Cisco Secure Client

Technical Deep Dive

Bill Yazji
Technical Security Architect
byazji@cisco.com | 𝕏 @BillYazji | in billyazji

CISCO Live!

BRKSEC-2834

Abstract

We have all heard the complaints or did the complaining ourselves: "Cisco has too many agents". Come learn from Bill Yazji, while he shows you that Cisco has listened to the complaints and delivered a unified security agent called Cisco Secure Client.

Cisco Secure Client (CSC) provides a modular framework allowing for AnyConnect VPN, Cisco Secure Endpoint (formerly AMP for Endpoints), Network Visibility Module, Umbrella Cloud Security, ISE Posture, Secure Firewall Posture (formerly Hostscan) and the Network Access Module (NAM) to all exist together; with a modern cloud-based management coming from Cisco XDR - connected intimately with XDR device insights.

In this session, we will dive into the technology behind the Secure Client, how things really work and how they do not. We will cover deployments models from the cloud and using your own software deployment mechanisms. We will learn all about the seamless upgrade flows from existing AnyConnect and Secure Endpoint (AMP) agents. We will talk about scenarios where it makes sense to upgrade to CSC and scenarios where it truly benefits you to stay with the existing AnyConnect and Secure Endpoint (AMP) agents - at least for now.

#me :: “the work”

- Technical Solutions Architect
- Over 15 years with Cisco and nearly 26 years of security, cloud and networking experience
- Heavily involved in internal Champion programs for SSE and XDR products
- Prior to Cisco…
  - Cisco competitor in Web Security space
  - Network and Security Consultant on the customer side
  - Large design, deployment, integration and troubleshooting focus

CISCO CERTIFIED CCNP SECURITY

GIAC CERTIFIED GCIH INCIDENT HANDLER

#me :: “the not work”

Cisco Webex App

Questions?

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

How

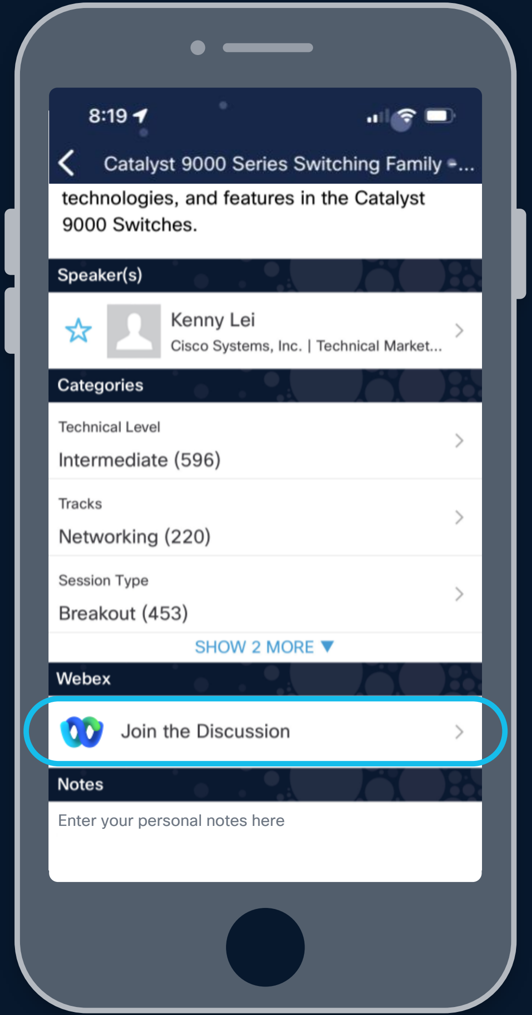
Ⓐ Find this session in the Cisco Live Mobile App

Ⓒ Click "Join the Discussion"

③ Install the Webex App or go directly to the Webex space

Ⓑ Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



8:19

Catalyst 9000 Series Switching Family •...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKSEC-2894

Important: Hidden Slide Alert

There are hidden slides with additional information

For Your Reference

Surveys are important...

Drop your email in the comments – I WILL respond!

