



ISE Posture

Deployment & Troubleshooting



[Zhang Yin](#)

Yinzhan@cisco.com

Topics

- Posture overview & solution evolution
- Posture Deployment & Policy design
- ISE Posture work flow
- ISE Posture Troubleshooting

Posture overview & evolution

- Posture Definition
- Posture status
- Posture assessment
- Posture solution evolution

Posture Defination

- **Posture**= The state-of-compliance with the company's security policy
- -Is the system running the current windows patches?
- -Anti-Virus/Anti-Spyware Installed? IS it UP-to-Date?
- -Is the endpoint running corporate application?
- -Is the endpoint running unauthorized application?

Posture & Security Detection

Employee Policy:

- Microsoft patches updated
- Trend Micro AV installed, running, and current
- Corp asset checks

Microsoft

TREND MICRO



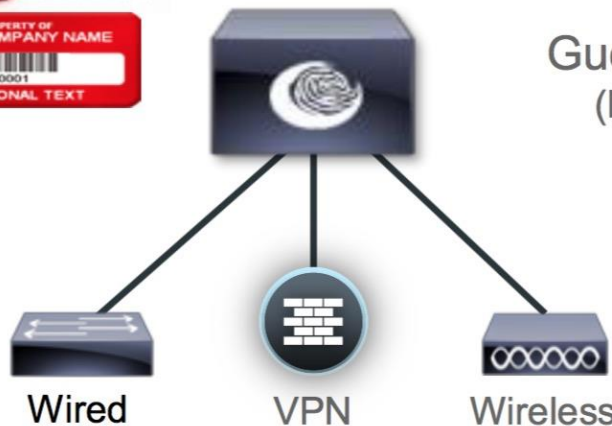
Contractor Policy:

- Any AV installed, running, and current

Windows OneCare Live

PREVX
LAVASOFT

Guest Policy: Accept AUP (No posture - Internet Only)



Employees



Contractors/Guests

Posture Status

- **Compliant**

When the posture assessment occurs, the endpoint meets all the mandatory requirements that are defined in the matching posture policy

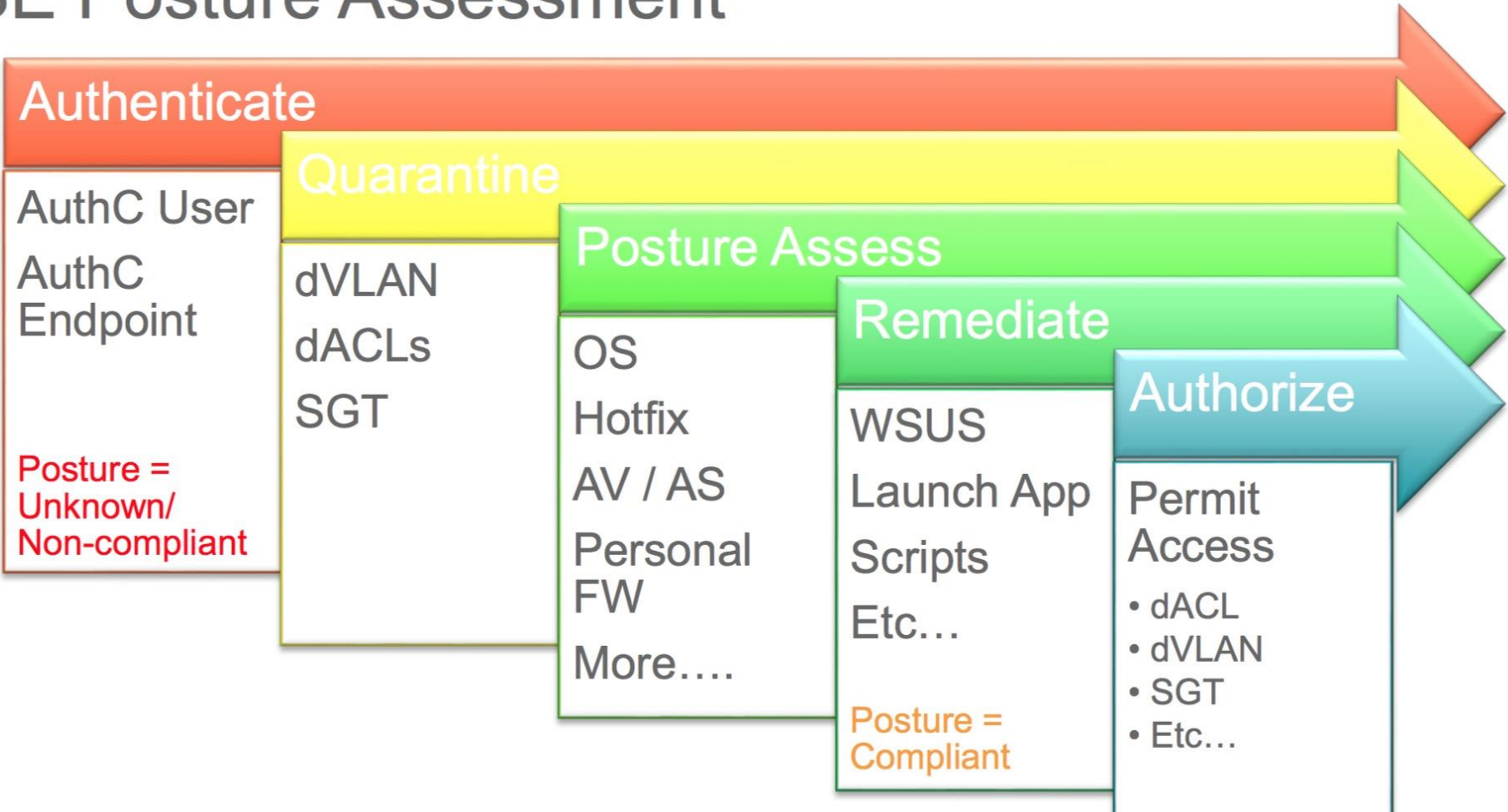
- **Uncompliant**

when a matching posture policy is defined for that endpoint but it fails to meet all the mandatory requirements during posture assessment.

- **Unknow**

an endpoint where a matching posture policy is enabled but posture assessment has not yet occurred for that endpoint

ISE Posture Assessment



Authenticate

AuthC User
AuthC
Endpoint

Posture =
Unknown/
Non-compliant

Quarantine

dVLAN
dACLs
SGT

Posture Assess

OS
Hotfix
AV / AS
Personal
FW
More....

Posture =
Compliant

Remediate

WSUS
Launch App
Scripts
Etc...

Authorize

Permit
Access
• dACL
• dVLAN
• SGT
• Etc...

Cisco's Posture Evolution

- **Cisco Clean Access Server**

Serves as an in-band or out-of-band device for network access control



- **Cisco Clean Access Manager**

Centralizes management for administrators, support personnel, and operators



- **Cisco Clean Access Agent**

Optional lightweight client for device-based registry scans in unmanaged environments

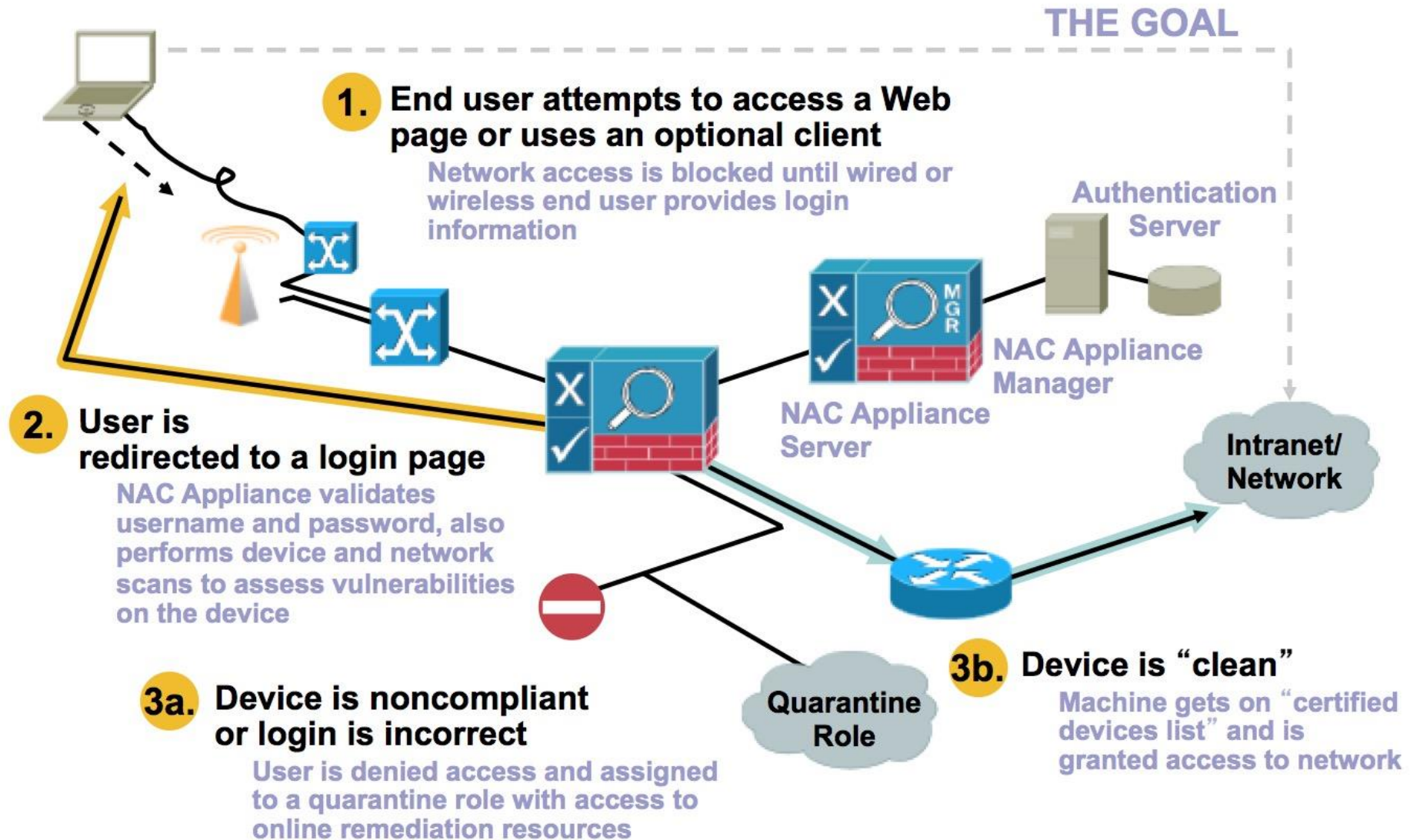


- **Rule-set Updates**

Scheduled automatic updates for anti-virus, critical hot-fixes and other applications



Cisco's Posture Evolution



Cisco's Posture Evolution

- SNMP → 802.1X

 - support more switch or controller based 802.1x standard
 - support OS supplicant agent.

- Cancel the enforcer role (CAS server)

 - reduce the deployment complexity
 - virtualization (cas not support virtualization)

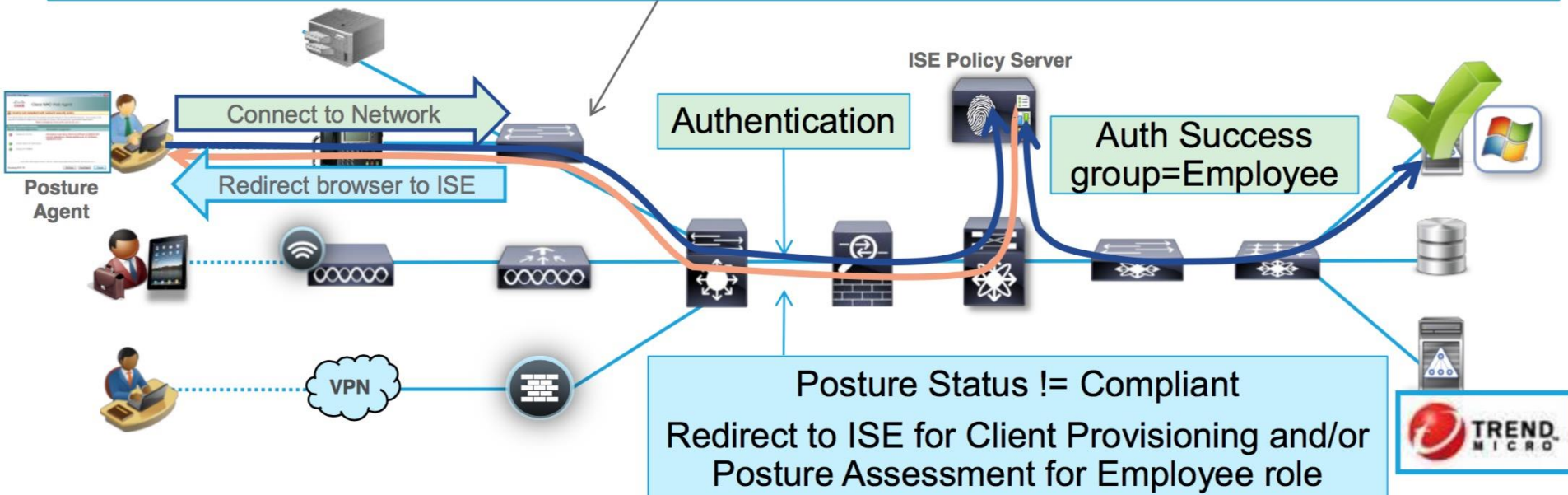
- Split Auth/Posture function to different components

