cisco *Live!*

Let's go

About me

- AAA TAC Engineer

- ThousandEyes Support Engineer

- Security Consulting Engineer

Warning!
Italian accent ahead

ACCENT

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.

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

Agenda

1 **Basic Posture**

- ISE Posture 101
- ISE Posture Journey

2 **Advanced Posture Processes**

- Session Sharing
- Discovery Process
- Compliant State

3 **Advanced Scenarios Application**

- Posture, MFA, VPN and Duo Proxy
- Posture, MFA, Duo DAG and ASA with SAML

4 **Posture Troubleshooting**

- Deep Dive Troubleshooting
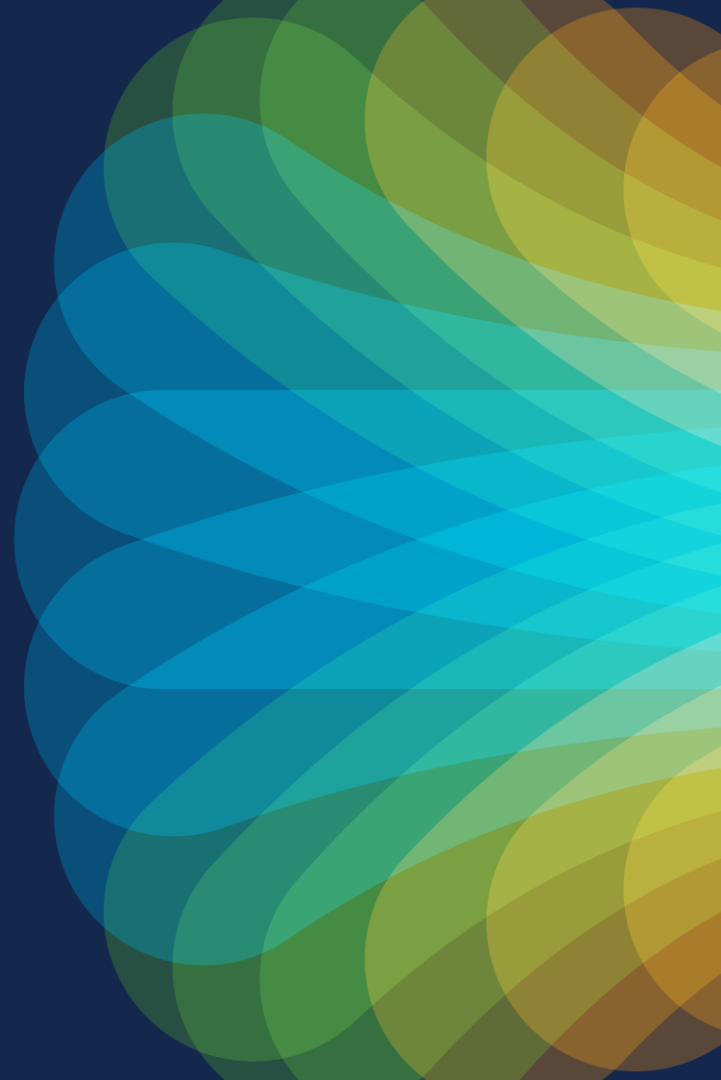- Learn on Example

Session Objectives

Session will cover:

- Theory of Posture
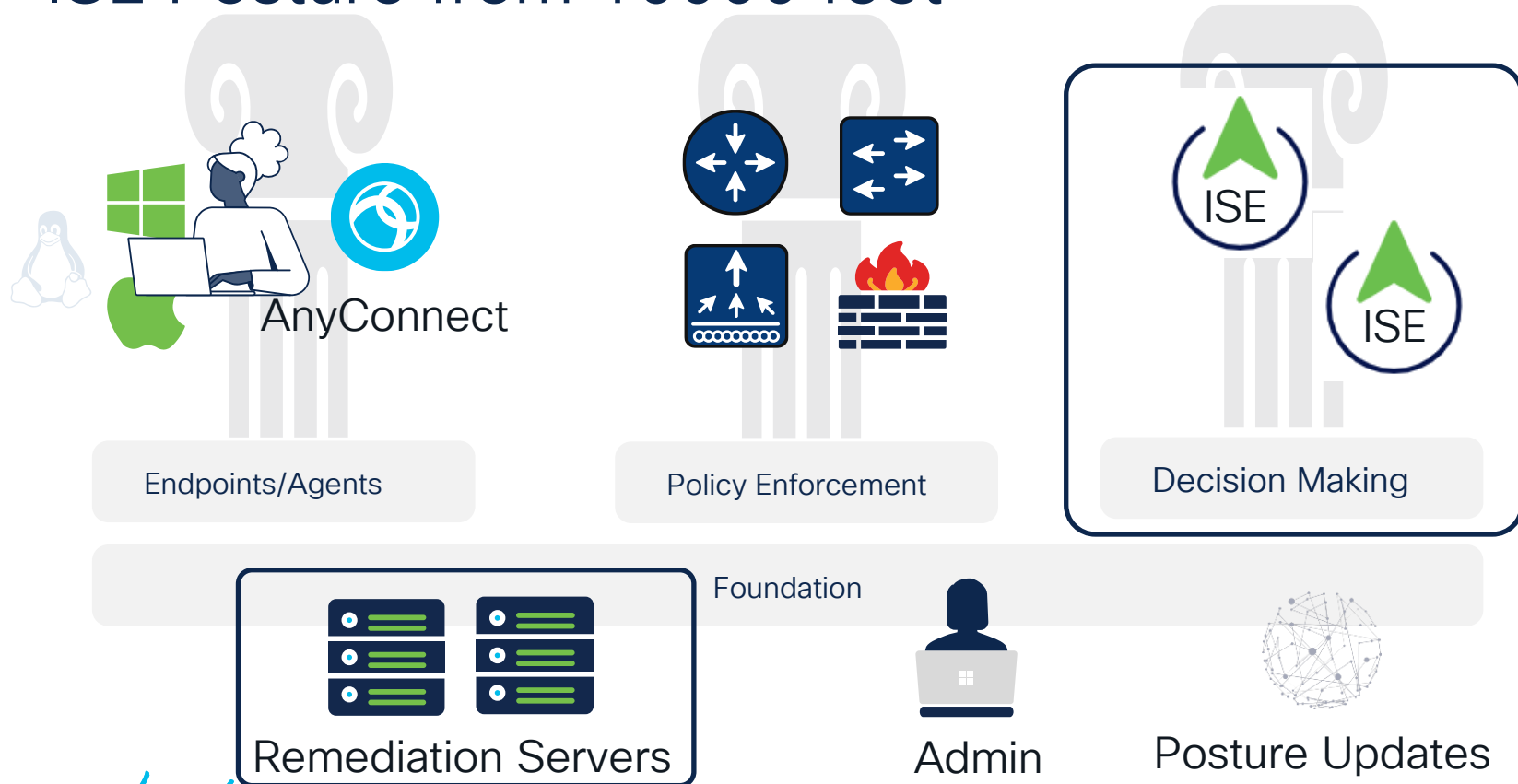
- Posture deployment scenarios

- Troubleshoot methodology

Session will not cover:

- Marketing

- Roadmaps

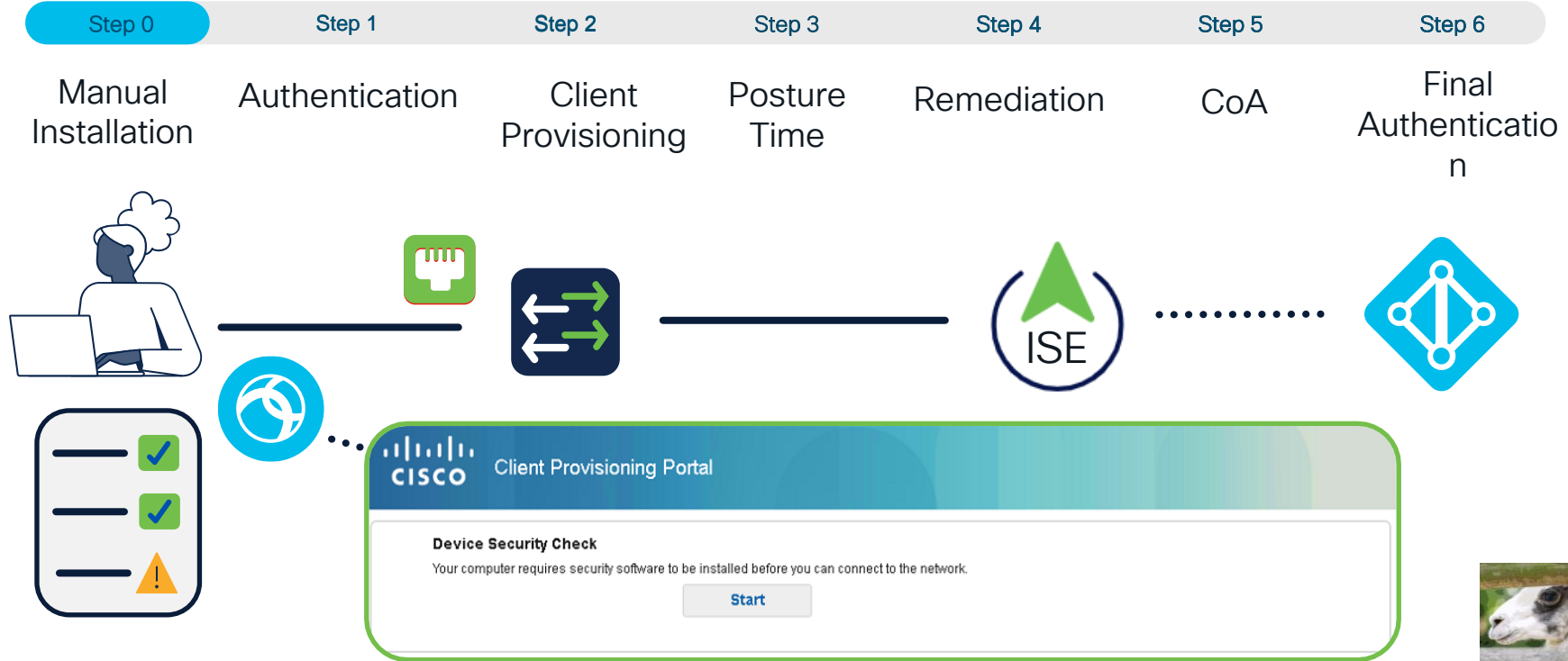- All possible ISE posture features

Posture 101

ISE Posture from 10000 feet

Endpoints/Agents

AnyConnect

Policy Enforcement

Decision Making

ISE

ISE

Foundation

Remediation Servers

Admin

Posture Updates

Posture Lifecycle

Step 0	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Manual Installation	Authentication	Client Provisioning	Posture Time	Remediation	CoA	Final Authentication

CISCO

Client Provisioning Portal

Device Security Check

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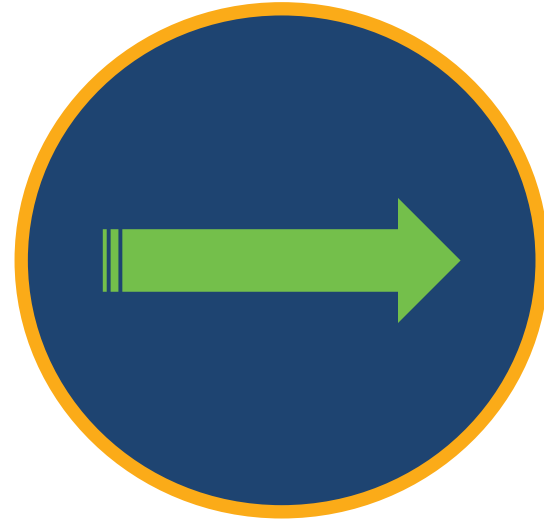
Start

ISE Posture Flow types

Redirect based

Non-redirect based

Posture with pre-installed Agent (no-profile)

ISEPostureCFG.xml HASH=321

ISEPostureCFG.xml
HASH=123

Overwrite

ISEPostureCFG.xml
HASH=321

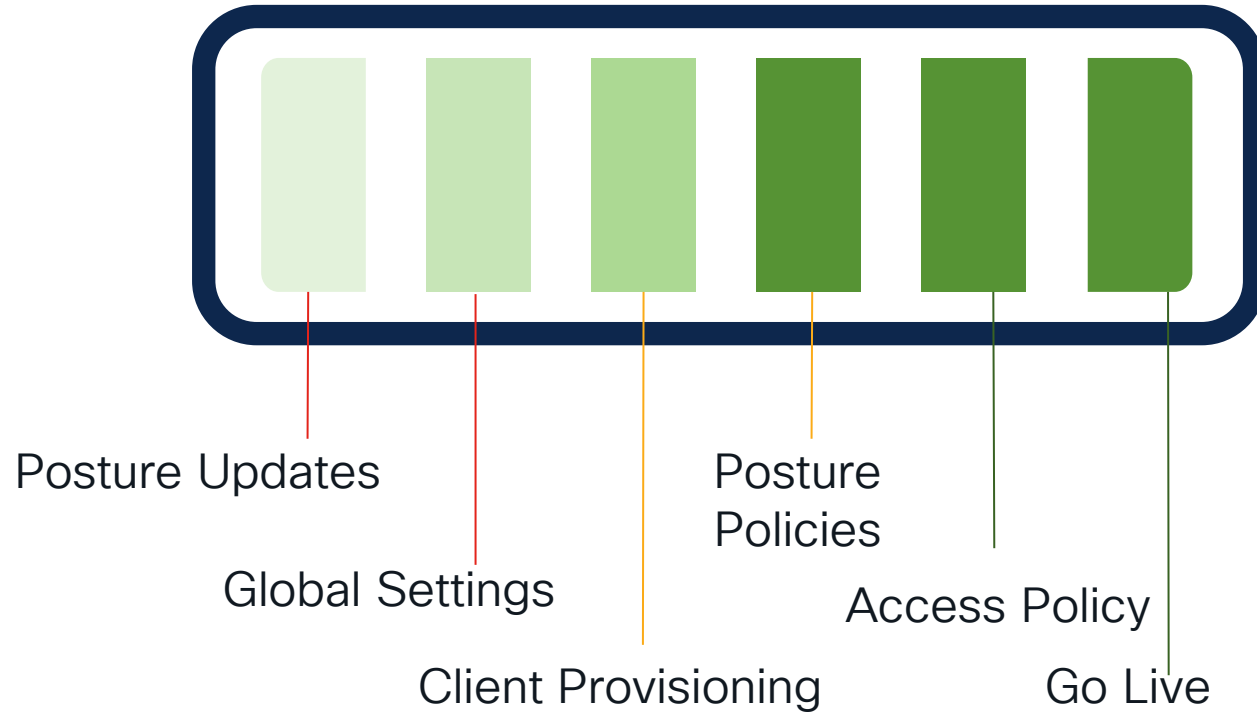# Posture with pre-installed Agent (no-profile)