Agenda

01 CSC Overview

02 CSC Architecture

03 Cloud Deployment & Management

04 Upgrading to CSC

05 FAQs, Tips and Tricks

“I want to install & support another agent on my end user workstations”

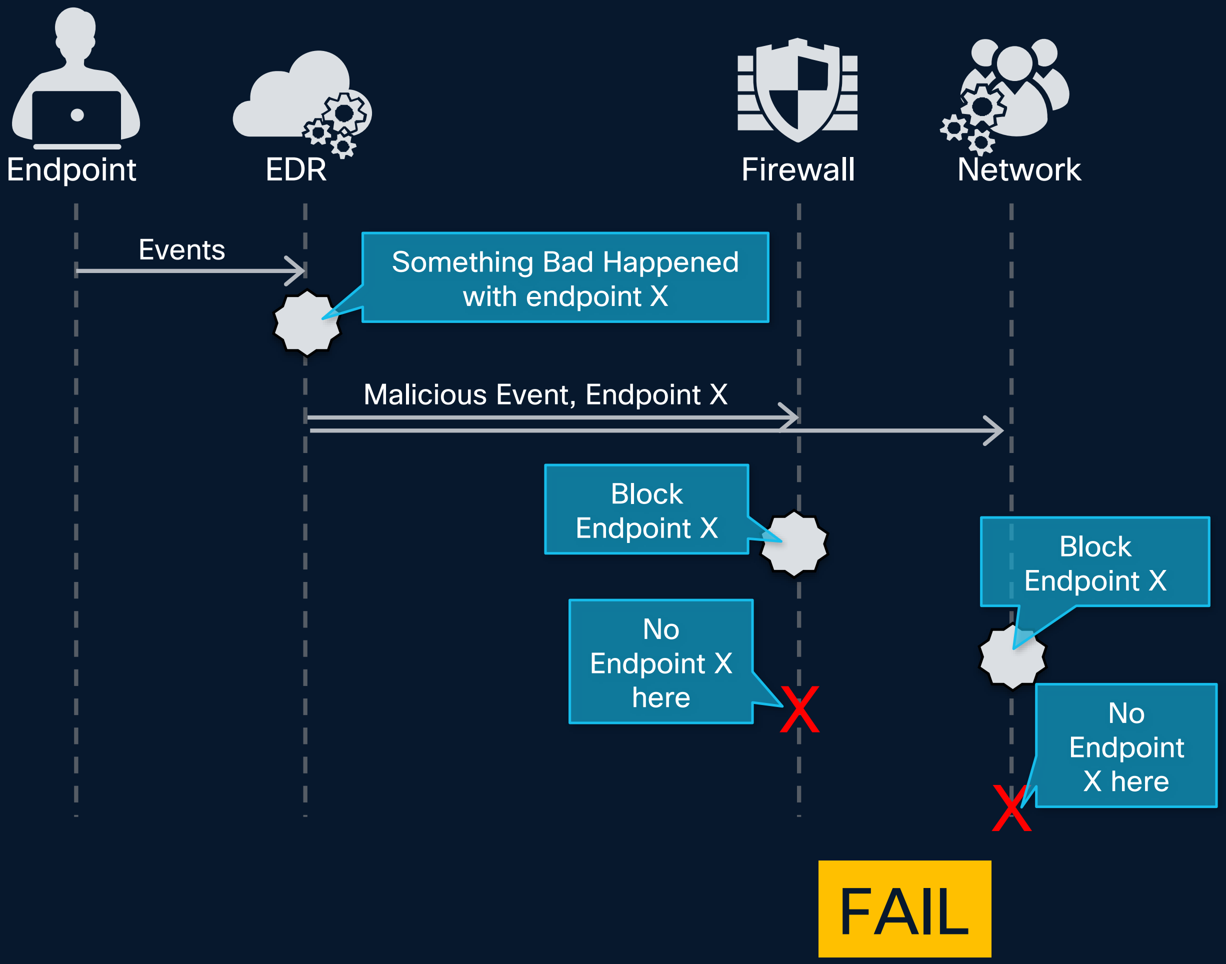
- No one, ever...

Why build a unified security agent?

- Our customers have identified operational challenges with deploying multiple endpoint agents (e.g., AnyConnect, Secure Endpoint, Orbital, Umbrella, Duo, Tetration, Meraki SM, Thousand Eyes, etc.)
- These operational challenges limit ability to deploy and consume various endpoint security functions
- Delivering a unified endpoint agent addresses a key customer operational pain point and meets customer demand

But also...

- SIEM & SOAR are guilty as well
- Each product views endpoint in its own way.
  - GUID (specific to product)
  - IP Address (ephemeral & changes all the time)
  - MAC Address (ephemeral, private, unavailable, duplicative)
  - Hostnames, serial number, more more more...
- Making the products work together is a challenge



We need a common endpoint “object”

We are doing two things about this

1. Cisco Secure Client
   - Bringing together Cisco Security tools in a single managed package
2. Device Insights
   - Normalizes, De-duplicates and correlates to create a common endpoint object from integrated sources

Shameless plug..

