



A song of ISE and Posture:

Advanced deployment and troubleshooting

Andrea Bertorello - Security Consulting Engineer
BRKSEC-3077

Abstract

Endpoint Security is nowadays a pillar of all organizations, and increasing their compliance checks before connecting to the organization networks is a trend. Your endpoint security is your armor. This armor is not a single piece of steel but instead, it's a set of security components, where a single weakness in one of them may destroy the efficiency of the entire system. ISE posture services help, to ensure that your endpoints armor is always in good shape. During the session, attendees will have the opportunity to explore advanced posture scenarios and settings, such as load balancing, posture session management, MFA and bidirectional-posture. A demo will provide in-depth information on these topics. Furthermore, after the session, attendees will possess the knowledge and skills to troubleshoot any posture-related issues using log references, to solve the problem of now from where I start if something is not working.

About me



- AAA TAC Engineer
- Security Consulting Engineer



Warning!
Italian accent ahead



Icon Used Through the Presentation



Content enlarging – when something is not visible good enough we highlight and enlarge this area.



GUI navigation assistant – This special type of highlighting is used to help you in navigation in the Graphical User Interface of a product.



For your Reference – these items could not be covered in detail during the session.



Warning – Extra attention during the configuration



Hidden Content – slides which won't be presented during the session. Those slides are here to give you later more context and detailed information

Webex App

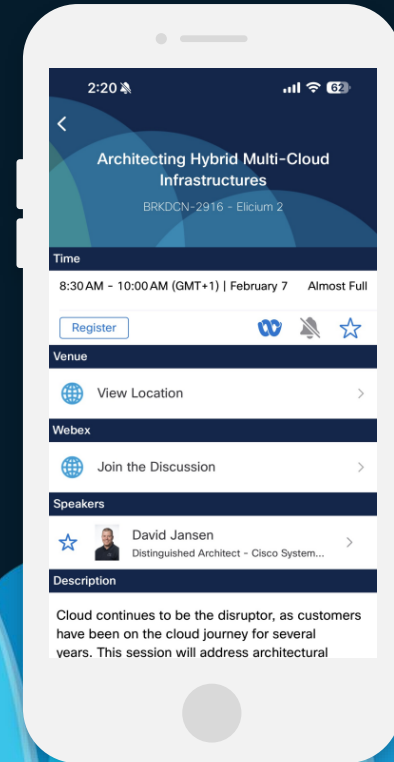
Questions?

Use the Webex app to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events mobile app
- 2 Click “Join the Discussion”
- 3 Install the Webex app or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.





Agenda

- Basic Posture
 - ISE Posture Journey
- Advanced Posture Processes
- Advanced Scenarios bootcamp
- Learn by Example – Posture Troubleshooting

Agenda

1

Basic Posture

- ISE Posture 101
- ISE Posture Journey

3

Advanced Scenarios Application

2

Advanced Posture Processes

- Session Sharing
- Discovery Process
- Compliant State

4

Posture Troubleshooting

- Deep Dive Troubleshooting
- Learn on Example

Session Objectives

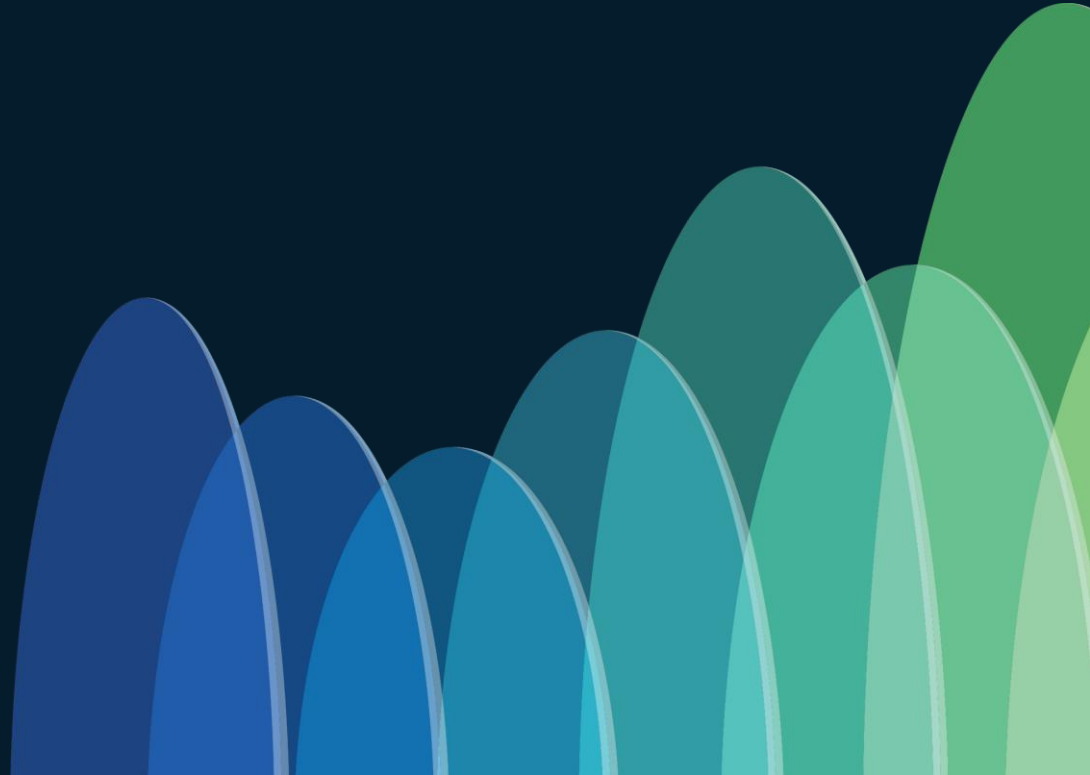
Session will cover:

- Theory of Posture
- Posture deployment scenarios
- Troubleshoot methodology

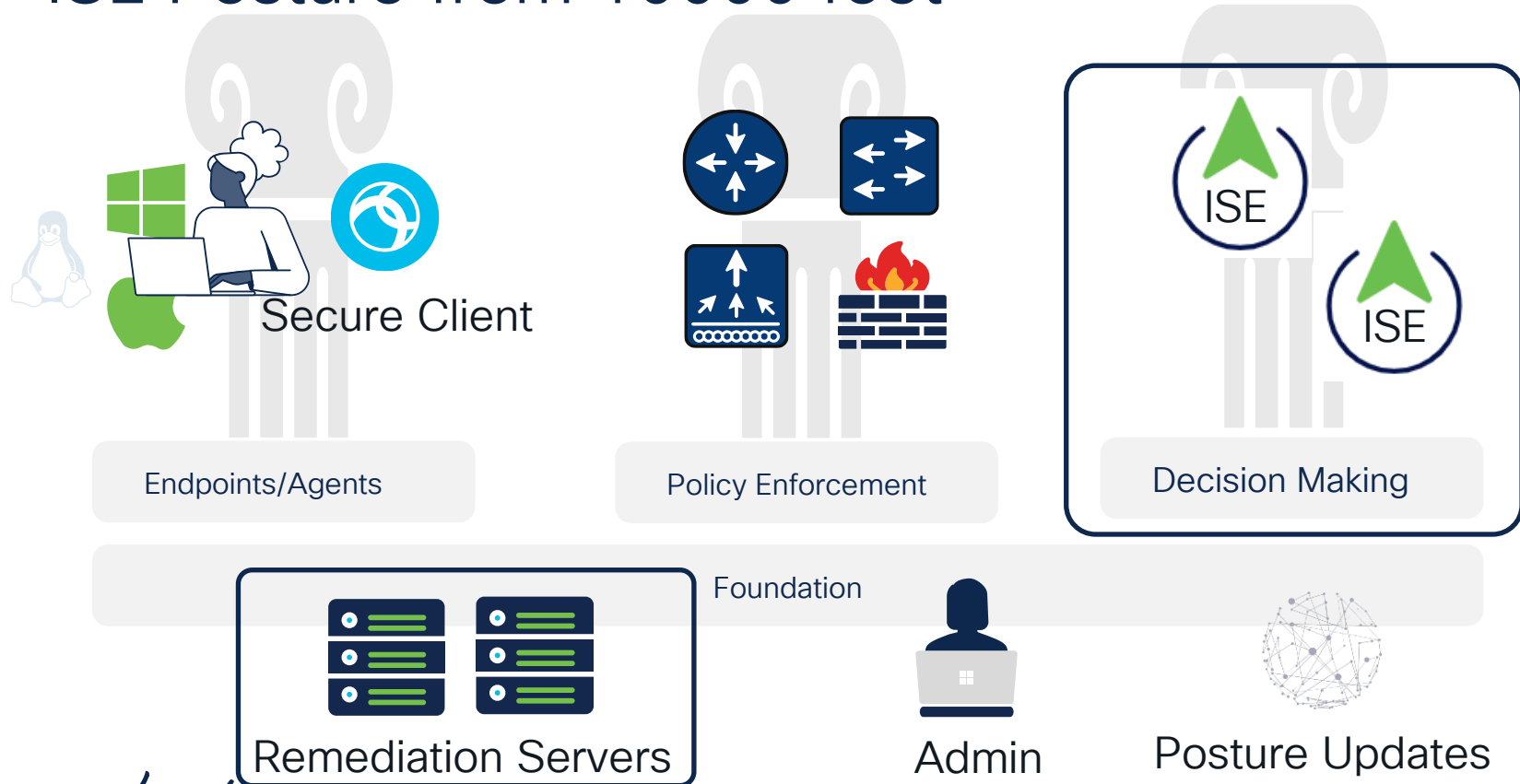
Session will not cover:

- Marketing
- Roadmaps
- All possible ISE posture features

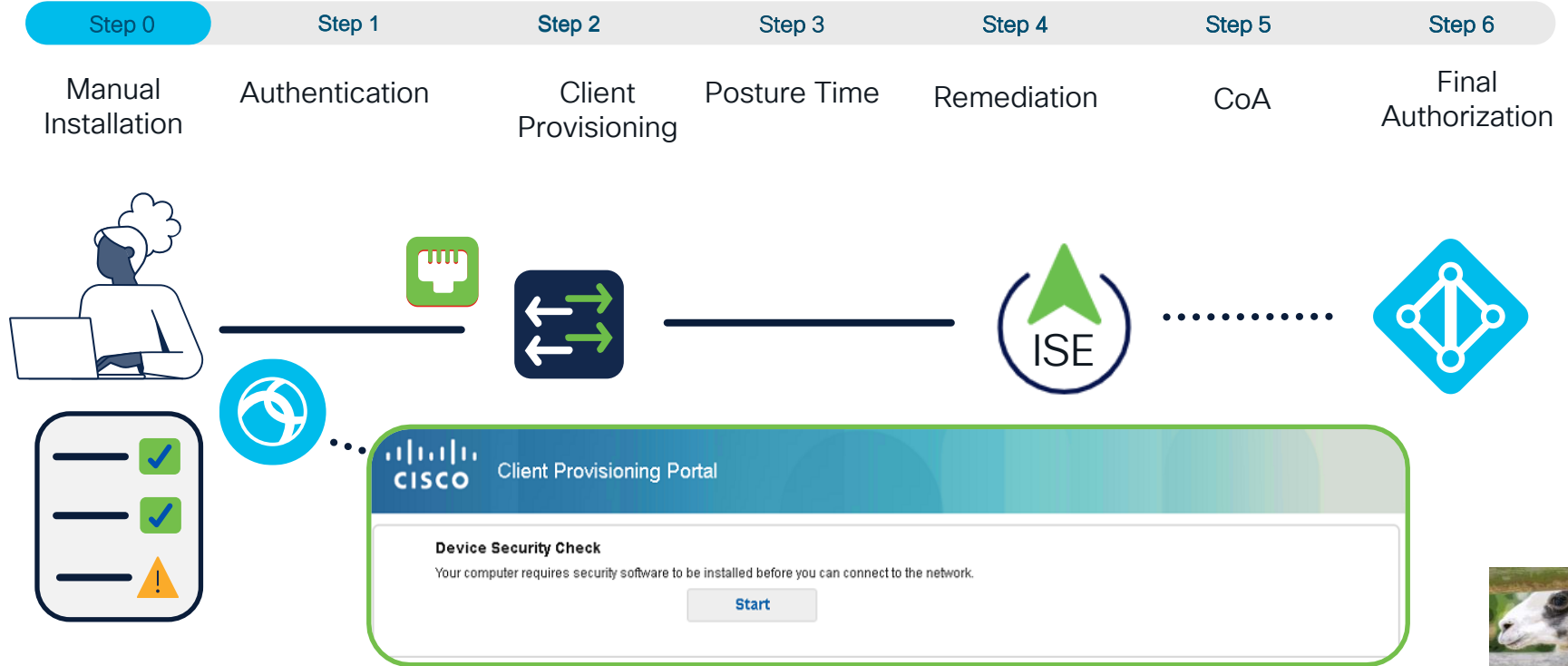
Posture 101



ISE Posture from 10000 feet



Posture Lifecycle

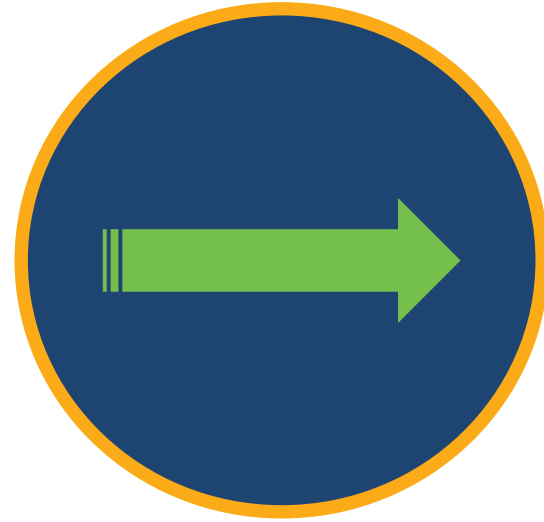


ISE Posture Flow types

Redirect based



Non-redirect based



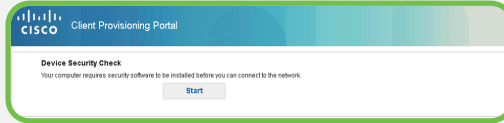
ISE Posture Flow types - comparison

Redirect

Initial Authentication
or Authorization

Redirect ACL and URL

Client Provisioning
Portal



PSN Discovery




Supported
Network Access
Devices



Non-Redirect

ACL/VLAN

 ise-cpp.demo.local



Call-Home



No redirection
support

Posture Style comparison

Components	Redirect	Non-redirect
Initial Authentication/Authorization access	Redirect ACL and URL	ACL/VLAN
Client provisioning portal (CPP)	Displayed after browsing to any site	Displayed after browsing to the CPP FQDN
PSN discovery	Using HTTP probes to redirect to ISE and list of previously connected PSNs as fallback	Using the “Call Home” List
Use with	Cisco Switches, WLCs and ASAs	Any Cisco or non-Cisco NAD
Configuration file	Endpoints do not need ISEPostureCFG.xml predeployed	Endpoints need ISEPostureCFG.xml predeployed

Redirect best practices Wired

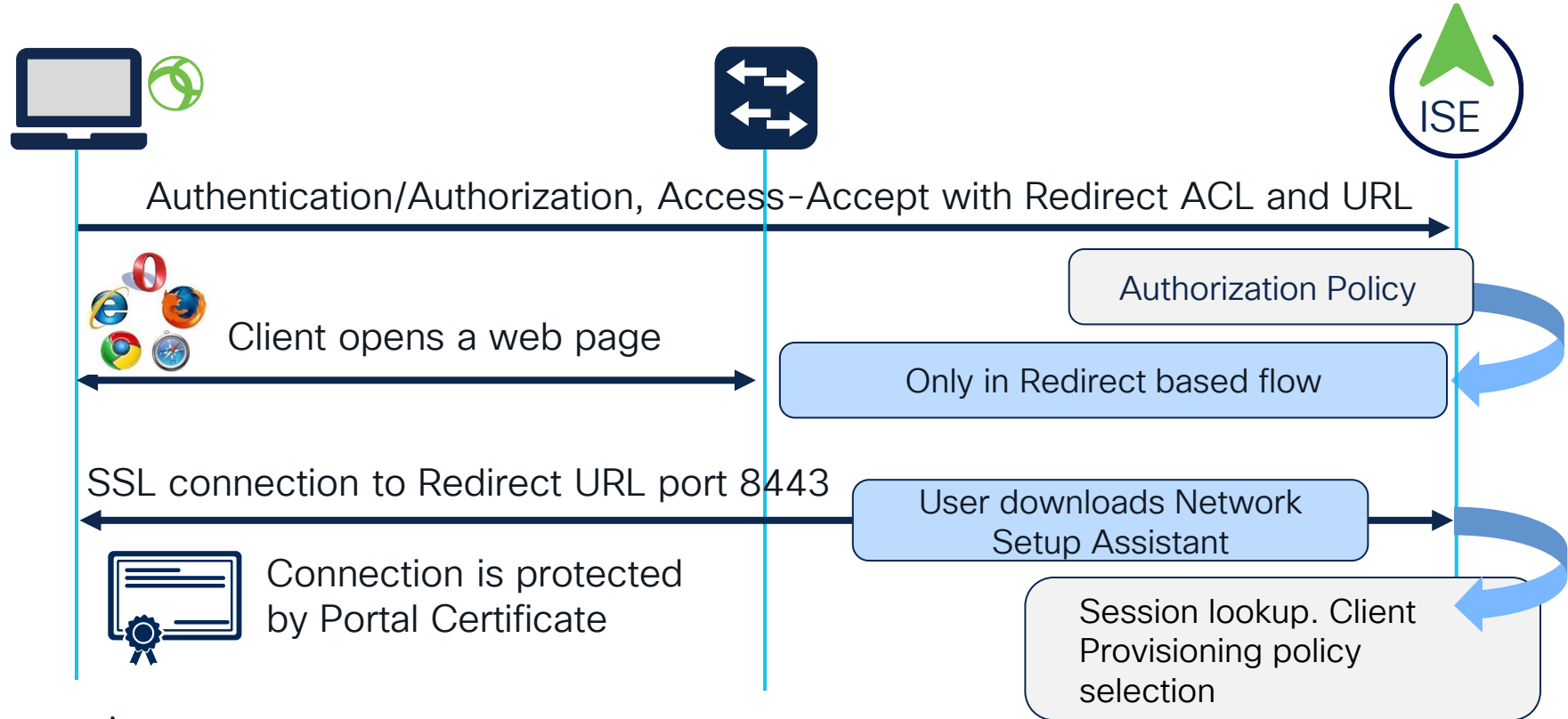
When client initiate http session NAD is intercepting and returning url-redirect as new page location

- **http server** – enabled, default port 80 should be used except situation when proxy is involved
- **IPDT** – enabled, IP device tracking is critical component for applying ACLs, (required for multi-domain and multi-auth)
- **SVI in client subnet** – otherwise traffic flow between client and switch need to be planned very carefully
- **DACL and redirect ACL** – tricky question, will be covered on next slide separately

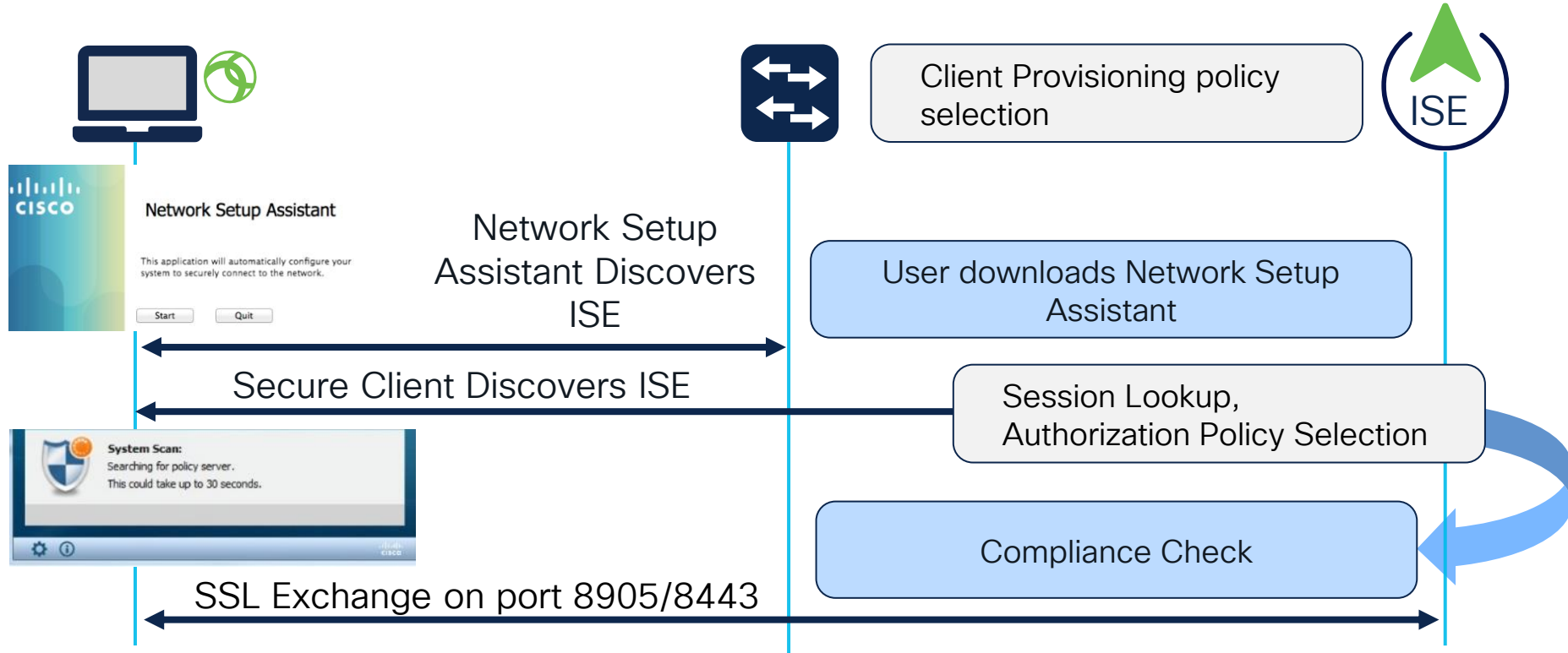
Redirect best practices Wireless

- **AAA override enabled** – this will allow WLC to apply Redirect ACL and Redirect URL to client
- **NAC=Radius NAC/ISE** – without this option COA won't be supported for WLAN, and this will prevent applying of redirect attributes
- **Redirect ACL/Airspace ACL** – the same recommendation as for switches. Protection provided by redirect ACL is enough

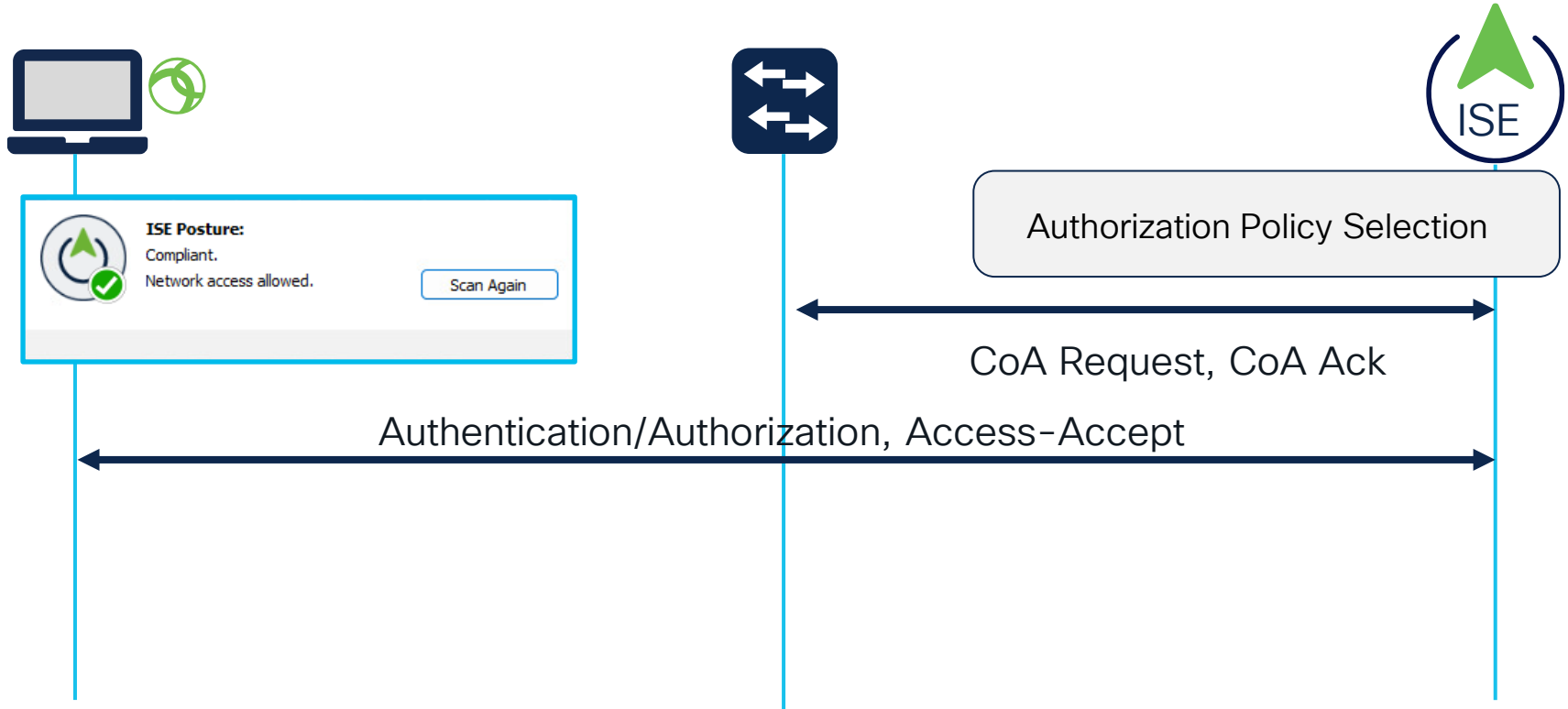
Posture Redirect – Let's visualize



Posture Redirect – Let's visualize



Posture Redirect – Let's visualize



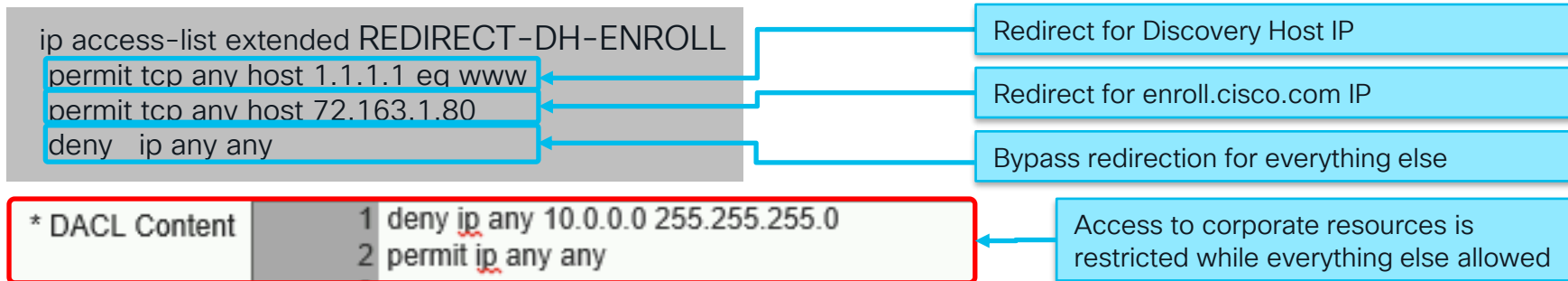
Posture process deep dive – before we begin



ISE posture module is pre-installed in our environment. Redirection and captive portal detection pop-ups are confusing for end-users.

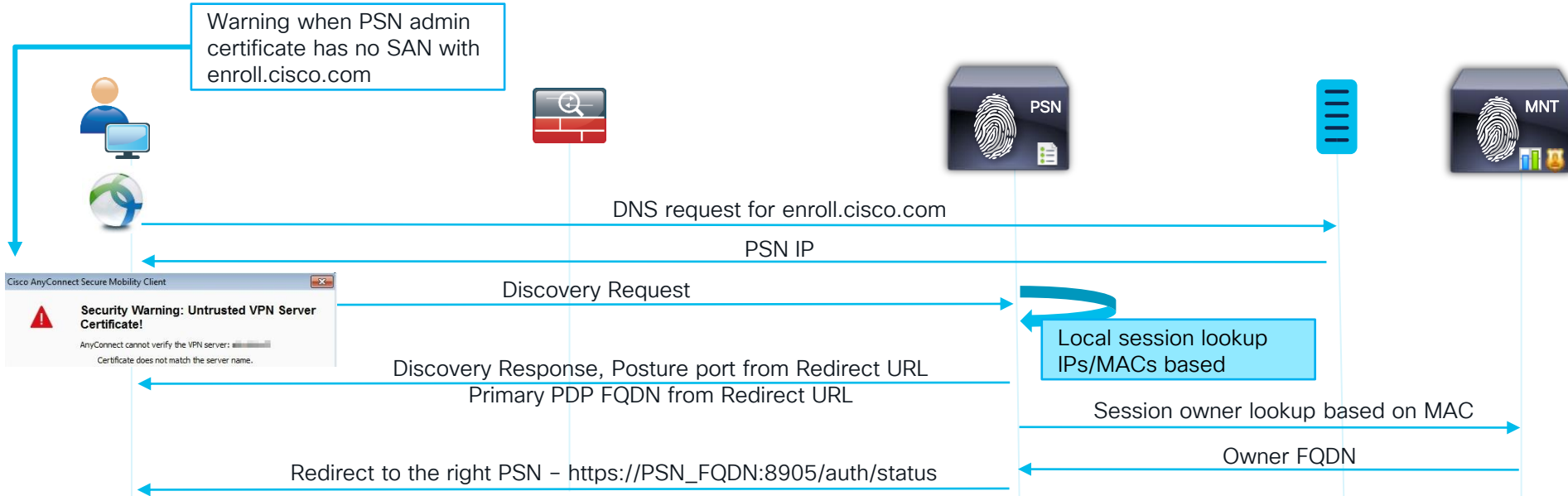


Redirection can be configured in the way when only certain probes are redirected



Posture non-redirect – Let's visualize

Pre-installed agent without profile



Posture non-redirect – Let's visualize

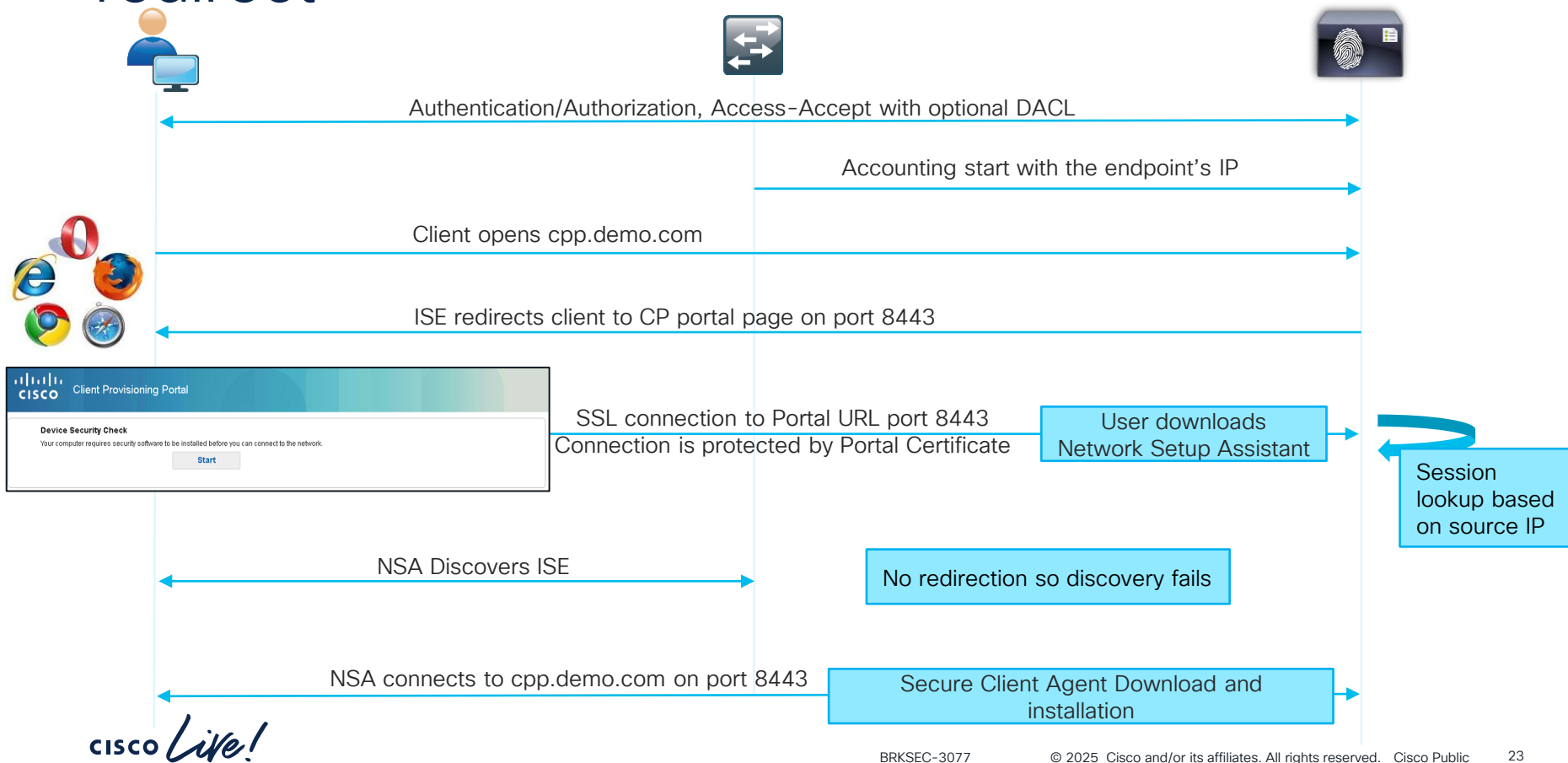
Call home addresses in PSN
can be IPs/FQDNs of PSNs
or IP/FQDN of LB VIP

Call Home List	<code>vip.example.com</code>
----------------	------------------------------

When port is not defined agent uses
8905

Call Home List	<code>vip.example.com:8443</code>
----------------	-----------------------------------

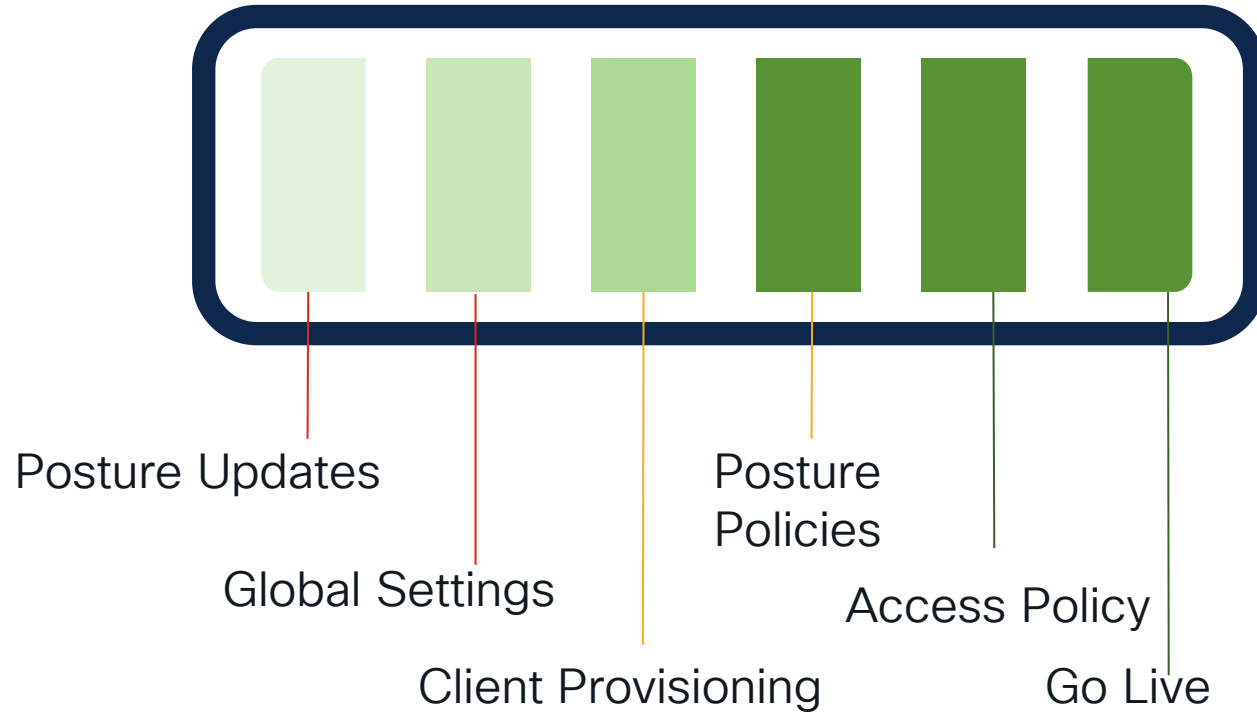
Posture flow with agent installation from CPP, no redirect



ISE Posture Journey



ISE Posture Journey

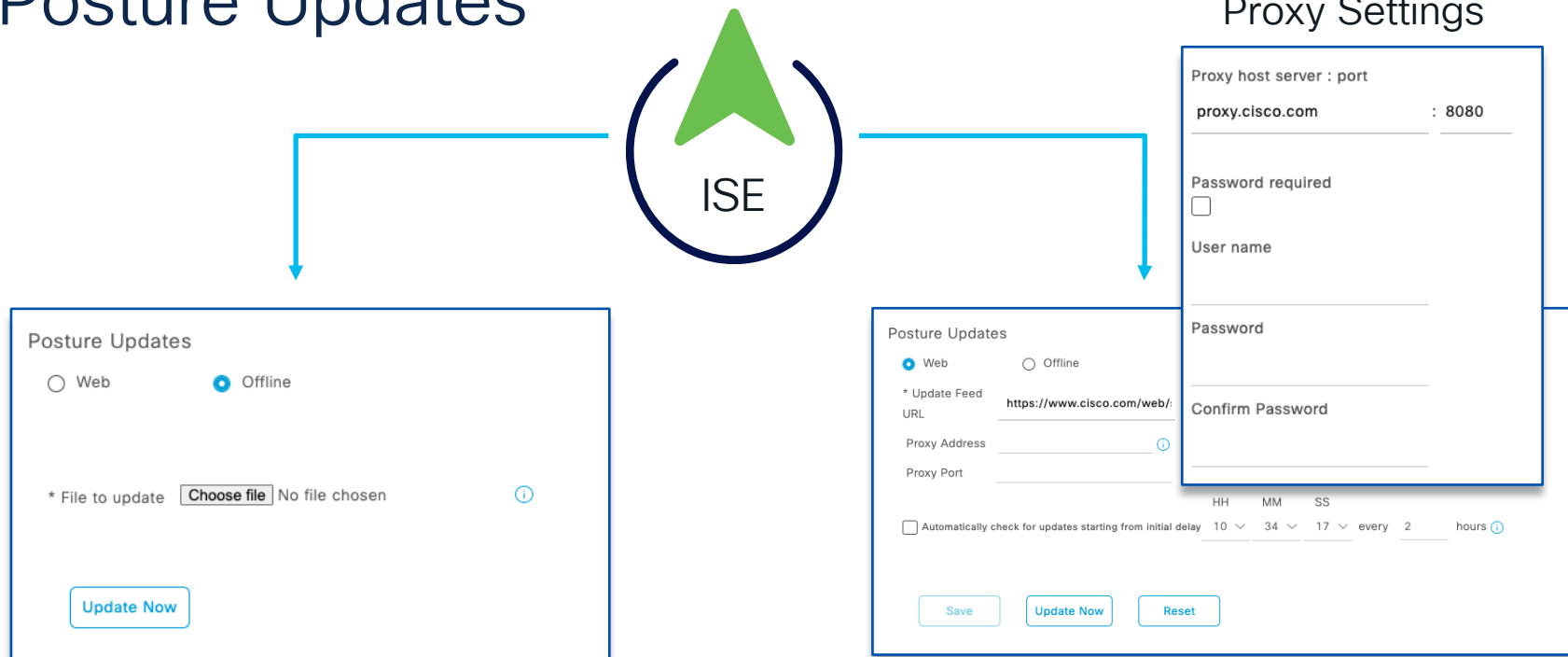


ISE Posture Journey: Posture Updates



Posture Updates

Posture Updates



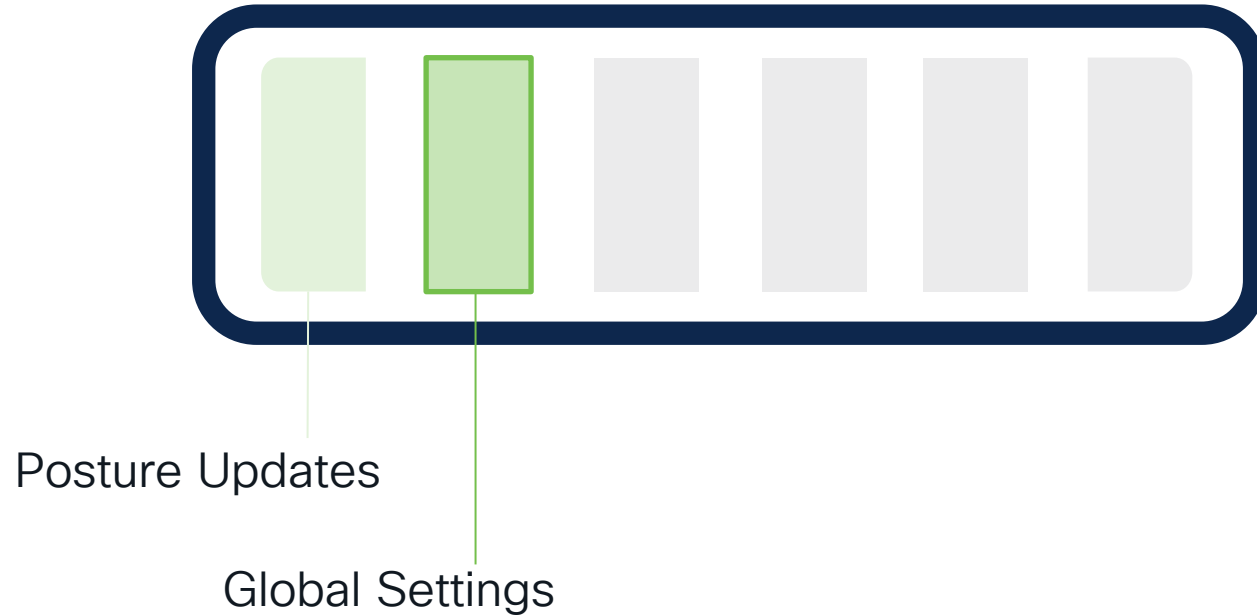
Deleted default posture elements are not created again during next updates

Posture Updates

Online Updates: Posture updates include a set of predefined checks, rules, and support charts for antivirus and antispyware for both Windows and Macintosh operating systems, and operating systems information that are supported by Cisco.

