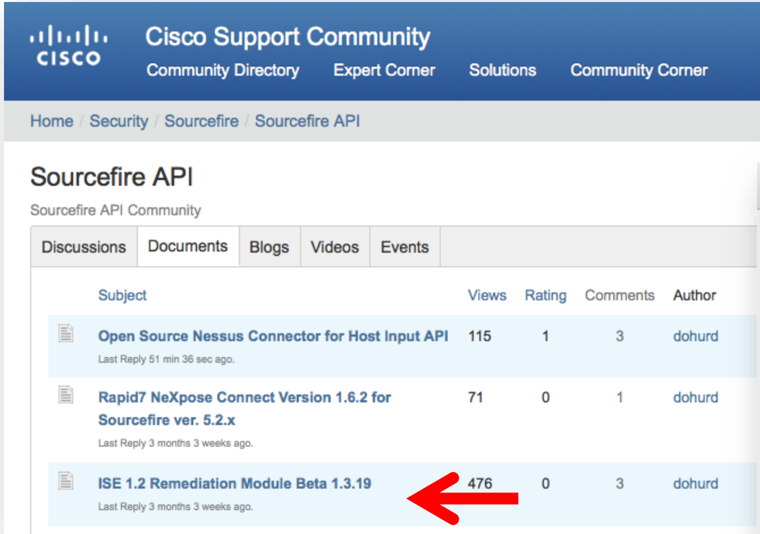






SourceFire Nation Remediation Plugins

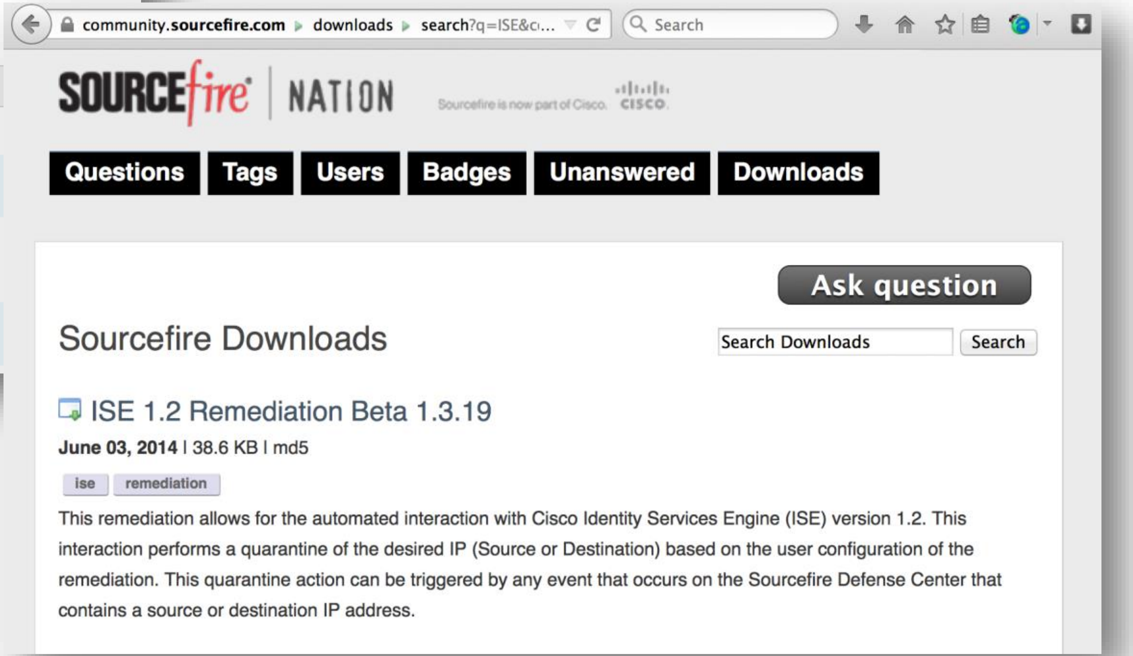
EXAMPLE



Sourcefire API

Sourcefire API Community

Subject	Views	Rating	Comments	Author
Open Source Nessus Connector for Host Input API Last Reply 51 min 36 sec ago.	115	1	3	dohurd
Rapid7 NeXpose Connect Version 1.6.2 for Sourcefire ver. 5.2.x Last Reply 3 months 3 weeks ago.	71	0	1	dohurd
ISE 1.2 Remediation Module Beta 1.3.19 Last Reply 3 months 3 weeks ago.	476	0	3	dohurd



Sourcefire Downloads

ISE 1.2 Remediation Beta 1.3.19

June 03, 2014 | 38.6 KB | md5

ise remediation

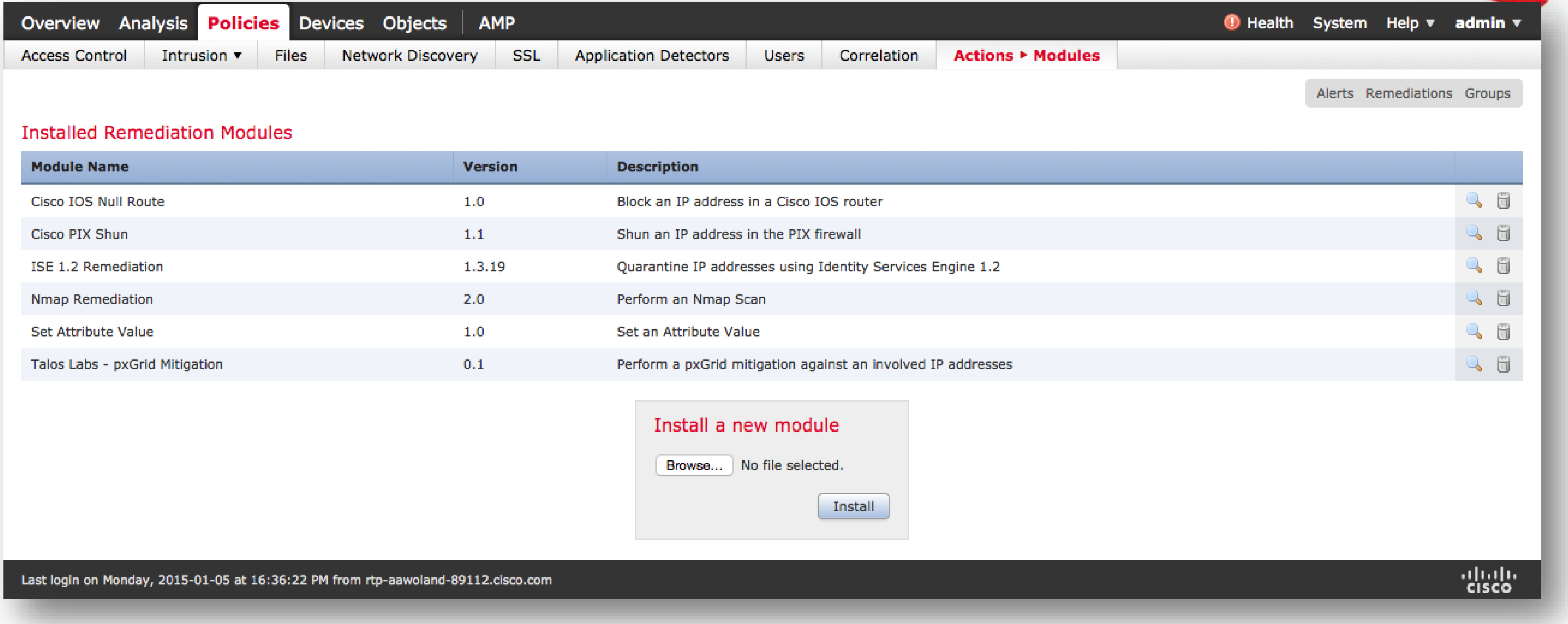
This remediation allows for the automated interaction with Cisco Identity Services Engine (ISE) version 1.2. This interaction performs a quarantine of the desired IP (Source or Destination) based on the user configuration of the remediation. This quarantine action can be triggered by any event that occurs on the Sourcefire Defense Center that contains a source or destination IP address.

- Modules are BETA
- Community Supported
- Not TAC Supported

https://supportforums.cisco.com/community/12226126/sourcefire-api#quicktabs-community_activity=1

Add the Remediation Module to FireSight

EXAMPLE


Overview Analysis Policies Devices Objects AMP
Health System Help ▾ admin ▾
Access Control Intrusion ▾ Files Network Discovery SSL Application Detectors Users Correlation Actions ▸ Modules
Alerts Remediations Groups

Installed Remediation Modules

Module Name	Version	Description
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Cisco PIX Shun	1.1	Shun an IP address in the PIX firewall
ISE 1.2 Remediation	1.3.19	Quarantine IP addresses using Identity Services Engine 1.2
Nmap Remediation	2.0	Perform an Nmap Scan
Set Attribute Value	1.0	Set an Attribute Value
Talos Labs - pxGrid Mitigation	0.1	Perform a pxGrid mitigation against an involved IP addresses

Install a new module

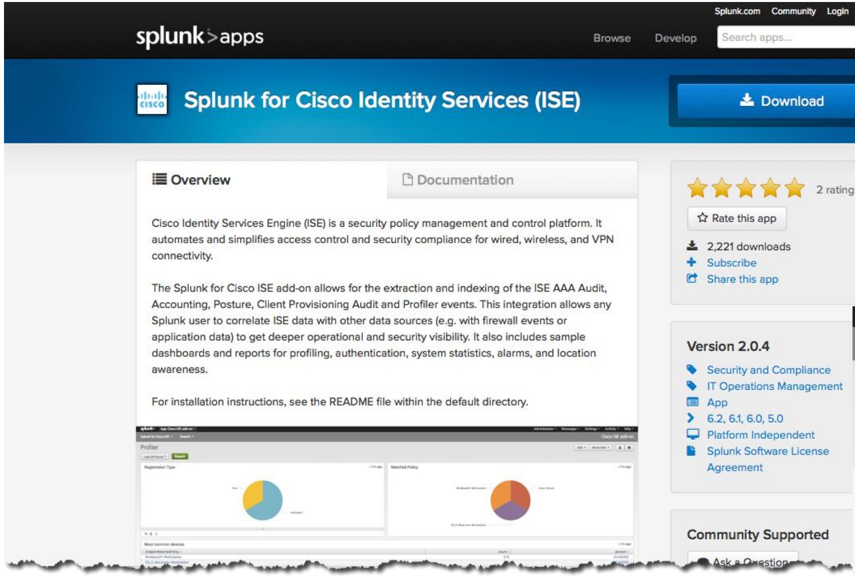
Browse... No file selected.

Install

Last login on Monday, 2015-01-05 at 16:36:22 PM from rtp-aawoland-89112.cisco.com

Splunk ISE App

EXAMPLE



Splunk for Cisco Identity Services (ISE)

Cisco Identity Services Engine (ISE) is a security policy management and control platform. It automates and simplifies access control and security compliance for wired, wireless, and VPN connectivity.

The Splunk for Cisco ISE add-on allows for the extraction and indexing of the ISE AAA Audit, Accounting, Posture, Client Provisioning Audit and Profiler events. This integration allows any Splunk user to correlate ISE data with other data sources (e.g. with firewall events or application data) to get deeper operational and security visibility. It also includes sample dashboards and reports for profiling, authentication, system statistics, alarms, and location awareness.

For installation instructions, see the README file within the default directory.