Device Insights

- Normalizes, De-duplicates and correlates to create a common endpoint object from integrated sources

Aaron Woland

Distinguished Engineer

Making XDR Investigations and SOAR Automation Work by Unifying Assets

BRKSEC-2754

On-Demand / Amsterdam 2023

On-Demand / Melbourne 2022

Our current endpoint security offering is confusing

	Windows	macOS	Android	iOS	Linux
RA VPN Connectivity	AnyConnect / DuoConnect	AnyConnect / DuoConnect	AnyConnect	AnyConnect	AnyConnect / DuoConnect
Malware Protection / EDR	AMPBE / Tetration Agent	AMPBE	AMPBE	-	AMPBE / Tetration Agent
Visibility / Telemetry	AnyConnnect NVM / Tetration Agent / AKEyes	AnyConnnect NVM / Tetration Agent / AKEyes	AnyConnnect NVM (Knox)	Cisco Security Connector (CSC)	AnyConnnect NVM / Tetration Agent / AKEyes
Posture	AnyConnnect / Duo Health	AnyConnnect / Duo Health	Duo (limited)	Duo (limited)	AnyConnect (ASA) not ISE
Umbrella (DNS)	ERC / AnyConnect	ERC / AnyConnect	AnyConnect	Cisco Security Connector (CSC)	-
Umbrella (SWG)	AnyConnect	AnyConnect	-	-	-

Some basics/history

- Unified agent - Windows (amd64/arm64) and macOS (amd64/arm64)
- Windows > Mac > iOS > Android > Linux
- Seamless upgrade from existing AnyConnect & Secure Endpoint [AMP for Endpoint] Clients to Cisco Secure Client
- Leverages Existing AnyConnect (AC) Framework
  - AC UI is starting point for new shared UI
  - AC already had modules for many services
  - Core AC services, such as trusted network detection, become available as common services for all modules
- Cloud management continued improvements
  - Hosted in XDR and Secure Client Cloud Management

Some basics/history

- Unified agent - Windows (amd64/arm64) and macOS (amd64/arm64)
- Windows > Mac > iOS > Android > Linux
- Seamless upgrade from existing AnyConnect & Secure Endpoint [AMP for Endpoint] Clients to Cisco Secure Client
- Leverages Existing AnyConnect (AC) Framework
  - AC UI is starting point for new shared UI
  - AC already had modules for many services
  - Core AC services, such as trusted network detection, become a s common services for all modules
- Cloud management continued improvements
  - Hosted in XDR and Secure Client Cloud Management

Cool Stuff

AnyConnect 4.x: End of Life Announcement

- Software maintenance for 4.x software releases ended **March 31, 2024**. No patches or maintenance releases will be provided for AnyConnect 4.x releases after this date.
- Application software support will not be available beyond **March 31, 2027**.
- Software maintenance and application software support requires an active term license or active service contract for perpetual licenses. After these dates, all support services for the product are unavailable and the product becomes obsolete.
- https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/anyconnect-secure-mobility-client-v4x-eol.html

We used to go around the world stating:

AnyConnect

is
more
than

VPN

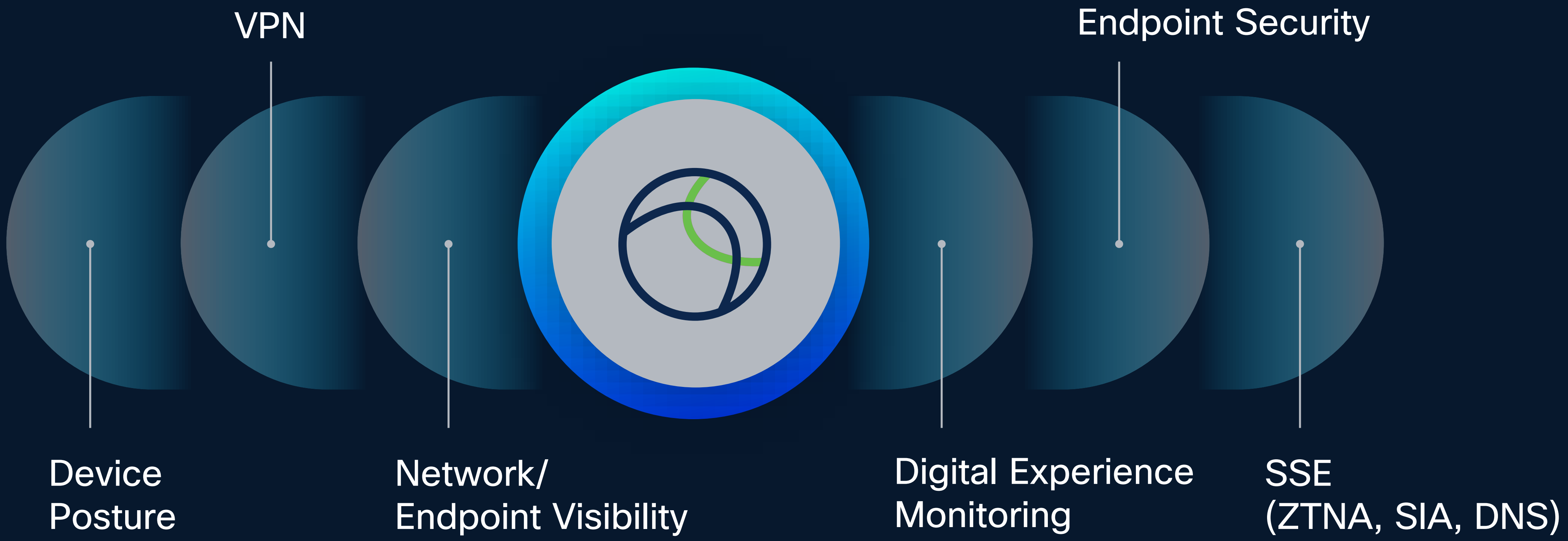
The Reality...