Offline Updates: You can also update Cisco ISE offline from a file on your local system, which contains the latest archives of updates.

ISE Posture Journey: Global Settings



Global Settings

Posture General Settings

These settings will be used if there is no profile under client provisioning policy.

Remediation Timer

4

Minutes



Network Transition Delay

3

Seconds



Acceptable Use Policy in Stealth Mode

Block



Default Posture Status

Compliant



☐ Automatically Close Login Success Screen After

0

Seconds



☒ Continuous Monitoring Interval

15

Minutes



Time for the user to remediate



What if client does not support posture ?



Global Settings

Posture Lease

☒ Perform posture assessment every time a user connects to the network

☐ Perform posture assessment every Days [i](#)

☒ Cache Last Known Posture Compliant Status

Last Known Posture Compliant State Days [v](#)

☐ Enable Port 8905 on non-Policy Service nodes for Posture services.

Posture Lease

Cisco ISE will use the last known posture state and will not reach out to the endpoint to check for compliance.

Agentless Plugin

Agentless Posture

These settings configure whether to display notifications about posture timeout. Agentless Posture uses Endpoint Connectivity Timeout, which is controlled by "Max retry attempts" and "Delay between retries for OS identification". For more information, see [\(Administration > System > Settings > Endpoint Scripts > Settings\)](#)

Agentless posture client timeout Minutes [i](#)

☐ Remove Agentless Plugin after each run



Endpoint Posture Attributes – Posture Lease

Posture lease is a feature which allows ISE to store endpoint posture status (Compliant) for up to 365 day

Posture Lease

☐ Perform posture assessment every time a user connects to the network

☒ Perform posture assessment every Days ⓘ

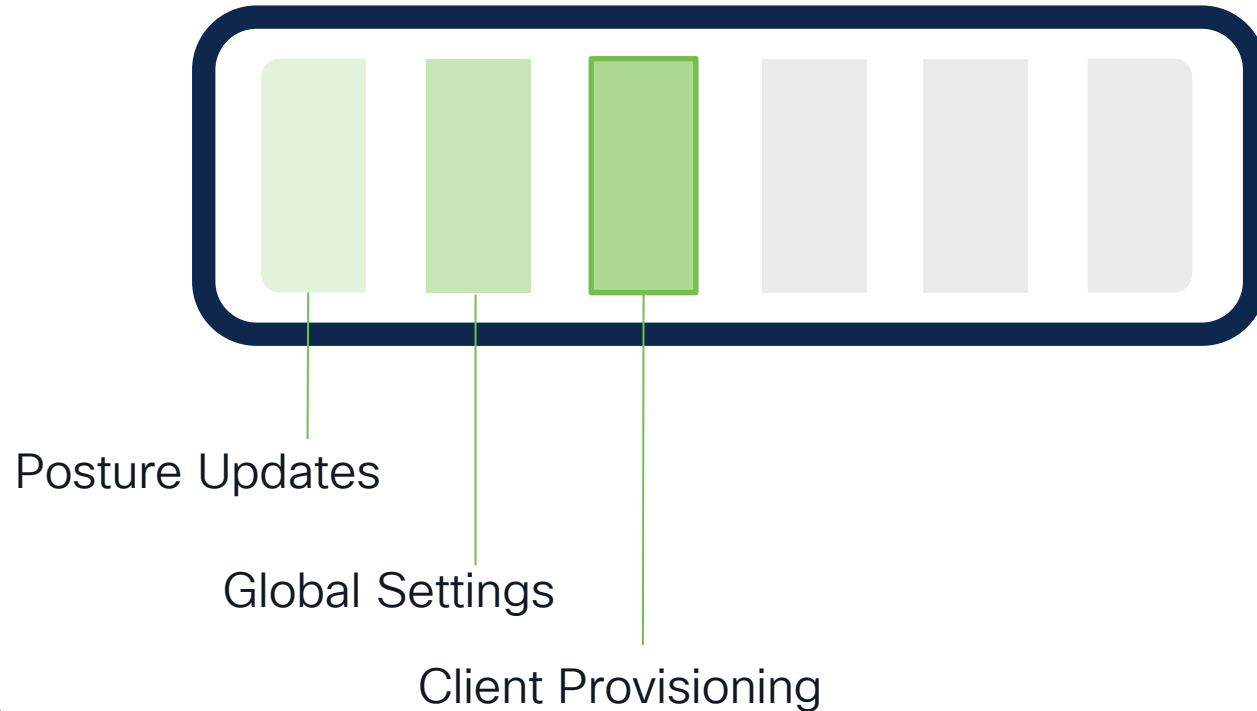
Posture Lease ⓘ

Valid range 1 to 365 days.
Note : This configuration applies only to AnyConnect Agent and not to NAC Agent and Web Agent.

When endpoint is in Posture lease ISE assigns authorization policy with 'Compliant' status right-away

Secure Client is NOT aware about the lease. To display proper posture status PSN discovery is performed. This discovery is example of valid cases when redirection does no happen in Redirect-Based environment.

ISE Posture Journey: Client Provisioning












ISE Posture: Agent types



Posture Deployment Options

- ✓ Supported
- ⚠ Limitations
- ✗ Not Supported

Client Provisioning

Capability	Cisco Secure Client			AC Stealth		Temporal		Agentless	
									
Anti-Malware Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Firewall Installation Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓
Application Inventory	✓	✓	✗	✓	✓	✓	✓	✓	✓
Hardware Inventory	✓	✓	✗	✓	✓	✓	✓	✓	✓
Process Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dictionary Conditions	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓
File Checks	✓	✓	⚠	✓	✓	✓	✓	⚠	✓
Service Checks	✓	✓	✗	✓	✓	✓	✓	✓	⚠
Disk Encryption	✓	✓	✗	✓	✓	⚠	⚠	⚠	⚠
Patch Management	✓	✓	⚠	✓	✓	⚠	⚠	⚠	⚠
Registry Checks	✓	N/A	N/A	✓	N/A	✓	N/A	⚠	N/A
USB Checks	✓	✗	✗	✓	✗	✓	✗	✓	✗
WSUS remediation (legacy)	✓	N/A	N/A	✓	N/A	✓	✗	✗	✗
Remediation	Auto Manual	Partial	Partial	Part Auto	Partial	Text	Text	✗	✗
Reassessment	✓	✓	✓	✓	✓	✗	✗	✗	✗

Visibility (Less Effort)

Experience (Less Time)

Security (More Protection)

Client Provisioning

Resources

Secure Client Profile

Client Provisioning Policy

Resources

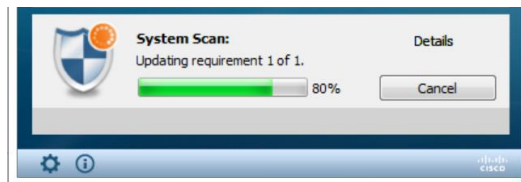
[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

<input type="checkbox"/>	Name	Type	Version	Last Update	Description
<input type="checkbox"/>	CiscoAgentlessWindows 5.0...	CiscoAgentlessWind...	5.0.529.0	2022/08/30 12:26:58	With CM: 4.3.2868.6145
<input type="checkbox"/>	CiscoAgentlessOSX 5.0.005...	CiscoAgentlessOSX	5.0.529.0	2022/08/30 12:27:00	With CM: 4.3.2490.4353
<input type="checkbox"/>	MacOsXSPWizard 2.7.0.1	MacOsXSPWizard	2.7.0.1	2022/08/30 12:26:50	Supplicant Provisioning ...
<input type="checkbox"/>	Cisco-ISE-Chrome-NSP	Native Supplicant Pro...	Not Applic...	2016/10/06 22:01:12	Pre-configured Native S...
<input type="checkbox"/>	CiscoTemporalAgentWindo...	CiscoTemporalAgent...	5.0.529.0	2022/08/30 12:26:51	With CM: 4.3.2868.6145
<input type="checkbox"/>	CiscoTemporalAgentOSX 5...	CiscoTemporalAgent...	5.0.533.0	2022/08/30 12:26:54	With CM: 4.3.2490.4353
<input type="checkbox"/>	WinSPWizard 3.2.0.1	WinSPWizard	3.2.0.1	2022/08/30 12:26:51	Supplicant Provisioning ...
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Pro...	Not Applic...	2022/08/30 13:37:08	Pre-configured Native S...

Some agents must be downloaded from Cisco Software Center and uploaded manually

Client Provisioning: What is compliance module

Compliance Module – Offers the ability to assess an endpoint's compliance.

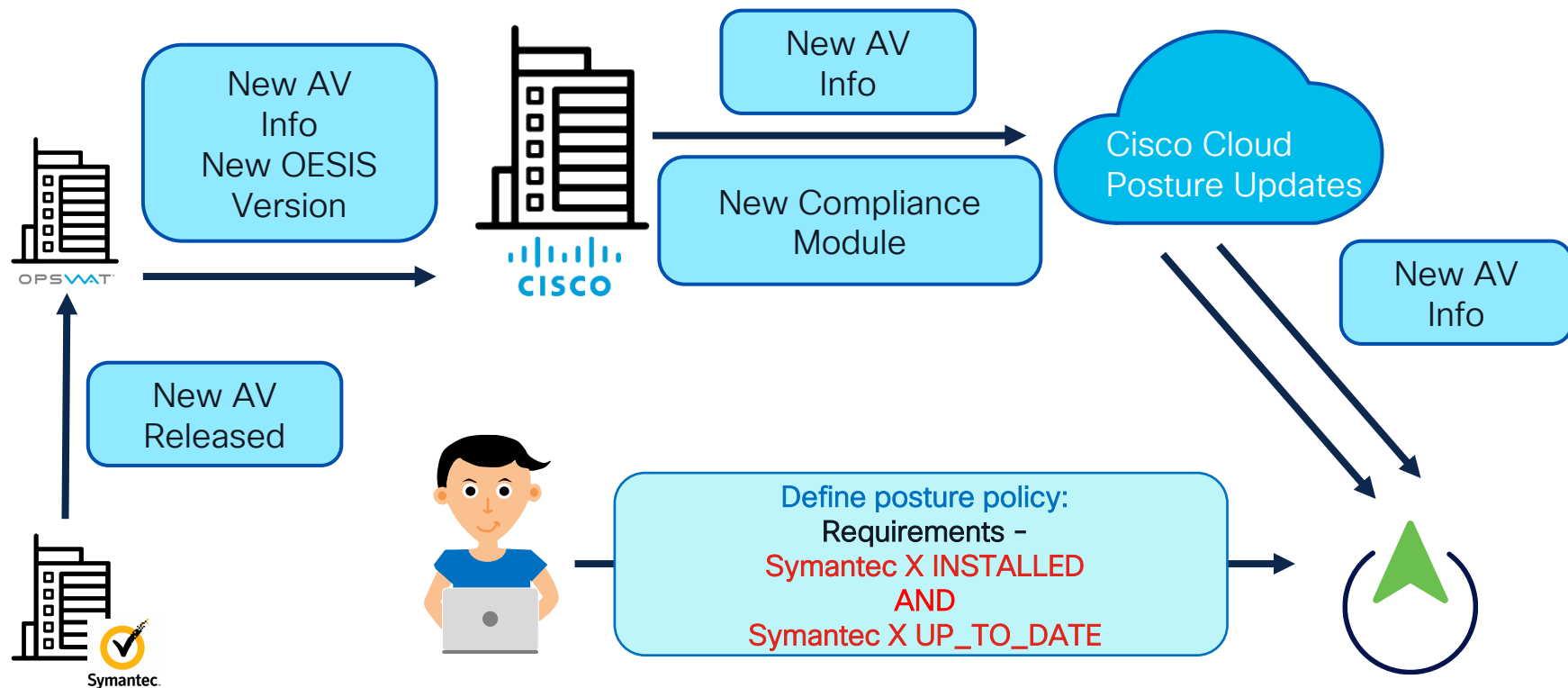


OPSWAT – Cisco Compliance module is using OESIS framework from OPSWAT for detection and remediation

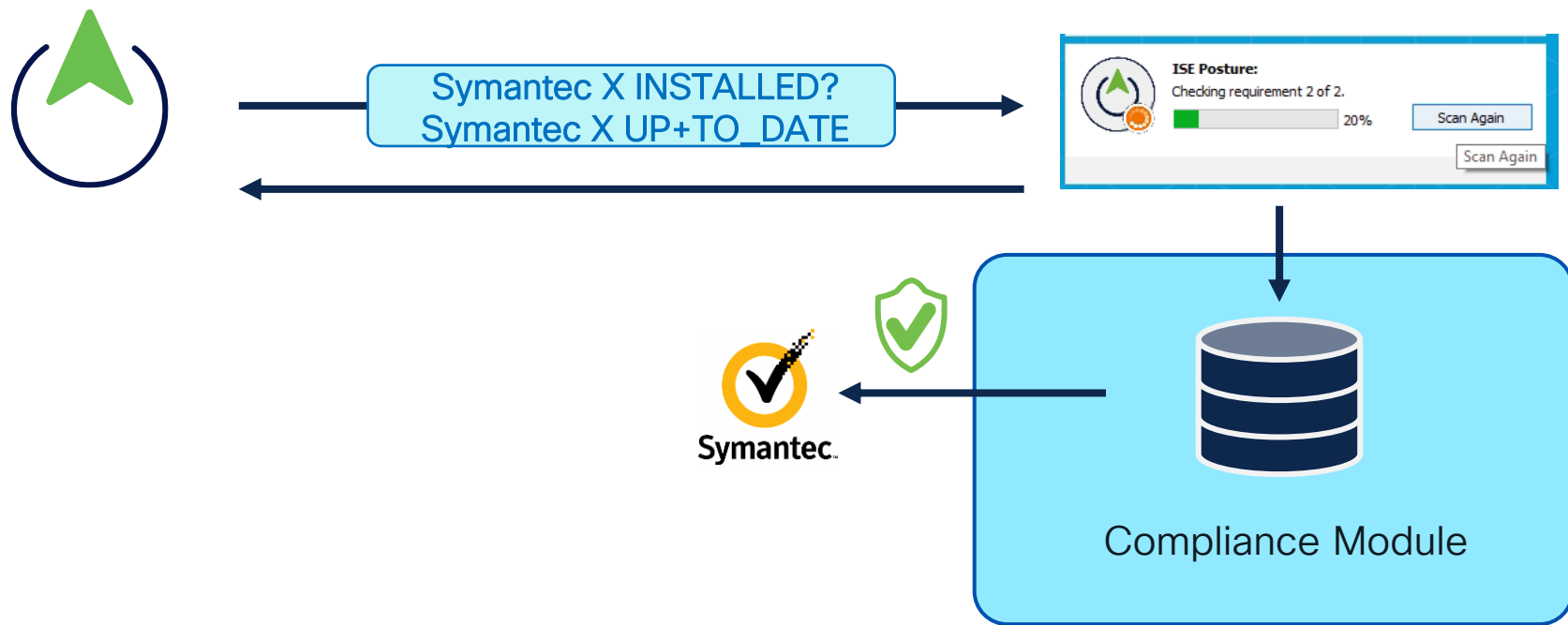
<https://www.slideshare.net/OPSWAT/introduction-to-oesis-framework>



Let's visualize



Let's visualize



Compliance Module Updates vs Posture updates

Compliance Module Updates



DB Application



Corresponding

Actions



Posture Updates



On ISE



Posture Policy

<input type="checkbox"/>	Avast Business Security	6.x	▼	23.x	4.3.3726.6145
<input type="checkbox"/>	Avast Premium Security	19.x	▼	23.x	4.3.3726.6145

Client Provisioning

Resources



Secure Client Profile



Client Provisioning Policy

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ	*	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Posture Profile



* Select Agent Package: AnyConnectDesktopWindows 4.5.5030. v

* Configuration Name: Agent Configuration

Description:

Description Value Notes

* Compliance Module: AnyConnectComplianceModuleWindow: v

AnyConnect Module Selection

- ISE Posture ☒
- VPN ☒
- Network Access Manager ☐
- Web Security ☐
- AMP Enabler ☐
- ASA Posture ☐
- Network Visibility ☐
- Umbrella Roaming Security ☐
- Start Before Logon ☐
- Diagnostic and Reporting Tool ☒

Agent Profile

Server name rules * i

Retransmission Delay i 60 secs

Description

This is the agent retry period if there is a Passive Reassessment communication failure

Time (in seconds) to wait before retrying.

Discovery host i

cisco.com

Default – enroll.cisco.com

Call Home List i

10.52.15.80, 10.52.15.81

Enable Rescan Button

Disabled ▼



System Scan:

No policy server detected.

Default network access is in effect.

[Scan Again](#)

ISE Configuration Details - Redirection

Discovery Host

Any IP/FQDN routed through the NAD

Discovery host ⓘ

Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.



```
<DiscoveryHost>internal.link.com</DiscoveryHost>
```

ISEPostureCFG.xml

ISE Configuration Details - Redirection

Server Name Rules

Wildcard of allowed Servers

Server name rules * ⓘ

*.lab.com

A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"



```
<ServerNameRules>*.lab.com</ServerNameRules>
```

ISEPostureCFG.xml

ISE Configuration Details

Call Home List

PSN IP Address List to try to contact

Call Home List ⓘ

|

A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.



```
<CallHomeList>10.52.X.X,10.52.X.X</CallHomeList>
```

ISEPostureCFG.xml

Posture files - ISEPostureCFG



Client Provisioning

Resources

Secure Client Profile

Client Provisioning Policy

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ	*	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.*.cisco.com"
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

* Select Agent Package: AnyConnectDesktopWindows 4.5.5030. v

* Configuration Name: Agent Configuration

Description:

Description Value Notes

* Compliance Module AnyConnectComplianceModuleWindow: v

AnyConnect Module Selection

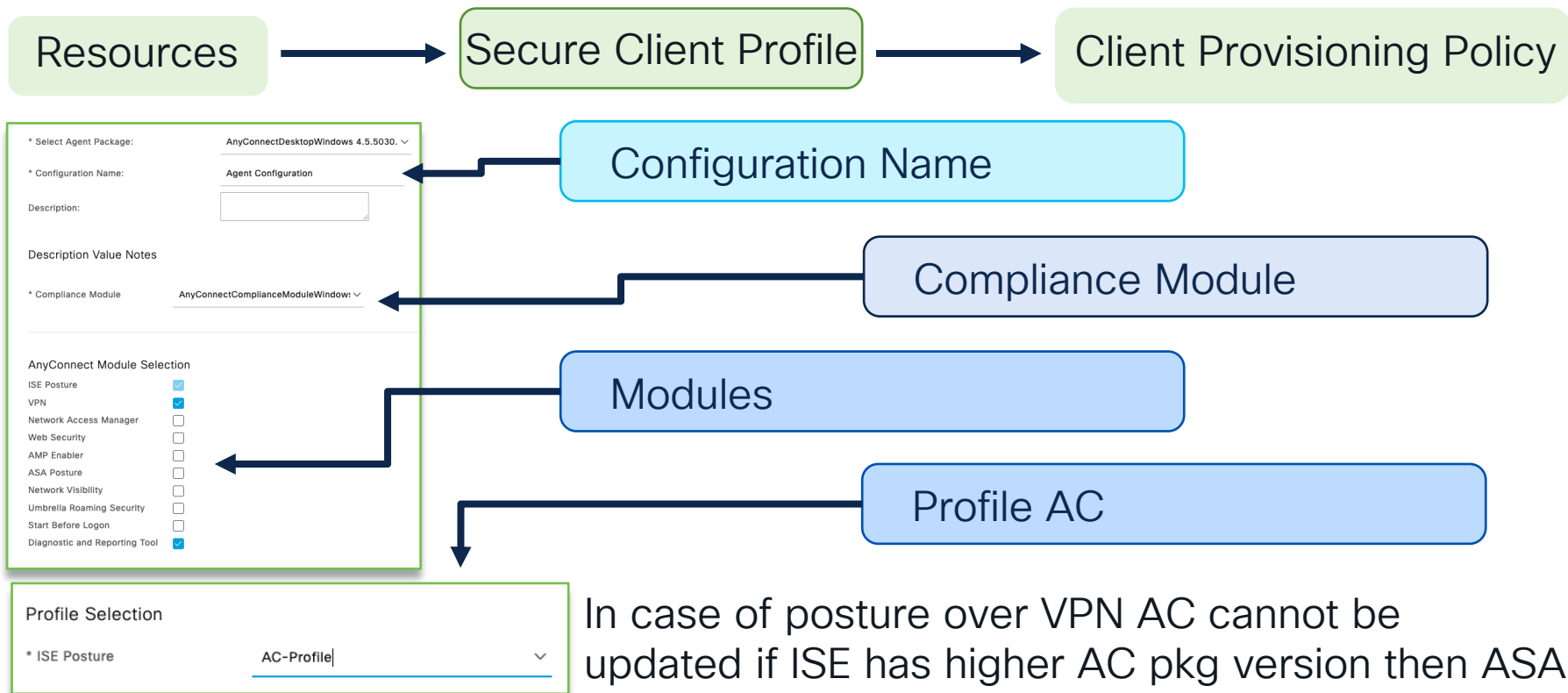
- ISE Posture ☒
- VPN ☒
- Network Access Manager ☐
- Web Security ☐
- AMP Enabler ☐
- ASA Posture ☐
- Network Visibility ☐
- Umbrella Roaming Security ☐
- Start Before Logon ☐
- Diagnostics and Reporting Tool ☒

Profile Selection

* ISE Posture

AC-Profile

Client Provisioning





Client Provisioning

Resources



Secure Client Profile



Client Provisioning Policy

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	
☰	<input checked="" type="checkbox"/> IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP	Edit
☰	<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP	Edit
☰	<input checked="" type="checkbox"/> Windows	If Any	and Windows All	and Condition(s)	CiscoTemporalAgentWindows 5.0.00529 And WinSPWizard 3.2.0.1 And Cisco-ISE-NSP	Edit
☰	<input checked="" type="checkbox"/> MAC OS	If Any	and Mac OSX	and Condition(s)	CiscoTemporalAgentWinOSX 5.0.00533 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP	Edit
☰	<input checked="" type="checkbox"/> Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP	Edit

Specify the
Secure Client
Agent
Configuration

Portal settings adjustment

- **Guest Portal** – posture can be executed as part of the Guest-Flow. This can be done on 'Self-Registered' and 'Sponsored' guest portals. Hot-Spot' portal is not supported for posture.

Posture inside of the Guest-Flow facts:

- Only one check box needs to be enabled in portal settings,
- Only Temporary Agent is supported in client provisioning
- Do not use VLAN change in the authorization profiles for Guests (like authorization profile with redirect has VLAN 10, and compliant authorization profile has VLAN 20) since when MAB is used endpoint cannot detect VLAN change,

Enable posture on the guest portal

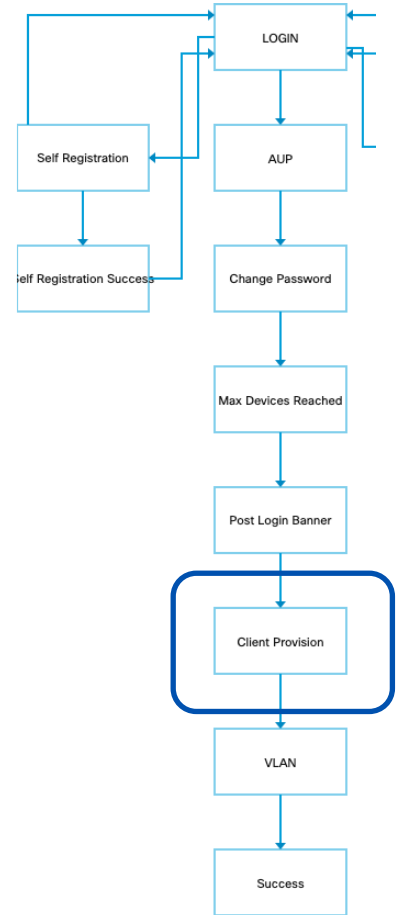
Navigate to **Work Centers > Guest Access > Portal & Components > Guest Portals**

Open portal on which you would like to enable posture and navigate to section 'Guest Device Compliance Settings'. After posture is enabled two additional components are added to the portal 'block diagram' on the right

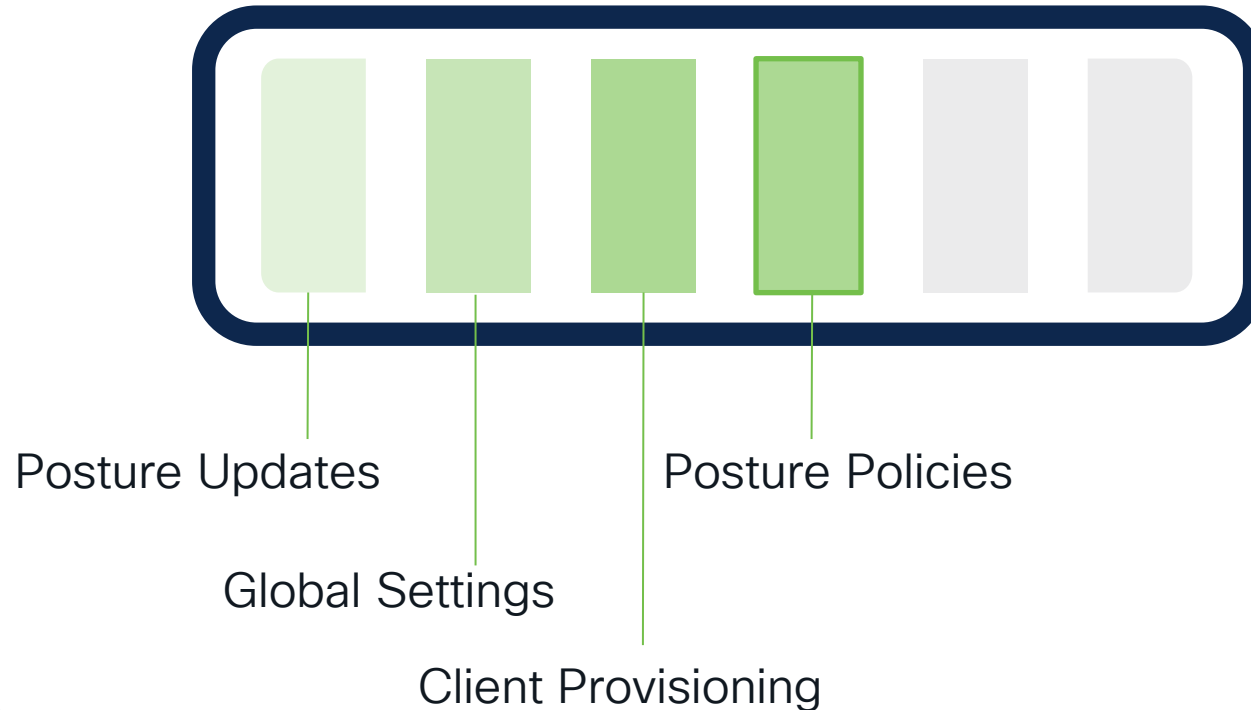
Guest Device Compliance Settings

☒ Require guest device compliance

This will add a Client Provisioning page to the guest flow.



ISE Posture Journey: Configuration



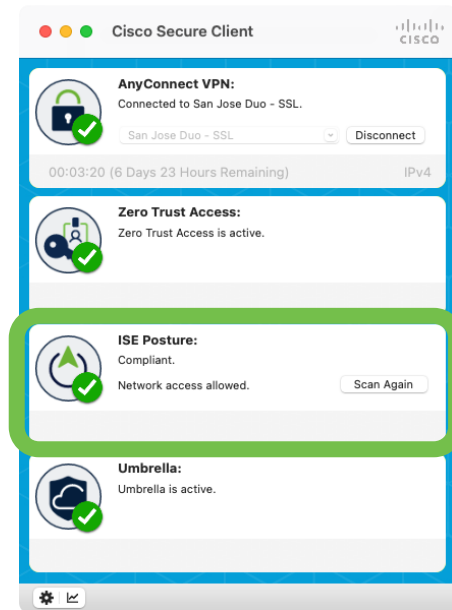
ISE Posture Checks

Condition + Remediation → Requirement

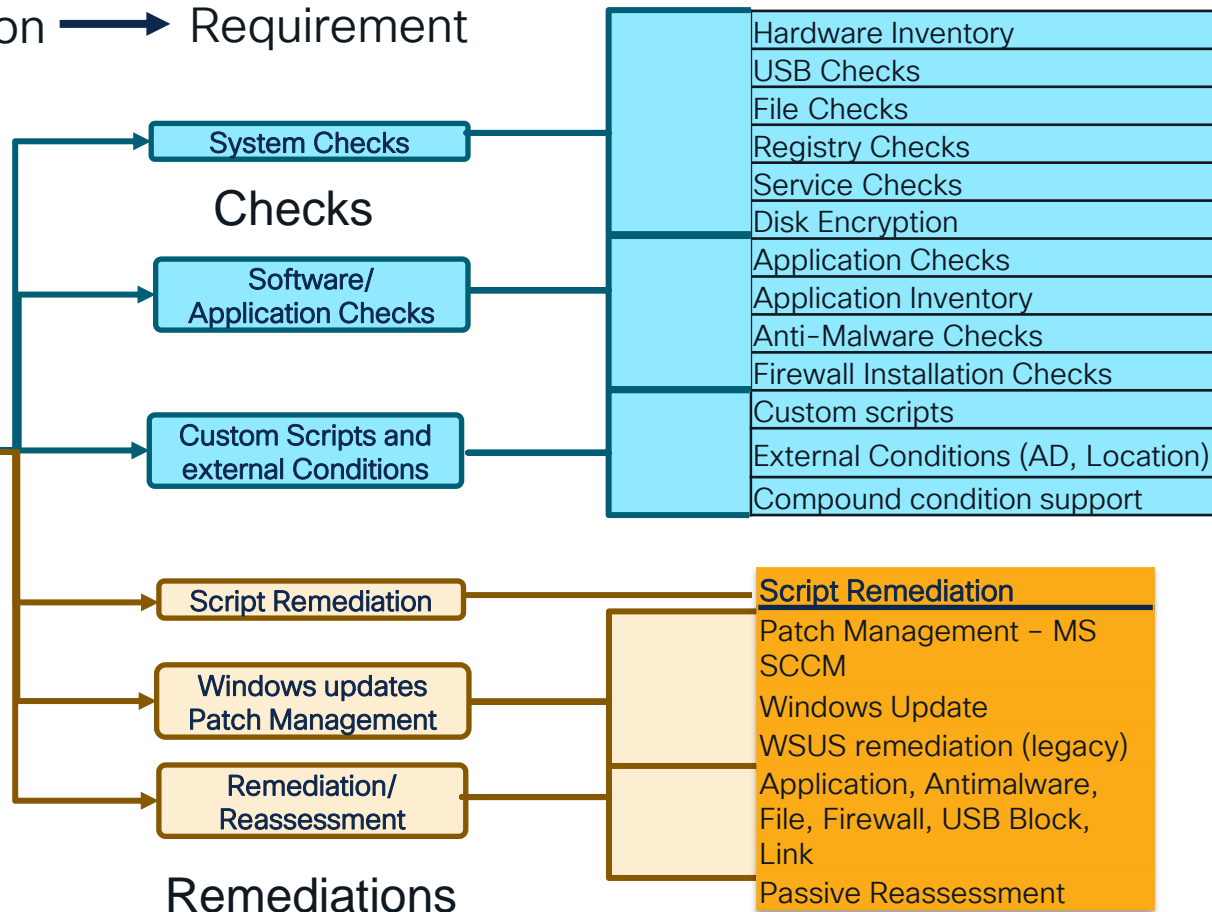


ISE Posture with Cisco Secure Client

Condition + Remediation → Requirement



cisco Live!



ISE Posture Policy

Policy Elements

Policy Sets

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Ma c	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Any_AM_Installation_Ma c Edit ▾
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Ma c_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Any_AM_Installation_Ma c_temporal Edit ▾

Policy Options

Grace period settings

Grace Period for:

0

Minutes



Delay notification by



(0 %) of Grace period.

Agent

Agent Stealth

Temporal Agent

Agentless

Requirements



Any_AM_Definition_Ma

Any_AM_Installation_Ma

Any_AM_Installation_Ma

Default_AppVis_Requirement_Ma

Default_Firewall_Requirement_Ma

Default_Hardware_Attributes_Requirem



Posture Script Condition or Remediation

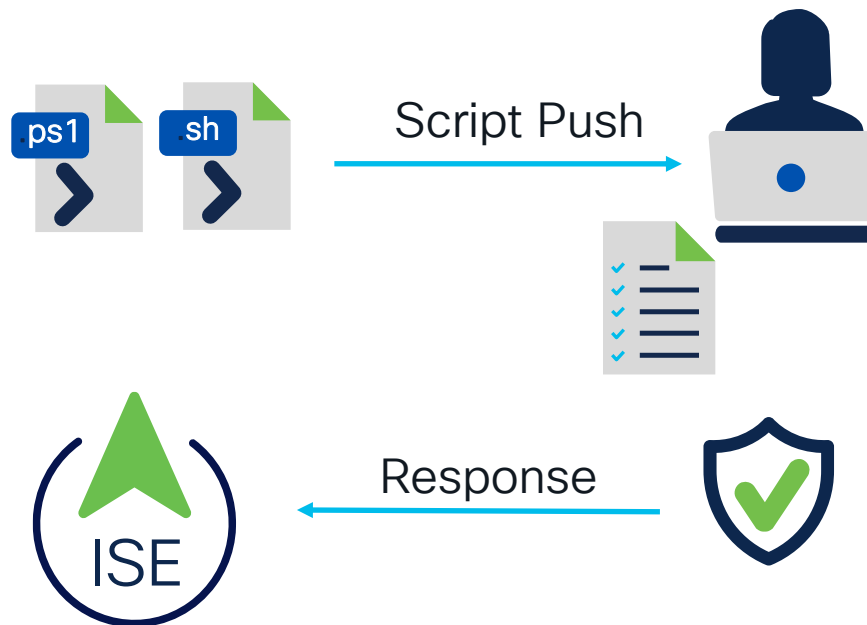
Dynamic requirements

Are all corporate CA certs and
no rogue CA certs installed ?

[...]



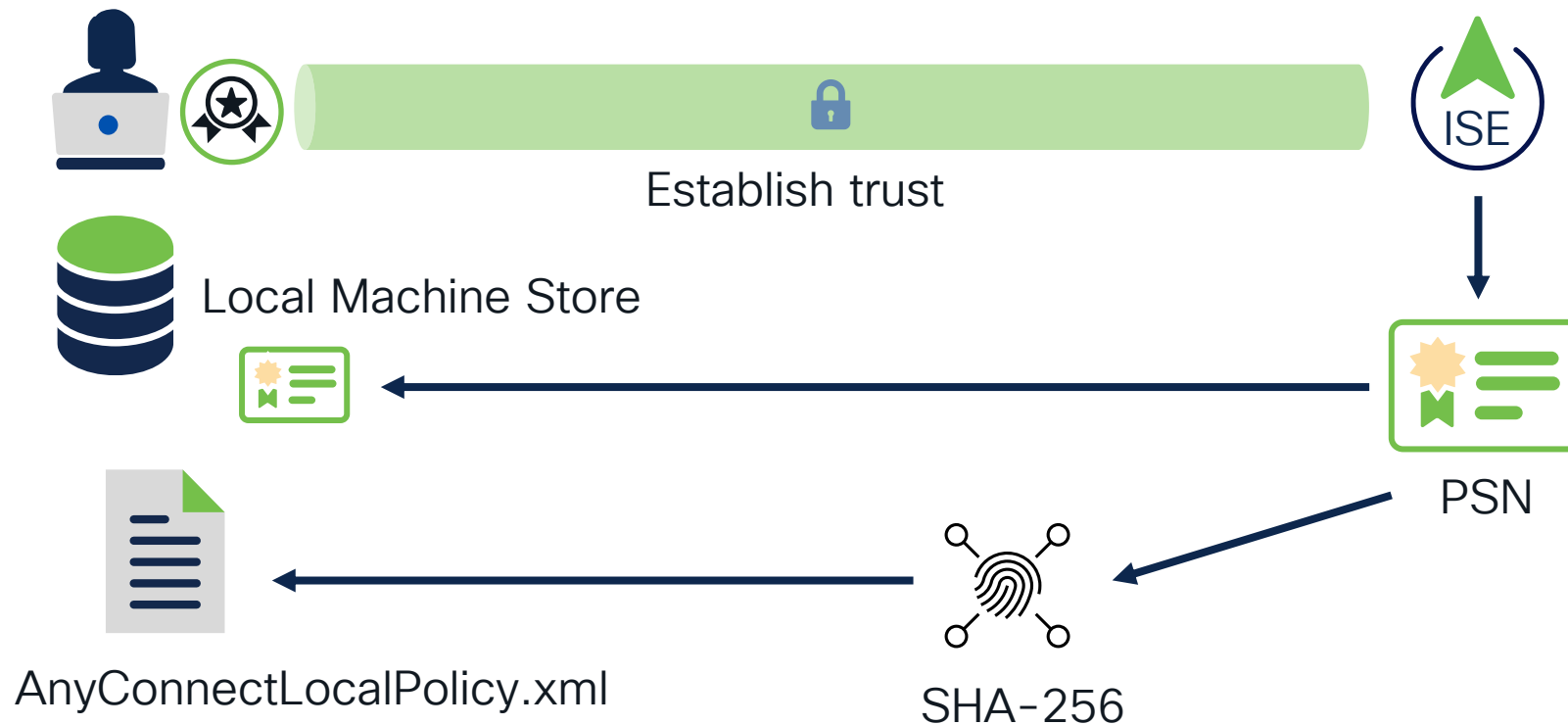
Has the user over-written
network configuration to
use specific DNS ?



New

Posture Script Condition

– Prerequisites



Posture Script Condition

– Prerequisites

New

```
openssl x509 -in 535-pos.crt -fingerprint -noout -  
sha256 SHA256
```



```
Fingerprint=B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:A  
B:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5
```



```
<TrustedISECertFingerprints>  
  <fingerprint>  
    <algorithm>SHA-256</algorithm>  
    <hash>30:5D:A8:0E:3B:36:6C:3A:04:0C:DF:66:D0:3  
B:9B:DE:94:B8:87:ED:17:5F:B7:A4:94:BF:3A:29:A5:7B:35:D0</hash>  
  </fingerprint>  
</TrustedISECertFingerprints>
```

Posture Script Condition

- Configuration

Add Script Condition

Name*

Description

Operating System **Windows**

Script Type
☒ PowerShell ☐ PowerShell Core

File to Upload* No file chosen Choose File
Accepted Files: .ps1

Timeout* 5 1 to 60 (seconds)

Script Condition execution failure or timeout
 Choose what happens to a condition if the script does not exit before the configured timeout or if script execution fails.
 If you choose Pass, the condition is marked as met.
 If you choose Fail, the condition is marked as not met.

☐ Pass ☒ Fail

Windows PowerShell execution policy:

☐ Bypass ☒ AllSigned ☐ None

Endpoint privilege for script execution
 Agentless Posture workflows use Admin privilege and temporal agents use Logged-in User privilege, regardless of the user privilege that you choose for this script.

