



The bridge to possible

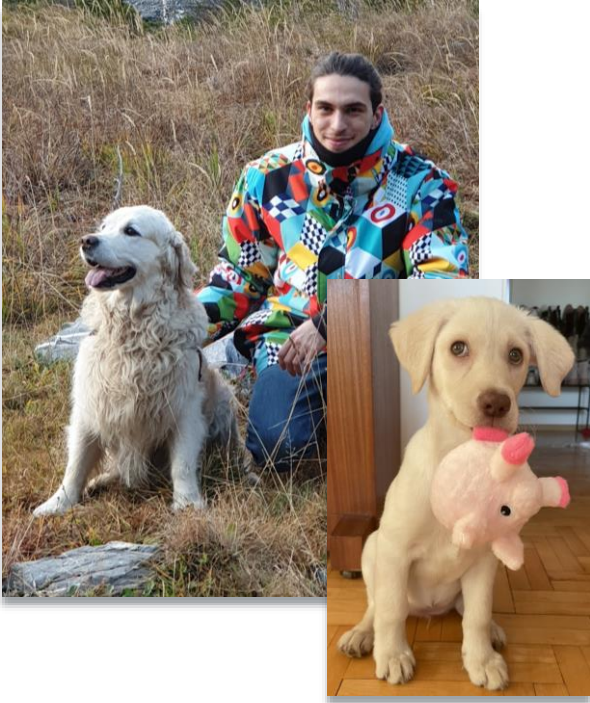
# The Art of ISE Posture, Configuration and Troubleshooting

Andrea Bertorello, Security Consulting Engineer  
[linkedin.com/in/andrea-bertorello/](https://www.linkedin.com/in/andrea-bertorello/)

# Abstract

Endpoint Security is a pillar of all the organisations and the trend is the increase for endpoint security and compliance of the endpoints connected the organization networks. ISE together with Cisco Secure Client and ISE posture module, is capable of verifying and remediating a vast suite of criteria before an endpoint is allowed to the network access. Now with the upcoming ISE 3.2 there will be multiple ISE posture possible flows and a new Posture Script Conditions. With this session you will be able to understand the different possible posture flows and extend the posture coverage to new endpoints earlier not covered, together with some real case scenarios and most common issues that can affect your implementation, but can be solved handily.

# About me



- AAA TAC Engineer
- ThousandEyes Support Engineer
- Security Consulting Engineer



Warning!  
Italian accent ahead



# Icon Used Throught the Presentation



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



New Feature – new features introduced in ISE 3.2



Waring – Extra attention during the configuration



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

# Cisco Webex App

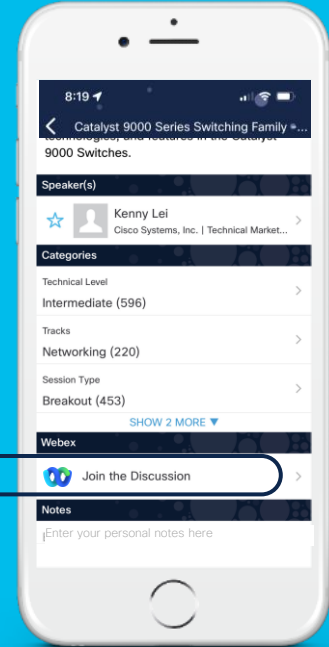
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live 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

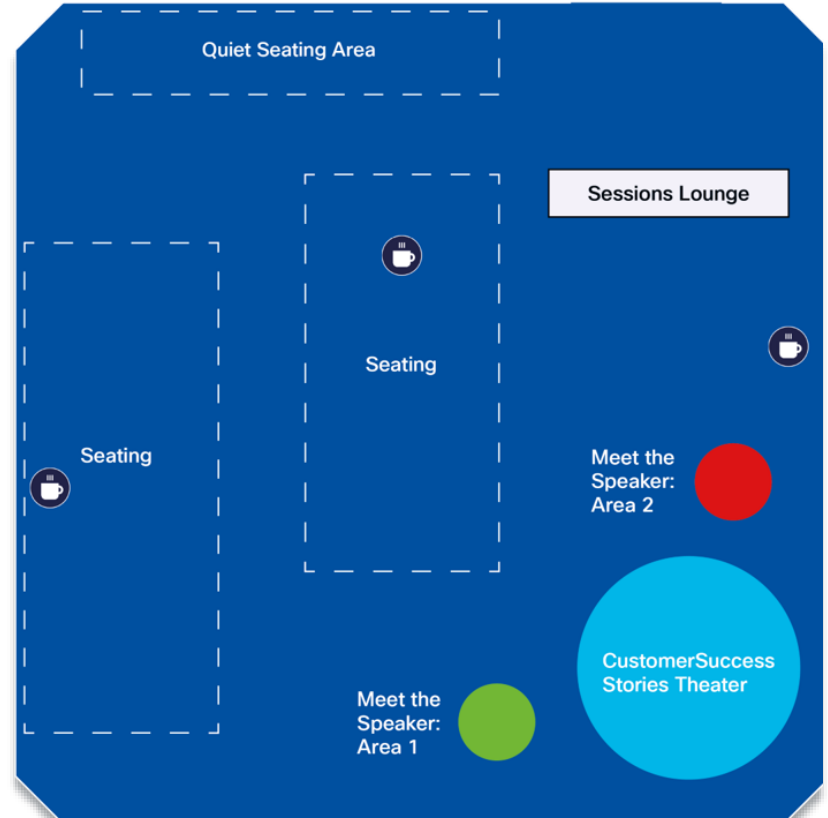
Webex spaces will be moderated until February 24, 2023.



# MTS – Meet the Speaker – Area 2

Let's continue the discussion/Q&A

Tuesday, Feb 7 12:20 -12:50 PM





# Agenda

- Introduction to DEMO company
- ISE Posture from 10000 meters
- ISE Posture Journey
- Implementation and Troubleshooting

# Session Objectives


Session will cover:

- Theory of Posture
- Posture configuration focused on agent deployment
- Troubleshoot methodology for some kind of agents

Session will not cover:

- Marketing
- Roadmaps
- All possible Posture feature and configuration





*Vigilance on what is on your network  
is just as important as who is on the  
network. Therefore, posture is so  
important.*

Based on a True  
Story



# Introduction to our scenario

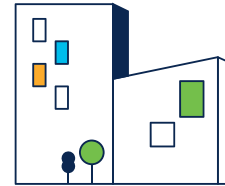
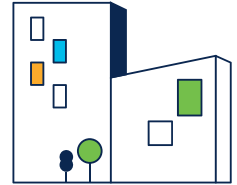
How to attain and maintain endpoint compliance as per the organization's security policy ?



Diana

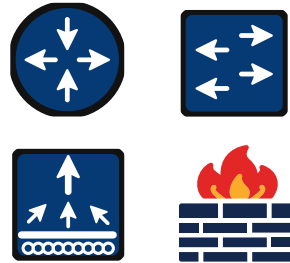


Amsterdam HQ



# ISE Posture – Theory

# ISE Posture from 10000 feet



Endpoints/Agents

Policy Enforcement

Foundation



Remediation Servers

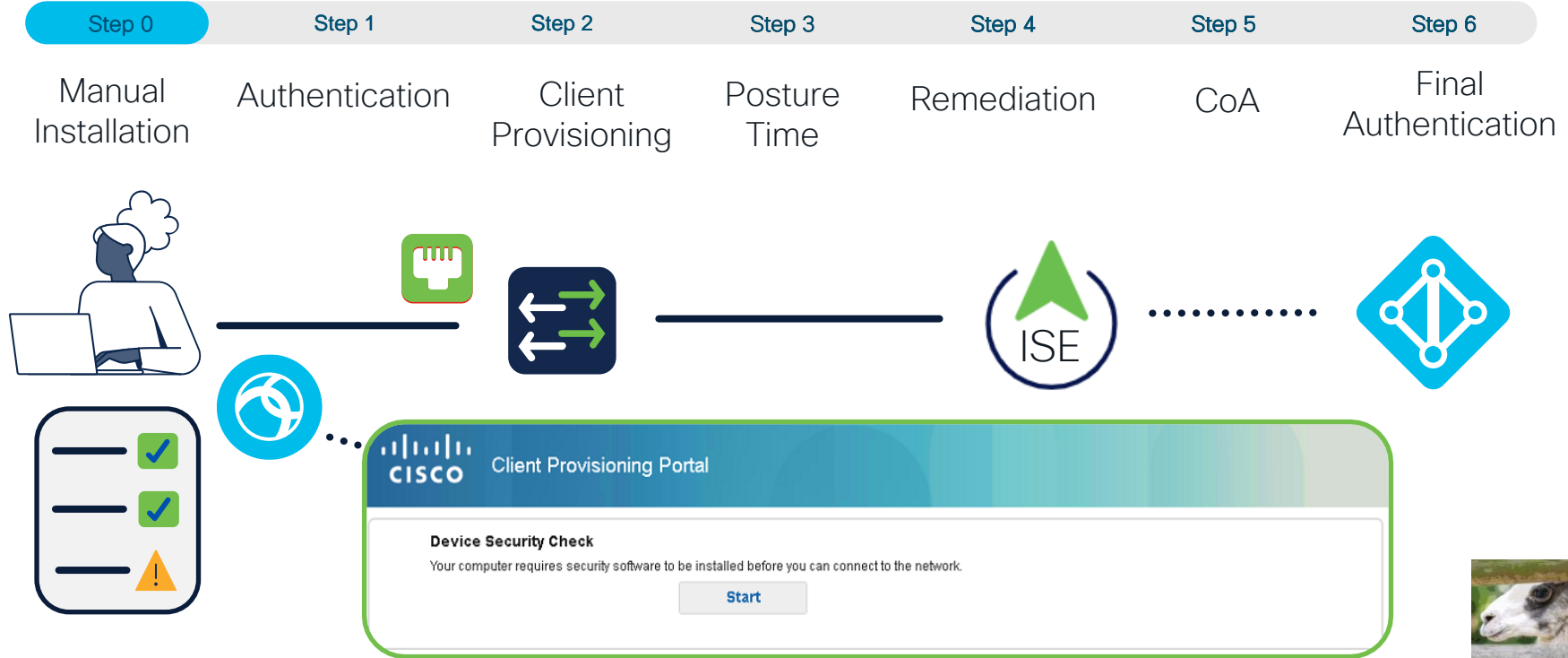


Admin

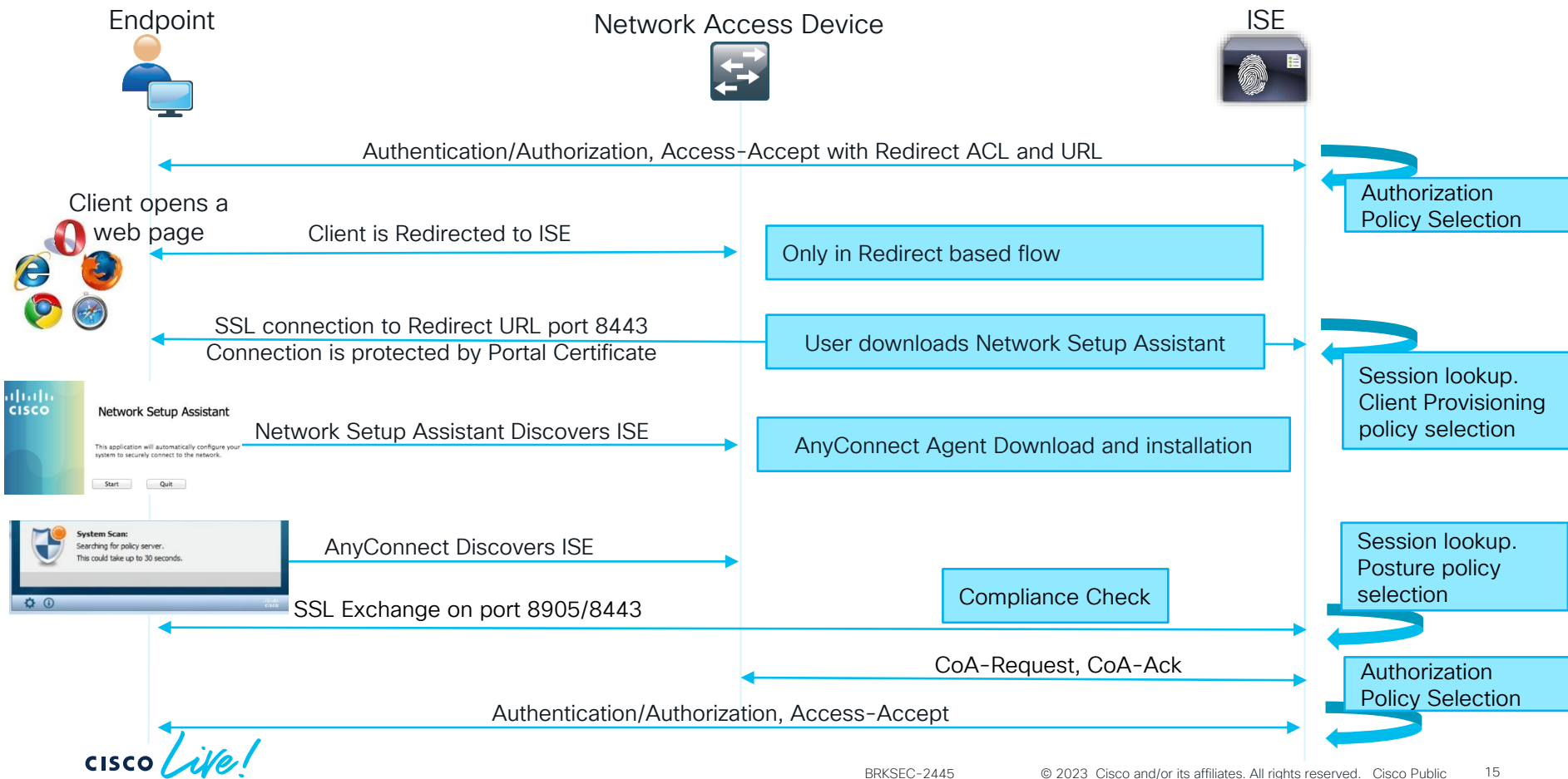


Posture Updates

# Posture Lifecycle



# Posture Lifecycle - Detailed



# Posture and Cisco COA types

Two main CoA types:

- **COA Reauth** – this type of COA is used for Wired and Wireless NADs, as a result of successful COA NAD will initiate full authentication process.
- **COA Push** – this type of COA are used by ASA for posture over VPN use-case. At time of posture over VPN re-authentication is impossible as it will cause disconnect for end user. Because of this COA Push contain new authorization attributes. This allows NAD to apply new access-level straight away without user disconnect.