Secure Client

is
wayyyyyyyy
more
than

VPN

One client, multiple functions



VPN

Endpoint Security

Device Posture

Network/ Endpoint Visibility

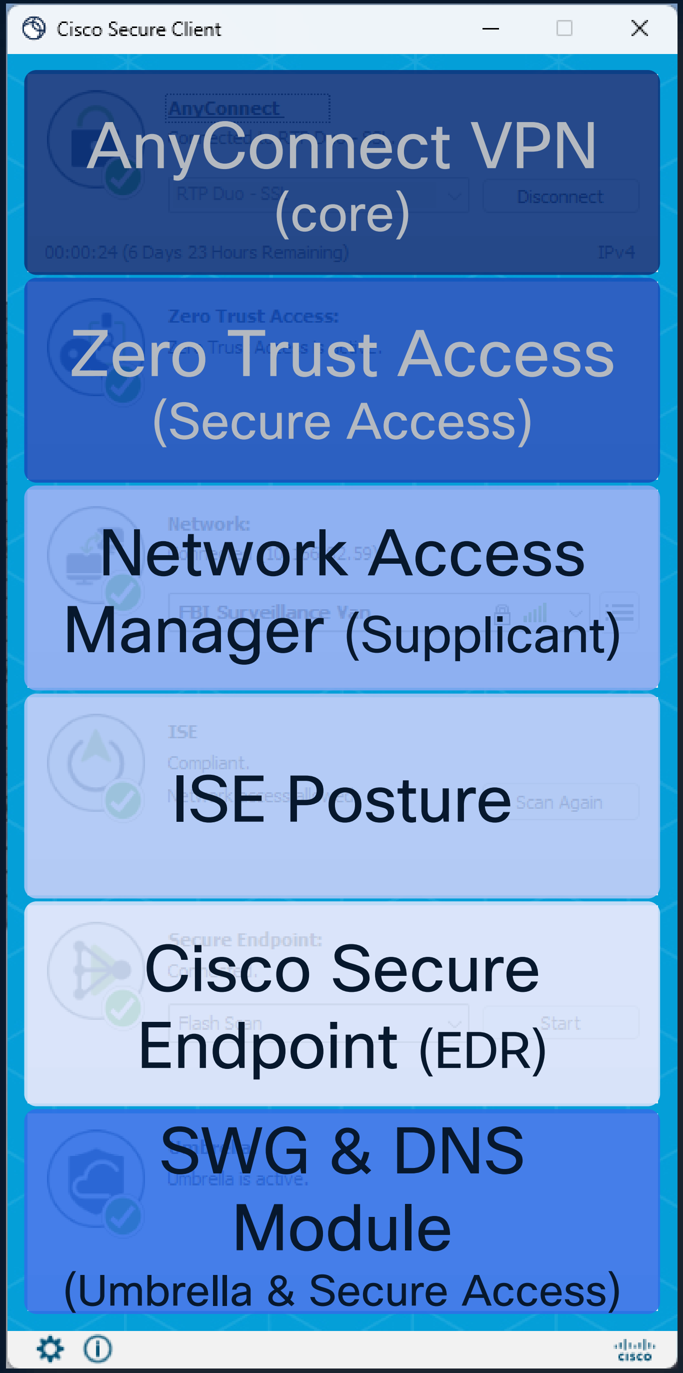
Digital Experience Monitoring

SSE (ZTNA, SIA, DNS)

Cisco Secure Client

Suite of security service modules

- Modules with UI Tile
- Plus modules with no UI Tile:
  - Cloud Management Module
  - Secure Firewall Posture (aka: HostScan)
  - Network Visibility Module (NVM)
  - Thousand Eyes
  - Diagnostics and Reporting Tool (DART)
  - Orbital
  - Forensics


AnyConnect VPN (core)

Zero Trust Access (Secure Access)