☒ Administrator / Root ☐ Logged-In User

Exit code

Fail - Other than 0
 Pass- < 0 Pass

Bypass

AllSigned

None



Admin vs Logged-in User

Folder

Posture script condition

- Script Download



New



%LOCALAPPDATA%\Cisco\Cisco Secure Client \scripts



~/ .cisco/iseposture/scripts

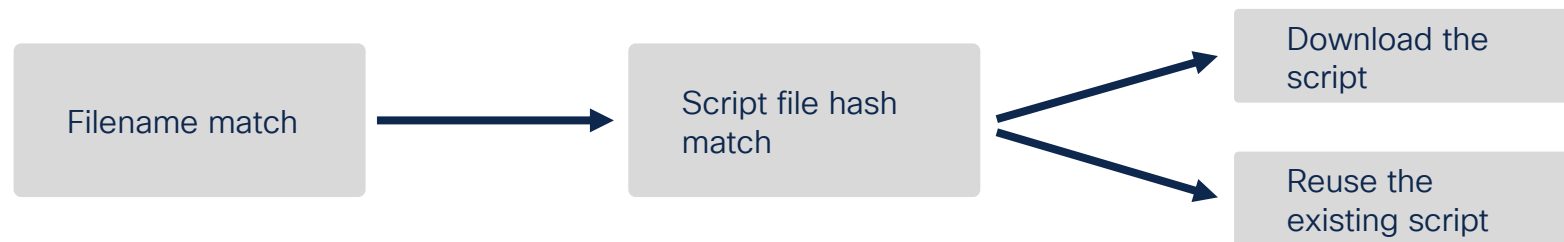
Elevated privileges



%ALLUSERPROFILE%\Cisco\Cisco Secure Client \ISE Posture\scripts



/opt/cisco/Secure Client/iseposture/scripts



Posture script condition

– Exit Code



Exit code



```
4 then
5     echo "Success: File $TESTFILE exist."
6     exit 0
7 else
8     echo "Failed: File $TESTFILE does not exist."
9     exit 1
10 fi
```



Other failure possibilities:



<0 : pre-defined exit code

>0 : user-defined exit code

Script exit code must be
between 0 and 255

Posture Script Exit Codes

Exit Code	Reason
0	Script execution was successful and exited with success
>0	Script execution was successful however, exit code returned the failure code
-1	Script execution check wasn't attempted
-2	Data integrity failed
-3	Error in Script download
-4	Script has verification failed
-5	Script executed, however, Script execution didn't complete within specified timeout
-6	Generic failure (not covered as part any failures)
-7	Script type is not supported
-8	Script failed to launch
-9	ISE certificate is not trusted

Remember: in case script exit code is out of bound then it is set to 255

Endpoint Posture Attributes – Grace Period



Grace period feature allows endpoint to get a 'Compliant' network access when it become Non-Compliant after being compliant in the past

Functionality is based on two attributes:

PostureLastCompliantExpiry – attribute has a Unix Epoch format. Grace period starts if posture status got changed to non-compliant within Last Known Posture Compliant State

☒ **Cache Last Known Posture Compliant Status**

Last Known Posture Compliant State

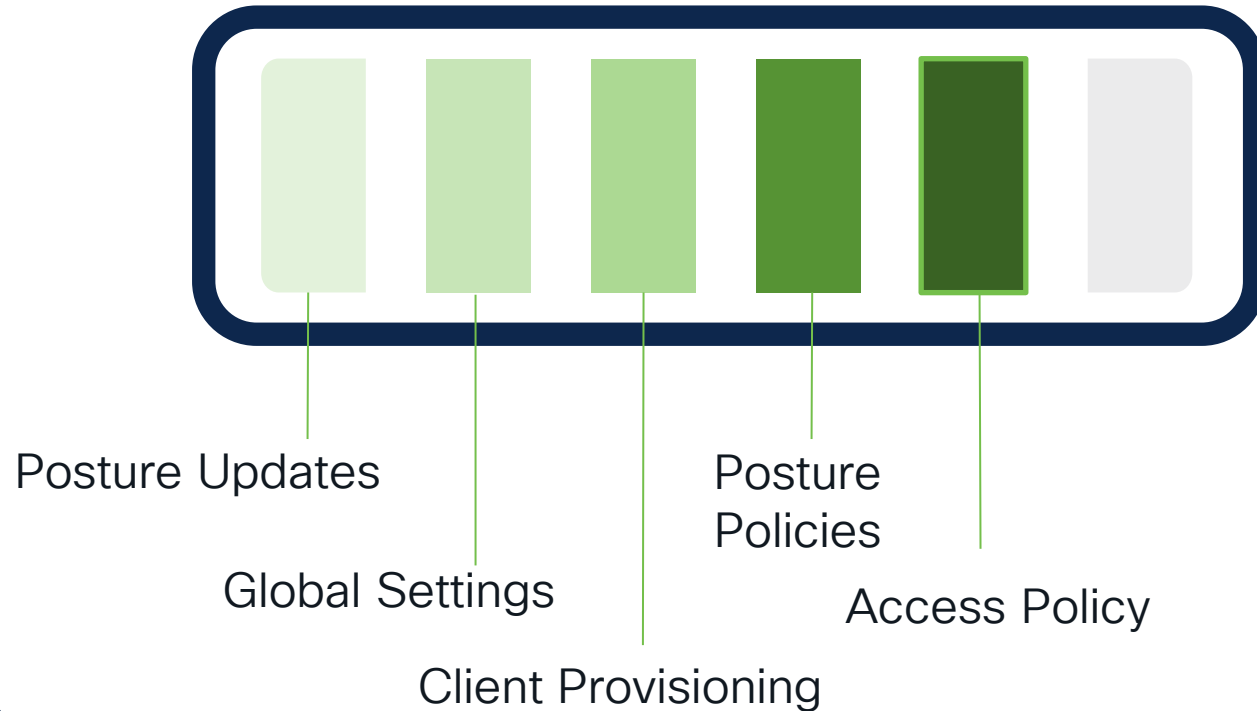
7

Days

Remaining Grace Period * – stored in oracle config DB table in special table. ISE starts populating LAST_GRACE_EXPIRY after endpoint has been marked as non-compliant while being within Last Known Posture Compliant State

* – While Grace Period feature itself has been added in 2.4 we started to store **Remaining Grace Period** in Oracle DB starting from 2.6. In 2.4 **Remaining Grace Period** stored in special In-Memory cache.

ISE Posture Journey: Access Policy



Access Policies – Redirect Chaining

We need to redirect our clients to the Client Provisioning Portal, provide access or deny it.

✓	Posture Compliant	Session-PostureStatus EQUALS Compliant	Posture_Compliant	+	Compliant	⚙
✓	Posture Non Compliant	Session-PostureStatus EQUALS NonCompliant	Posture_NonCompliant	+	NonCompliant	⚙
✓	Posture Unknown	Session-PostureStatus NOT_EQUALS Compliant	Posture_Unknown	+	Unknown	⚙

* Name: Agent-Posture-Redirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: ☐

Track Movement: ☐ ⓘ

Agentless Posture: ☐ ⓘ

Passive Identity Tracking: ☐ ⓘ

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

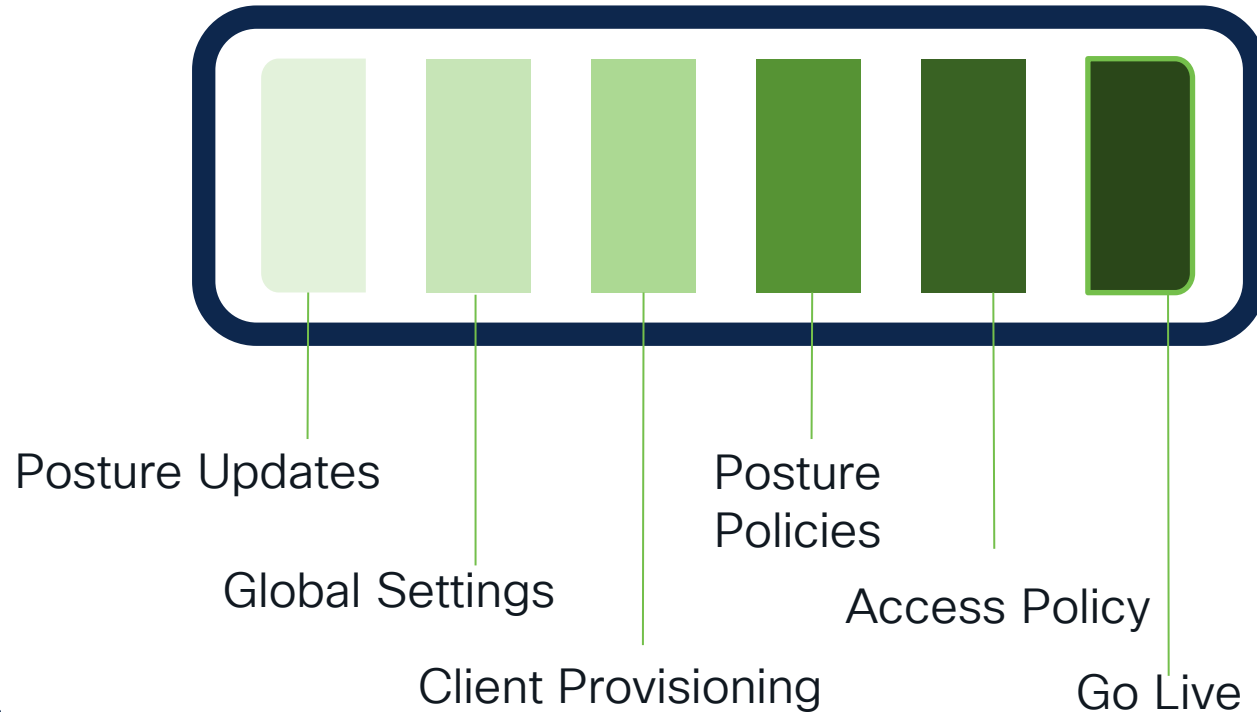
Client Provisioning (Posture) ACL redirect-posture Value Client Provisioning Portal (def:)

☐ Static IP/Host name/FQDN

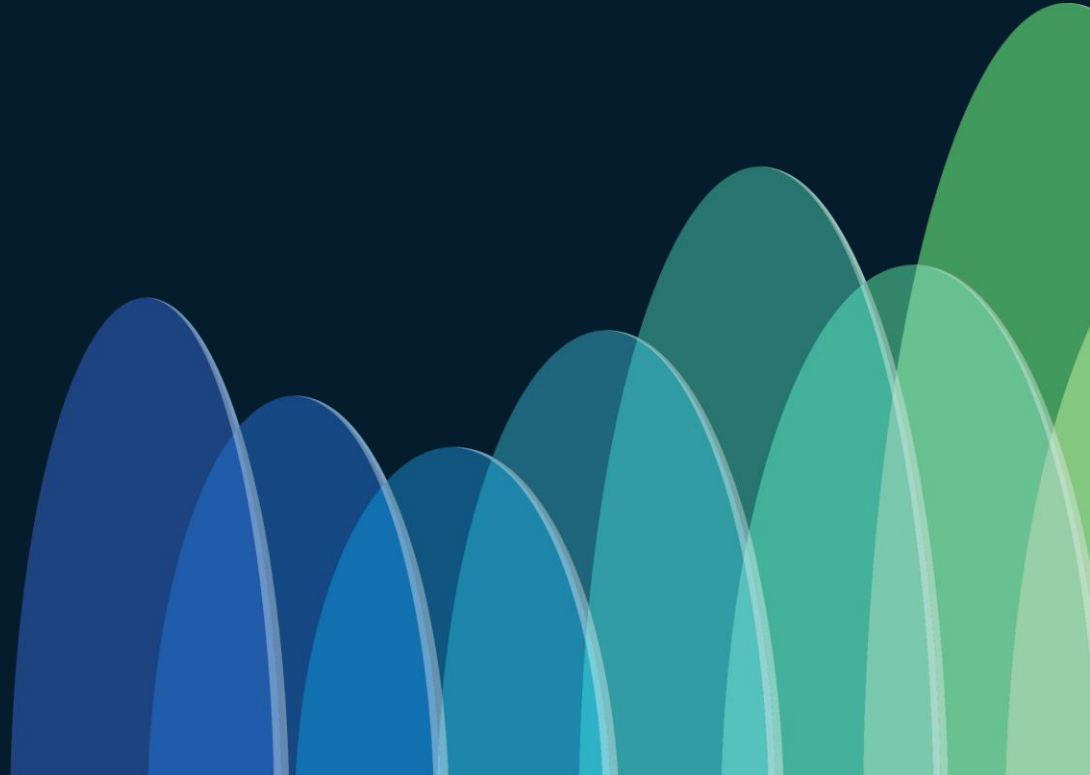
☐ Suppress Profiler CoA for endpoints in Logical Profile

Must exists on NAD

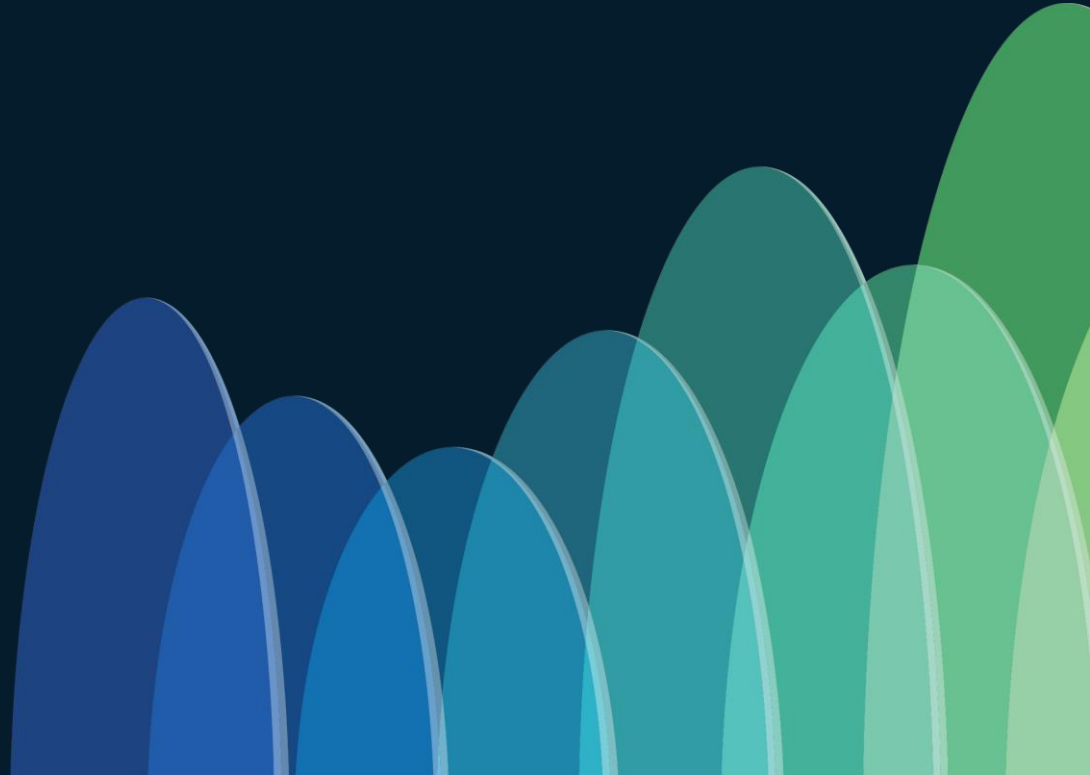
ISE Posture Journey: Time to Go Live



Advanced Posture Processes



Misconception 2: Discovery Process



Posture Discovery and Authentication

“Every time when dot1x authentication happens, Discovery process is restarted by the ISE posture module”





Every time when dot1x authentication happens, Discovery process is restarted by the ISE posture module

① Start presenting to display the poll results on this slide.

Demo – Identification



Discovery



Power Events



User Login



Initial AC
Installation



Return
sleep



Default GW
change



Interface
Up

Posture files – Connection Data

- ConnectionData.xml file created on the first posture attempt
- For every primary record you have a <time> tag
- Every next server is added as a separate Primary record

```
<?xml version="1.0" ?>
<records>
  <record>
    <primary>ise-p.lab.com</primary>
    <port>8443</port>
    <status_path>/auth/status</status_path>
    <ng-discovery>/auth/ng-discovery</ng-discovery>
    <time>1702031250</time>
    <backups>
      <backup>ise-s.lab.com</backup>
    </backups>
  </record>
  <record>
    <primary>ise-s.lab.com</primary>
    <port>8443</port>
    <status_path>/auth/status</status_path>
    <ng-discovery>/auth/ng-discovery</ng-discovery>
    <time>1702030758</time>
    <backups>
      <backup>ise-p.lab.com</backup>
    </backups>
  </record>
</records>
```

ConnectionData.xml

What does 'Discovery' mean and how to start it?

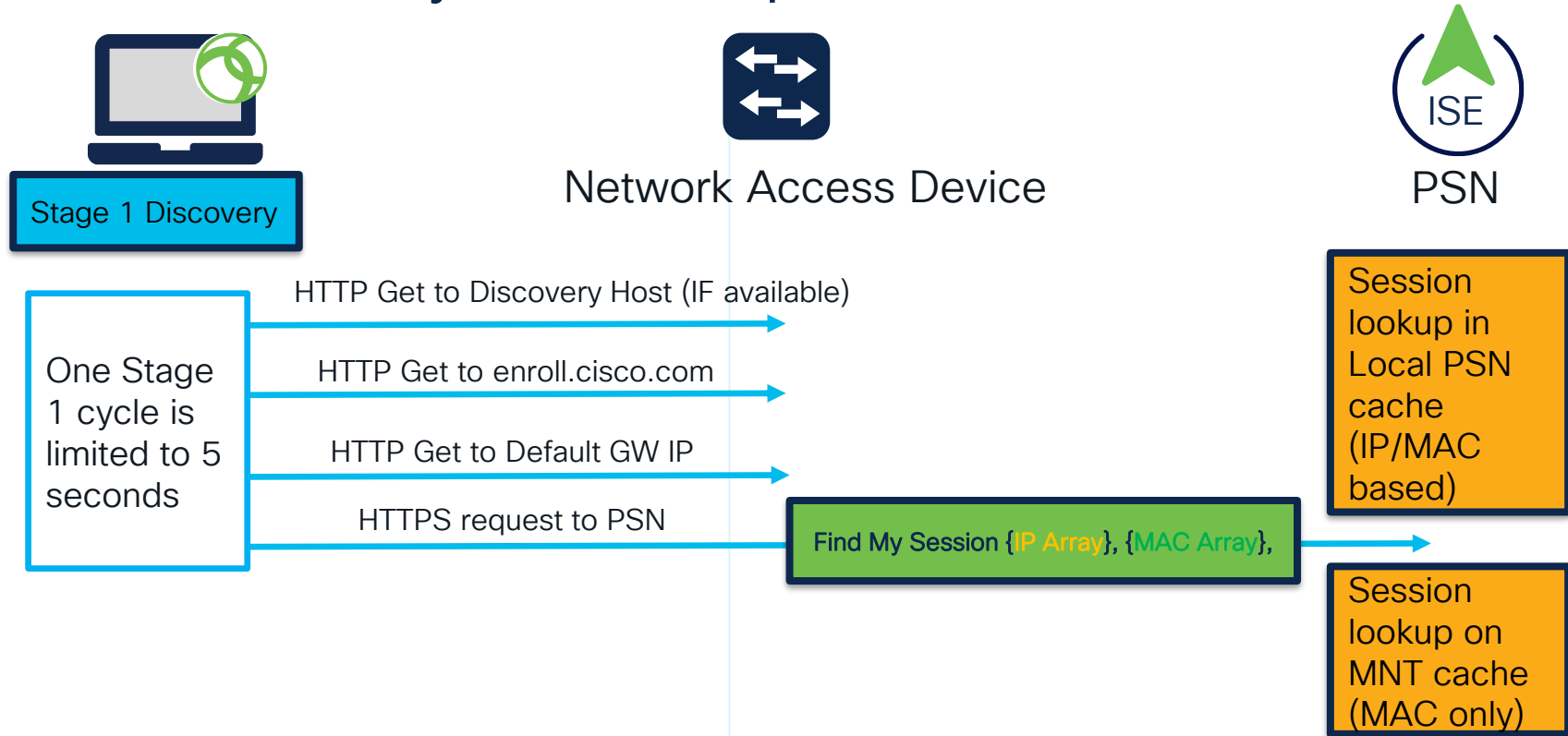
Discovery* is a process executed by AC ISE posture module to locate PSN where user/device has been authenticated. After correct PSN is located agent will check for client provisioning policy on PSN (to see if any updates are needed) and will request posture requirements which needs to be validated.

Discovery starts on:

- Initial AC posture module installation
- User login,
- Power events,
- Interface is going up,
- Return device from sleep,
- Default Gateway change

Note: Dot1x authentication and PC lock/unlock are not triggering Discovery process.

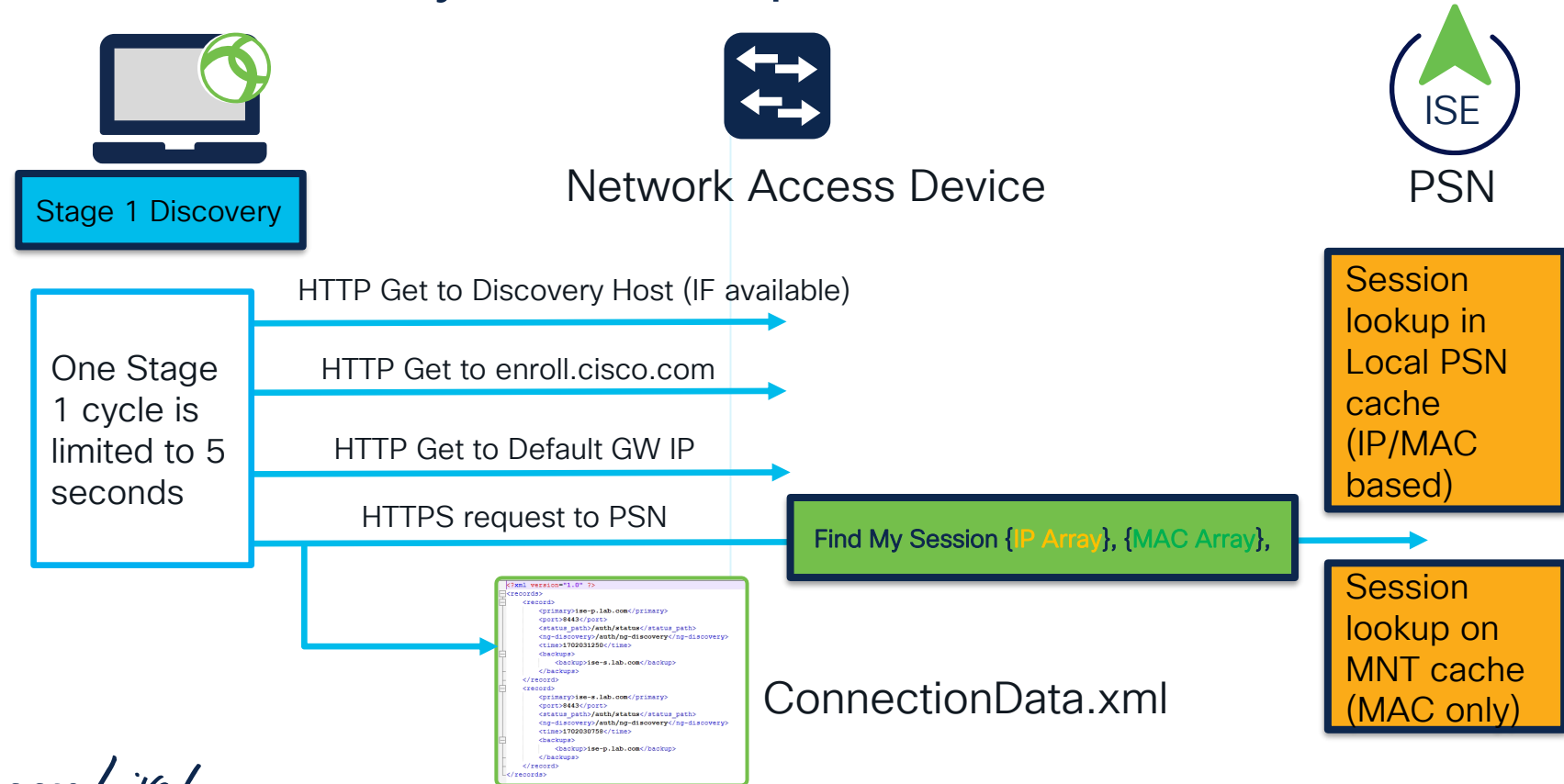
PSN discovery Redirect probes



PSN discovery Redirect probes



PSN discovery Redirect probes



ISE Configuration Details – Redirection

Discovery Host

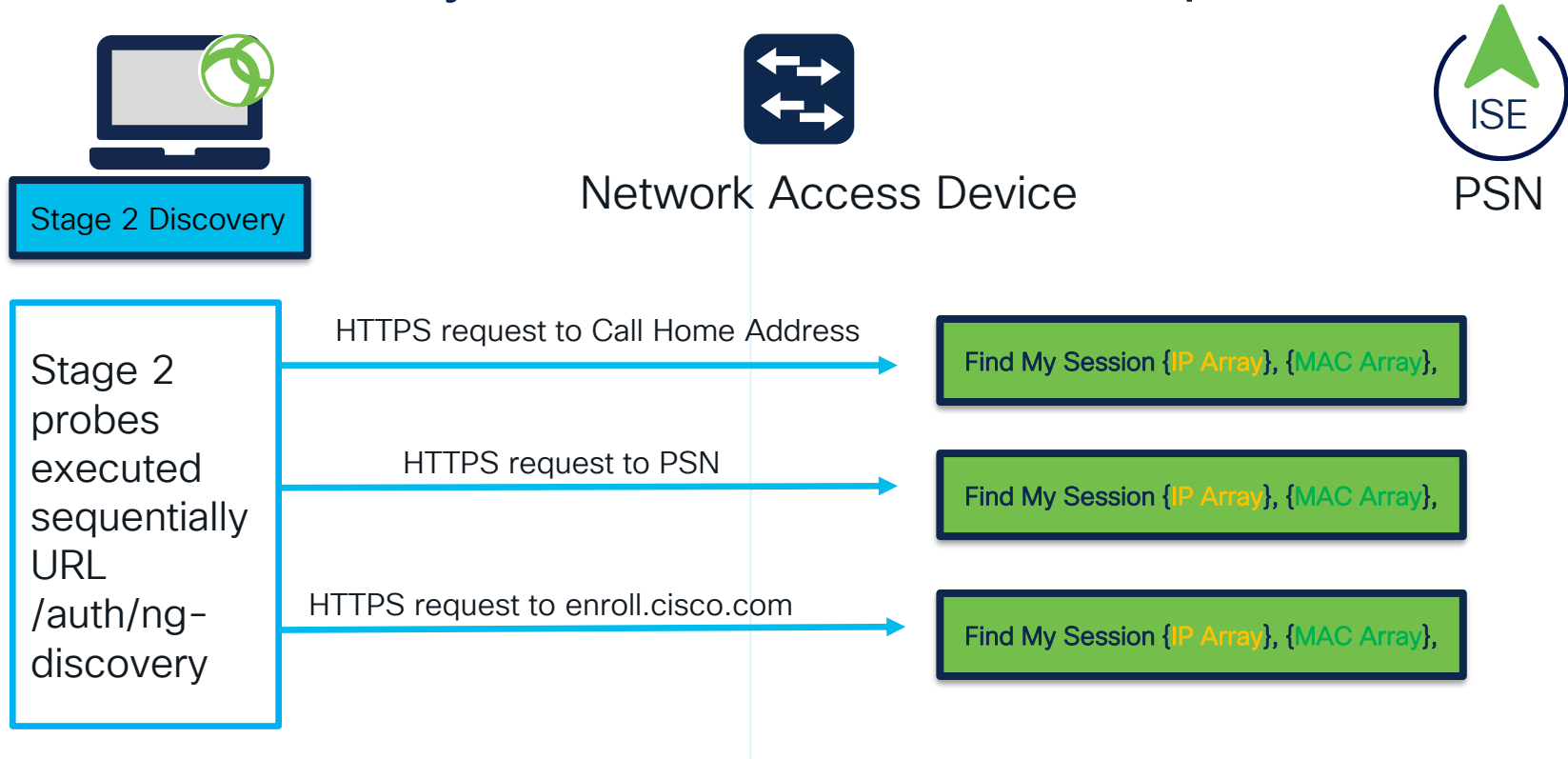
Any IP/FQDN routed through the NAD

Server Name Rules

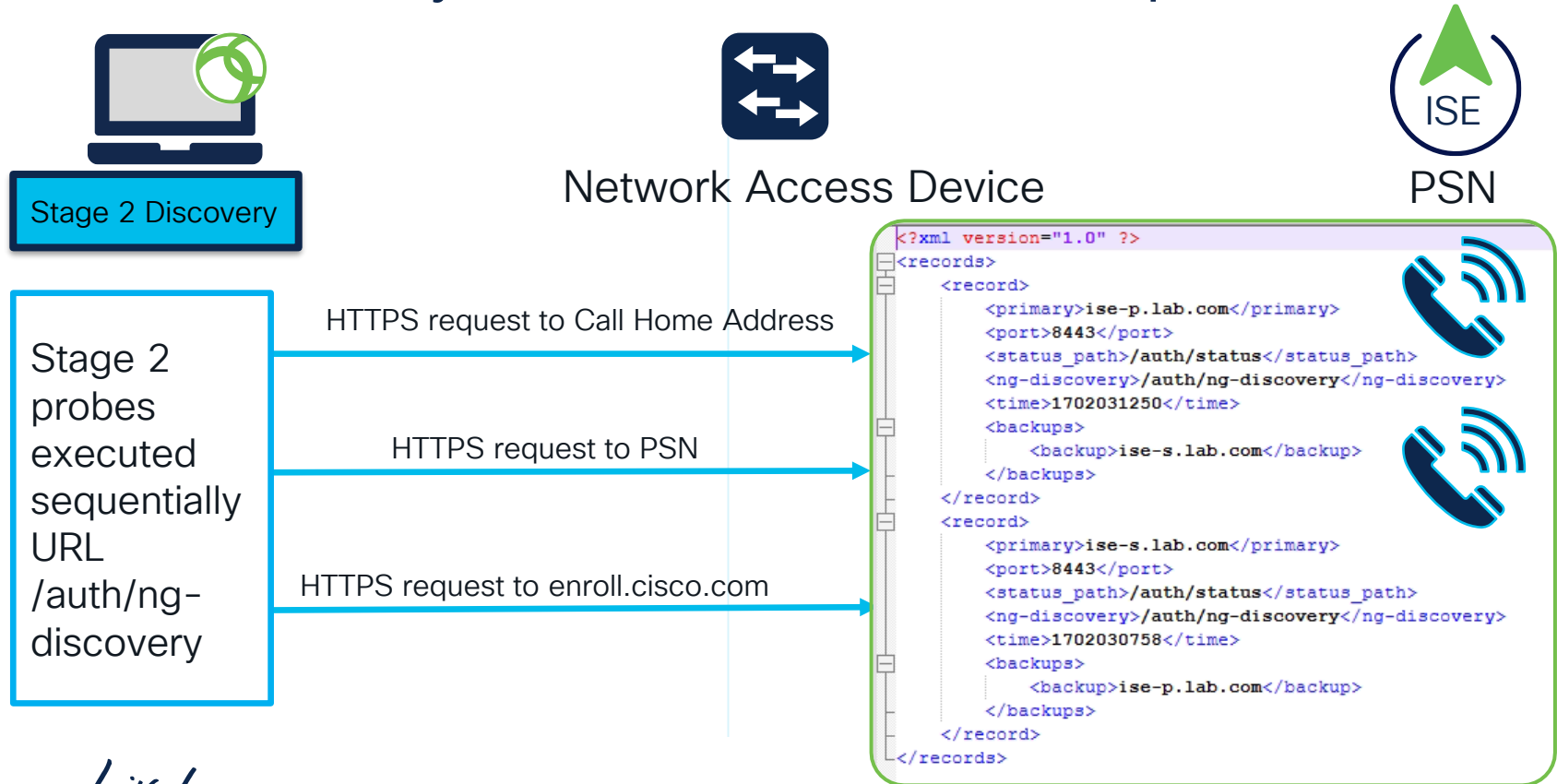
Wildcard of allowed Servers

In case of Split Tunnel – Redirection has to go through the tunnel

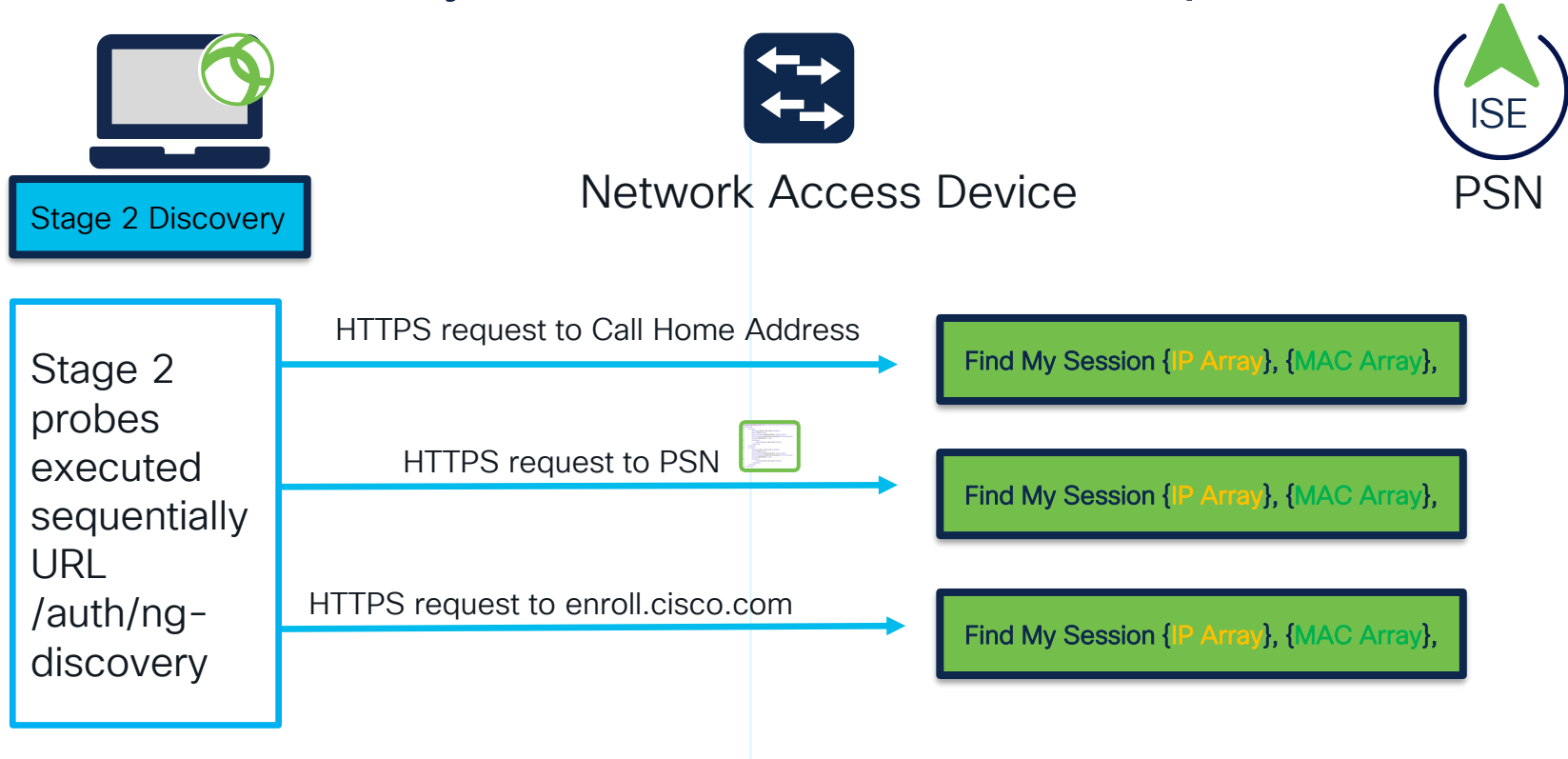
PSN discovery Non-Redirect based probes



PSN discovery Non-Redirect based probes



PSN discovery Non-Redirect based probes



ISE Configuration Details - Redirectionless

Discovery Host

~~Any IP/FQDN routed through the NAD~~

Server Name Rules

Wildcard of allowed Servers

Call Home List

IP Address List to have contact with

In case of Split Tunnel - Probes have to go through the tunnel

ISE Configuration Details – Non-Redirect

First deployment – No ConnectionData



ConnectionData.xml



ISEPostureCFG.xml

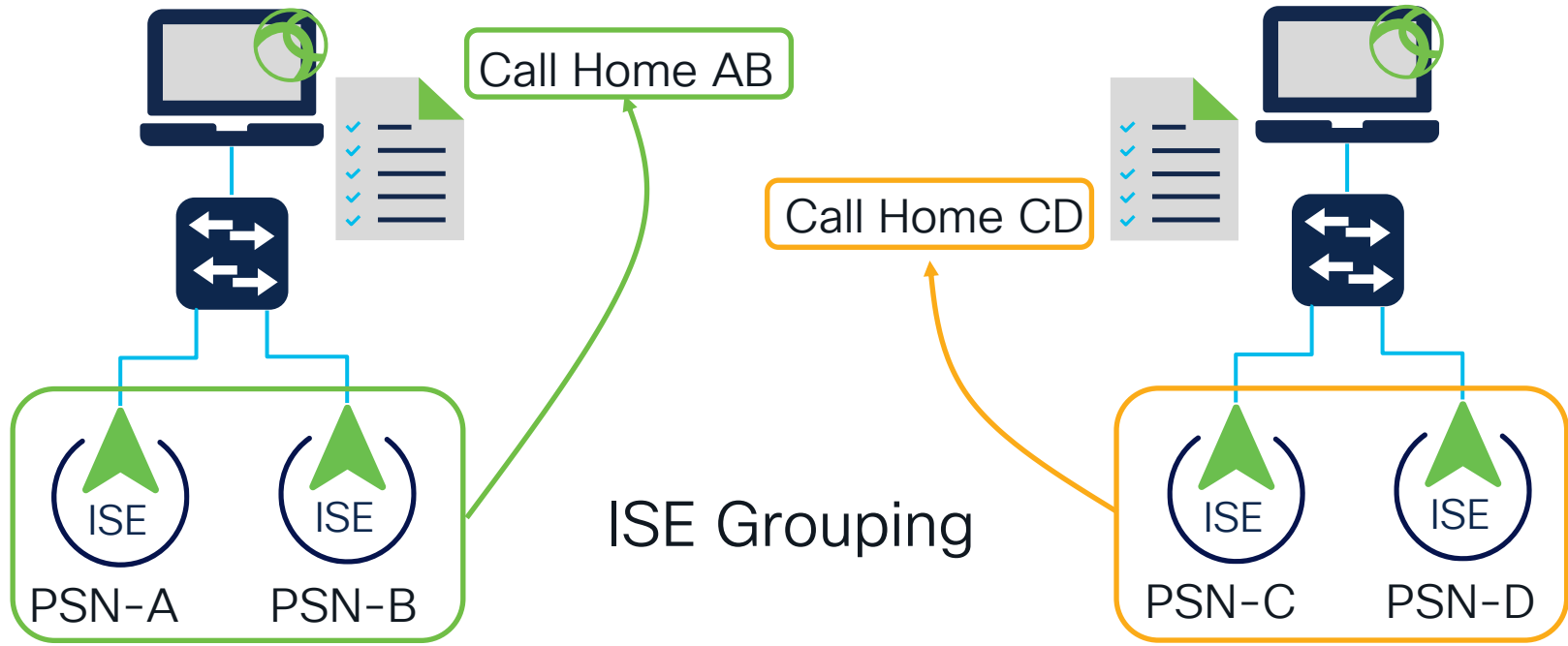
```
<ServerNameRules>*.lab.com</ServerNameRules>
```

```
<discoveryPsnList>ise-  
s.lab.com,ise-  
p.lab.com</discoveryPsnList>
```

```
<CallHomeList>10.52.X.X,10.52.X.X<  
/CallHomeList>
```

ISE Configuration Details – Non-Redirect

Design for Big Deployment




ISE Configuration Details – Redirectionless

Multiple Profiles creation

The screenshot displays the 'Profile Editor' interface in Cisco ISE. The top section shows 'Preferences' for a 'Profile: Untitled'. A blue box highlights the 'Profile Editor' title, and an orange box highlights the 'Enable extra probes so non-redirection flow can work' setting, which is set to 'Yes' with a dropdown arrow. A green arrow points from this setting to the 'Enable Posture Non-Redirection Flow' checkbox in the 'Agent Behaviour' section, which is checked. The 'Call Home List' section at the bottom contains a text input field with the value 'psn1, psn2'.

Preferences
Profile: Untitled

Profile Editor

Enable extra probes so non-redirection flow can work Yes  **ISE**

NAC Profile Editor

Agent Behaviour

- Enable Signature Check ☐
- Enable Agent Log Trace ☐
- Operate On Non-802.1X Wireless Networks ☐
- Enable Posture Non-Redirection Flow ☒



Call Home List

ISE Configuration Details - Redirectionless

Network Device Group

<input type="checkbox"/> ▾ Posture	--
<input type="checkbox"/> Redirection NAD	0
<input type="checkbox"/> Redirectionless NAD	0

Policy Set

✓	Posture Redirectionless Unknown	 DEVICE·Posture EQUALS Posture#Redirectionless NAD
✓	Posture Redirection Unknown	 DEVICE·Posture EQUALS Posture#Redirection NAD

Common misconception #1: Session Sharing

Session Sharing

“Session context is shared within ISE deployment so PSN can run posture even when authentication hit another node”



Node Group



Light Session Directory

slido



Is session context shared
within ISE deployment ?

① Start presenting to display the poll results on this slide.

Session management - theory walkthrough

Who is responsible for session management in ISE deployment?



Sessions are created:



Sessions are updated:



Session management - theory walkthrough

Who is responsible for session management in ISE deployment?