- 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
<?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>
```
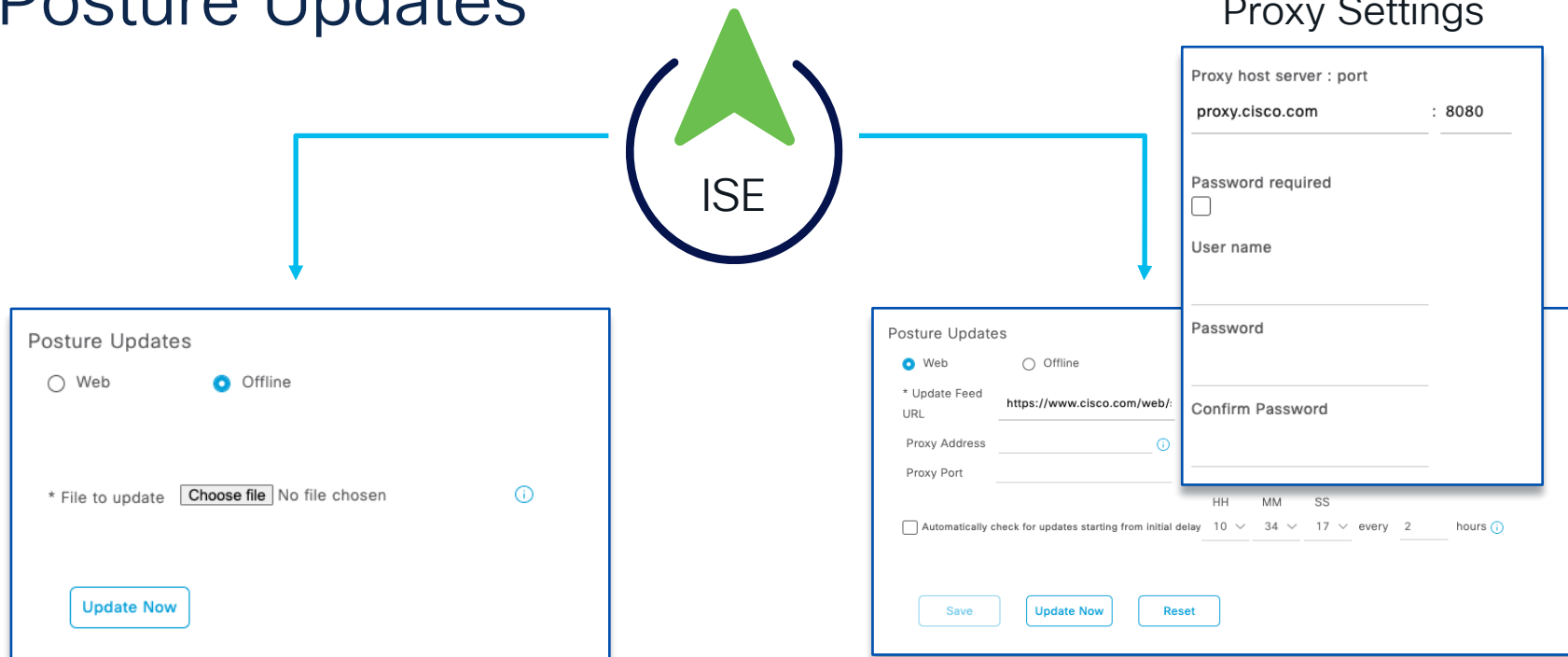
ConnectionData.xml

ISE Posture Journey

ISE Posture Journey

Posture Updates

Global Settings

Client Provisioning

Posture Policies

Access Policy

Go Live

ISE Posture Journey: Posture Updates

Posture Updates

Posture Updates

ISE

Proxy Settings

Proxy host server : port

proxy.cisco.com : 8080

Password required
☐

User name
_____

Password
_____

Confirm Password
_____

Posture Updates

○ Web   ● Offline

* File to update [Choose file] No file chosen   ⓘ

[Update Now]

Posture Updates

● Web   ○ Offline

* Update Feed URL   https://www.cisco.com/web/

Proxy Address _____ ⓘ

Proxy Port

HH   MM   SS

☐ Automatically check for updates starting from initial delay   10 ⌄   34 ⌄   17 ⌄   every   2   hours ⓘ

[Save]   [Update Now]   [Reset]

⚠ Deleted default posture elements are not created again during next updates

ISE Posture Journey: Global Settings

Posture Updates
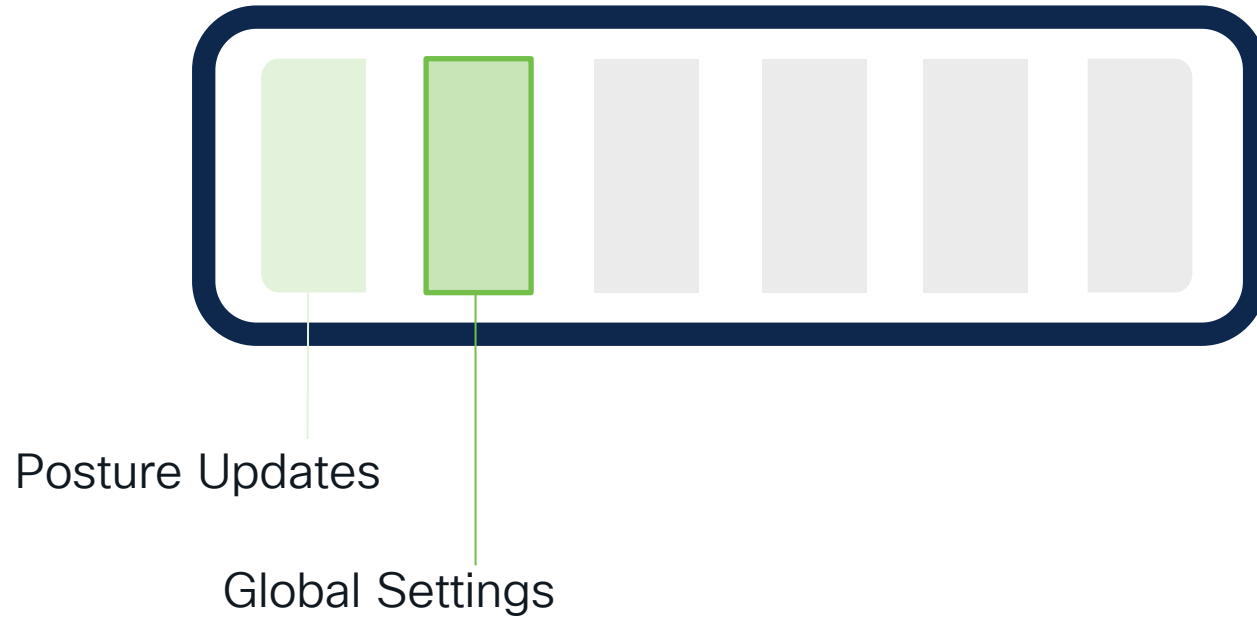
Global Settings

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 `1` Days ⓘ

☑ Cache Last Known Posture Compliant Status

Last Known Posture Compliant State `31` Days ⌄

☐ 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.
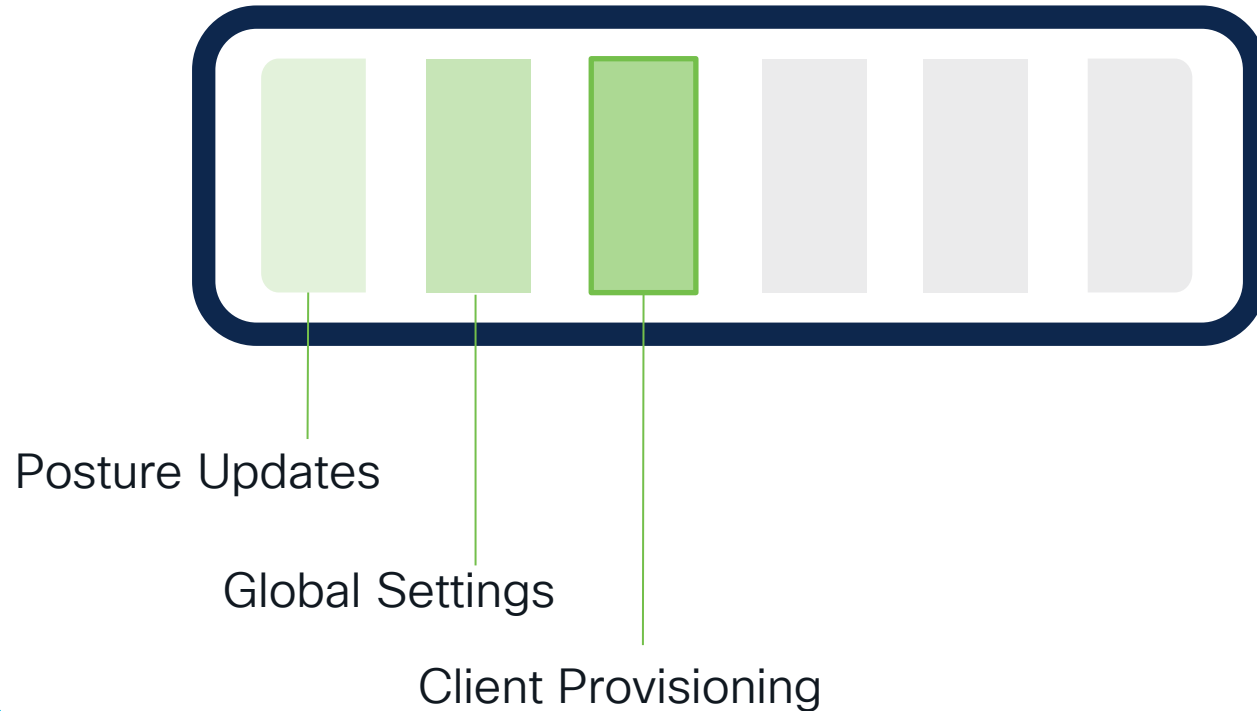
Agentless Plugin

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 `1` Minutes ⓘ
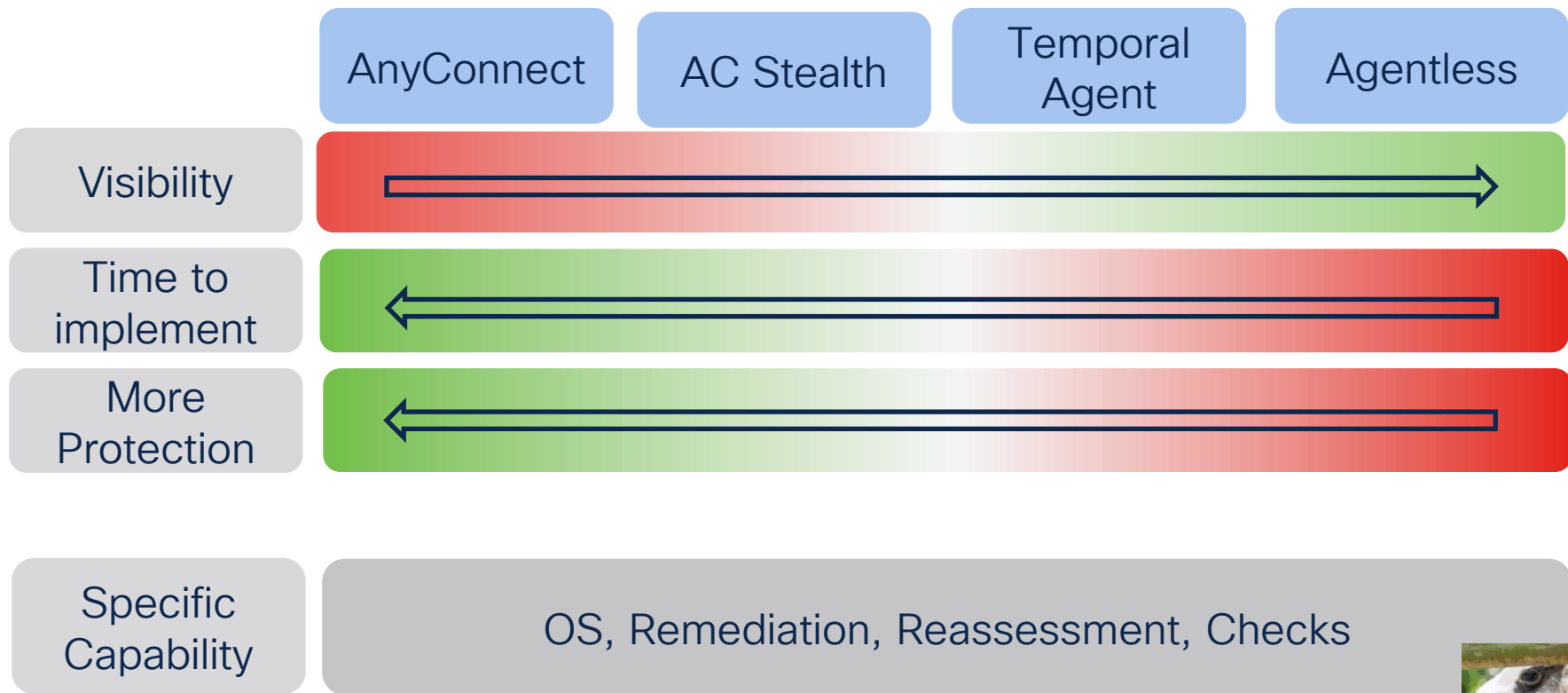
☐ Remove Agentless Plugin after each run

ISE Posture Journey: Client Provisioning

Posture Updates

Global Settings

Client Provisioning

ISE Posture: Agent types

AnyConnect

Agentless

ISE

Temporal Agent

AnyConnect Stealth

Which agent you need ?

AnyConnect	AC Stealth	Temporal Agent	Agentless

Visibility	→

Time to implement	←

More Protection	←

Specific Capability	OS, Remediation, Reassessment, Checks

Client Provisioning

Resources $\longrightarrow$ AnyConnect Profile $\longrightarrow$ Client Provisioning Policy

Resources

✎ Edit   ＋ Add ⌄   ⎘ Duplicate   🗑 Delete

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

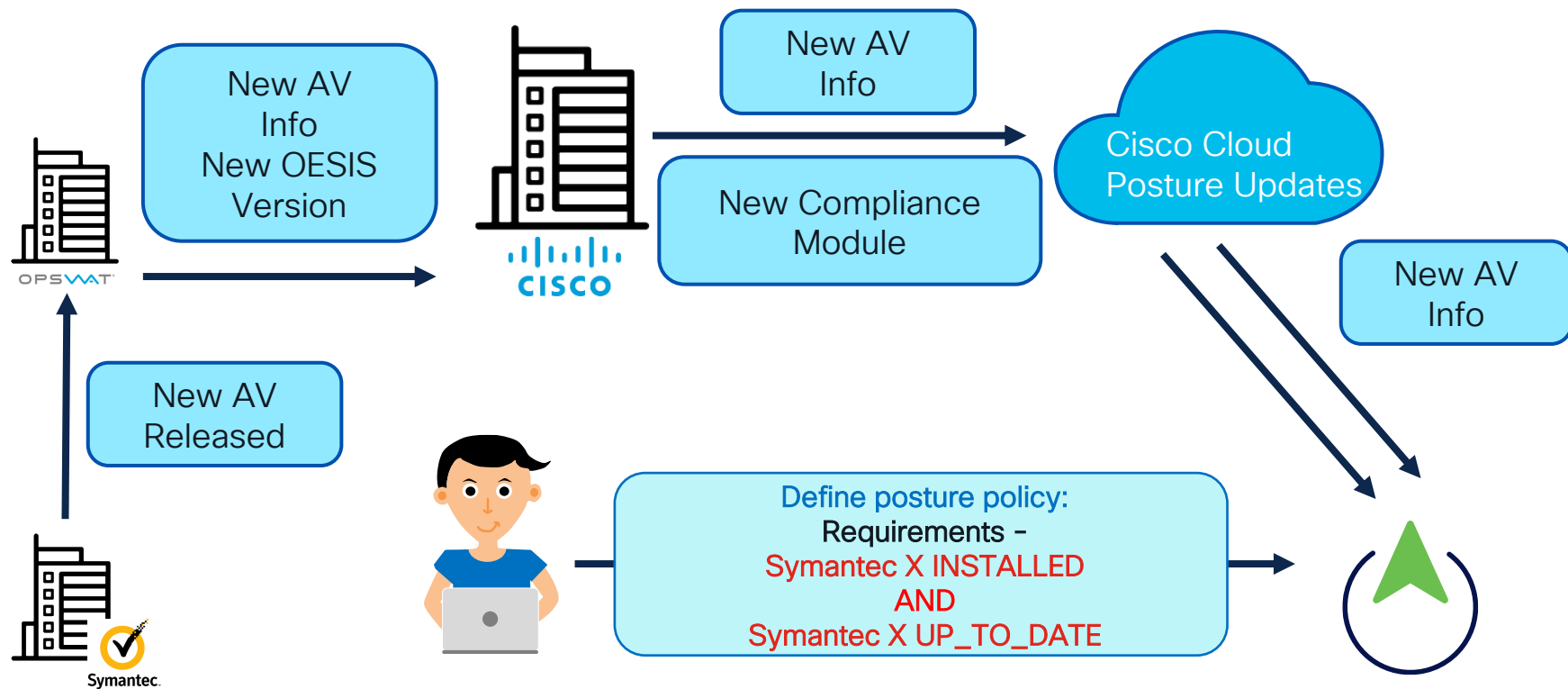**Compliance Module** – Offers the ability to assess an endpoint's compliance.
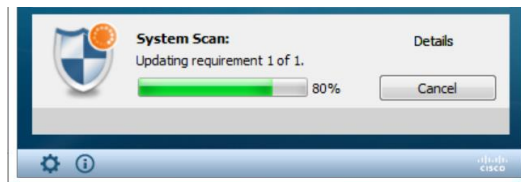
OPSWAT – Cisco Compliance module is using OESIS framework from OPSWAT for detection and remediation
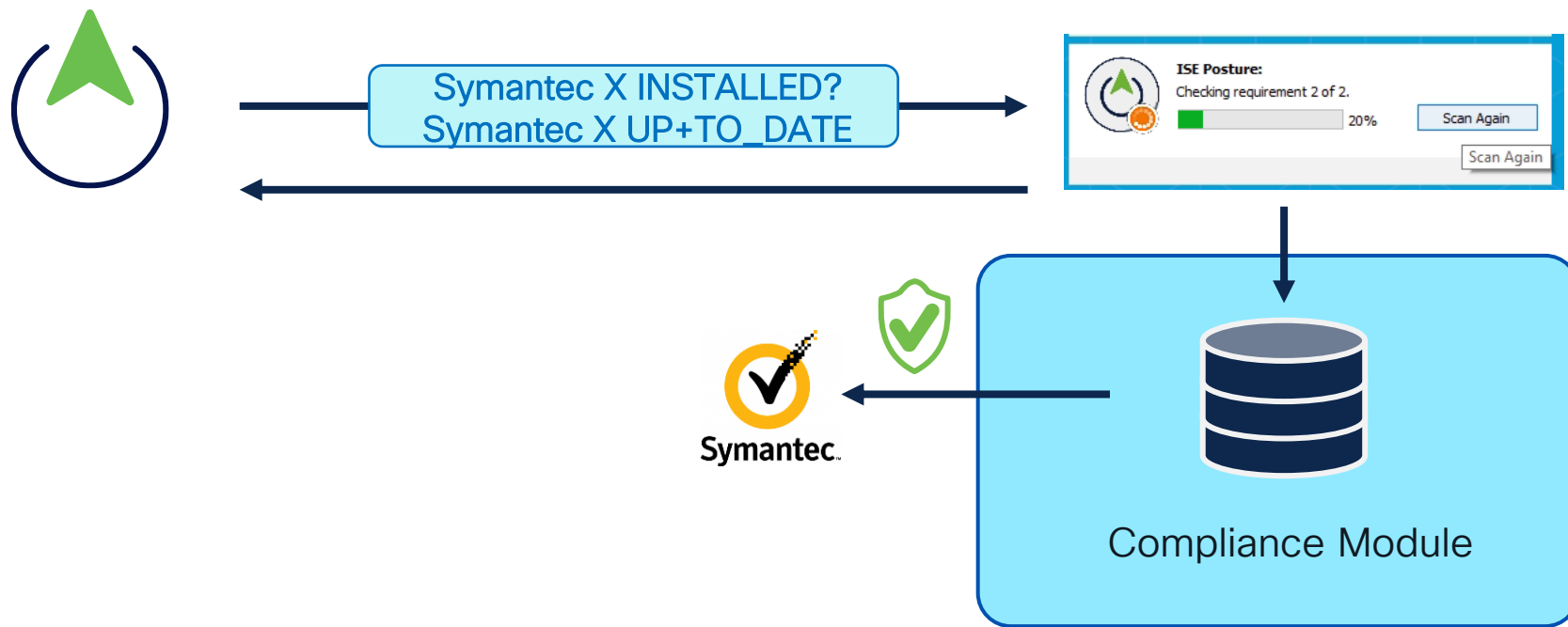
https://www.slideshare.net/OPSWAT/introduction-to-oesis-framework

Let's visualize

Symantec X INSTALLED?