 - Nac agent only for posture function
 - Native client or anyconnect for authentication

ISE working flow

- If Posture Status = Unknown/Non-Compliant, then Redirect to ISE for Posture Assessment
- If Posture Agent not deployed, then provision Web Agent or Persistent NAC Agent

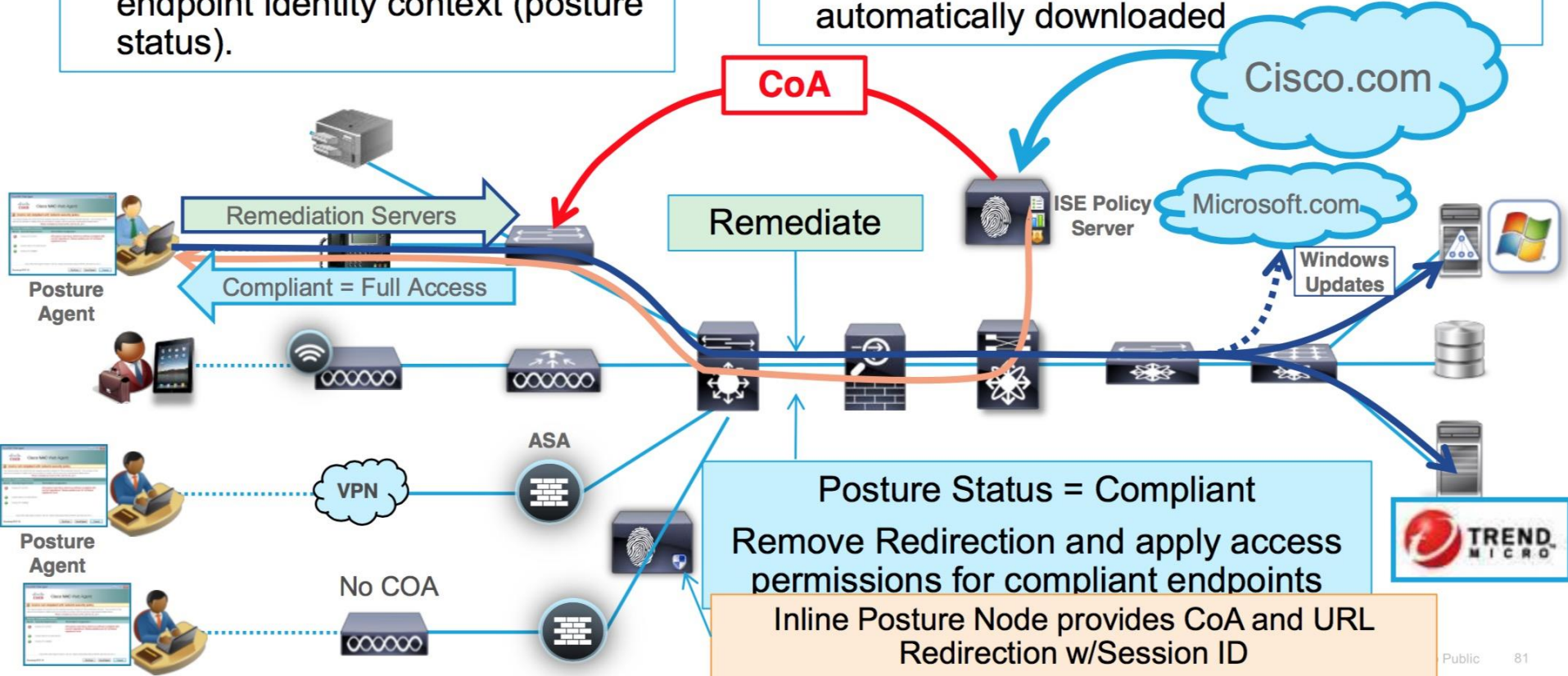
<https://ise.company.com:8443/guestportal/gateway?sessionId=0A010A...73691A&action=cpp>



ISE working flow

- CoA allows re-authentication to be processed based on new endpoint identity context (posture status).

- Hourly updates for latest posture definitions
- New posture agents and modules automatically downloaded



Posture Deployment

- Posture & license & Compatibility
- Provisioning working flow
- Provisioning policy
- Posture agent type
- Posture condition
- Posture policy
- Posture working flow

ISE Posture Deployment- license

If you have not installed the Apex license on the PAN, then the posture requests will not be served in Cisco ISE.

Cisco ISE License Package	Focus	Perpetual or Subscription (Terms Available)	Notes
Evaluation	Limited use of Cisco ISE product for presales customer trials/evaluations	Temporary (90 days)	Full Cisco ISE functionality (Device Admin, Base, Plus and Apex) is provided for 100 endpoints. See license details below
Device Administration	Enables Device Administration/TACACS + support for networking devices	Perpetual	Add-on to Base licenses. Deployment wide license.
Base	Provides highly secure endpoint and user access	Perpetual	-
Plus	Provides context about endpoints for more detailed access policies	Subscription (1, 3, or 5 years)	Does not include Base services; Base licenses are required to install Plus licenses
Apex	Provides compliance details about endpoints for more detailed access policies	Subscription (1, 3, or 5 years)	Does not include Base or Plus services; Base licenses are required to install Apex licenses. Please note that Cisco AnyConnect Apex user licenses are required in addition to Cisco ISE Apex licenses when making use of Cisco AnyConnect unified agent services across wired, wireless, and VPN
Mobility Upgrade	Helps enable wired endpoint support for Wireless/Mobility license deployments	Subscription (1, 3, or 5 years)	See the Cisco ISE License Ordering Guidelines section for quantity requirements

ISE Posture Deployment- license



Apex	Subscription (1, 3, or 5 years)	<ul style="list-style-type: none"> • Third Party Mobile Device Management (MDM) • Posture Compliance 	Does not include Base services; a Base license is required to install the Apex license.
------	---------------------------------	--	---

ISE Posture Feature Compatibility

Table 1 Supported Network Access Devices

Device	Recommended OS ¹	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec ²
	Minimum OS ³							
Cisco Access Switches								
IE2000 IE3000	IOS 15.2(2) E4	√	√	√	√	√	√	√
	IOS 15.0(2) EB	√	√	√	√	√	√	√
CGS 2520	IOS 15.2(3)E3	√	√	√	√	√	√	√
	IOS 15.2(3)E3	√	√	√	√	√	√	√
Catalyst 2960 LAN Base	IOS 12.2.55- SE10	√	√	√	√	√	√	X
	IOS v12.2. (55)SE5	√	√	√	√	√	√	X

http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/compatibility/ise_sdt.html#pgfId-55038

ISE Agent compatibility

Cisco NAC Agent Interoperability Between Cisco NAC Appliance and Cisco ISE

The Cisco NAC Agent versions 4.9.5.3 and later can be used on both Cisco NAC Appliance Releases 4.9(3), 4.9(4), 4.9(5) and Cisco ISE Releases 1.1.3-patch 11, 1.1.4-patch 11, 1.2, 1.3, 1.4, 2.0, 2.1. This is the recommended model of deploying the NAC agent in an environment where users will be roaming between ISE and NAC deployments.



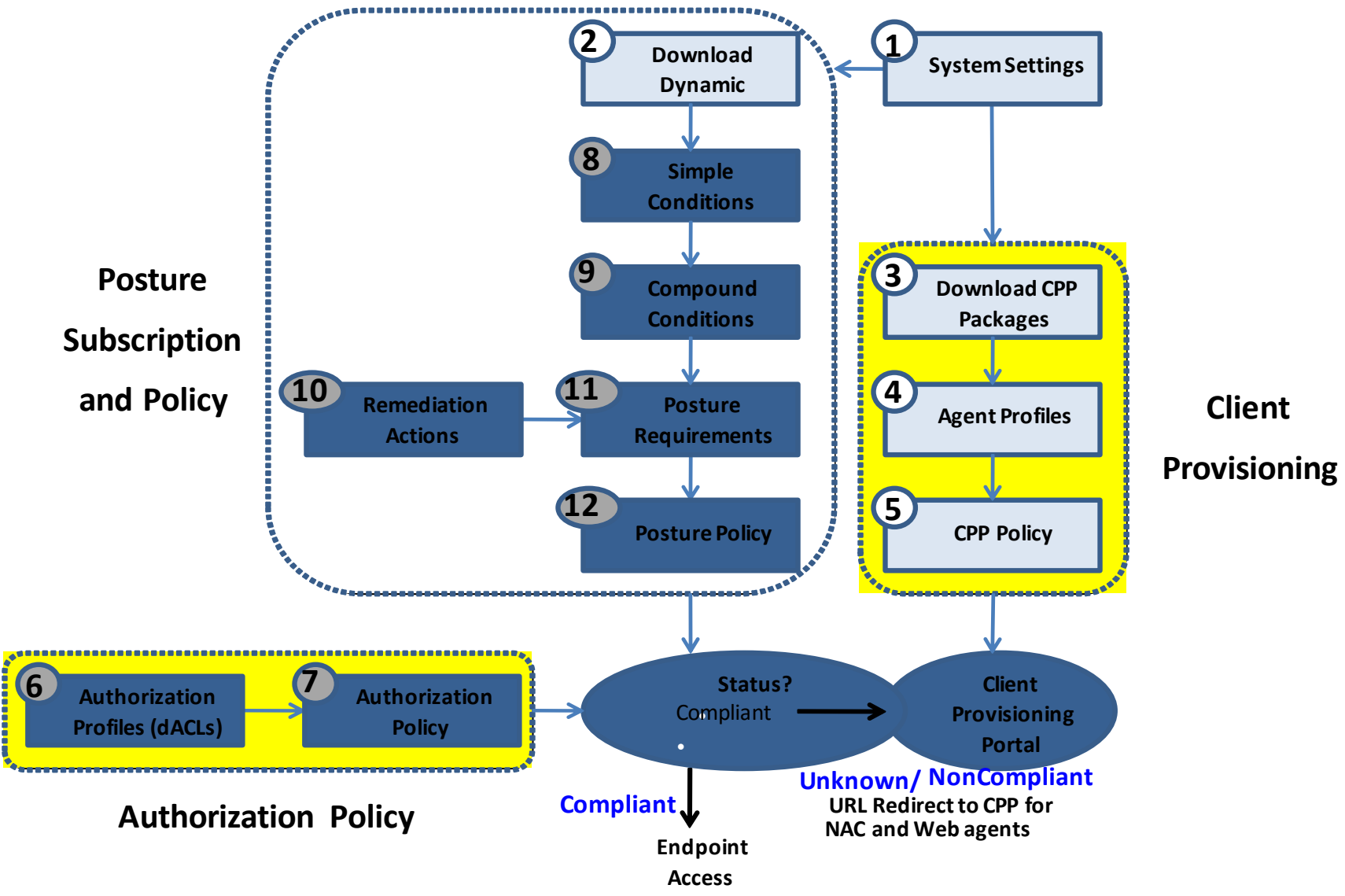
Note The new features introduced in Cisco ISE 1.4 and later releases, such as the Service Check (MAC OS X), File Check (MAC OS X), Application Check (MAC OS X), and Patch Management Check (MAC OS X and Windows), are available only with AnyConnect 4.1.00028 or later. Refer to the [Cisco Identity Services Engine Administrator Guide, Release 2.1](#) for more information.