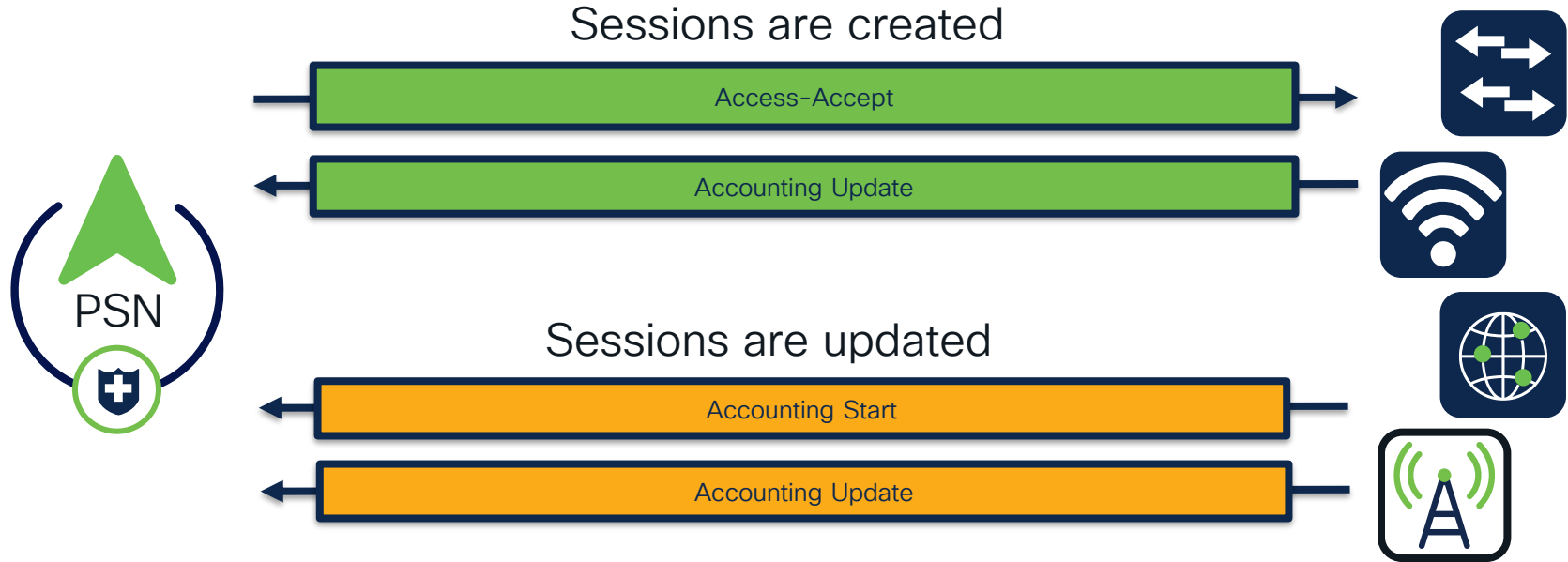


Session removal:

- Sessions after 15 without accounting start (**Authenticated**) removed after 60 minutes,
- Sessions with accounting stop (**Terminated**) removed minutes
- Sessions in '**Started**' state (MNT got accounting start) removed after 120 hours without Interim update.

Session management - theory walkthrough

Who is responsible for session management in ISE deployment?



Session management – theory walkthrough

Who is responsible for session management in ISE deployment?



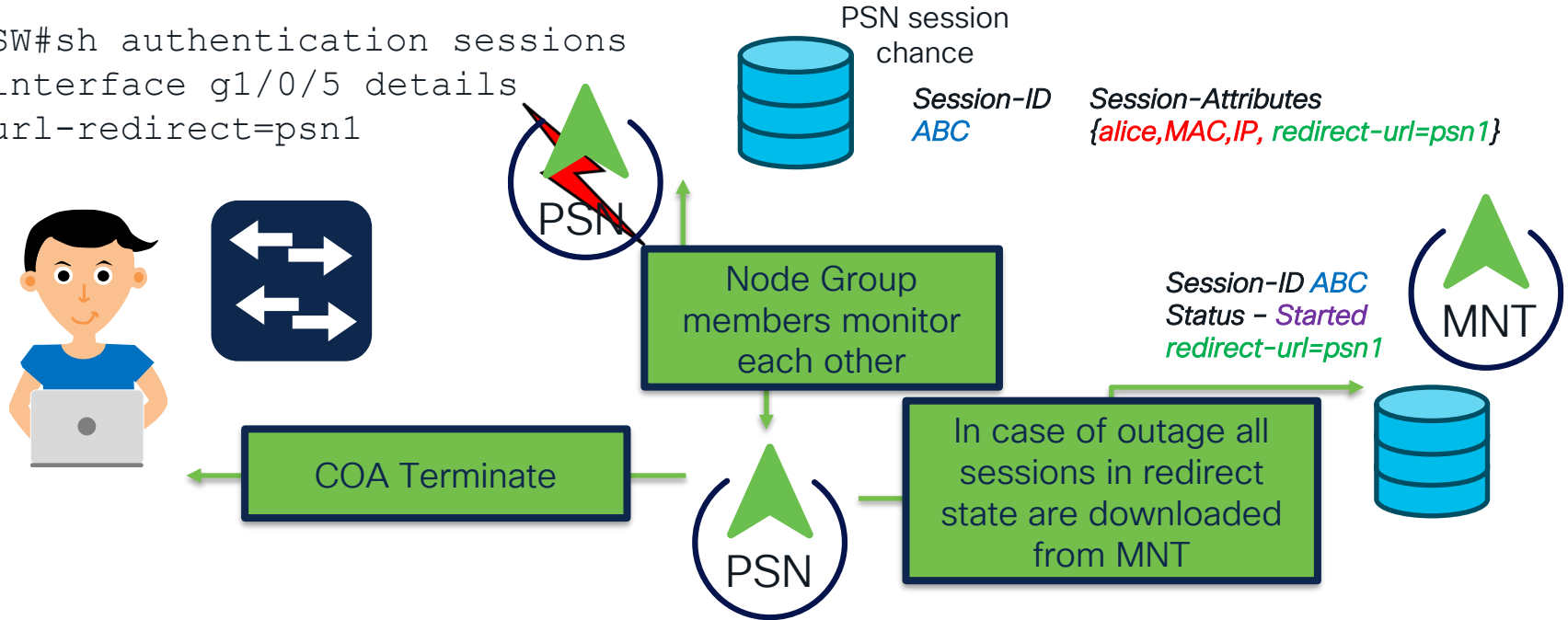
Rules for sessions removal

- a. Sessions are removed upon processing Accounting stop
- b. Least recently used sessions are removed after reaching platform [limit](#)
- c. Session cache is cleared upon PSN reload or Application Server restart

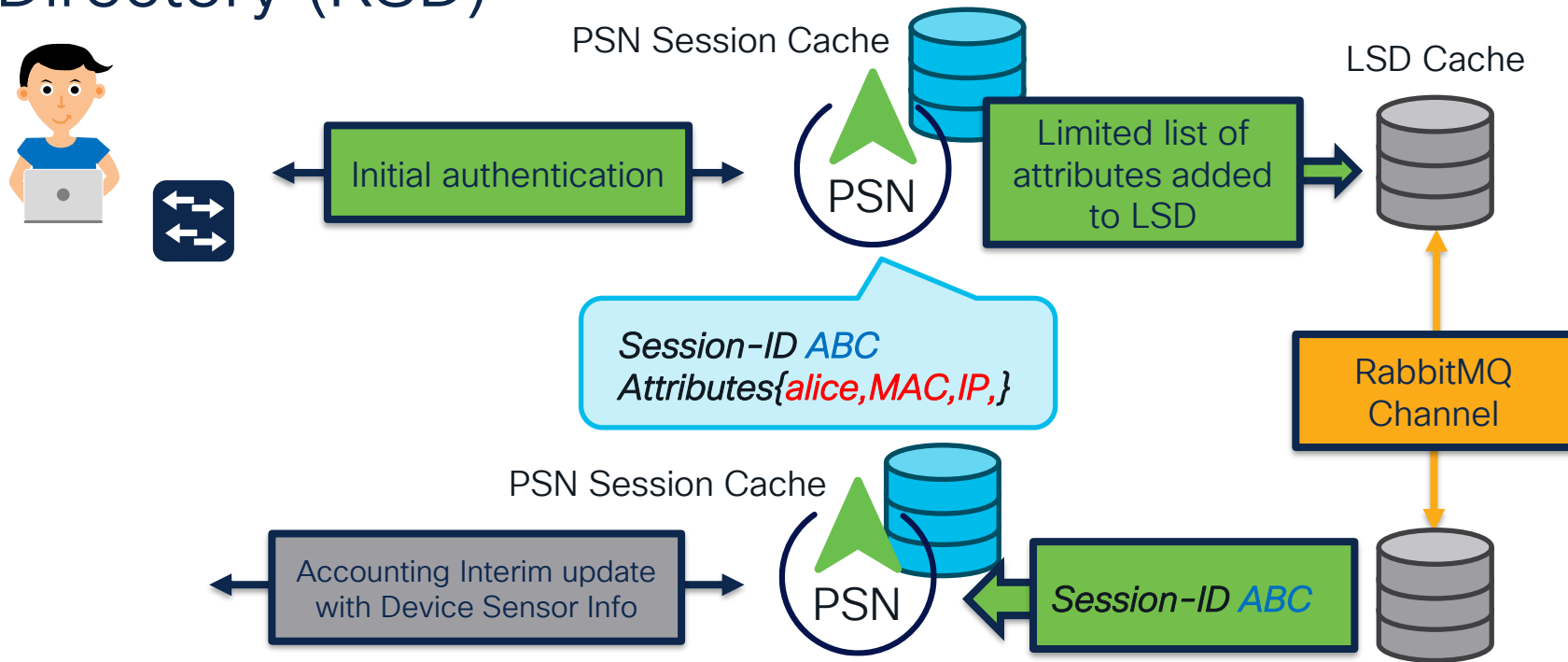
Node Group

Main idea behind is to minimize amount of global replication events

```
SW#sh authentication sessions  
interface g1/0/5 details  
url-redirect=psn1
```

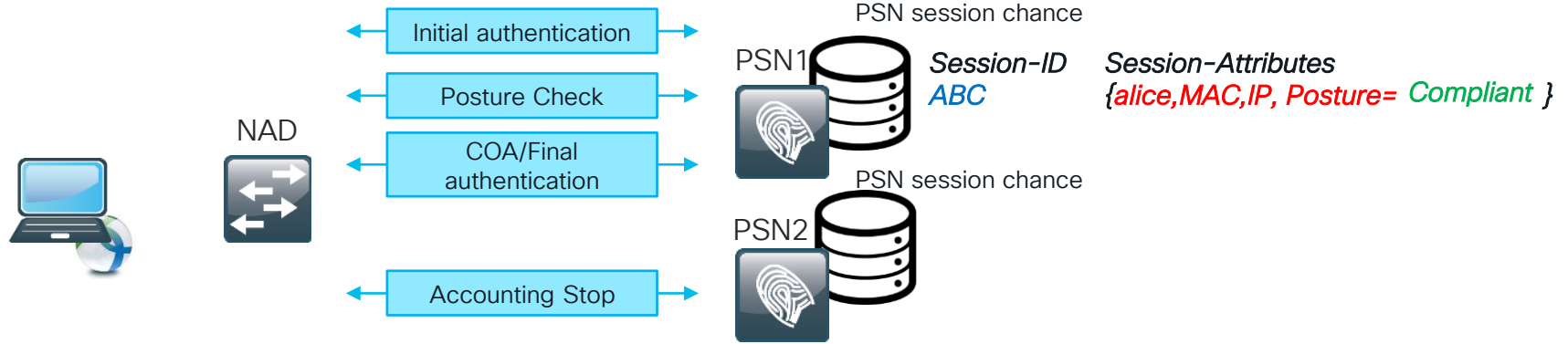


Light Data Distribution (LDD) Radius Session Directory (RSD)

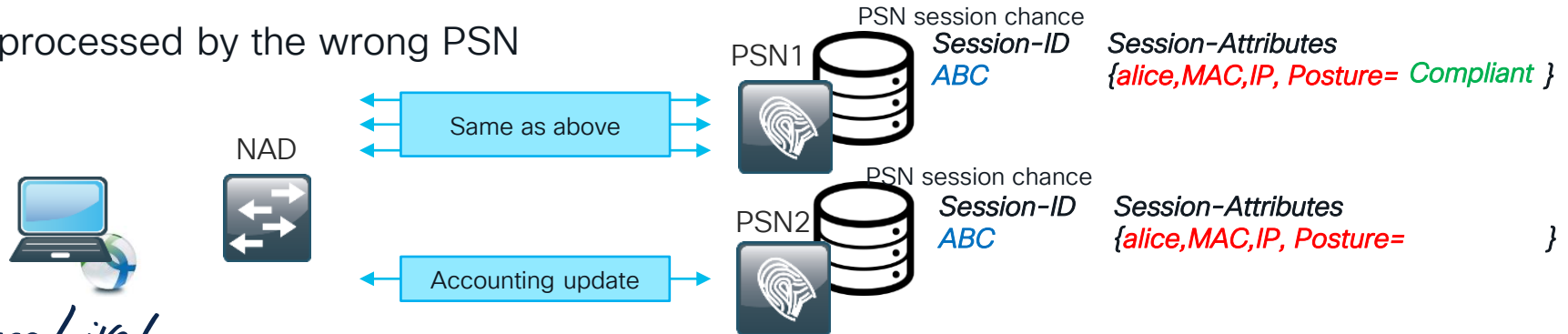


Session management - What it brings

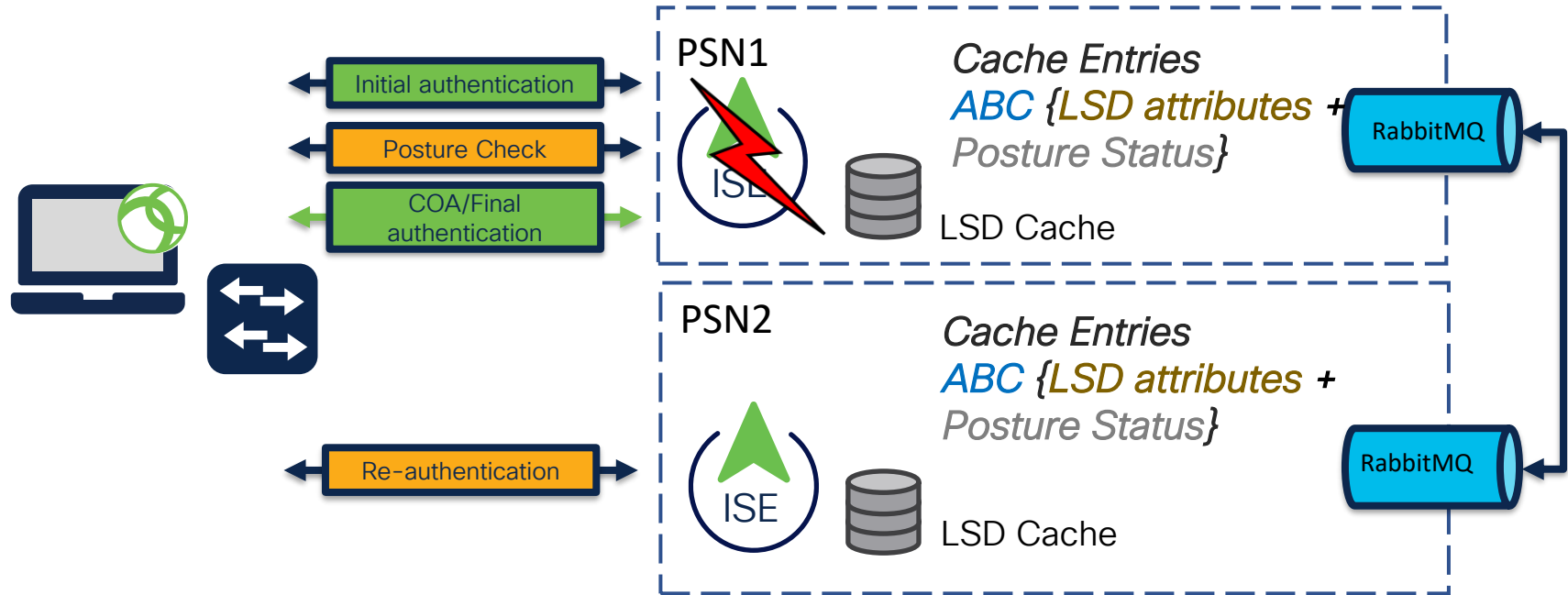
Stale session - a scenario when accounting stop was processed by the wrong PSN



Phantom session - scenario when one of the accounting interim update packets was processed by the wrong PSN



How Light Data Distribution (LDD) solve posture problems - #1



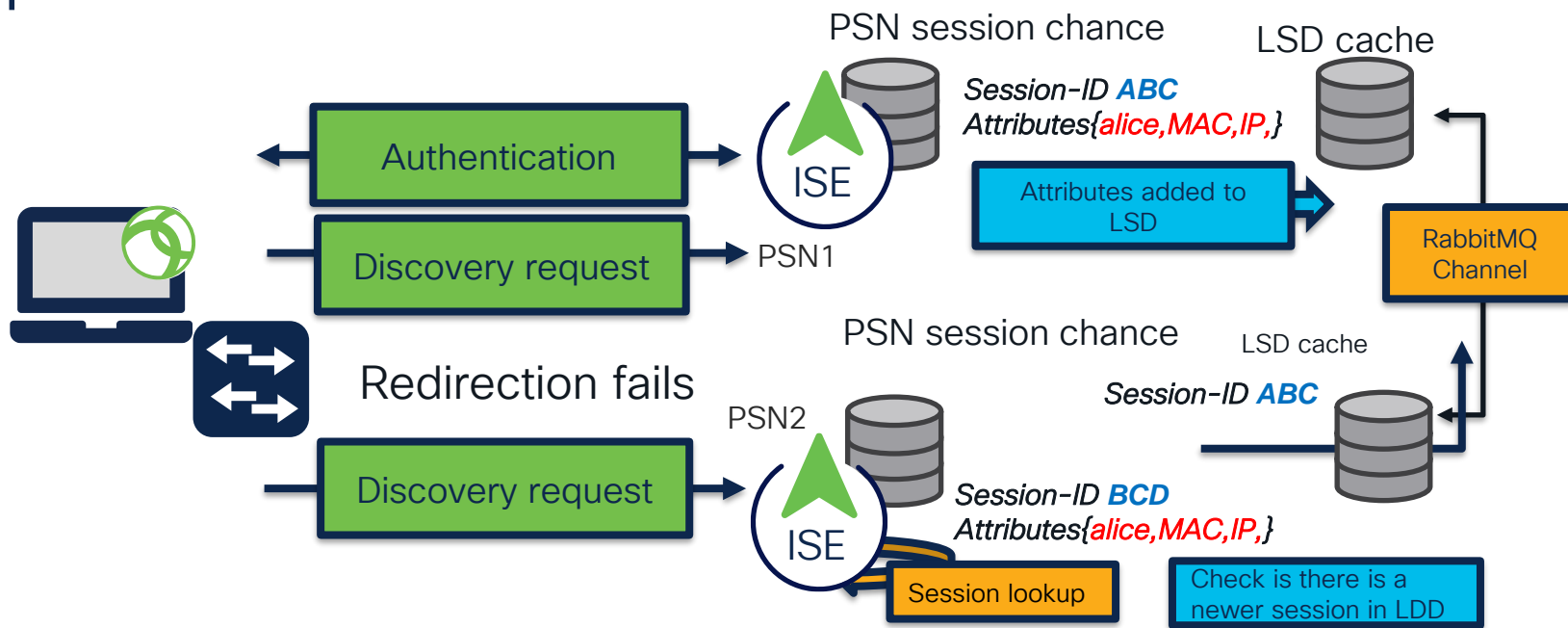
Reauthentication to different PSN

1. Endpoint authenticates to PSN1, posture is performed and user gets compliant access
2. **Posture lease is not configured**
3. **PSN1 becomes unavailable**
4. Reauthentication is triggered from NAD
5. As discovery is not triggered on the endpoint, status on **AC remains compliant**
6. Access request is sent to PSN2 and the endpoint gets posture unknown access
7. PSN2 doesn't receive a posture report and the session remains at **posture pending status on ISE**



1. Endpoint authenticates to PSN1, posture is performed and user gets compliant access
2. Posture lease is not configured
3. **Posture status** is shared through RSD
4. PSN1 becomes unavailable
5. Reauthentication is triggered from NAD
6. As discovery is not triggered on the endpoint, status on AC remains compliant
7. Access request is sent to PSN2 and PSN2 identifies the endpoint **posture status is compliant by looking into RSD**
8. The endpoint gets **compliant access**

How Light Data Distribution (LDD) solve posture problems - #2



Stale/Phantom Session

1. **Redirection fails**
2. Connectiondata probes reach two or more PSNs
3. **PSN with stale/phantom session responds** before real session owner
4. Posture scan is initiated on **AC and returns compliant**
5. As the report is not sent to the authenticating PSN, CoA is never triggered and the session remains at **posture pending status on ISE**



0. **and PSN** where authentication happened are shared through RSD
1. Redirection fails
2. Connectiondata probes reach two or more PSNs
3. **PSN with stale/phantom** identifies the latest session for the endpoint in RSD and **doesn't respond**
4. The PSN that authenticated the endpoint responds to discovery probe
5. Posture scan is initiated, report is sent to authenticating PSN, CoA is triggered and user gets **compliant access**

How Light Data Distribution (LDD) solve posture problems

In case when stale/phantom session is detected you can see following messages in the guest.log

```
2020-04-08 13:30:48,217 DEBUG [https-jsse-nio-192.168.43.226-8443-exec-4][ ] cisco.cpm.client.posture.Util -::-  
Local session 0A3E946C0000007D5B679296 is stale. Newer session for 00-50-56-B6-0B-C6 is  
0A3E946C000000805B7C43A3. Owned by skuchere-ise26-1.example.com
```

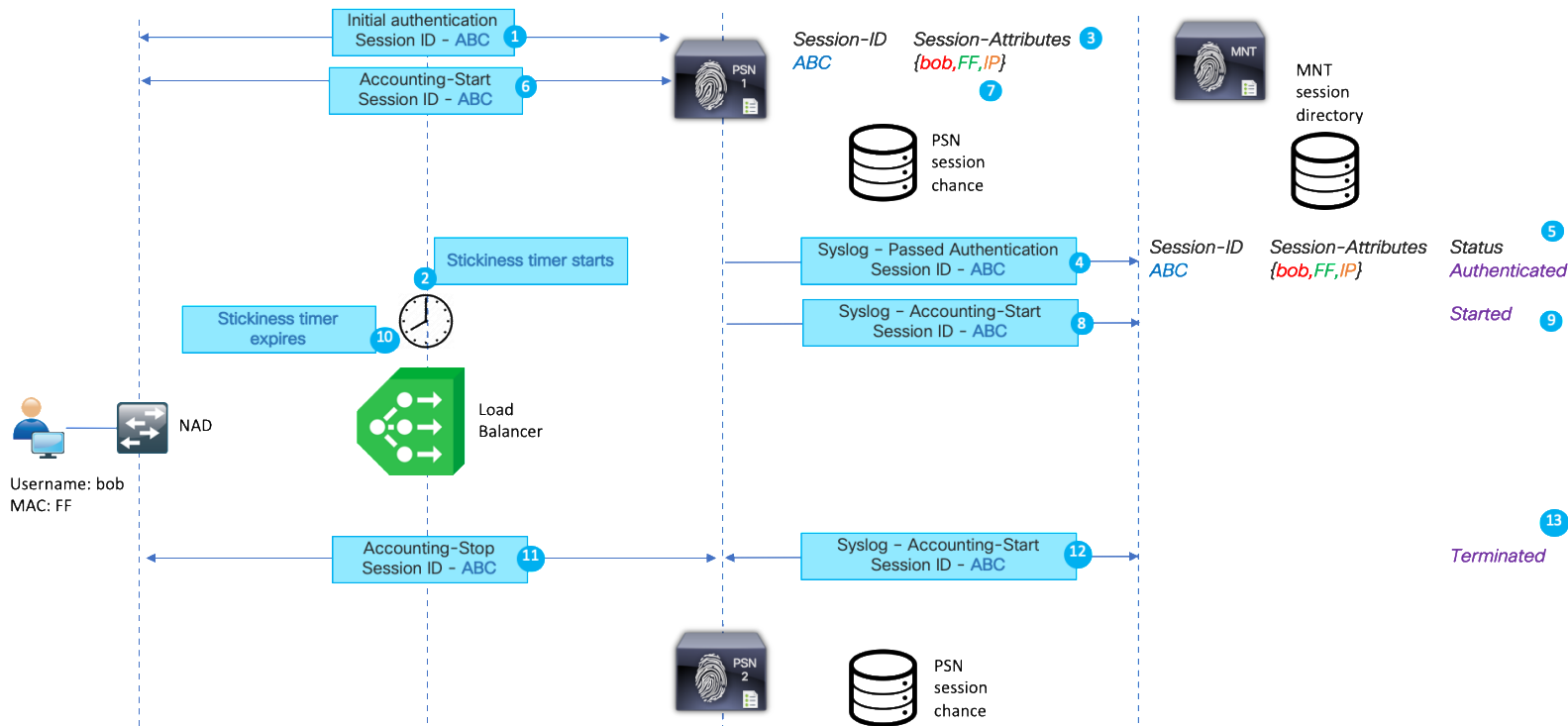
Keep in mind that LDD posture enchantments does not solve:

- Failover between different ISE deployments
- Any scenario when L2 changes happens (re-auth due to any reason with the same PSN but with new session ID)

Those two scenarios are goanna to be addressed in the future from both Agent and ISE sides

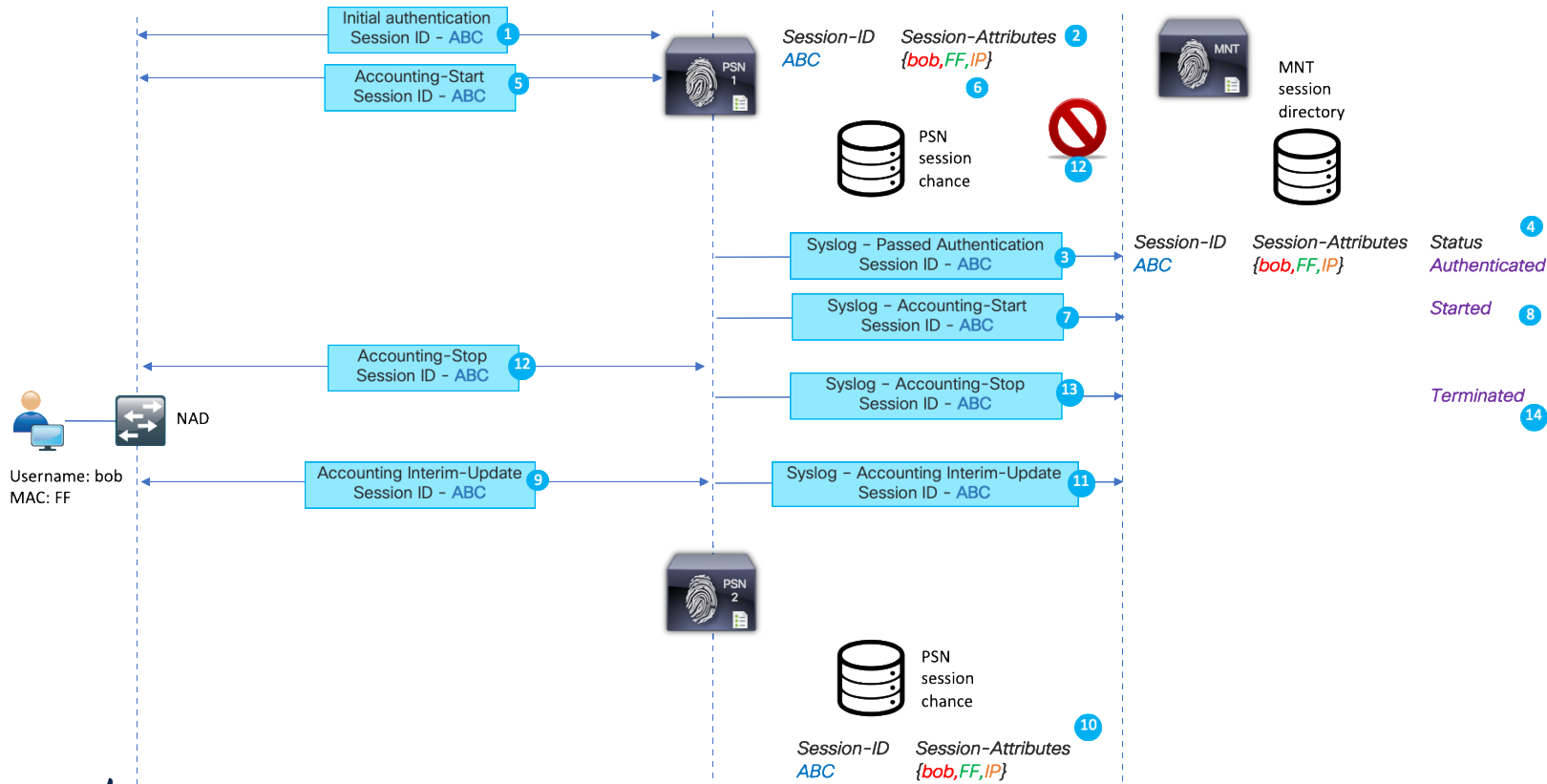


Stale session detailed flow



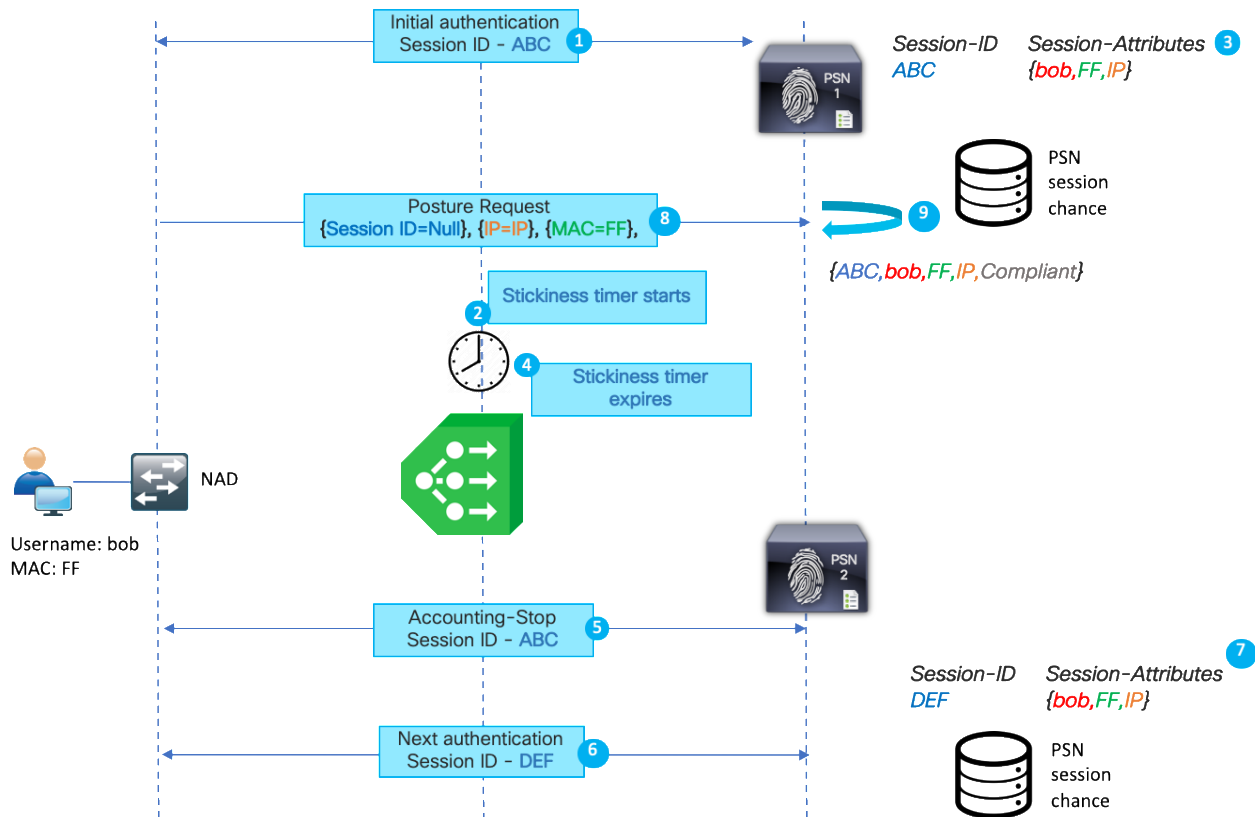


Phantom session detailed flow





How problem appears – Detailed flow



Demo – Node Group



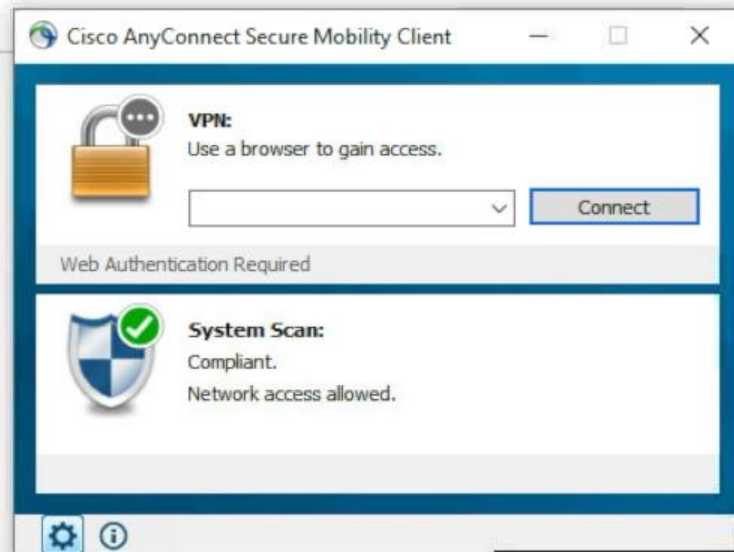


Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Start



How to avoid issues without LSD

- USE REDIRECTION when it's supported by NAD
- Enabled stickiness on LB for authentication and accounting with Calling-Station-ID as a stickiness key. [More details](#)
- Use stickiness timer a bit higher than average working day (e.g. 10 hours).
- Set reauthentication timer from ISE with value a bit lower than stickiness timer (e.g. 8 hours).
- On VPN set higher accounting interim-update interval than 'vpn-session-timeout',
To avoid accounting flapping between PSNs on a long living sessions



Misconception 1 – How to avoid? (continue)

- Often in configuration examples for posture over VPN it's recommended to setup

```
aaa-server ISE protocol radius  
interim-accounting-update periodic 1
```

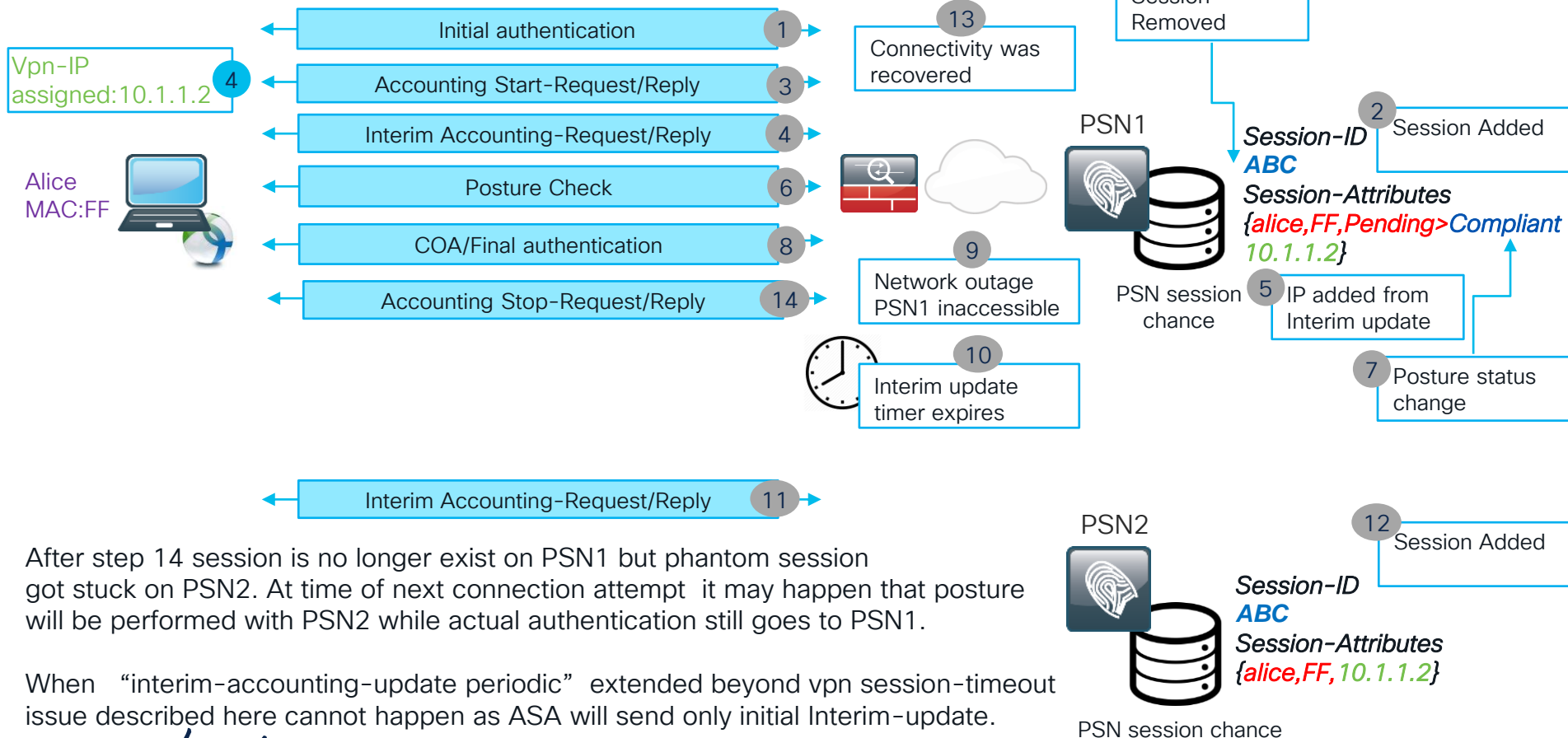
- At the same time VPN configuration examples commonly propose to configure `vpn-session-timeout` and `vpn-idle-timeout` with quite high number of hours. This allows users to resume VPN sessions without re-entering credentials.

```
group-policy SSL-VPN attributes  
vpn-idle-timeout 1200 (20 hours)  
vpn-session-timeout 1200 (20 hours)
```

At the same time long-living VPN sessions with interim accounting interval of 1 hour bring risk of phantom sessions being created on ISE PSNs.

See next slides for more details ...

Phantom session - VPN



After step 14 session is no longer exist on PSN1 but phantom session got stuck on PSN2. At time of next connection attempt it may happen that posture will be performed with PSN2 while actual authentication still goes to PSN1.

When “interim-accounting-update periodic” extended beyond vpn session-timeout issue described here cannot happen as ASA will send only initial Interim-update.

cisco Live!

How to avoid? But without redirect

One 'Compliant' policy

Authorization profile assign ACL which allows probes only to PSN specified in the policy

Amount of 'Unknown' policies equal to number of PSNs

'Unknown' policies having ISE node name as condition



Call Home Request PSN2



Call Home Request PSN1



Access Request

Access Accept
ACL=PSN1

PSN1.demo.local

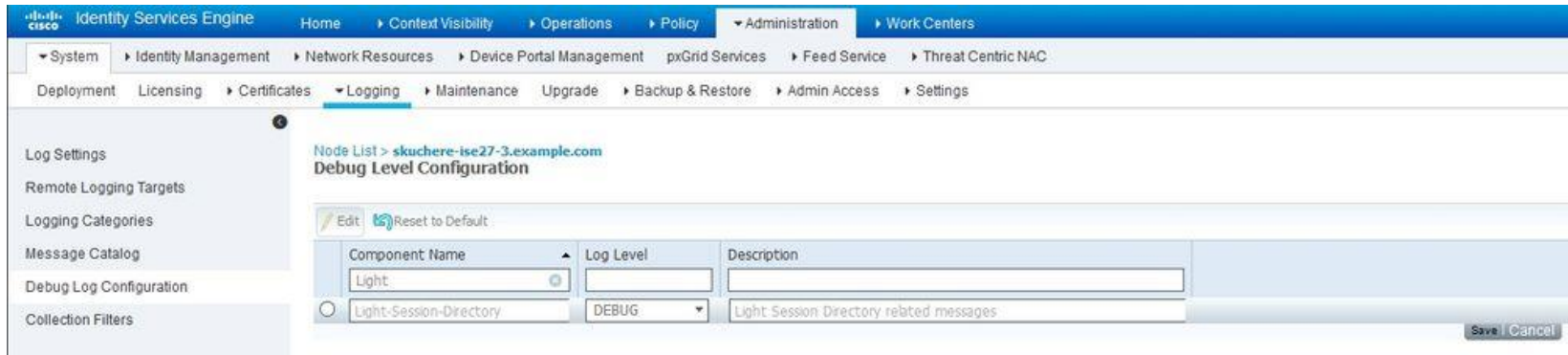


Radius Session Directory (RSD) Architecture

- Session ID.
- Endpoint MAC.
- CallingStationID.
- Endpoint IP.
- PSN IP - PSN where authentication happened.
- PSN FQDN - same as above.
- NAS-IP-Address.
- NAS-IPv6-Address.
- State - Authenticated, Started, Stopped.