Symantec X UP+TO_DATE

ISE Posture:
Checking requirement 2 of 2.
20% Scan Again
Scan Again

Compliance Module

Compliance module updates vs Posture updates

Compliance Module

DB Application → Actions

Corresponding

Posture Updates

On ISE → Posture Policy

ISE

	Avast Business Security	6.x ⌄	23.x	4.3.3726.6145
	Avast Premium Security	19.x ⌄	23.x	4.3.3726.6145

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: AnyConnectComplianceModuleWindows ⌄

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 ⌄

	Description
Server name rules * (i)	
	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay (i) 60 secs	Time (in seconds) to wait before retrying.
	Number of retries allowed for a message.
Discovery host (i) cisco.com	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.
	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"
Call Home List (i) 10.52.15.80, 10.52.15.81	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.
	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

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   AnyConnectComplianceModuleWindows ⌄

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

Resources $\longrightarrow$ AnyConnect Profile $\longrightarrow$ Client Provisioning Policy

* 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 ☑

Configuration Name

Compliance Module

Modules

Profile AC

Profile Selection

* ISE Posture   AC-Profile ∨

In case of posture over VPN AC cannot be updated if ISE has higher AC pkg version then ASA

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	
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	Cisco-ISE-NSP	Edit ⌄
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	Edit ⌄
☑	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 ⌄
☑	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 ⌄
☑	Chromebook	If	Any	and	Chrome OS All	and	Condition(s)	then	Cisco-ISE-Chrome-NSP	Edit ⌄

Specify the AnyConnect Agent Configuration

ISE Posture Journey: Configuration

Posture Updates

Global Settings

Client Provisioning
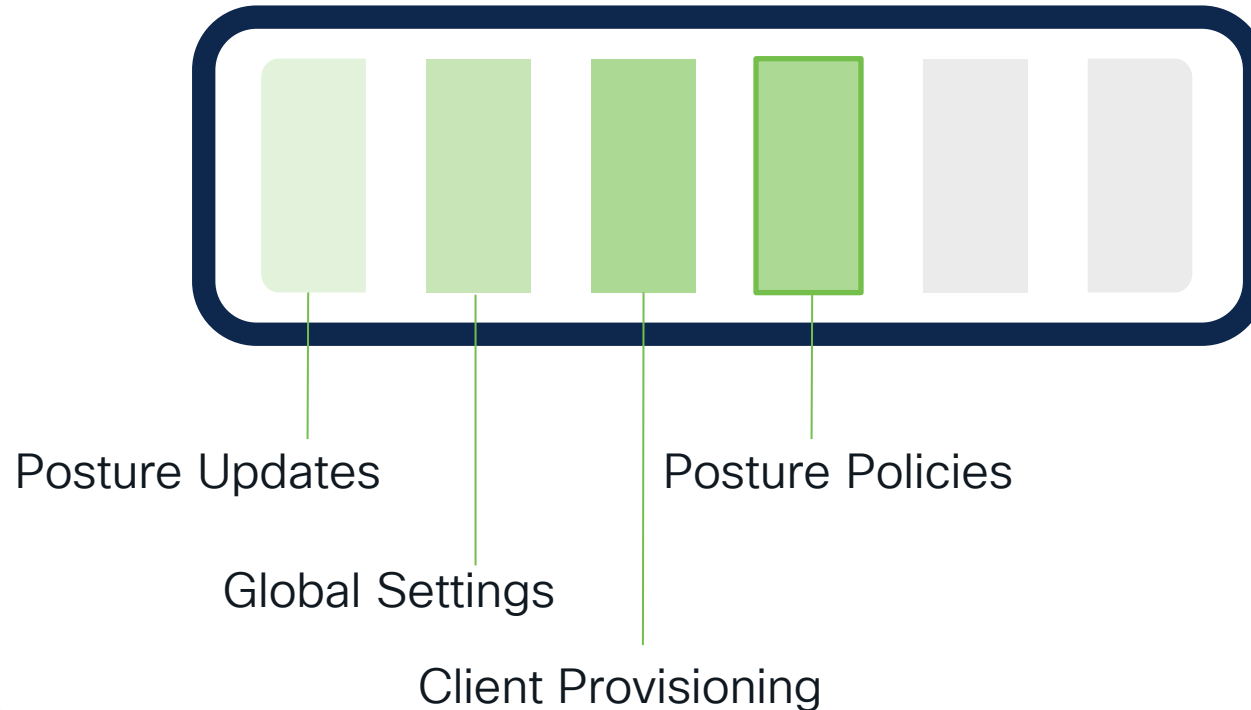
Posture Policies

ISE Posture Checks

Condition + Remediation → Requirement

Conditions

ISE

Remediation

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

ISE Posture Policy

Policy Elements

Policy Sets

Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements	
☐	Policy Options	Default_AntiMalware_Policy_Mac	If	Any	and	Mac OSX	and	4.x or later	and	Agent	and		then	Any_AM_Installation_Mac	Edit ⌄