Client Machine Operating Systems and Agent Support in Cisco ISE

- [Google Android](#)
- [Apple iOS](#)
- [Apple Mac OS X](#)
- [Microsoft Windows](#)
- [Google Chromebook](#)
- [Others](#)

http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/compatibility/ise_sdt.html#79794

ISE Posture Deployment- Provisioning



Redirect traffic to ISE

- Example of ACL on switch

ip access-list extended Redirect

deny udp any eq bootpc any eq bootps

deny udp any any eq domain

deny ip any host x.x.x.x (ISE server)

deny ip any host y.y.y.y (AD,CA,Patch,AV update server etc)

permit ip any any

ip http server

ip http secure-server

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

Client Provisioning (Posture) ▼

ACL Redirect

Value Client Provisioning Portal (defa ▼)

ISE Posture Deployment- Provisioning

Client Provisioning

* Enable Provisioning: ▾


* Enable Automatic Download: ▾ ⓘ



* Update Feed URL:

* Native Supplicant Provisioning Policy Unavailable: ▾

Edit <input type="button" value="+ Add"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/>					
<input type="checkbox"/>	Name	Version	Last Update	Description	
<input type="checkbox"/>	Agent resources from Cisco site				
<input type="checkbox"/>	Agent resources from local disk				
<input type="checkbox"/>	Native Supplicant Profile	Supplicant Profile	Not Applicable	2016/05/25 04:11:22	Pre-configured Native Supplicant...
<input type="checkbox"/>	WinSPWizard	WinSPWizard	1.0.0.46	2016/06/08 04:30:56	Supplicant Provisioning Wizard f...
<input type="checkbox"/>	MacOSXSPWizard	MacOSXSPWizard	2.0.2.37	2016/06/08 04:31:17	Supplicant Provisioning Wizard f...
<input type="checkbox"/>	MacOSAMP Enabler Profile	MacOSAMP Enabler Profile	1.0.0.36	2016/06/08 04:31:29	Supplicant Provisioning Wizard f...
<input type="checkbox"/>	WinSPWizard 2.0.1.46	WinSPWizard	2.0.1.46	2016/06/08 04:33:29	Supplicant Provisioning Wizard f...
<input type="checkbox"/>	MACComplianceModule 3.6.10591.2	MACComplianceModule	3.6.10591.2	2016/06/08 04:34:10	MACAgent ComplianceModule v...
<input type="checkbox"/>	AnyConnectComplianceModuleOSX ...	AnyConnectComplianceMo...	3.6.10547.2	2016/06/08 04:37:09	AnyConnect OS X Compliance ...
<input type="checkbox"/>	MacOSXSPWizard 2.1.0.40	MacOSXSPWizard	2.1.0.40	2016/06/08 04:37:27	Supplicant Provisioning Wizard f...
<input type="checkbox"/>	MacOSXAgent 4.9.5.3	MacOSXAgent	4.9.5.3	2016/06/08 04:37:51	NAC Posture Agent for Mac OS...
<input type="checkbox"/>	AnyConnectComplianceModuleWind...	AnyConnectComplianceMo...	3.6.10547.2	2016/06/08 04:39:07	AnyConnect Windows Complian...
<input type="checkbox"/>	AgentCustomizationPackage 1.1.1.6	AgentCustomizationPackage	1.1.1.6	2016/06/08 04:39:44	This is the NACAgent Customiza...

ISE Posture Deployment- Provisioning

Search...  [Expand All](#) | [Collapse All](#)

Release 2.1.0 [Release Notes for 2.1.0](#)  [Add Device](#)  [Add Notification](#)

▼ Latest
2.1.0
1.4
1.3
2.0
▼ All Releases
▶ 2
▶ 1
▶ Deferred Releases

File Information	Release Date	Size	
Offline Mac OS SPW Installation Package mac-spw-dmg-2.1.0.40-isebundle.zip	31-MAY-2016	0.58 MB	Download Add to cart Publish
Offline Mac Agent Installation Package macagent-4.9.5.3-isebundle.zip	31-MAY-2016	4.05 MB	Download Add to cart Publish
Offline NAC Agent Installation Package nacagent-4.9.5.8-isebundle.zip	31-MAY-2016	8.90 MB	Download Add to cart Publish
Offline Web Agent Installation Package webagent4.9.5.7-isebundle.zip	31-MAY-2016	4.21 MB	Download Add to cart Publish
Offline Win SPW Installation Package win_spw-2.1.0.51-isebundle.zip	31-MAY-2016	1.80 MB	Download

ISE Posture Deployment- Provisioning

- **Agent**

NAC install agent - for managed clients, Persistent Agent
NAC web agent - for unmanaged guest client, Temporary Agent
Anyconnect client

- **Compliance module**

The compliance module contains a list of fields, such as vendor name, product version, product name, and attributes provided by OPSWAT that supports Cisco ISE posture conditions.

Vendors frequently update the product version and date in the definition files, therefore, you must look for the latest version and date in the definition files for each vendor product by frequently polling the compliance module for updates.

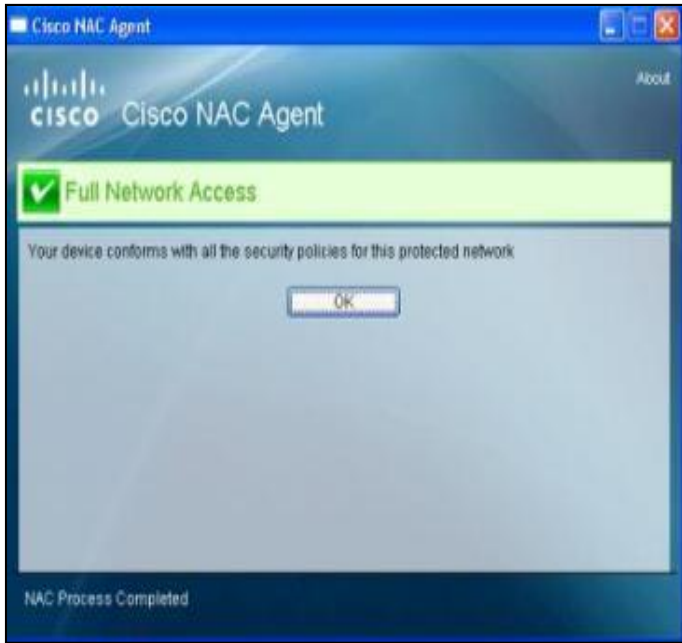
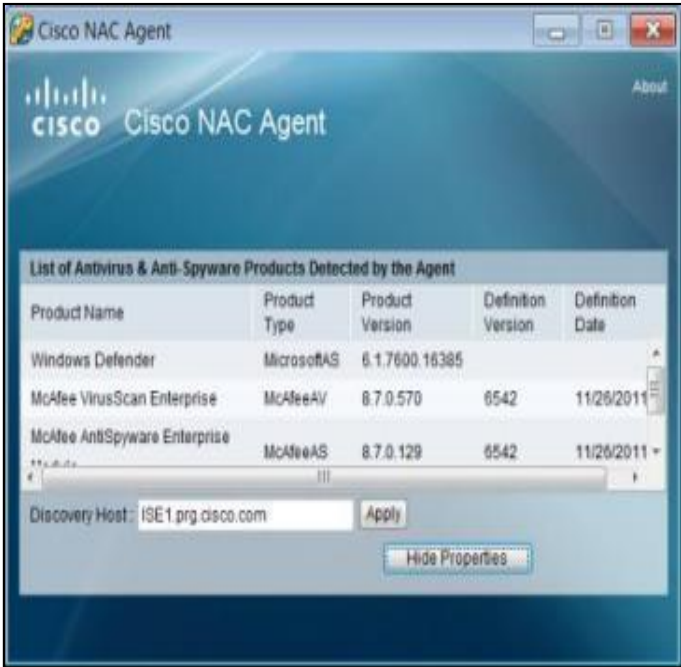
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/ac_compliance_module/m_ac_av_as_pm_de_3_6_10146_2.pdf

- **NAC Agent or AnyConnect Posure Profile**

Provision NAC Agent

- Windows or MAC

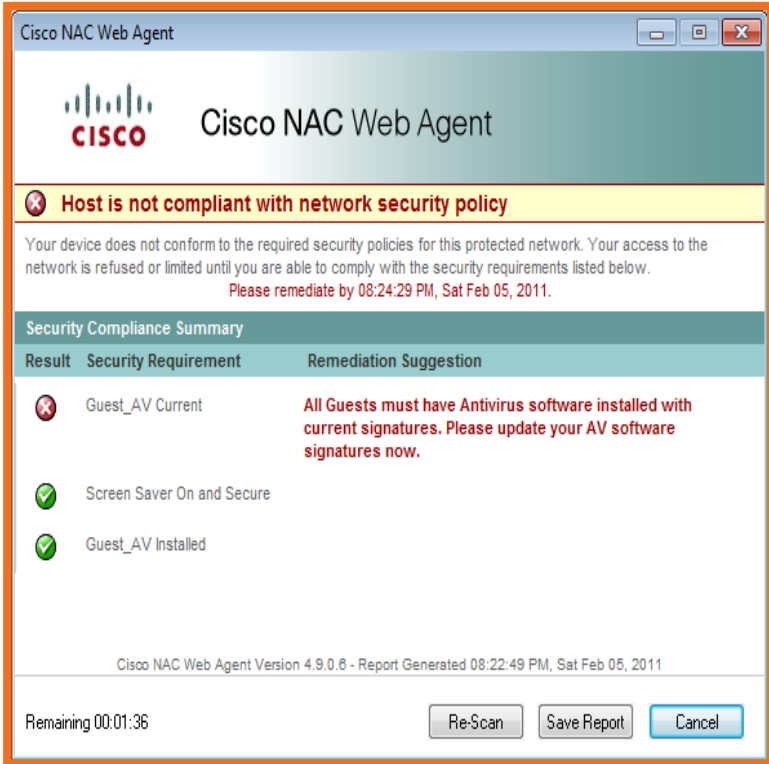
Typical Use Case:
Managed Devices



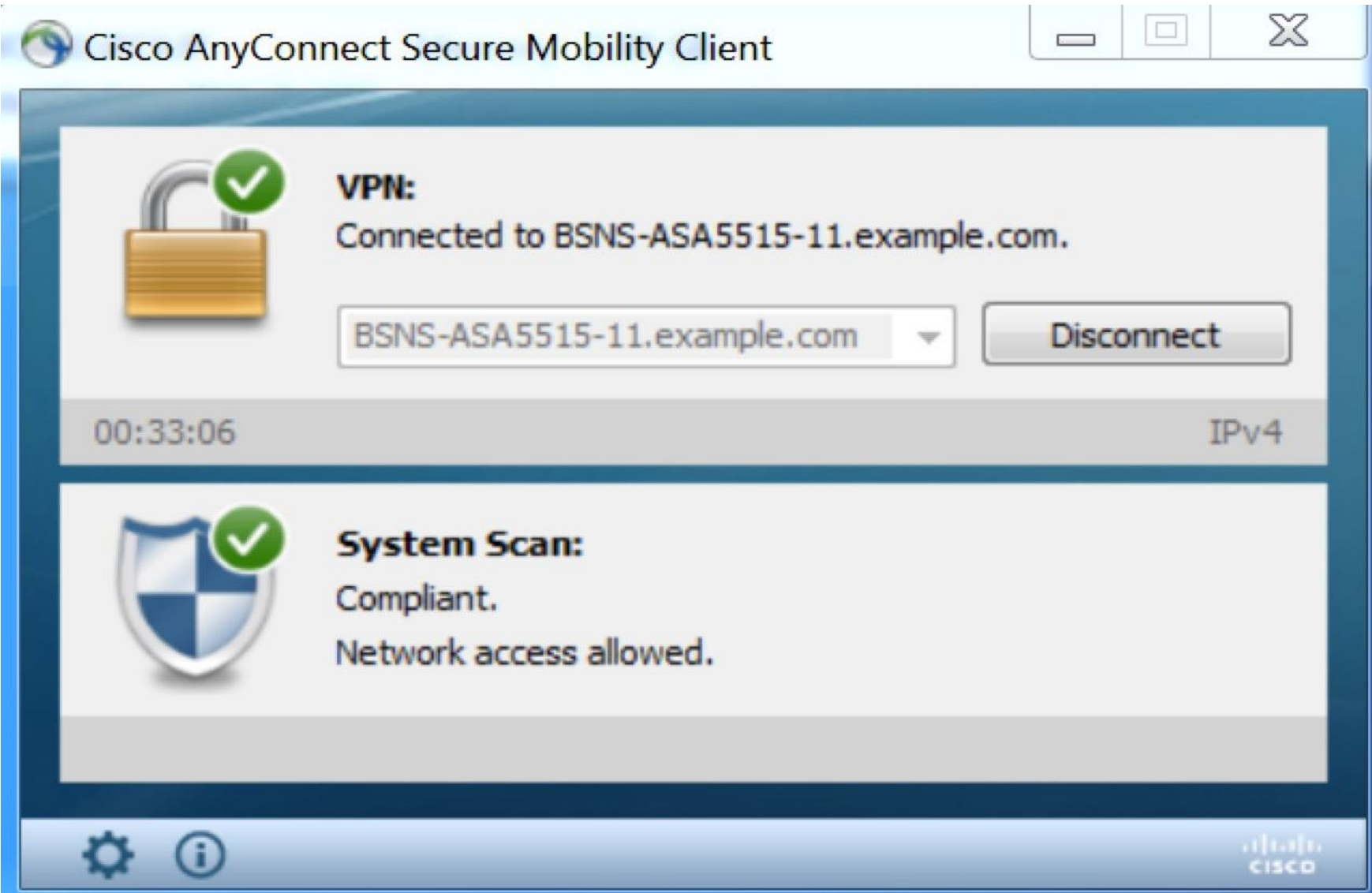
Provision NAC Agent



Typical Use Case:
Unmanaged PCs,
Guests, Contractors



Provision Anyconnect agent



Provisioning Policy

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
<input checked="" type="checkbox"/> Windows_NAC_Install	If Any	and Windows All	and YIN:ExternalGroups EQUALS ...	then NACAgent 4...
<input checked="" type="checkbox"/> Windows_NAC_Web	If Any			
<input checked="" type="checkbox"/> MAC OS	If Any			
<input checked="" type="checkbox"/> Chromebook	If Any			