Troubleshooting LSD

To troubleshoot communication over LDD on the ISE you can enable **Light Session Director** component into DEBUG:



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes tabs for Home, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The left sidebar contains a tree view with categories like Log Settings, Remote Logging Targets, Logging Categories, Message Catalog, Debug Log Configuration (selected), and Collection Filters. The main content area displays the 'Node List > skuchere-ise27-3.example.com' and 'Debug Level Configuration' page. It features an 'Edit' button and a 'Reset to Default' link. Below this is a table with columns for Component Name, Log Level, and Description. The table lists two components: 'Light' and 'Light-Session-Directory'. The 'Light-Session-Directory' component has its Log Level set to 'DEBUG'.

Component Name	Log Level	Description
Light		
Light-Session-Directory	DEBUG	Light Session Directory related messages

Save Cancel

Troubleshooting LSD

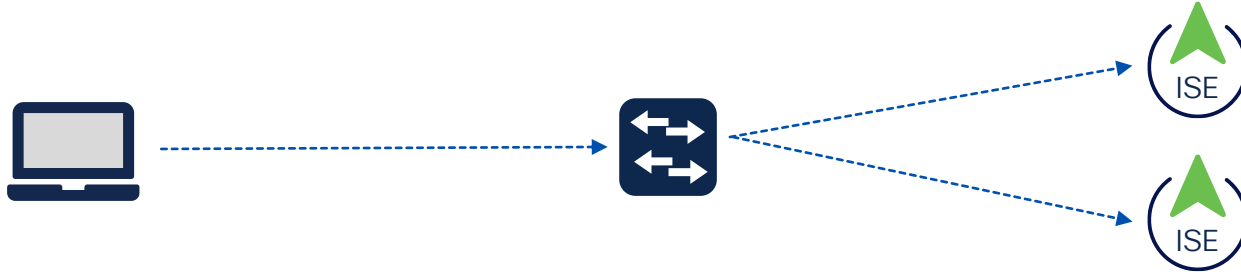
```
DEBUG [pool-45-thread-6][] cisco.cpm.lsd.service.LSDRedisClient -::::-  
Mapping Session ID 0a3e9498000008e05e071990 to session  
{ "sessionID": "0a3e9498000008e05e071990", "endpointMAC": "C0-4A-00-1F-6B-  
39", "callingStationId": "c0-4a-00-1f-6b-  
39", "ipv6AdressLst": [], "psnIP": "192.168.43.26", "deviceIP": "192.168.255.102"  
, "destinationIP": "192.168.43.26", "nasIP": "192.168.255.102", "auditSessionID"  
: "0a3e9498000008e05e071990", "acctSessionID": "5e07197b/c0:4a:00:1f:6b:39/229  
9", "timeStamp": 1577523495, "status": "Started", "id": "614f6c44-6c78-4289-b9fd-  
b352ff012ca4" }
```

```
DEBUG [PrRTEvents-Executor-2][]  
cisco.cpm.lsd.service.LSDNetAccessEventListener -::::- Publishing session  
update for session 0a3e9498000008e05e071990
```

```
DEBUG [PrRTEvents-Executor-2][] cisco.cpm.lsd.service.SessionPublisher -  
::::- Forwarding session 07a26b4b-ea13-438b-99b5-0bbadc9d8bac to batch  
manager
```

Posture Status Sharing over RSD

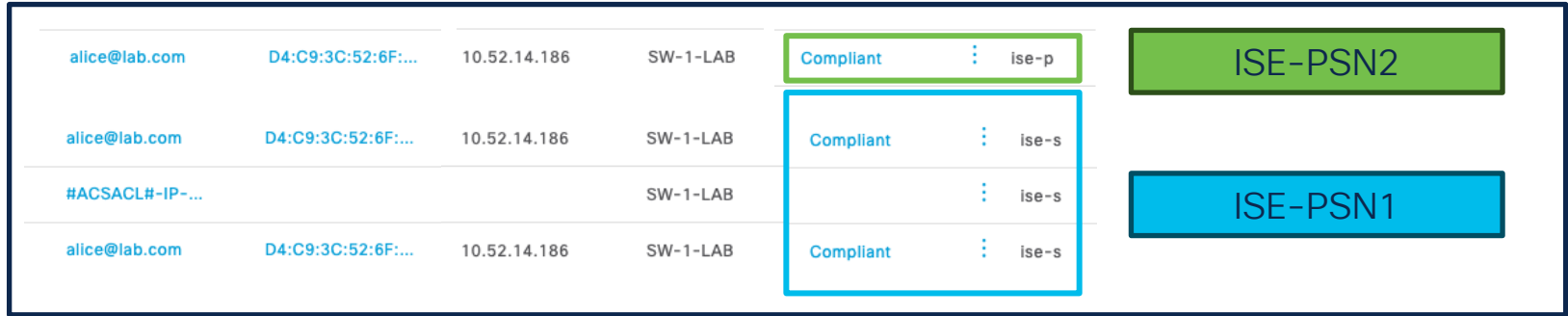
Stale/Phantom Sessions



1. Accounting-Start messages processed by PSN-1.
2. Interim Accounting-Update for the same session processed by PSN-2.
3. The session finishes later on PSN-1.

Stop	3.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1	0A3E946C0000007D5B679296
Interim-Update	2.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-3	0A3E946C0000007D5B679296
Start	1.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1	0A3E946C0000007D5B679296

Posture Status Sharing over RSD – PSN Failover



1. Authentication happens on PSN-1, authorization profile with redirection is assigned.
2. COA after successful posture assessment.
3. Next authentication when authorization profile for the compliant state is assigned.
4. Authentication hits different PSN but it still gets authorization profile for the compliant state.

Demo RSD

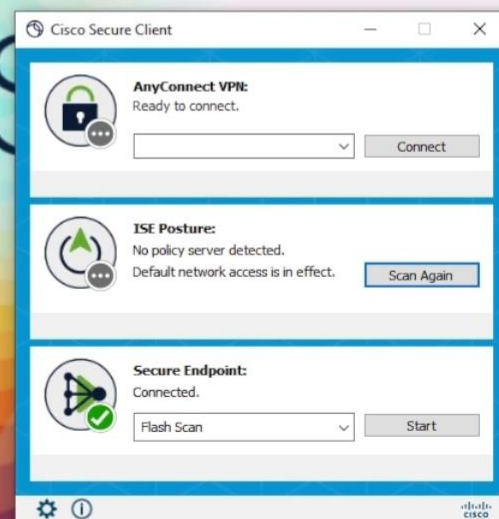




CISCO *Live!*

Amsterdam | February 5-9, 2024

Let's



Activate Windows
Go to Settings to activate Windows

Posture Status Sharing over RSD

PSN Failover

```
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.impl.SessionCache -::::- Looking up session 0A3E946C000000896011D045 for attribute
Session Session.PostureStatus
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.api.ExecutionContext -::::- Execution context has session id
0A3E946C000000896011D045
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.impl.PIPManager -::::- Returning a PIP com.cisco.cpm.nsf.session.impl.SessionPIP for
type SESSION and flow null
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.api.ExecutionContext -::::- Execution context has session id
0A3E946C000000896011D045
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.impl.SessionCache -::::- Looking up session 0A3E946C000000896011D045
2020-04-09 11:06:42,176 DEBUG [SessionLifecycleNotifier] [] cpm.nsf.session.internal.LRUagingAlgorithm -::::- Accessed session
0A3E946C000000896011D045
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.impl.SessionCache -::::- Returning for session 0A3E946C000000896011D045 data Attrs:
{SavedUserNames=[bob@example.com], Acs.LastStepTime=1586423202174, Acs.AD-User-Qualified-Name=bob@example.com, Acs.AD-User-Resolved-
DNs=CN=bob,CN=Users,DC=example,DC=com, Acs.StepData=[110=EXAMPLE, 111=bob@example.com, 112=example.com, 113=example.com, 115=example.com,
116=EXAMPLE], Acs.AD-Log-Id=[1585911138/4778, 1585911138/4779], __IntIdGrps__[Ljava.lang.String;@6d3c29b5,
IdentityGroup.Description=[Ljava.lang.String;@3fca88fb, EXAMPLE.ExternalGroups=S-1-5-21-875452798-754861120-3039794717-513, Acs.AD-Groups-
Names=example.com/Users/Domain Users, Acs.AuthenCPMSessionID=0A3E946C000000896011D045, Acs.IsMachineAuthentication=false,
InternalEndpoint.IdentityGroup=[Ljava.lang.String;@6daf4c5, IDStoreUserQueryCache=[EXAMPLE#bob@example.com], Acs.CurrentIDStoreName=EXAMPLE,
Acs.AD-User-Join-Point=EXAMPLE.COM, Acs.Step=[24432, 24325, 24313, 24319, 24323, 24355, 24416], Acs.CustomerMessageDuplicator=, Network
Access.WasMachineAuthenticated=false, IdentityGroup.Name=[Ljava.lang.String;@570ab37a, Acs.StepDataStart=110, Acs.AD-User-DNS-Domain=example.com,
Network Access.AuthenticationMethod=4, Acs.AD-User-Resolved-Identities=bob@example.com, InternalUser.IdentityGroup=[Ljava.lang.String;@51a6caed,
Acs.AuthenticationMethod=4, Acs.AD-User-NetBios-Name=EXAMPLE, Normalised Radius.RadiusFlowType=0, Network
Access.AuthenticationIdentityStore=EXAMPLE, EXAMPLE.IdentityAccessRestricted=false, Acs.AD-User-SamAccount-Name=bob}
IndexValues: {}

2020-04-09 11:06:42,177 DEBUG [Thread-7979] [] cisco.cpm.posture.pip.PostureStatusPIP -::::- set postureStatus based on posture LSD dictionary:
Compliant
2020-04-09 11:06:42,177 DEBUG [Thread-7979] [] cisco.cpm.posture.pip.PostureStatusPIP -::::- PostureStatusPIP for mac 00-50-56-B6-0B-C6 - Attribute
Session.PostureStatus value is Compliant
```

Misconception n. 3: Compliant State ISE vs Secure Client

Secure Client Compliant State

“Secure Client is aware of its Compliant State on ISE”



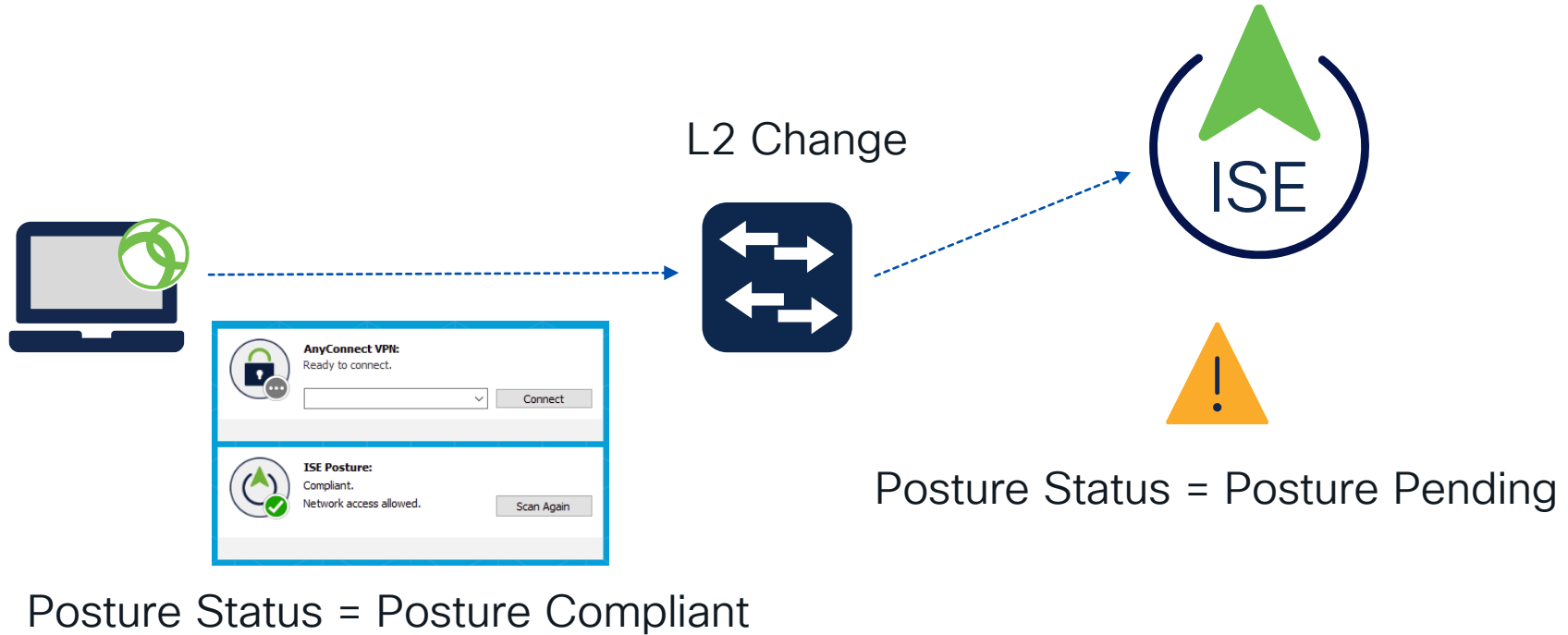
slido



Secure Client is aware of its Compliant State on ISE

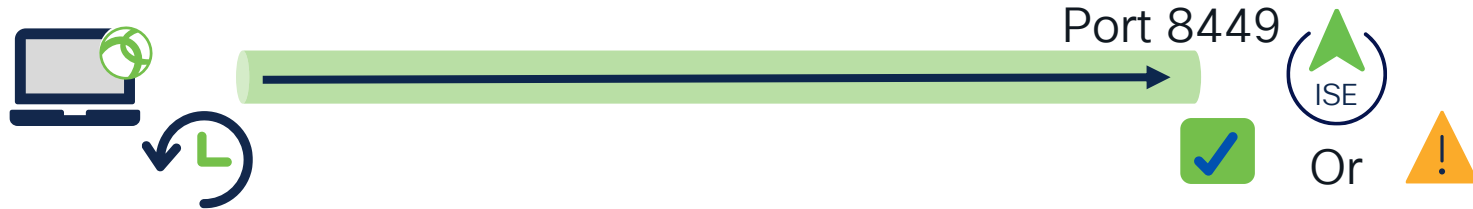
① Start presenting to display the poll results on this slide.

The problematic scenario



Bidirectional Posture

Secure Client will probe ISE if in Compliant state



Secure Client 4.10+

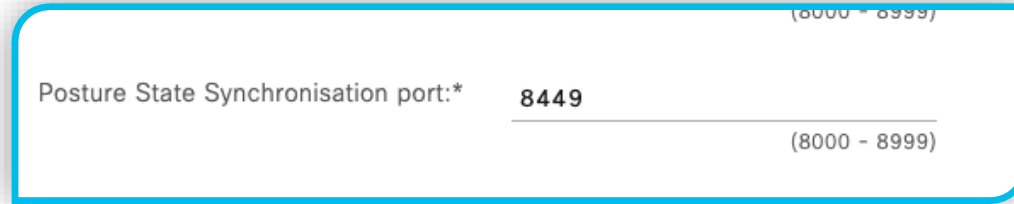


ISE 3.1+



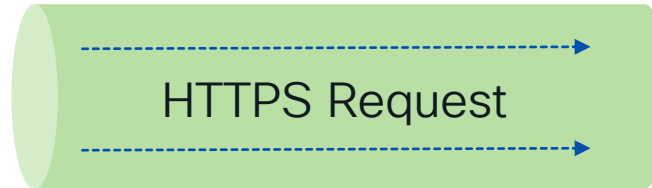
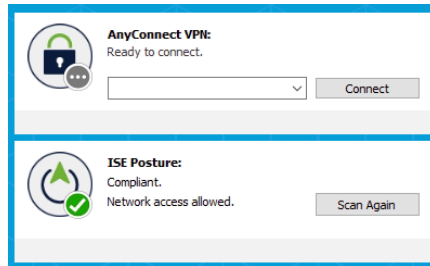
Bidirectional Posture - facts

Probed port: 8449 => Configurable in CPP Portal



A screenshot of a configuration field in the CPP Portal. The field is labeled "Posture State Synchronisation port:*" and contains the value "8449". Above and below the input field, the range "(8000 - 8999)" is displayed. The entire configuration area is enclosed in a blue rounded rectangle.

Probes will only fire off if the posture module is compliant



Client Provisioning Policy

Resources

Client Provisioning Portal

Portal Settings and Customization

Portal Name

Client Provisioning Portal (default)

Portal and user experience user

Language



Portal test

Portal and Flow Settings

Portal Customization

Portal & Page Settings

Portal Settings

HTTPS port:*

8443

{8080 - 8999}

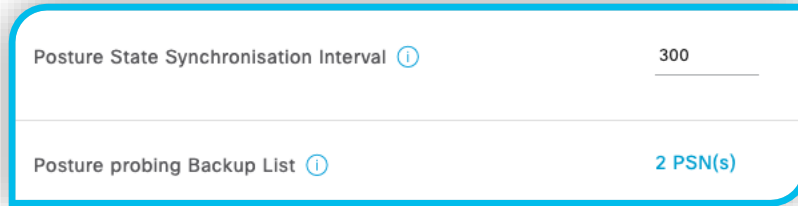
Posture State Synchronisation port:*

8449

BRKSEC-3077

Bidirectional Posture – Configuration

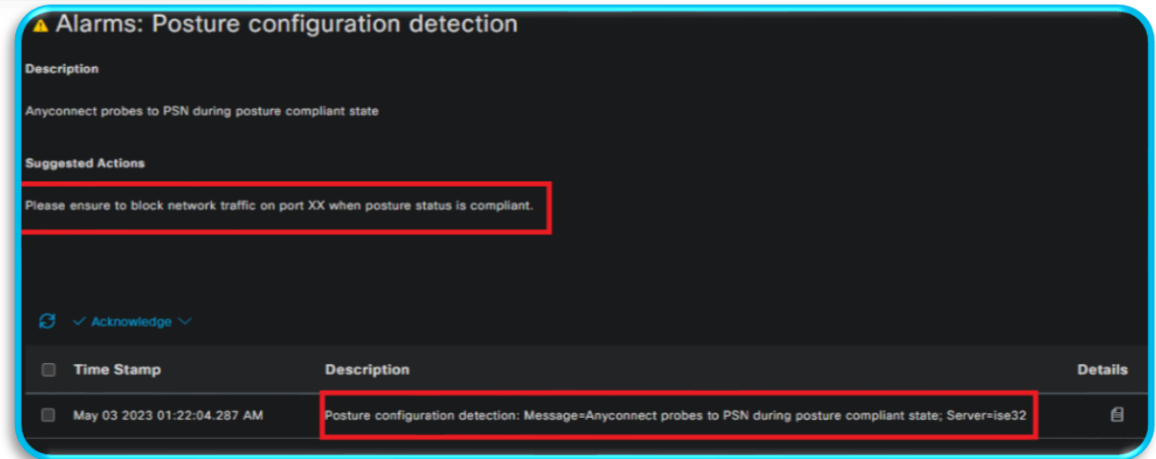
Enable Posture State Synchronization:



Posture State Synchronisation Interval ⓘ 300

Posture probing Backup List ⓘ 2 PSN(s)

The issue appearing:



Alarms: Posture configuration detection

Description

Anyconnect probes to PSN during posture compliant state

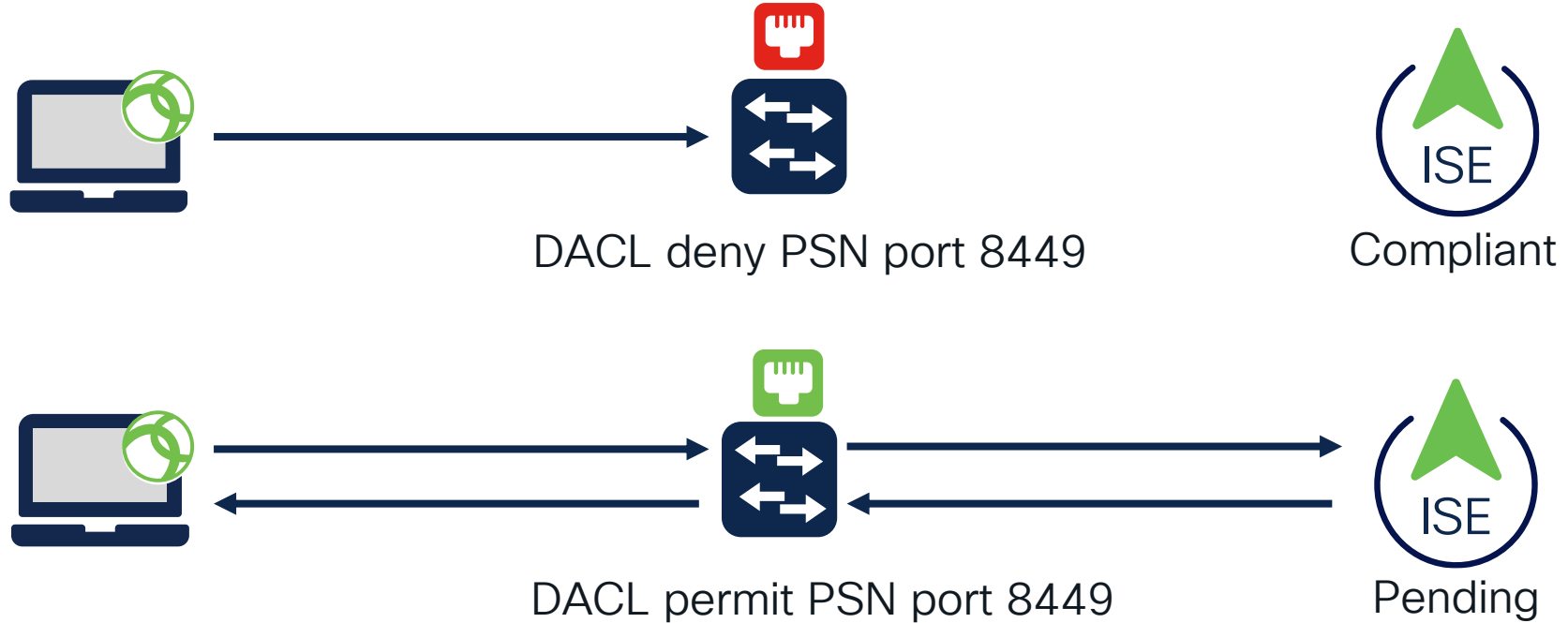
Suggested Actions

Please ensure to block network traffic on port XX when posture status is compliant.

✓ Acknowledge

Time Stamp	Description	Details
May 03 2023 01:22:04.287 AM	Posture configuration detection: Message=Anyconnect probes to PSN during posture compliant state; Server=ise32	

Bidirectional Posture – Correct Implementation



Bidirectional Posture – Troubleshooting

Logs to be enabled:

- Guest
- Client Provisioning
- Posture

Sample Log:

```
2021-04-29 05:59:23,352 DEBUG [https-jsse-nio-10.0.10.130-8443-exec-1][] cisco.cpm.posture.runtime.PostureHandlerImpl -:autouserwin7::-  
DM_PKG report non-AUP : html = <!--X-Perfigo-DM-Error=0--><!--error=0--><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0--><!--X-  
Perfigo-Auto-Close-Login-Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0--><!--user role=--><!--X-Perfigo-OrigRole=--><!--X-Perfigo-  
UserKey=dummykey--><!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-Perfigo-Session=--><!--X-Perfigo-SSO-Done=1--><!--X-  
Perfigo-Provider=Device Filter--><!--X-Perfigo-UserName=autouserwin7--><!--X-Perfigo-VLAN-Change-Delay=3--><!--X-Perfigo-Monitoring-  
Interval=5--><!--X-Perfigo-StateSynch-Url=auth/StateSynch--><!--X-Perfigo-StateSynch-Port=8449--><!--X-Perfigo-StateSynch-  
ProbeList=Positron-vm-3.demo.local-->
```

Logs to check: ise-psc.log and guest.log

Demo- Bidirectional Posture Configuration



Resources

Selected 0 Total 12 ↻

 Edit  Add ▾  Duplicate  Delete

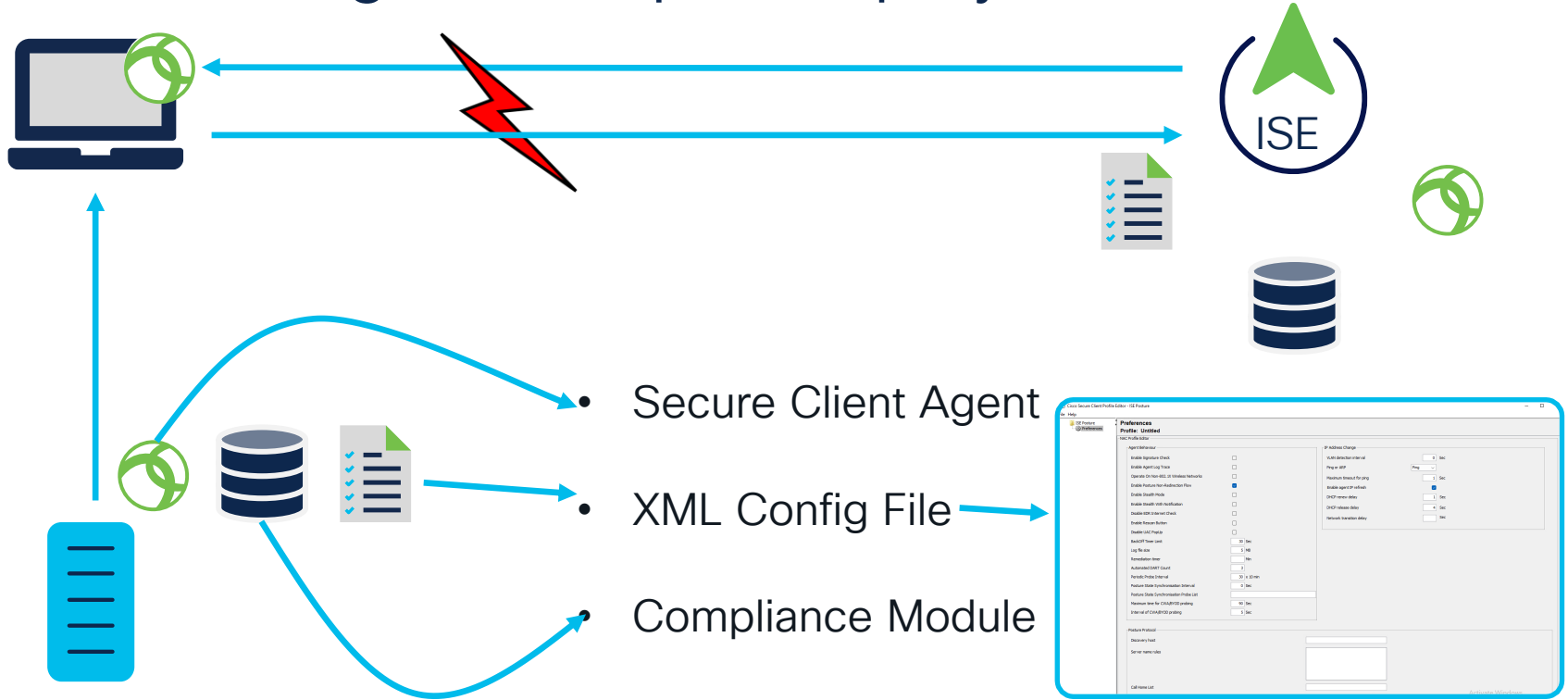
All ▾ 

<input type="checkbox"/>	Name	Type	Version	Last Update	Description
<input type="checkbox"/>	AnyConnectComplianceMod...	AnyConnectComplian...	4.3.3765....	2023/11/29 19:45:51	Cisco Secure Client Win..
<input type="checkbox"/>	CiscoAgentlessOSX 5.0.005...	CiscoAgentlessOSX	5.0.529.0	2022/10/19 16:56:01	With CM: 4.3.2490.4353
<input type="checkbox"/>	CiscoSecureClientDesktopW...	CiscoSecureClientDe...	5.1.0.136	2023/11/29 19:58:57	Cisco Secure Client for ..
<input type="checkbox"/>	Cisco-ISE-Chrome-NSP	Native Supplicant Pro...	Not Applic...	2016/10/06 22:01:12	Pre-configured Native S..
<input type="checkbox"/>	MacOsXSPWizard 2.7.0.1	MacOsXSPWizard	2.7.0.1	2022/10/19 16:55:51	Supplicant Provisioning ..
<input type="checkbox"/>	CiscoTemporalAgentWindo...	CiscoTemporalAgent...	5.0.529.0	2022/10/19 16:55:52	With CM: 4.3.2868.6145
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Pro...	Not Applic...	2022/10/19 17:56:43	Pre-configured Native S..
<input type="checkbox"/>	Win_Posture_Profile	AgentProfile	Not Applic...	2023/11/29 19:44:42	
<input type="checkbox"/>	CiscoAgentlessWindows 5.0...	CiscoAgentlessWind...	5.0.529.0	2022/10/19 16:55:58	With CM: 4.3.2868.6145

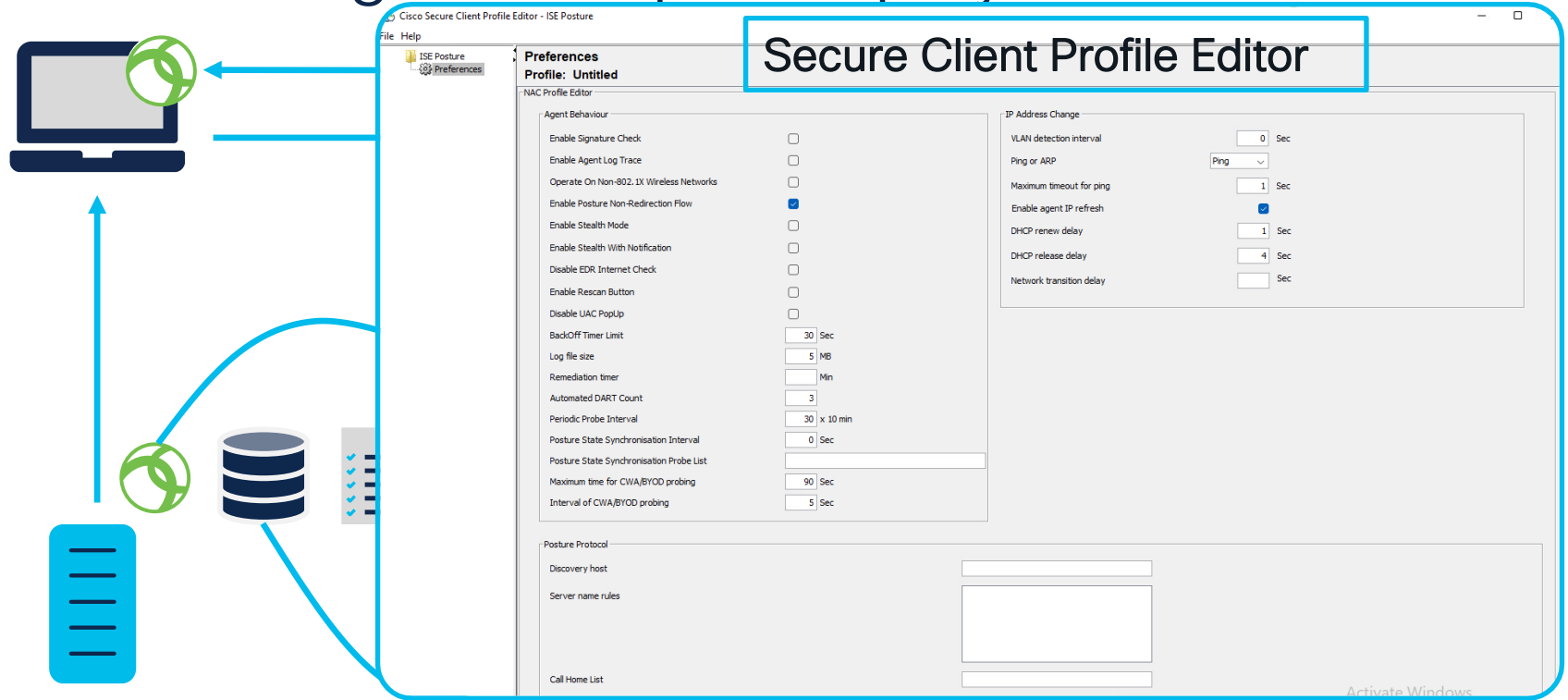
Advanced ISE Posture Deployments – Use Cases



Posture large-scale pre-deployment



Posture large-scale pre-deployment



Posture large-scale pre-deployment



Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files

`cisco-secure-client-win-5.1.6.103-predeploy-k9.zip`

[Advisories](#)



ISE Posture Compliance Library - Windows / Standalone installer (MSI). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later.

`cisco-secure-client-win-4.3.4214.8192-isecompliance-predeploy-k9.msi`

[Advisories](#)



ISEPostureCFG.xml

C:\ProgramData\Cisco\Cisco Secure Client\ISE Posture\

File location - MacOS



Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files

`cisco-secure-client-win-5.1.6.103-predeploy-k9.zip`

[Advisories](#)



ISE Posture Compliance Library - Windows / Standalone installer (MSI). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later.

`cisco-secure-client-win-4.3.4214.8192-isecompliance-predeploy-k9.msi`

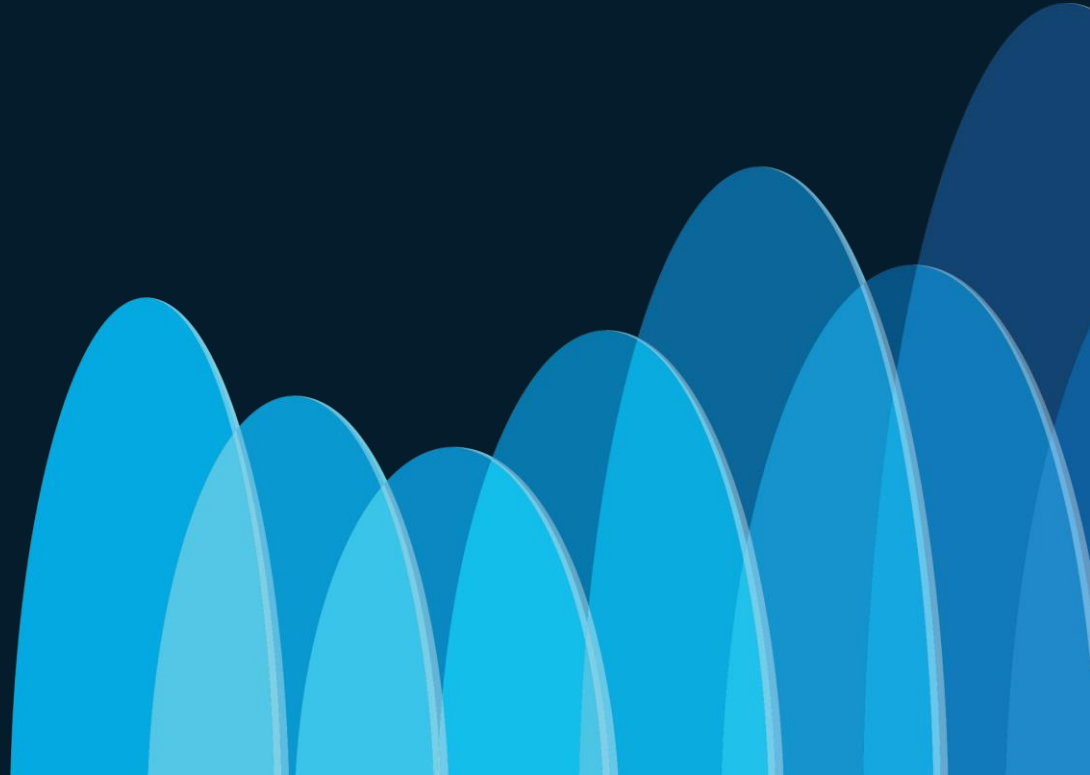
[Advisories](#)



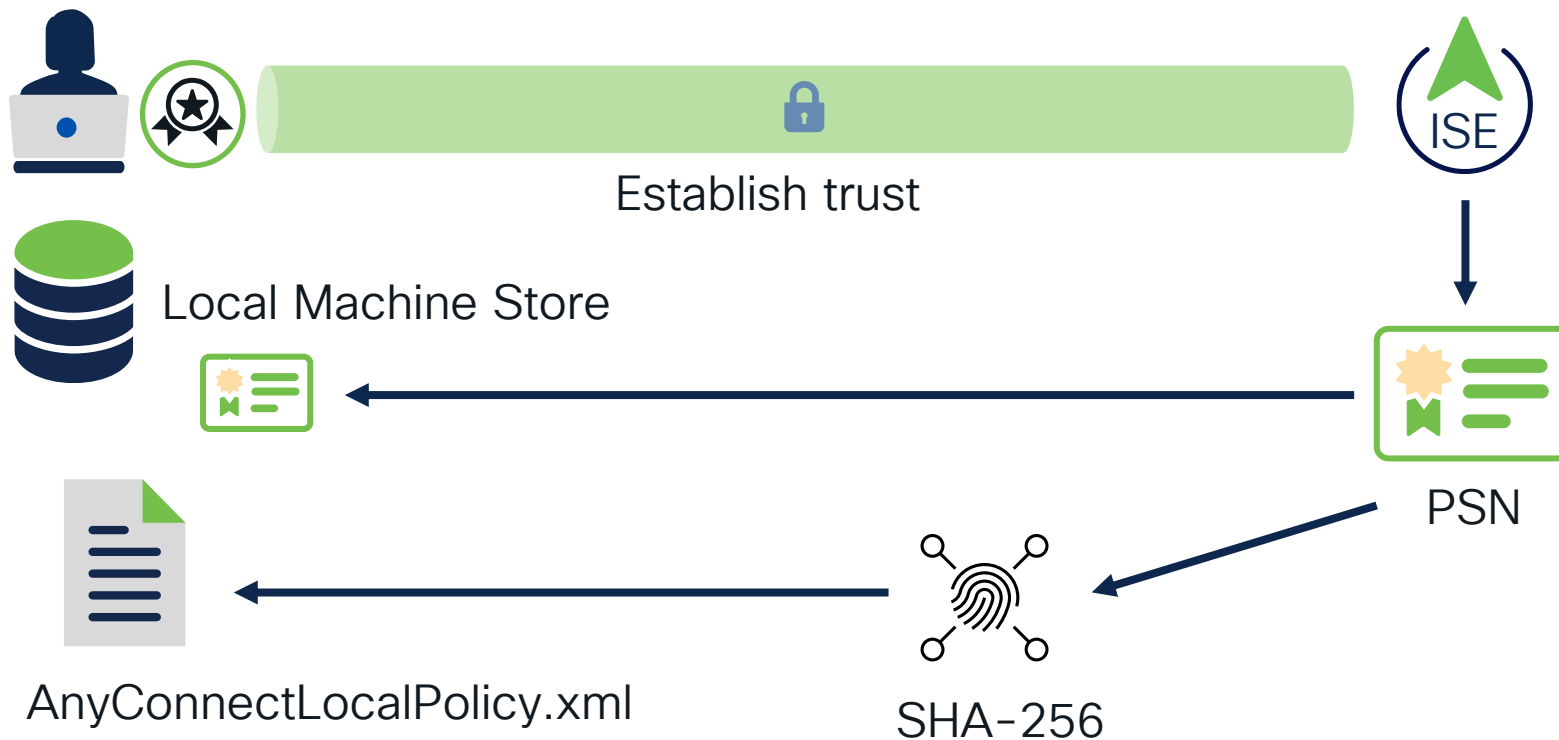
ISEPostureCFG.xml

`/opt/cisco/secureclient/iseposture/`

Posture Script Condition



Posture Script Condition – Prerequisites



Posture Script Condition – Prerequisites

New

```
openssl x509 -in 535-pos.crt -fingerprint -noout -  
sha256 SHA256
```



```
Fingerprint=B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:A  
B:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5
```



```
<TrustedISECertFingerprints>  
  <fingerprint>  
    <algorithm>SHA-256</algorithm>  
    <hash>30:5D:A8:0E:3B:36:6C:3A:04:0C:DF:66:D0:3  
B:9B:DE:94:B8:87:ED:17:5F:B7:A4:94:BF:3A:29:A5:7B:35:D0</hash>  
  </fingerprint>  
</TrustedISECertFingerprints>
```

Posture Script Condition - Configuration

Add Script Condition

Name*

Description

Operating System **Windows**

Script Type
☒ PowerShell ☐ PowerShell Core

File to Upload* **Choose File**
Accepted Files: .ps1

Timeout* 1 to 60 (seconds)

Script Condition execution failure or timeout
 Choose what happens to a condition if the script does not exit before the configured timeout or if script execution fails.
 If you choose Pass, the condition is marked as met.
 If you choose Fail, the condition is marked as not met.

☐ Pass ☒ Fail

Windows PowerShell execution policy:

☐ Bypass ☒ AllSigned ☐ None

Endpoint privilege for script execution
 Agentless Posture workflows use Admin privilege and temporal agents use Logged-in User privilege, regardless of the user privilege that you choose for this script.