★★★★★ 2 ratings

☆ Rate this app

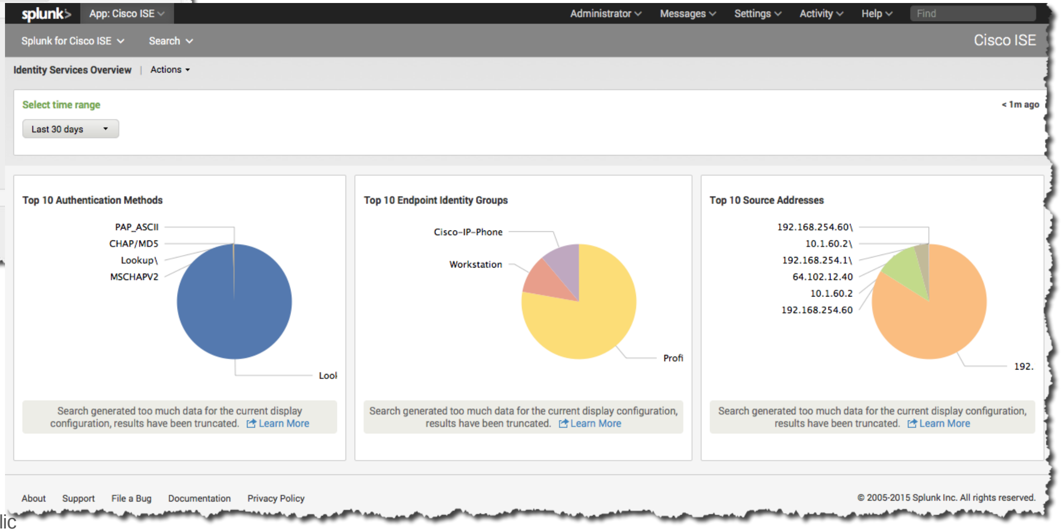
2,221 downloads
Subscribe
Share this app

Version 2.0.4

- Security and Compliance
- IT Operations Management
- App
- 6.2, 6.1, 6.0, 5.0
- Platform Independent
- Splunk Software License Agreement

Community Supported

Ask a Question



splunk> App: Cisco ISE
Administrator Messages Settings Activity Help Find
Splunk for Cisco ISE Search
Cisco ISE
Identity Services Overview | Actions

Select time range: Last 30 days

< 1m ago

Top 10 Authentication Methods

Search generated too much data for the current display configuration, results have been truncated. Learn More

Top 10 Endpoint Identity Groups

Search generated too much data for the current display configuration, results have been truncated. Learn More

Top 10 Source Addresses

Search generated too much data for the current display configuration, results have been truncated. Learn More

© 2005-2015 Splunk Inc. All rights reserved.

http://apps.splunk.com/app/1589

LanCope SteathWatch

EXAMPLE

Monitor Mode

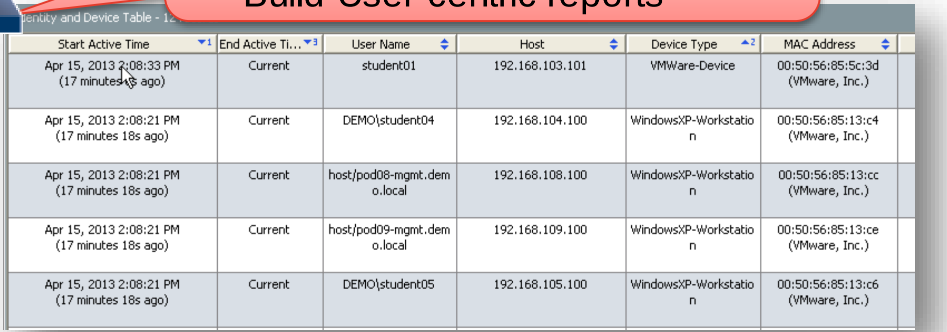
- Open Mode, Multi-Auth
- Unobstructed Access
- No impact on productivity
- Profiling, posture assessment
- Gain Visibility

syslog

StealthWatch Management Console

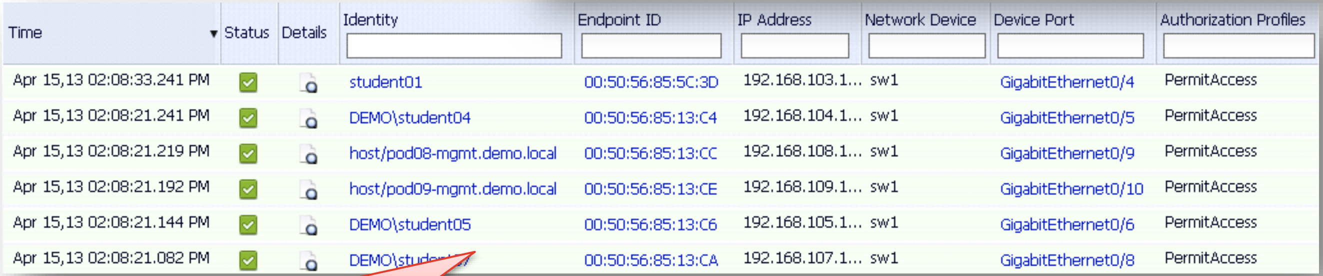
SMC

- Maintain historical session table
- Correlate NetFlow to username
- Build User-centric reports



dentity and Device Table - 12

Start Active Time	End Active Ti...	User Name	Host	Device Type	MAC Address
Apr 15, 2013 2:08:33 PM (17 minutes [illegible] ago)	Current	student01	192.168.103.101	VMWare-Device	00:50:56:85:5c:3d (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student04	192.168.104.100	WindowsXP-Workstation	00:50:56:85:13:c4 (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod08-mgmt.demo.local	192.168.108.100	WindowsXP-Workstation	00:50:56:85:13:cc (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod09-mgmt.demo.local	192.168.109.100	WindowsXP-Workstation	00:50:56:85:13:ce (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student05	192.168.105.100	WindowsXP-Workstation	00:50:56:85:13:c6 (VMware, Inc.)

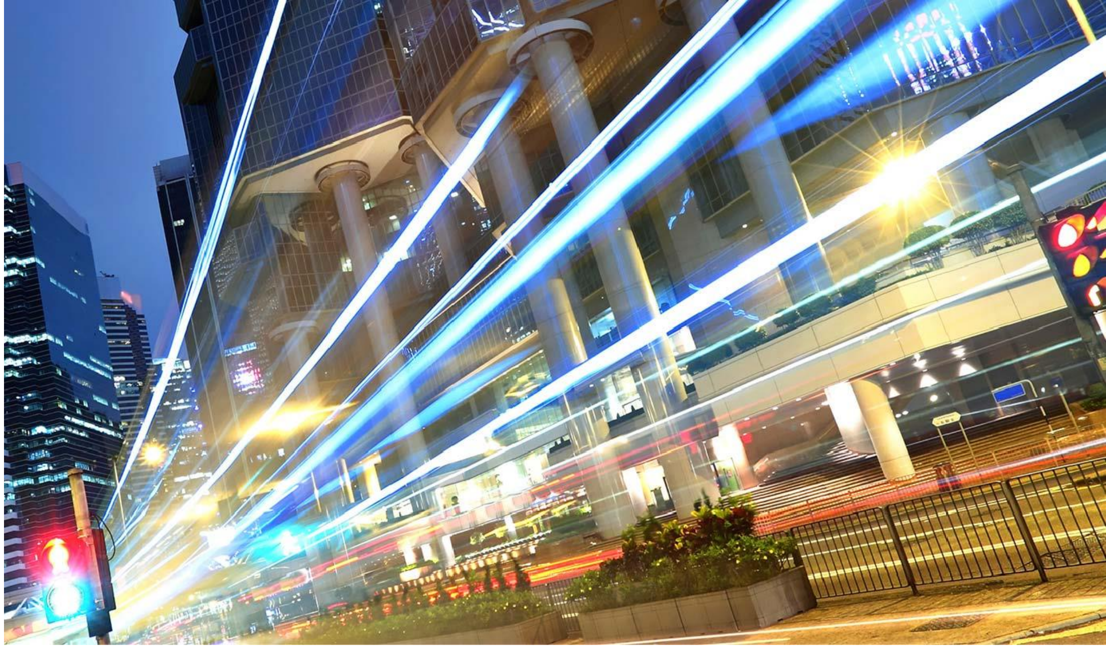


Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Apr 15,13 02:08:33.241 PM	✓		student01	00:50:56:85:5C:3D	192.168.103.1...	sw1	GigabitEthernet0/4	PermitAccess
Apr 15,13 02:08:21.241 PM	✓		DEMO\student04	00:50:56:85:13:C4	192.168.104.1...	sw1	GigabitEthernet0/5	PermitAccess
Apr 15,13 02:08:21.219 PM	✓		host/pod08-mgmt.demo.local	00:50:56:85:13:CC	192.168.108.1...	sw1	GigabitEthernet0/9	PermitAccess
Apr 15,13 02:08:21.192 PM	✓		host/pod09-mgmt.demo.local	00:50:56:85:13:CE	192.168.109.1...	sw1	GigabitEthernet0/10	PermitAccess
Apr 15,13 02:08:21.144 PM	✓		DEMO\student05	00:50:56:85:13:C6	192.168.105.1...	sw1	GigabitEthernet0/6	PermitAccess
Apr 15,13 02:08:21.082 PM	✓		DEMO\student07	00:50:56:85:13:CA	192.168.107.1...	sw1	GigabitEthernet0/8	PermitAccess

Authenticated Session Table

Agenda

- Introduction
- Certificates, Certificates, Certificates
- BYOD Best Practices
- Integrating with Cisco and Non-Cisco
- ISE in a Security EcoSystem
- Serviceability & Troubleshooting
- Staged Deployments (Time Permitting)
- Conclusion