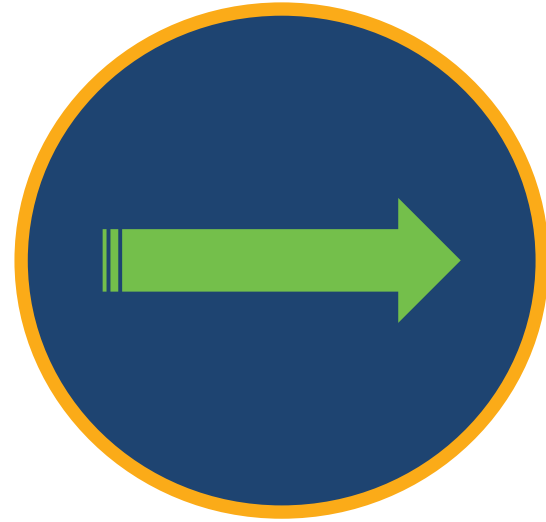


# ISE Posture Flow types

Redirect based



Non-redirect based



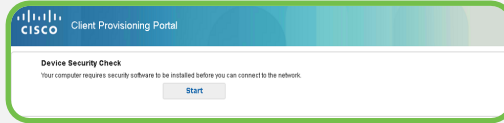
# ISE Posture Flow types - comparison

## 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

# 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

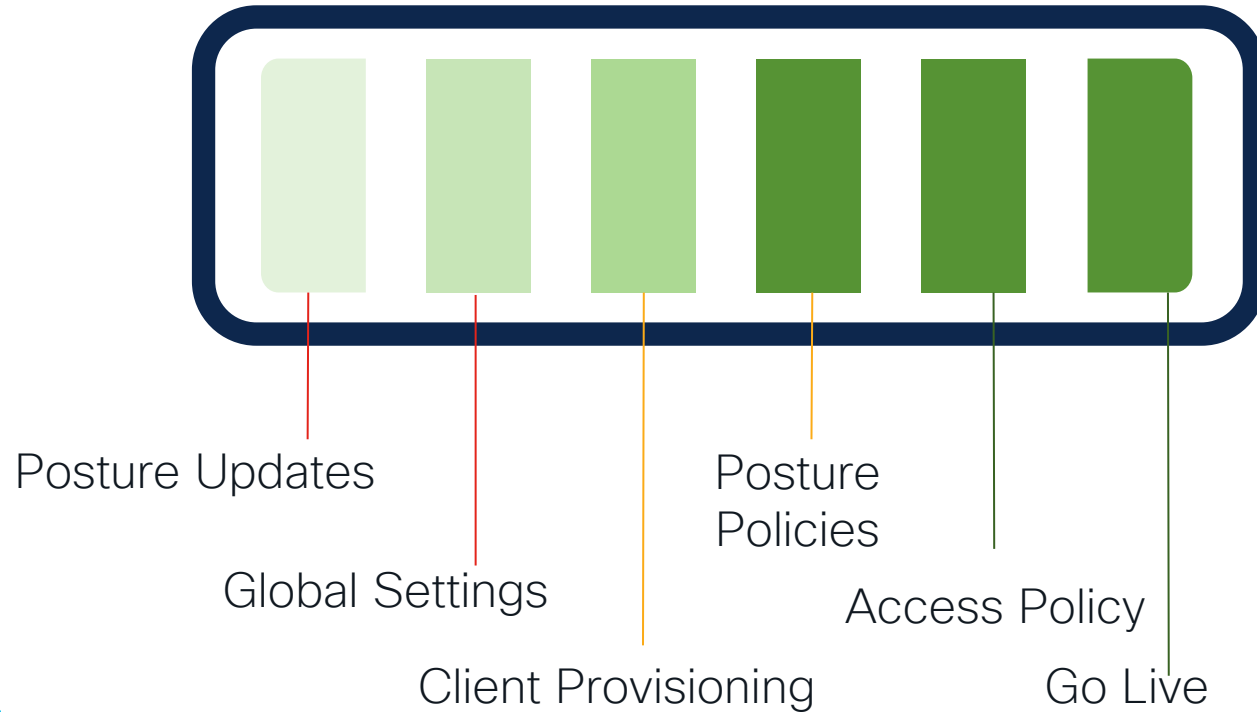
# Redirect best practices Wireless

- **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

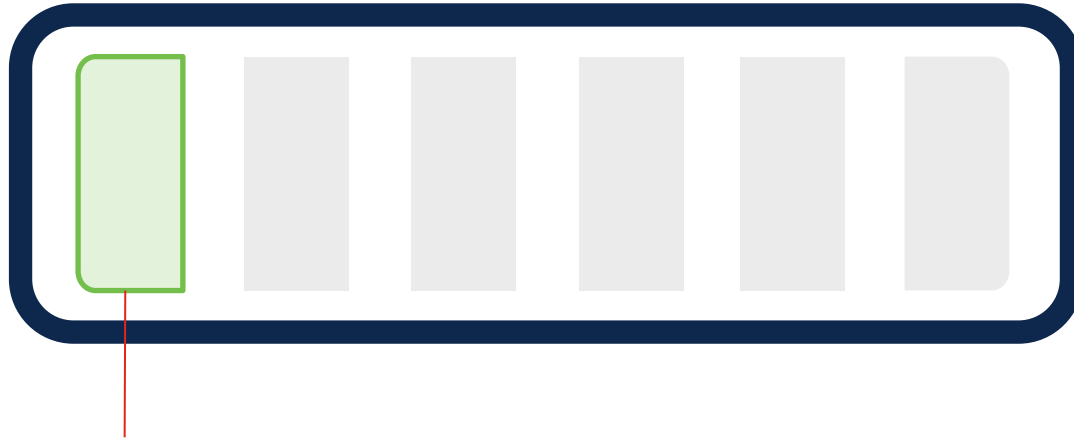
# ISE Posture Journey



# ISE Posture Journey

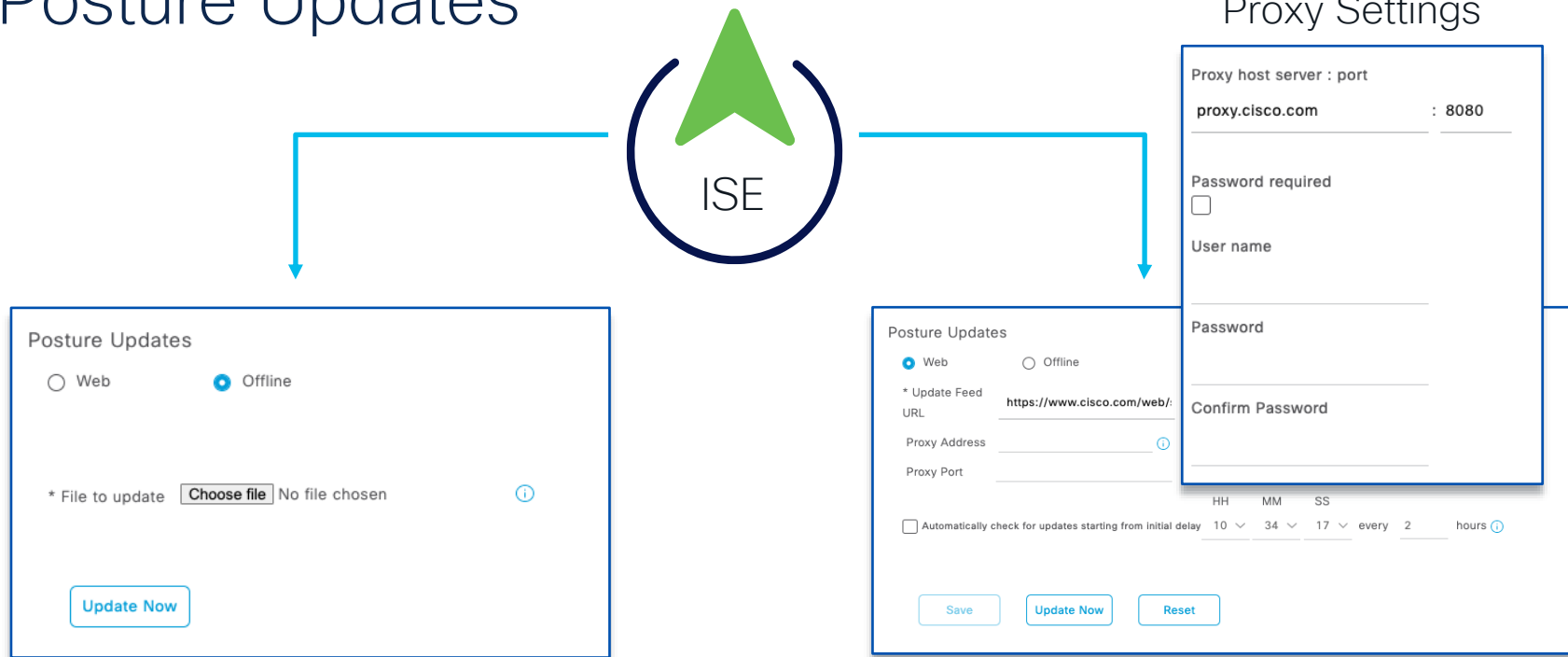


# ISE Posture Journey: Posture Updates



Posture Updates

# Posture Updates



Deleted default posture elements are not created again during next updates

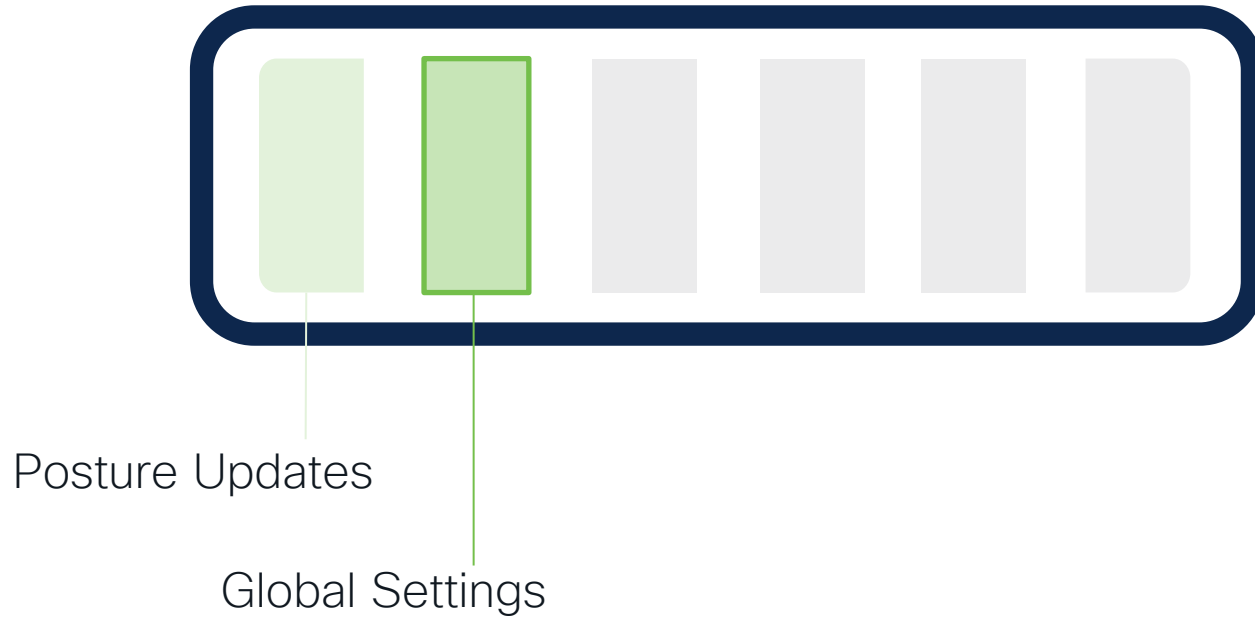


# Posture Updates

**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.

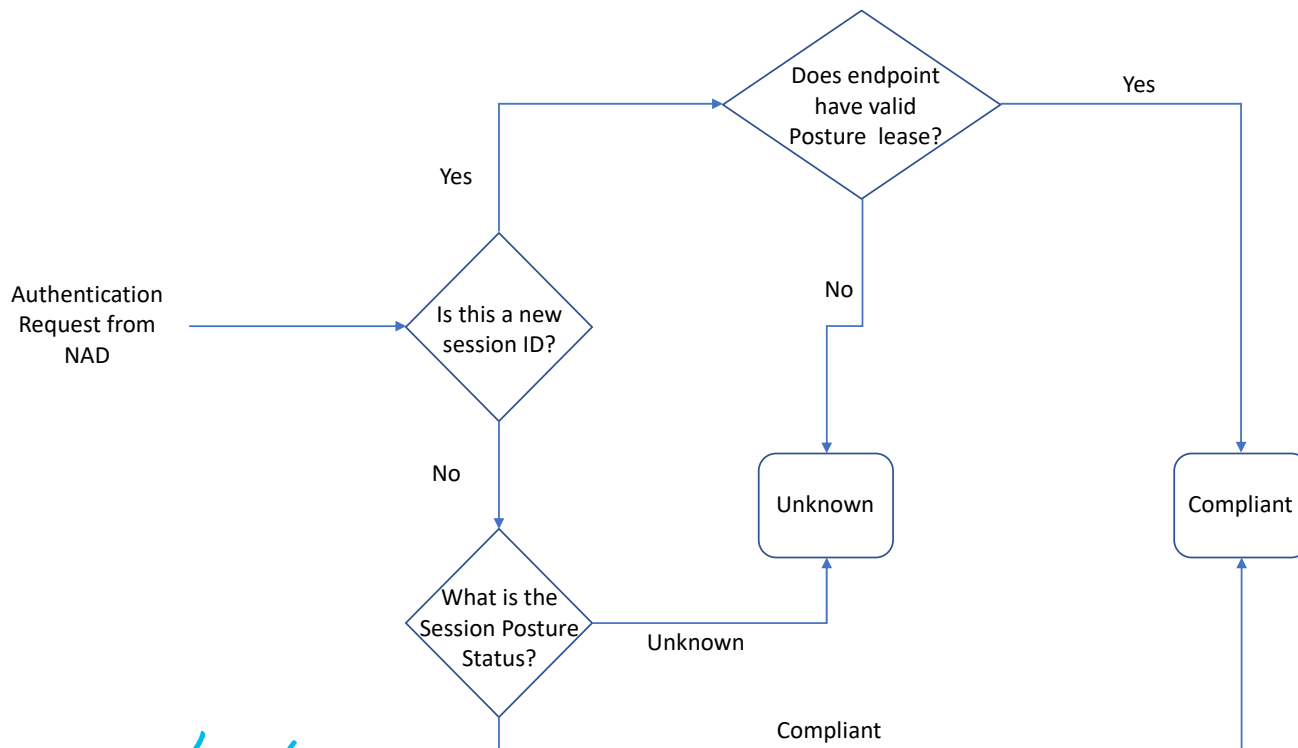
When endpoint is in Posture lease ISE assigns authorization policy with 'Compliant' status right-away

AnyConnect 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.

# Endpoint Session Attributes – Posture Status



Initial posture state of the session determined according to below diagram



Session moved from Unknown state to:

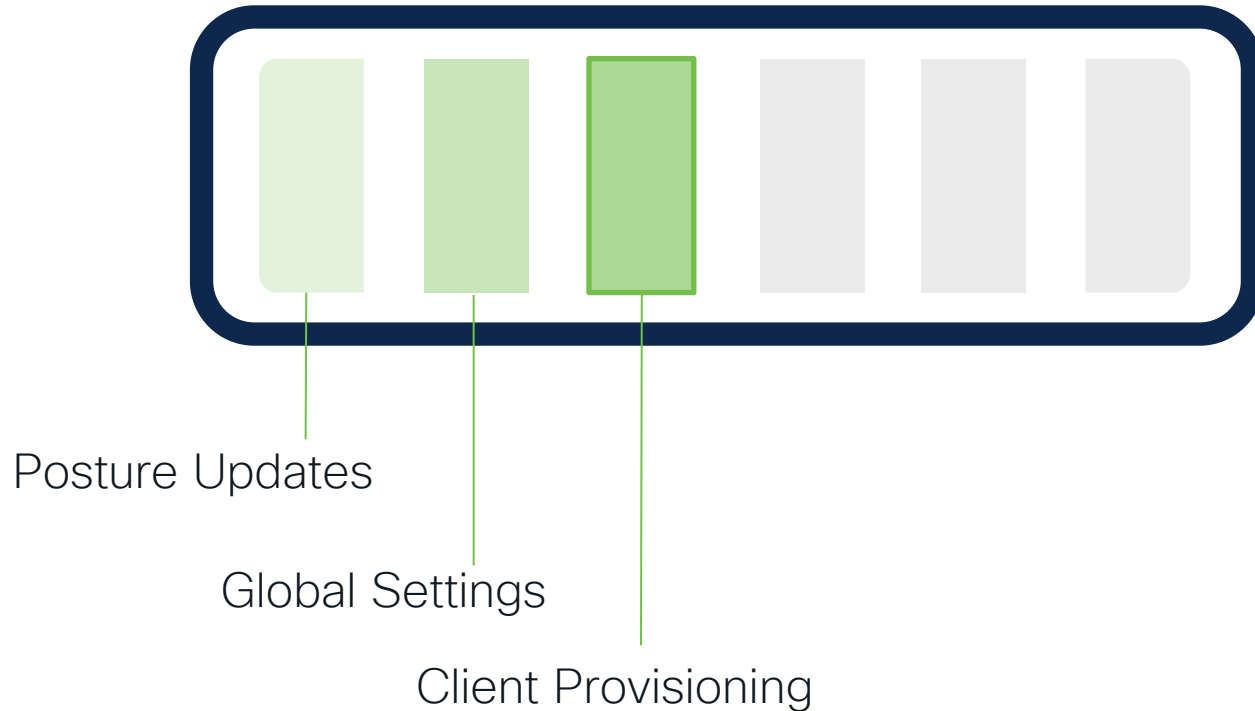
Compliant

OR

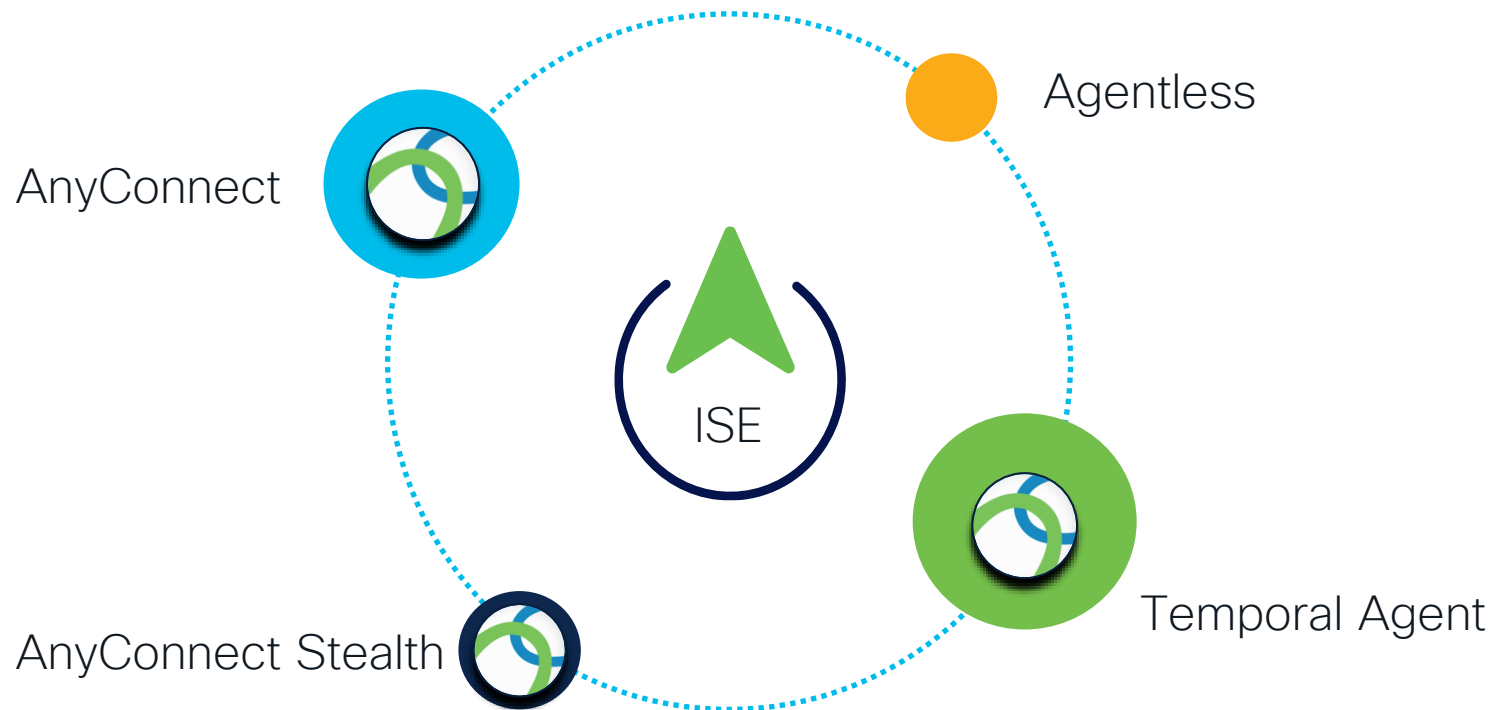
Non-Compliant

After PSN processes posture report from endpoint

# ISE Posture Journey: Client Provisioning

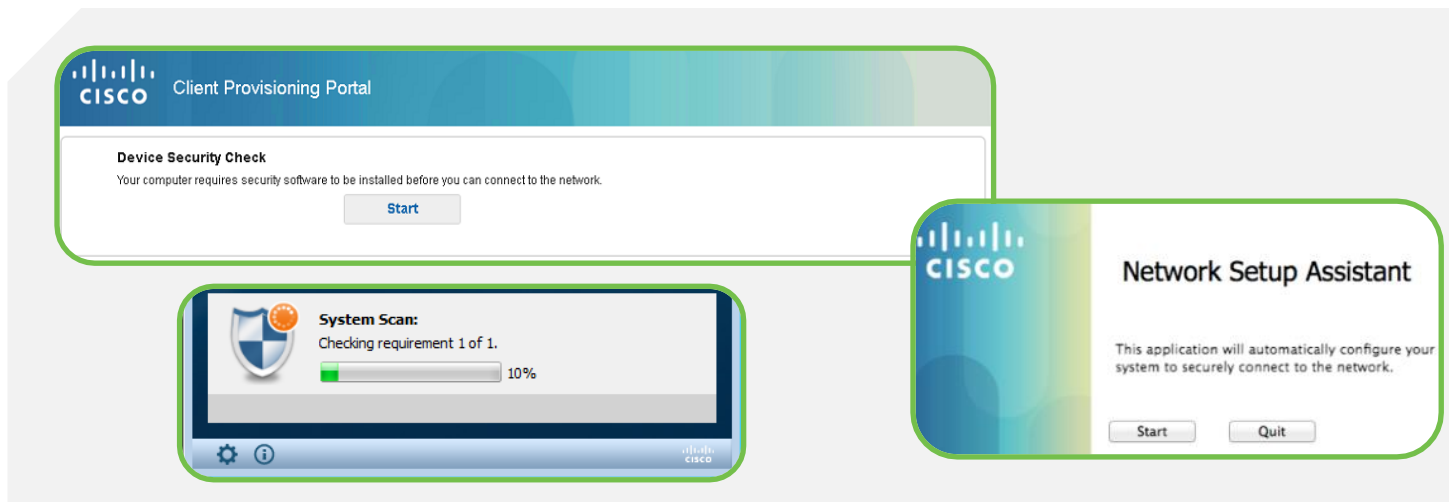
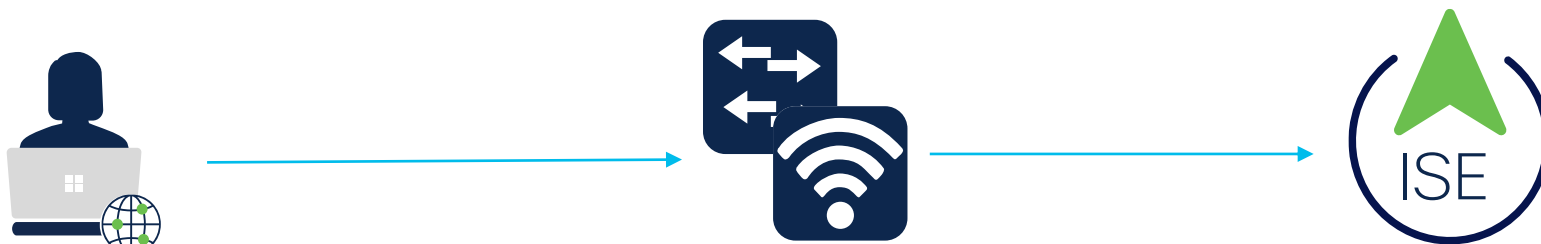


# ISE Posture: Agent types





# Posture Agents – Agent



# Posture Agents – Agent

Posture Lease

Periodic Reassessments (PRA)

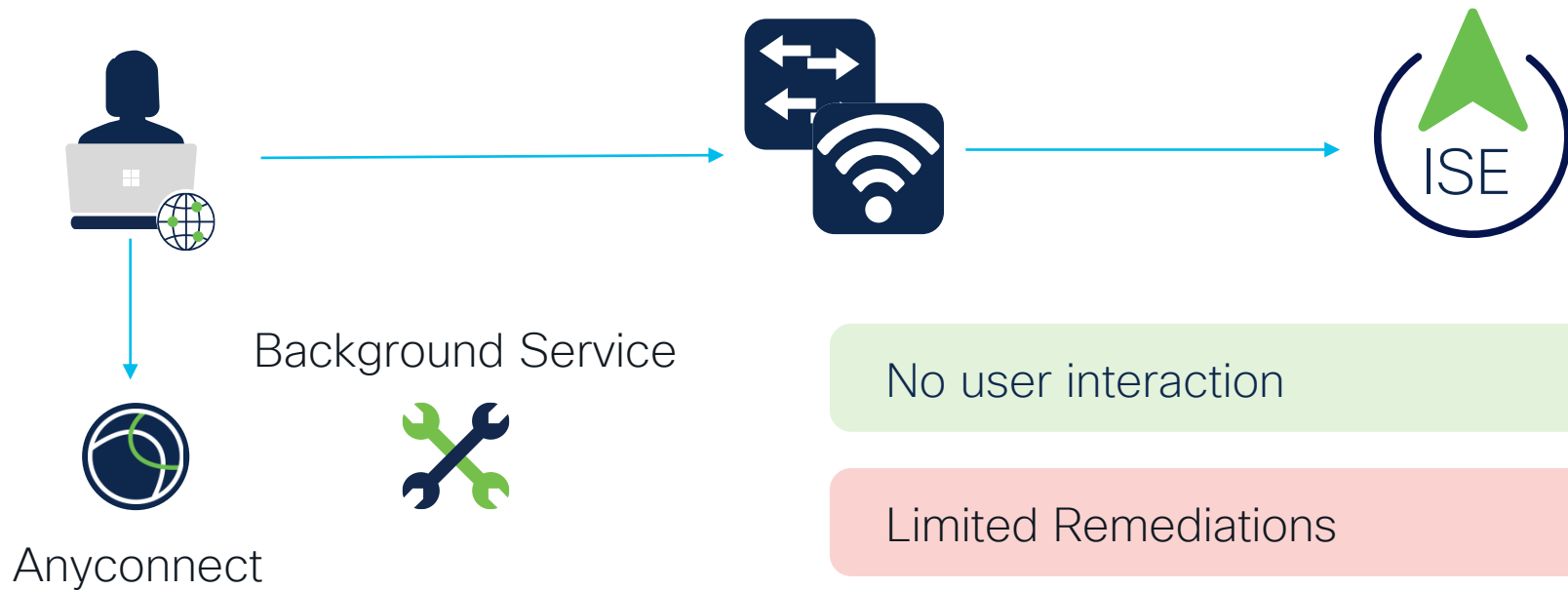
Grace Period

Manual Remediation

Conditions

Deployed by ISE or VPN head-end

# Posture Agents – Agent Stealth

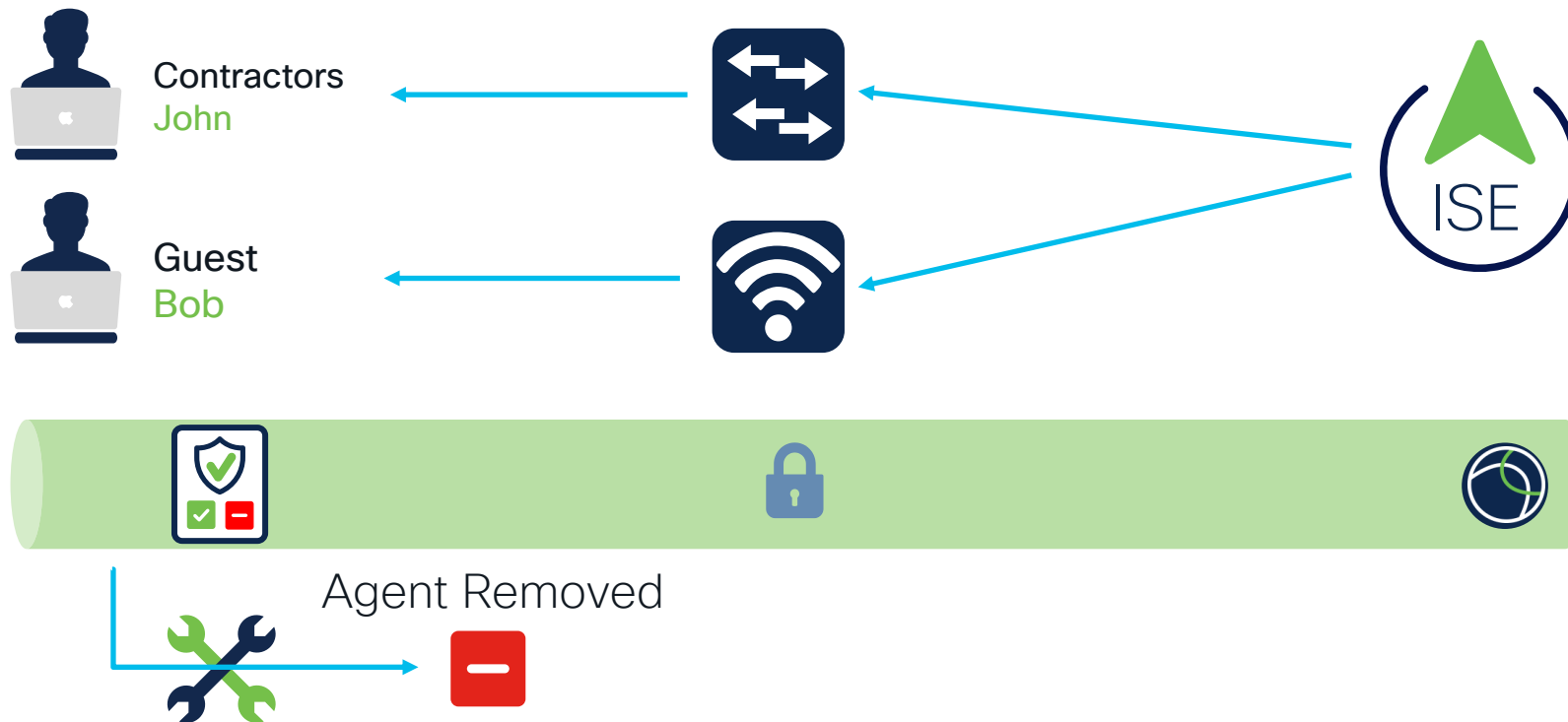


No user interaction

Limited Remediations

Deployed by ISE or VPN head-end

# Posture Agents – Temporal Agent



# Posture Agents – Temporal Agent

The Temporal Agent does not support the following conditions:

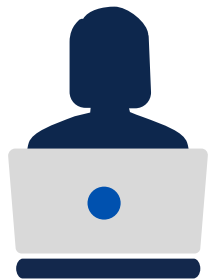
- Service Condition MAC–System Daemon check
- Service Condition–MAC–Daemon or User Agent check
- PM–Up To Date check
- PM–Enabled check
- DE–Encryption check

## VLAN Controlled Posture

Temporal Agent does not support VLAN-controlled posture for macOS.

Recognizing the new IP address requires root privileges, but the Temporal Agent runs as a user process.

# Agentless posture



Windows



macOS



PowerShell



5.1 &gt;

Shell (.sh)



SSH



Port 5985



Port 22

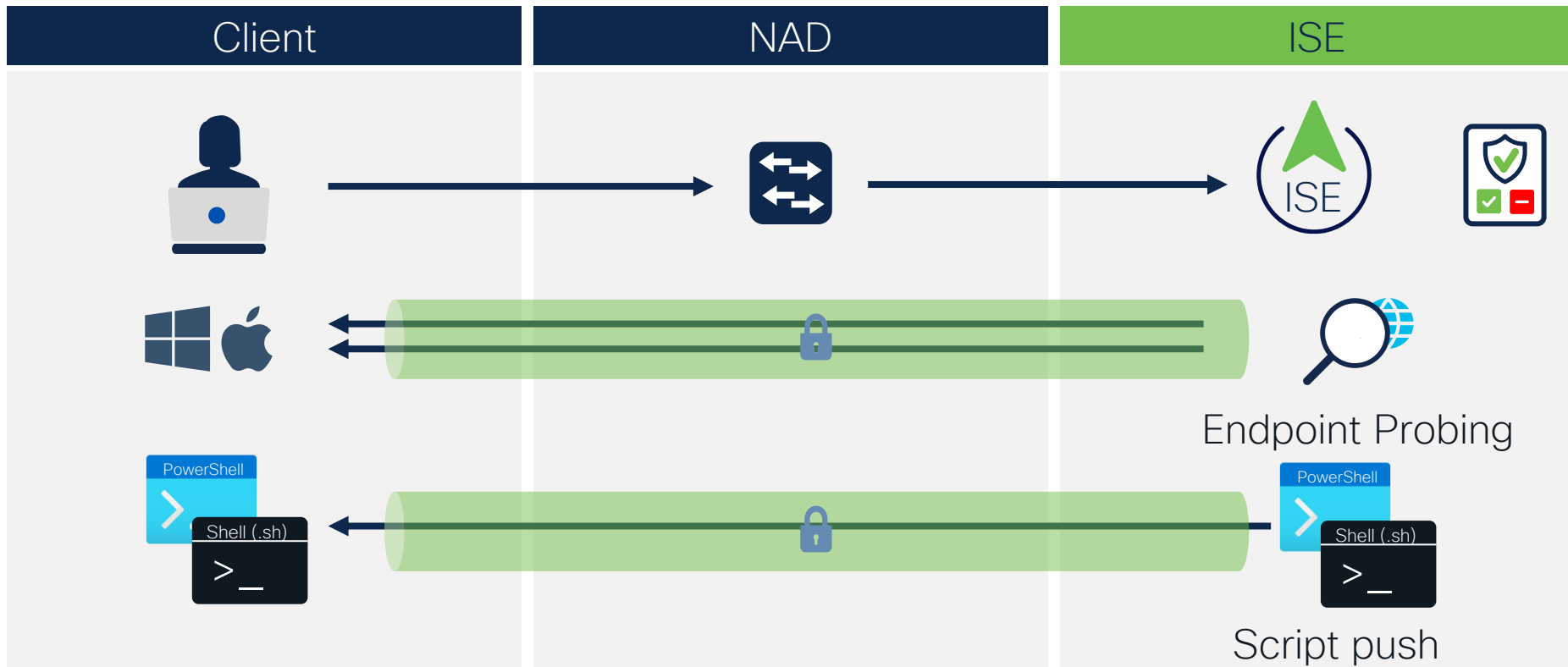
cURL

7.34 &gt;