Agent Configuration

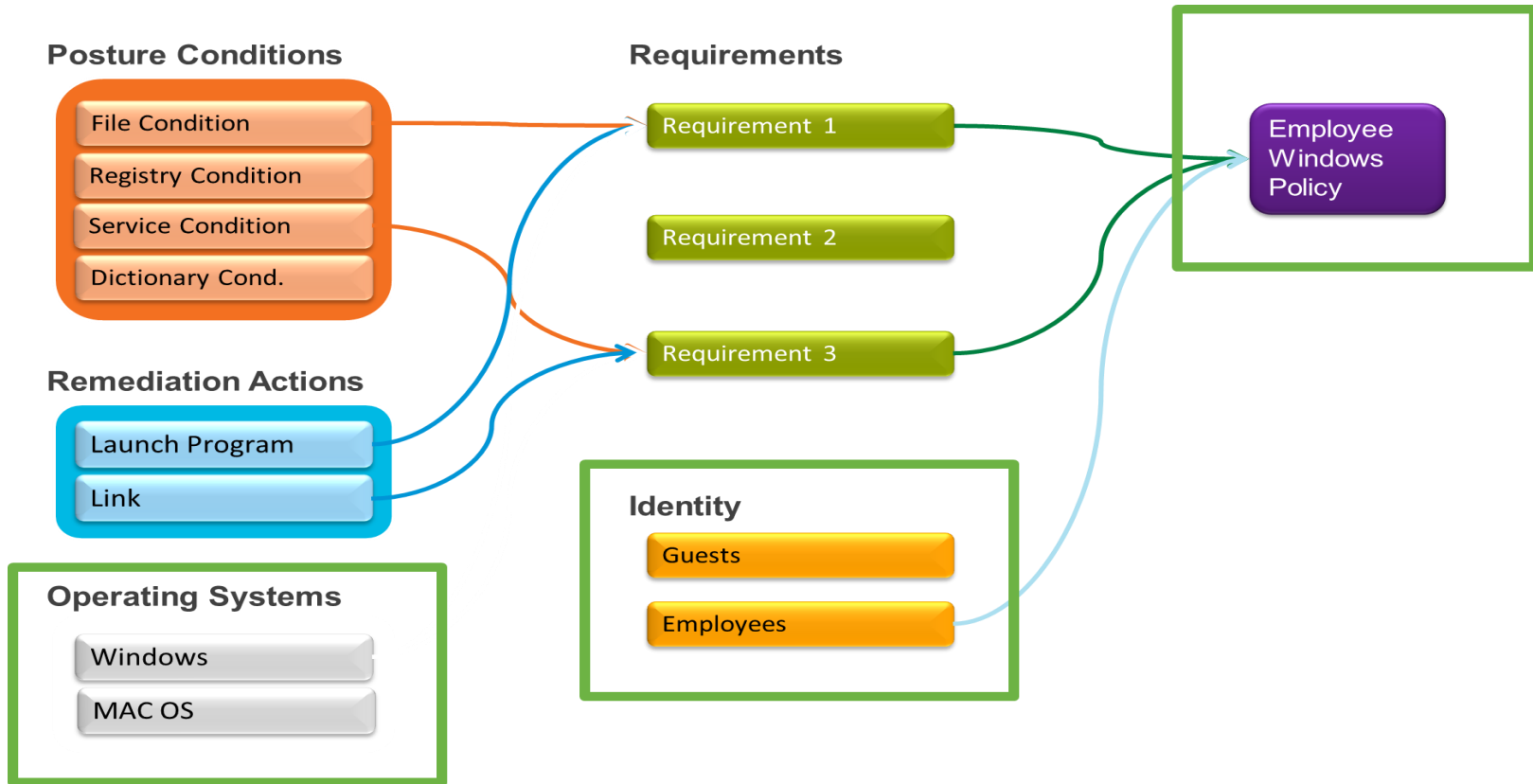
Agent:	NACAgent 4.9.5.8	<input checked="" type="checkbox"/> Is Upgrade Mandatory
Profile:	nacxml	
Compliance Module:	ComplianceModule 3.6.10591.2	
Agent Customization Package:	Choose a Customization Package	

Native Sunnlicant Configuration

Posture Policy Compents

NAC Appliance	Description	ISE – NEW
Checks	File, Service, Registry, AV/AS checks	Posture Conditions
Rules	Multiple simple conditions are built together	Compound Posture Conditions
Requirements	Requirements are used with <u>Operating Systems</u> . They contain compound conditions. Each Requirement has a selected <u>Remediation action</u> .	Posture Requirements
Role Requirements	Posture policies can be evaluated based on <u>Identity Groups, OS and dictionary attributes</u> . Policies contain the Requirements	Posture Policy

Posture Policy Logic



Unknown:

-No data was collected in order to determine posture state.

Noncompliant:

- A posture assessment was performed, and one or more requirements failed.

Compliant:

- The endpoint is compliant with all mandatory requirements.

Posture status & Authorization

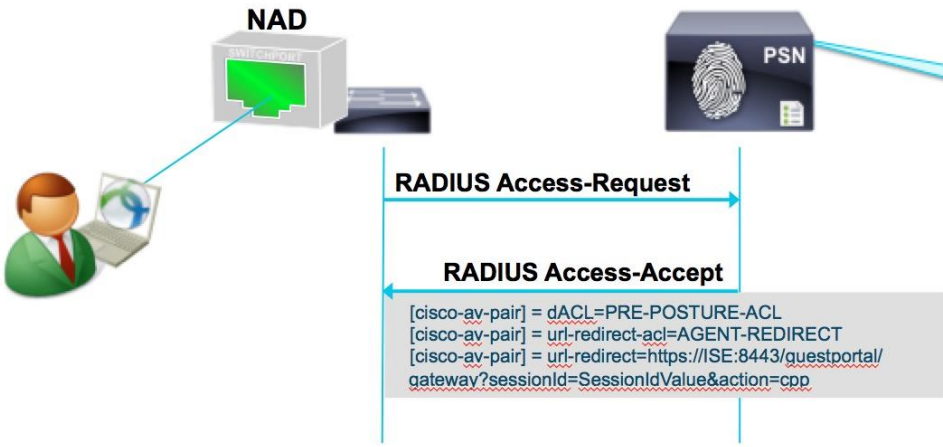
AGENT-REDIRECT (local to Switch)

```
ip access-list extended AGENT-REDIRECT
deny  udp any any eq domain
permit tcp any any eq www
```

PRE-POSTURE-ACL (downloaded)

```
permit udp any any eq domain
permit icmp any any
permit tcp any host 10.1.1.3 eq 8443
permit tcp any host 10.1.1.3 eq 8905
permit udp any host 10.1.1.3 eq 8905
permit tcp any any eq 80
permit tcp any any eq 443
```

Rule Name	Conditions	Permissions
IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phone
Employee_NoCompliant	if Employee & Posture != Compliant	then Posture
Employee	if Employee & Posture = Compliant	then Employee
GUEST	if GUEST	then GUEST
Default	If no matches, then	WEBAUTH

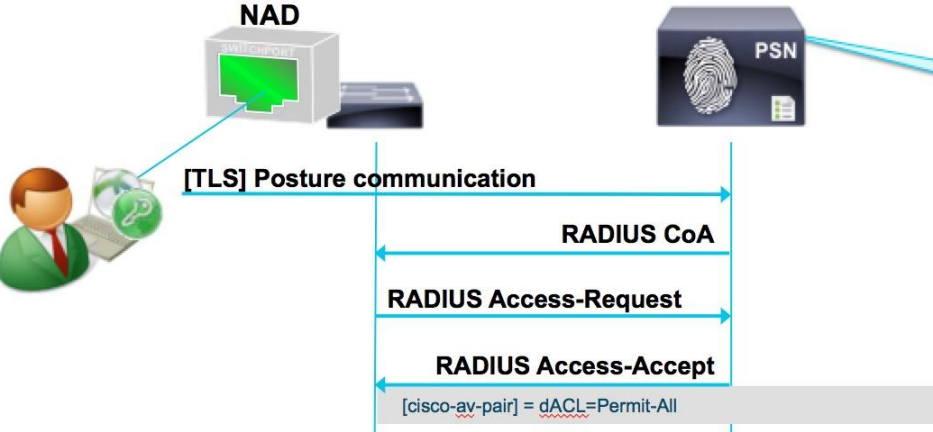


Matched Rule = Employee_NoCompliant

Posture status & Authorization

```
Permit-All (downloaded ACL)
permit ip host any
```

Rule Name	Conditions	Permissions
IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phone
Employee_NoCompliant	if Employee & Posture != Compliant	then Posture
Employee	if Employee & Posture = Compliant	then Employee
GUEST	if GUEST	then GUEST
Default	If no matches, then	WEBAUTH



Matched Rule = Employee

Posture Condition

User defined

Cisco Pre defined

▼ Posture

Anti-Malware Condition

Anti-Spyware Condition

Anti-Virus Condition

Application Condition

Compound Condition

Disk Encryption Condition

File Condition

Patch Management Condition

Registry Condition

Service Condition

USB Condition

Dictionary Simple Condition

Dictionary Compound Condition

Posture Condition Example- Av install

Anti-virus Conditions List > **symantec_av_install**

Anti-Virus Condition

* Name

Description

Compliance Module 3.x or earlier ⓘ

* Operating System +

Vendor ⌵

Check Type Installation Definition

▼ Products for Selected Vendor

	Product Name ▼	Version	Remediation Support	Definition Check	Latest Definition Date	Latest Definition Version
<input type="checkbox"/>	Symantec unknown product	x	NO	YES	06/08/2016	6/8/2016 rev. 81
<input type="checkbox"/>	Symantec Scan Engine	5.x	NO	YES	06/08/2016	6/8/2016 rev. 81
<input type="checkbox"/>	Symantec Hosted Endpoint Prot...	2.x	YES	YES	10/26/2011	10/26/2011 rev. 2
<input type="checkbox"/>	Symantec Endpoint Protection fo...	89.x	YES	YES	10/26/2011	10/26/2011 rev. 2
<input type="checkbox"/>	Symantec Endpoint Protection A...	5.x	NO	YES	10/26/2011	
<input checked="" type="checkbox"/>	Symantec Endpoint Protection	12.1.x	YES	YES	06/08/2016	6/8/2016 rev. 81
<input checked="" type="checkbox"/>	Symantec Endpoint Protection	12.x	YES	YES	06/08/2016	6/8/2016 rev. 81
<input checked="" type="checkbox"/>	Symantec Endpoint Protection	11.x	YES	YES	06/08/2016	6/8/2016 rev. 81

Posture Condition Example- Running Process

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Authorization

Profiling

Posture

- Anti-Malware Condition
- Anti-Spyware Condition
- Anti-Virus Condition
- Application Condition**
- Compound Condition

Application Conditions List > cmd

Application Condition

* Name: cmd

Description: cmd process running or not

* Operating System: Windows All

Compliance Module: Any version

*** Process Name: cmd.exe**

Application Operator: Running

Save Reset

Posture Condition Example- File exist

File Conditions List > **1txtfile_exist_diskc**

File Condition

* Name

Description

* Operating System 

Compliance Module Any version

* File Type 

* File Path

* File Operator

Save

Reset

Posture Condition Example- USB storage

Dictionarys ▾ Conditions ▸ Results

- Authentication
- Authorization
- Profiling
- Posture**
 - Anti-Malware Condition
 - Anti-Spyware Condition
 - Anti-Virus Condition
 - Application Condition
 - Compound Condition
 - Disk Encryption Condition
 - File Condition
 - Patch Management Condition
 - Registry Condition
 - Service Condition
 - USB Condition**
 - Dictionary Simple Condition
 - Dictionary Compound Condition

Name USB_Check
Description Cisco Predefined Check: Checks if USB mass storage device is connected.