☐	Policy Options	Default_AntiMalware_Policy_Mac_temporal	If	Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and		then	Any_AM_Installation_Mac_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

☰Q

< 🔳

Any_AM_Definition_Mac

Any_AM_Installation_Mac

Any_AM_Installation_Mac

Default_AppVis_Requirement_Mac

Default_Firewall_Requirement_Mac

Default_Hardware_Attributes_Requirem

Posture Script Condition

New

Dynamic requirements

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

[...]

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

Response

ISE

ps1   sh

Script Push
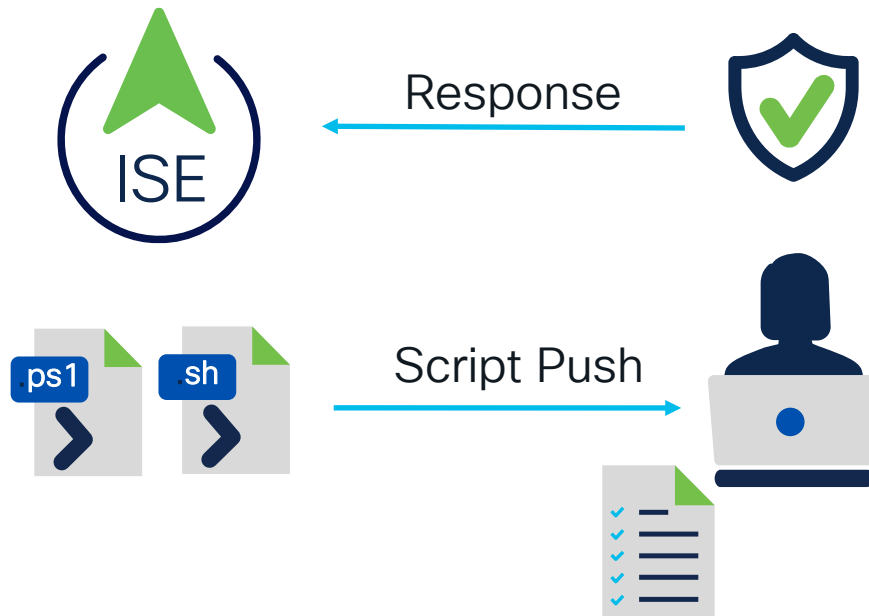
Posture Script Condition – Prerequisites

New

Establish trust

ISE

Local Machine Store

PSN

AnyConnectLocalPolicy.xml

SHA-256
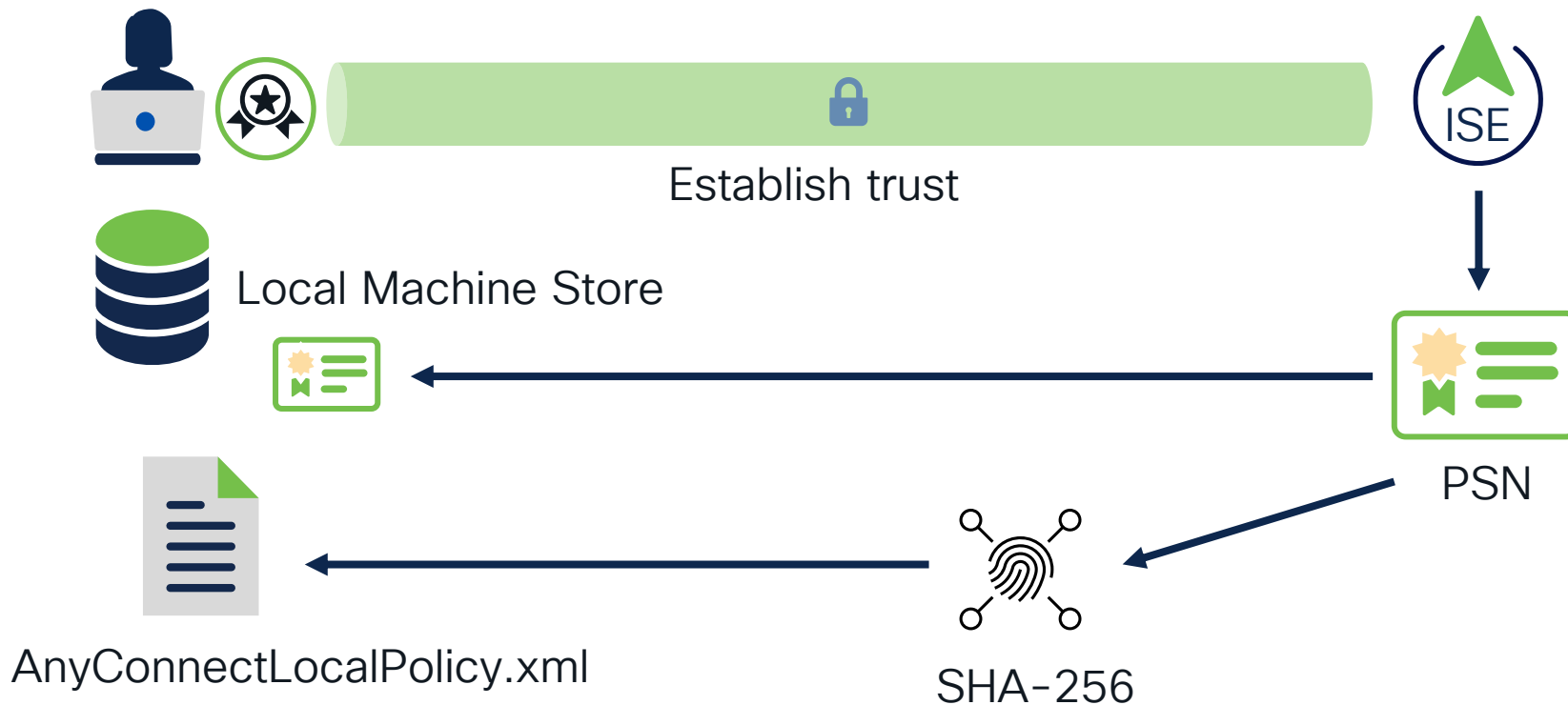
Posture script condition – Script Dowload

New

📄

Elevated privileges ⚠️

🪟 %LOCALAPPDATA%\Cisco\Cisco Anyconnect Secure Mobility Client\scripts

🍎 ~/.cisco/iseposture/scripts

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

🍎 /opt/cisco/anyconnect/iseposture/scripts

Filename match	→	Script file hash match

→ Download the script

→ Reuse the existing script
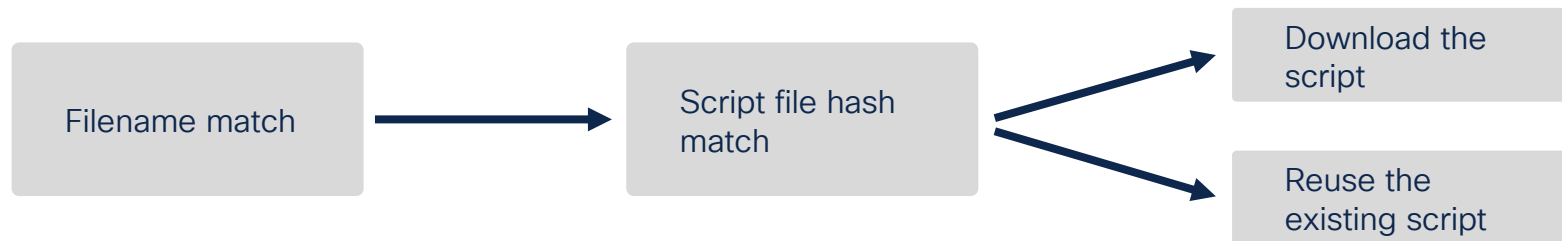
Posture script condition – Exit Code

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

ISE Posture Journey: Access Policy

Posture Updates

Global Settings

Client Provisioning

Posture Policies
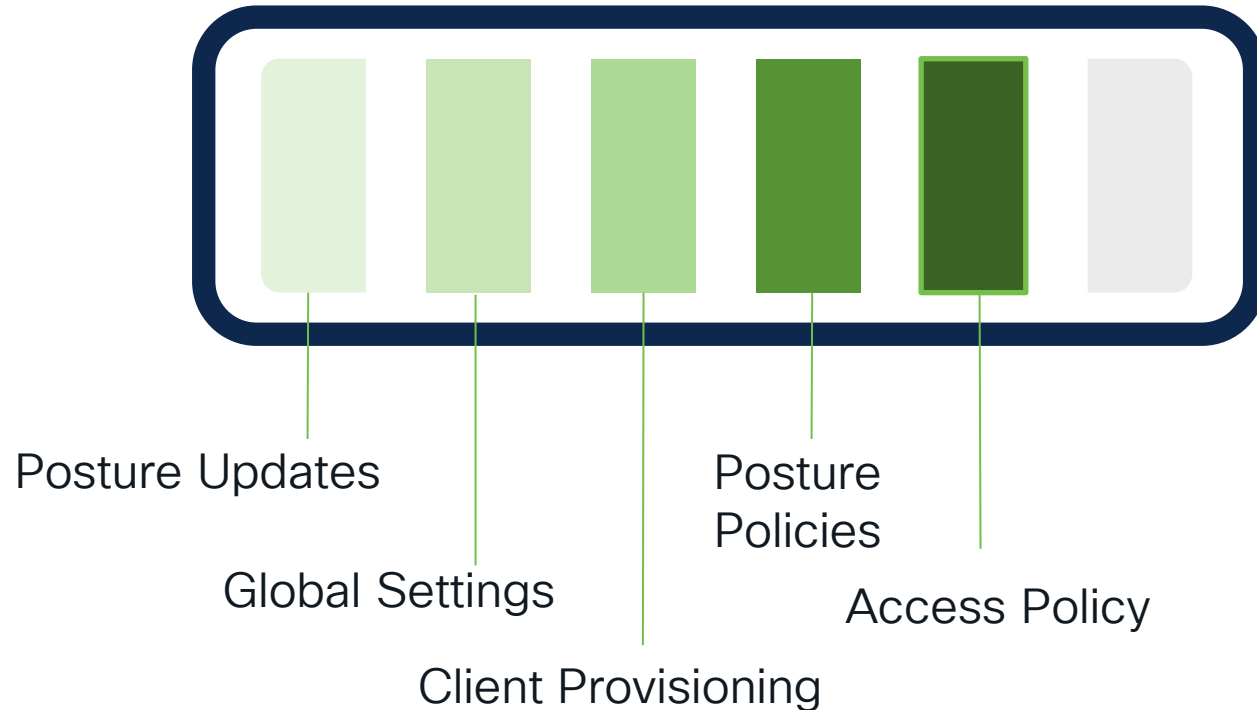
Access Policy

Access Policies – Redirect Chaining

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

Must exists on NAD

ISE Posture Journey: Time to Go Live

Posture Updates

Global Settings

Client Provisioning

Posture Policies

Access Policy

Go Live
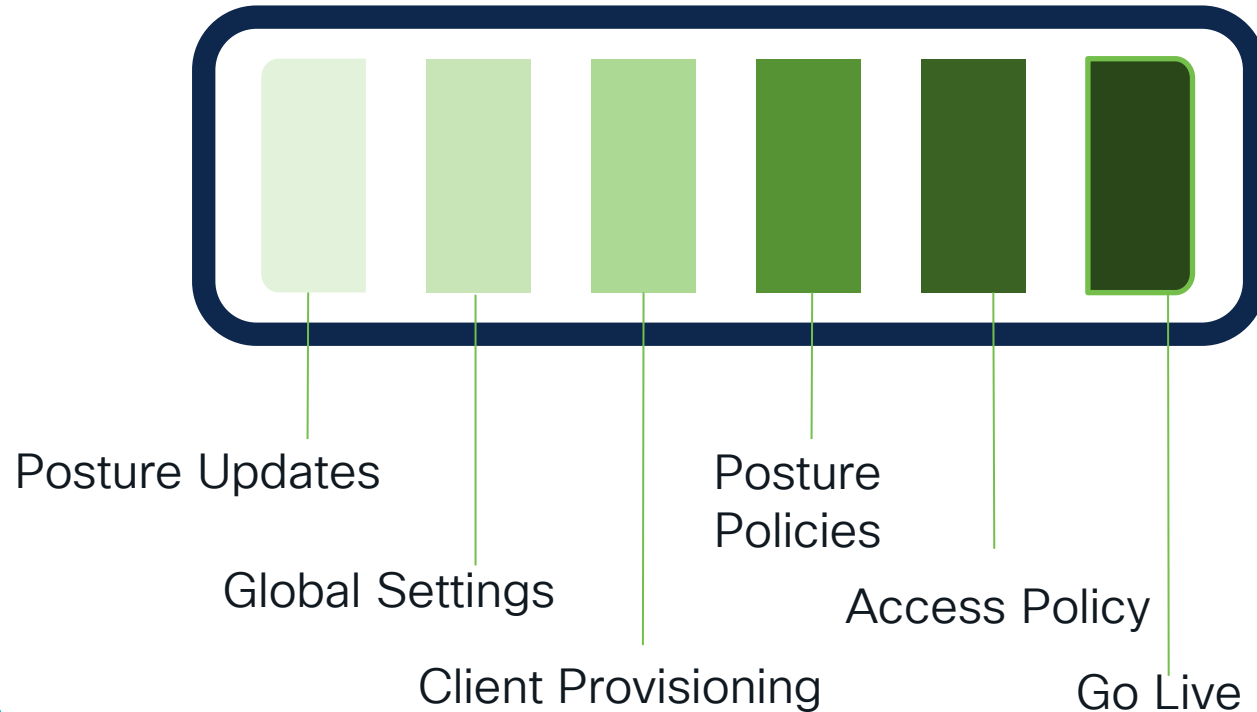
Advanced Posture Processes
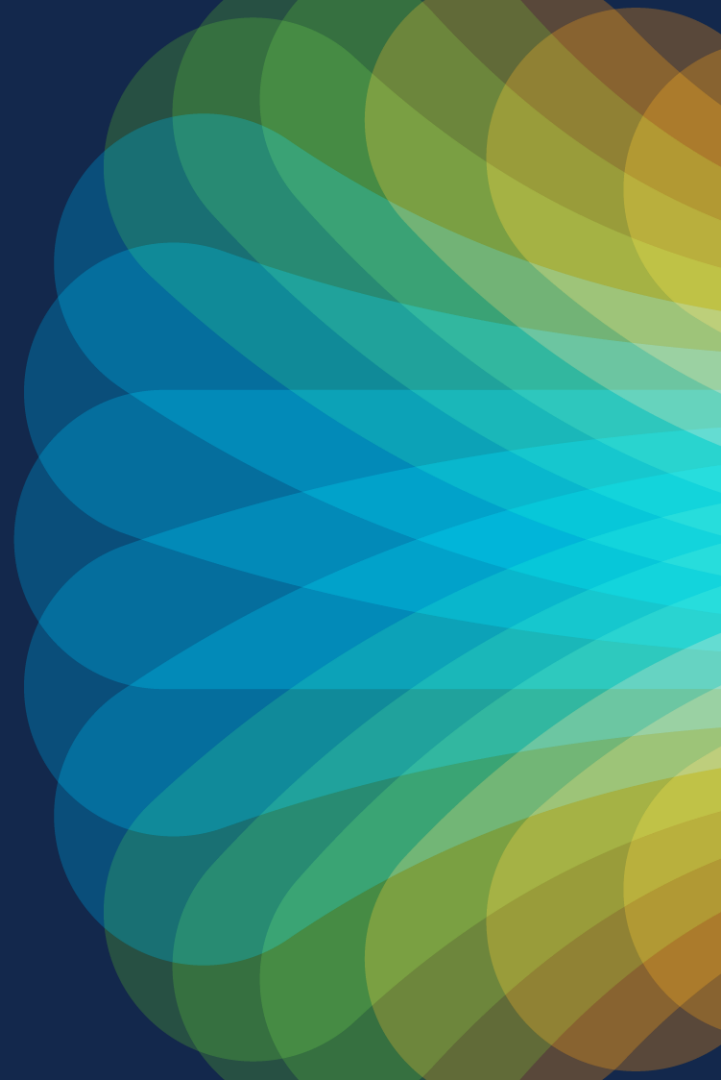
Session Sharing

"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 ?

ⓘ 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:

Syslog – Authentication Passed
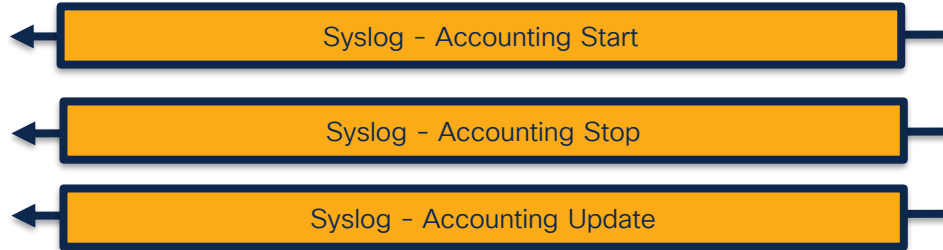
MNT

Sessions are updated:

Syslog – Accounting Start

Syslog – Accounting Stop

Syslog – Accounting Update

PSN

Session management – theory walkthrough

Who is responsible for session management in ISE deployment?

PSN

Sessions are created

Access-Accept

Accounting Update

Sessions are updated

Accounting Start

Accounting Update
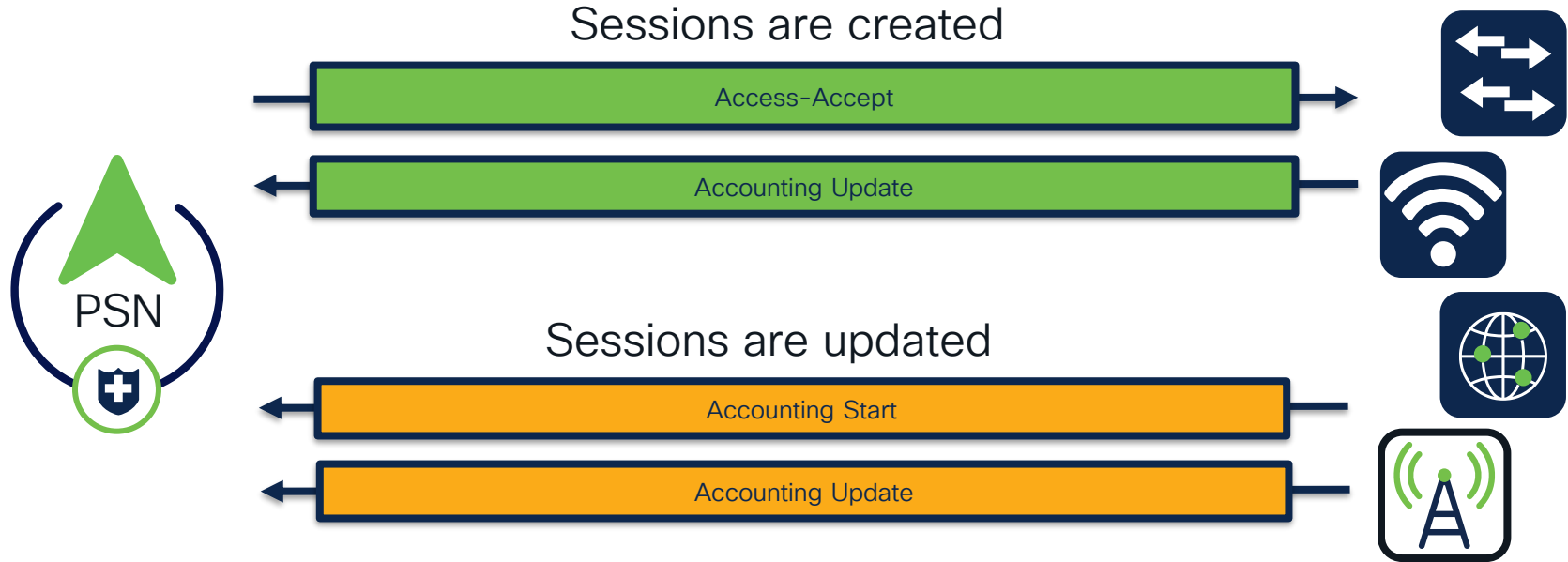
Node Group

Main idea behind is to minimize amount of global replication events

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

PSN session chance

Session-ID Session-Attributes