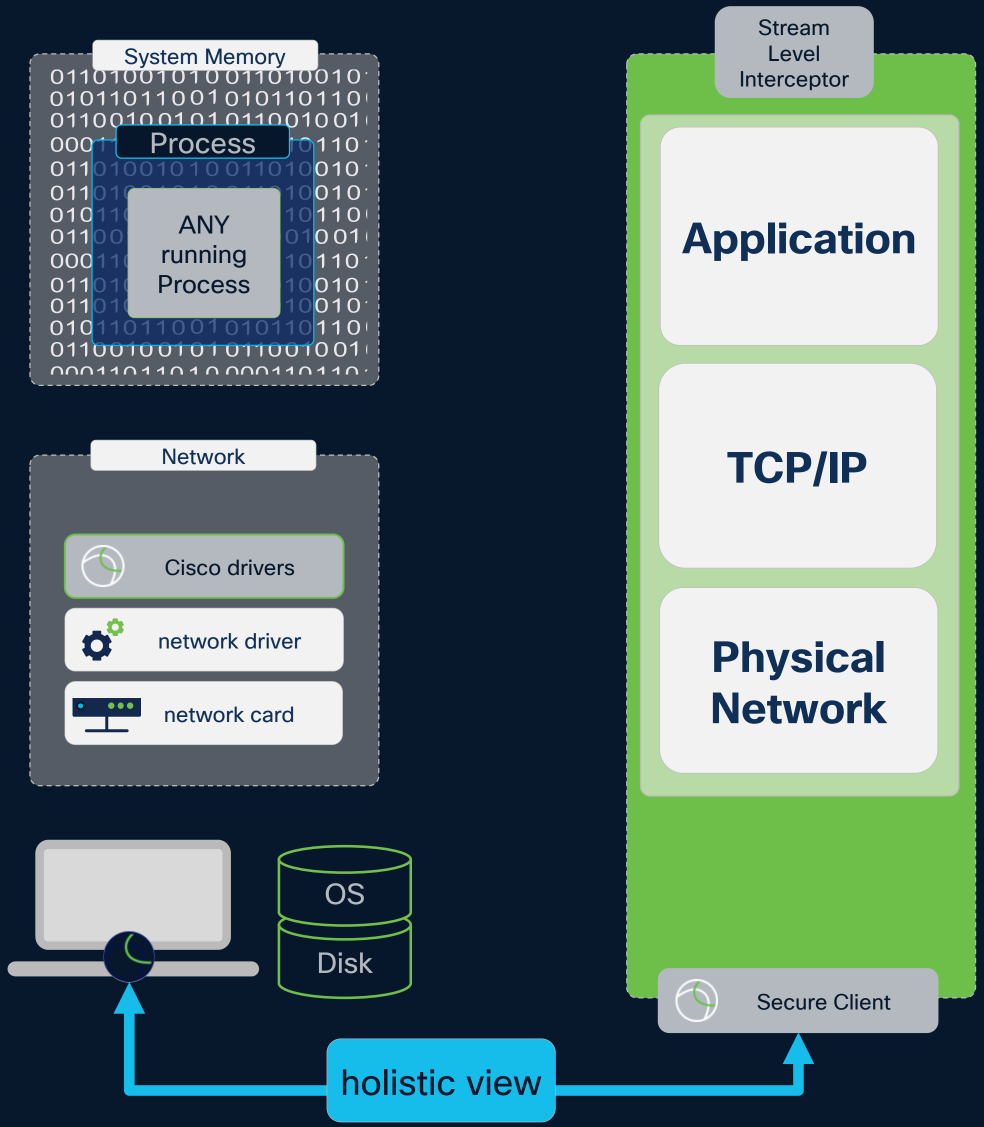
Network Access Manager (Supplicant)

ISE Posture

Cisco Secure Endpoint (EDR)

SWG & DNS Module (Umbrella & Secure Access)