Operating System Windows All

Compliance Module 4.x or later ⓘ

Binding Multiple Condition-Compound

Compound Conditions List > **2rules**

Compound Condition

* Name

Description

* Operating System 

Compliance Module Any version

Select a condition to insert below  () ! & |

&

Validate Expression

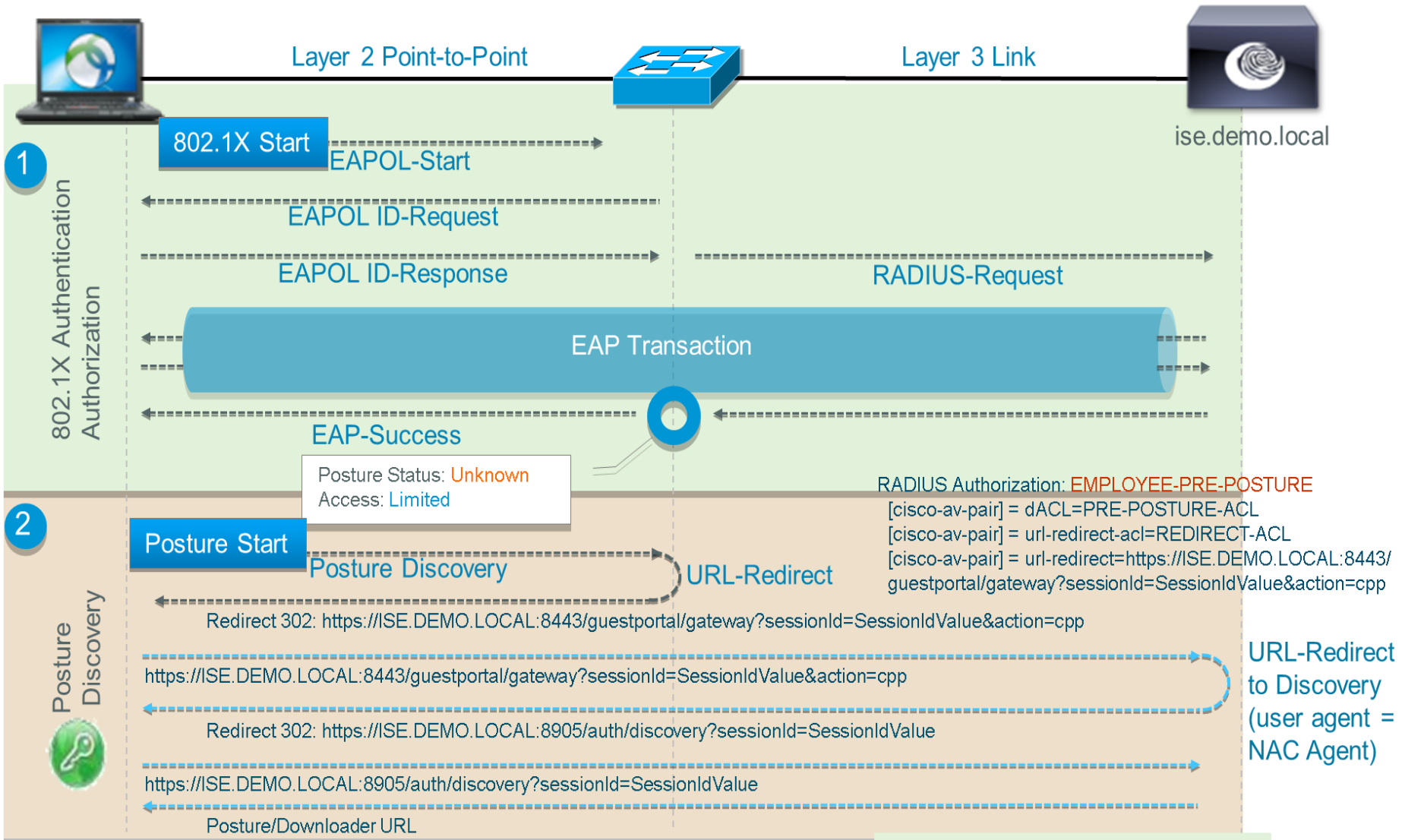
Posture Policy

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

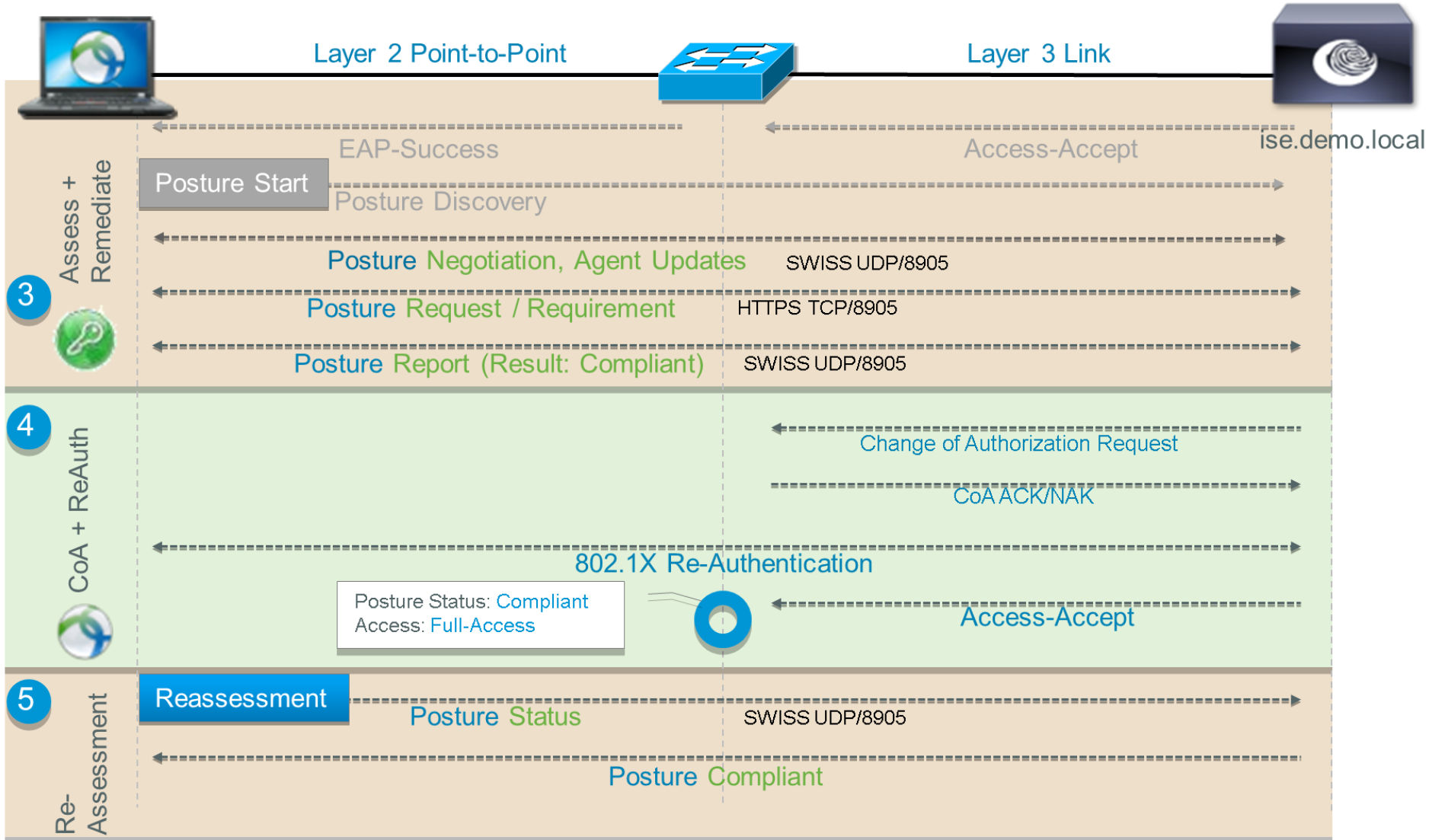
Status	Rule Name	Identity Groups	Operating Systems	Compliance Module	Other Conditions	Requirements
✓	USB BLOCK	If Any	and Windows All	and 4.x or later	and YIN:ExternalGroups EQUALS yin.local/Users/Domain Users	then USB_Block
✓	cmd process running	If Any	and Windows All	and Any version	and YIN:ExternalGroups EQUALS yin.local/Users/Domain Users	then cmd_running
✓	cmd_and_txt	If Any	and Windows All	and Any version	and	then cmd_and_txt

802.1X Posture Work-Flow

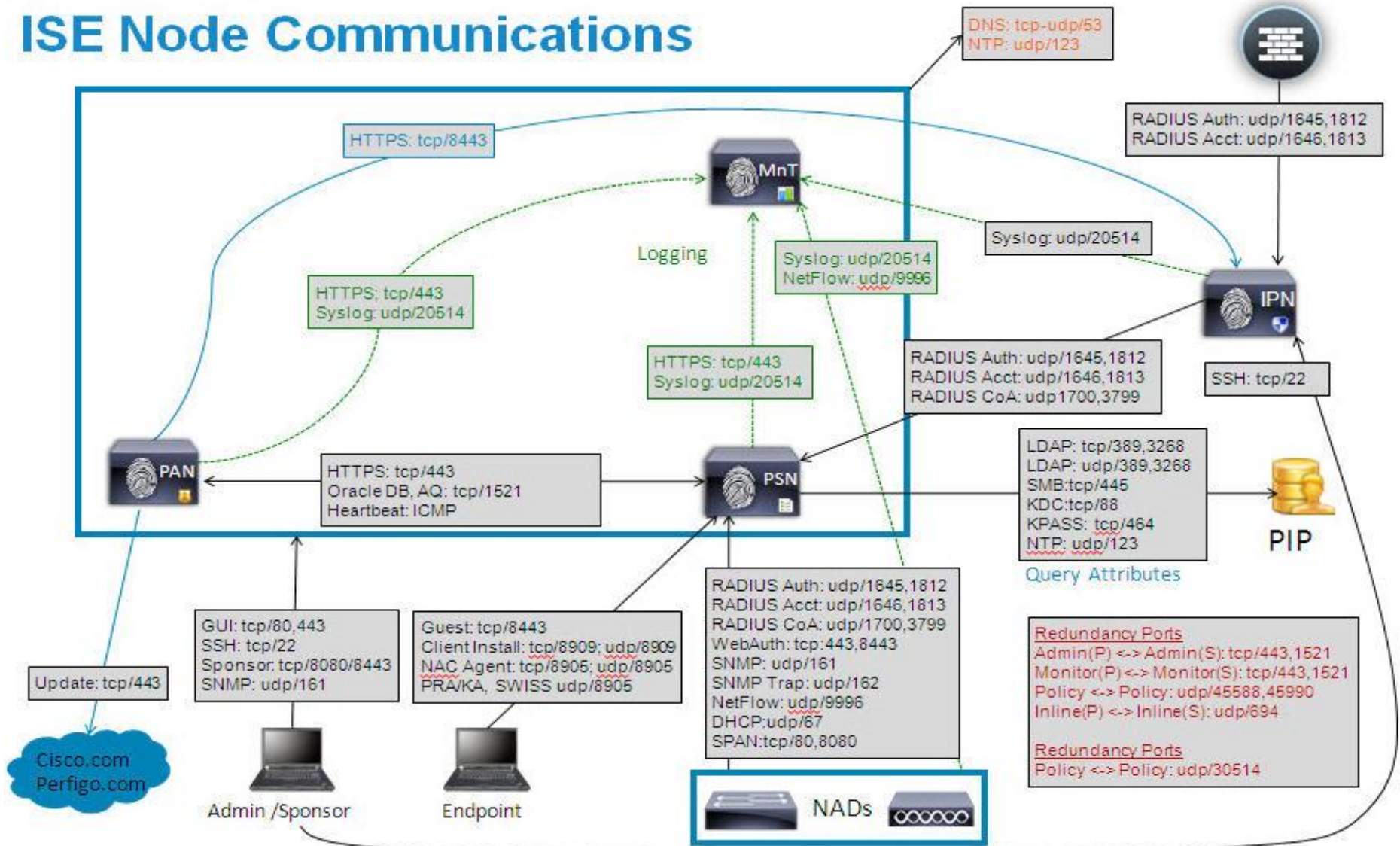


Flow continues to next slide

802.1X Posture Work-Flow



ISE Node Communications



ISE Troubleshooting

- What to do on ISE?
- What to do on NAS? - switch
- What to do on Client?