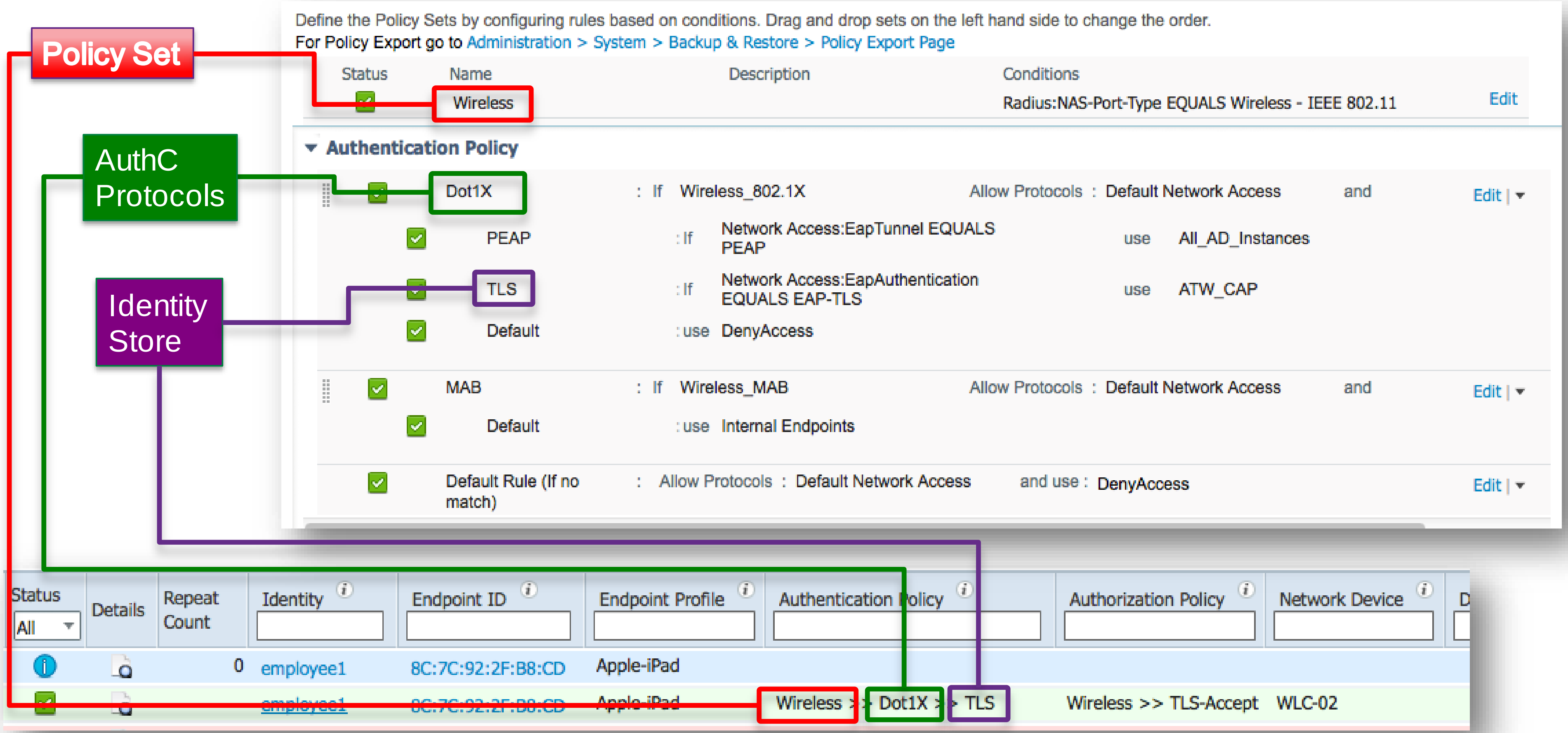


Serviceability: ISE 1.3

Serviceability User Stories

- To make ISE easier to troubleshoot
- To make ISE easier to deploy
- To make ISE easier to use

Tree View



Policy Set

AuthC Protocols

Identity Store

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions	
✓	Wireless		Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11	Edit

▾ **Authentication Policy**

✓ Dot1X : If Wireless_802.1X Allow Protocols : Default Network Access and Edit | ▾

✓ PEAP : If Network Access:EapTunnel EQUALS PEAP use All_AD_Instances

✓ TLS : If Network Access:EapAuthentication EQUALS EAP-TLS use ATW_CAP

✓ Default : use DenyAccess

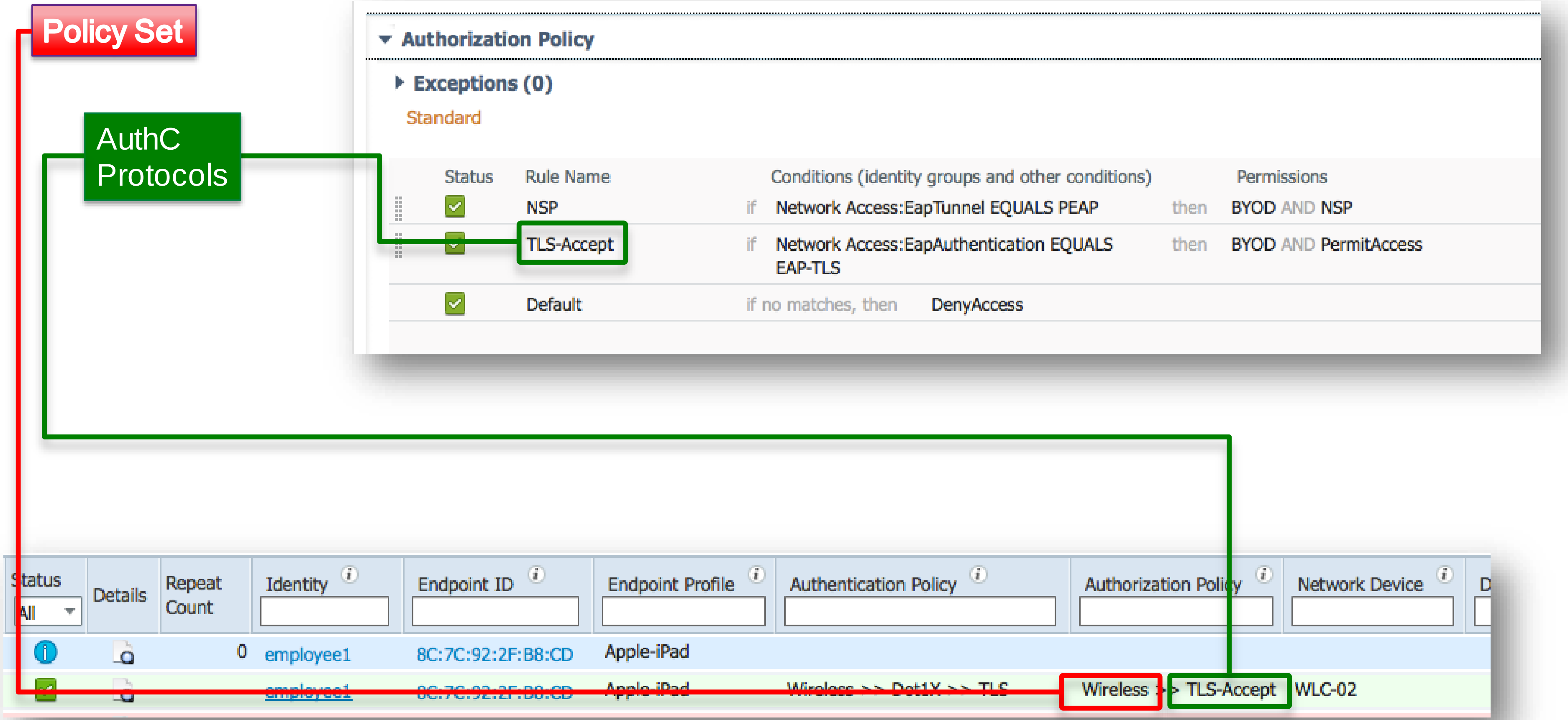
✓ MAB : If Wireless_MAB Allow Protocols : Default Network Access and Edit | ▾

✓ Default : use Internal Endpoints

✓ Default Rule (If no match) : Allow Protocols : Default Network Access and use : DenyAccess Edit | ▾

Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Network Device	D
All ▾									
ⓘ		0	employee1	8C:7C:92:2F:B8:CD	Apple-iPad				
✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	WLC-02	

Tree View



Policy Set

AuthC Protocols

▾ Authorization Policy

▸ Exceptions (0)

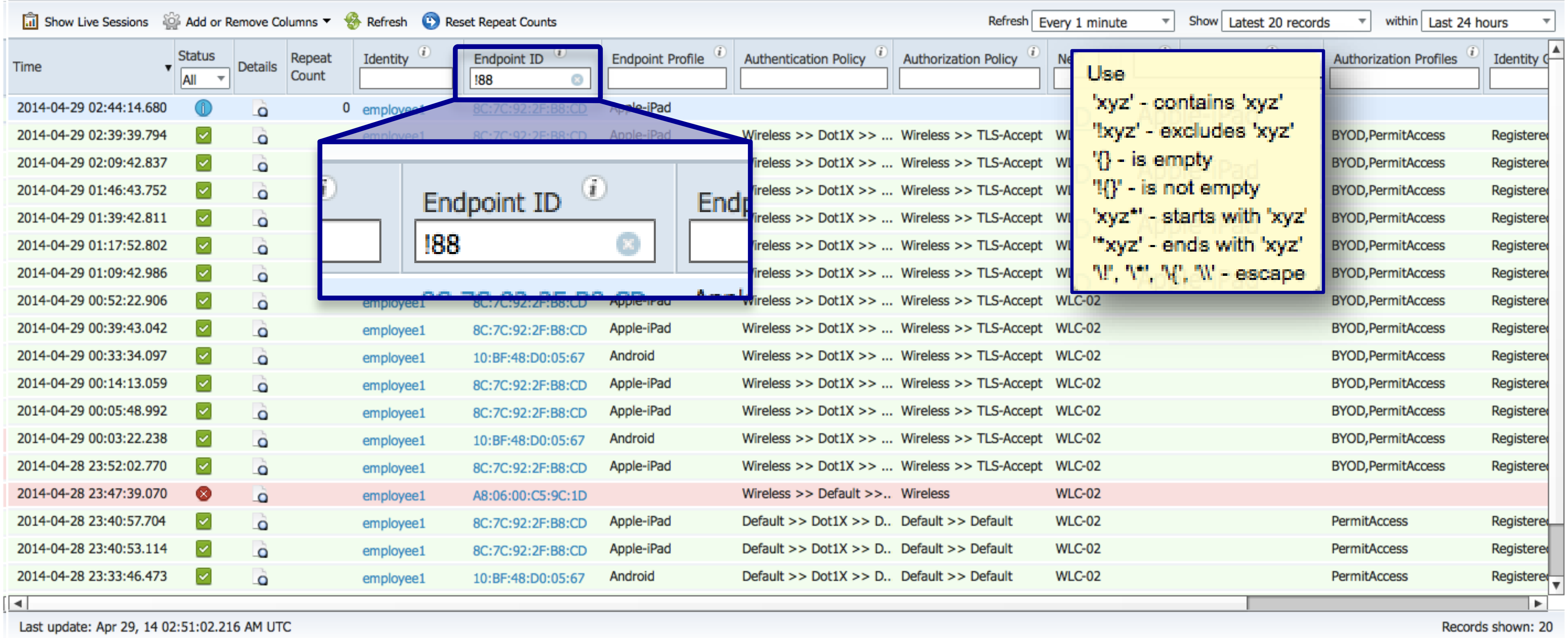
Standard

	Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
	☑	NSP	if	Network Access:EapTunnel EQUALS PEAP	then	BYOD AND NSP
	☑	TLS-Accept	if	Network Access:EapAuthentication EQUALS EAP-TLS	then	BYOD AND PermitAccess
	☑	Default		if no matches, then		DenyAccess

Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Network Device	D
ⓘ		0	employee1	8C:7C:92:2F:B8:CD	Apple-iPad				
☑			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	WLC-02	