☒ Administrator / Root ☐ Logged-In User

Exit code Fail - Other than 0
 Pass- < 0 Pass

Bypass AllSigned None



Folder

Admin vs Logged-in User

Posture script condition – Script Download

New

%LOCALAPPDATA%\Cisco\Cisco Secure Client \scripts



~/ .cisco/ise posture/scripts

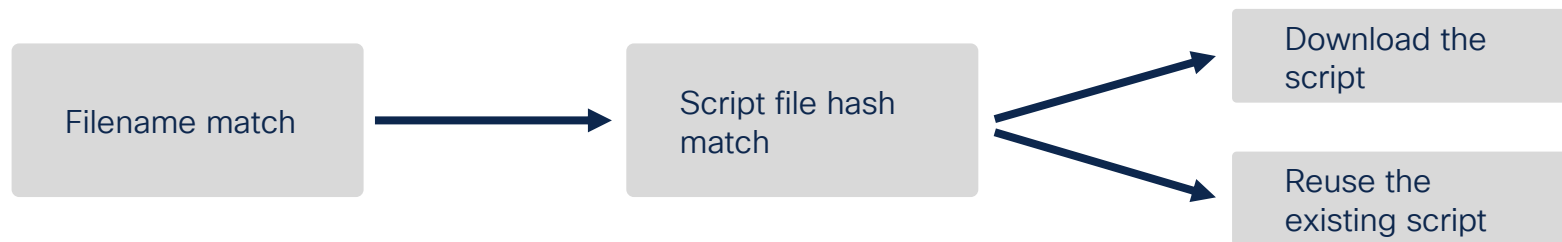
Elevated privileges



%ALLUSERPROFILE%\Cisco\Cisco Secure Client \ISE Posture\scripts



/opt/cisco/Secure Client/ise posture/scripts





Posture script condition – Exit Code



Other failure possibilities:



<0 : pre-defined exit code

>0 : user-defined exit code

Script exit code must be
between 0 and 255

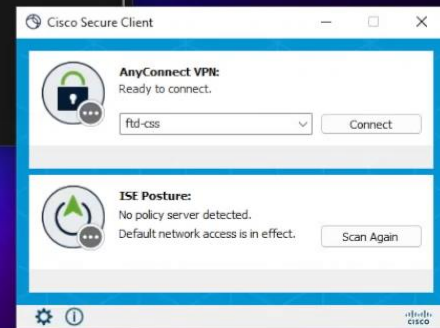
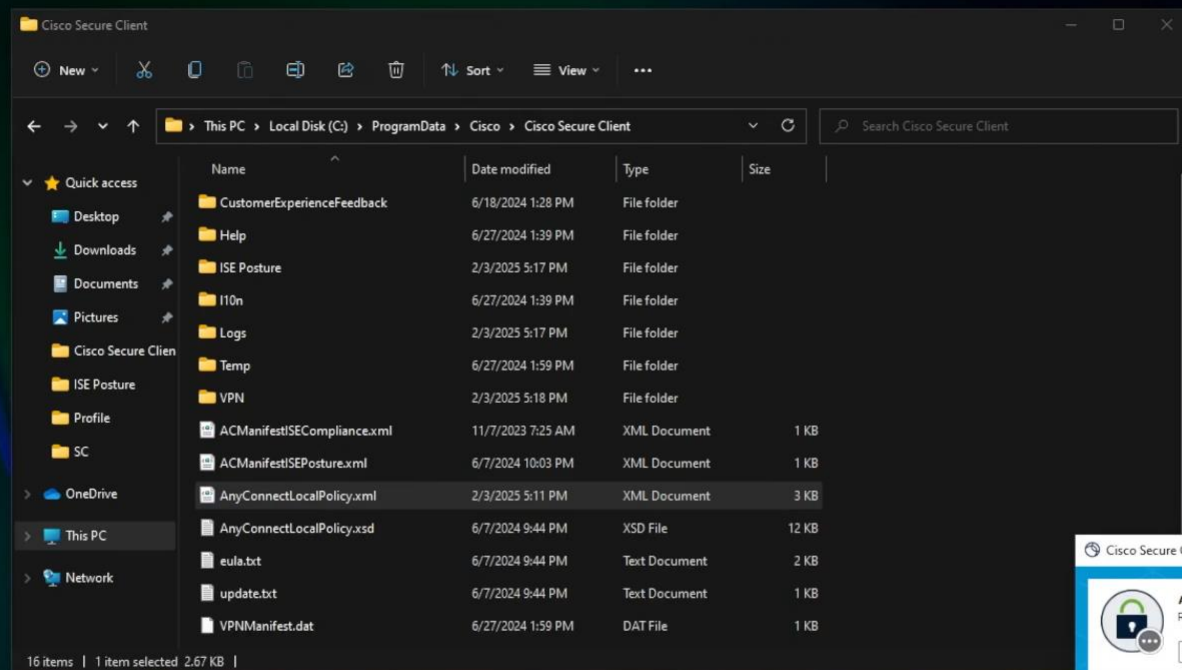
Posture Script Exit Codes

Exit Code	Reason
0	Script execution was successful and exited with success
>0	Script execution was successful however, exit code returned the failure code
-1	Script execution check wasn't attempted
-2	Data integrity failed
-3	Error in Script download
-4	Script has verification failed
-5	Script executed, however, Script execution didn't complete within specified timeout
-6	Generic failure (not covered as part any failures)
-7	Script type is not supported
-8	Script failed to launch
-9	ISE certificate is not trusted

Remember: in case script exit code is out of bound then it is set to 255

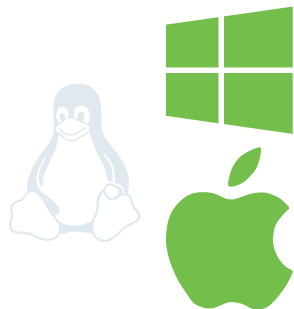
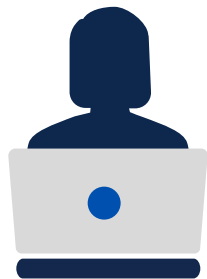
Demo Posture Script





Agentless Posture

Posture Agentless - Requirements



Windows



macOS



PowerShell



5.1 >

Shell (.sh)



SSH



Port 5985



Port 22

cURL

7.34 >

cURL

7.34 >

Posture Agentless

Client

NAD

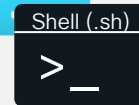
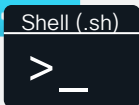
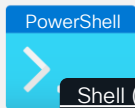
ISE



No Redirection



OS Discovery



PS Remoting

Posture Agentless

Client

NAD

ISE



Posture Check



Posture Report



Agentless: Failure Flow

×

Create Guest Portal - Choose Portal Type

Choose the type of portal you want to create.

☐ Sponsored-Guest Portal

Sponsors create guests' accounts. Guests cannot create their own accounts.

☐ Self-Registered Guest Portal

Guests provide information to automatically create an account, with sponsor approval as an optional requirement.

☒ Hotspot Guest Portal

Guests can access the network without credentials, but you can add a welcome message and AUP.

Cancel

Continue...

NonCompliant

▼ Common Tasks

☐ VLAN

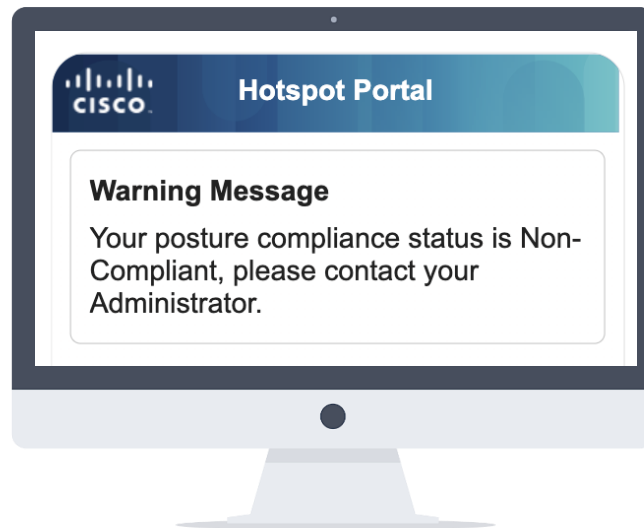
☐ Voice Domain Permission

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

Hot Spot ▼

ACL ▼

Value Self-Registered Guest Port... ▼



- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration
- Work Centers**
- Interactive Features

- Overview
- Network Devices
- Client Provisioning
- Policy Elements**
- Posture Policy
- Policy Sets
- Troubleshoot
- Reports
- Settings

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall
- Hardware Attributes
- osquery
- Patch Management
- Registry
- Script
- Service
- USB

Remediations

Requirements

- Allowed Protocols
- Authorization Profiles
- Downloadable ACLs

Requirements

Name		Operating System		Compliance Module		Posture Type		Conditions		
Any_AM_Installation_Win	for	Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_inst	then	
Any_AM_Definition_Win	for	Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_def	then	
Any_AM_Installation_Mac	for	Mac OSX	using	4.x or later	using	Agent	met if	ANY_am_mac_inst	then	
Any_AM_Definition_Mac	for	Mac OSX	using	4.x or later	using	Agent	met if	ANY_am_mac_def	then	
Any_AM_Installation_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_inst	then	
Any_AM_Definition_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_def	then	
USB_Block	for	Windows All	using	4.x or later	using	Agent	met if	USB_Check	then	
Default_AppVis_Requirement_Win	for	Windows All	using	4.x or later	using	Agent	met if	Default_AppVis_Condition_Win	then	
Default_AppVis_Requirement_Mac	for	Mac OSX	using	4.x or later	using	Agent	met if	Default_AppVis_Condition_Mac	then	

Note:

Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External conditions.
Remediations Actions are not applicable for Agentless Posture type.

Save

Agentless: Failure – Temporal Agent Fallback

Client Provisioning for the failure flow

Agentless Posture FAILED	If Any	and Windows All	and Session:AgentlessFlowStatus EQUALS Failure AND DC1:ExternalGroups EQUALS Agentless Posture	then CiscoTemporalAgentWindows 5.0.00529	Edit ▾
Agentless Posture	If Any	and Windows All	and DC1:ExternalGroups EQUALS Agentless Posture	then CiscoAgentlessWindows 5.0.00529	Edit ▾

Access policy to redirect user to CPP

Authorization Profile

* Name: temporal-agent

Description:

* Access Type: ACCESS_ACCEPT ▾

Network Device Profile: Cisco ▾ ⓘ

Service Template: ☐

Track Movement: ☐ ⓘ

Agentless Posture: ☐ ⓘ

Passive Identity Tracking: ☐ ⓘ

Common Tasks

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

Client Provisioning (Posture) ▾ ACL initial ▾ Value Client Provisioning Portal (defa ▾

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

☐ Auto Smart Port



Agentless Posture: Policy

✓	Agentless_Compliant	AND	<div>Session-PostureStatus EQUALS Compliant</div> <div>DC1-ExternalGroups EQUALS Agentless Posture Users</div>	PermitAccess ×	+
✓	CPP_Agentless_Failure	AND	<div>Session-PostureStatus NOT_EQUALS Compliant</div> <div>DC1-ExternalGroups EQUALS Agentless Posture Users</div> <div>Session-AgentlessFlowStatus EQUALS Failure</div>	CPP Temporal Agent F... ×	+
✓	CPP_Agentless	AND	<div>Session-PostureStatus NOT_EQUALS Compliant</div> <div>DC1-ExternalGroups EQUALS Agentless Posture Users</div>	CPP Agentless Posture ×	+

Authorization Profile

* Name **CPP Agentless Posture**

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile **Cisco**

Service Template ☐

Track Movement ☐

Agentless Posture ☒

Passive Identity Tracking ☐

Authorization Profile

* Name **CPP Temporal Agent Fallback**

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile **Cisco**

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

☒ Web Redirection (CWA, MDM, NSR, CPP)

Client Provisioning (Posture) **ACL** **redirect-posture** Value **Client Provisioning Portal (defi**

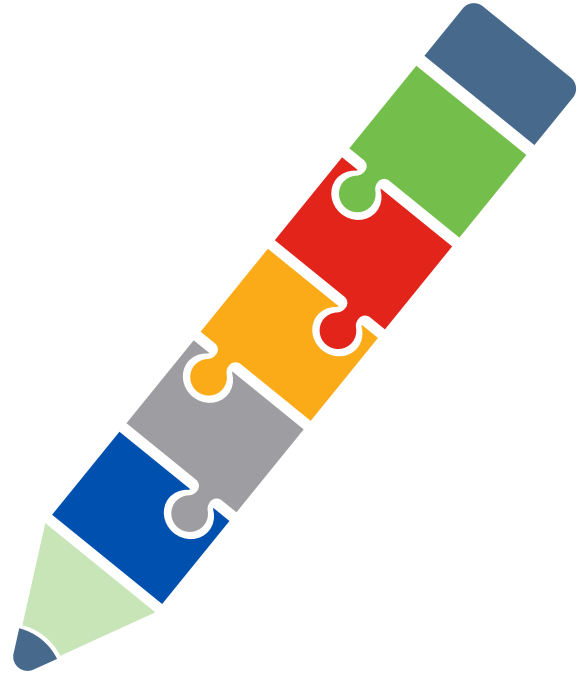
☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

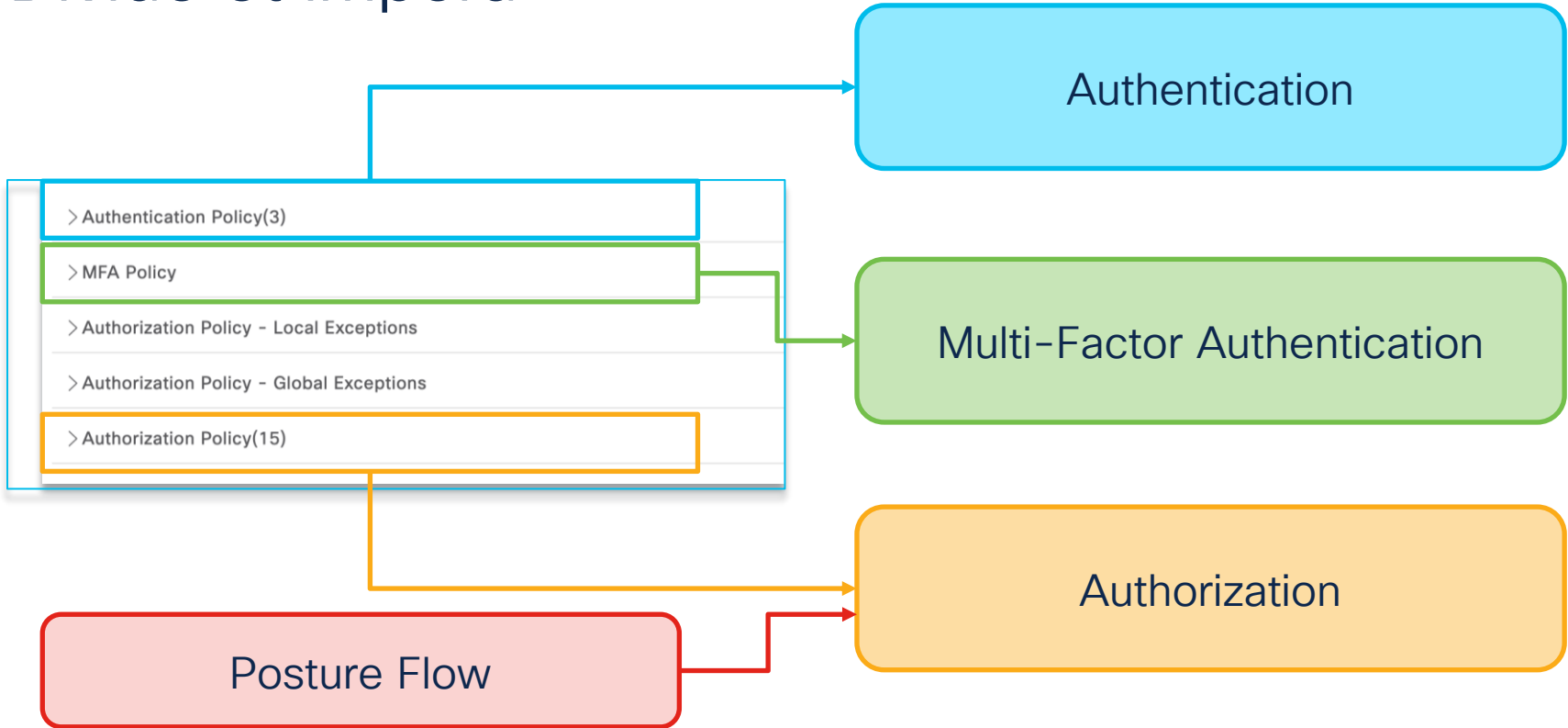
Advanced Use Cases

- ASA/FTD VPN + Posture
- Posture and MFA with Duo and VPN Access
- ASA SAML with SSO and ISE Posture

Posture is the last piece of the Puzzle,
it's easy to be included



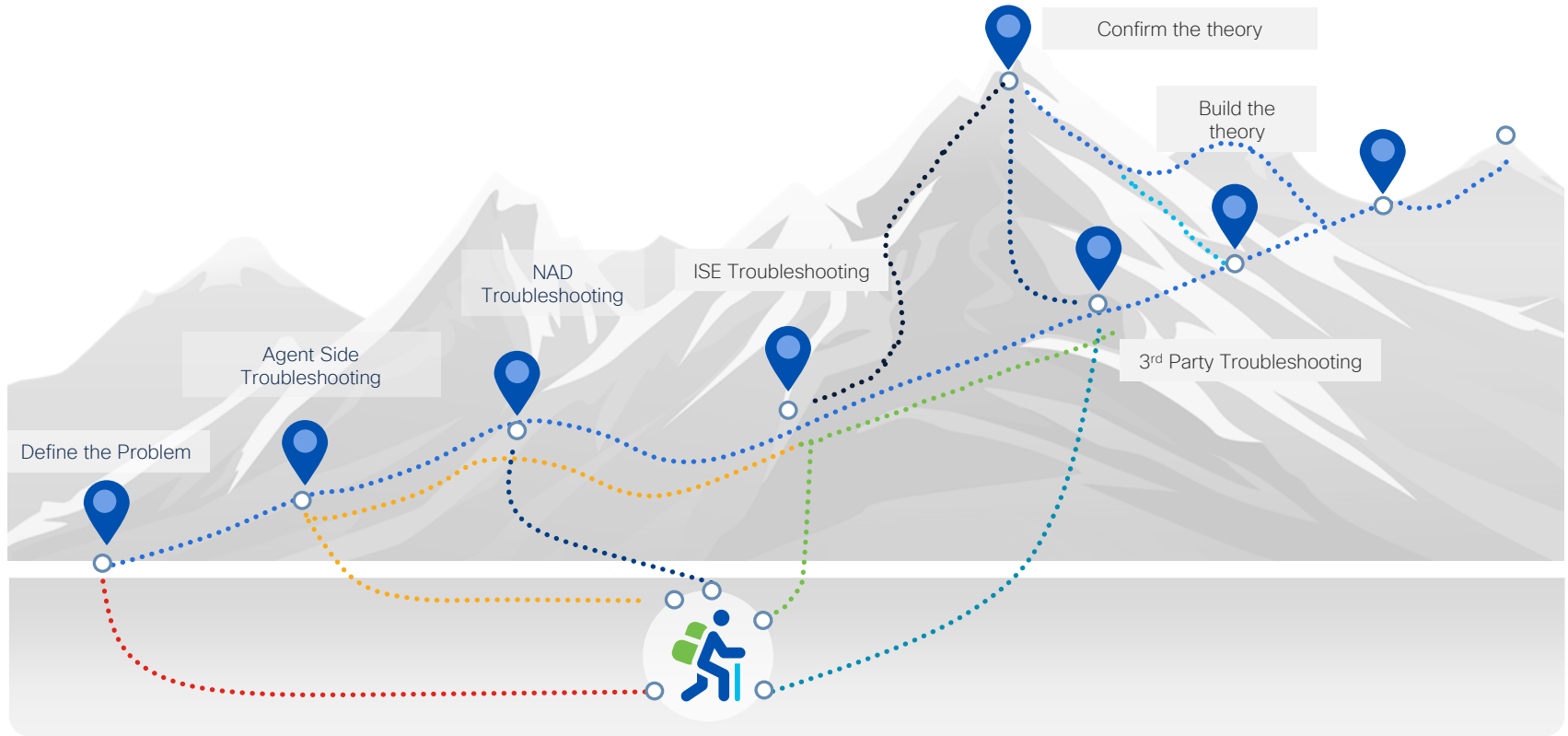
Divide et impera



ISE Posture troubleshoot deep dive



ISE Posture Troubleshooting Journey



Troubleshooting methodology

Define the problem

Understand how it
should work

Decide what to
collect and collect
the data

Confirm the theory

Analyze the data to
build the theory

Troubleshooting methodology

Define the problem

Formulate in as much details as possible what do you know about the issue? What are the symptoms? When did the issue start? Is it reproducible? What has been changed? Describe the environment.

Understand how it should work

Research how the affected functionality should work to define a baseline of normal behavior.

Decide what to collect and collect the data

What additional information you need to form a theory? Configuration? Debugs? Packet capture? Knowledge of working baseline and comparing it with Problem Definition should help you with this.

Analyze the data to build the theory

Compare working baseline with the collected data to understand the possible area of the issue. Define what needs to be done to proof the theory.

Confirm the theory

Confirm your theory. In case if issue is still presented you may need to do more research on how feature should work and collect more data.

Posture troubleshooting, what to collect

Most commonly
needed



Exact Timestamp

Status of the authentication session at
time of the issue

Live Logs/Detailed authentication
reports for affected endpoint

Screenshots/Recording of user
experience

Device configuration

Radius Authentication/Accounting
reports for the affected endpoint

System Scan Details from Secure
Client

Debugs for Authentication/Accounting
and Redirect activities

Client Provisioning Report filtered by
endpoint MAC

Packet capture collected when issue
manifested

Posture Report filtered by endpoint
MAC

DART bundle collected after the
problem

Screenshots of related ISE
configuration

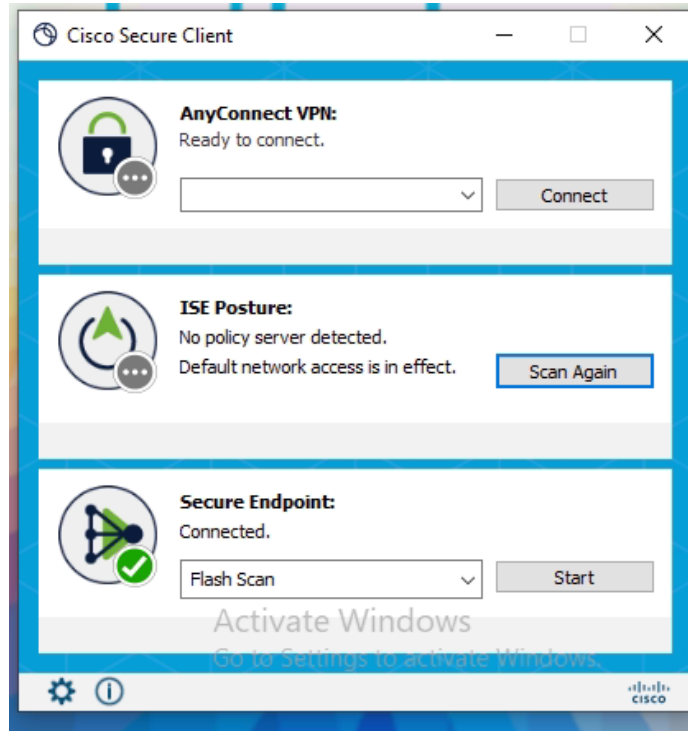
Packet capture collected when issue
manifested

Support bundle with posture related
components in 'DEBUG'

Less commonly
needed

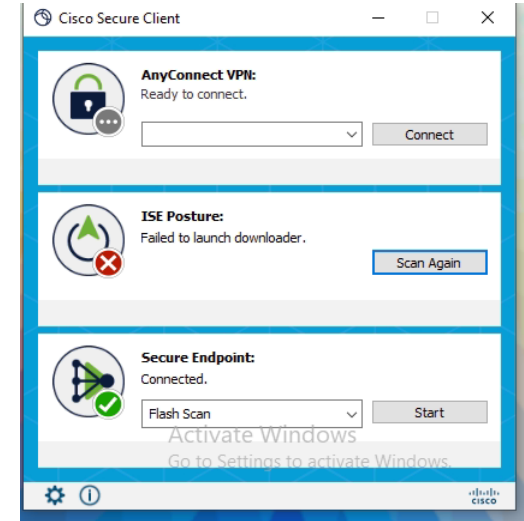
CISCO *Live!*

Learn on Example



No Policy Server Detected

Learn on Example – Failed to launch Downloader




CISCO *Live!*


Amsterdam | February 5-9, 2024

go


Cisco Secure Client

**AnyConnect VPN:**
Ready to connect.

Connect



**ISE Posture:**
Failed to launch downloader.

Scan Again

**Secure Endpoint:**
Connected.

Flash Scan

Start



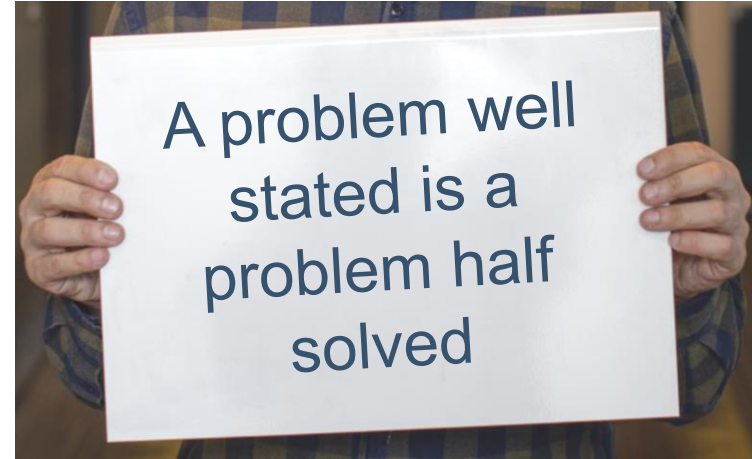
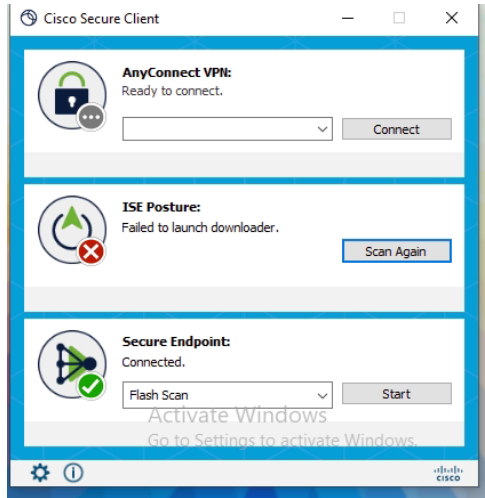
© 2024 Cisco

Define the Problem

ISE Posture Agent is now failing with Failed to Launch Downloader

Define the Problem

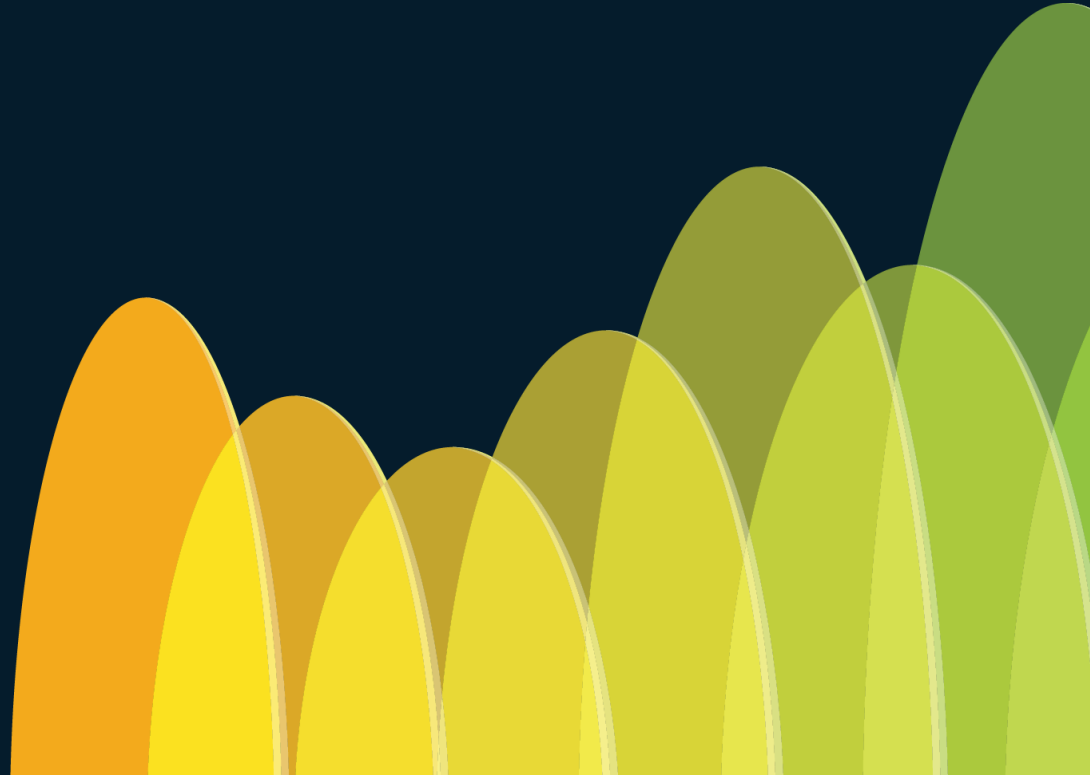
ISE Posture Agent is now failing
with Failed to Launch Downloader



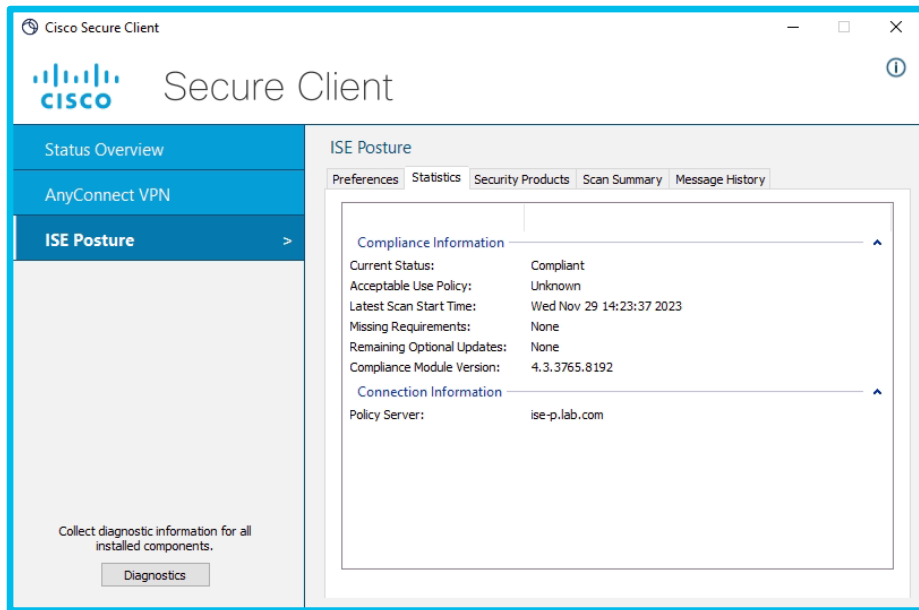
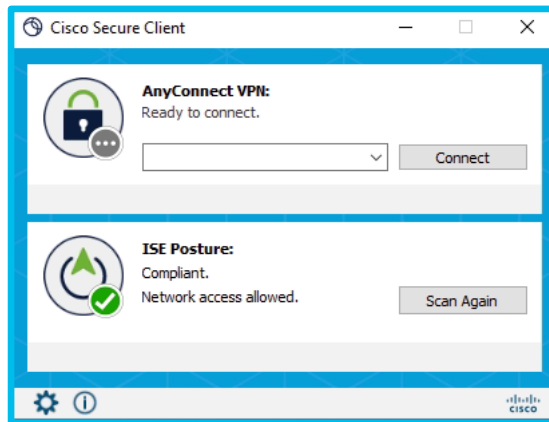
Which is the problematic pillar ?



Agent Side Troubleshooting



System Scan Details



ISE Posture - Details

The screenshot shows the Cisco Secure Client interface with the 'ISE Posture' section selected. The 'Compliance Information' tab is active, displaying the following details:

Compliance Information	
Current Status:	Compliant
Acceptable Use Policy:	Unknown
Latest Scan Start Time:	Wed Nov 29 14:23:37 2023
Missing Requirements:	None
Remaining Optional Updates:	None
Compliance Module Version:	4.3.3765.8192

Below the compliance information, the 'Connection Information' section shows:

Connection Information	
Policy Server:	ise-p.lab.com

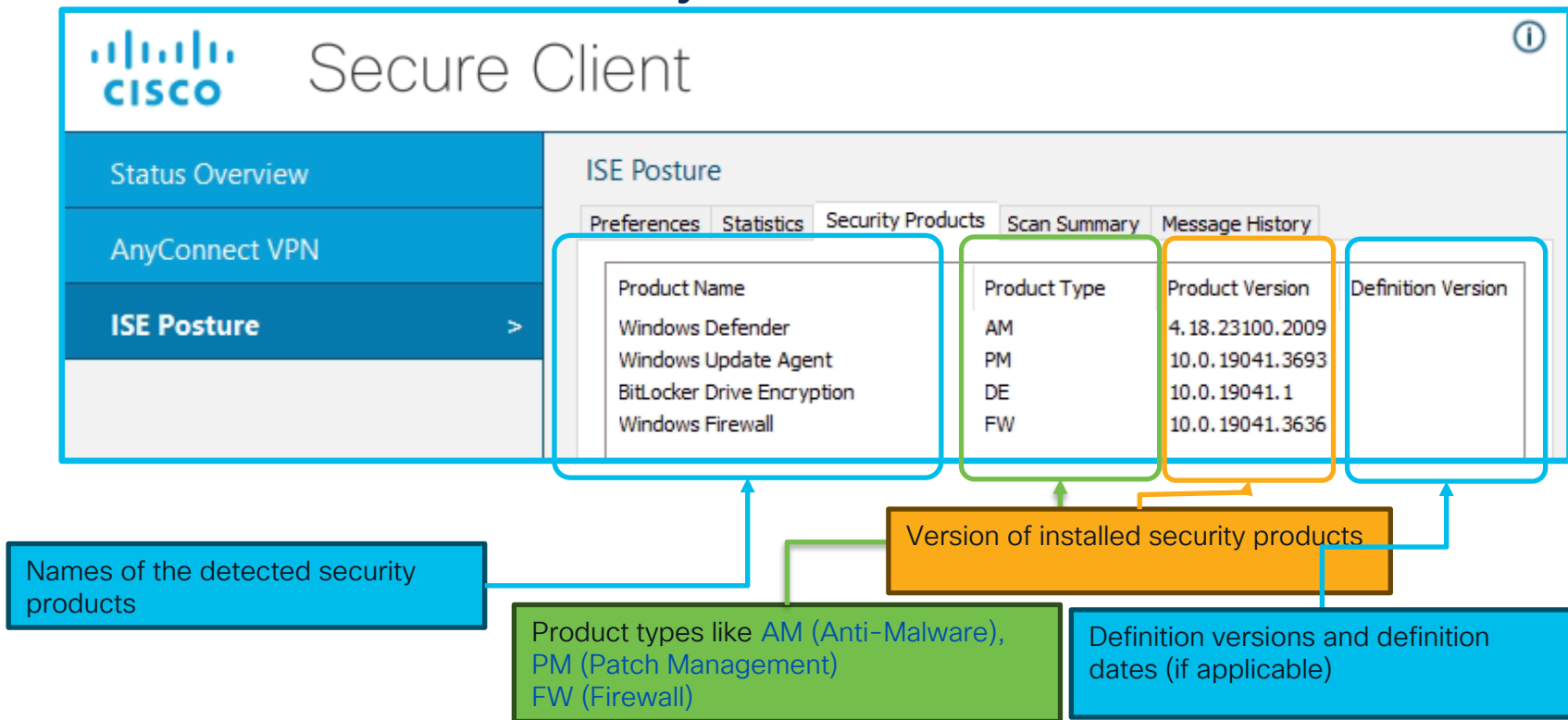
At the bottom left, there is a button labeled 'Diagnostics' with the text 'Collect diagnostic information for all installed components.' above it.

Current posture status returned from ISE to endpoint

Time and data of last scan

FQDN of the PSN which performed last posture check

ISE Posture - Security Products



ISE Posture – Scan Summary

Cisco Secure Client

Secure Client

Status Overview

AnyConnect VPN

ISE Posture >

ISE Posture

Preferences Statistics Security Products Scan Summary Message History

	Required	Updates	Status
1	✓	Any_AM_Installation_Win	Done
2	✓	Win_10_FW	Done

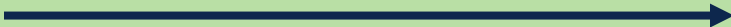
Status for each Requirement
obtained from PSN (Passed/Failed)

List of the Requirement obtained
from ISE. Requirements names here
are the same which defined on ISE.

Browser



Default Gateway IP



Discovery Host

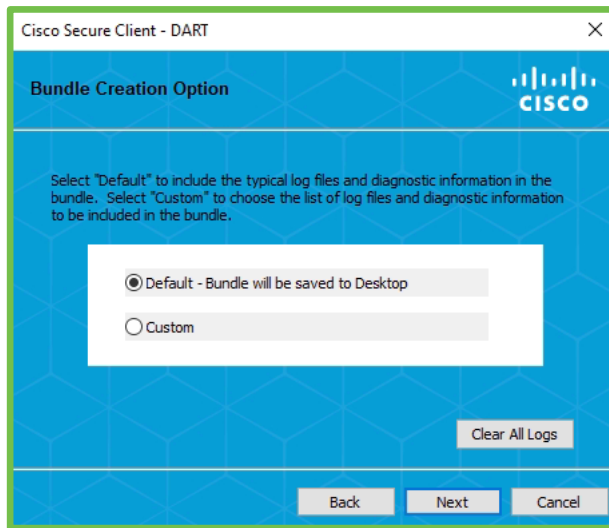


enroll.cisco.com



Disable proxy in
browser to get
proper results


Clearing Logs



Packet Capture

Enable Rescan Button	Enabled ▾
Disable UAC Prompt	No ▾



**ISE Posture:**
Compliant.
Network access allowed.

Scan Again

http

For general redirect troubleshooting
tcp.port==80 is more effective

DNS

In case if we know which FQDN
we are looking for:
dns.qry.name ==
"posture.demo.local"

IP address of PSNs

In unknown environment better
to use CP portal port as a file:
tcp.port==8443



Packet Capture

HTTP Discovery Host

HTTP Default GW

Enroll.cisco.com

Nslookup psn-1.cisco.com

http

For general redirect troubleshooting
tcp.port==80 is more effective

DNS

In case if we know which FQDN we are looking for:
dns.qry.name ==
"posture.demo.local"

IP address of PSNs

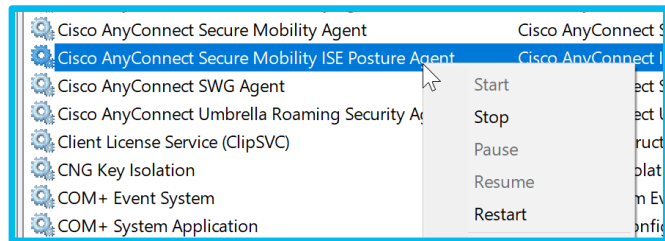
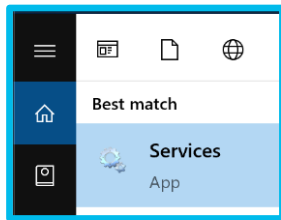
In unknown environment better to use CP portal port as a file:
tcp.port==8443

How to get the right data

1. Start Wireshark

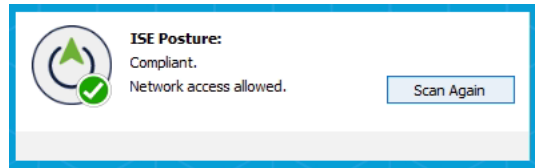


2. Manually restart ISE Posture service to trigger discovery host



3. Make it easy and enable rescan button

Enable Rescan Button	Enabled
Disable UAC Prompt	No



99 5.517196 104.86.110.209 192.168.255.250 HTTP 734 HTTP/1.1 200 OK (text/html)

94 5.481287 192.168.255.250 104.86.110.209 HTTP 368 GET /favicon.ico HTTP/1.1
99 5.517196 104.86.110.209 192.168.255.250 HTTP 734 HTTP/1.1 200 OK (text/html)

Redirect URL in the response. FQDN from this URL can be used to make DNS filter more specific

Frame 99: 734 bytes on wire (5872 bits), 734 bytes captured (5872 bits) on interface 0
Ethernet II, Src: Cisco_44:c2:60 (24:e9:b3:44:c2:60), Dst: Tp-LinkT_15:6c:c3 (c0:4a:00:15:6c:c3)
Internet Protocol Version 4, Src: 104.86.110.209, Dst: 192.168.255.250

Transmission Location: https://posture.demo.local:8443/portal/gateway?sessionId=0a3e949c000000405c03e8ed&portal=

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Location: https://posture.demo.local:8443/portal/gateway?sessionId=0a3e949c000000405c03e8ed&portal=40f01bd0-2e02-11e8-ba71

109 6.463447 192.168.255.250 192.168.28.100 DNS 78 Standard query 0xa91a A posture.demo.local

192.168.28.100 192.168.255.250 DNS 94 Standard query response 0xa91a A posture.demo.local

Frame 110: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
Ethernet II, Src: Vmware_b6:39:8a (00:50:56:b6:39:8a), Dst: Tp-LinkT_15:6c:c3 (c0:4a:00:15:6c:c3)
Internet Protocol Version 4, Src: 192.168.28.100, Dst: 192.168.255.250
User Datagram Protocol, Src Port: 53, Dst Port: 60395

Domain Name System (response)

Transaction ID: 0xa91a

Flags: 0x8580 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

posture.demo.local: type A, class IN

Name: posture.demo.local

[Name Length: 18]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

posture.demo.local: type A, class IN

IP address from 'Answer' can be used to filter communication with specific PSN

posture.demo.local: type A, class IN, addr 192.168.28.110

Answers

posture.demo.local: type A, class IN, addr 192.168.28.110

Endpoint – Packet Capture

By looking on URL in the browser we can confirm that redirection works in general

During investigation of packet capture we need to focus on:

- DNS requests for ISE FQDN – Are we getting response or not?
- Connection attempts to the ISE IP over Client Provisioning Portal port

DNS Query/Response for ISE FQDN

No.	Time	Source	Destination	Protocol	Length	Info
Standard query 0x13be A clemea19-ise1.demo.local						
171	25.347751	192.168.255.173	192.168.28.110	DNS	84	Standard query 0x13be A clemea19-ise1.demo.local
172	25.382641	192.168.28.110	192.168.255.173	DNS	170	Standard query response 0x3fa1 AAAA d3ag4hukkh62yn.cloudfront.net SOA ns-130.awsdns-16.com
173	25.404620	192.168.28.110	192.168.255.173	DNS	100	Standard query response 0x13be A clemea19-ise1.demo.local A 192.168.28.110
Standard query response 0x13be A clemea19-ise1.demo.local A 192.168.28.110						
181	25.730833	192.168.255.173	192.168.28.110	TCP	66	51764 → 8443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
182	25.757203	192.168.28.110	192.168.255.173	TCP	54	8443 → 51764 [RST, ACK] Seq=1 Ack=1 Win=8192 Len=0
183	26.269726	192.168.255.173	192.168.28.110	TCP	66	[TCP Spurious Retransmission] 51764 → 8443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
184	26.276804	192.168.255.173	192.168.28.110	TCP	66	51764 → 8443 [SYN]
185	26.784552	192.168.28.110	192.168.255.173	TCP	54	8443 → 51764 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	26.789294	192.168.28.110	192.168.255.173	TCP	54	8443 → 51764 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

SYN requests getting RST immediately

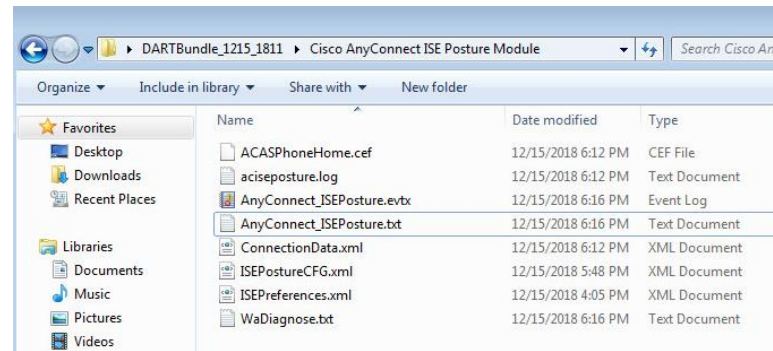
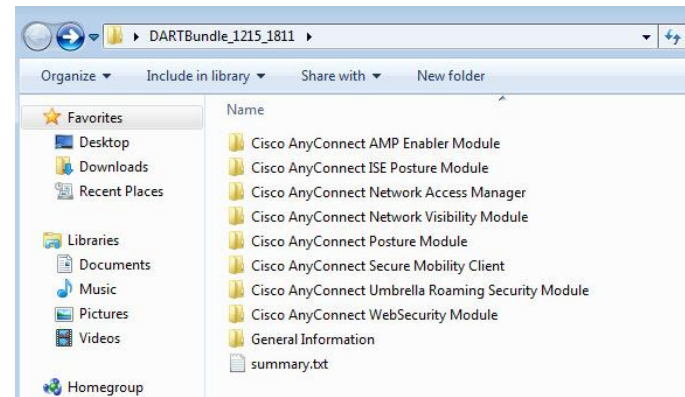
Agent side troubleshooting

- DART analysis

Main file to start - **Secure Client_ISEPosture.txt**.