ABC {alice,MAC,IP, redirect-url=psn1}

PSN

MNT

Session-ID ABC
Status – Started
redirect-url=psn1

Node Group members monitor each other

COA Terminate

PSN

In case of outage all sessions in redirect state are downloaded from MNT

Live Sessions
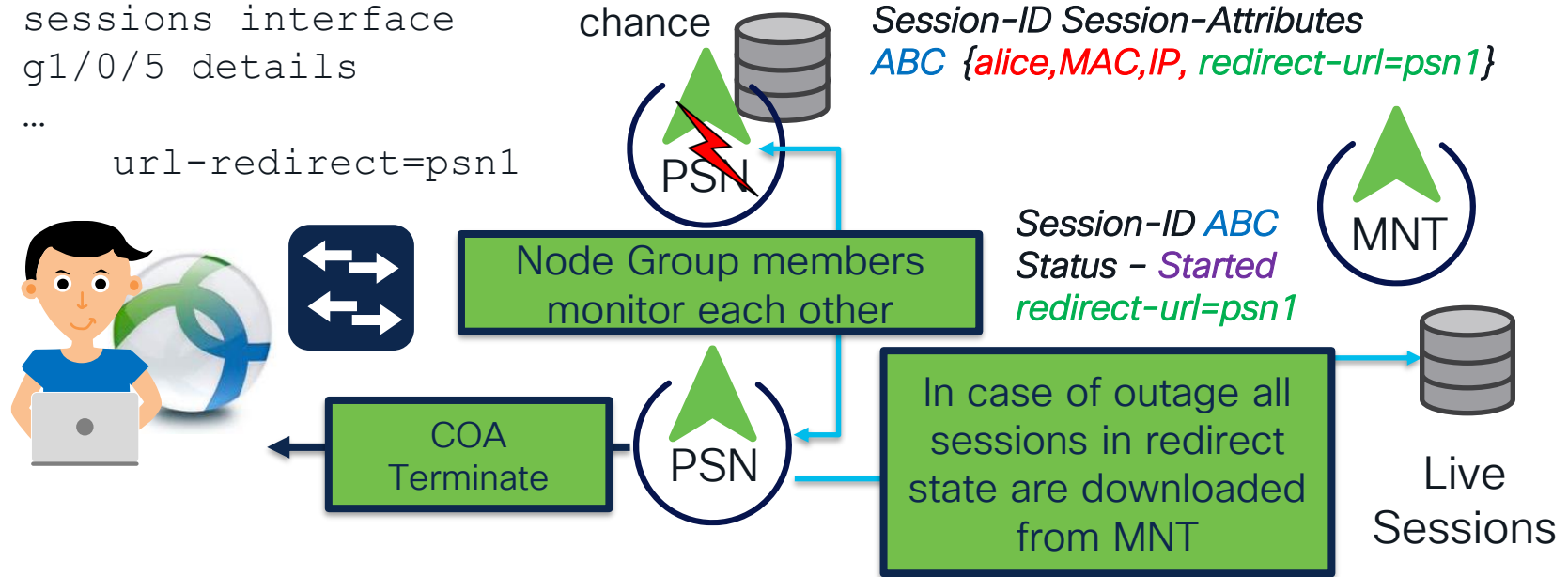
Light session directory (LSD) AKA Light Data Distribution (LDD)

PSN Session Cache

LSD Cache

Initial authentication

PSN

Limited list of attributes added to LSD

Session-ID *ABC*
Attributes{*alice,MAC,IP,*}

RabbitMQ Channel

PSN Session Cache

Accounting Interim update with Device Sensor Info

PSN

Session-ID *ABC*
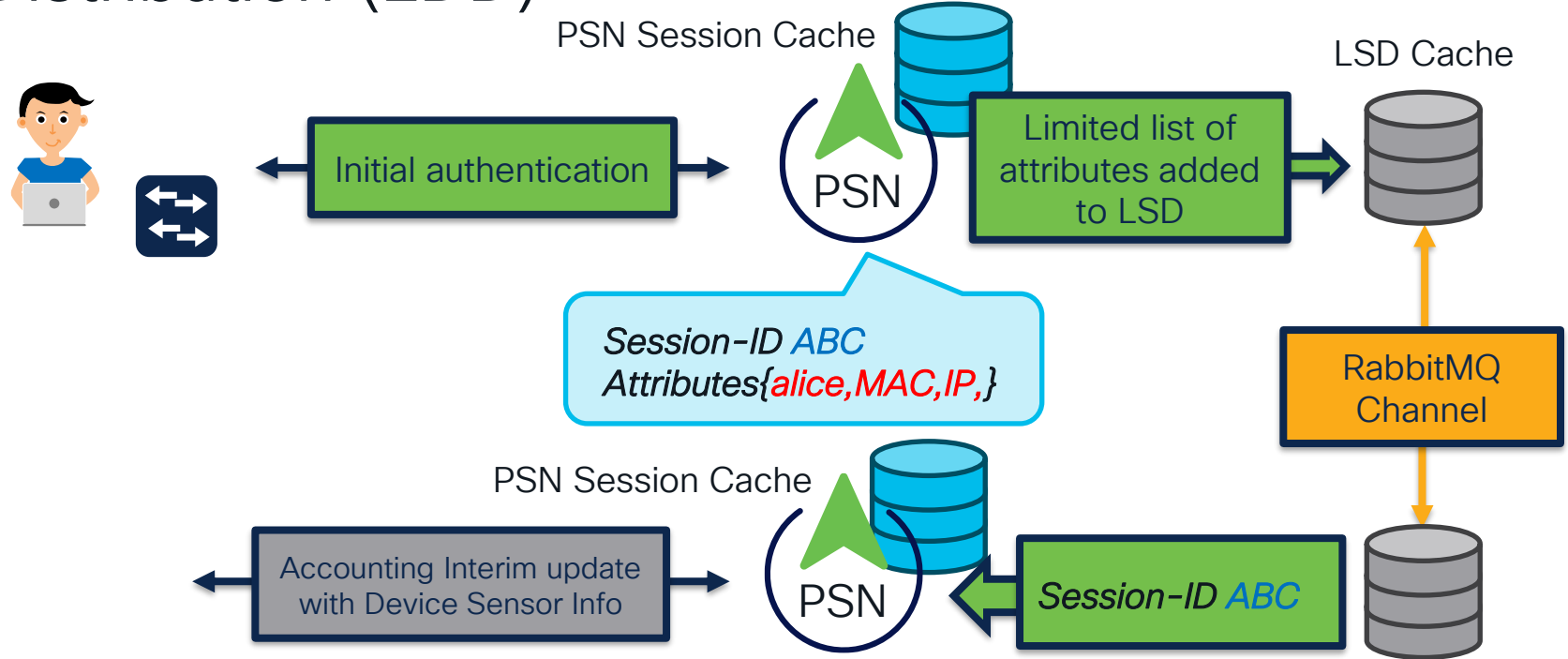
How Light Data Distribution (LDD) solve posture problems
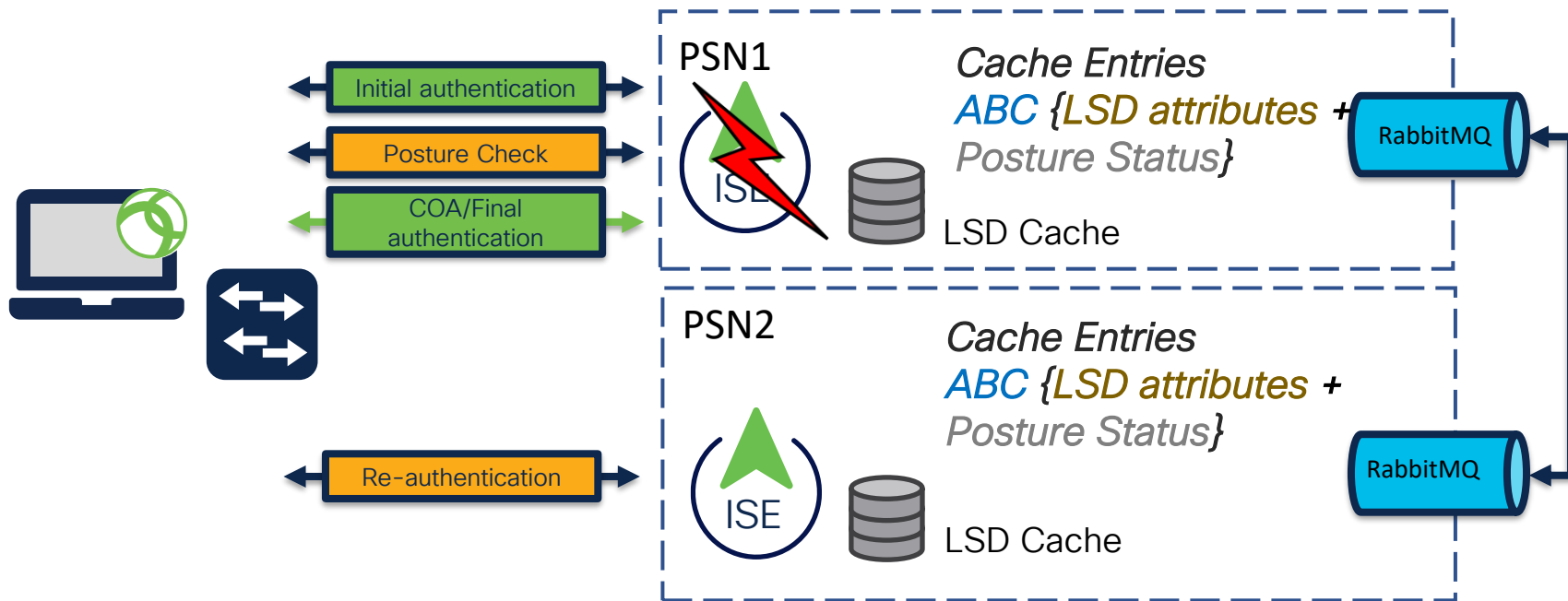
How Light Data Distribution (LDD) solve posture problems
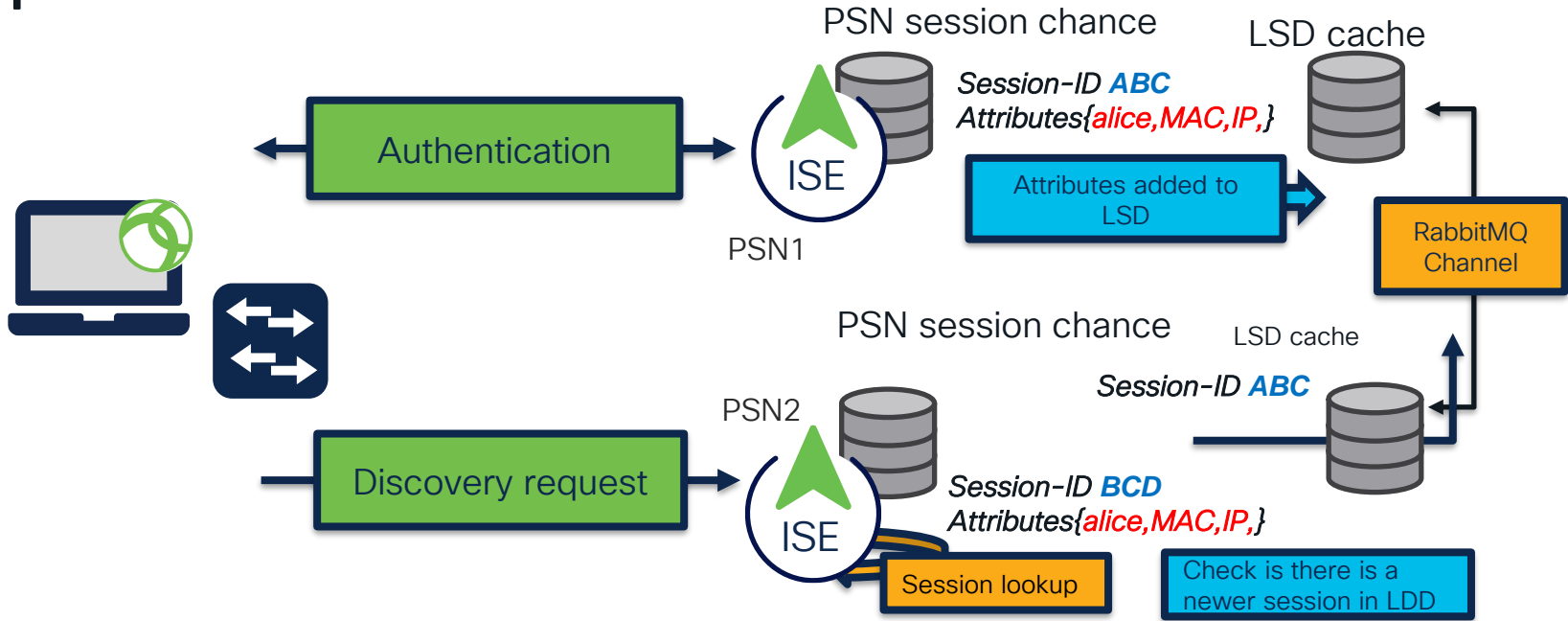
Demo – Node Group and Phantom Session

https://ciscolive-ise1.demo.local:8443/portal/PortalSetup.action?portal=40f01bd0-2e02-11e8-ba71-00: | Search

CISCO Client Provisioning Portal

Device Security Check

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

Start

Cisco AnyConnect Secure Mobility Client

VPN:
Use a browser to gain access.

Connect

Web Authentication Required

System Scan:
Compliant.
Network access allowed.

Cisco AnyConn

Posture Status Sharing over RSD – PSN Failover

alice@lab.com	D4:C9:3C:52:6F:...	10.52.14.186	SW-1-LAB	Compliant	⋮	ise-p	ISE-PSN2
alice@lab.com	D4:C9:3C:52:6F:...	10.52.14.186	SW-1-LAB	Compliant	⋮	ise-s	
#ACSACL#-IP-...			SW-1-LAB		⋮	ise-s	
alice@lab.com	D4:C9:3C:52:6F:...	10.52.14.186	SW-1-LAB	Compliant	⋮	ise-s	ISE-PSN1

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
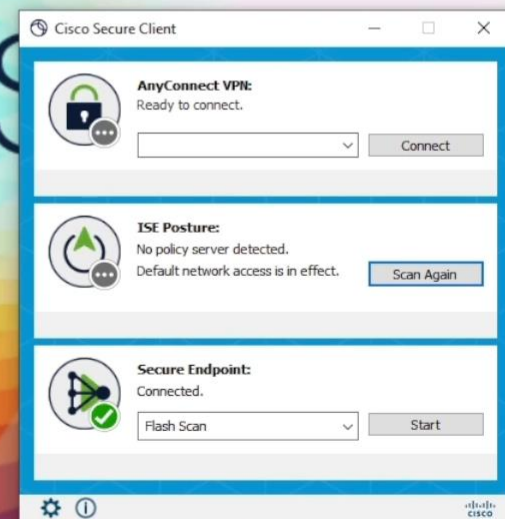
Posture Discovery and Authentication

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

Demo – Identification

Discovery

Power Events

User Login
alice
*****

Initial AC Installation

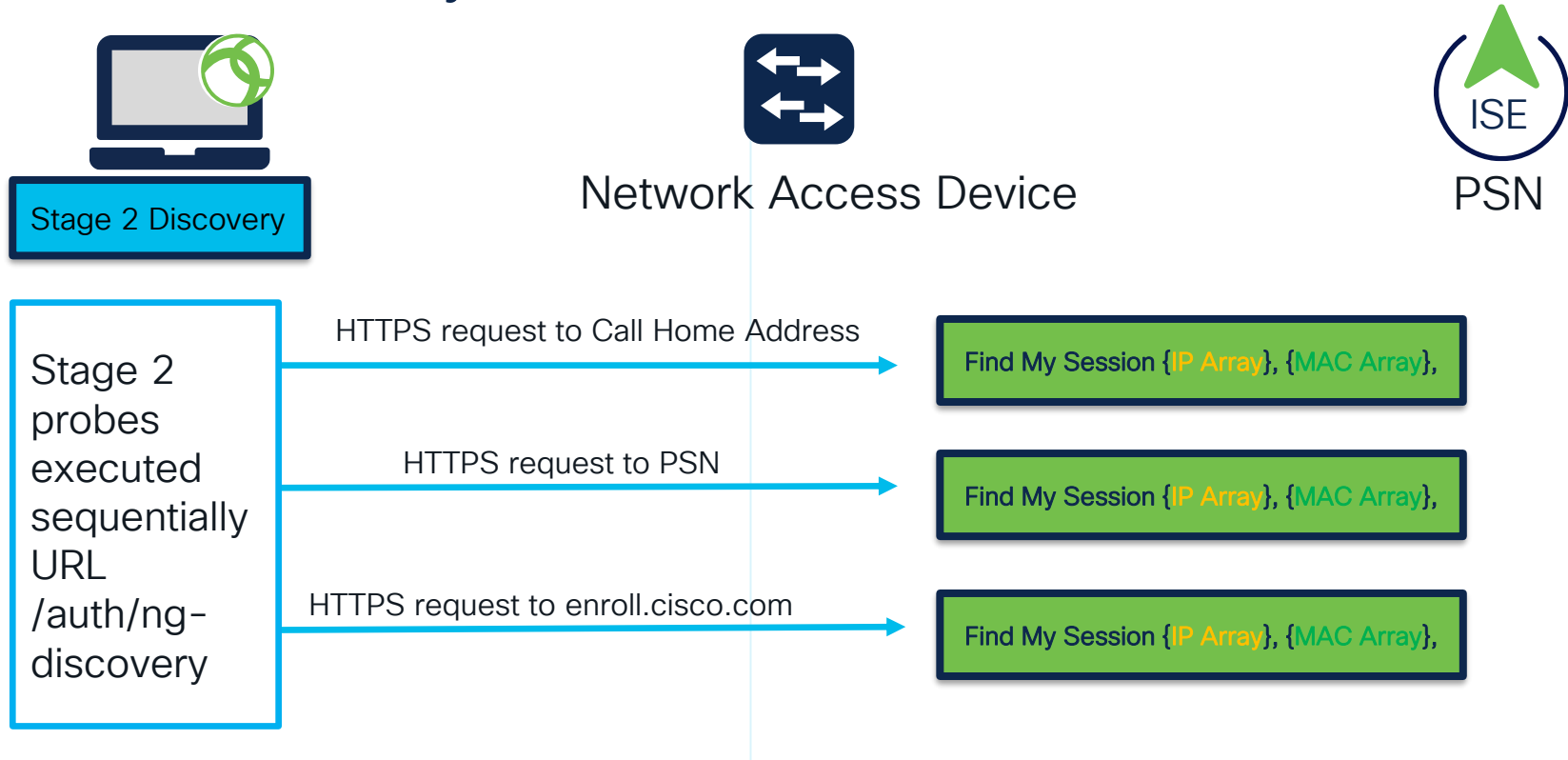Return sleep

Default GW change

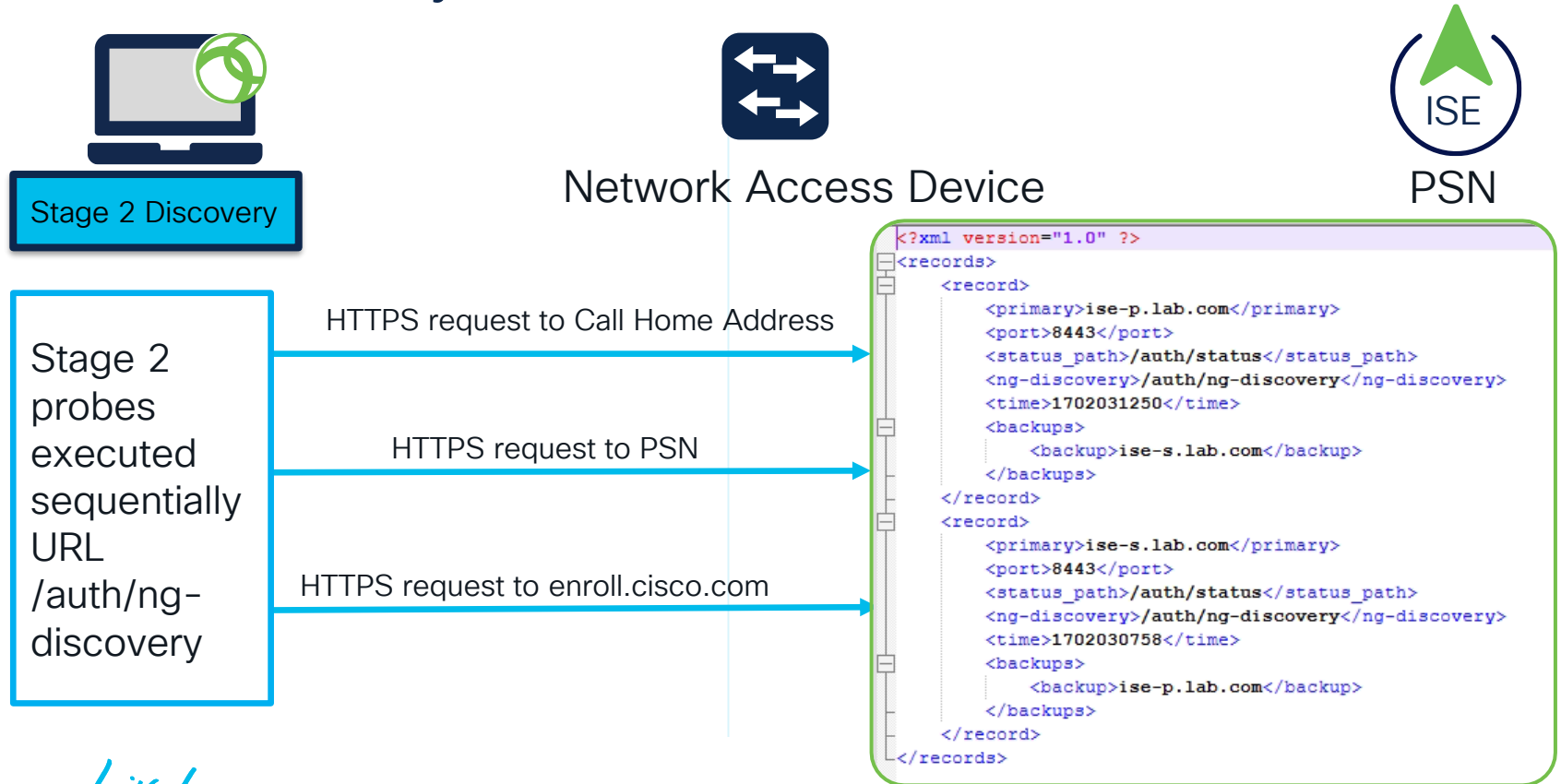Interface Up

PSN discovery Redirect flow

Stage 1 Discovery

Network Access Device

ISE
PSN

One Stage 1 cycle is limited to 5 seconds

HTTP Get to Discovery Host (IF available)

HTTP Get to enroll.cisco.com

HTTP Get to Default GW IP

HTTPS request to PSN

Find My Session {IP Array}, {MAC Array},

Session lookup in Local PSN cache (IP/MAC based)

Session lookup on MNT cache (MAC only)

CISCO *Live!*

PSN discovery Redirect flow

Stage 1 Discovery

One Stage 1 cycle is limited to 5 seconds

HTTP G

HTTP

HTTP

HT

PSN

ISE