Filters in Live Log & Live Sessions

At Long Last! Regex in Filters



Refresh Every 1 minute   Show Latest 20 records   within Last 24 hours

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Ne	Authorization Profiles	Identity G
	All				!88						
2014-04-29 02:44:14.680	ⓘ		0	employee1	8C:7C:92:2F:B8:CD	Apple-iPad					
2014-04-29 02:39:39.794	✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Wireless >> Dot1X >> ...	Wireless >> TLS-Accept	WL	BYOD,PermitAccess	Registere
2014-04-29 02:09:42.837	✓						ireless >> Dot1X >> ...	Wireless >> TLS-Accept	WL	BYOD,PermitAccess	Registere
2014-04-29 01:46:43.752	✓						ireless >> Dot1X >> ...	Wireless >> TLS-Accept	WL	BYOD,PermitAccess	Registere
2014-04-29 01:39:42.811	✓						ireless >> Dot1X >> ...	Wireless >> TLS-Accept	WL	BYOD,PermitAccess	Registere
2014-04-29 01:17:52.802	✓						ireless >> Dot1X >> ...	Wireless >> TLS-Accept	WL	BYOD,PermitAccess	Registere
2014-04-29 01:09:42.986	✓						ireless >> Dot1X >> ...	Wireless >> TLS-Accept	WL	BYOD,PermitAccess	Registere
2014-04-29 00:52:22.906	✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Wireless >> Dot1X >> ...	Wireless >> TLS-Accept	WLC-02	BYOD,PermitAccess	Registere
2014-04-29 00:39:43.042	✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Wireless >> Dot1X >> ...	Wireless >> TLS-Accept	WLC-02	BYOD,PermitAccess	Registere
2014-04-29 00:33:34.097	✓			employee1	10:BF:48:D0:05:67	Android	Wireless >> Dot1X >> ...	Wireless >> TLS-Accept	WLC-02	BYOD,PermitAccess	Registere
2014-04-29 00:14:13.059	✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Wireless >> Dot1X >> ...	Wireless >> TLS-Accept	WLC-02	BYOD,PermitAccess	Registere
2014-04-29 00:05:48.992	✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Wireless >> Dot1X >> ...	Wireless >> TLS-Accept	WLC-02	BYOD,PermitAccess	Registere
2014-04-29 00:03:22.238	✓			employee1	10:BF:48:D0:05:67	Android	Wireless >> Dot1X >> ...	Wireless >> TLS-Accept	WLC-02	BYOD,PermitAccess	Registere
2014-04-28 23:52:02.770	✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Wireless >> Dot1X >> ...	Wireless >> TLS-Accept	WLC-02	BYOD,PermitAccess	Registere
2014-04-28 23:47:39.070	✗			employee1	A8:06:00:C5:9C:1D		Wireless >> Default >>..	Wireless	WLC-02		
2014-04-28 23:40:57.704	✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Default >> Dot1X >> D..	Default >> Default	WLC-02	PermitAccess	Registere
2014-04-28 23:40:53.114	✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Default >> Dot1X >> D..	Default >> Default	WLC-02	PermitAccess	Registere
2014-04-28 23:33:46.473	✓			employee1	10:BF:48:D0:05:67	Android	Default >> Dot1X >> D..	Default >> Default	WLC-02	PermitAccess	Registere

Endpoint ID

!88

Endp

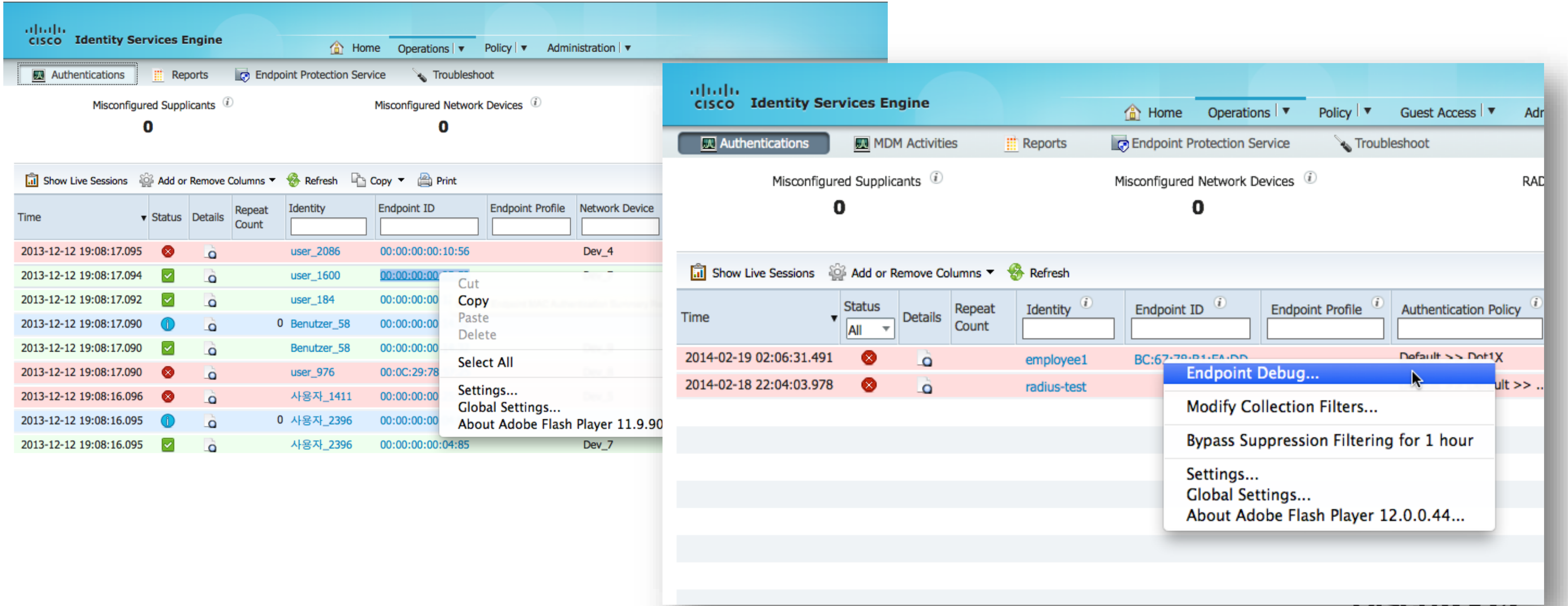
Use
'xyz' - contains 'xyz'
'!xyz' - excludes 'xyz'
'{}' - is empty
'!{}' - is not empty
'xyz*' - starts with 'xyz'
'*xyz' - ends with 'xyz'
'\!', '*', '\{', '\\' - escape

Last update: Apr 29, 14 02:51:02.216 AM UTC

Records shown: 20

Right Click in Live Log & Live Sessions

Adds Right-Click > Copy for the Endpoint ID & Identity Fields in Live Log



Misconfigured Supplicants 0

Misconfigured Network Devices 0

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-12-12 19:08:17.095	☒			user_2086	00:00:00:00:10:56		Dev_4
2013-12-12 19:08:17.094	☑			user_1600	00:00:00:00		
2013-12-12 19:08:17.092	☑			user_184	00:00:00:00		
2013-12-12 19:08:17.090	ⓘ		0	Benutzer_58	00:00:00:00		
2013-12-12 19:08:17.090	☑			Benutzer_58	00:00:00:00		
2013-12-12 19:08:17.090	☒			user_976	00:0C:29:78		
2013-12-12 19:08:16.096	☒			사용자_1411	00:00:00:00		
2013-12-12 19:08:16.095	ⓘ		0	사용자_2396	00:00:00:00		
2013-12-12 19:08:16.095	☑			사용자_2396	00:00:00:00:04:85		Dev_7

Misconfigured Supplicants 0

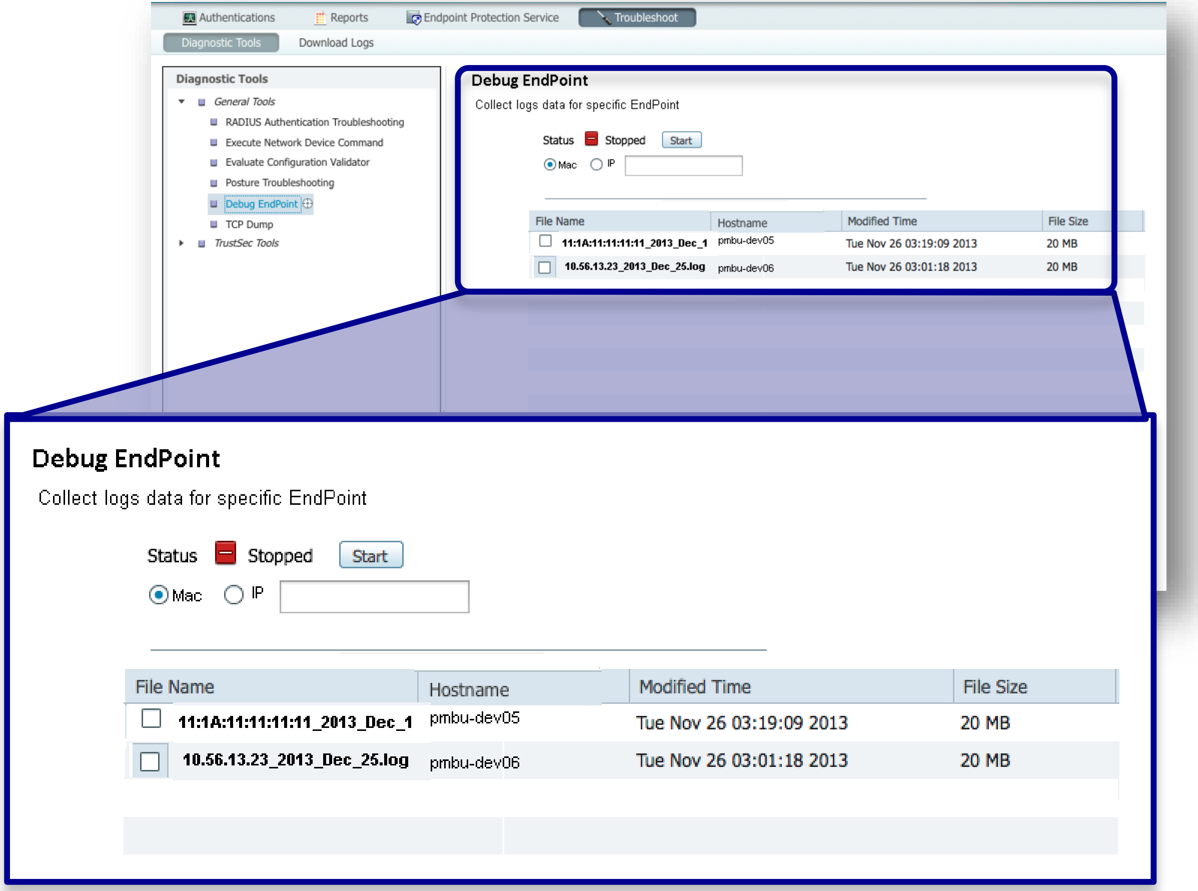
Misconfigured Network Devices 0

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy
	All						
2014-02-19 02:06:31.491	☒			employee1	BC:67:78:B1:FA:DD		Default >> Dot1X
2014-02-18 22:04:03.978	☒			radius-test			ult >> ..

Endpoint Debug...
Modify Collection Filters...
Bypass Suppression Filtering for 1 hour
Settings...
Global Settings...
About Adobe Flash Player 12.0.0.44...