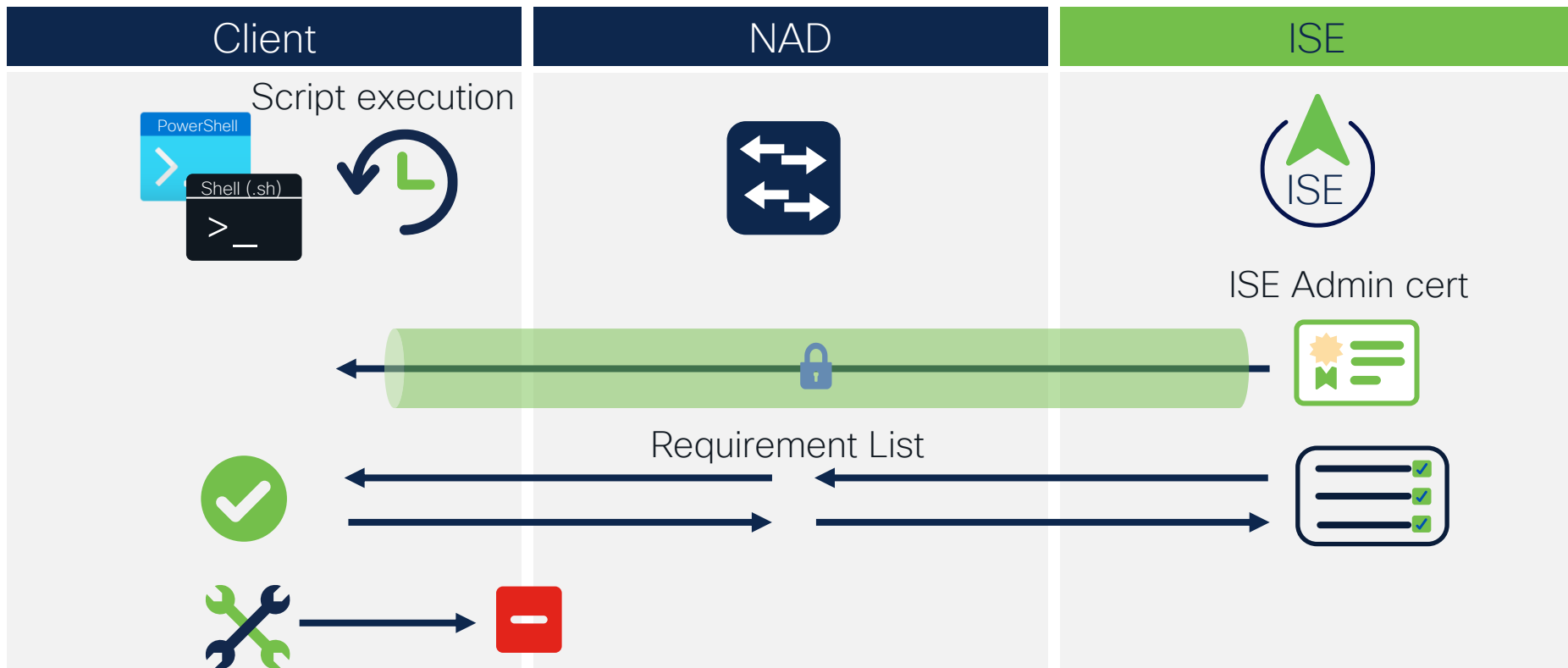
cURL

7.34 &gt;

# Posture Agentless



# Posture Agentless

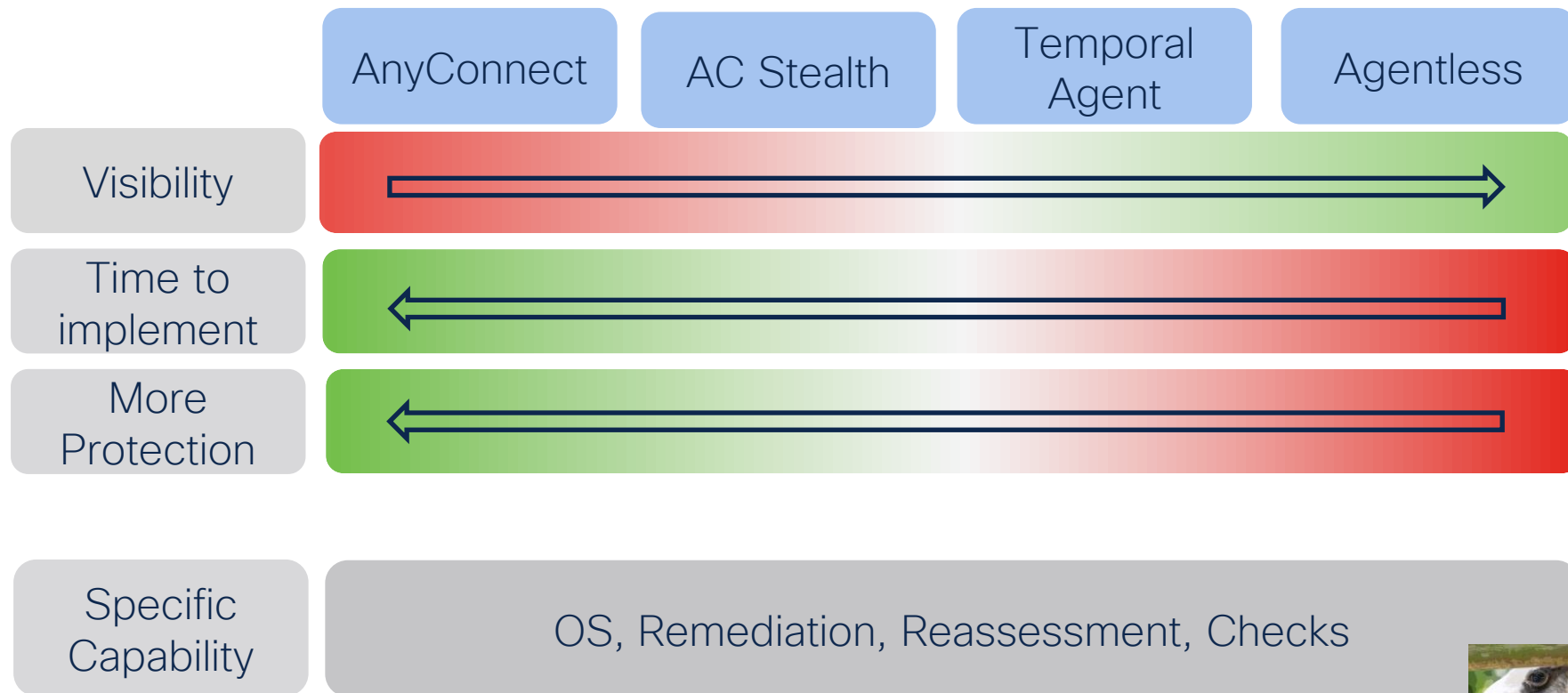




# Which Posture Agent to choose












# Which agent you need ?



# Posture Deployment Options

- ✓ Supported
- ! Limitations
- ✗ Not Supported

## Client Provisioning

Capability	AnyConnect			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	✓	✓	✓	✓	✓	✗	✗	✗	✗

# Client Provisioning

Resources

AnyConnect Profile

Client Provisioning Policy

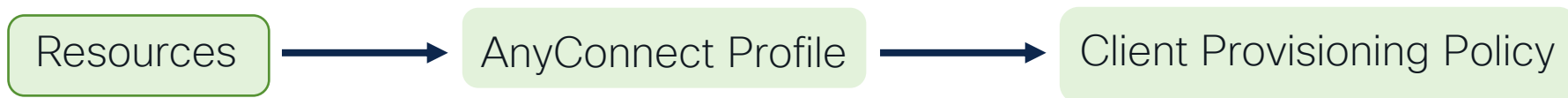
## Resources

[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



## How agent checks endpoint armor?

**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>

**Posture Updates** - Include predefined checks, rules, support charts and latest definition versions.

# Client Provisioning

Resources



AnyConnect 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 ☐
- Diagnostic and Reporting Tool ☒

## Profile Selection

\* ISE Posture

AC-Profile

## Posture Protocol

Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Server name rules *		Time (in seconds) to wait before retrying.
Discovery Backup Server List	Choose	Number of retries allowed for a message.
Server name rules *		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.
Enable agent IP refresh	Yes	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.
		A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "**.cisco.com"
		Policy service nodes that the agent will try to connect to if the primary service nodes don't respond for some reason.
		Targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Enable Rescan Button

Disabled



### System Scan:

No policy server detected.

Default network access is in effect.

Scan Again

# Client Provisioning

Resources



AnyConnect 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. ▾

\* Configuration Name:

Agent Configuration

Description:

Description Value Notes

\* Compliance Module

AnyConnectComplianceModuleWindow: ▾

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

☒

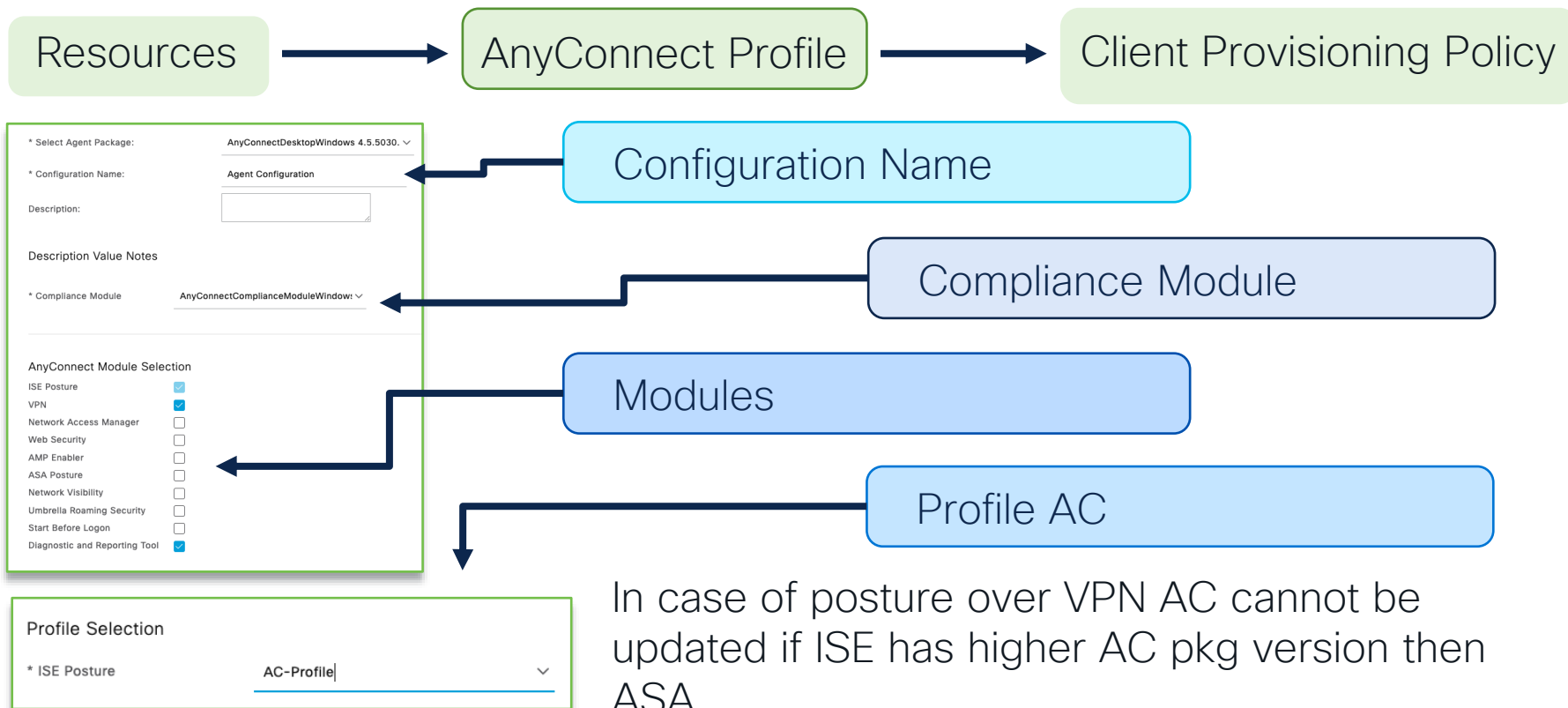
## Profile Selection

\* ISE Posture

AC-Profile ▾



# Client Provisioning



# Client Provisioning

Resources



AnyConnect 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)	then 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)	then CiscoTemporalAgentOSX 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  
AnyConnect  
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

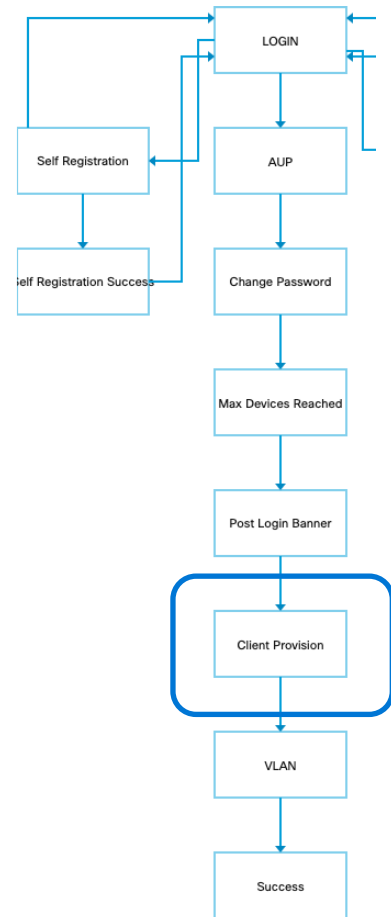
Navigate to **Work Centers > Guest Access > Portal & Components > Guest Portals**

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

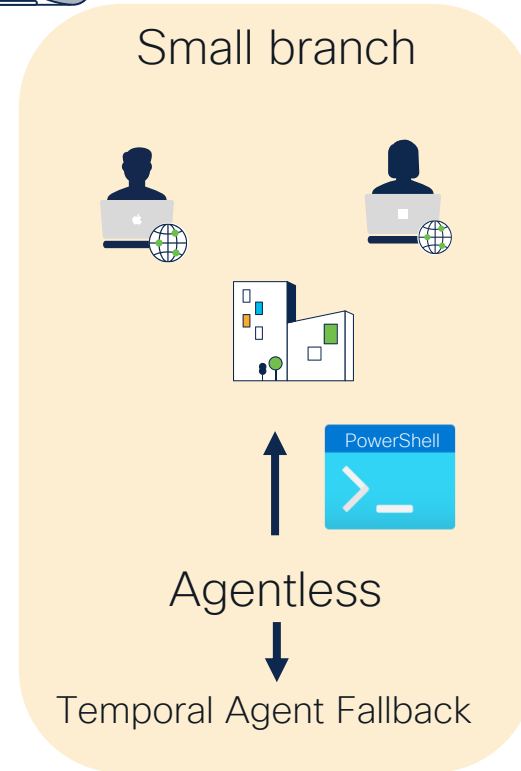
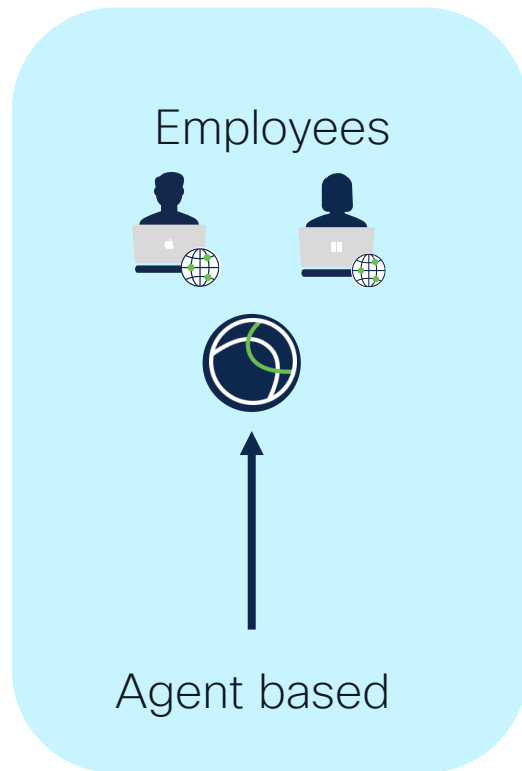
☒ Require guest device compliance

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

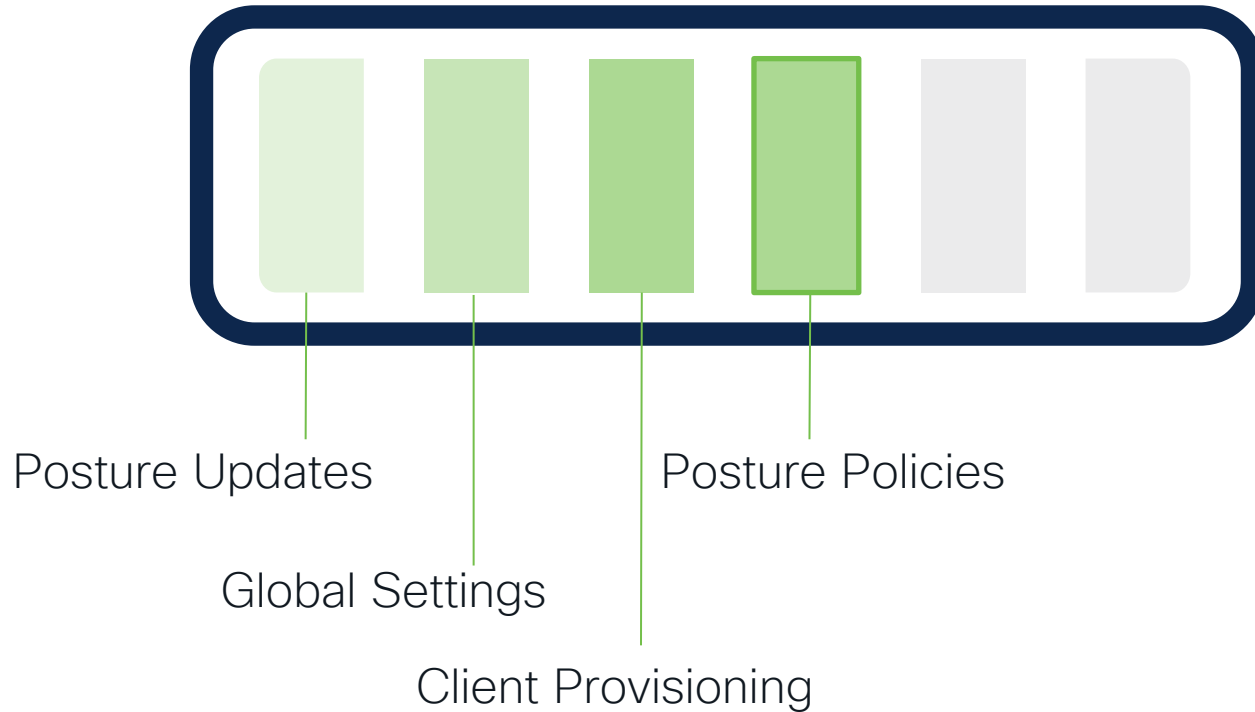




# Posture Agents – our choice



# ISE Posture Journey: Configuration



# ISE Posture Checks

Condition + Remediation → Requirement



# 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 <a href="#">Edit</a> ▾
<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 <a href="#">Edit</a> ▾

### 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\_Require



# 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.



# Posture Conditions – Our requirements

Employee



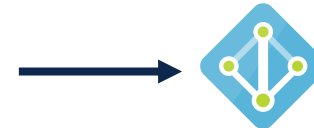
Anti-Malware



Contractors



External Data Source



Small branch



Win10 latest patch  
Firewall Enabled



# The last minute request



“Does the endpoint has necessary corporate CA certs installed ?”