What to do on ISE - Radius live logs

[RADIUS](#)
[TC-NAC Live Logs](#)
[TACACS](#)
[Reports](#)
[Troubleshoot](#)
[Adaptive Network Control](#)

[Live Logs](#)
[Live Sessions](#)

[Refresh](#)
[Reset Repeat Counts](#)
[Export To](#)

Time	Status	Details	Identity	Endpoint ID	Authorization Policy	Authorization...	Posture Status
Jun 15, 2016 02:33:03.277 PM			u11	00:50:56:B1:3A:AD	Default >> Success-Posture	PermitAccess	Compliant
Jun 15, 2016 02:33:02.954 PM			u11	00:50:56:B1:3A:AD	Default >> Success-Posture	PermitAccess	Compliant
Jun 15, 2016 02:33:02.881 PM				00:50:56:B1:3A:AD			Compliant
Jun 15, 2016 02:30:14.076 PM			u11	00:50:56:B1:3A:AD	Default >> Unknown-Posture-switch	Posture-Rule	Pending
Jun 15, 2016 02:29:30.831 PM			#ACSACL#-IP-DACL-575d1c				
Jun 15, 2016 02:29:30.571 PM			00:50:56:B1:3A:AD	00:50:56:B1:3A:AD	Default >> Unknown-Posture-switch	Posture-Rule	Pending

What to do on ISE – Radius live session logs

▼ RADIUS TC-NAC Live Logs ▶ TACACS Reports ▶ Troubleshoot ▶ Adaptive Network Control

Live Logs Live Sessions

Refresh Every 1 minute Show Latest 20 records Within All

Refresh Export To Filter

Initiated	Updated	Session Status	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture Status	Security G
Jun 19, 2016 01:28:...	Jun 19, 2016 01:28:4...	Started	00:50:56:B1:3A:AD	u11	10.75.61.211	Windows7-Workstation	Compliant	
Timestamp	Event	Identity	IP Address	Posture Status	Auth Method			
2016-06-19 13:28:42.865	Authentication succeeded	u11	10.75.61.211	Compliant	dot1x			
2016-06-19 13:28:42.815	Dynamic Authorization succeeded			Compliant				
2016-06-19 13:26:05.374	RADIUS Accounting start request	u11	10.75.61.211					
2016-06-19 13:26:04.898	Authentication succeeded	u11	10.75.61.211	Pending	dot1x			
Jun 19, 2016 01:24:...	Jun 19, 2016 01:24:3...	Started	00:00:00:00:00:03	00:00:00:00:00:03	Windows7-Workstation	Pending		
Jun 18, 2016 03:31:...	Jun 19, 2016 01:24:3...	Started	00:50:56:B1:4D:C3	00:50:56:B1:4D:C3	10.75.61.208	Windows7-Workstation	Pending	

What to do on ISE – Session ID & CoA

Authentication Details

Source Timestamp 2016-06-19 13:28:42.582

Received Timestamp 2016-06-19 13:28:42.815

Policy Server ISE210

Event 5205 Dynamic Authorization succeeded

Endpoint Id 00:50:56:B1:3A:AD

Calling Station Id 00-50-56-B1-3A-AD

Audit Session Id 0A4B3DCE0000005932CB8E19

Network Device 3560switch

What to do on ISE – Session ID & CoA

```
3560-security-8F#show auth sessions
```

Interface	MAC Address	Method	Domain	Status	Session ID
Fa0/9	0000.0000.0003	mab	DATA	Authz Success	0A4B3DCE0000005732CA78AF
Fa0/9	0050.56b1.4dc3	mab	DATA	Authz Success	0A4B3DCE0000005632CA75EE
Fa0/9	0050.56b1.3aad	dot1x	DATA	Authz Success	0A4B3DCE0000005932CB8E19

```
-----  
Interface: FastEthernet0/9  
MAC Address: 0050.56b1.3aad  
IP Address: 10.75.61.211  
User-Name: ull  
Status: Authz Success  
Domain: DATA  
Security Policy: Should Secure  
Security Status: Unsecure  
Oper host mode: multi-auth  
Oper control dir: both  
Authorized By: Authentication Server  
  
Vlan Group: N/A  
ACS ACL: xACSACLx-IP-DACL-5762a70c  
URL Redirect ACL: red  
URL Redirect: https://ISE210.yin.local:8443/portal/gateway?sessionId=0A4B3DCE0000005932CB8E19&  
portal=a6bb0db0-2230-11e6-99ab-005056bf55e0&...  
Session timeout: N/A  
Idle timeout: N/A  
Common Session ID: 0A4B3DCE0000005932CB8E19  
Acct Session ID: 0x00000091  
Handle: 0x32000059  
  
Runnable methods list:  
Method State  
mab Not run  
dot1x Authc Success
```

What to do on ISE – Session ID & CoA



- Session is created when NAD sends RADIUS authentication request to the RADIUS server
- Used for correlation of events
- Used for Change of Authorization (CoA)
- Depends on time

What to do on ISE

Check & review Posture Result with “Report” tools

- Operations---Report---ISE Reports---Endpoint & Users---client provisioning

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows the 'Report Selector' with 'ISE Reports' expanded to show 'Audit', 'Device Administration', and 'Diagnostics'. Under 'Endpoints and Users', 'Client Provisioning' is selected, with a 'Time Range' filter set to 'Last 7 Days'. The main content area shows a table of 'Client Provisioning' events from 06/09/2016 to 06/15/2016. The table has columns for 'Logged At', 'Server', 'Event', 'Identity', 'Endpoint ID', 'IP Address', and 'Client Provisioning Policy'. Several rows are highlighted with red boxes, indicating specific events of interest.

Logged At	Server	Event	Identity	Endpoint ID	IP Address	Client Provisioning Policy
2016-06-15 16:08:16.294	ISE210	Client provisioning succeeded	u22	00:50:56:B1:36:30	10.75.61.212	Windows_NAC_Web
2016-06-15 16:03:26.55	ISE210	Client provisioning succeeded	u22	00:50:56:B1:36:30	10.75.61.212	Windows_NAC_Web
2016-06-15 16:02:56.138	ISE210	Client provisioning succeeded	u22	00:50:56:B1:36:30	10.75.61.212	Windows_NAC_Web
2016-06-15 15:59:53.004	ISE210	Client provisioning succeeded	u22	00:50:56:B1:36:30	10.75.61.212	Windows_NAC_Web
2016-06-15 14:32:02.128	ISE210	Client provisioning succeeded	u11	00:50:56:B1:3A:AD	10.75.61.211	Windows_NAC_Install
2016-06-15 14:30:32.362	ISE210	Client provisioning succeeded	u11	00:50:56:B1:3A:AD	10.75.61.211	Windows_NAC_Install
2016-06-14 12:35:26.478	ISE210	Client provisioning succeeded	u22	00:50:56:B1:36:30	10.75.61.212	Windows_NAC_Web
2016-06-14 08:43:14.462	ISE210	Client provisioning succeeded	u33	00:50:56:B1:4D:C3	10.75.61.208	anyconnect
2016-06-14 07:40:39.395	ISE210	Client provisioning succeeded	u33	00:50:56:90:5F:D7	10.75.61.208	anyconnect
2016-06-14 07:29:24.467	ISE210	Client provisioning succeeded	u22	00:50:56:90:5F:D7	10.75.61.208	Windows_NAC_Web
2016-06-14 07:23:18.359	ISE210	Client provisioning succeeded	u33	00:50:56:90:5F:D7	10.75.61.208	anyconnect
2016-06-14 07:13:05.502	ISE210	Client provisioning succeeded	u22	00:50:56:B1:36:30	10.75.61.212	Windows_NAC_Web
2016-06-14 06:57:05.344	ISE210	Client provisioning succeeded	u11	00:50:56:B1:3A:AD	10.75.61.211	Windows_NAC_Install

What to do on ISE

Check Posture Result with “Posture Troubleshooting” tools

- Operations---Troubleshoot---Diagnostic Tools---Posture Troubleshooting

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Operations' menu is expanded to show 'RADIUS', 'TC-NAC Live Logs', 'TACACS', 'Reports', 'Troubleshoot', and 'Adaptive Network Control'. The 'Troubleshoot' menu is further expanded to show 'Diagnostic Tools' and 'Download Logs'. The left sidebar contains 'General Tools' (RADIUS Authentication Troubleshooting, Execute Network Device Command, Evaluate Configuration Validator, Posture Troubleshooting, EndPoint Debug, TCP Dump) and 'TrustSec Tools'. The main content area is titled 'Diagnosis and Resolution' and shows the results of a posture check for Mac Address 00:50:56:B1:3A:AD. The posture policy 'cmd process running' has passed. A table lists requirements, status, and remediations. The 'Resolution' section indicates no applicable steps are available. A 'Troubleshooting Summary' section shows a checked posture record with details: Timestamp (2016-06-15 14:33:00.234), MAC Address (00:50:56:B1:3A:AD), Username (u11), Operating System (Windows 7 Ultimate 64-bit), Status (Compliant), and Failure Reason.

Diagnosis and Resolution

Diagnosis

Details of policy(s) for Mac Address - 00:50:56:B1:3A:AD
Posture policy - **cmd process running** - has Passed
Here is the list of requirements that failed and associated conditions, also the remediations that can be applied

Requirements	Status	Passed Conditions	Failed Conditions	Skipped Conditions	Remediations
cmd_running[Mandatory]	Passed	cmd_is_runnin	None	None	Message Text Only(Predefined message text only)

Resolution

No applicable resolution steps available.

Troubleshooting Summary

✓ Investigated posture record with following details:

Details

Timestamp	2016-06-15 14:33:00.234
MAC Address	00:50:56:B1:3A:AD
Username	u11
Operating System	Windows 7 Ultimate 64-bit
Status	Compliant
Failure Reason	

Show Progress Details Done

What to do on ISE

Check & review Posture Result with “Report” tools

- Operations---Report---ISE Reports---Endpoint & Users
- “Posture Assessment by Condition”
- “Posture Assessment by Endpoint”

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar contains a 'Report Selector' with 'ISE Reports' highlighted. Under 'ISE Reports', 'Posture Assessment by Condition' and 'Posture Assessment by Endpoint' are listed, with 'Posture Assessment by Endpoint' selected. The main content area displays the report title 'Posture Assessment by Endpoint' and a time range 'From 06/15/2016 12:00:00.000 AM to 06/15/2016 04:09:21.754 PM'. A table below shows the report data with columns: Logged At, Status, Details, PRA Action, Identit, Endpoint ID, IP Address, Endpoint OS, and Agent. Two rows are visible, both highlighted with a red border. The first row shows a failed assessment (red X) for user 'u22' on 2016-06-15 at 16:08:56.957. The second row shows a successful assessment (green checkmark) for user 'u11' on 2016-06-15 at 14:33:00.234. The bottom left of the interface has a 'Filters' section with a 'Time Range' dropdown set to 'Today' and a 'Run' button.

Logged At	Status	Details	PRA Action	Identit	Endpoint ID	IP Address	Endpoint OS	Agent
2016-06-15 16:08:56.957	✘		N/A	u22	00:50:56:B1:36:30	10.75.61.212	Windows 7 Ultim	Cisco NAC Web Agent for Windows 4.9.5.7
2016-06-15 14:33:00.234	✔		N/A	u11	00:50:56:B1:3A:AD	10.75.61.211	Windows 7 Ultim	Cisco NAC Agent for Windows 4.9.5.8

What to do on ISE

Adjust specified ISE log to “**Trace**” level?

Administration---system---logging---Debug Log Configuration
**posture & provision & swiss
runtime-AAA**

Operations---Troubleshoot---Download Logs
**ise-psc.log
prrt-management.log**
(choose the log with the fresh timestamp)

What to do on ISE

=====lse-psc.log=====

2016-06-15 14:32:10,869 DEBUG [**portal-http-service85**][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -::::

- receiving request from client 00:50:56:B1:3A:AD 10.75.61.211

2016-06-15 14:32:12,129 DEBUG [portal-http-service85][[] cisco.cpm.posture.runtime.PostureHandlerImpl

- NAC agent xml <?xml version="1.0" encoding="UTF-8"?><cleanmachines>

<version>2</version>

<encryption>0</encryption>

<package>

<id>10</id>

<name>cmd_running</name>

<version/>

<description>cmd is running</description>

<type>3</type>

<optional>0</optional>

<action>3</action>

<check>

<id>cmd_is_running</id>

<category>4</category>

<type>401</type>

<param>cmd.exe</param>

<operation>running</operation>

</check>

<criteria>(cmd_is_running)</criteria>

</package>

</cleanmachines>

What to do on ISE

=====lse-psc.log=====

2016-06-15 14:33:00,120 DEBUG [**portal-http-service86**] cisco.cpm.posture.runtime.PostureHandlerImpl

-::- receiving request from client 00:50:56:B1:3A:AD 10.75.61.211

- **Decoding Swiss request**, decrypted buffer, Operation = 17
- SwissData type: 1 and Data: 0A4B3DCE000000341E6C7F99
- receiving request from client 00:50:56:B1:3A:AD 10.75.61.211
- Received posture request [parameters: reqtype=report, userip=10.75.61.211, clientmac=00-50-56-B1-3A-AD,
- **Decrypting report**
- **Decrypted report**
- Increase MnT counter at POSTURE:**Posture.Requirement.Success**.cmd_running
- Increase MnT counter at POSTURE:**Posture.SimpleCondition.Success**.cmd_is_running
- Increase MnT counter at POSTURE:**Posture.Policy.Success**.cmd process running
- Posture report token for **endpoint mac 00-50-56-B1-3A-AD is Healthy**
- **Posture state is compliant** for endpoint with mac 00-50-56-B1-3A-AD
- entering triggerPostureCoAfor session 0A4B3DCE000000341E6C7F99
- Posture CoA is scheduled for session id [0A4B3DCE000000341E6C7F99]

What to do on Switch?