Debug Endpoint

- Creates debug file of all activity for all services related to that specific endpoint
- Executes and stored per PSN
- Can be downloaded as separate files per-PSN
- Or Merged as a single file



Debug EndPoint

Collect logs data for specific EndPoint

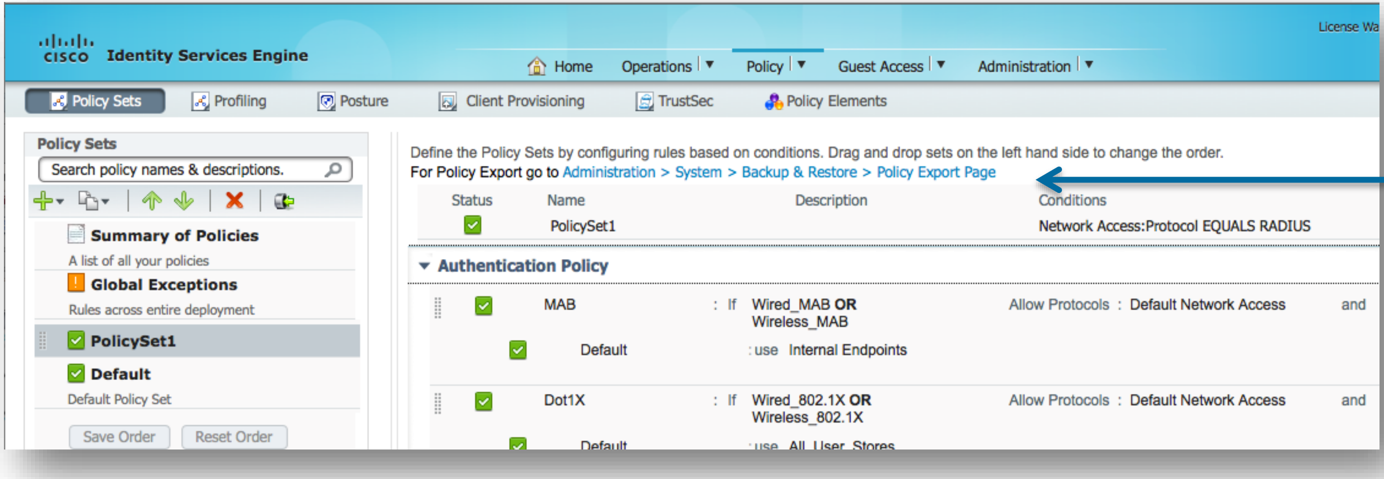
Status 🟥 Stopped Start

● Mac ○ IP

	File Name	Hostname	Modified Time	File Size
□	11:1A:11:11:11:11_2013_Dec_1	pmbu-dev05	Tue Nov 26 03:19:09 2013	20 MB
□	10.56.13.23_2013_Dec_25.log	pmbu-dev06	Tue Nov 26 03:01:18 2013	20 MB

Off-Line Examination of Configuration

Exportable Policy



Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

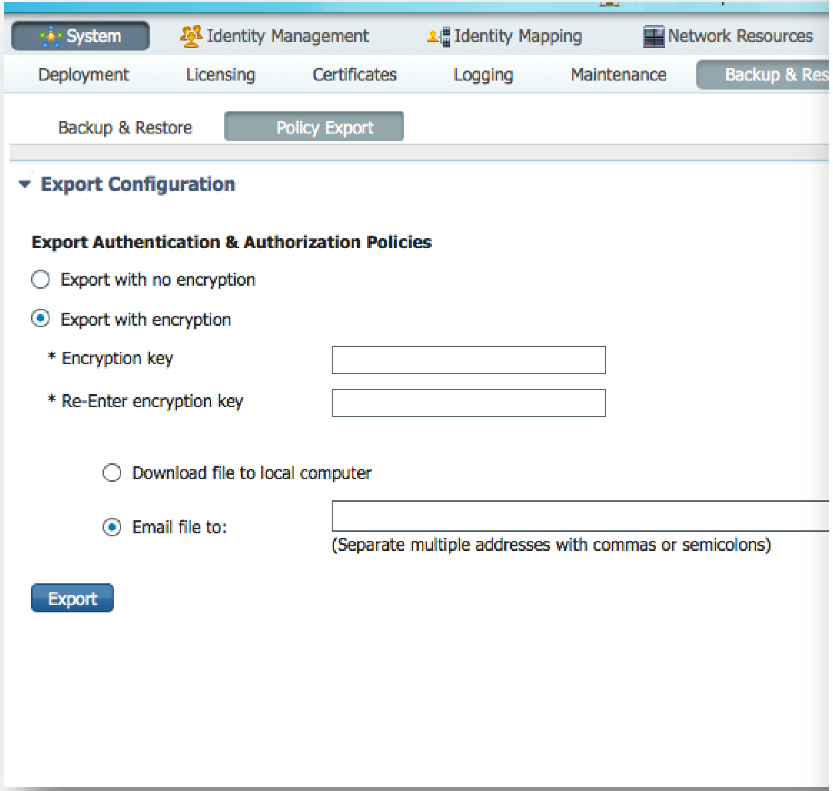
Status	Name	Description	Conditions
☑	PolicySet1		Network Access:Protocol EQUALS RADIUS

Authentication Policy

☑	MAB	: If	Wired_MAB **OR** Wireless_MAB	Allow Protocols : Default Network Access	and
☑	Default	:use	Internal Endpoints		
☑	Dot1X	: If	Wired_802.1X **OR** Wireless_802.1X	Allow Protocols : Default Network Access	and
☑	Default	:use	All_User_Stores		

Quick Link to Export Page

Exports as XML



Export Configuration

Export Authentication & Authorization Policies

○ Export with no encryption

● Export with encryption

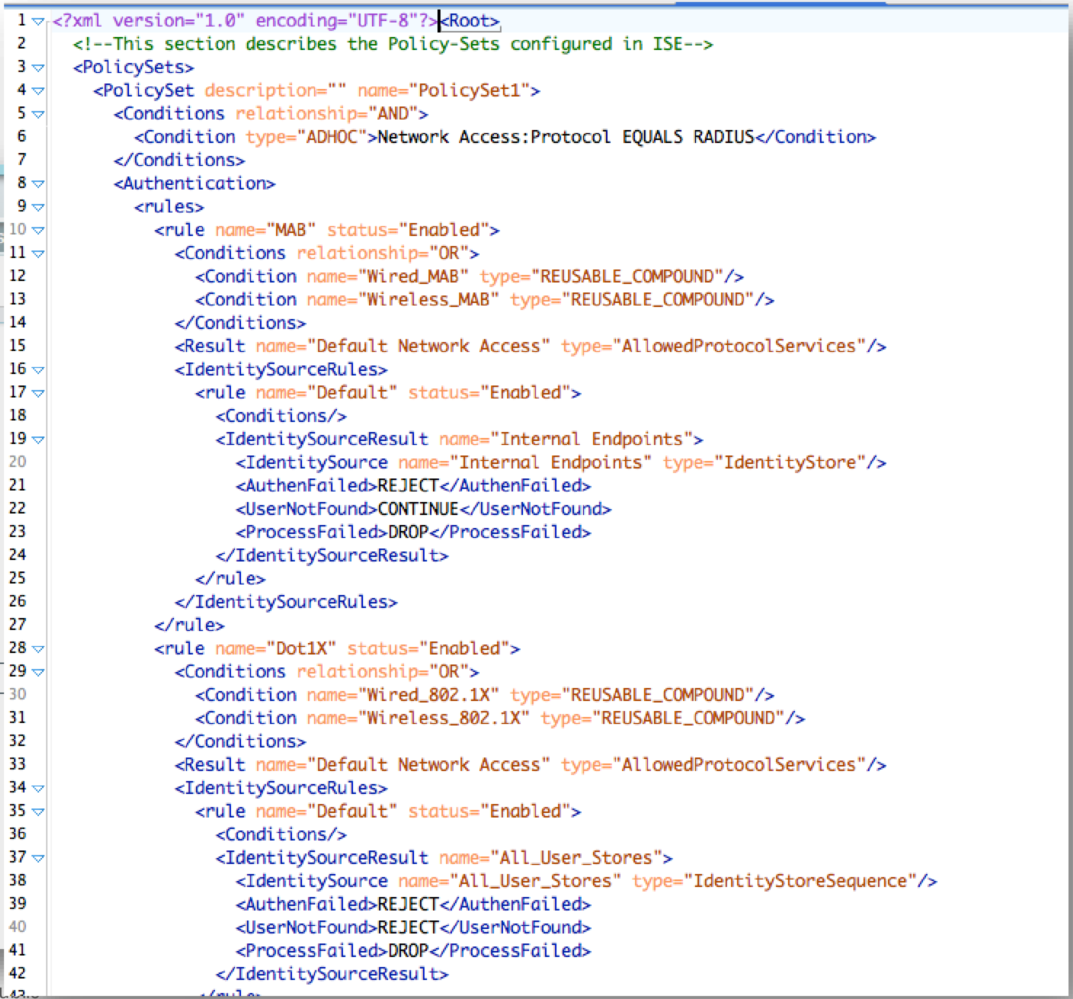
* Encryption key

* Re-Enter encryption key

○ Download file to local computer

● Email file to:

(Separate multiple addresses with commas or semicolons)



```xml
<?xml version="1.0" encoding="UTF-8"?><Root>
 <!--This section describes the Policy-Sets configured in ISE-->
 <PolicySets>
  <PolicySet description="" name="PolicySet1">
   <Conditions relationship="AND">
    <Condition type="ADHOC">Network Access:Protocol EQUALS RADIUS</Condition>
   </Conditions>
   <Authentication>
    <rules>
     <rule name="MAB" status="Enabled">
      <Conditions relationship="OR">
       <Condition name="Wired_MAB" type="REUSABLE_COMPOUND"/>
       <Condition name="Wireless_MAB" type="REUSABLE_COMPOUND"/>
      </Conditions>
      <Result name="Default Network Access" type="AllowedProtocolServices"/>
      <IdentitySourceRules>
       <rule name="Default" status="Enabled">
        <Conditions/>
        <IdentitySourceResult name="Internal Endpoints">
         <IdentitySource name="Internal Endpoints" type="IdentityStore"/>
         <AuthenFailed>REJECT</AuthenFailed>
         <UserNotFound>CONTINUE</UserNotFound>
         <ProcessFailed>DROP</ProcessFailed>
        </IdentitySourceResult>
       </rule>
      </IdentitySourceRules>
     </rule>
     <rule name="Dot1X" status="Enabled">
      <Conditions relationship="OR">
       <Condition name="Wired_802.1X" type="REUSABLE_COMPOUND"/>
       <Condition name="Wireless_802.1X" type="REUSABLE_COMPOUND"/>
      </Conditions>
      <Result name="Default Network Access" type="AllowedProtocolServices"/>
      <IdentitySourceRules>
       <rule name="Default" status="Enabled">
        <Conditions/>
        <IdentitySourceResult name="All_User_Stores">
         <IdentitySource name="All_User_Stores" type="IdentityStoreSequence"/>
         <AuthenFailed>REJECT</AuthenFailed>
         <UserNotFound>REJECT</UserNotFound>
         <ProcessFailed>DROP</ProcessFailed>
        </IdentitySourceResult>
       </rule>
```

VMWare OVA Templates!

- Finally! We have supported OVA Templates
- Ensures customers will not mis-configure their VMWare settings
  - Preset: Reservations, vCPU's, Storage
- Based on following Specs:

ISE-1.3.x.x-Eval-100-endpoint.ova:

- 4 CPU cores
- 4 GB RAM
- 200 GB disk
- 4 NICs

ISE-1.3.x.x-Virtual-SNS-3415.ova:

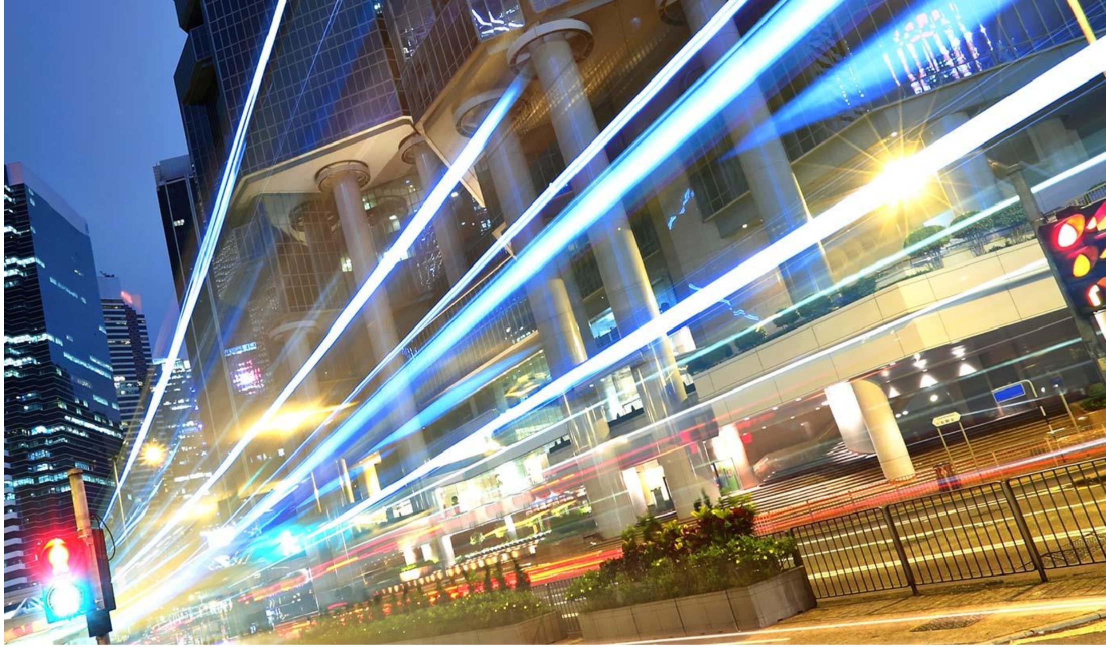
- 4 CPU cores
- 16 GB RAM
- 600 GB disk
- 4 NICs