# Posture Script Condition

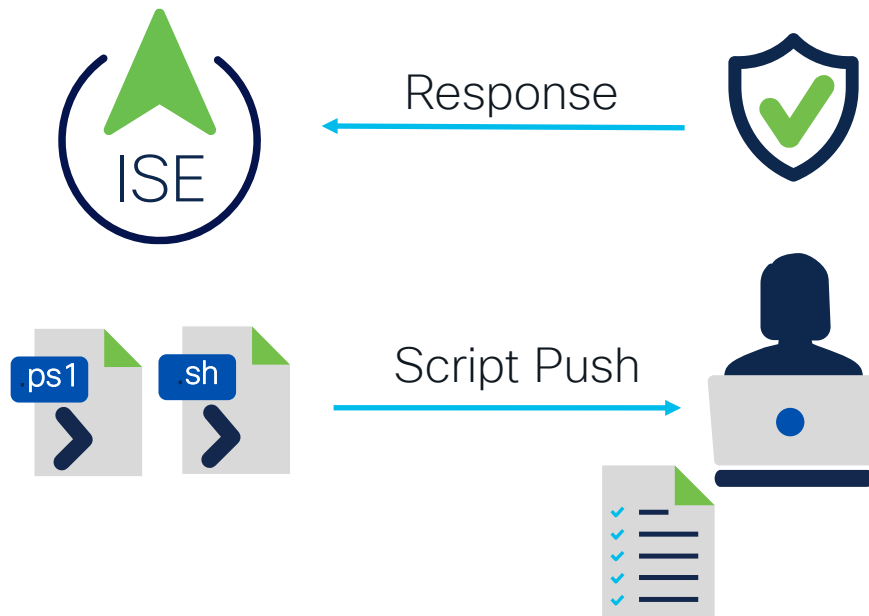
## Dynamic requirements

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

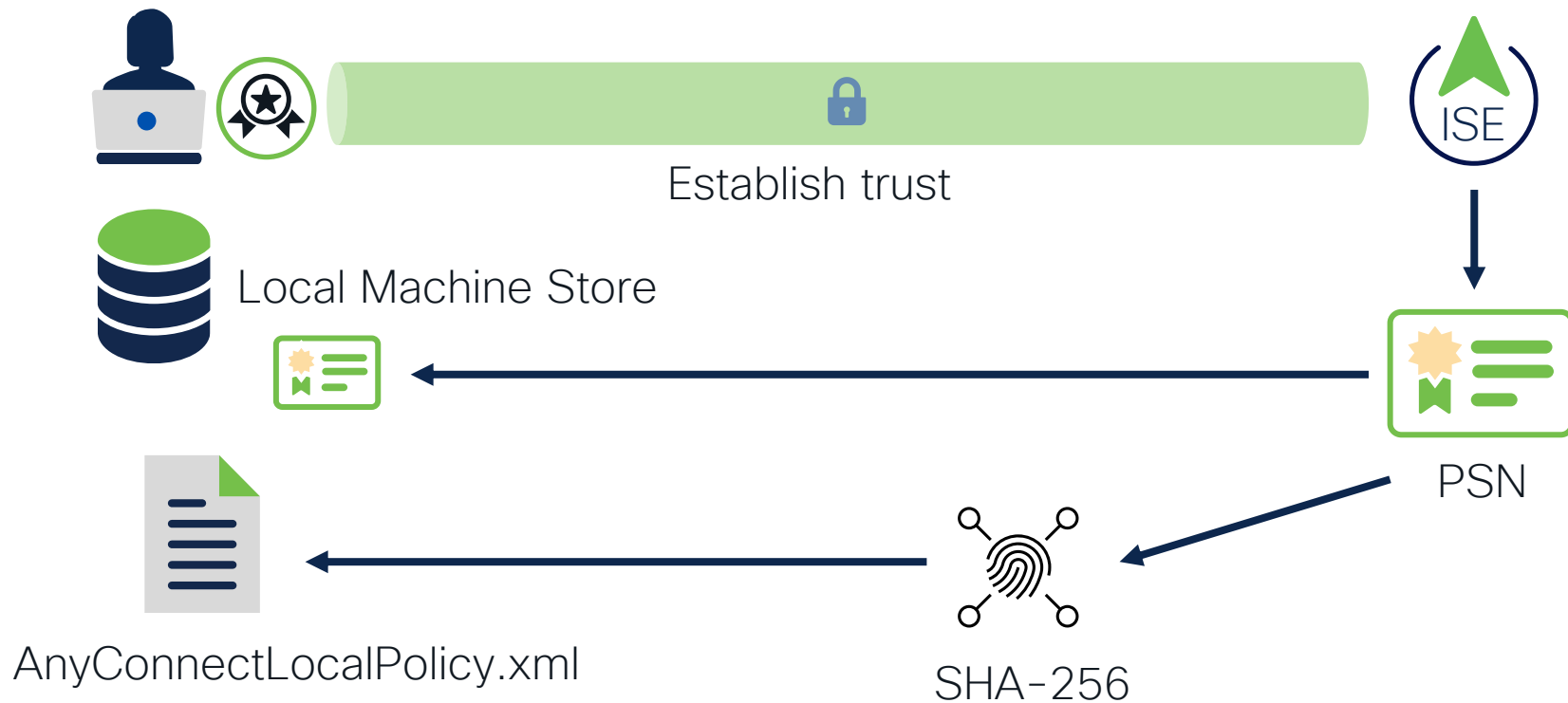
[ ... ]



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



# 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  
Anyconnect Secure Mobility Client\scripts



~/cisco/ise posture/scripts

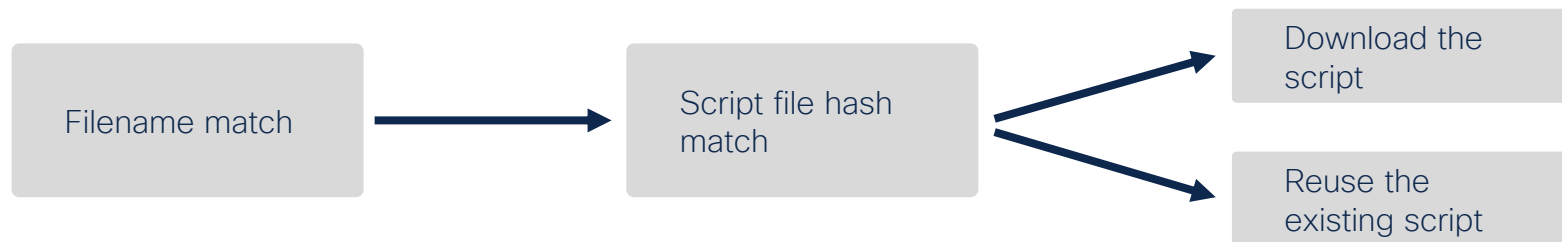
## Elevated privileges



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



/opt/cisco/anyconnect/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

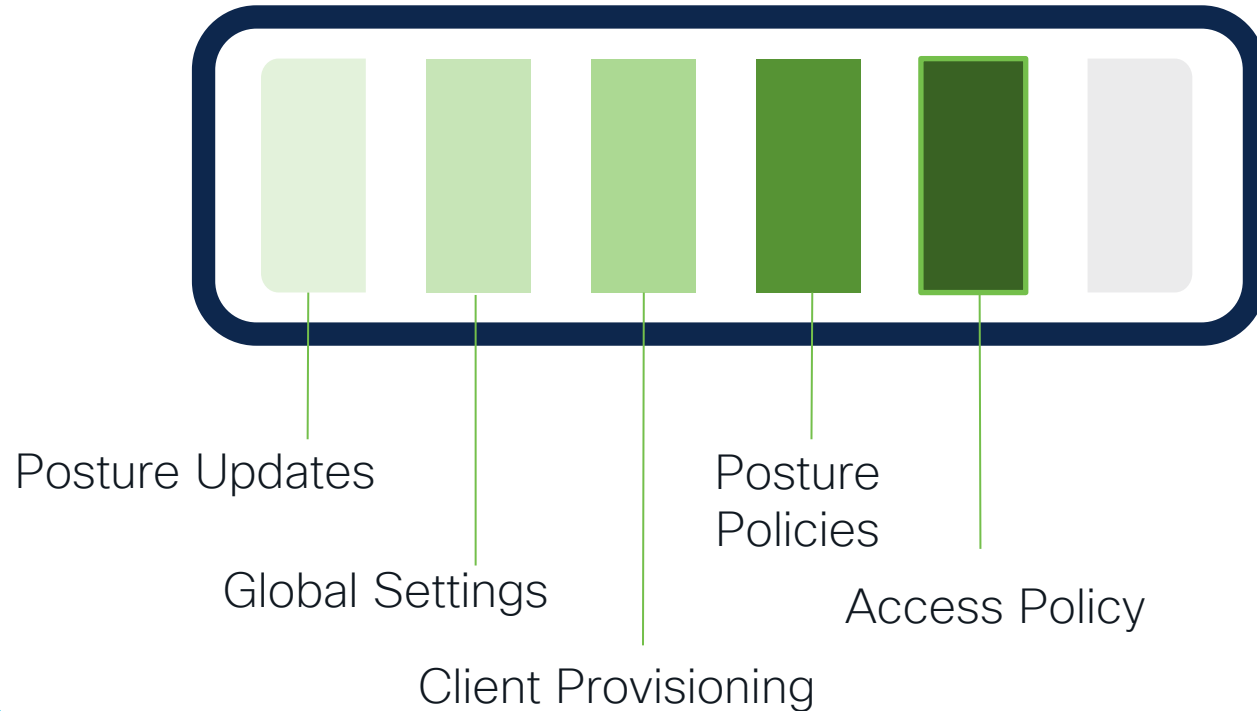


# Posture Script Exit Codes

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

# 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.

✓	Wired_Agent_Compliant	Session-PostureStatus EQUALS Compliant	Compliant	PermitAccess ×	⌵ +
✓	Wired_Agent_Redirect_copy	Session-PostureStatus EQUALS NonCompliant	NonCompliant	DenyAccess ×	⌵ +
✓	Wired_Agent_Redirect	Session-PostureStatus EQUALS Unknown	Unknown	Agent-Posture-Redirect ×	⌵ +

\* 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) ⓘ

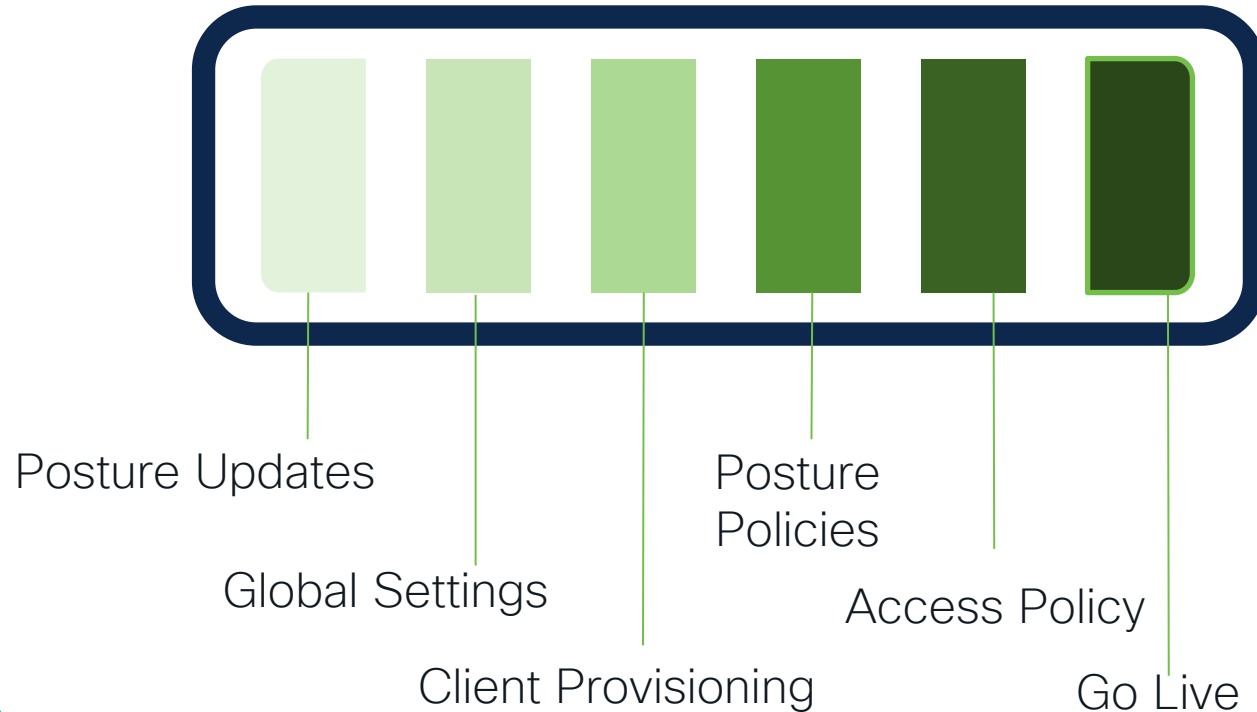
Client Provisioning (Posture) ⌵ ACL redirect-posture Value Client Provisioning Portal (def: ⌵

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

Must exists on NAD

# ISE Posture Journey: Time to Go Live



# Implementation and Troubleshooting together



# DEMO Implementation



Diana

Employee



Anti-Malware  
Script for CA



Contractors



External Data Source



Small branch



Win10 latest patch  
Firewall Enabled



A decorative graphic in the top right corner consisting of a dense cluster of circles in various colors including blue, green, orange, red, and yellow, with some smaller grey circles scattered around them.

Employee – Agent based

# Agent Posture – Employee Client Provisioning

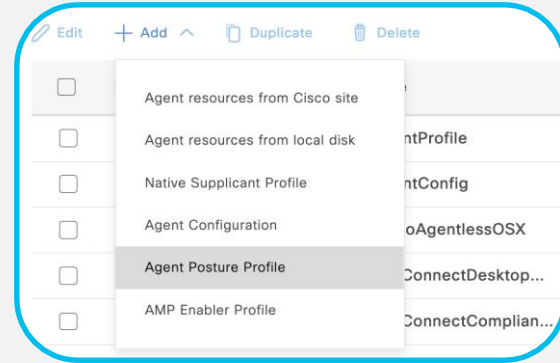
Posture Updates



AC Package +  
Compliance Module



## AC Posture Profile



Client Provisioning

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
KRK Windows	AD: Agent_Posture			then AgentConfig-Wired And WinSPWizard 3.2.0.1 And Cisco-ISE-NSP <a href="#">Edit</a>



# Agent Posture – Employee Posture Configuration

## Posture Condition

The diagram illustrates the configuration of a posture condition. On the left, a list of posture categories is shown, with 'Anti-Malware' selected. An arrow points from this list to a central target icon. Two arrows from the target icon point to a script upload interface on the right. Below the target icon is a checkbox labeled 'ANY\_am\_win\_inst' with the description 'Any AM installation check on Windows'.