Stream Level Interceptor

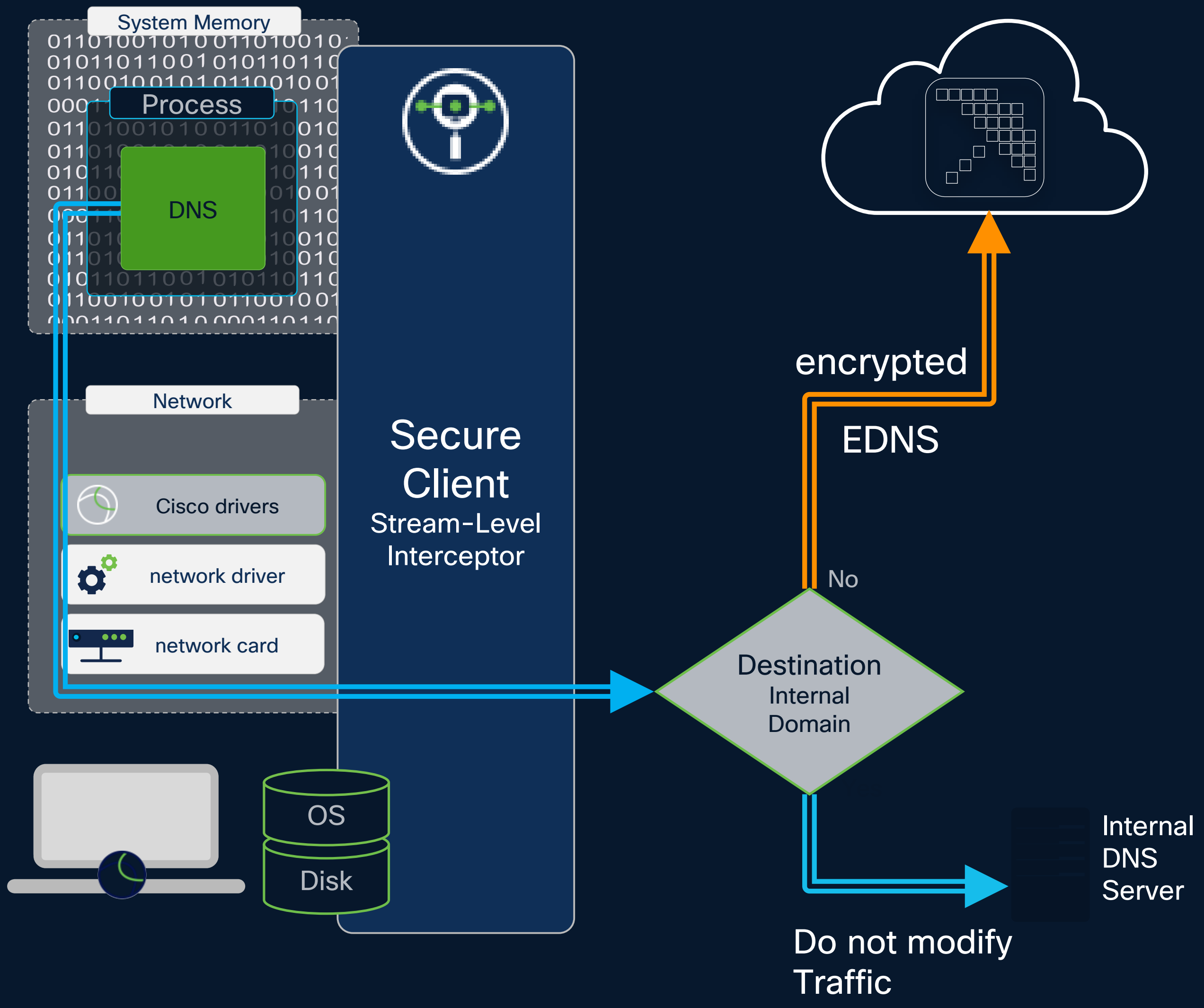


- The **Stream Level Interceptor** included in Secure Client enables a full holistic, pre-encrypted view on the endpoint network activity

- This core function from Cisco Secure Client makes the solution so powerful
- **It enables other modules like the Umbrella Module or/and NVM to work**

- This holistic view examines & manipulates information for any network communication
  - **from the running application**
  - **to the physical network layer**