```xml
<?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>
```

Array},

Session lookup in Local PSN cache (IP/MAC based)

Session lookup on MNT cache (MAC only)

CISCO Live!

PSN discovery Redirect flow

Stage 1 Discovery

Network Access Device

ISE
PSN

One Stage 1 cycle is limited to 5 seconds

HTTP Get to Discovery Host (IF available)

HTTP Get to enroll.cisco.com

HTTP Get to Default GW IP

HTTPS request to PSN

Find My Session {IP Array}, {MAC Array},

Session lookup in Local PSN cache (IP/MAC based)

Session lookup on MNT cache (MAC only)

```xml
<?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

PSN discovery Non-redirect based flow

Stage 2 Discovery

Network Access Device

ISE
PSN

Stage 2 probes executed sequentially URL /auth/ng-discovery

HTTPS request to Call Home Address

Find My Session {IP Array}, {MAC Array},

HTTPS request to PSN

Find My Session {IP Array}, {MAC Array},

HTTPS request to enroll.cisco.com

Find My Session {IP Array}, {MAC Array},

PSN discovery Non-redirect based flow

Stage 2 Discovery

Network Access Device

ISE
PSN

Stage 2 probes executed sequentially URL /auth/ng-discovery

HTTPS request to Call Home Address →

HTTPS request to PSN →

HTTPS request to enroll.cisco.com →

```xml
<?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>
```

PSN discovery Non-redirect based flow

Stage 2 Discovery

Network Access Device

ISE
PSN

Stage 2 probes executed sequentially URL /auth/ng-discovery

HTTPS request to Call Home Address

Find My Session {IP Array}, {MAC Array},

HTTPS request to PSN

Find My Session {IP Array}, {MAC Array},

HTTPS request to enroll.cisco.com

Find My Session {IP Array}, {MAC Array},

Misconception n. 3: Compliant State ISE vs Secure Client

AnyConnect Compliant State

"*Secure Client is aware of its Compliant State on ISE*"

The problematic scenario

L2 Change

ISE

AnyConnect VPN:
Ready to connect.

Connect

ISE Posture:
Compliant.
Network access allowed.

Scan Again

Posture Status = Posture Pending

Bidirectional Posture

Secure Client/AnyConnect will probe ISE if in Compliant state

Port 8449

Or
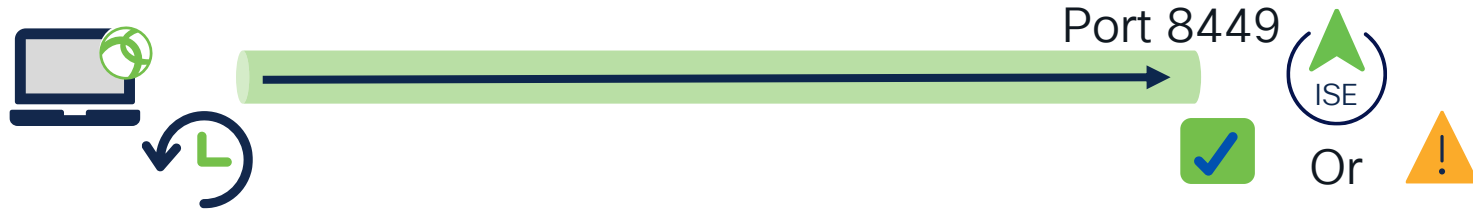
Anyconnect 4.10+

ISE 3.1+

Bidirectional Posture – Correct Implementation

DACL deny PSN port 8449 — ISE Compliant

DACL permit PSN port 8449 — ISE Pending
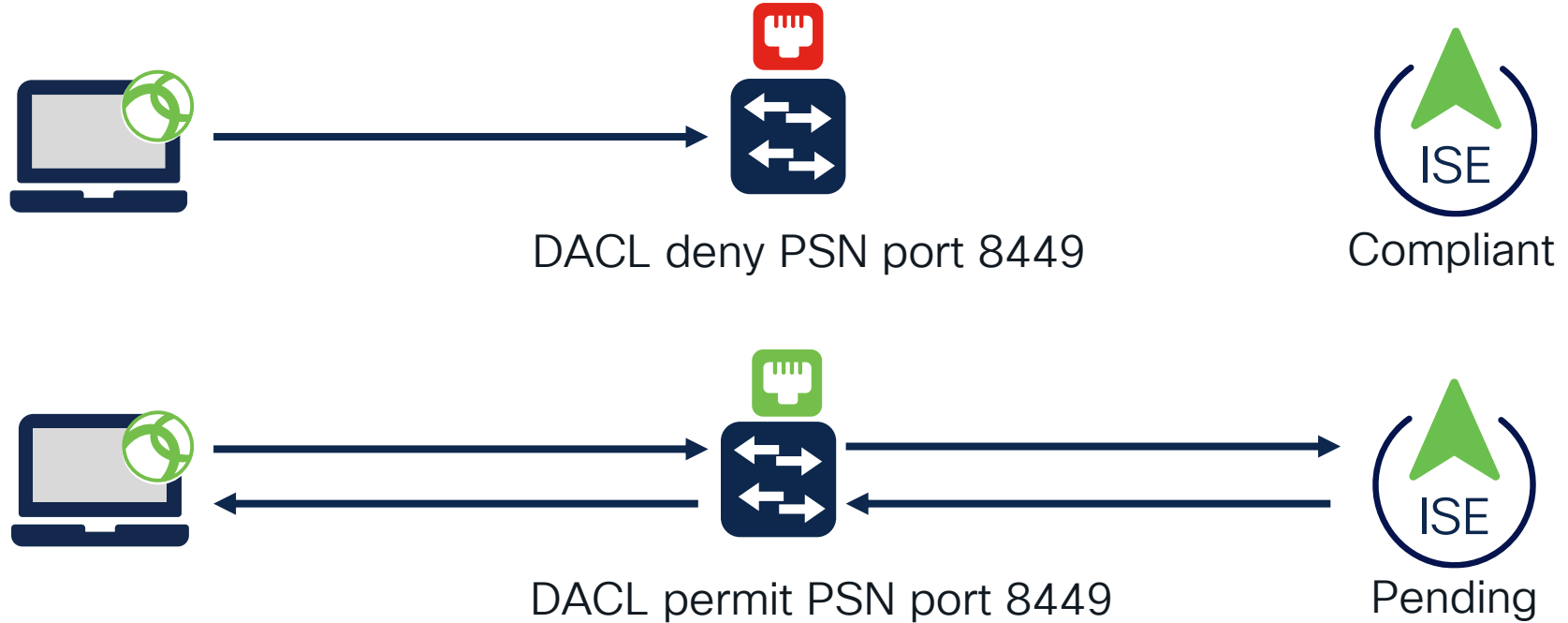
Demo – Bidirectional Posture Configuration

CISCO Live!

Cisco ISE

Overview | Network Devices | **Client Provisioning** | Policy Elements | Posture Policy | Policy Sets | Troubleshoot | More ∨

Client Provisioning Policy

Resources

Client Provisioning Portal

Resources

Selected 0 Total 12

✎ Edit   ╋ Add ∨   ⧉ Duplicate   🗑 Delete

All ∨   ⛛

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

CISCO *Live!*

Posture and MFA

Possible scenarios:

1. Posture over VPN with ASA or FTD when DUO proxy is used

2. Posture over VPN with ASA configured for SAML authentication on DUO Access Gateway (DAG)

3. Posture on dot1x media with DUO proxy
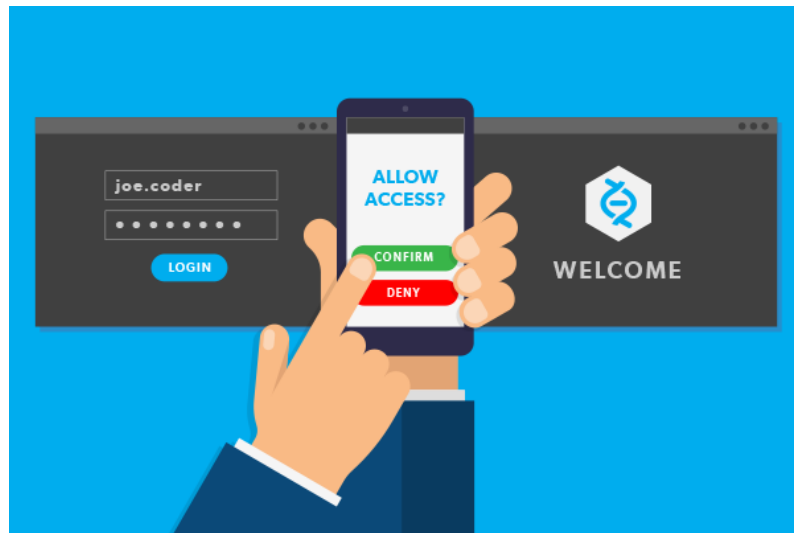
Posture and MFA – VPN with DUO proxy (flow)

VPN Authentication

Radius
Access-Request

LDAP
authentication

Request for second factor

Radius
Access-Accept

Radius
Access-Accept

Allow Access

DUO Push

Accept
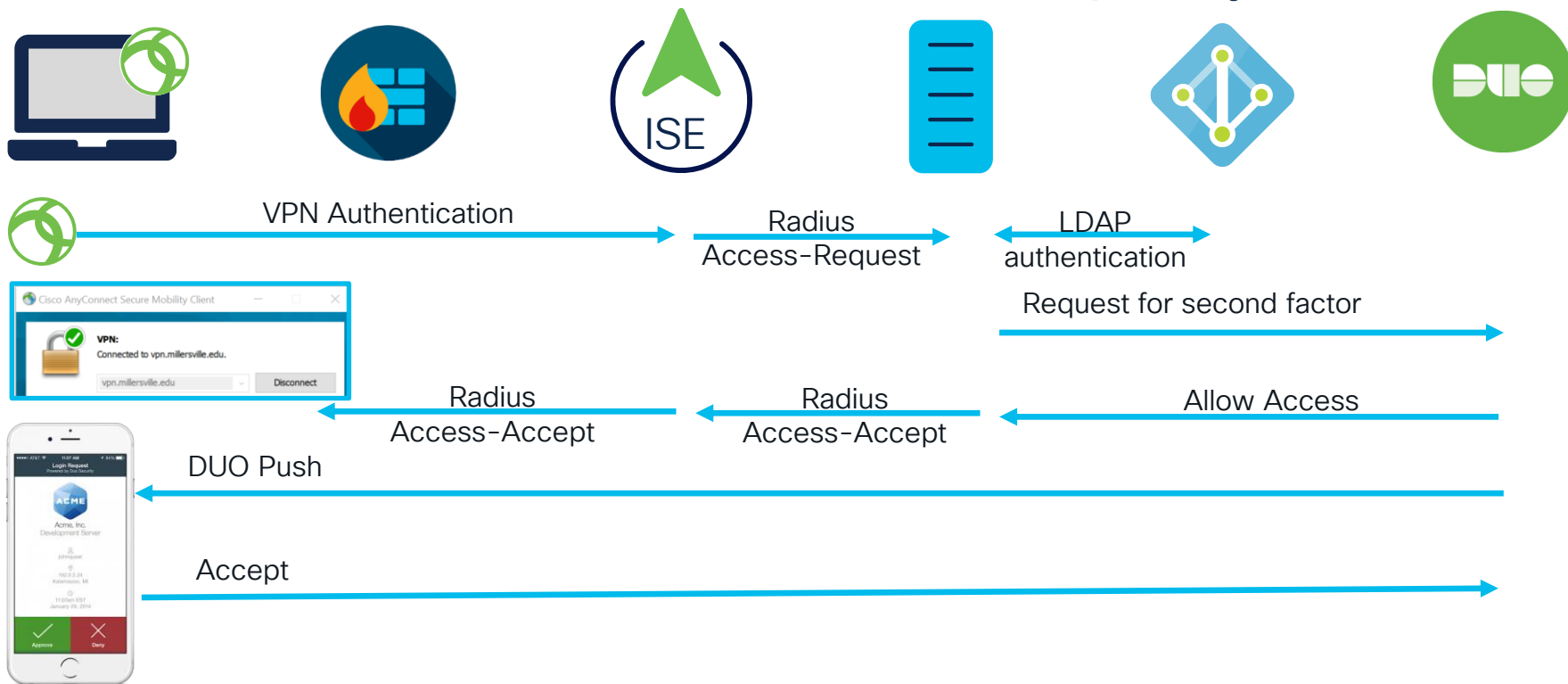
Demo – ISE Configuration

Remote-Access-VPN

Enter Description

Save   Cancel

Policy Assignments (1)