**Posture Condition Configuration Interface:**

- Name:** Corp-CA-installed
- Description:** (Empty text area)
- Operating System:** Windows
- Script Type:** PowerShell (Selected), PowerShell Core
- File to Upload:** Cert-corporate-CA.ps1 (Choose File button)
- 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

# Agent Posture – Employee Posture Configuration

Posture Remediation



Warning with explanation

Posture Requirements

Any\_Branch\_Win    for    Windows All    using    4.x or later    using    Agent    met if    ANY\_am\_win\_inst & Corp-CA-installed    then    Message Text Only


Posture Policy

Policy Options    AMS\_BRANCH\_WIN    If    Any    and    Windows All    and    4.x or later    and    Agent    and    (Optional) Dictionary Attributes    then    Any\_Branch\_Win    [Edit](#) ▾

# Agent Posture: Final Step

✓	Wired_Agent_Compliant	AND	Session-PostureStatus EQUALS Compliant		PermitAccess ×	+
			DC1-ExternalGroups EQUALS Agent_Posture			
✓	Wired_Agent_Redirect	AND	Session-PostureStatus NOT_EQUALS Compliant		Agent-Posture-Redirect ×	+
			DC1-ExternalGroups EQUALS Agent_Posture			





AD: Agent Posture

### Authorization Profile

\* 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 (d...**

☐ Static IP/Host name/FQDN

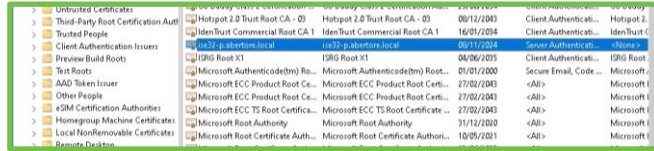
☐ Suppress Profiler CoA for endpoints in Logical Profile

# Time to test

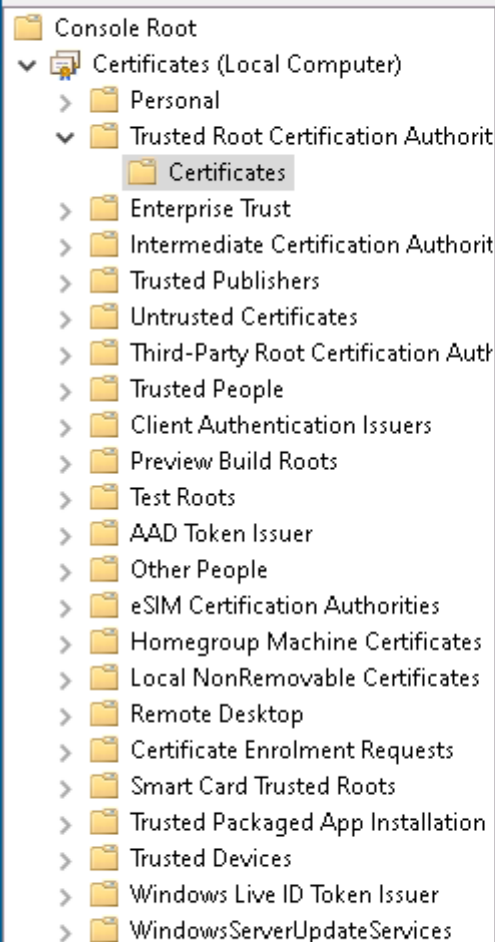


# Script Troubleshoot

## 1. Prerequisites check

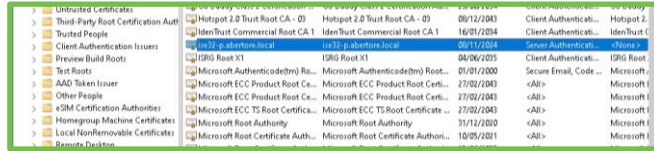


```
4 <TrustedISECertFingerprints>
5 <fingerprint>
6 <algorithm>SHA-256</algorithm>
7 <hash>CD:25:B2:84:F6:CD:B3:59:3A:F6:B0:B3:1F:CD:70:05:C5:C5:63:93:5A:27:1C:38:C4:44:78:CF:A8:58:92:F70</hash>
8 </fingerprint>
9 </TrustedISECertFingerprints>
```



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
DigiCert High Assurance EV Root...	DigiCert High Assurance EV Root ...	10/11/2031	Client Authenticati...	DigiCert
DST Root CA X3	DST Root CA X3	30/09/2021	Client Authenticati...	DST Root C
Entrust Root Certification Auth...	Entrust Root Certification Authori...	07/12/2030	Client Authenticati...	Entrust.net
GlobalSign	GlobalSign	18/03/2029	Client Authenticati...	GlobalSign
GlobalSign	GlobalSign	15/12/2021	Client Authenticati...	Google Tru
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Client Authenticati...	GlobalSign
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	29/06/2034	Client Authenticati...	Go Daddy
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	08/12/2043	Client Authenticati...	Hotspot 2.
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	16/01/2034	Client Authenticati...	IdenTrust C
ise32-p.abertore.local	ise32-p.abertore.local	08/11/2024	Server Authenticati...	<None>
ISRG Root X1	ISRG Root X1	04/06/2035	Client Authenticati...	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 Authenticati...	QuoVadis F
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	12/01/2042	Client Authenticati...	QuoVadis F
SecureTrust CA	SecureTrust CA	31/12/2029	Client Authenticati...	Trustwave
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	29/06/2034	Client Authenticati...	Starfield CI

## 1. Prerequisites check



```
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>
```

```
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>
```

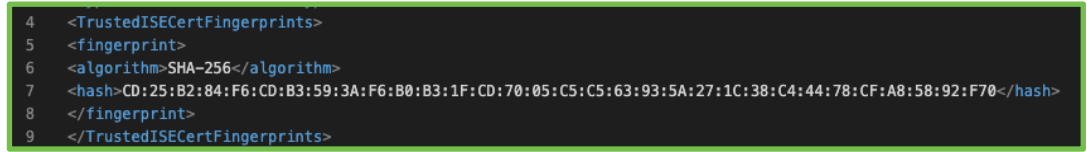
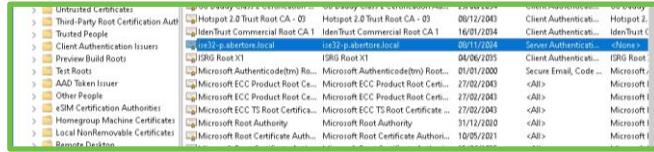


## 1. Prerequisites check



# 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	C0A8FF6400000867B2D2D7E	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	C0A8FF6400000867B2D2D7E	00:50:56:88:8B...

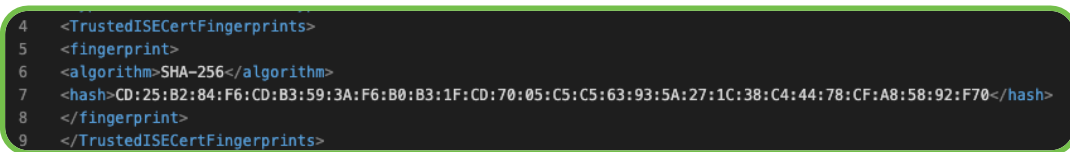
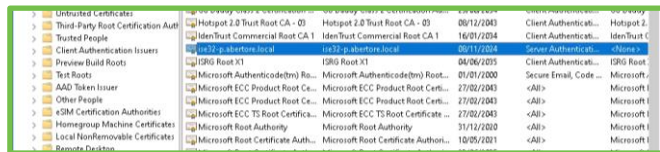
# Script Troubleshoot

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

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

# Script Troubleshoot

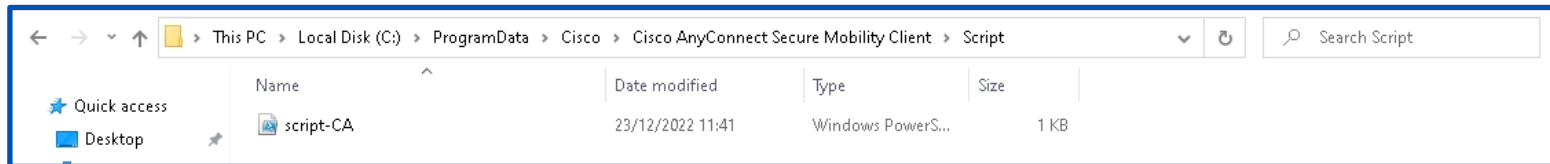
## 1. Prerequisites check

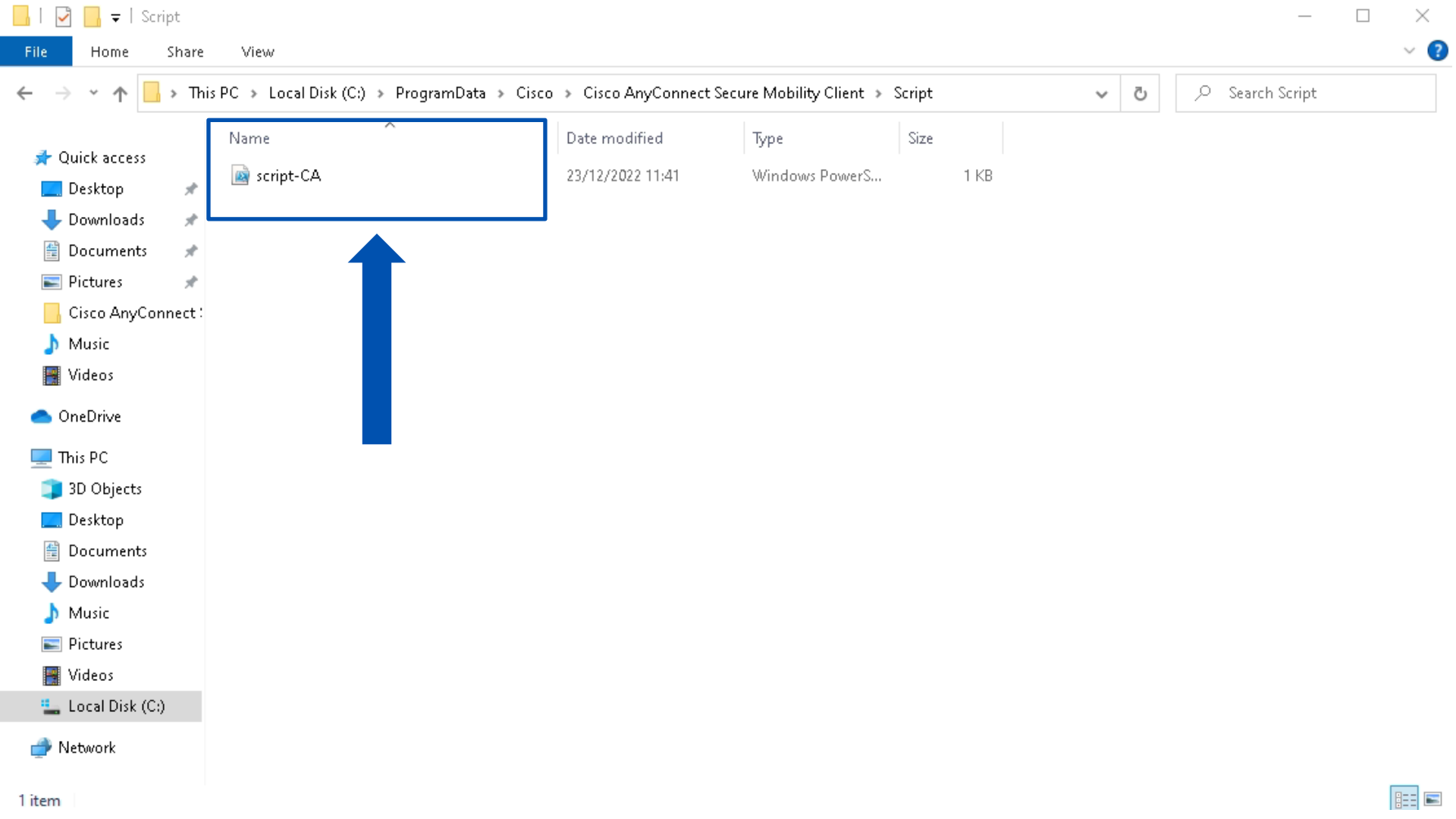


## 2. Check script failure report

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	

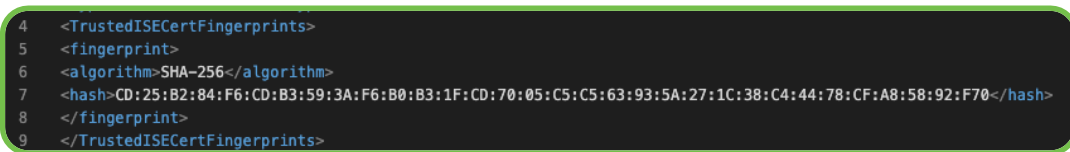
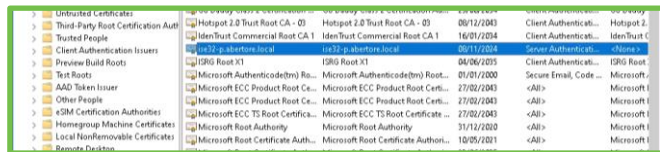
## 3. Check if the script is downloaded correctly





# Script Troubleshoot

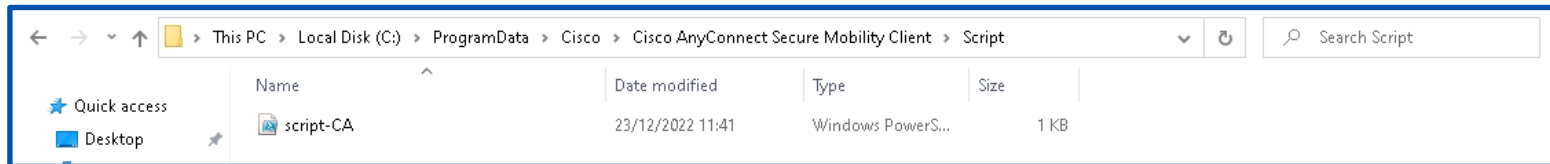
## 1. Prerequisites check



## 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: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

## 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) (UnauthorizedAccess:Scripting)) (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 information, see about_Execution_Policies. https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\script.ps1
+ ~~~~~
+ CategoryInfo          : (Error) ( (FullYqualifiedErrorId : UnauthorizedAccess
```

Running script is disabled on this system

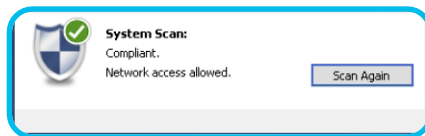
Windows PowerShell execution policy:

☒ 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

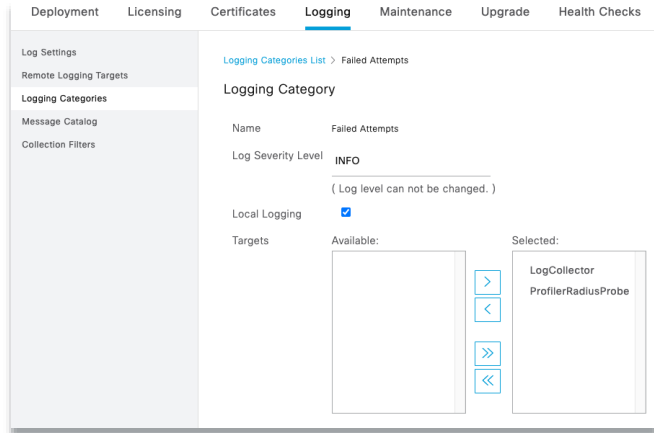
## 6. Results



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

# Troubleshoot Posture by ISE logs – iseLocalStore

By default for 1 day each ISE node stores all syslog messages of certain logging categories locally:



## Local Log Settings

Local Log Storage period

\* Keep up to 1 days(Logs may be deleted earlier if resources are needed)

(Valid Range 1 to 365)

CLI:

```
ise32/admin#show logging application | include iseLocal
573509 Jan 24 2023 09:57:54 localStore/iseLocalStore.log
1362872 Jan 23 2023 23:59:55 localStore/iseLocalStore.log.2023-01-23-00-00-00-736
```

# Troubleshoot Posture by ISE logs- iseLocalStore

To include iseLocalStore in your support bundle remember to check the checkbox:

Important message codes from iseLocalStore

80002 INFO Profiler: Profiler EndPoint profiling event occurred

5205 NOTICE Dynamic-Authorization: Dynamic Authorization succeeded

3002 NOTICE Radius-Accounting: RADIUS Accounting watchdog update

3000 NOTICE Radius-Accounting: RADIUS Accounting start request

Appliance node list

ise32

Support Bundle Debug Logs

- ☐ Include full configuration database ⓘ
- ☐ Include debug logs ⓘ
- ☒ Include local logs ⓘ
- ☐ Include core files ⓘ
- ☐ Include monitoring and reporting logs ⓘ
- ☐ Include system logs ⓘ
- ☐ Include policy configuration ⓘ

From Date

# What we have on ISE for posture - PrRT

Logs: prrt-server.log with runtime-aaa in DEBUG

Search Keys for all radius packets for a specific endpoint.