ISE-1.3.x.x-Virtual-SNS-3495.ova:

- 8 CPU cores
- 32 GB RAM
- 600 GB disk
- 4 NICs

Agenda

- Introduction
- Certificates, Certificates, Certificates
- BYOD Best Practices
- Integrating with Cisco and Non-Cisco
- ISE in a Security EcoSystem
- Serviceability & Troubleshooting
- Staged Deployments (Time Permitting)
- Conclusion



Staged Deployments

Monitor Mode Policies

- BE CAREFUL

- Monitor Mode needs to keep Authorisation Results simple
  - Access-Accept / Reject
  - For Phones, needs: Voice Domain also

- Local Authorisations Still Possible (be careful):

```
interface X
 authentication event fail action next-method
 authentication event server dead action reinitialize vlan 11
 authentication event server dead action authorize voice
 authentication event server alive action reinitialize
 authentication violation restrict
```

Good for Monitor Mode

```
interface X
 authentication event fail action authorize vlan 4096
 authentication event server dead action reinitialize vlan 11
 authentication event server dead action authorize voice
 authentication event server alive action reinitialize
 authentication violation restrict
```

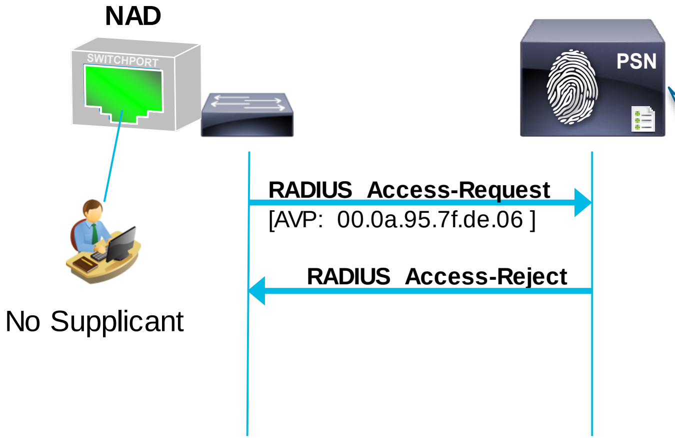
Dangerous for Monitor Mode

Moving from Monitor to Low-Impact Mode

- Monitor Mode

```
interface GigabitEthernet1/0/1
 authentication open
 mab
 dot1x pae authenticator
```

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
BYOD	if	BYOD and Employee	then	Employee
Non_AuthZ	if	i-device or Android	then	GUEST
Contractor	if	Contractor	then	Contractor
Employee	if	Employee	then	Employee
Default	If no matches, then	Deny Access		



Matched Rule = Default

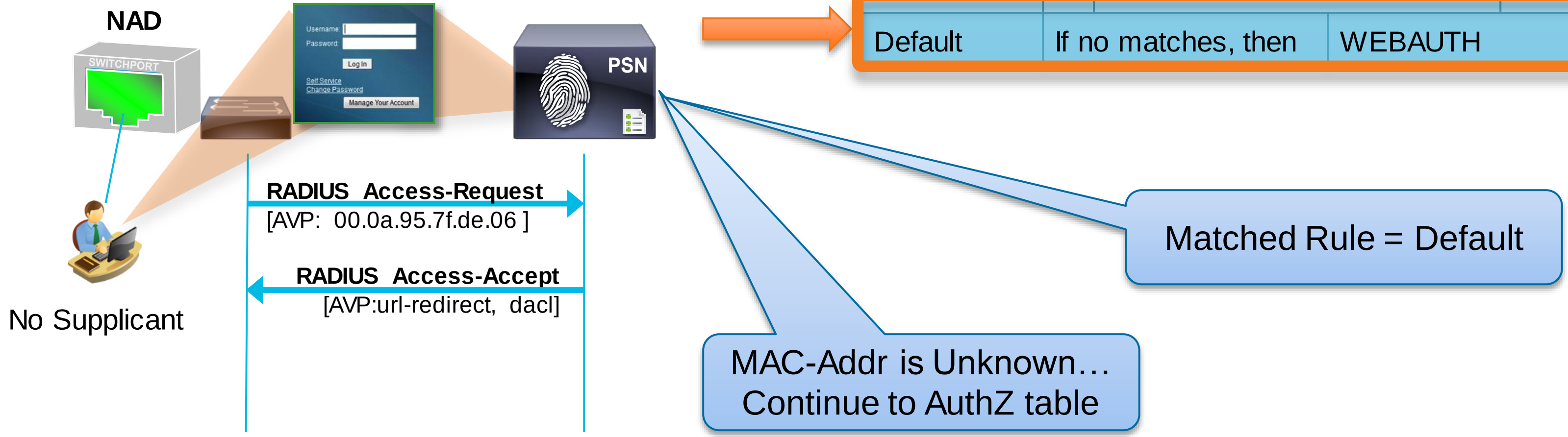
MAC-Addr is Unknown…
Continue to AuthZ table

Moving from Monitor to Low-Impact

- Low-Impact

```
interface GigabitEthernet1/0/1
 authentication open
 mab
 dot1x pae authenticator
 ip access-group ACL-DEFAULT in
```

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
BYOD	if	BYOD and Employee	then	Employee
Non_AuthZ	if	i-device or Android	then	GUEST
Contractor	if	Contractor	then	Contractor
Employee	if	Employee	then	Employee
Default	If no matches, then	WEBAUTH		



No Supplicant

RADIUS Access-Request
[AVP: 00.0a.95.7f.de.06]

RADIUS Access-Accept
[AVP:url-redirect, dacl]

Matched Rule = Default

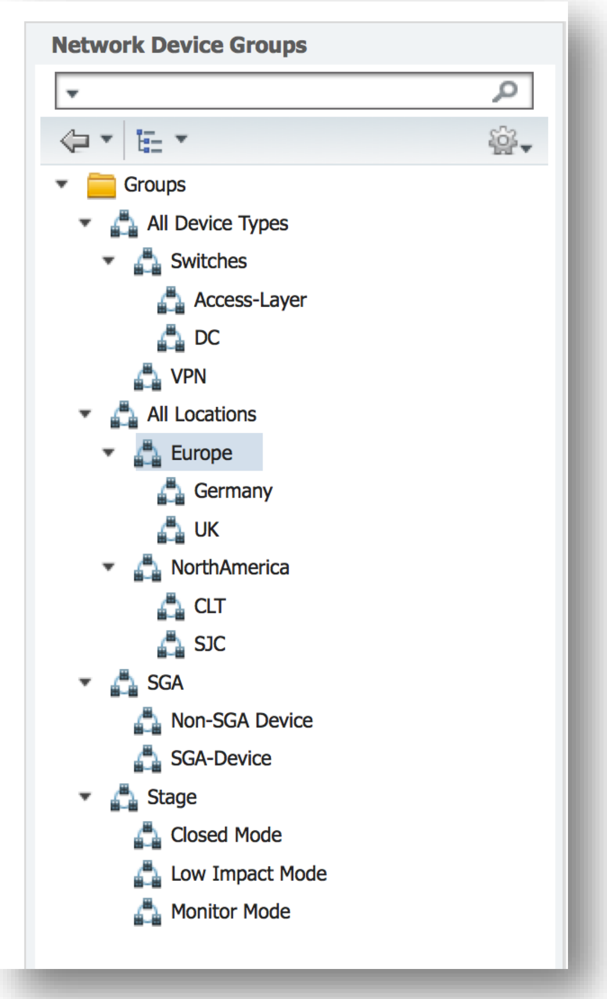
MAC-Addr is Unknown…
Continue to AuthZ table

Network Device Groups

- Creation of many: Organise & Why use them

- A little up-front work, can really help you get specific in your policies.

- Organise by:
  - Device Type
    - Wired / Wireless / Firewall / VPN
    - OEAP / CVO
  - Place in Network
    - Access-Layer / Data Centre
  - Geographic Location



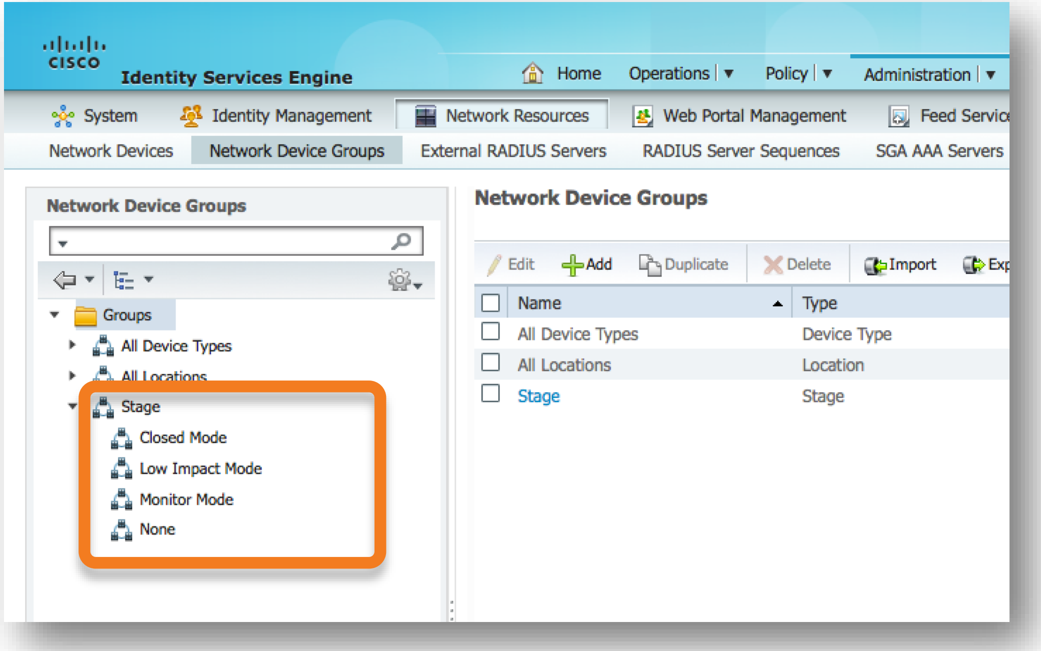
Network Device Groups

- Groups
  - All Device Types
    - Switches
      - Access-Layer
      - DC
    - VPN
  - All Locations
    - Europe
      - Germany
      - UK
    - NorthAmerica
      - CLT
      - SJC
  - SGA
    - Non-SGA Device
    - SGA-Device
  - Stage
    - Closed Mode
    - Low Impact Mode
    - Monitor Mode

Moving from Monitor to Low-Impact

- Low-Impact: An *Entire* Switch at a Time

- Create a Network Device Group for all Switches that will use Low-Impact.