This file is located in **Cisco Secure Client ISE Posture Module** folder

This file contains all information related to discovery process.



Agent side troubleshooting

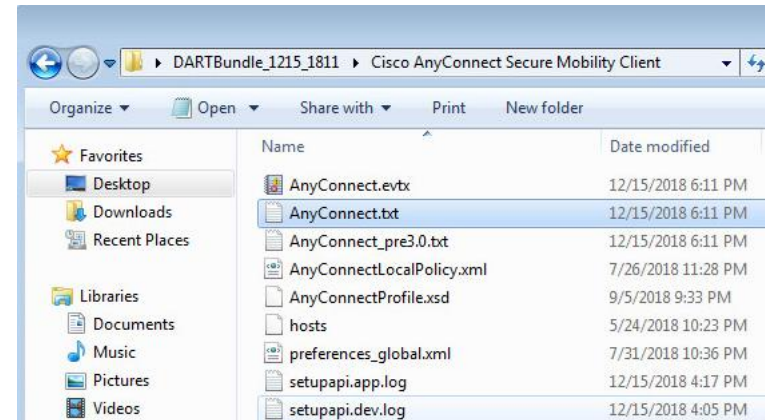
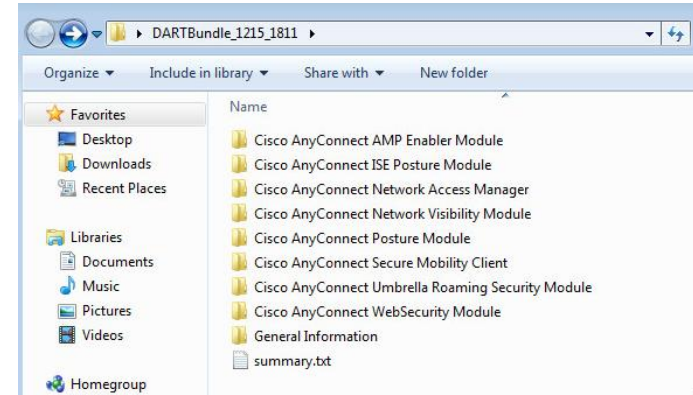
- DART analysis (continue)

General Secure Client log file - **Secure Client.txt**

File is located in **Cisco Secure Client Secure Mobility Client** folder

Is extremely useful for troubleshooting:

- Any certificate related Error/Warnings seen during posture process,
- Any issues related to upgrade of Secure Client components,
- In Posture-over-VPN use case can be used as additional source of data – like when session has been initiated by the user, when banner has been accepted and so on,



Agent side troubleshooting

– DART analysis (continue)

Log location for MAC OS is not obvious

- before 4.6 – DART > /DARTBundle_0824_1451/General Information/system.log
- 4.6, 4.7(?), 4.9(?) – DART > /DARTBundle_0824_1451/General Information/log_result.txt
- 4.9 again system.log
- files are quite huge and contain a lot of unneeded information



Agent side troubleshooting

– DART analysis

1. Find Discovery Restart event closest to the issue timestamp (keywords ‘Restarting Discovery’, ‘HTTP Discovery’),

Restart Discovery

```
Line 3575: 2018/12/15 17:48:08 1251 Level: info Restarting Discovery.  
Line 3840: 2018/12/15 17:48:59 1251 Level: info Restarting Discovery.  
Line 3991: 2018/12/15 17:50:24 1251 Level: info Restarting Discovery.  
Line 4214: 2018/12/15 18:00:54 1251 Level: info Restarting Discovery.  
Line 4308: 2018/12/15 18:01:14 1251 Level: info Restarting Discovery.  
Line 4530: 2018/12/15 18:11:45 1251 Level: info Restarting Discovery.  
Line 4642: 2018/12/15 18:12:01 1251 Level: info Restarting Discovery.
```

<output omitted>

2. Highlight every stage 1 probe target (Keyword ‘Probing no MNT stage targets’),

2024/01/16 02:05:15 [Information] csc_iseagent Function: SwiftHttpRunner::collectNoMntTargets Thread Id: 0x1070 File: SwiftHttpRunner.cpp Line: 1400 Level: debug

Probing no MNT stage targets (#5): Redirection target 10.52.14.254, Redirection target fe80::5:73ff:fea0:e, Redirection target enroll.cisco.com,

Auth-Status target ise-p.lab.com with path /auth/status, Auth-Status target ise-s.lab.com with path /auth/status, .

3. Follow the logs to see result for each probe

2024/01/16 02:05:17 [Information] csc_iseagent Function: Target::Probe Thread Id: 0x1140 File: Target.cpp
Line: 212 Level: debug Status of Redirection target 10.52.14.254 is 6 <Not Reachable.>.



Agent side troubleshooting

– DART analysis

Secure Client ISE posture module uses the following codes to display operation results:

- 0 – UNKNOWN,
- 1 – FOUND_SERVER,
- 2 – FOUND_SERVER_INVALID_CERT,
- 3 – UNAUTHORIZED_HEADEND,
- 4 – LEGACY_HEADEND ,
- 5 – INVALID_SERVER,
- 6 – NOT_REACHABLE,
- 7 – GENERAL_ERROR

In all modern Secure Client versions after every code description is printed as well in <>

DART analysis

4. Find which PSN in the deployment replied to the agent

```
Target::fetchPostureStatus Thread Id: 0xBF0 File:  
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libnaccommon  
\Target.cpp Line: 401 Level: debug POST request to URL (  
https://ciscolive-ise2.demo.local:8443/auth/ng-discovery), returned status 0  
<Operation Success.>.
```

5. Make a note of the session ID from reply

```
SwiftHttpRunner::invokePosture Thread Id: 0x1340 File:  
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libswift\Swift  
HttpRunner.cpp Line: 1407 Level: debug MSG NS SWISS NEW SESSION,  
{ise_fqdn="ciscolive-ise2.demo.local"}, {posture_port="8443"},  
{posture_path="/auth/perfigo_validate.jsp"},  
{posture_domain="posture_domain"}, {posture_status="Compliant"},  
{session_id="0a3e949c000002585cf00588"},
```

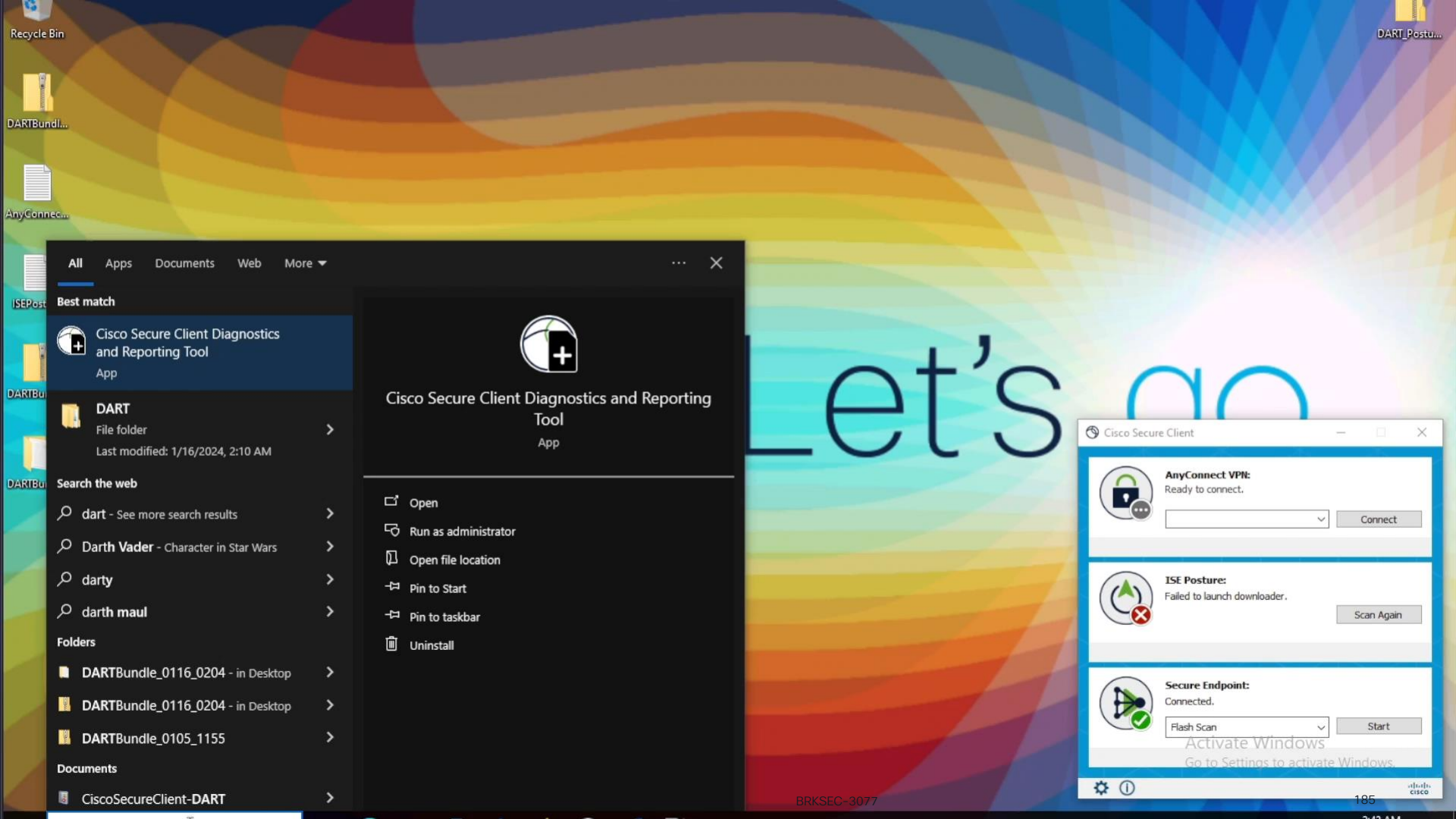
DART analysis

Table below contain list of important keywords which can be used during DART analysis

Keyword	Meaning
Probing no MNT stage targets	Lists the stage 1 discovery targets
MSG_NS_SWISS_NEW_SESSION	Indicates that PSN is found. This message has the FQDN, session id and the URL information
MSG_SU_AVASLIST	Lists the softwares installed in the endpoint
MAC List	Helps find the list of Mac
IP List	Helps find the list of IP
Perfigo-DM-Error=1010	Indicates posture status is pending
Perfigo-DM-Error=0	Indicates posture status is Compliant
Perfigo-DM-Error=5008	Indicates posture status is Non-Compliant
Perfigo-DM-Error=5009	Indicates network is blocked
Perfigo-DHCP-Release-Delay	DHCP release delay sent by PSN
Perfigo-DHCP-Renew-Delay	DHCP renew delay sent by PSN
Bypass posture	This message is seen when lease is enabled. This message can also be erroneously seen when stale session exist in PSN

Demo – Learn on the example





Recycle Bin

DART_Postu...

DARTBundl...

AnyConnec...


ISEPost


DARTBu

DARTBu


All Apps Documents Web More


Best match


 Cisco Secure Client Diagnostics and Reporting Tool
App


 DART
File folder
Last modified: 1/16/2024, 2:10 AM

Search the web


 dart - See more search results


 Darth Vader - Character in Star Wars


 darty

 darth maul


Folders


 DARTBundle_0116_0204 - in Desktop

 DARTBundle_0116_0204 - in Desktop

 DARTBundle_0105_1155

Documents

 CiscoSecureClient-DART



Cisco Secure Client Diagnostics and Reporting Tool
App

Open

Run as administrator


Open file location

Pin to Start


Pin to taskbar

Uninstall


Cisco Secure Client

 **AnyConnect VPN:**
Ready to connect.

Connect

 **ISE Posture:**
Failed to launch downloader.



Scan Again

 **Secure Endpoint:**
Connected.

Flash Scan


Start

Activate Windows
Go to Settings to activate Windows

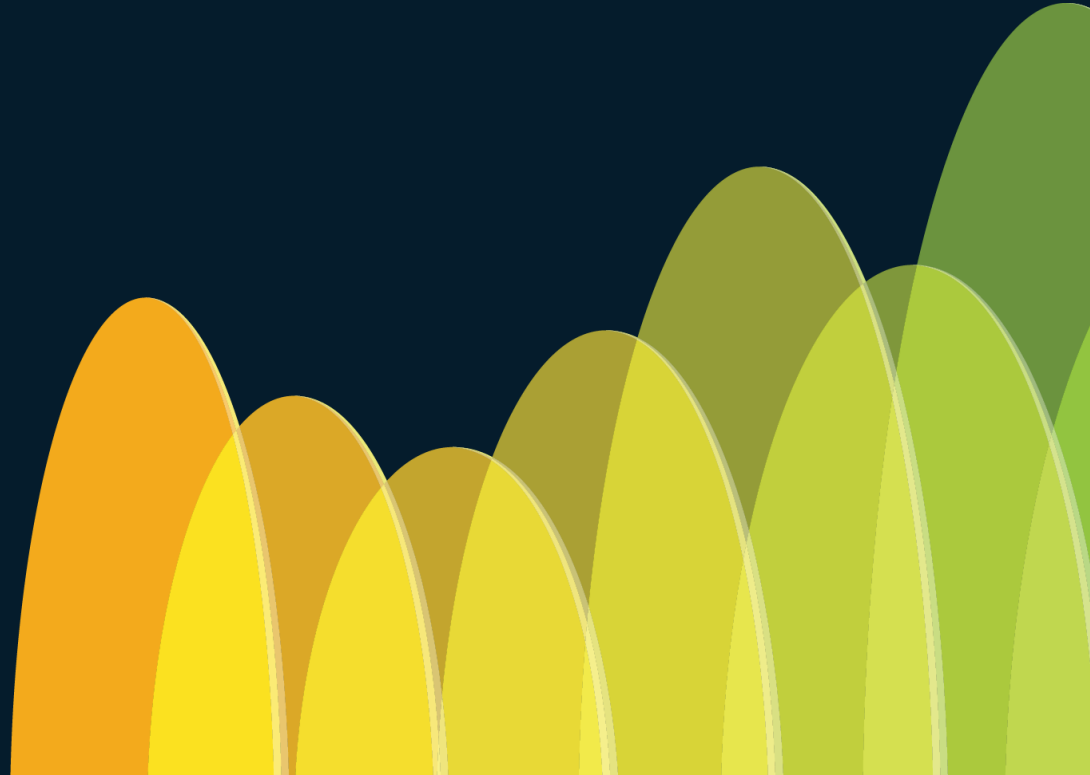
BRKSEC-3077

185

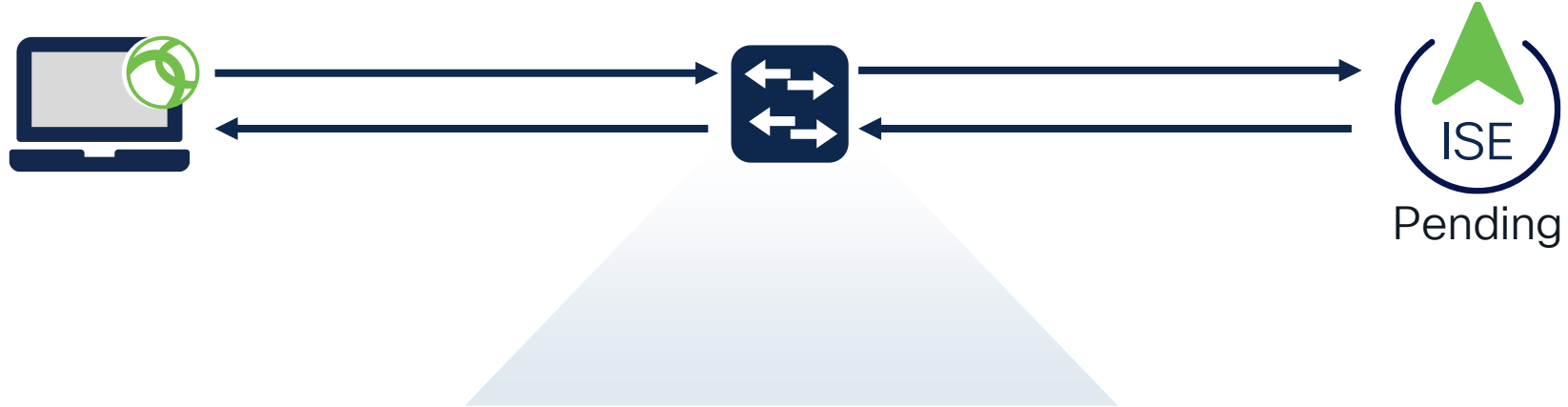



```
C:\Users\pc-1\Desktop\DARTBundle_0116_0204\Cisco Secure Client\ISE Posture\Logs\ISEPosture.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
ConnectionData.xml ISEPosture.txt new 1
162 igData.cpp Line: 43 Level: info ISEPostureCFG.xml present. Using it for config.
163 wiftHttpRunner.cpp Line: 895 Level: warn Discarding Ng-Discovery target ise-s.lab.com with path /auth/ng-discovery as it is already present.
164 wiftHttpRunner.cpp Line: 895 Level: warn Discarding Ng-Discovery target ise-p.lab.com with path /auth/ng-discovery as it is already present.
165 le: SwiftHttpRunner.cpp Line: 1483 Level: debug Probing MNT stage targets (#4): Ng-Discovery target ise-p.lab.com with path /auth/ng-discovery, Ng-I
166 ile: SwiftHttpRunner.cpp Line: 1757 Level: debug Probing Mnt stage Ng-Discovery target ise-p.lab.com with path /auth/ng-discovery.
167 Connection.cpp Line: 330 Level: debug Url=https://ise-p.lab.com:8443/auth/ng-discovery.
168 : 0x1070 File: DefaultGatewayRecordManager.cpp Line: 91 Level: info PSN found previously for gateway 10.52.14.254, so it won't take much time in dis
169 Connection.cpp Line: 332 Level: debug Encoded Url=https://ise-p.lab.com:8443/auth/ng-discovery.
170 070 File: SwiftHttpRunner.cpp Line: 580 Level: info Enabling next round timer.
171 Line: 552 Level: debug initialization done.
172 nsport_winhttp.c Line: 5987 Level: debug Connection to the server failed.
173 t.cpp Line: 472 Level: debug POST request to URL (https://ise-p.lab.com:8443/auth/ng-discovery), returned status -1 <Operation Failed.>, stage 2.
174 12 Level: debug Status of Ng-Discovery target ise-p.lab.com with path /auth/ng-discovery is 6 <Not Reachable.>.
175 ile: SwiftHttpRunner.cpp Line: 1757 Level: debug Probing Mnt stage Ng-Discovery target ise-s.lab.com with path /auth/ng-discovery.
176 Connection.cpp Line: 330 Level: debug Url=https://ise-s.lab.com:8443/auth/ng-discovery.
177 Connection.cpp Line: 332 Level: debug Encoded Url=https://ise-s.lab.com:8443/auth/ng-discovery.
178 Line: 552 Level: debug initialization done.
179 nsport_winhttp.c Line: 5987 Level: debug Connection to the server failed.
180 t.cpp Line: 472 Level: debug POST request to URL (https://ise-s.lab.com:8443/auth/ng-discovery), returned status -1 <Operation Failed.>, stage 2.
181 12 Level: debug Status of Ng-Discovery target ise-s.lab.com with path /auth/ng-discovery is 6 <Not Reachable.>.
182 ile: SwiftHttpRunner.cpp Line: 1757 Level: debug Probing Mnt stage Ng-Discovery target ise-p.lab.com with path /auth/ng-discovery.
183 pConnection.cpp Line: 330 Level: debug Url=https://ise-p.lab.com:8905/auth/ng-discovery.
184 pConnection.cpp Line: 332 Level: debug Encoded Url=https://ise-p.lab.com:8905/auth/ng-discovery.
185 c Line: 552 Level: debug initialization done.
186 .c Line: 430 Level: debug --- Http Response Headers ---.
187 .c Line: 437 Level: debug HTTP-Version: 1.1.
188 .c Line: 437 Level: debug Status-Code: 200.
189 .c Line: 437 Level: debug Connection: keep-alive.
190 .c Line: 437 Level: debug Date: Tue, 16 Jan 2024 10:04:17 GMT.
191 .c Line: 437 Level: debug Keep-Alive: timeout=20.
192 .c Line: 437 Level: debug Content-Length: 23.
193 .c Line: 437 Level: debug Server: server.
194 .c Line: 437 Level: debug X-Frame-Options: SAMEORIGIN.
195 .c Line: 437 Level: debug Strict-Transport-Security: max-age=31536000; includeSubDomains.
196 .c Line: 437 Level: debug X-Content-Type-Options: nosniff.
197 .c Line: 437 Level: debug Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inl
198 .c Line: 437 Level: debug X-XSS-Protection: 1; mode=block.
199 .c Line: 437 Level: debug Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform-Version,Sec-CH-UA-
Activate Windows
```

Network Device Troubleshooting



Cisco Switch



- Show access-session
- IP Device Tracking DB
- Redirect ACL

Cisco Switch



```
KSEC-3850-1#sh authentication sessions interface g1/0/5 details
  Interface: GigabitEthernet1/0/5
    IIF-ID: 0x18486C6C
    MAC Address: 0050.56b6.0bc6
    IPv6 Address: fe80::6c97:5272:c80c:5ef7
                  2001:10::107
    IPv4 Address: Unknown
    User-Name: EXAMPLE\bob
    Status: Authorized
    Domain: DATA
    Oper host mode: multi-auth
    Oper control dir: both
    Session timeout: N/A
    Common Session ID: 0A3E946C000015073D01055F
    Acct Session ID: 0x000000b2
    Handle: 0xc10000a9
    Current Policy: POLICY_Gi1/0/5

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy: Should Secure

Server Policies:
  ACS ACL: xACSACLx-IP-CPP-DACL-5f8592bd
  URL Redirect ACL: skuchere_redirect
  URL Redirect: https://skuchere-ise30-1.example.com:8443/portal/gateway?sessionId=0A3E946C000015073D01055F
```

Cisco Switch - Access Session Details



```

DOT1X-SW-1#show access-session int
Nov 30 14:20:55.126: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to upgi0
Nov 30 14:20:56.126: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up/2 det
      Interface: GigabitEthernet0/2
      MAC Address: d4c9.3c52.6f46
      IPv6 Address: Unknown
      IPv4 Address: 10.52.14.186
      User-Name: alice@lab.com
      Status: Authorized
      Domain: DATA
      Oper host mode: multi-auth
      Oper control dir: both
      Session timeout: N/A
      Restart timeout: N/A
      Periodic Acct timeout: 172800s (local), Remaining: 172797s
      Common Session ID: 0A340E670000001405DDD4EF
      Acct Session ID: 0x0000000A
      Handle: 0x57000006
      Current Policy: DOT1X

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy: Should Secure
  Security Status: Link Unsecure

Server Policies:
  URL Redirect: https://ise-p.lab.com:8443/portal/gateway?sessionId=0A340E670000001405DDD4EF&portal=d9276eb2-c440-42d6-8055-3d72ed4769ab&action=da20d8ff2dcc0ad28
  URL Redirect ACL: POSTURE-REDIRECT

Method status list:
  Method      State
  dot1x       Authc Success
  
```

Cisco Switch – Device Tracking



```
DOT1X-SW-1#show ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0
```

IP Address	MAC Address	Vlan	Interface	Probe-Timeout	State	Source
10.52.14.186	d4c9.3c52.6f46	14	GigabitEthernet0/2	30	ACTIVE	ARP

```
Total number interfaces enabled: 1
Enabled interfaces:
Gi0/2
```

Redirection - HTTP Server

Http server on the switch disabled by default and need to be enabled by typing:

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

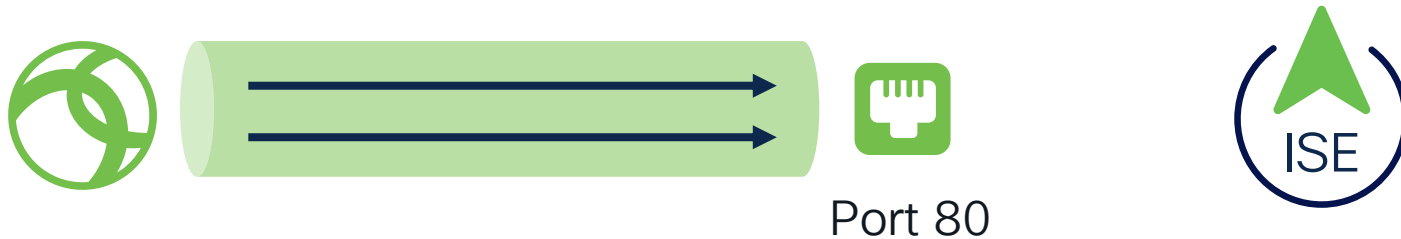
Often customers are against enabling http server since it may make switch vulnerable.

To keep only web redirect functionality and disable everything else we use:

```
(config)#ip http active-session-modules none
```



Cisco Switch (Proxy)



NADs – Cisco switch (Troubleshooting)

- Status of session and ACLs assigned to interface

```
# show authentication [access] sessions  
interface <interface_ID> [details]  
# show ip access-list interface  
<interface_ID>
```

- Debugs for Radius, Dot1x, authentication, redirection

```
# debug radius  
# debug dot1x all  
# debug authentication all  
# debug epm plugin redirect all
```

- Check configuration

```
# show run | s aaa  
# show run | s radius  
# show run | s access-list
```

NADs – Cisco WLC (intro)

Since we don't support WLC from AAA side normally we should not be going deep into platform problems.

To review status of authentication session we need –

GUI go to **Clients > Detail**

CLI issue **show client detail** *<ep mac address>*

Client state. In case of posture it will be either **POSTURE_REQD** or **CENTRAL_WEB_AUTH**

Redirect ACL name assigned from ISE

Redirect URL. Note: To get a full URL client details needs to be collected in CLI

Max Number of Records 10 Clear AVC Stats

General **AVC Statistics**

Policy Manager State POSTURE_REQD

Management Frame Protection No

Policy Manager State POSTURE_REQD

Data RateSet 1.0,2.0,5.5,11.0,6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

KTS CAC Capability No

802.11u Not Supported

802.11v BSS Transition Not Supported

Security Information

Security Policy Completed No

Policy Type RSN (WPA2)

Auth Key Mgmt 802.1x

Encryption Cipher CCMP (AES)

EAP Type EAP-TLS

AAA Override ACL Name DEMO-CPP-ACL

CTS Security Group Tag Not Applicable

AAA Override ACL Name DEMO-CPP-ACL

AAA Override ACL Applied Status Yes

Redirect URL https://posture.demo.local:8443/portal/

BRKSEC-9077

Redirect URL https://posture.demo.local:8443/portal/gateway?ses

NADs – Cisco WLC (continue)

AAA Servers investigation –

GUI go to **WLANs** > *<Choose your WLAN>* > **Security** > **AAA Servers**

CLI issue **show wlan** *<WLAN ID>*, scroll to “**Radius Servers**” section

Investigate Order of Radius servers on WLAN.
Ask yourself if those IPs are real IPs assigned
to server or those are IPs of LB VIP

Authentication Servers		Accounting Servers	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	
IP:192.168.28.110, Port:1812	⌵ ⌶ ⌴	IP:192.168.28.110, Port:1813	⌵ ⌶ ⌴
IP:192.168.28.111, Port:1812	⌵ ⌶ ⌴	IP:192.168.28.111, Port:1813	⌵ ⌶ ⌴

Note: There is no possibility to check from GUI which server is currently in use for authentication/accounting

```
(Cisco Controller) >show wlan 3  
<output omitted>
```

Radius Servers

```
Authentication..... 192.168.28.110 1812  
Authentication..... 192.168.28.111 1812 *  
Accounting..... 192.168.28.110 1813  
Accounting..... 192.168.28.111 1813 *
```

RADIUS Servers

RADIUS Server Overwrite interface ☒ Enabled

Interface Priority WLAN

Authentication Servers		Accounting Servers	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	
Server 1 IP:192.168.28.110, Port:1812	⌵ ⌶ ⌴	Server 1 IP:192.168.28.110, Port:1813	⌵ ⌶ ⌴
Server 2 IP:192.168.28.111, Port:1812	⌵ ⌶ ⌴	Server 2 IP:192.168.28.111, Port:1813	⌵ ⌶ ⌴

NADs – Cisco WLC (continue)

Redirect ACL name can be taken from Client Details, as well make a note of ISE server IP addresses configured under WLAN

GUI go to **SECURITY > Access Control Lists > Access Control Lists**

Enable Counters ☒

Name	Type
PERMIT-ALL-TRAFFIC	IPv4 <input checked="" type="checkbox"/>
ACL WEBAUTH_REDIRECT	IPv4 <input checked="" type="checkbox"/>
DEMO-CPP-ACL	IPv4 <input checked="" type="checkbox"/>

5	Permit	/	0.0.0.0	/	192.168.28.110
6	Permit	/	0.0.0.0	/	255.255.255.255

7	Permit	/	0.0.0.0	/	192.168.28.111
8	Permit	/	0.0.0.0	/	255.255.255.255

Access List Name DEMO-CPP-ACL

Deny Counters 40403

Ensure that PSNs IP addressed are properly excluded from redirection

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port						
1	Permit	/	/	UDP	Any	DNS	Any	Any	9106	<input checked="" type="checkbox"/>	
2	Permit	/	/	UDP	DNS	Any	Any	Any	8882	<input checked="" type="checkbox"/>	
3	Permit	/	/	UDP	Any	DHCP Server	Any	Any	0	<input checked="" type="checkbox"/>	
4	Permit	/	/	UDP	DHCP Server	Any	Any	Any	0	<input checked="" type="checkbox"/>	
5	Permit	/	192.168.28.110	Any	Any	Any	Any	Any	69383	<input checked="" type="checkbox"/>	
6	Permit	192.168.28.110	/	Any	Any	Any	Any	Any	129709	<input checked="" type="checkbox"/>	
7	Permit	/	192.168.28.111	Any	Any	Any	Any	Any	16773	<input checked="" type="checkbox"/>	
8	Permit	192.168.28.111	/	Any	Any	Any	Any	Any	30591	<input checked="" type="checkbox"/>	
9	Permit	/	192.168.30.110	Any	Any	Any	Any	Any	11	<input checked="" type="checkbox"/>	
10	Permit	/	192.168.30.110	Any	Any	Any	Any	Any	0	<input checked="" type="checkbox"/>	

Ensure that PSNs IP addressed are properly excluded from redirection

NADs – Cisco WLC (continue)

NAD Troubleshooting

RADIUS Authentication Servers > New

Server Index (Priority)

Server IP Address(Ipv4/Ipv6) **Specify IP of PSN**

Shared Secret Format

Shared Secret **Define shared secret**

Confirm Shared Secret

Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number

Server Status

Support for CoA **Enable CAO support (needed for Guest/Profiling/Posture)**

Server Timeout seconds **Put timeout larger then default 2 ses (5-10 sec)**

Network User ☒ Enable

Management ☒ Enable

Management Retransmit Timeout seconds

IPSec ☐ Enable

Basic config validation

General **Security** **QoS** **Policy-Mapping** **Advanced**

**Enable AAA override. This is needed to Assign authorization attributes from AAA server
For example: VLAN, ACL, Redirect**

Allow AAA Override ☒ Enabled

Coverage Hole Detection ☒ Enabled

Enable Session Timeout ☒ 1800 Session Timeout (secs)

Aironet IE ☒ Enabled

Diagnostic Channel ☐ Enabled

Override Interface ACL IPv4 IPv6

Layer2 Acl

URL ACL

P2P Blocking Action

Client Exclusion ☒ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling ☐ Enabled

Wi-Fi Direct Clients Policy

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☐ Required

OEAP

Split Tunnel ☐ Enabled

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

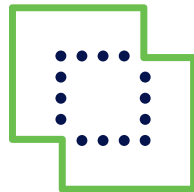
802.11b/g/n (1 - 255)

NAC

NAC State **Enable COA support on WLAN**

ASA/FTD

What is different



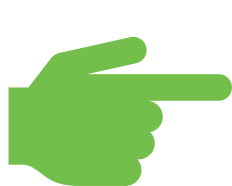
Cisco Secure
Firewall



1. Not all traffic may go into tunnel (tunnel-all VS split-tunneling)
2. MAC OS has no default GW on VPN adapters (utunX)
3. ASA can push Secure Client posture resources to client (ISE posture module, ISE posture profile but not a compliance module)

Cisco ASA/FTD – Resources

Ideally same AC version should be installed on both ASA/FTD and ISE



ASA > ISE



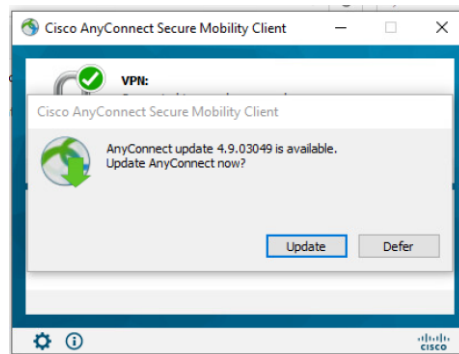
ASA = ISE



If ISE > ASA

It's possible to enable 'defer update' settings in ISE AC config but if user will press update accidentally this will result in error

Deferred Update	
Allowed for AnyConnect Software	Yes
Minimum Version Required for AnyConnect Software	4.9.1095
Allowed for Compliance Module	No
Minimum Version Required for Compliance Module	0.0.0.0
Prompt Auto Dismiss Timeout	None
Prompt Auto Dismiss Default Response	Update



NADs – Cisco ASA/FTD troubleshooting

What to check–

- Status of VPN client,
- Debugs for Radius, COA and Redirection
- VPN related configuration
- ASP drop capture/Capture on the interface where ISE is connected

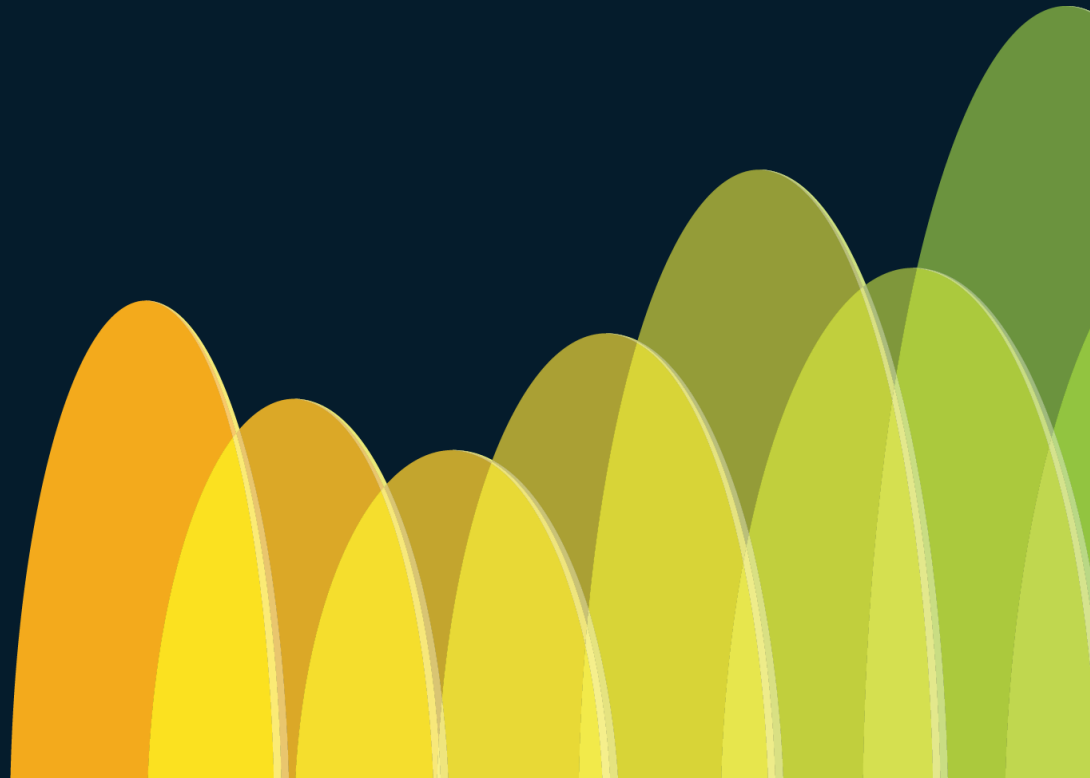
```
# show vpn-sessiondb detail  
Secure Client filter name  
<username>
```

```
# debug radius all  
# debug aaa url-redirect
```

```
# show run webvpn  
# show run access-list  
# show run tunnel-group  
# show run aaa-server  
# show run group-policy
```

```
# capture <NAME> type asp-drop  
# capture <NAME> interface <int> <filter>
```











Troubleshooting ISE



Troubleshooting ISE

Detailed Authentication report is always a good starting point

Live Logs

Status	Details	Repea...	Identity	Endpoint ID	Endpoint Prof...	Authentication Policy	Authorization Policy	Authorization Profiles
	▼		Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
		0	alice@lab.com	D4:C9:3C:52:6F:...	Windows10-Wo...	CiscoLive_LAB >> Default	CiscoLive_LAB >> Posture_Compliant	Posture_Compliant
			#ACSACL#-IP-...					
			alice@lab.com	D4:C9:3C:52:6F:...	Windows10-Wo...	CiscoLive_LAB >> Default	CiscoLive_LAB >> Posture_Compliant	Posture_Compliant
				D4:C9:3C:52:6F:...				
			alice@lab.com	D4:C9:3C:52:6F:...	Windows10-Wo...	CiscoLive_LAB >> Default	CiscoLive_LAB >> Posture_Unknown	Posture_Unknown

Troubleshooting ISE

Detailed Authentication report is always a good starting point

Overview	
Event	5200 Authentication succeeded
Username	alice@lab.com
Endpoint Id	D4:C9:3C:52:6F:46 ⓘ
Endpoint Profile	Windows10-Workstation
Authentication Policy	CiscoLive_LAB >> Default
Authorization Policy	CiscoLive_LAB >> Posture_Unknown
Authorization Result	Posture_Unknown

Take a note of authorization policy and authorization profile name. This may be needed for further configuration validation

Troubleshooting ISE

Authentication Details

Source Timestamp 2023-12-01 00:17:12.944

Received Timestamp 2023-12-01 00:17:12.944

Policy Server ise-p

Event 5200 Authentication succeeded

Username alice@lab.com

Endpoint Id D4:C9:3C:52:6F:46

Write down name of the PSN
which performed authentication

Troubleshooting ISE

Result

Class	CACS:0A340E670000001405DDD4EF:ise-p/490071257/58
EAP-Key-Name	19:65:68:a7:72:1b:80:f8:c0:1d:51:06:f7:7f:bc:af:17:00:b3:e7:c1:9b:86:27:9e:84:f1:ff:31:8d:6f:4d:9a:47:e2:ac:fe:2d:fc:f9:e8:58:62:01:7f:10:a3:7d:2b:85:7a:f4:dc:f2:e9:c8:fb:d2:c9:3c:99:f0:78:f3:84
cisco-av-pair	url-redirect-acl=POSTURE-REDIRECT
cisco-av-pair	url-redirect=https://ise-p.lab.com:8443/portal/gateway?sessionId=0A340E670000001405DDD4EF&portal=d9276eb2-c440-42d6-8055-3d72ed4769ab&action=cpp&token=07ce672dcfab3ada20d8ff2dcc0ad28
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Essential license consumed.