Switch#Show auth session int fastethernet 0/9

```
-----  
      Interface: FastEthernet0/9  
      MAC Address: 0050.56b1.3aad  
      IP Address: 10.75.61.211  
      User-Name: u11  
      Status: Authz Success  
      Domain: DATA  
      Security Policy: Should Secure  
      Security Status: Unsecure  
      Oper host mode: multi-auth  
      Oper control dir: both  
      Authorized By: Authentication Server  
  
      Vlan Group: N/A  
      ACS ACL: xACSACLx-IP-DACL-575d1c58  
      URL Redirect ACL: red  
      URL Redirect:  
https://ISE210.yin.local:8443/portal/gateway?sessionId=0A4B3DCE000000372345460A&portal=a6bb0db0-2230-11e6-99ab-005056bf55e0&action=cpp&token=1e79fb3b1861ce546ee0d92e029b57e0  
      Session timeout: N/A  
      Idle timeout: N/A  
      Common Session ID: 0A4B3DCE000000372345460A  
      Acct Session ID: 0x00000061  
      Handle: 0xA4000037  
  
Runnable methods list:  
  Method  State  
  mab     Not run  
  dot1x   Authc Success
```

What to do on switch? – Redirect & Download ACL

Redirect ACL – On Switch

```
ip access-list extended red
deny udp any any eq bootp
deny udp any any eq domain
permit tcp any any eq www
permit tcp any any eq 443
```

```
3560-security-8F#show access-lists
Extended IP access list red
 10 deny udp any any eq domain (1781 matches)
 30 permit tcp any any eq www (330 matches)
 40 permit tcp any any eq 443
```

Download ACL – On Switch

Downloadable ACL List > **DACL**

Downloadable ACL

```
Extended IP access list xACSACLx-IP-DACL-5762a70c (per-user)
 10 permit ip any host 10.75.179.210
 20 permit ip any host 10.75.179.100
 30 permit ip any host 10.75.179.211
 40 permit udp any any
 50 permit icmp any any
```

* Name

Description

* DACL Content	1234567	permit ip any host 10.75.179.210
	8910111	permit ip any host 10.75.179.100
	2131415	permit ip any host 10.75.179.211
	1617181	permit udp any any
	9202122	permit icmp any any
	2324252	

What to do on switch?

3560-security-8F#show debug

AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Radius debugs debugging is on

3560-security-8F#**test aaa group radius u11 cisco new-code**

User successfully authenticated

*Mar 9 13:12:14.907: %AUTHMGR-5-START:

Starting 'dot1x' for client (0050.56b1.3aad) on Interface Fa0/9 AuditSessionID 0A4B3DCE000000452C081FC0

*Mar 9 13:12:25.150: %AUTHMGR-7-RESULT:

Authentication result 'success' from 'dot1x' for client (0050.56b1.3aad) on Interface Fa0/9 AuditSessionID 0A4B3DCE000000452C081FC0

*Mar 9 13:12:26.047: %AUTHMGR-5-SUCCESS:

Authorization succeeded for client (0050.56b1.3aad) on Interface Fa0/9 AuditSessionID 0A4B3DCE000000452C081FC0

What to do on switch?

Enable change of authorization (CoA)

```
C3750X(config)#aaa server radius dynamic-author
```

```
C3750X(config-locsvr-da-radius)#client use _ip_address server-key shared_secret
```

Enable Download ACL Support

```
C3750X(config)#ip device tracking
```

Enable http traffic redirect support

```
C3750X(config)#ip http server
```

```
C3750X(config)#ip http secure-server
```


What to do on client? – Important Checklist

DNS

- ISE Fully Qualified Domain Name (FQDN) must be resolvable by the client

Browser

- Active X (Allow)
- Java Plugin (Firefox or Chrome)
- Compatibility Mode (IE 10 later, Add ISE IP or FQDN to site list)
- Import ISE certificates to Trust list

Port & Firewall or ACL

TCP 8905:

Used for posture communication between NAC Agent and ISE (Swiss port).

Used for client provisioning.

TCP 8443:

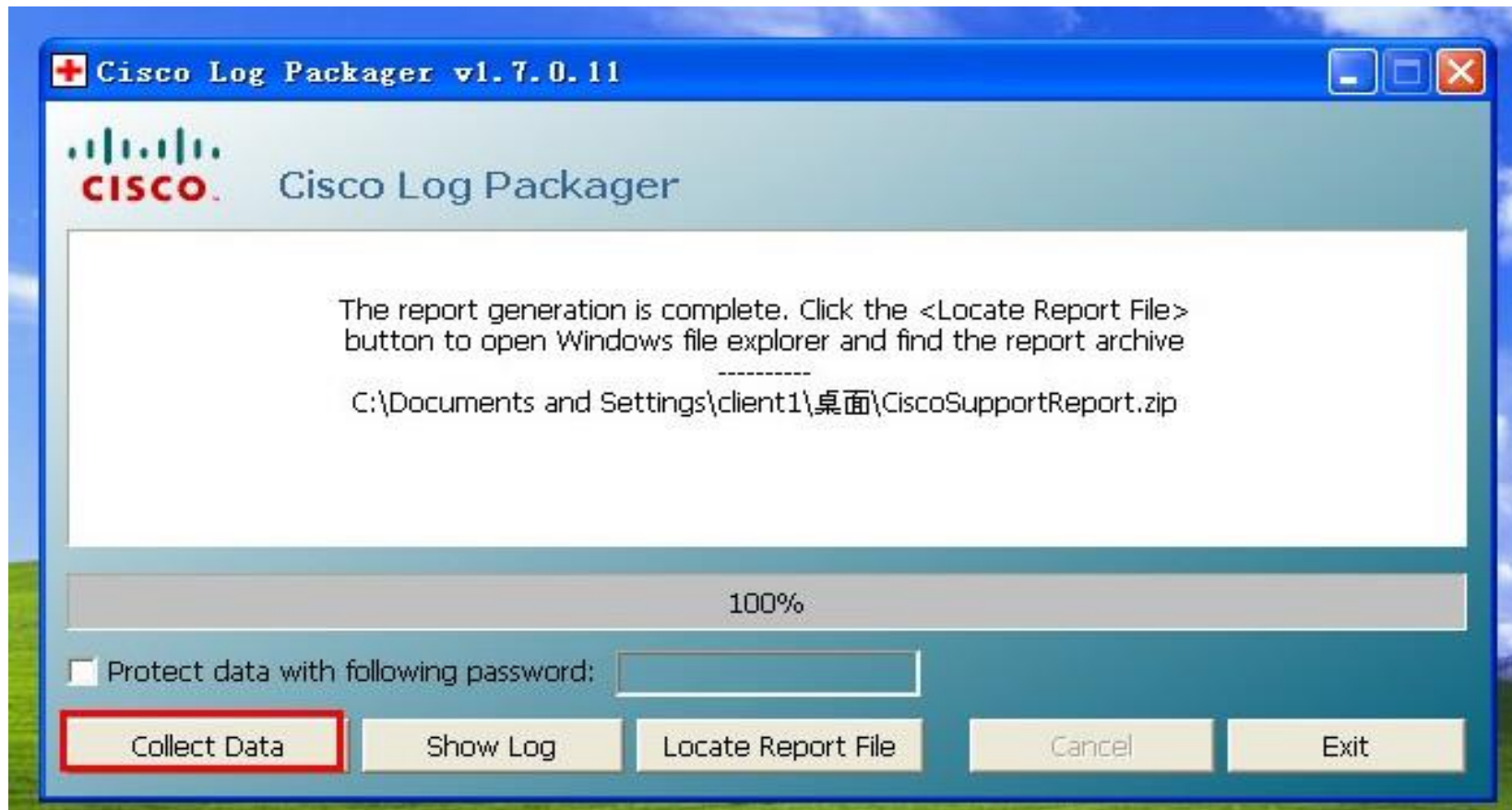
Used for guest and posture discovery.

If no discovery host is defined: The NAC Agent sends HTTP request on port 80 to the gateway; this traffic must be redirected to the posture discovery link (CPP) in order for discovery to work properly.

If a discovery host is defined: The NAC Agent sends HTTP request on port 80 to the host; this traffic must be redirected to the posture discovery link (CPP) in order for discovery to work properly. If there is a problem with redirection, the NAC Agent tries to directly contact the discovery host defined on port 8905;

What to do on client? – Nac Client Package

Program→CISCO→Client utilities→Cisco Log packager



What to do on client? – Nac Client Decode

Using CAM “support logs tool” to decode



Cisco Clean Access Standard Manager Version 4.9.3

Administration > Clean Access Manager

Network | Failover | System Time | SSL | Software Upload | Licensing | Policy Sync | **Support Logs** | Agent Logs

Agent Logs:

Upload

Created On	Name	Preview	Download	Delete
03/08/14 17:18:47	NACAgentLogCurrent.log	Preview		

```
--- START OF DECODE ---
1: PC210: Mar 8 2014 09:12:37.140 UTC: %NACAGENT-6-APP_VER: %[ver=4.9.0.52][os]=: NAC Agent version 4.9.0.52 st
2: PC210: Mar 8 2014 09:12:37.187 UTC: %NACAGENT-7-IPRR_DEBUG: %[sev=debug][func=IPConfigHandler::initialize]:
Config Module.
3: PC210: Mar 8 2014 09:12:37.703 UTC: %NACAGENT-6-MINIDUMP: %[sev=info][func=CExceptionHandlerEx::CExceptionHandler
MiniDump is enabled - will save 2 dumpfiles
4: PC210: Mar 8 2014 09:12:37.734 UTC: %NACAGENT-6-IPC: %[func=IpcServer::internalInitialize]: IPC server on po
listening on new connection
5: PC210: Mar 8 2014 09:12:37.750 UTC: %NACAGENT-7-REG_INFO: %[sev=debug][func=REG_SaveVolatiledWORD]: Key alre
SOFTWARE\Cisco\Cisco NAC Agent
6: PC210: Mar 8 2014 09:12:37.750 UTC: %NACAGENT-6-SERVICE: %[func=AgentMainThread]: Eventloop started
```

OOB Management

- Profiles
- Devices

User Management

- User Roles
- Auth Servers
- Local Users

Monitoring

- Summary
- Reporting
- Online Users
- Event Logs
- SNMP

Administration

- **CCA Manager**
- User Pages
- Admin Users
- Backup

What to do on client? – Nac Client Decode

There is no external public decode tools link


Install a stand alone CAM manager (Virtual machine) as decode tool



[Downloads Home](#) > [Products](#) > [Security](#) > [Access Control and Policy](#) > [Network Admission Control](#) > [NAC Appliance \(Clean Access\)](#) > [NAC Appliance 4.9](#) > **Network Admission Control (NAC) Manager and Server System Software-4.9.5**

NAC Appliance 4.9



[Expand All](#) | [Collapse All](#)

Release 4.9.5 [Release Notes for 4.9.5](#)  [Add Device](#)
 [Add Notification](#)

File Information	Release Date	Size	
Tar file for upgrading from 4.8.x and 4.9.0 releases.  cca_upgrade-4.9.5-from-4.8.x-4.9.x.tar.gz	08-MAR-2015	653.07 MB	Download Add to cart
ISO file for fresh installation.  nac-4.9_5-K9.iso	08-MAR-2015	722.26 MB	Download Add to cart

▼ Latest

- 4.9.5**
- 4.9.4
- 4.9.2
- 4.9.3

▼ All Releases

- ▶ 4.9

What to do on client? – Nac Client Decode

Apply for a NAC evaluation license

<http://www.cisco.com/go/license>

Get Demo and Evaluation Licenses



1. Select Product | 2. Specify Target Device and Options | 3. Review and Submit

Search by Keyword

Make a selection from this list of products.