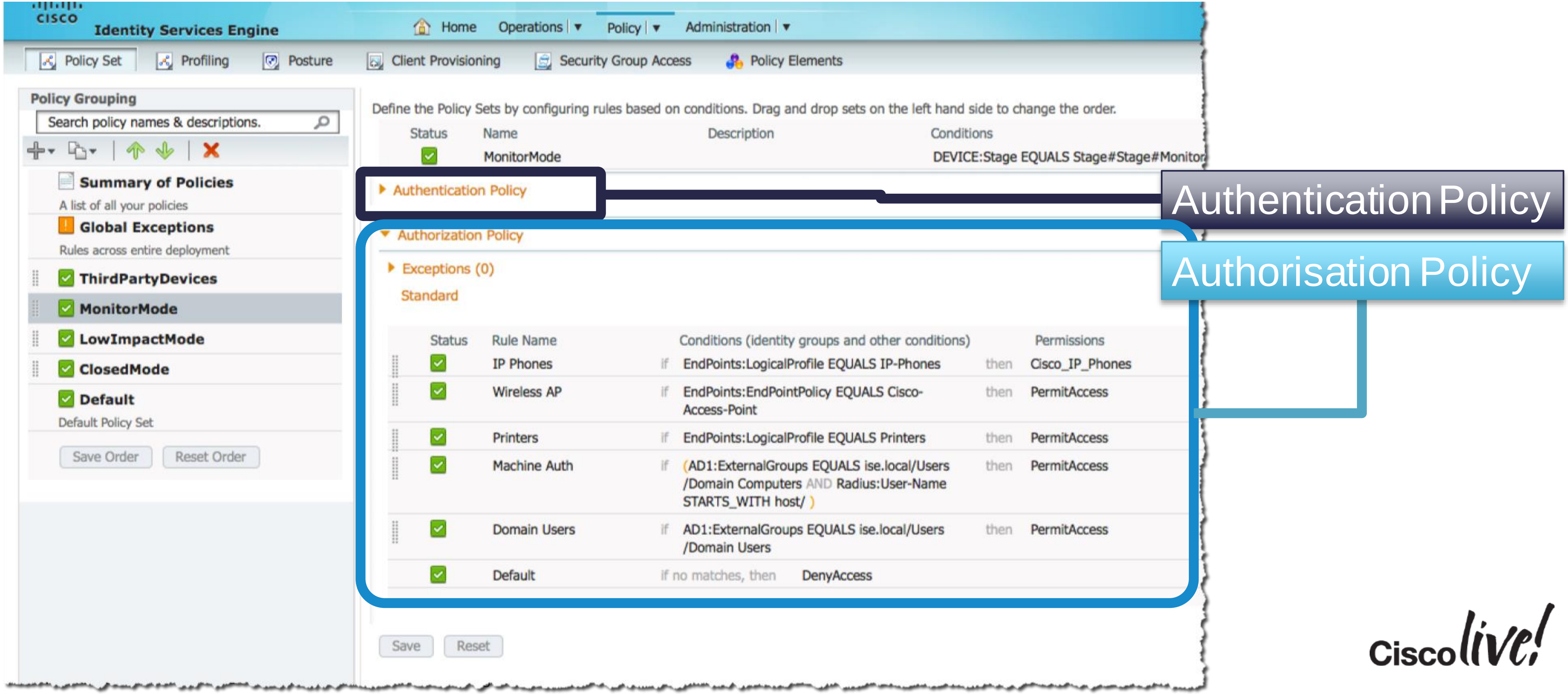


☐	Name	Type
☐	All Device Types	Device Type
☐	All Locations	Location
☐	Stage	Stage

ISE 1.2: Policy Sets

ISE 1.2+

- Separate Set of Policies for Each Mode of Deployment



Policy Grouping

Search policy names & descriptions.

Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

☑ **ThirdPartyDevices**

☑ **MonitorMode**

☑ **LowImpactMode**

☑ **ClosedMode**

☑ **Default**
Default Policy Set

Save Order | Reset Order

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.

Status	Name	Description	Conditions
☑	MonitorMode		DEVICE:Stage EQUALS Stage#Stage#Monitor

▸ Authentication Policy

▾ Authorization Policy

▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	IP Phones	if	EndPoints:LogicalProfile EQUALS IP-Phones	then	Cisco_IP_Phones
☑	Wireless AP	if	EndPoints:EndPointPolicy EQUALS Cisco-Access-Point	then	PermitAccess
☑	Printers	if	EndPoints:LogicalProfile EQUALS Printers	then	PermitAccess
☑	Machine Auth	if	(AD1:ExternalGroups EQUALS ise.local/Users /Domain Computers AND Radius:User-Name STARTS_WITH host/)	then	PermitAccess
☑	Domain Users	if	AD1:ExternalGroups EQUALS ise.local/Users /Domain Users	then	PermitAccess
☑	Default		if no matches, then		DenyAccess

Save | Reset

Authentication Policy

Authorisation Policy

Moving from Monitor to Low-Impact

- mab eap Trick of the Trade

- What is “mab eap”?
  - Option of MAB configuration uses EAP-MD5 to transmit the MAB data.
- Behaviour with ISE will be the same.
  - We can use this as a differentiator ports that should be in Low-Impact.

```
C3750X(config-if)#mab ?
  eap  Use EAP authentication for MAC Auth Bypass
  <cr>
C3750X(config-if)#mab eap
C3750X(config-if)#description Conference Room B
```

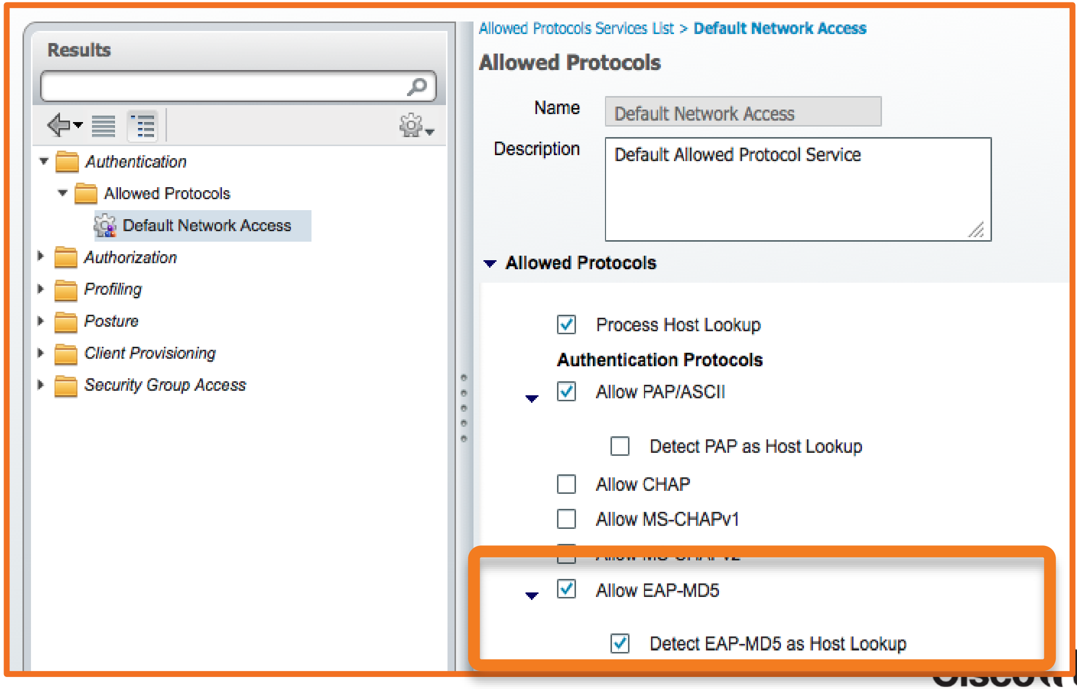
Available with ISE 1.1+

*6500 added support in SXJ4

Moving from Monitor to Low-Impact

- MAB EAP Trick of the Trade

- Policy → Policy Elements → Authentication → Results →Allowed Protocols
  - Allow EAP-MD5
  - Detect EAP-MD5 as Host Lookup



Results

Authentication
Allowed Protocols
Default Network Access
Authorization
Profiling
Posture
Client Provisioning
Security Group Access

Allowed Protocols Services List > **Default Network Access**

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII

☐ Detect PAP as Host Lookup

☐ Allow CHAP

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

☑ Allow EAP-MD5

☑ Detect EAP-MD5 as Host Lookup

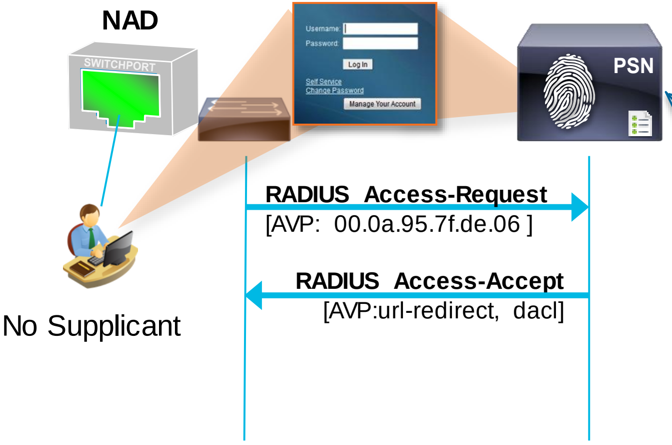
Note: Best-Practice is to never modify default objects

Moving from Monitor to Low-Impact

- MAB EAP Trick of the Trade

```
interface GigabitEthernet1/0/1
 authentication open
 mab eap
 dot1x pae authenticator
 ip access-group ACL-DEFAULT in
```

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
BYOD	if	BYOD and Employee	then	Employee
Non_AuthZ	if	i-device or Android	then	GUEST
Contractor	if	Contractor	then	Contractor
Employee	if	Employee	then	Employee
Conf_Rooms	if	Network Access:EapAuthentication EQUALS EAP-MD5	then	WEBAUTH
Default	If no matches, then	Deny Access		



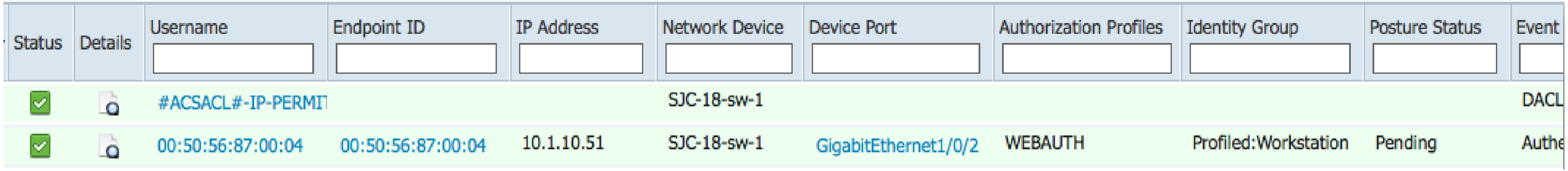
Matched Rule = Conf_Rooms

MAC-Addr is Unknown…
Continue to AuthZ table

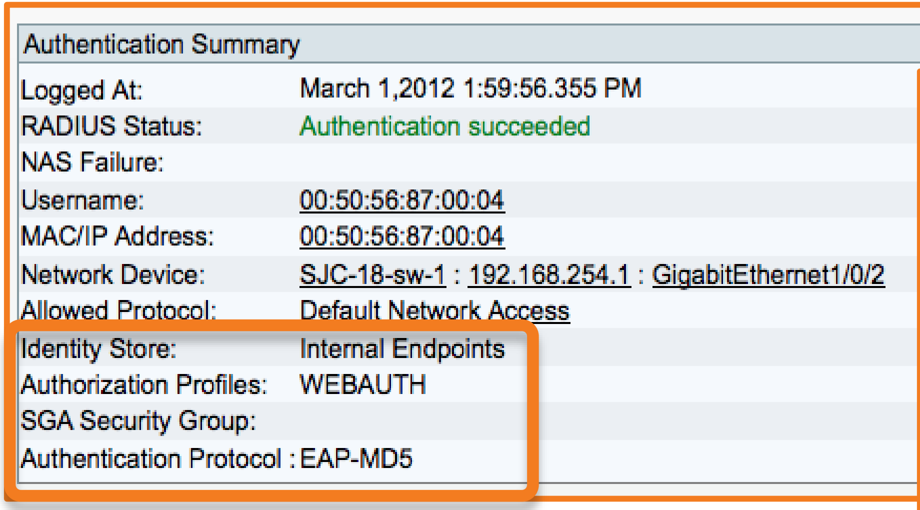
All Other Switches
Will still be in Monitor
Mode!