Stream Level Interceptor

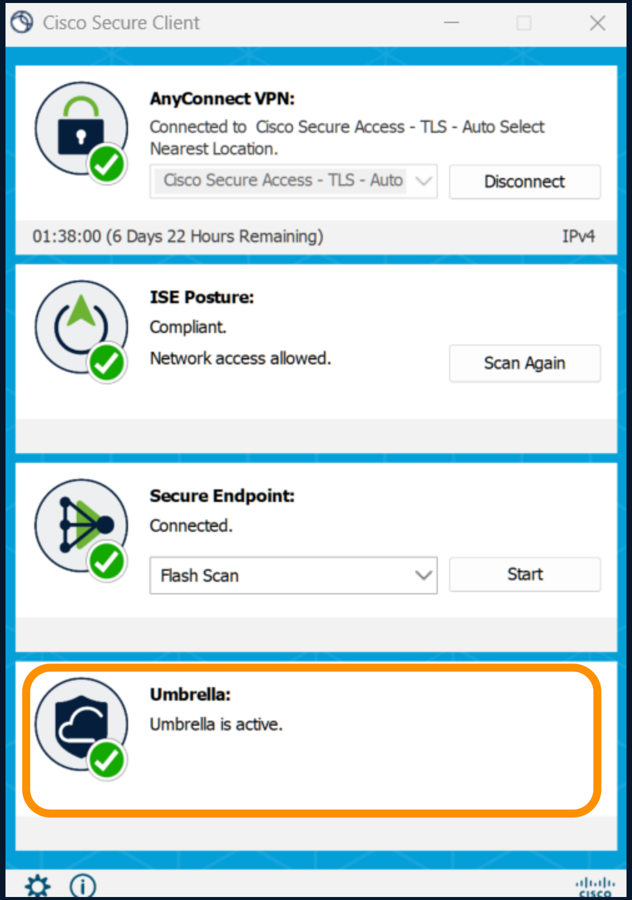


- Umbrella (DNS) Example:
  - DNS Request Sent Down the Stack:
  - DNS identified in the stream
    - From Chrome
    - User was Lee (employee)
  - Destination checked against Umbrella Policy
    - Internal Domain – Leave untouched
    - External Domain – Modify the DNS Traffic
      - Wrap request in EDNS
      - Insert Identity Data for Umbrella
      - Encrypt
      - Ship it off to the Umbrella Resolver

Umbrella Module

Same Umbrella Roaming from AnyConnect:

- Umbrella DNS
- Umbrella Secure Web Gateway
- Secure Access



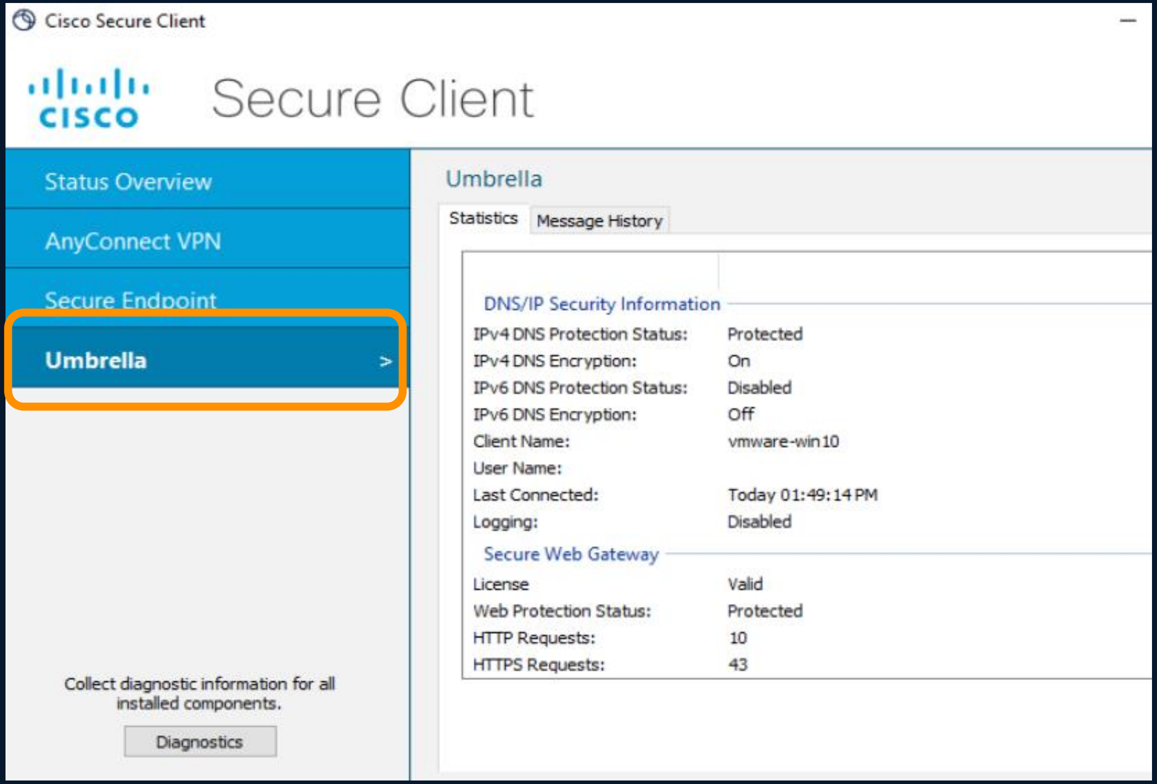
Cisco Secure Client

AnyConnect VPN:
Connected to Cisco Secure Access - TLS - Auto Select Nearest Location.
Cisco Secure Access - TLS - Auto | Disconnect
01:38:00 (6 Days 22 Hours Remaining) IPv4

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

Secure Endpoint:
Connected.
Flash Scan | Start

Umbrella:
Umbrella is active.