`CallingStationID=F0:78:07:11:11:17.*RADIUS PACKET.*Code=`

Example: we have a posture COA failure and would like to see more details in the logs (VPN example):

```
ade # cat prrt-server.log | grep -a 'CallingStationID=10.61.238.240.*RADIUS PACKET.*Code='
Radius,2022-10-23 12:22:40,492,DEBUG,0x7f496a3e6700,cntx=0027628155,sesn=skuchere-ise26-1/384213726/11919,CallingStationID=10.61.238.240,RADIUS PACKET::
Code=1(AccessRequest) Identifier=79 Length=673
Radius,2022-10-23 12:22:44,122,DEBUG,0x7f496a2e5700,cntx=0027628155,sesn=skuchere-ise26-
1/384213726/11919,CPMSessionID=c0a81c010073e0005f92af8b,user=bob@example.com,CallingStationID=10.61.238.240,RADIUS PACKET:: Code=2(AccessAccept)
Identifier=79 Length=471
Radius,2022-10-23 12:22:44,159,DEBUG,0x7f496a1e4700,cntx=0027628189,sesn=skuchere-ise26-
1/384213726/11921,CPMSessionID=c0a81c010073e0005f92af8b,CallingStationID=10.61.238.240,RADIUS PACKET:: Code=4(AccountingRequest) Identifier=81 Length=728
Radius,2022-10-23 12:22:44,169,DEBUG,0x7f496a6e9700,cntx=0027628189,sesn=skuchere-ise26-
1/384213726/11921,CPMSessionID=c0a81c010073e0005f92af8b,user=bob@example.com,CallingStationID=10.61.238.240,RADIUS PACKET:: Code=5(AccountingResponse)
Identifier=81 Length=20,RADIUSHandler.cpp:2214
RadiusClient,2022-10-23 12:23:03,481,DEBUG,0x7f495e92c700,cntx=0027628350,sesn=1a8cd632-9b18-4076-af60-3eef7af79cb4,CallingStationID=10.61.238.240, RADIUS
PACKET: Code=43 (CoARequest) Identifier=25 Length=205
RadiusClient,2022-10-23 12:23:03,485,DEBUG,0x7f496a1e4700,cntx=0027628350,sesn=1a8cd632-9b18-4076-af60-3eef7af79cb4,CallingStationID=10.61.238.240, RADIUS
PACKET: Code=44 (CoAAck) Identifier=25 Length=20,RadiusClientHandler.cpp:49
```

# What we have on ISE for posture - Policy

Authorization policy troubleshooting:

Component in DEBUG mode:

epm-pip  
epm-pdp

Debugs are saved into ise-psc,  
Example to troubleshoot posture status

```
ade # cat ise-psc.log | grep -a '.pip.*PostureStatus'
```

```
2022-10-23 12:22:44,066 DEBUG [Thread-253][ ] cisco.cpm.posture.pip.PostureStatusPIP -::::- PostureStatusPIP for mac 00-0C-29-A6-39-  
CD - Attribute Session.PostureStatus value is Unknown  
2022-10-23 12:52:31,559 DEBUG [Thread-616][ ] cisco.cpm.posture.pip.PostureStatusPIP -::::- fast reconnect is enabled  
2022-10-23 12:52:31,590 DEBUG [Thread-616][ ] cisco.cpm.posture.pip.PostureStatusPIP -::::- the posture expiry value is null  
2022-10-23 12:52:31,590 DEBUG [Thread-616][ ] cisco.cpm.posture.pip.PostureStatusPIP -::::- PostureStatusPIP for mac 00-0C-29-A6-39-  
CD - Attribute Session.PostureStatus value is Unknown
```

# What we have on ISE for posture – Provisioning

## Client Provisioning Troubleshooting

Component in DEBUG mode

**client-webapp**  
**provisioning**

Target files are **ise-psc** and **guest.log** (here specifically we see agent exchanges with ISE):

```
ade # cat guest.log | grep -C 10 -a '2022-10-23 12:52.*192.168.253.11'
```

Use **EP MAC** or **IP** as a search key, add data/time to focus on specific posture attempt.

Start from

```
2022-10-23 12:52:44,750 DEBUG [https-jsse-nio-192.168.43.26-8443-exec-2][  
cisco.cpm.client.posture.PostureStatusServlet -::- Got http request from 192.168.253.11 user agent  
is: Mozilla/4.0 (compatible; WINDOWS; 1.2.1.10.0.48; AnyConnect Posture Agent v.4.9.01095)
```

And follow the logs

## What we have on ISE for posture - Posture

If you need to debug posture events

## Component in DEBUG: posture

Target file is ise-psc

```
cat ise-psc.log | grep -a '2022-10-23 12:52:. *posture.runtime.PostureHandlerImpl.*receiving request from client.*00:0C:29:A6:39:D7|2022-10-23 12:52:. *https-jsse-nio.*Sending response to endpoint.*00-0C-29-A6-39-CD'
```

It's better to use data/time in a search to narrow down search results to specific posture attempt. To investigate entire flow start from very first - receiving request from client message and follow the logs.

```
2022-10-23 12:52:52,526 DEBUG [https-jsse-nio-192.168.43.26-8443-exec-8]] cisco.cpm.posture.runtime.PostureHandlerImpl -:- receiving request from client  
497be29bbe8a6936f7cbb0b539b451d3c6a5028 192.168.253.11  
00:0C:29:A6:39:D7,00:0C:29:A6:39:D7,00:0C:29:A6:39:D7,00:0C:29:A6:39:D7,00:0C:29:A6:39:D7,00:0C:29:A6:39:D7,00:0C:29:A6:39:C  
D,00:0C:29:A6:39:CD,00:0C:4F:50,00:0C:4F:50,00:0C:4F:50,8C:85:90:7A:E5:57,8C:85:90:7A:E5:57  
192.168.253.11,fe80::ceed:4:f40:5e83:b231,fe80::6591:5:a94:e697:26b0,169.254.170.158,fe80::b8d4:3ff6:bc0a:aa9e,2001:99::10,2001:78::10,2001:64::10,172.16.231.140,fe8  
0::989c:608c:5da0:d0f3,169.254.144.137,fe80::35f9:85df:8f4e:9089,169.254.68.191,fe80::a8d8:3cf d:41d6:44bf w13vkpoq  
2022-10-23 12:52:52,618 DEBUG [https-jsse-nio-192.168.43.26-8443-exec-8]] cisco.cpm.posture.runtime.PostureHandlerImpl -:bob@example.com::- Sending response to  
endpoint 00-0C-29-A6-39-CD http response [[ <!--X-Perfigo-UserKey--><!--X-Perfigo-Provider=Device Filter--><!--X-Perfigo-UserName=bob@example.com--><!--  
error=1010--><!--X-Perfigo-DM-Error=1010--><!--user role==><!--X-Perfigo-OriginRole==><!--X-Perfigo-DM-Scan-Req=0--><!--X-ISE=  
IV=EPM3w/uVxW1Wavdpw2oM4w===>
```

# Contractors – Agent Stealth



# Contractor: External Data Source – AD



UDID



Compliant Status

```
PS C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe -u  
UDID: 6784390258062387648723123687284638
```

Attributes:

Attribute	Value
thumbnailPhoto	<not set>
title	<not set>
udid	BBB7EBCF3391CE62E8DE4C61A535F1A7
uid	1111111
uidNumber	22

Attributes:

Attribute	Value
catalogs	<not set>
cn	DESKTOP-R2CH8G5
co	<not set>
codePage	0
comment	<not set>
company	<not set>
compliantStatus	Compliant
controlAccessRights	<not set>

# Agent Stealth – Contractors

Client Provisioning

☒ Stealth Agent    If Any    and Windows    **AD: Agent Stealth**    then Agent Configuration And WinSPWizard 3.2.0.1

Condition

**Conditions**

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource**
- File

External DataSource Condition > External DataSource Condition

Name\*  
External-DC1

Description

AD Join Point\*  
DC1

Device Id\*  
udid

Expression

Attribute	Operator	Value
compliantStatus	Equals	1

Cancel Save

Device ID

Attribute

# Small Branch – Agentless based

# Agentless: Small Branch

## Client Provisioning

Agentless Posture

if Any

AD: Agentless Posture Users

CiscoAgentlessWindows 4.9.01059

Edit

## Condition and Requirements

Default\_Firewall\_Condition\_Win

Description  
Cisco Predefined Check for Firewall

Compliance module\*  
4.x or later

Operating System\*  
Windows All

Vendor\*  
ANY


☐ Enable

At least one product must be selected\*

Product Name	Version
ANY	ANY

Cancel

Save



Win10\_Update

Description

Operating System  
Windows All

Compliance Module  
4.x or later


Vendor Name  
Microsoft Corporation

Check Type  
☐ Installation ☐ Enabled ☒ Up to Date

Check patches installed  
Critical only

Products for Selected Vendor

Product Name	Version	Enabled	Checked S...	Update Checked Su...	Minimum Compliant Mod...
<input type="checkbox"/> Microsoft Intune Client	5.x	NO	NO	4.2.520.0	
<input type="checkbox"/> Microsoft Intune Management Extension	1.x	NO	NO	4.3.2815.6145	
<input type="checkbox"/> System Center Configuration Manager Client	4.x	YES	YES	4.2.1331.0	
<input type="checkbox"/> System Center Configuration Manager Client	5.x	YES	YES	4.2.520.0	
<input checked="" type="checkbox"/> Windows Update Agent	10.x	YES	YES	4.2.520.0	



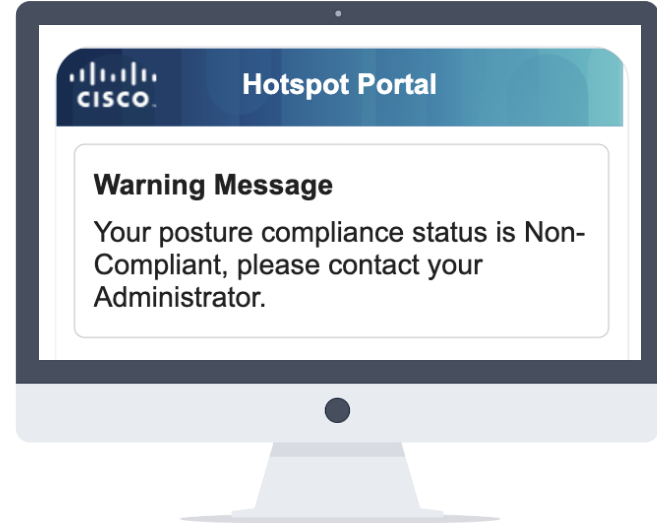
# Agentless: Failure Flow

### 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...](#)



Session-AgentlessFlowStatus

✓	Agentless_Failure_Warning	AND	<div>Session-PostureStatus EQUALS NonCompliant</div> <div>DC1-ExternalGroups EQUALS Agentless Posture Users</div> <div>Session-AgentlessFlowStatus EQUALS Failure</div>	Agentless Warning ×	↓ +	Select from list	↓ +	0	⚙
---	---------------------------	-----	---	---------------------	-----	------------------	-----	---	---

# Agentless: Failure Flow

✓	Agentless_Compliant	AND	<div>Session-PostureStatus EQUALS Compliant</div> <div>DC1-ExternalGroups EQUALS Agentless Posture Users</div>	PermitAccess ×	▼ +	Select from list	▼ +	0	⚙
✓	Agentless_Failure_Warning	AND	<div>Session-PostureStatus EQUALS NonCompliant</div> <div>DC1-ExternalGroups EQUALS Agentless Posture Users</div> <div>Session-AgentlessFlowStatus EQUALS Failure</div>	Agentless Warning ×	▼ +	Select from list	▼ +	0	⚙
✓	CPP_Agentless	AND	<div>Session-PostureStatus NOT_EQUALS Compliant</div> <div>DC1-ExternalGroups EQUALS Agentless Posture Users</div>	CPP Agentless Posture ×	▼ +	Select from list	▼ +	0	⚙

\* Name

Agentless Warning

Description

\* Access Type

ACCESS\_ACCEPT

Network Device Profile

Cisco

Service Template

☐

Track Movement

☐

Agentless Posture

☐

Passive Identity Tracking

☐

## Common Tasks

☐ VLAN

☐ Voice Domain Permission

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

Hot Spot



ACL



Value

Self-Registered Guest Port...



# Agentless: Failure Flow #2

## 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	<a href="#">Edit</a> ▾
Agentless Posture	If Any	and Windows All	and DC1:ExternalGroups EQUALS Agentless Posture	then CiscoAgentlessWindows 5.0.00529	<a href="#">Edit</a> ▾

## 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

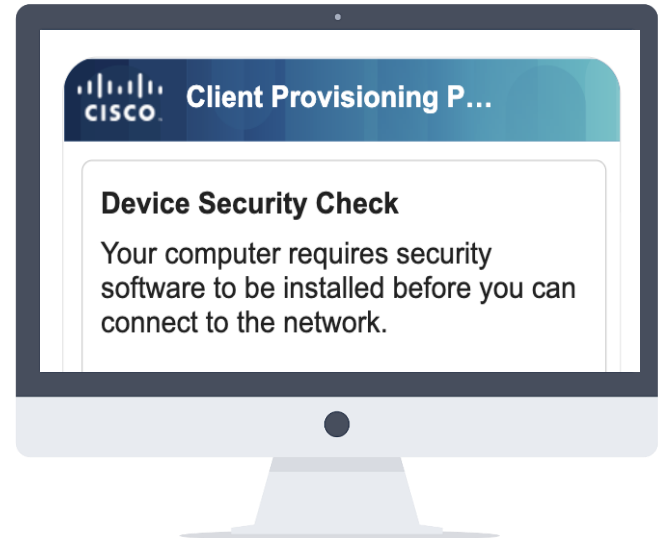
☒ Web Redirection (CWA, MDM, NSP, CPP) ⓘ

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





# Agentless: Troubleshooting, our tools



General Tools

RADIUS Authentication Troubl...

Execute Network Device Com...

Evaluate Configuration Validat...

Posture Troubleshooting

Agentless Posture Troublesh...

EndPoint Debug

TCP Dump

Session Trace Tests

### Agentless Posture Troubleshooting

The Agentless Posture Troubleshooting tool collects agentless posture activity from a specific client. Cisco ISE collects the required information, and you can then export a ZIP file of the logs.

☒ Run Agentless Posture Flow ⓘ

☐ Only Download Client Logs ⓘ

☐ Agentless Posture Prerequisites Check ⓘ

MAC Address\*

00:50:56:88:8B:A3

Authentication Flow Verification

Client Provisioning Verification

Posture Report

# ISE posture related debugs

*ise-psc.log*



- Processing of initial and final posture report
- Posture policy selection
- PRA operations

Debug to  
enable

posture

*guest.log*



- Session lookup process when Discovery probe has reached PSN without redirect
- Client provisioning policy selection

Debug to  
enable

provisioning

guestaccess

client-  
webapp

## Search Keys

One from list (order defines priority):

- *Session ID, EP MAC, EP IP,*

Combined with



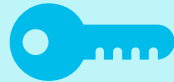
- *cisco.cpm.posture.runtime*

## Search Keys

One from list (order defines priority):

- *EP MAC, Endpoint IP, username*

Combined with



- *cisco.cpm.client.posture*

# 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

Endpoint not Reacheable

Add to My ReportsExport ToSchedule

FilterRefresh⚙️

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

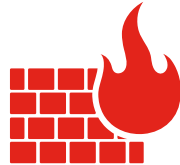
```
2022-10-01 06:56:47,609 INFO [pool-233-thread-7][] cisco.cpm.posture.events.PostureMessagesConsumer
-:::- Received on queue=SCRIPT-UPLOAD-FAILED, sessionId=25276A0A0000105BE2F00935,
endpointIP=10.106.39.38, mac=B4-96-91-22-A9-48, os=WINDOWS, failureReason=null
```

# Agentless: Common issues #1

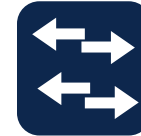


Port 5985

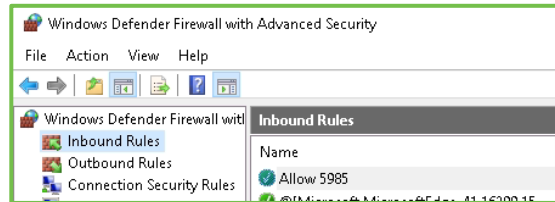
No.	Time	Source	Destination	Protocol	Length	Destination Port	Source Port	Source Port	Info
2360	18:08:18.85	10.127.197.83	10.106.39.38	TCP	74		59027	59027	59027 → 5985 [SYN] Seq=0 W
2454	18:08:18.85	10.127.197.83	10.106.39.38	TCP	74		59039	59039	59039 → 5985 [SYN] Seq=0 W
2477	18:08:18.85	10.127.197.83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