Local Realm: None   Dynamic Access Policy: None

Connection Profile   Access Interfaces   Advanced

Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	🖼 DfltGrpPolicy	✏ 🗑
Remote-Access-VPN	Authentication: ISE_Radius (RADIUS) Authorization: ISE_Radius (RADIUS) Accounting: ISE_Radius (RADIUS)	🖼 DfltGrpPolicy	✏ 🗑

ASA Configured for SAML with SSO

Demo

Protect an Application

i	Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others. Documentation: Getting Started ⧉ **Choose an application below to get started.**

asa

Application	Protection Type
⚙ **Asana**	2FA with SSO hosted by Duo (Single Sign-On)
⚙ **Cisco ASA**	2FA with SSO hosted by Duo (Single Sign-On)
⚙ **Cisco RADIUS VPN**	2FA

Sidebar navigation:

- Dashboard
- Device Insight ⌄
- Policies ⌄
- Applications ⌃
  - Protect an Application
  - Authentication Proxy
- Single Sign-On ⌄
- Users ⌄
- Groups ⌄
- Endpoints ⌄
- 2FA Devices ⌄
- Trusted Endpoints
- Trust Monitor ⌄
- Reports ⌄
- Settings

ISE Posture Troubleshooting Journey

Confirm the theory

Build the theory

NAD Troubleshooting

ISE Troubleshooting

Agent Side Troubleshooting

3rd Party Troubleshooting

Define the Problem
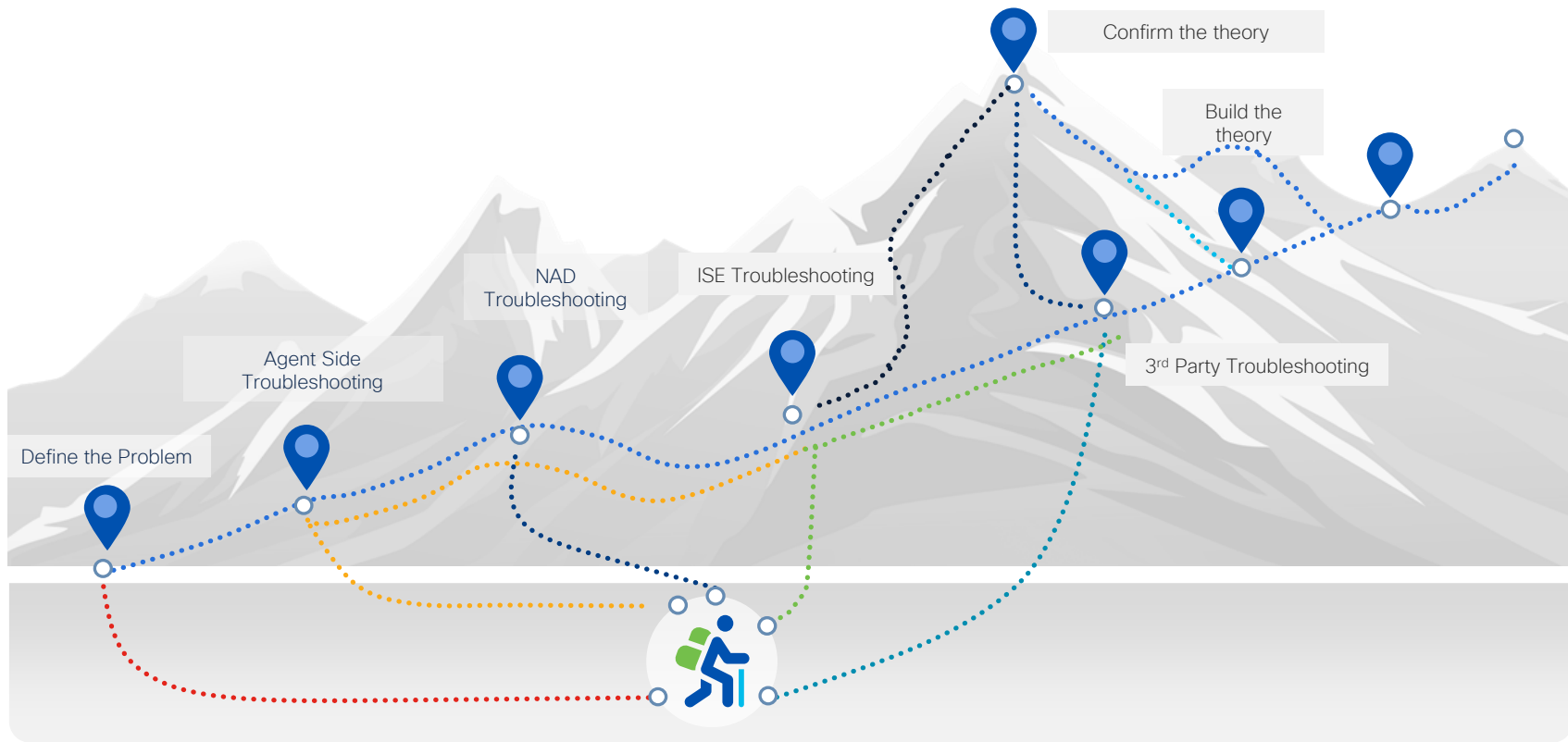
Posture troubleshooting, what to collect

Most commonly needed

Less commonly needed

Laptop (AnyConnect):
- Exact Timestamp
- Screenshots/Recording of user experience
- System Scan Details from AnyConnect
- Packet capture collected when issue manifested
- DART bundle collected after the problem

Switch:
- Status of the authentication session at time of the issue
- Device configuration
- Debugs for Authentication/Accounting and Redirect activities

ISE:
- Live Logs/Detailed authentication reports for affected endpoint
- Radius Authentication/Accounting reports for the affected endpoint
- Client Provisioning Report filtered by endpoint MAC
- Posture Report filtered by endpoint MAC
- Screenshots of related ISE configuration
- Packet capture collected when issue manifested
- Support bundle with posture related components in 'DEBUG'

Learn on Example

No Policy Server Detected

Learn on Example – Failed to launch Downloader
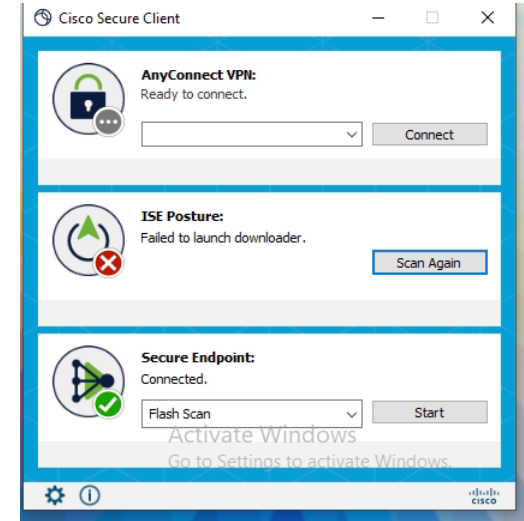
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public
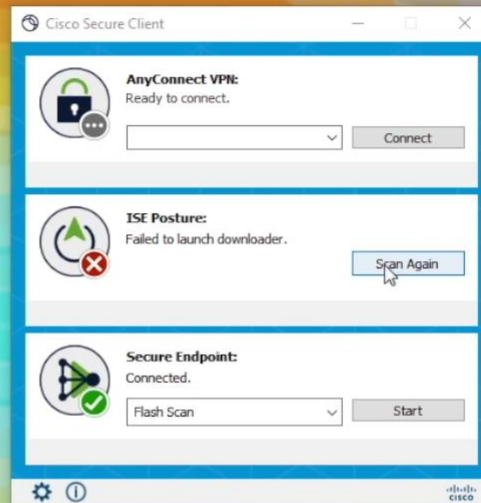
Define the Problem

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

A problem well stated is a problem half solved
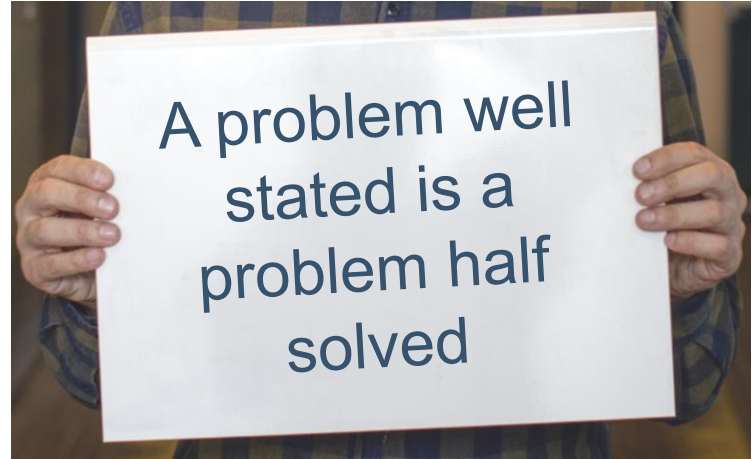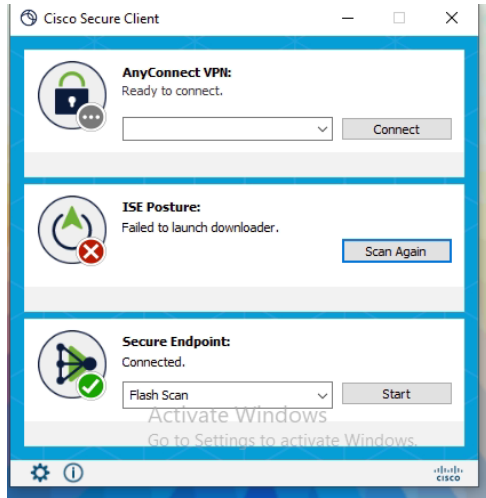
Which is the problematic pillar ?

Agent Side Troubleshooting

System Scan Details
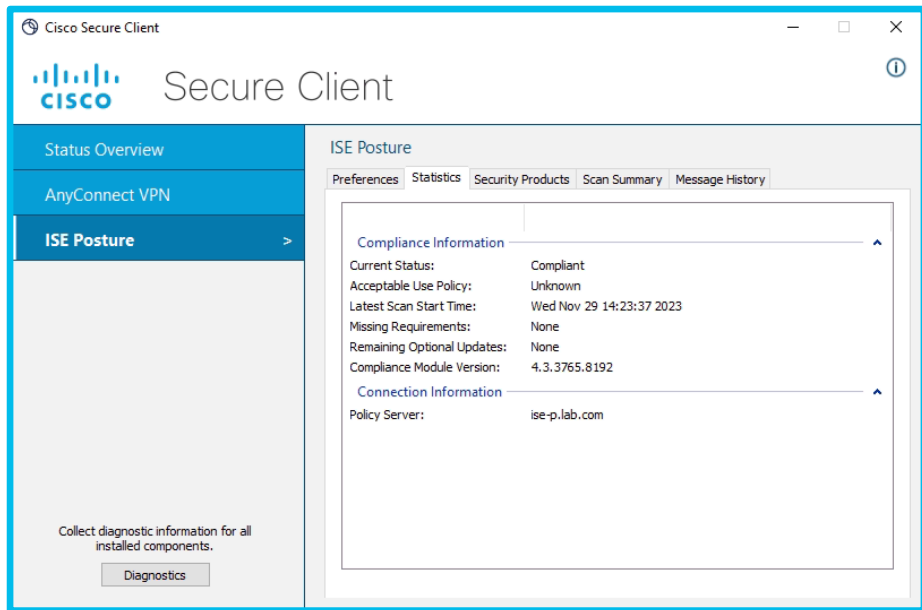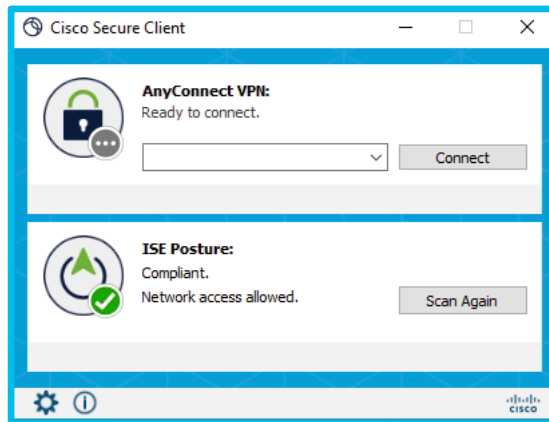
ISE Posture - Details
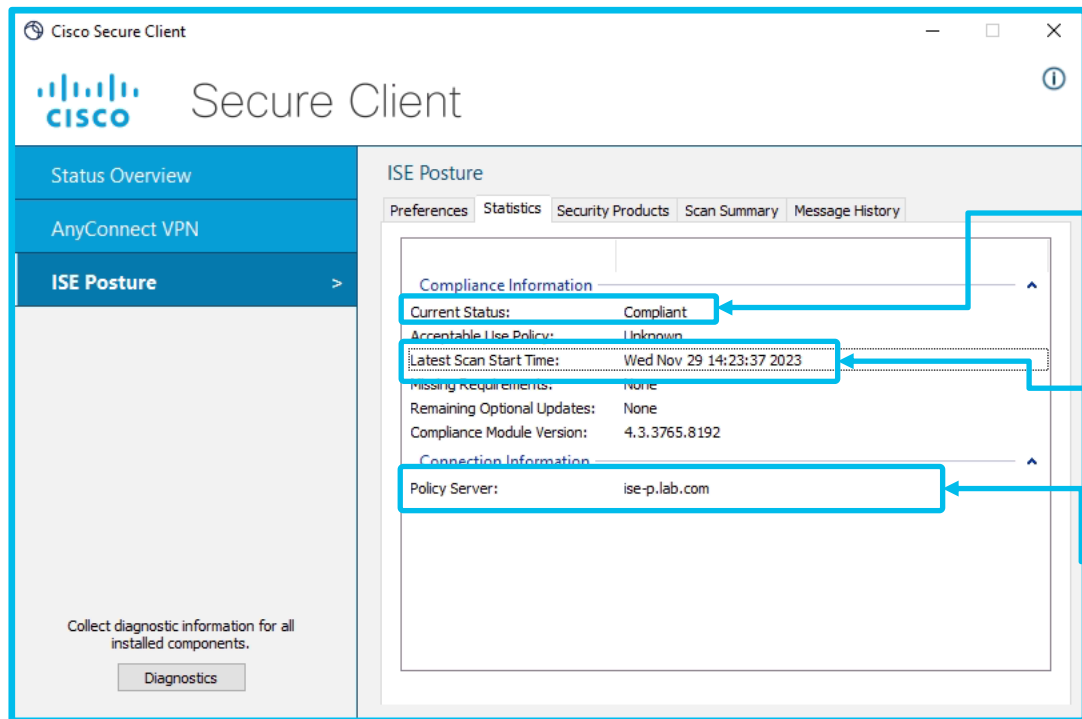
Current posture status returned from ISE to endpoint