Moving from Monitor to Low-Impact

- MAB EAP Trick of the Trade

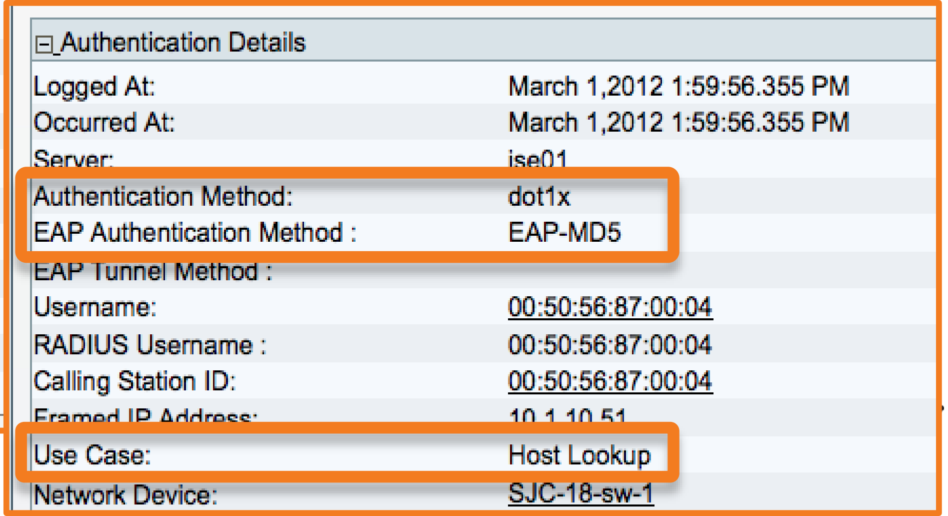


Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
✓		#ACSACL#-IP-PERMIT			SJC-18-sw-1					DACL
✓		00:50:56:87:00:04	00:50:56:87:00:04	10.1.10.51	SJC-18-sw-1	GigabitEthernet1/0/2	WEBAUTH	Profiled:Workstation	Pending	Authe



Authentication Summary

Logged At:	March 1,2012 1:59:56.355 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	00:50:56:87:00:04
MAC/IP Address:	00:50:56:87:00:04
Network Device:	SJC-18-sw-1 : 192.168.254.1 : GigabitEthernet1/0/2
Allowed Protocol:	Default Network Access
Identity Store:	Internal Endpoints
Authorization Profiles:	WEBAUTH
SGA Security Group:	
Authentication Protocol :	EAP-MD5

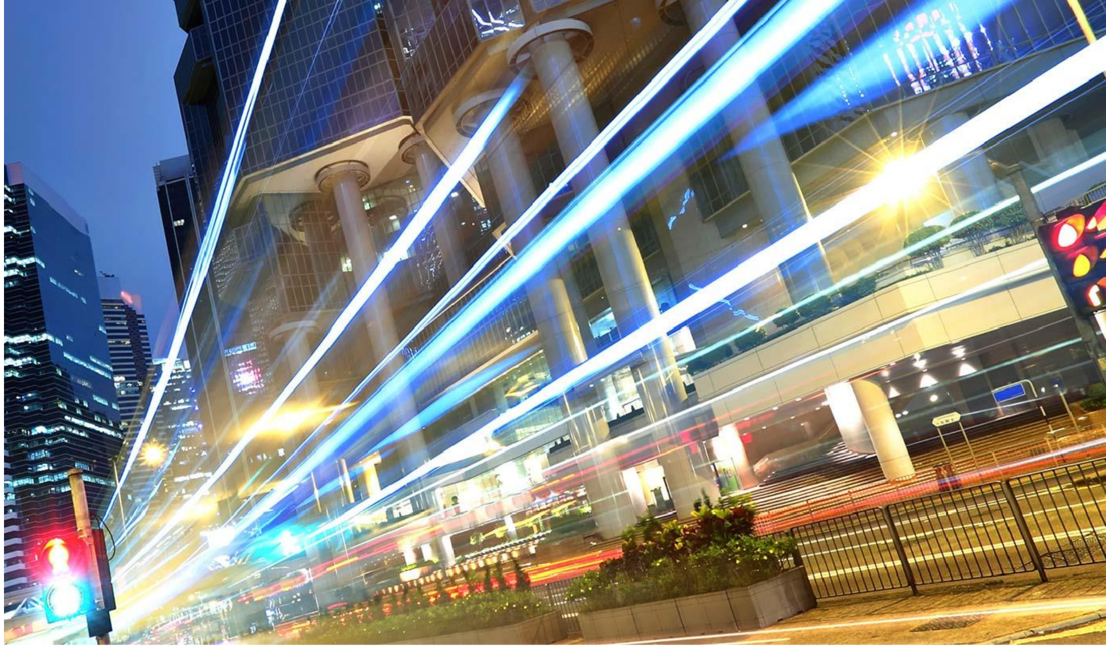


⊟ Authentication Details

Logged At:	March 1,2012 1:59:56.355 PM
Occurred At:	March 1,2012 1:59:56.355 PM
Server:	ise01
Authentication Method:	dot1x
EAP Authentication Method :	EAP-MD5
EAP Tunnel Method :	
Username:	00:50:56:87:00:04
RADIUS Username :	00:50:56:87:00:04
Calling Station ID:	00:50:56:87:00:04
Framed IP Address:	10.1.10.51
Use Case:	Host Lookup
Network Device:	SJC-18-sw-1

Agenda

- Introduction
- Certificates, Certificates, Certificates
- BYOD Best Practices
- Integrating with Cisco and Non-Cisco
- ISE in a Security EcoSystem
- Serviceability & Troubleshooting
- Staged Deployments (Time Permitting)
- Conclusion



Recommended Reading

- Buy our book, help us afford more beer!
- http://amzn.com/1587143259

SECURITY

Cisco Identity Services Engine for Secure Unified Access:

BYOD Network Security with ISE

Aaron T. Woland, CCIE No. 20113
Jamey Heary, CCIE No. 7680

Call to Action

- Visit the World of Solutions for
  - Cisco Campus – (speaker to add relevant demos/areas to visit)
  - Walk in Labs – (speaker to add relevant walk in labs)
  - Technical Solution Clinics
- Meet the Engineer (Speaker to specify when they will be available for meetings)
- Lunch time Table Topics
- DevNet zone related labs and sessions
- Recommended Reading: for reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2015

IPv6-only Experimental SSID (with NAT64)

SSID: IPV6ONLYEXP

PASS: iknowbesteffort

Addressing: SLAAC + stateless DHCPv6

Offsite NAT64 (Thanks to Go6 Institute)

Questions/support: @ayourtch

Hashtag: #IPV6ONLYEXP

SLA: it's in the password ☺

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

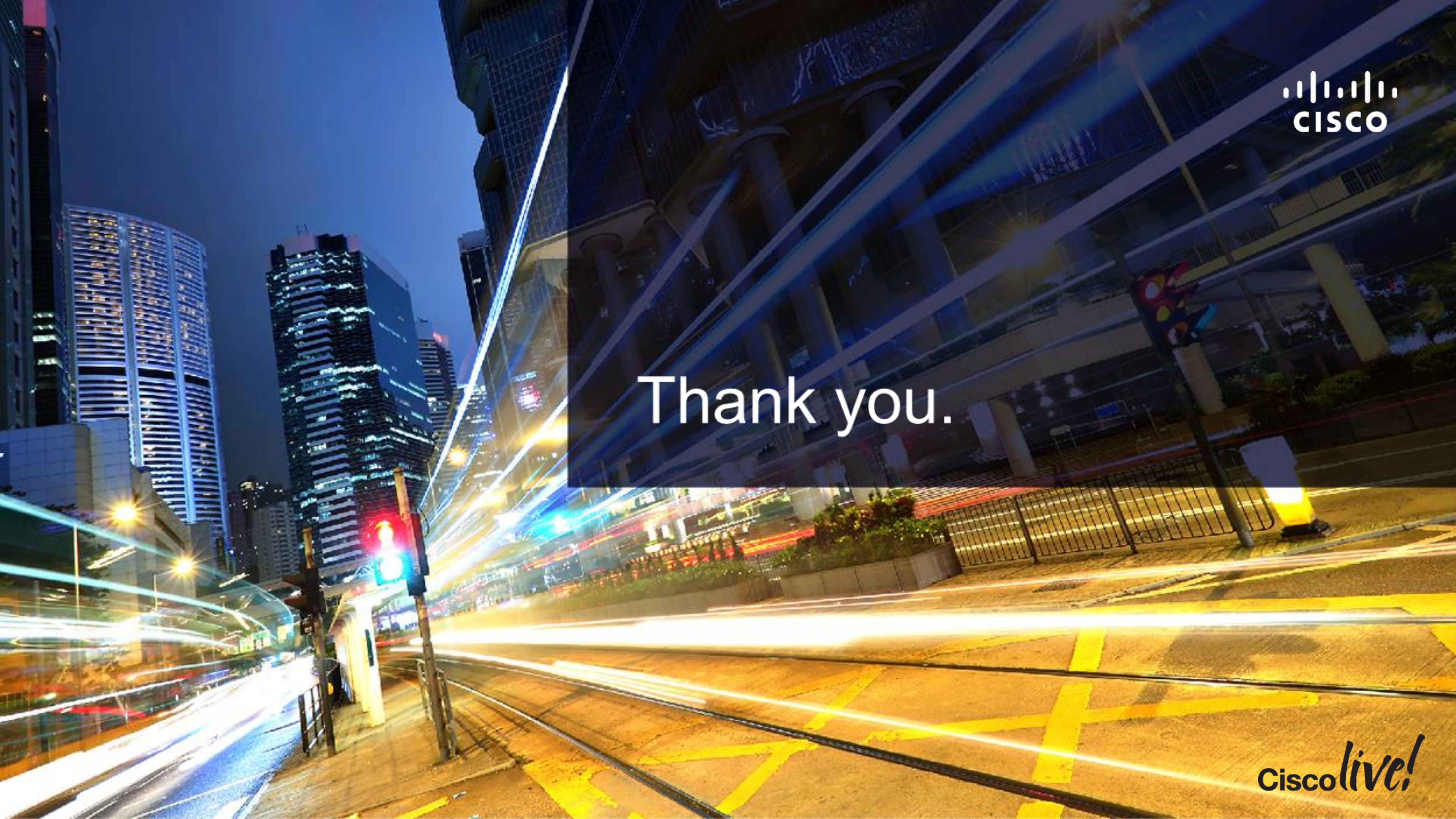
Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Cisco live!



Thank you.

CISCO

CISCO