Product Family

- Cable Broadband Troubleshooter
- Network Mgmt Products
- Security Products**
- Unified Communications Products
- Routers & Switches
- Wireless
- Energy Management

Product

- Cisco Security MARS Demo License
- AnyConnect Plus/Apex (ASA) Demo License
- SA500 Series Security Appliances - 60-day IPS Trial License
- SA540 SSL License
- Cisco Security Agent Demo License
- Cisco Services for IPS **trial** license (Version 6.1 and later)
- Cisco Services for IPS **trial** license (Version 6.0.x and earlier)
- Cisco Clean Access Evaluation License**
- Cisco NAC Profiler server and Cisco NAC Collector 100 Device Demo License
- Cisco Smart Business Portal
- Cisco Unified CallConnector for Microsoft Windows
- Cisco Email/Web/Content Security Virtual Demo License

What to do on client? – Client log analysis

SWISS_RUNNER

6465: U1PC: Jun 18 2016 08:04:41.664 UTC: %NACAGENT-6-SWISS_RUNNER: %[func=SwissRunner::logTargetList]: target list: 10.75.61.211(L)/10.75.61.129(R)/8905 0.0.0.0(L)/10.75.179.210(R)/8905

6791: U1PC: Jun 18 2016 08:05:17.170 UTC: %NACAGENT-6-SWISS_RUNNER: %[func=SwissHttpsRunner::collectTargets]: List of targets for HTTPS probes: 10.75.61.129(default GW) ISE210.yin.local

6795: U1PC: Jun 18 2016 08:05:17.170 UTC: %NACAGENT-6-SWISS_RUNNER: %[func=SwissHttpsRunner::probeDiscoveryUrl]: Probe Discovery URL of 10.75.61.129 with HTTPS

6843: U1PC: Jun 18 2016 08:05:17.669 UTC: %NACAGENT-6-SWISS_RUNNER: %[func=SwissHttpsRunner::probeDiscoveryUrl]: DiscoveryHostContent X-Perfigo-CAS=ISE210.yin.local

6846: U1PC: Jun 18 2016 08:05:17.669 UTC: %NACAGENT-6-SWISS_RUNNER: %[func=SwissHttpsRunner::probeDiscoveryUrl]: Discovery URL returns CAS address ISE210.yin.local

6850: U1PC: Jun 18 2016 08:05:21.366 UTC: %NACAGENT-3-SWISS_RUNNER: %[func=getOpDataDynamicUrls]: printputing number of urls 6, length is 335

6853: U1PC: Jun 18 2016 08:05:21.366 UTC: %NACAGENT-7-SWISS_RUNNER: %[func=SwissUdpExchange::getSwissResponse]: SwissRunner received a Swiss response from ISE210.yin.local, port 8905, OP type 22

7302: U1PC: Jun 18 2016 08:05:44.205 UTC: %NACAGENT-7-SWISS_RUNNER: %[func=SwissUdpExchange::sendSwissRequest]: SwissRunner sent a Swiss request to address ISE210.yin.local, port 8905, OP type 17, event ID 2, IP/Mac list '10.75.61.211|00:50:56:b1:3a:ad '

7330: U1PC: Jun 18 2016 08:05:44.220 UTC: %NACAGENT-7-SWISS_RUNNER: %[func=SwissUdpExchange::getSwissResponse]: SwissRunner received a Swiss response from ISE210.yin.local, port 8905, OP type 18

What to do on client? – Client log analysis

Discovery Process

When the NAC agent starts, it follows this sequence:

1. HTTP discovery probe on port 80 to discovery host, if one is configured.
 2. HTTPS discovery probe on port 8905 to the discovery host, if one is configured.
 3. HTTP discovery probe on port 80 to default gateway.
 4. HTTPS reconnect probe on 8905 to previously contacted ISE policy node.
- Repeat from 1.

In order to verify whether the NAC agent will be able to reach the policy node, open a browser on the client machine and go to this URL:

<https://<ise-hostname>:8905/auth/discovery>



What to do on client? – Client log analysis

HTTP_DEBUG

6729: U1PC: Jun 18 2016 08:05:12.038 UTC: %NACAGENT-7-HTTP_DEBUG:
%[sev=debug][func=HTTPConnection::GetResponseHeader]: The requested location is
<https://ise210.yin.local:8905/auth/discovery?sessionId=0A4B3DCE000000502C7F7B95>

6732: U1PC: Jun 18 2016 08:05:12.038 UTC: %NACAGENT-7-HTTP_DEBUG:
%[sev=debug][func=HTTPConnection::ProcessRequest]: Received redirect to location
<https://ise210.yin.local:8905/auth/discovery?sessionId=0A4B3DCE000000502C7F7B95>

6735: U1PC: Jun 18 2016 08:05:12.038 UTC: %NACAGENT-7-HTTP_DEBUG:
%[sev=debug][func=HTTPConnection::CrackURL]: CrackUrl: host = ise210.yin.local path =
/auth/discovery?sessionId=0A4B3DCE000000502C7F7B95 user = port = 8905 scheme = 2 flags = 8388608

6741: U1PC: Jun 18 2016 08:05:12.677 UTC: %NACAGENT-7-HTTP_DEBUG:
%[sev=debug][func=HTTPConnection::ProcessRequest]: The HTTP response header for the message is:
HTTP/1.1 200 OK Date: Sat, 18 Jun 2016 08:05:40 GMT Content-Length: 30 Server: X-Perfigo-CAS:
ISE210.yin.local

What to do on client? – Client log analysis

HTTP_WARNING

1759: U1PC: Jun 18 2016 08:00:02.081 UTC: %NACAGENT-4-HTTP_WARNING:
%[sev=warning][func=HTTPConnection::RetrySendRequest]: First HttpSendRequestA **returns error (12002):** The request has timed out.

2753: U1PC: Jun 18 2016 08:00:18.663 UTC: %NACAGENT-4-HTTP_WARNING:
%[sev=warning][func=HTTPConnection::RetrySendRequest]: First HttpSendRequestA **returns error (12029):** Returned if connection to the server failed.

2766: U1PC: Jun 18 2016 08:00:18.929 UTC: %NACAGENT-4-HTTP_WARNING:
%[sev=warning][func=HTTPConnection::RetrySendRequest]: First HttpSendRequestA **returns error (12007):** The server name cannot be resolved.

7012: U1PC: Jun 18 2016 08:05:27.232 UTC: %NACAGENT-4-HTTP_WARNING:
%[sev=warning][func=HTTPConnection::RetrySendRequest]: First HttpSendRequestA **returns error (12175):** One or more errors were found in the Secure Sockets Layer (SSL) certificate sent by the server. To determine what type of error was encountered, check for a WINHTTP_CALLBACK_STATUS_SECURE_FAILURE notification in a status callback function. For more information, see WINHTTP_STATUS_CALLBACK.

What to do on client? – Client log analysis

XML_PARSE

Once the endpoint downloads agent, agent tries to discover positron box. If discovery is successful, ISE sends all applicable posture policies to the agent in xml format

```
7035: U1PC: Jun 18 2016 08:05:28.698 UTC: %NACAGENT-6-XML_PARSE:
%[sev=info][func=Authenticator::parseHTTPResponsePkt][part=7035.1/2]: Posture data parse begin :
<msg><id>MSG_NS_HTTP_RESPONSE</id><result>success</result><message><!--X-Perfigo-UserKey=--><!--X-Perfigo-
Provider=Device Filter--><!--X-Perfigo-UserName=u11--><!--X-Perfigo-Ref=63Af40heTOX+BJPERV70aQ===--><!--error=1010--
--><!--X-Perfigo-DM-Error=1010--><!--user role=--><!--X-Perfigo-OrigRole=--><!--X-Perfigo-DM-Scan-Req=0--><!--X-Perfigo-DM-
Software-List=2G1KS+WPf+jYCSJe6HFUZQCJfqCv8Uej
```

```
7036: U1PC: Jun 18 2016 08:05:28.698 UTC: %NACAGENT-6-XML_PARSE:
%[sev=info][func=Authenticator::parseHTTPResponsePkt][part=7035.2/2]:
u1EQyTQxDD/RefKXD4TX6dbl8L1oGSGZc6f7T9maNOxvpfCynzh043E+cxByEpJ/C6lmpRwtpjnRIMAYzWoMrjDaHYmLPTNGI
24Y7v8UfjIN9jzvhpVUS5/i18IMzOdOT4kGIPaZo+Pr8kLEKU7b+S6AjsPOjJXs02S7Yc2Ywi1QpNnU2K4etmjKtHnAbcKxIBMRG
w60xEhKgwkpeNNOCT8ddRMsL9kUKwM5LIY70yluXYJOWvTcEhLsSe9KS VHY=--><!--X-Perfigo-DM-Session-Time=240--
--></message></msg>
```

```
7039: U1PC: Jun 18 2016 08:05:28.698 UTC: %NACAGENT-7-XML_PARSE:
%[sev=debug][func=AuthInfo::processPostureData]: Decrypted posture data, X-Perfigo-DM-Software-List =
<cleanmachines><version>2</version><encryption>0</encryption><package><id>10</id><name>cmd_running</name><versi
on/><description>cmd is
running</description><type>3</type><optional>0</optional><action>3</action><check><id>cmd_is_running</id><category>
4</category><type>401</type><param>cmd.exe</param><operation>running</operation></check><criteria>(cmd_is_runnin
g)</criteria></package></cleanmachines>
```

```
7042: U1PC: Jun 18 2016 08:05:28.698 UTC: %NACAGENT-6-XML_PARSE: %[sev=info][func=AuthInfo::parseAuthInfo]:
XML parse success
```

What to do on client? – Client log analysis

REQUIREMENT_PROC

7072: U1PC: Jun 18 2016 08:05:28.714 UTC: %NACAGENT-6-REQUIREMENT_PROC:
%[sev=info][func=Rqmt::doCheck]: **Checking rqmt, [cmd_running]:Mandatory**

7078: U1PC: Jun 18 2016 08:05:28.714 UTC: %NACAGENT-7-PROCESS_CHK:
%[sev=debug][result=res][func=CheckProcess::doCheck]: The service: cmd.exe is Running. The requested check:
cotRunning and **the result: Successful**

7081: U1PC: Jun 18 2016 08:05:28.714 UTC: %NACAGENT-6-REQUIREMENT_PROC:
%[sev=info][func=Rqmt::completeCheck]: **Check result of rqmt, [cmd_running]:PASSED**

7135: U1PC: Jun 18 2016 08:05:35.328 UTC: %NACAGENT-6-REQUIREMENT_PROC:
%[sev=info][func=PostureInfo::generatePostureReport][part=
7135.1/2]: Posture check report =
<report><version>1000</version><encryption>0</encryption><key></key><os_type>WINDOWS_7_64_ULTIMATE</os_ty
pe><osversion>1.2.1.6.1.1</osversion><build_number>7600</build_number><architecture>9</architecture><user_name>[
device-
filter]</user_name><agent>4.9.5.8</agent><opswat>3.6.10591.2</opswat><sys_name>U1PC</sys_name><sys_user>c
isco</sys_user><sys_domain>n/a</sys_domain><sys_user_domain>U1PC</sys_user_domain><av><av_prod_id>Microso
ftAS</av_prod_id><av_prod_name>Windows
Defender</av_prod_name><av_prod_version>6.1.7600.16385</av_prod_version><av_def_version>1.187.1714.0</av_def_
version><av_def_date>11/10/2014</av_def_date><av_pr

7136: U1PC: Jun 18 2016 08:05:35.328 UTC: %NACAGENT-6-REQUIREMENT_PROC:
%[sev=info][func=PostureInfo::generatePostureReport][**part=7135.2/2**]:
od_features>AS</av_prod_features></av><package><id>10</id><status>1</status><check><chk_id>cmd_is_running</ch
k_id><chk_status>1</chk_status></check></package></report>

What to do on client? – Client log analysis

APP_VER

3: U1PC: Jun 18 2016 07:57:19.965 UTC:
%NACAGENT-6-APP_VER: %[ver=4.9.5.8][os=]:
NAC Agent version 4.9.5.8 started

NET_ACCESS

7242: U1PC: Jun 18 2016 08:05:41.210 UTC:
%NACAGENT-5-NET_ACCESS: %[comp=BFE]
[level=Full]: Net Access Granted [Full]

What to do on client? – Web Client log locate

C:\Document and Settings*<user>*\Local Settings\Temp\webagent.log

C:\Document and Settings*<user>*\Local Settings\Temp\webagentsetup.log

-Quick go to “run”----- “%TEMP%“

-Webagent.log is encrypted by cipher need decode

What to do on client? – Web Client log Decode

```
[Sat Jun 18 17:55:34 2016] [DEBUG]
<name>cmd_running</name><version/><description>cmd is
running</description><type>3</type><optional>0</optional>
<check><id>cmd_is_running</id>
<param>cmd.exe</param>
<operation>running</operation></check>
<criteria>(cmd_is_running)</criteria>
```

```
[Sat Jun 18 17:55:34 2016] [DEBUG] [TAOpswat]
OPSWAT AV SDK Version: 3.6.10363.2
```

```
[Sat Jun 18 17:55:37 2016] [DEBUG] [PerfigoDMPackage]
Package: cmd_running [Mandatory]
```

```
[Sat Jun 18 17:55:37 2016] [DEBUG] [PerfigoDMCheck]
process, cmd.exe, running status is running
```

```
[Sat Jun 18 17:55:37 2016] [DEBUG] [PerfigoDMCheck]
Check process result: successful
```

What to do on client? – Efficient Analysis

- Ask more question !
 - whether all clients meet error?
 - whether error can re-occur stability?
 - whether reboot client or reinstall client can fix?
 - what's the error or alert message pop up, if have?
- Synchronized clock & timestamp (ISE,Client), NTP
- Verify whether agent process is running or not, like nacagent.exe, nacagentgui.exe
- Verify session start point & end point (“grant access full”)
- Verify what step process pending or failure
- Simple and extract the symptom contents from huge repeated cycle logs.
- Better get a valid good example as normal simple for compare difference.



CISCO

Thank You!