Time and data of last scan

FQDN of the PSN which performed last posture check

ISE Posture – Security Products

Names of the detected security products

Product types like AM (Anti-Malware), PM (Patch Management) FW (Firewall)

Version of installed security products

Definition versions and definition dates (if applicable)
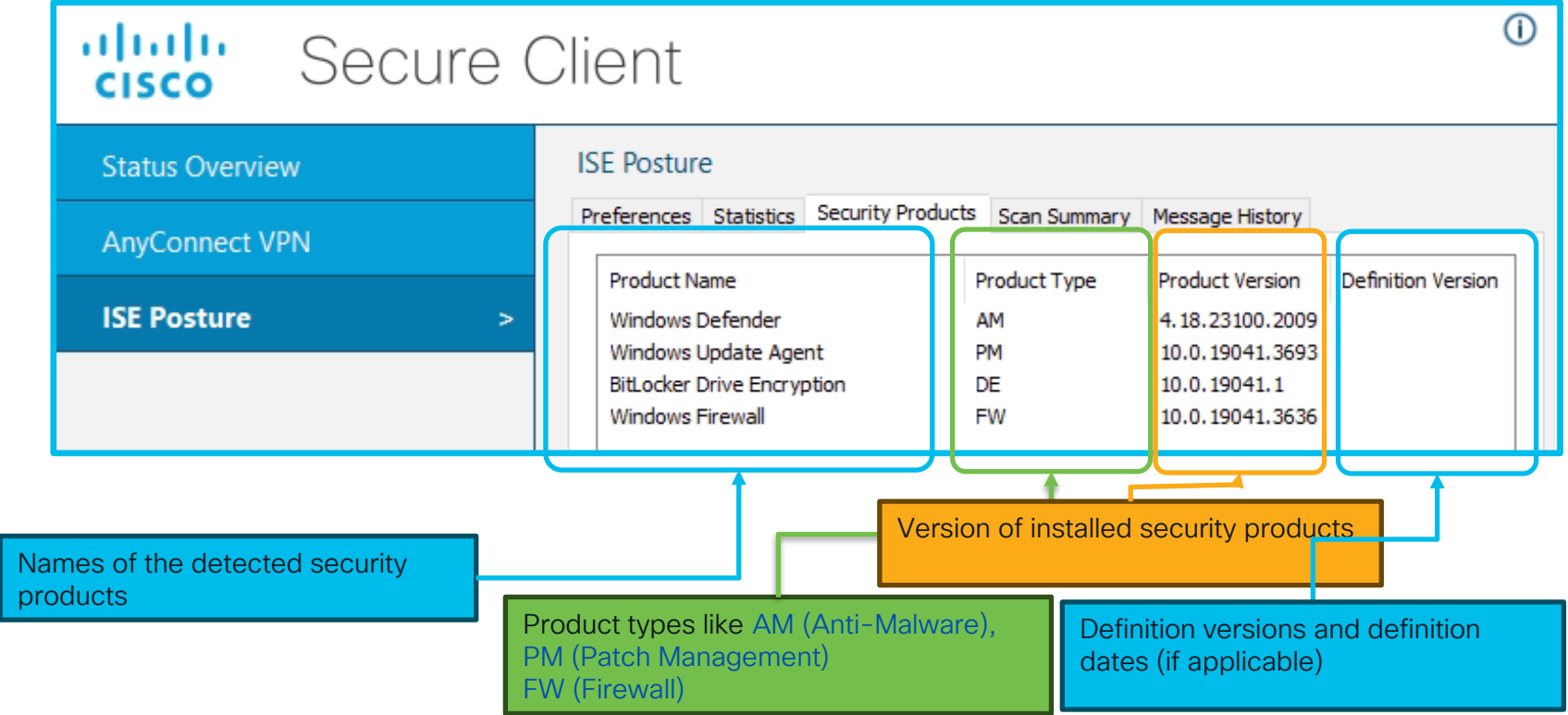
ISE Posture – Scan Summary

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.

Clearing Logs
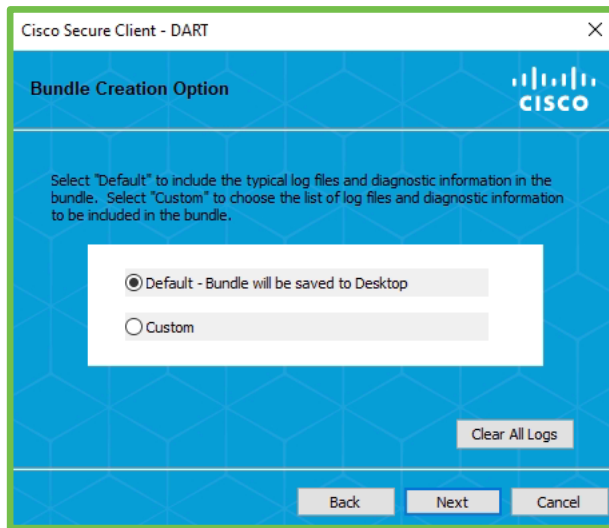
Packet Capture

Enable Rescan Button	Enabled ▼
Disable UAC Prompt	No ▼

ISE Posture:
Compliant.
Network access allowed.
`Scan Again`

http	**DNS**	**IP address of PSNs**
For general redirect troubleshooting tcp.port==80 is more effective	In case if we know which FQDN we are looking for: dns.qry.name == "posture.demo.local	In unknown environment better to use CP portal port as a filet: tcp.port==8443

Agent side troubleshooting – DART analysis

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

```
1251 Level: info   Restarting Discovery.
1251 Level: info   Restarting Discovery.
```

1. 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, .

2. 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.>.

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\Swi
ftHttpRunner.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"},
{config_uri="/auth/anyconnect?uuid=f62337c2-7f2e-4b7f-a89a-3508d761173c"},
{acpack_uri="/auth/provisioning/download/066ac0d6-2df9-4a2c-a129-fabf1ace36aa"},
 {acpack_port="8443"}, {acpack_ver="4.6.3049.0"}, {pra_enabled=0}}.
```

Demo – Learn on the example

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-U
```

Activate Windows

Network Device Troubleshooting

Cisco Switch
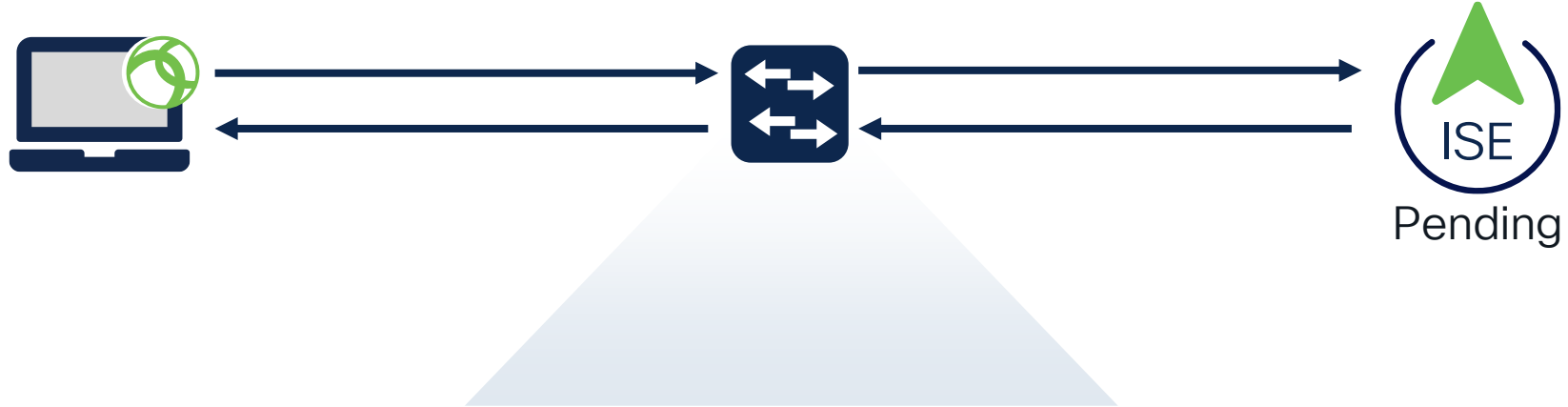
- Show access-session

- IP Device Tracking DB

Cisco Switch


```
KSEC-3850-1#sh authentication sessions interface g1/0/5 details
            Interface:  GigabitEthernet1/0/5
              IIF-ID:  0x184B6C6C
        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&actio
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
```

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

ASA/FTD

What is different
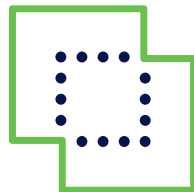
Cisco Secure Firewall

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 AnyConnect 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 accidently 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
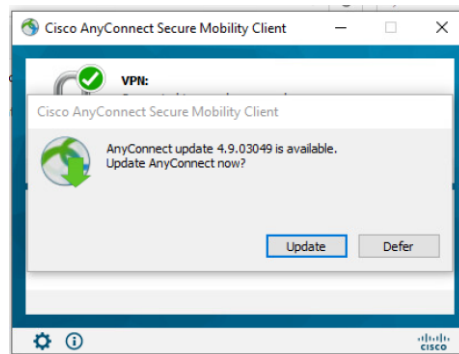
Cisco AnyConnect Secure Mobility Client

VPN:

Cisco AnyConnect Secure Mobility Client

AnyConnect update 4.9.03049 is available.
Update AnyConnect now?

[Update]   [Defer]

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
ℹ	📄	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:c 1:9b:86:27:9e:84:f1:ff:31:8d:6f:4d:9a:47:e2:ac:fe:2d:fc:f9:e8:5 8:62:01:7f: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=07ce672dcfabc3ada20d8ff 2dcc0ad28
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Essential license consumed.

Redirect attributes returned to NAD

Posture Assessment Report

Posture Assessment Report

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 ⓘ	Misconfigured Network Devices ⓘ	RADIUS Drops ⓘ	Client Stopped Responding ⓘ	Repeat Counter ⓘ
0	0	0	0	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	Authorizat	Authorization Profiles	Posture Status	S
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

Last Updated: Sat Jan 27 2024 14:04:27 GMT+0100 (Central European Standard Time)
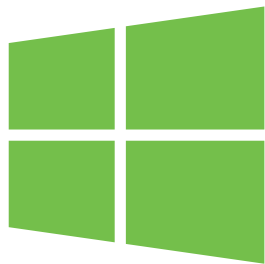
Records Shown: 5

Where we are

- Captures shows no communication over port 8443

- Packets are not crossing the switch

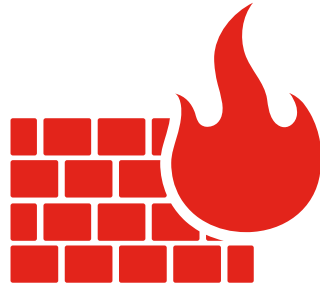- Pending state on ISE, no posture Reports received

Third party Firewall

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

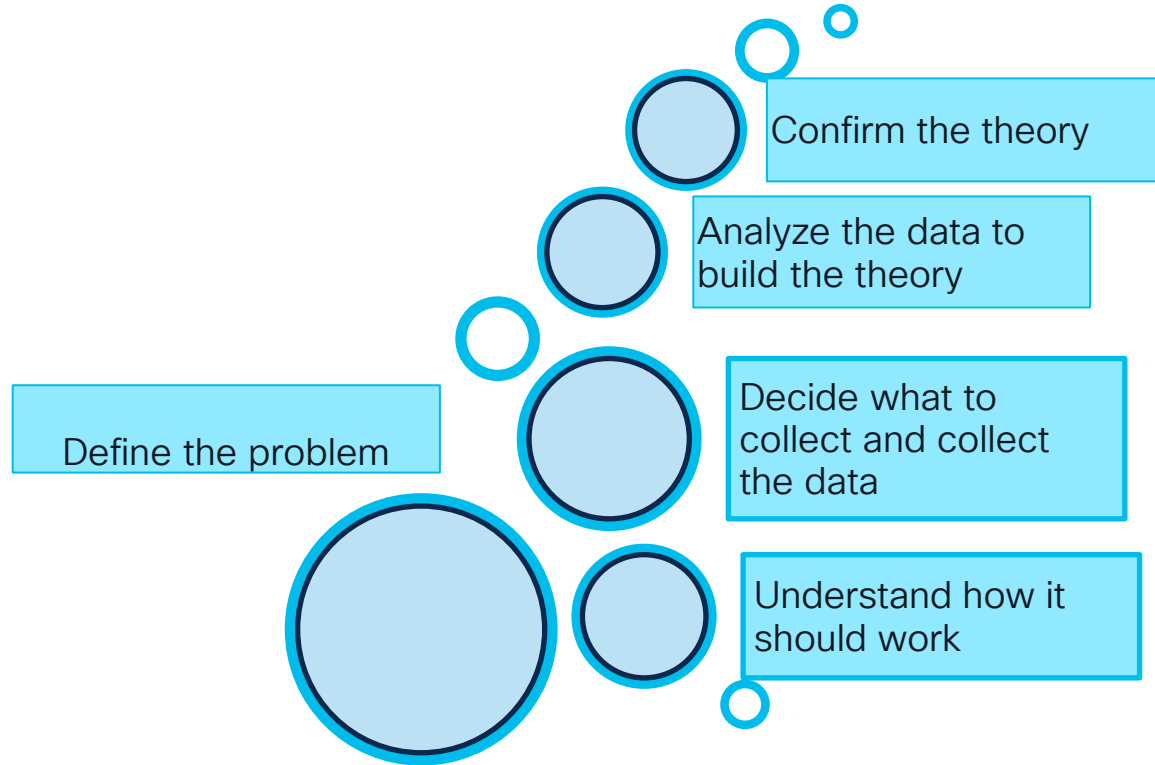This was breaking the communications over port 8443 to ISE

TCP.PORT 8443

Wrap up time

Key Takeaways

Confirm the theory

Analyze the data to build the theory

Define the problem

Decide what to collect and collect the data

Understand how it should work

Key Takeaways Posture Deployment

Work on the different ISE Pillars

Advanced Scenarios are just bigger puzzles

01

02

03

04

Posture is only part of the puzzle

Understand exactly the flow and where posture is going to fit

Security

ISE

Learn how Cisco ISE will help you implement Network access Control in your campus. Sessions will cover how to plan and deploy, how to leverage the new cloud capabilities, best practices and other topics.

START

Monday, February 5 | 8:45 a.m.
TECSEC-3416
Walking on Solid ISE: Advanced use cases and deployment best practices

Monday, February 5 | 2:15 p.m.
TECSEC-3503
Segmenting industrial networks with Trustsec and Cisco Identity Services Engine

Tuesday, February 6 | 8:00 a.m.
BRKSEC-2889
Mastering ISE Upgrades: Best Practices, Tips, and Tricks

Tuesday, February 6 | 5:00 p.m.
BRKSEC-2660
ISE Deployment Staging and Planning

Wednesday, February 7 | 10:30 a.m.
BRKSEC-2039
Secure Access with ISE in the Cloud

Thursday, February 8 | 8:45 a.m.
BRKSEC-2100
ISE Your Meraki Network with Group Based Adaptive Policy

Thursday, February 8 | 2:30 p.m.
BRKSEC-3077
A song of ISE and Posture: Advanced deployment and troubleshooting

Thursday, February 8 | 4:30 p.m.
BRKSEC-2234
Cisco ISE Performance, Scalability and Best Practices

FINISH
Friday, February 9 | 9:15 a.m.
BRKSEC-3412
Unleashing the Art of Troubleshooting Authenticaton Latency issues.

Cisco *Live!*

Let's go