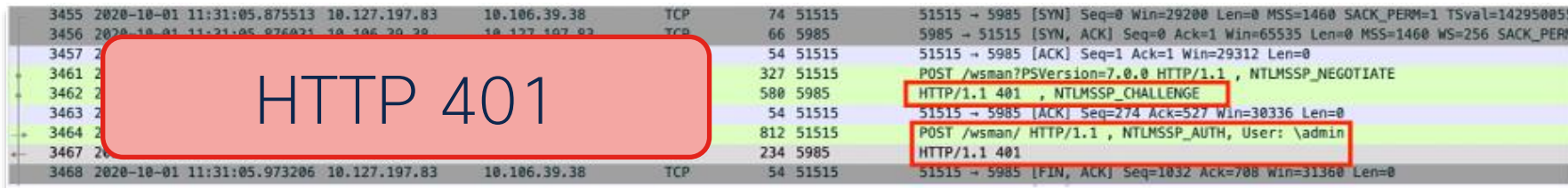
Ips are unreachable

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

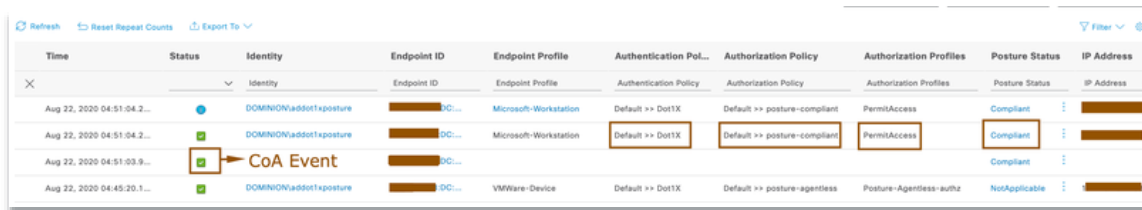
My Rep

# 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
```




No.	Time	Source	Destination	Protocol	Length	Info
3455	2020-10-01 11:31:05.875513	10.127.197.83	10.106.39.38	TCP	74	51515 → 5985 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=142950051
3456	2020-10-01 11:31:05.876021	10.106.39.38	10.127.197.83	TCP	66	5985 → 51515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
3457	2020-10-01 11:31:05.876021	10.127.197.83	10.106.39.38	TCP	54	51515 → 5985 [ACK] Seq=1 Ack=1 Win=29312 Len=0
3461	2020-10-01 11:31:05.876021	10.127.197.83	10.106.39.38	TCP	327	51515 → 5985 [ACK] Seq=1 Ack=1 Win=29312 Len=0
3462	2020-10-01 11:31:05.876021	10.127.197.83	10.106.39.38	TCP	580	5985 → 51515 [ACK] Seq=1 Ack=1 Win=29312 Len=0
3463	2020-10-01 11:31:05.876021	10.127.197.83	10.106.39.38	TCP	54	51515 → 5985 [ACK] Seq=274 Ack=527 Win=30336 Len=0
3464	2020-10-01 11:31:05.876021	10.127.197.83	10.106.39.38	TCP	812	51515 → 5985 [ACK] Seq=274 Ack=527 Win=30336 Len=0
3467	2020-10-01 11:31:05.876021	10.127.197.83	10.106.39.38	TCP	234	5985 → 51515 [ACK] Seq=1 Ack=1 Win=29312 Len=0
3468	2020-10-01 11:31:05.973206	10.127.197.83	10.106.39.38	TCP	54	51515 → 5985 [FIN, ACK] Seq=1032 Ack=708 Win=31360 Len=0



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

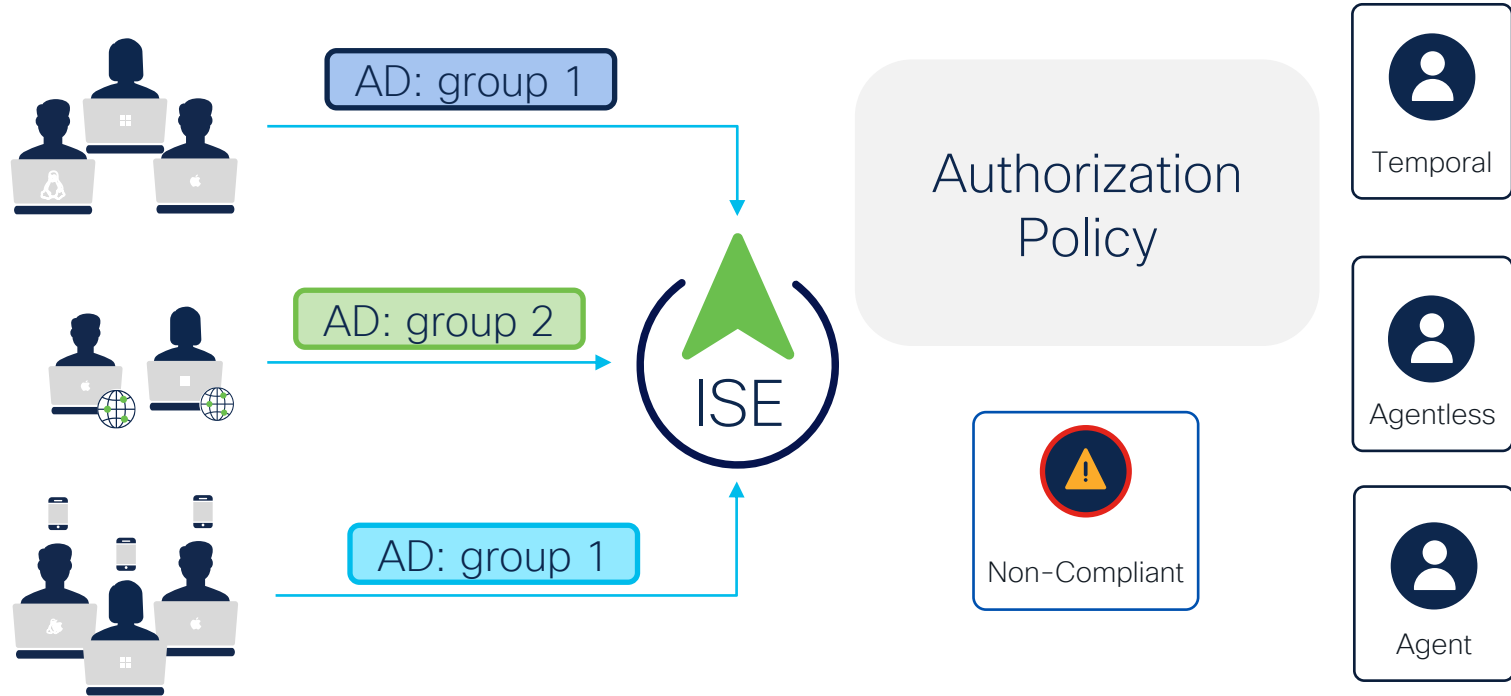
Refresh Reset Repeat Counts Export To Filter

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	...
Aug 22, 2020 04:51:04.2...	✓	DOMINION\addot1xposture	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\addot1xposture	DC...	VMWare-Device	Default >> Dot1X	Default >> posture-agentless	Posture-Agentless-authz	NotApplicable	...

# Implementation caveats recap

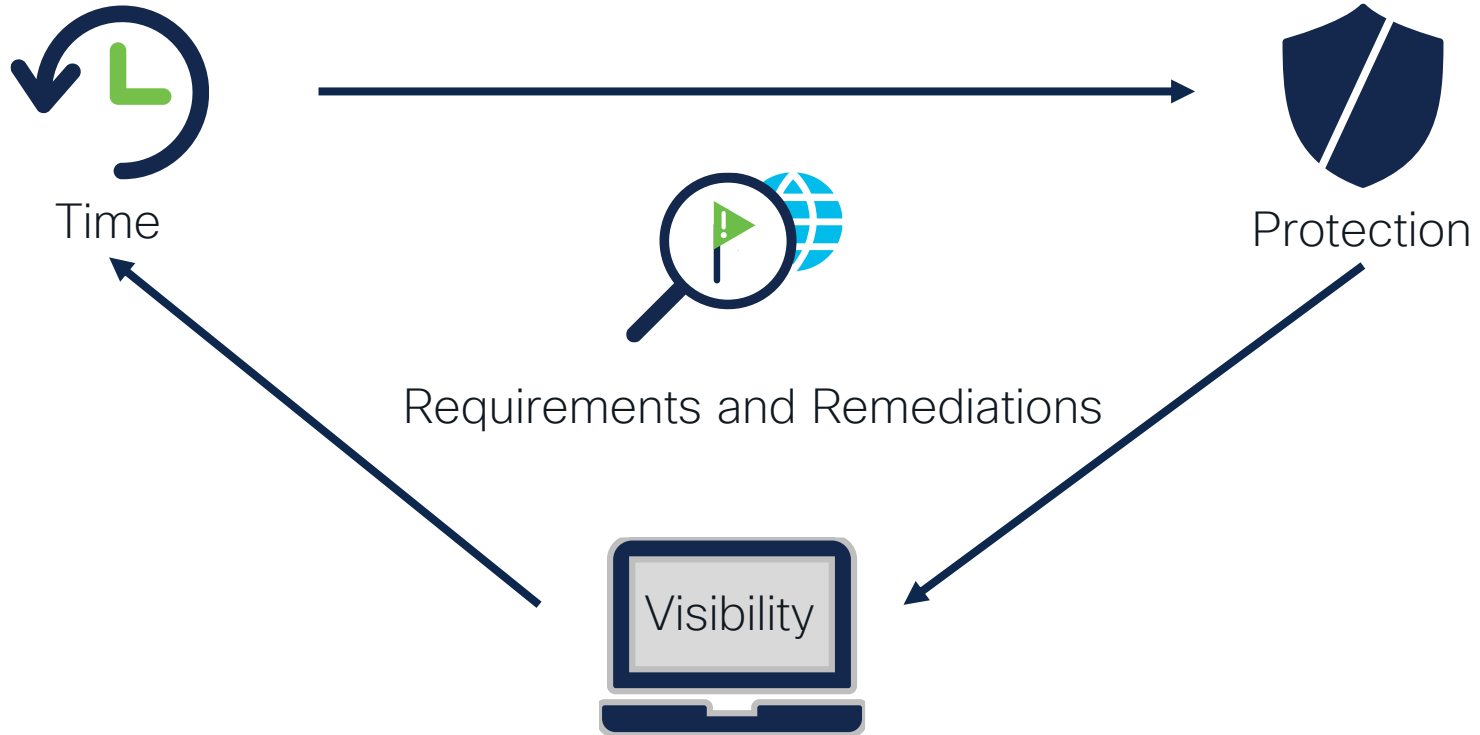
Client provisioning per user group


Policy Authorization per user group





# Key Takeaways





*Vigilance on what is on your network  
is just as important as who is on the  
network. Therefore, posture is so  
important.*

# Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand).

# Security Technologies

## Network Security

Learn about a broad range of solution and technologies which will help you better understand how to secure your network. You will find topics such as VPN, ISE, IPv6, DDoS, IoT....

START

Feb 5 | 19:00

### **LABSEC-2333**

ISE integrations via pxGrid with FTD, WSA, StealthWatch

Feb 6 | 08:45

### **TECSEC-3781**

Walking on solid ISE - Advanced Use Cases and Deployment Best Practices

Feb 7 | 08:45

### **BRKSEC-2445**

The Art of ISE Posture, Configuration and Troubleshooting

Feb 7 | 11:30

### **BRKSEC-2037**

Securing Starlink Internet Services

Feb 8 | 10:45

### **BRKSEC-2096**

Securing Industrial Networks: Where do I start?

Feb 8 | 13:30

### **BRKSEC-2678**

DDoS Mitigation: Introducing Radware Deployment on Firepower Appliances

Feb 9 | 08:30

### **BRKSEC-2660**

ISE Deployment Staging and Planning

Feb 9 | 10:30

### **BRKSEC-2101**

Malware Execution As A Service: a Deep Dive into CSMA Advanced File Analysis

Feb 9 | 15:45

### **BRKSEC-3058**

Route based VPNs with Cisco Secure Firewall

Feb 9 | 15:45

### **BRKSEC-2044**

Secure Operations for an IPv6 Network

Feb 10 | 09:00

### **BRKSEC-3019**

Visibility, Detection and Response with Cisco Secure Network Analytics

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

**CISCO** *Live!*

# Security Technologies

## Zero Trust

Learn how Cisco will help you deploy a broad range of technologies in order to deploy your end to end Zero Trust strategy.

START

Feb 5 | 16:00

### **LABSEC-2089**

Multi-factor Authentication:  
Integration of DUO with ISE for MFA

Feb 6 | 08:45

### **TECSEC-2007**

Find Your Zen with Cisco Secure  
Workload for Zero Trust Segmentation

Feb 6 | 08:45

### **TECSEC-2781**

Zero Trust: From understanding the  
risks to architecting a practical solution

Feb 6 | 15:20

### **PSOSEC-1210**

A global view on Zero-Trust  
- mapping your business resilience  
requirements

Feb 7 | 08:45

### **BRKSEC-2445**

The Art of ISE Posture, Configuration  
and Troubleshooting

Feb 7 | 16:45

### **BRKSEC-2053**

Zero Trust: Securing the  
Evolving Workplace

Feb 7 | 17:00

### **BRKSEC-1139**

Application Security  
- The Final Frontier

Feb 8 | 10:45

### **BRKSEC-2096**

Securing Industrial Networks:  
Where do I start?

Feb 8 | 13:30

### **BRKSEC-2748**

Taking Authentication to the Next Level  
with Cisco Secure Access by Duo

Feb 8 | 17:00

### **BRKSEC-2123**

Solving the Segmentation Puzzle!  
Secure Workload and Secure  
Firewall Integration

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

**CISCO** *Live!*

# Complete your Session Survey

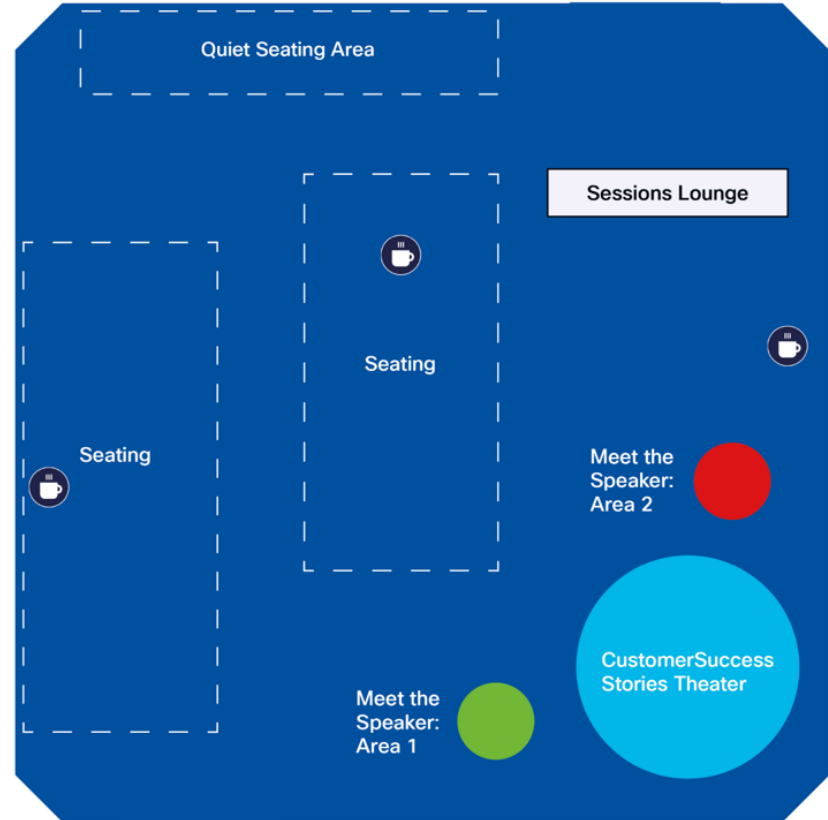
- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>



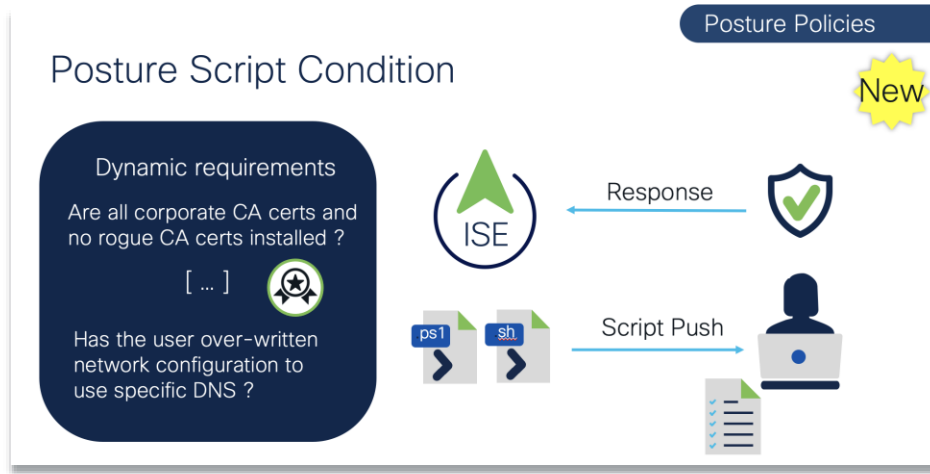
# MTS – Meet the Speaker – Area 2

Let's continue the discussion/Q&A

Tuesday, Feb 7 12:20 -12:50 PM



# Next action



New Posture script condition

Task for you: Test it in your lab !





The bridge to possible

# Thank you

CISCO *Live!*

CISCO *Live!*

ALL IN