Redirect attributes returned to NAD

Posture Assessment Report

My Reports

Reports

Audit

Device Administration

Diagnostics

Endpoints and Users

Agentless Posture

Authentication Summary

Client Provisioning

Current Active Sessions

Endpoint & Logical Profi...

Endpoint Scripts Provisi...

External Mobile Device ...

Manual Certificate Provi...

PassiveID

Posture Assessment by ...

Posture Assessment by...

Posture Script Remediat...

Posture Script Condition

Profiled Endpoints Sum...

Operations · Reports

License Warning

Search

Help

Settings

Posture Assessment by Endpoint

From 2023-12-01 00:00:00.0 To 2023-12-01 01:06:10.0

Reports exported in last 7 days 0

Add to My Reports

Export To

Schedule

Filter

Refresh

Settings

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address	Endpoint OS	Agent
<div>×</div> <div>Today</div> <div>×</div>				Identity	Endpoint ID		Endpoint OS	
2023-12-01 00:22:19.928	✓		N/A	alice@lab.com	D4:C9:3C:52:6F:46	10.52.14.239	Windows 10 Professional 64-bit	Posture Agent for
2023-12-01 00:17:20.246	✓		N/A	alice@lab.com	D4:C9:3C:52:6F:46	10.52.14.239	Windows 10 Professional 64-bit	Posture Agent for
2023-12-01 00:17:18.512	✓		N/A	alice@lab.com	D4:C9:3C:52:6F:46	10.52.14.239	Windows 10 Professional 64-bit	Posture Agent for

Rows/Page

3

<<

<

1

>

>>

3 Total Rows

BRKSEC-3077

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

207

Posture Assessment Report

The screenshot shows the Cisco ISE interface for a Posture Assessment by Endpoint report. The report is titled "Posture Assessment by Endpoint" and shows data for the period "From 2023-12-01 00:00:00.0 To 2023-12-01 01:06:10.0". The report is filtered for "Today" and shows 3 rows of data. The table columns are: Logged At, Status, Details, PRA Action, Identity, Endpoint ID, IP Address, Endpoint OS, and Agent. The first row is highlighted with a green box around the "Logged At" column and a blue box around the "Status" column. The second row is highlighted with an orange box around the "Details" column. Annotations include: a blue box pointing to the "Status" column with the text "Check what decision ISE made (Compliant/Non-Compliant)"; a green box pointing to the "Logged At" column with the text "Take a note of last posture scan time"; and an orange box pointing to the "Details" column with the text "Open detailed report to gather more data".

Operations · Reports

License Warning

My Reports

Reports

Audit

Device Administration

Diagnostics

Endpoints and Users

Agentless Posture

Authentication Summary

Client Provisioning

Current Active Sessions

Endpoint & Logical Profi...

Endpoint Scripts Provisi...

External Mobile Device ...

Manual Certificate Provi...

PassiveID

Posture Assessment by ...

Posture Assessment by...

Posture Script Remediat...

Posture Script Condition

Profiled Endpoint Sum

Posture Assessment by Endpoint

From 2023-12-01 00:00:00.0 To 2023-12-01 01:06:10.0

Reports exported in last 7 days 0

Add to My Reports Export To Schedule

Filter Refresh

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address	Endpoint OS	Agent
2023-12-01 00:22:19.928	✓		N/A	alice@lab.com	D4:C9:3C:52:6F:46	10.52.14.239	Windows 10 Professional 64-bit	Posture Agent for
2023-12-01 00:17:20.246	✓		N/A	alice@lab.com	D4:C9:3C:52:6F:46	10.52.14.239	Windows 10 Professional 64-bit	Posture Agent for
2023-12-01 00:17:18.512	✓		N/A	alice@lab.com	D4:C9:3C:52:6F:46	10.52.14.239	Windows 10 Professional 64-bit	Posture Agent for

Rows/Page 3 1 3 Total Rows

Check what decision ISE made (Compliant/Non-Compliant)

Take a note of last posture scan time

Open detailed report to gather more data

Posture Assessment Report

Posture Report

Posture Status	Compliant
Logged At	2023-12-01 01:11:13.774

Posture Policy Details

Policy	Name	Enforcement Type	Status	Passed Conditions	Failed Conditions
Default_AntiMalware_Policy_Win	Any_AM_Installation_Win	Mandatory	Passed	am_inst_v4_ANY_vendor	
LAB_CiscoLive_Win	Win_10_FW	Mandatory	Passed	fw_enabled_v4_WindowsFirewall_10_x	

List of matched posture Policies

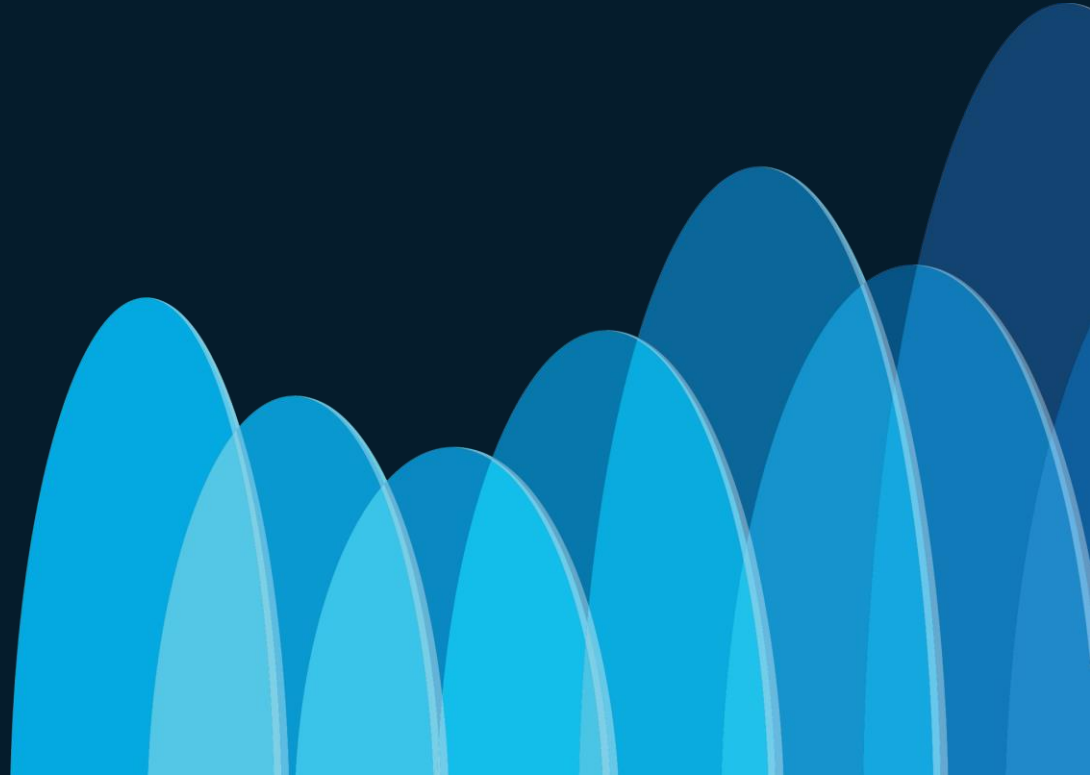
Posture requirements taken from Posture Policies

Type of the requirement

Result of posture check

Names of passed posture conditions

Learn on Example



Live Logs Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authorization Profiles	Posture Status	Se
×		▼		Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorization Profiles	Posture Status	Si
Jan 27, 2024 10:01:53.5...	🔵	📄	0	alice@lab.com	D4:C9:3C:52:6F:...	Windows1...	CiscoLive...	CiscoLive...	Posture_Unknown	Pending	⋮ ise
Jan 27, 2024 09:55:49.9...	✅	📄		alice@lab.com	D4:C9:3C:52:6F:...	Windows1...	CiscoLive...	CiscoLive...	Posture_Unknown	Pending	⋮ ise
Jan 27, 2024 09:31:33.3...	✅	📄		alice@lab.com	D4:C9:3C:52:6F:...	Windows1...	CiscoLive...	CiscoLive...	Posture_Compliant	Compliant	⋮ ise
Jan 27, 2024 09:31:33.0...	✅	📄			D4:C9:3C:52:6F:...					Compliant	⋮ ise
Jan 27, 2024 09:31:19.7...	✅	📄		alice@lab.com	D4:C9:3C:52:6F:...	Windows1...	CiscoLive...	CiscoLive...	Posture_Unknown	Pending	⋮ ise

Where we are

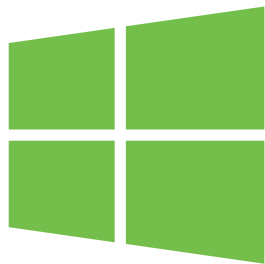
- Captures shows no communication over port 8443
- Packets are not crossing the switch
- Pending state on ISE, no posture Reports received



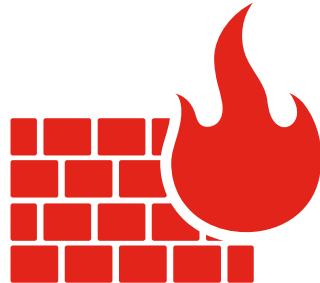
Third party Firewall

Local team added on Secure Endpoint more restrictive rules due to a missing fix on a specific CVE.

This was breaking the communications over port 8443 to ISE



TCP.PORT 8443



Learn on Example #2



Agentless: Common issues #1

Agentless Posture

From 2023-01-05 00:00:00.0 To 2023-01-05 15:36:55.0
Reports exported in last 7 days 0

Add to My Reports Export To Schedule

Endpoint not Reacheable

Filter Refresh

Server	Event	Session ID	EndPoints ID	IP Address	OS	Failure Reason
EndPoints ID						

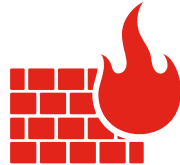
```
2022-10-01 06:56:47,609 INFO [pool-233-thread-7][] cisco.cpm.posture.events.PostureMessagesConsumer
-:::- Received on queue=SCRIPT-UPLOAD-FAILED, sessionId=25276A0A0000105BE2F00935,
endpointIP=10.106.39.38, mac=B4-96-91-22-A9-48, os=WINDOWS, failureReason=null
```

Agentless: Common issues #1

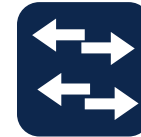


Port 5985

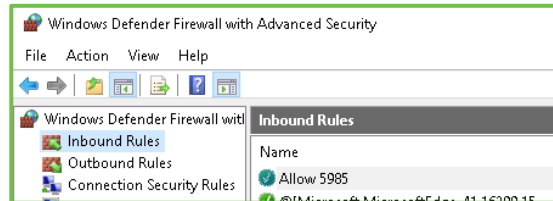
No.	Time	Source	Destination	Protocol	Length	Destination Port	Source Port	Source Port	Info
2360	18:08:18.85	10.127.197.83	10.106.39.38	TCP	74		59027	59027	59027 → 5985 [SYN] Seq=0 W
2454	18:08:18.85	10.127.197.83	10.106.39.38	TCP	74		59039	59039	59039 → 5985 [SYN] Seq=0 W
2477	18:08:18.85	10.127.197.83	10.106.39.38	TCP	74		59039	59039	[TCP Retransmission] 59039
2534	18:08:18.85	10.127.197.83	10.106.39.38	TCP	74		59041	59041	59041 → 5985 [SYN] Seq=0 W
2684	18:08:18.85	10.127.197.83	10.106.39.38	TCP	74		59059	59059	59059 → 5985 [SYN] Seq=0 W



Firewall



ACL/DACL



Agentless: common issues #2

✓	🔒	posture_user	B4:96:91:22:A9:...	Pending	⋮	AgentlessPosture >> DOT1X-CPP-Agentless-Posture_Failure	CPP Regular Posture	AgentlessPosture >> Default	10.106.39.38
✓	🔒		B4:96:91:22:A9:...		⋮				
✓	🔒	posture_user	B4:96:91:22:A9:...	NotApplicable	⋮	AgentlessPosture >> DOT1X-CPP-Agentless-Posture :	CPP Agentless Posture	AgentlessPosture >> Default	

Export Summary

My Reports >

Reports ▾

Audit >

Device Administration >

Diagnostics >

Endpoints and Users ▾

Agentless Posture

Agentless Posture ⓘ

From 2020-09-29 00:00:00.0 To 2020-10-06 04:20:07.0

Reports exported in last 7 days 0

IPs are unreachable

2020-10-					
2020-10-					
2020-10-01 03:48:41.6...	Agentless script upload failed	25276A0A00001058E2467C59	Ips are unreachable	B4:96:91:22:A9:48	10.106.39.38

Agentless: Common issues #2

```
2020-10-01 06:56:47,609 INFO [pool-233-thread-7][ cisco.cpm.posture.events.PostureMessagesConsumer
-::::- Received on queue=SCRIPT-UPLOAD-FAILED, sessionId=25276A0A0000105BE2F00935,
endpointIP=10.106.39.38, mac=B4-96-91-22-A9-48, os=WINDOWS, failureReason=null
```

HTTP 401

Time	Status	Identity	Endpoint ID	Endpoint Profile	Authentication Pol...	Authorization Policy	Authorization Profiles	Posture Status	IP Address
Aug 22, 2020 04:51:04.2...		DOMINION\adott1xposture	DC...	Microsoft-Workstation	Default >> Dot1X	Default >> posture-compliant	PermitAccess	Compliant	
Aug 22, 2020 04:51:04.2...		DOMINION\adott1xposture	DC...	Microsoft-Workstation	Default >> Dot1X	Default >> posture-compliant	PermitAccess	Compliant	
Aug 22, 2020 04:51:03.9...		CoA Event	DC...					Compliant	
Aug 22, 2020 04:45:20.1...		DOMINION\adott1xposture	DC...	VMWare-Device	Default >> Dot1X	Default >> posture-agentless	Posture-Agentless-authz	NotApplicable	

Agentless: Common issues #2

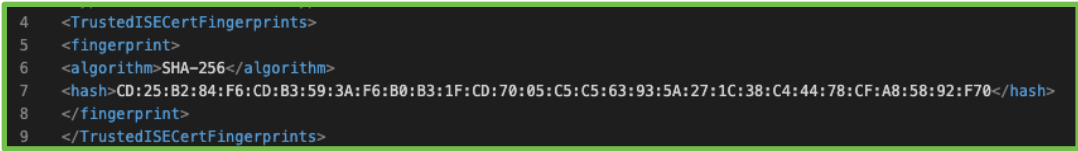
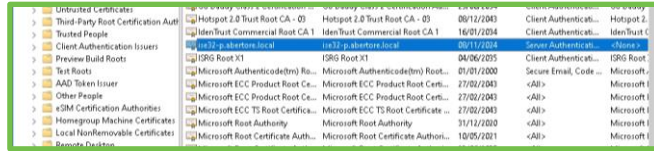
3455	2020-10-01 11:31:05.875513	10.127.197.83	10.106.39.38	TCP	74	51515	51515 → 5985 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=14295005
3456	2020-10-01 11:31:05.876031	10.106.39.38	10.127.197.83	TCP	66	5985	5985 → 51515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
				TCP	54	51515	51515 → 5985 [ACK] Seq=1 Ack=1 Win=29312 Len=0
				HTTP	327	51515	POST /wsman?PSVersion=7.0.0 HTTP/1.1 , NTLMSSP_NEGOTIATE
				HTTP	580	5985	HTTP/1.1 401 , NTLMSSP_CHALLENGE
				TCP	54	51515	51515 → 5985 [ACK] Seq=274 Ack=527 Win=30336 Len=0
				HTTP	812	51515	POST /wsman/ HTTP/1.1 , NTLMSSP_AUTH, User: \admin
				HTTP	234	5985	HTTP/1.1 401
3468	2020-10-01 11:31:05.973206	10.127.197.83	10.106.39.38	TCP	54	51515	51515 → 5985 [FIN, ACK] Seq=1032 Ack=708 Win=31360 Len=0

HTTP 401

Refresh	Reset Repeat Counts	Export To								Filter	
Time	Status	Identity	Endpoint ID	Endpoint Profile	Authentication Pol...	Authorization Policy	Authorization Profiles	Posture Status	IP Address		
		Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status	IP Address		
Aug 22, 2020 04:51:04.2...		DOMINION\addot1xposture	DC:...	Microsoft-Workstation	Default >> Dot1X	Default >> posture-compliant	PermitAccess	Compliant	DC:...		
Aug 22, 2020 04:51:04.2...		DOMINION\addot1xposture	DC:...	Microsoft-Workstation	Default >> Dot1X	Default >> posture-compliant	PermitAccess	Compliant	DC:...		
Aug 22, 2020 04:51:03.9...		CoA Event	DC:...					Compliant	DC:...		
Aug 22, 2020 04:45:20.1...		DOMINION\addot1xposture	DC:...	VMWare-Device	Default >> Dot1X	Default >> posture-agentless	Posture-Agentless-authz	NotApplicable	DC:...		

Script Troubleshoot

1. Prerequisites check



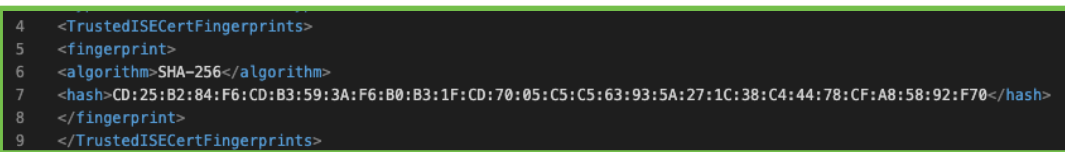
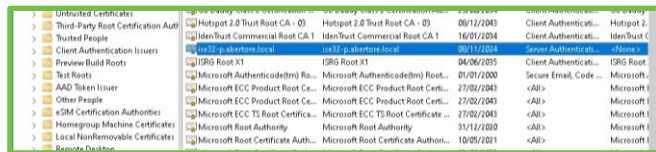


- Console Root
 - Certificates (Local Computer)
 - Personal
 - Trusted Root Certification Authorities
 - Certificates
 - Enterprise Trust
 - Intermediate Certification Authorities
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certification Authorities
 - Trusted People
 - Client Authentication Issuers
 - Preview Build Roots
 - Test Roots
 - AAD Token Issuer
 - Other People
 - eSIM Certification Authorities
 - Homegroup Machine Certificates
 - Local NonRemovable Certificates
 - Remote Desktop
 - Certificate Enrolment Requests
 - Smart Card Trusted Roots
 - Trusted Packaged App Installation
 - Trusted Devices
 - Windows Live ID Token Issuer
 - WindowsServerUpdateServices

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
DigiCert High Assurance EV Root...	DigiCert High Assurance EV Root ...	10/11/2031	Client Authentication...	DigiCert
DST Root CA X3	DST Root CA X3	30/09/2021	Client Authentication...	DST Root C
Entrust Root Certification Auth...	Entrust Root Certification Authori...	07/12/2030	Client Authentication...	Entrust.net
GlobalSign	GlobalSign	18/03/2029	Client Authentication...	GlobalSign
GlobalSign	GlobalSign	15/12/2021	Client Authentication...	Google Tru
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Client Authentication...	GlobalSign
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	29/06/2034	Client Authentication...	Go Daddy
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	08/12/2043	Client Authentication...	Hotspot 2.
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	16/01/2034	Client Authentication...	IdenTrust C
ise32-p.abertore.local	ise32-p.abertore.local	08/11/2024	Server Authentication...	<None>
ISRG Root X1	ISRG Root X1	04/06/2035	Client Authentication...	ISRG Root:
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	01/01/2000	Secure Email, Code ...	Microsoft,
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	27/02/2043	<All>	Microsoft I
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	27/02/2043	<All>	Microsoft I
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	27/02/2043	<All>	Microsoft I
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<All>	Microsoft I
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10/05/2021	<All>	Microsoft I
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23/06/2035	<All>	Microsoft I
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	22/03/2036	<All>	Microsoft I
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	22/10/2039	<All>	Microsoft
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	08/01/2004	Time Stamping	VeriSign Ti
QuoVadis Root CA 2	QuoVadis Root CA 2	24/11/2031	Client Authentication...	QuoVadis F
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	12/01/2042	Client Authentication...	QuoVadis F
SecureTrust CA	SecureTrust CA	31/12/2029	Client Authentication...	Trustwave
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	29/06/2034	Client Authentication...	Starfield C

Script Troubleshoot

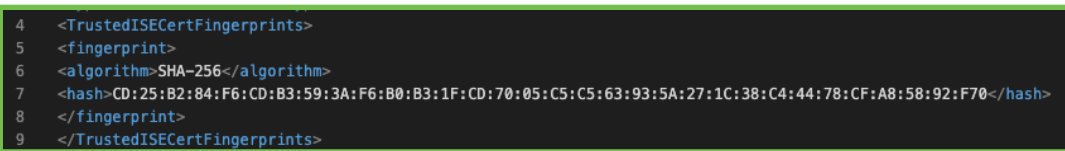
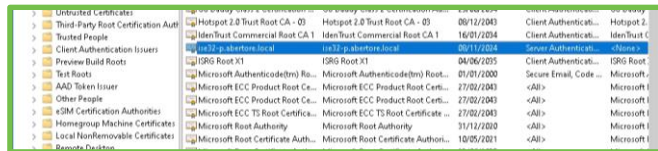
1. Prerequisites check



```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
3 <BypassDownloader>false</BypassDownloader>
4 <TrustedISECertFingerprints>
5 <fingerprint>
6 <algorithm>SHA-256</algorithm>
7 <hash>CD:25:B2:84:F6:CD:B3:59:3A:F6:B0:B3:1F:CD:70:05:C5:C5:63:93:5A:27:1C:38:C4:44:78:CF:A8:58:92:F70</hash>
8 </fingerprint>
9 </TrustedISECertFingerprints>
10 <EnableCRLCheck>false</EnableCRLCheck>
11 <ExcludeFirefoxNSSCertStore>false</ExcludeFirefoxNSSCertStore>
12 <ExcludeMacNativeCertStore>false</ExcludeMacNativeCertStore>
13 <ExcludePemFileCertStore>false</ExcludePemFileCertStore>
14 <ExcludeWinNativeCertStore>false</ExcludeWinNativeCertStore>
15 <FipsMode>false</FipsMode>
16 <RestrictHelpWebDeploy>false</RestrictHelpWebDeploy>
17 <RestrictLocalizationWebDeploy>false</RestrictLocalizationWebDeploy>
18 <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
19 <RestrictResourceWebDeploy>false</RestrictResourceWebDeploy>
20 <RestrictScriptWebDeploy>false</RestrictScriptWebDeploy>
21 <RestrictServerCertStore>false</RestrictServerCertStore>
22 <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
23 <RestrictWebLaunch>false</RestrictWebLaunch>
24 <StrictCertificateTrust>false</StrictCertificateTrust>
25 <UpdatePolicy>
26 <AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
27 <AllowHelpUpdatesFromAnyServer>true</AllowHelpUpdatesFromAnyServer>
```

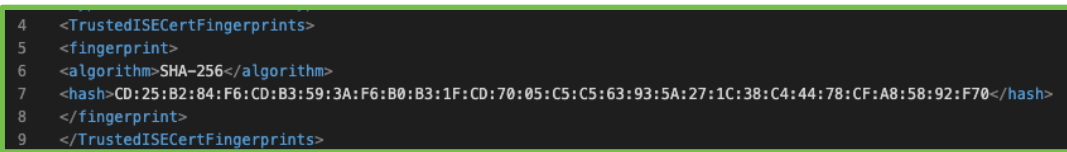
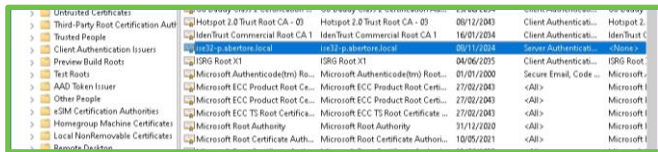
Script Troubleshoot

1. Prerequisites check



Script Troubleshoot

1. Prerequisites check



2. Check script failure report

Logged At	Server	Status	Policy Name	Requirement Name	Session ID	EndPoints ID
Today	Server	Status	Policy Name	Requirement Name	Session ID	EndPoints ID
2022-12-23 11:26:12.582	ise32-p	Condition Script was executed, and the script exited wit...	AMS_BRANCH_WIN	Any_Branch_Win	COA8FF6400000867B2D2D7E	00:50:56:88:8B...
2022-12-23 11:21:07.288	ise32-p	Condition Script was executed, and the script exited with failure code 1.	H_WIN	Any_Branch_Win	COA8FF6400000867B2D2D7E	00:50:56:88:8B...

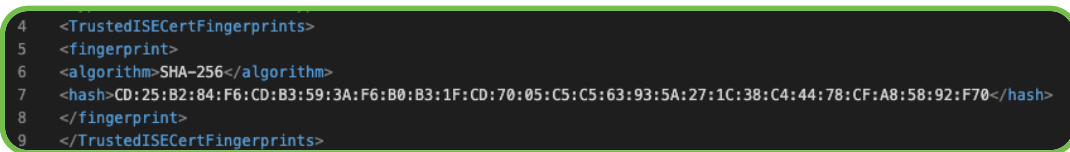
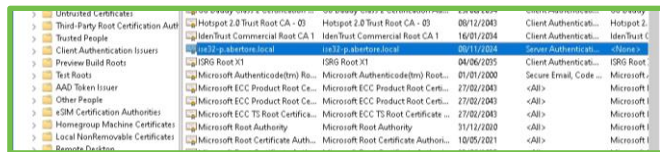
Script Troubleshoot

Logged At		Server	Status	Policy Name	Req
×	Today ▾ ×	Server	Status	Policy Name	Req
2022-12-23 11:26:12.582		ise32-p	Condition Script was executed, and the script exited wit...	AMS_BRANCH_WIN	Any_I
2022-12-23 11:21:07.288		ise32-p	Condition Script was executed, and the script exited with failure code 1.	H_WIN	Any_I

Condition Script was executed, and the script exited with failure code 1

Script Troubleshoot

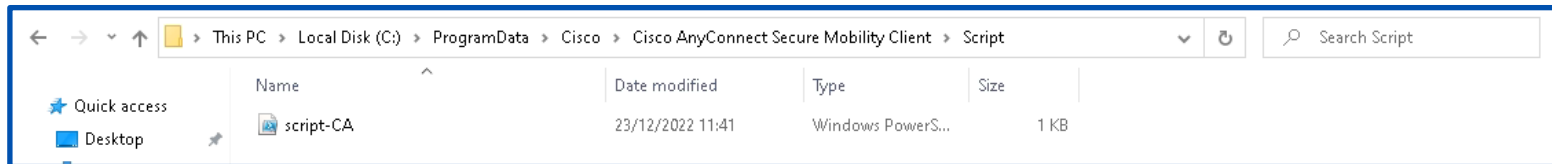
1. Prerequisites check

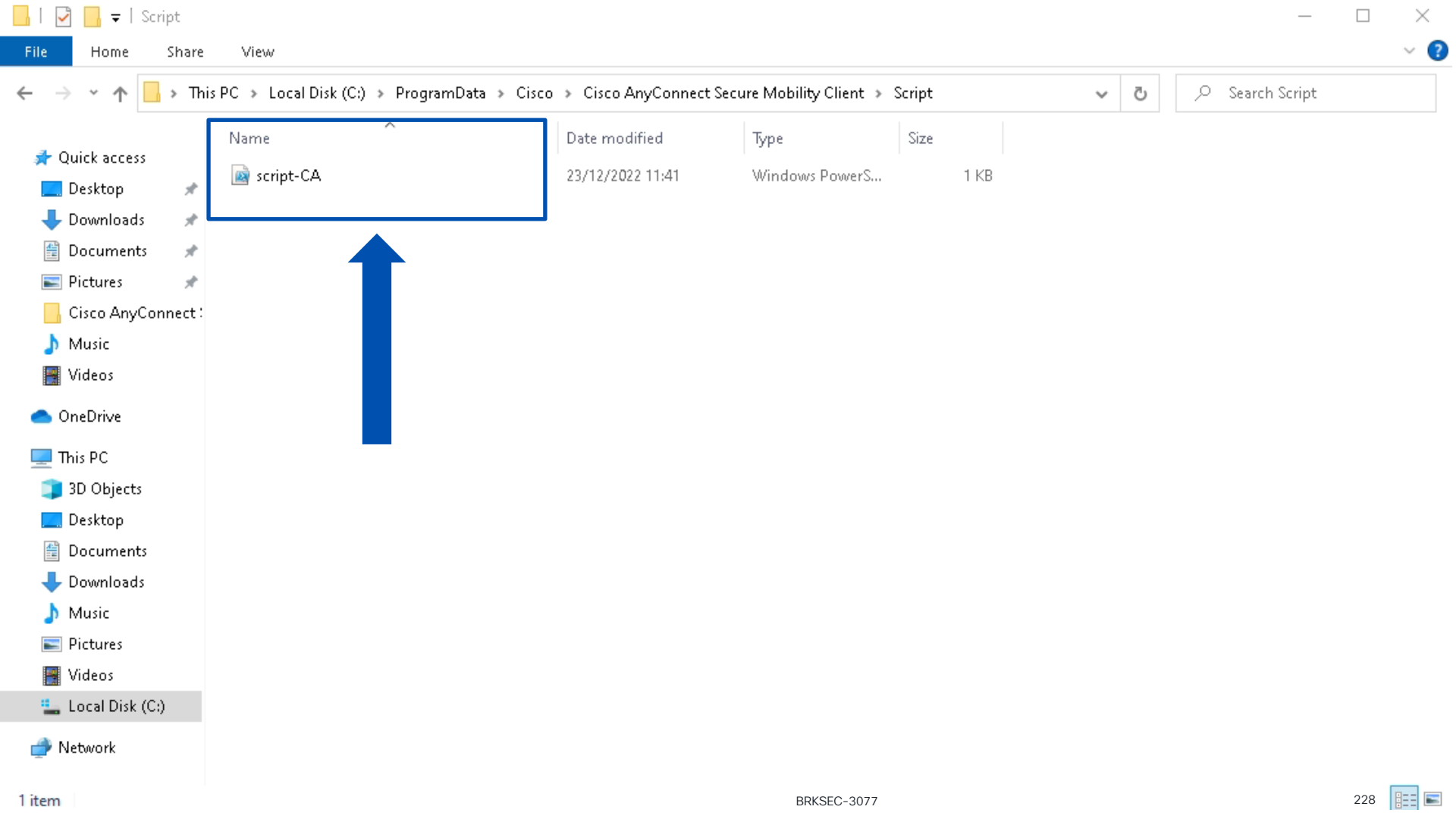


2. Check script failure report

Logged At		Server	Status	Policy Name	Requirement Name	Session ID	🕒 EndPoints ID	
✕	Today	✕	Server	Status	Policy Name	Requirement Name	Session ID	EndPoints ID
2022-12-23 11:26:12.582		ise32-p	Condition Script was executed, and the script exited wit...	AMS_BRANCH_WIN	Any_Branch_Win	C0A8FF6400000867B2D2D7E	00:50:56:88:8B:7	
2022-12-23 11:21:07.288		ise32-p	Condition Script was executed, and the script exited with failure code 1.	H_WIN	Any_Branch_Win	C0A8FF6400000867B2D2D7E	00:50:56:88:8B:7	

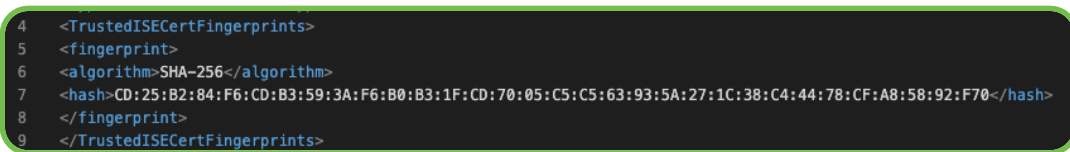
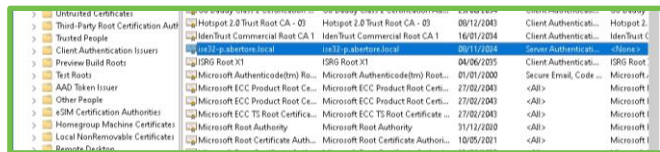
3. Check if the script is downloaded correctly





Script Troubleshoot

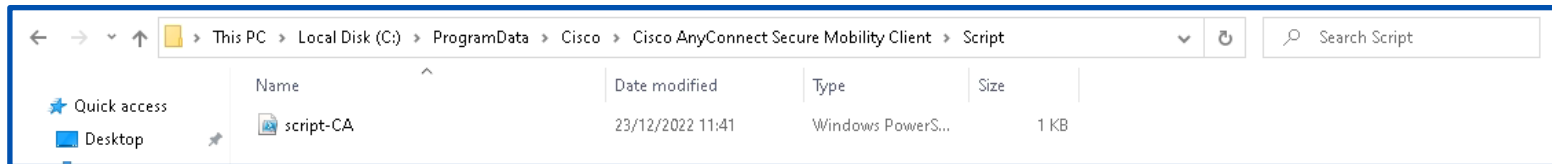
1. Prerequisites check



2. Check script failure report

Logged At		Server	Status	Policy Name	Requirement Name	Session ID	🕒 EndPoints ID	
✕	Today	✕	Server	Status	Policy Name	Requirement Name	Session ID	EndPoints ID
2022-12-23 11:26:12.582		ise32-p	Condition Script was executed, and the script exited wit...	AMS_BRANCH_WIN	Any_Branch_Win	C0A8FF6400000867B2D2D7E	00:50:56:88:8B:7F	
2022-12-23 11:21:07.288		ise32-p	Condition Script was executed, and the script exited with failure code 1.	H_WIN	Any_Branch_Win	C0A8FF6400000867B2D2D7E	00:50:56:88:8B:7F	

3. Check if the script is downloaded correctly



Script Troubleshoot

4. Manually run the script on the endpoint

```
PS C:\Users\bob\Desktop> powershell .\script.ps1
.\script.ps1 : File C:\Users\bob\Desktop\script.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_Policies. https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\script.ps1
+ ~~~~~
+ CategoryInfo          : (Error: (Scripting: CannotLoad)) (Scripting: CannotLoad) (FullQualifiedErrorId: UnauthorizedAccess)
+ FullyQualifiedErrorId : UnauthorizedAccess
```

Running script is disabled on this system

```
PS C:\Users\bob\Desktop> powershell .\script.ps1
.\script.ps1 : File C:\Users\bob\Desktop\script.ps1 cannot be loaded because running scripts is
disabled on this
system. For more information, see about_Execution_Policies at https://go.microsoft.com/fwlink/?
LinkID=135170.
At line:1 char:1
+ .\script.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
```

Running script is disabled on
this system

Windows PowerShell execution policy:

☒ Bypass ⓘ ☐ AllSigned ⓘ ☐ None ⓘ

```
PS C:\Users\bob\Desktop> powershell -ExecutionPolicy Bypass -File .\script.ps1
Check passed: File existPS C:\Users\bob\Desktop> powershell -ExecutionPolicy Bypass -File .\script.ps1
Check passed: File exist
```



Script Troubleshoot

4. Manually run the script on the endpoint

```
PS C:\Users\bob\Desktop> powershell .\script.ps1
.\script.ps1 : File C:\Users\bob\Desktop\script.ps1 cannot be loaded because running scripts is
disabled on this
system. For more
LinkID=135170.
At line:1 char:1
+ .\script.ps1
+ ~~~~~
+ CategoryInfo          : (Error) ( (FullY)
+ FullyQualifiedErrorId : UnauthorizedAccess
```

Running script is disabled on this system

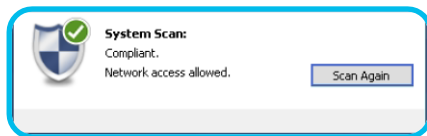
Windows PowerShell execution policy:

☒ Bypass ⓘ ☐ AllSigned ⓘ ☐ None ⓘ

```
PS C:\Users\bob\Desktop> powershell -ExecutionPolicy Bypass -File .\script.ps1
Check passed: File existPS C:\Users\bob\Desktop> powershell -ExecutionPolicy Bypass -File .\script.ps1
Check passed: File exist
```

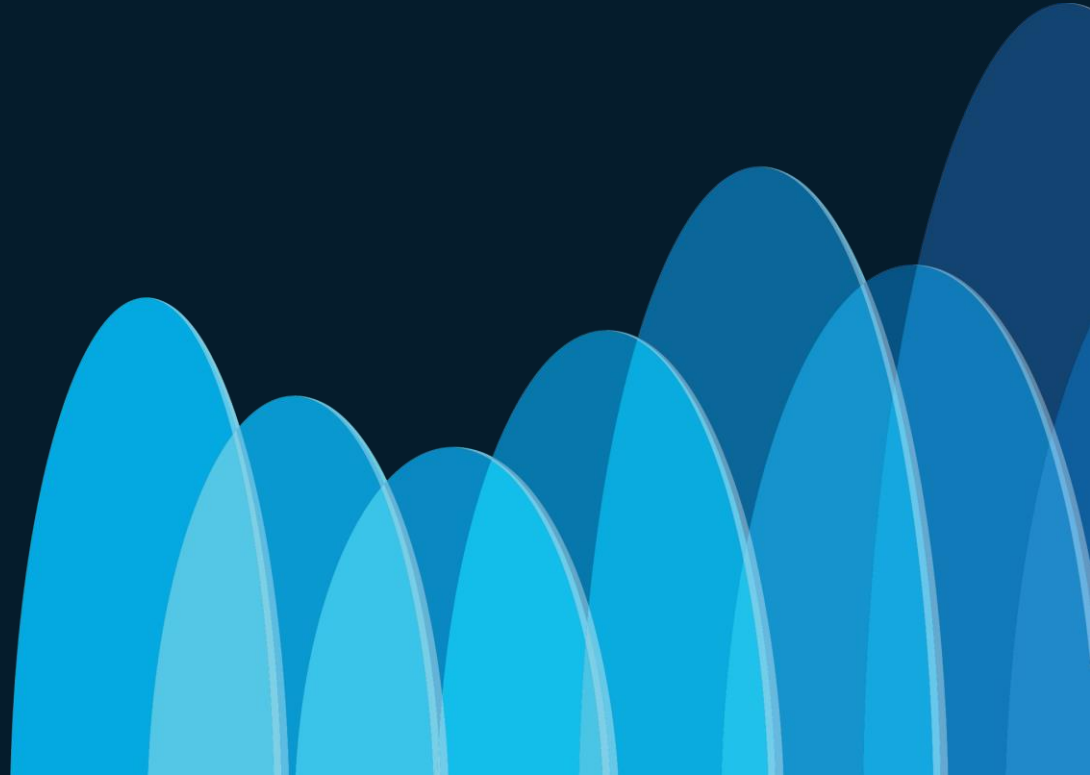
5. Make sure exit code is correct

6. Results



Logged At	Server	Status	Policy Name	Requirement Name
< Today > x	Server	Status	Policy Name	Requirement Name
2022-12-23 11:42:32.415	ise32-p	Condition Script execution was successful.	AMS_BRANCH_WIN	Any_Branch_Win

Wrap up time



Key Takeaways Posture Deployment

Work on the different ISE Pillars

Advanced Scenarios are just bigger puzzles



Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.



Thank you

CISCO *Live!*



CISCO *Live!*

GO BEYOND

The background of the slide is white. On the right side, there is a series of overlapping, teardrop-shaped elements in various shades of blue, ranging from light to dark. These shapes are arranged in a way that they appear to be layered, creating a sense of depth and movement. The text 'GO BEYOND' is centered horizontally across the middle of the slide. The word 'GO' is in a large, dark blue, sans-serif font. The word 'BEYOND' is in a larger, bold, dark blue, sans-serif font. The overall design is clean and modern.