Cisco Secure Client

Secure Client

Umbrella

DNS/IP Security Information

IPv4 DNS Protection Status:	Protected
IPv4 DNS Encryption:	On
IPv6 DNS Protection Status:	Disabled
IPv6 DNS Encryption:	Off
Client Name:	vmware-win10
User Name:	
Last Connected:	Today 01:49:14 PM
Logging:	Disabled

Secure Web Gateway

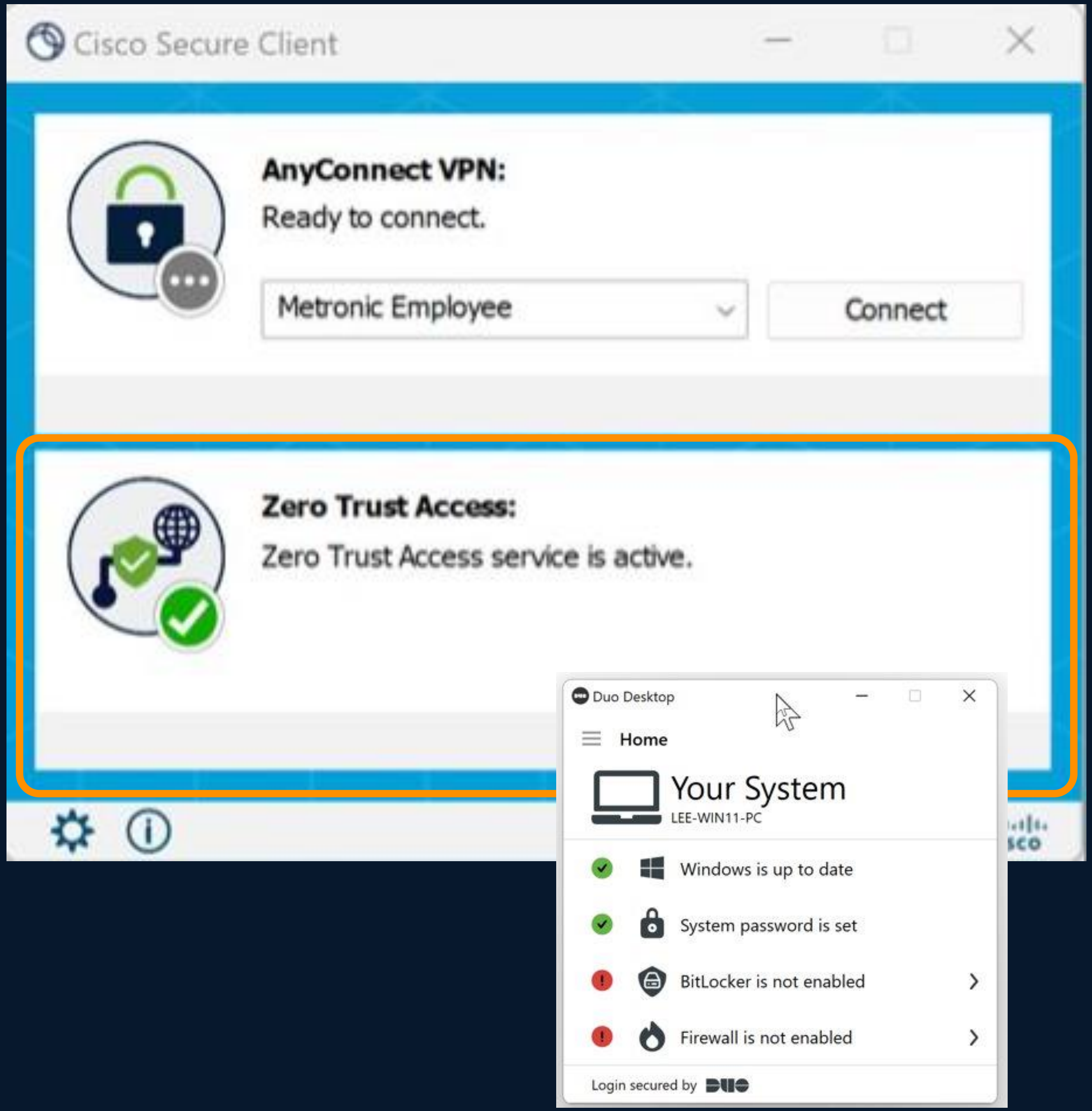
License	Valid
Web Protection Status:	Protected
HTTP Requests:	10
HTTPS Requests:	43

Collect diagnostic information for all installed components.

ZTA Module

Dedicated module for **Secure Access**

- Side-loads the Duo Desktop
  - (formerly Duo Health Agent)
- Zero Trust has ability to use **MASQUE + QUIC** for seamless transport



AnyConnect VPN:
Ready to connect.

Metronic Employee

Zero Trust Access:
Zero Trust Access service is active.

Your System
LEE-WIN11-PC

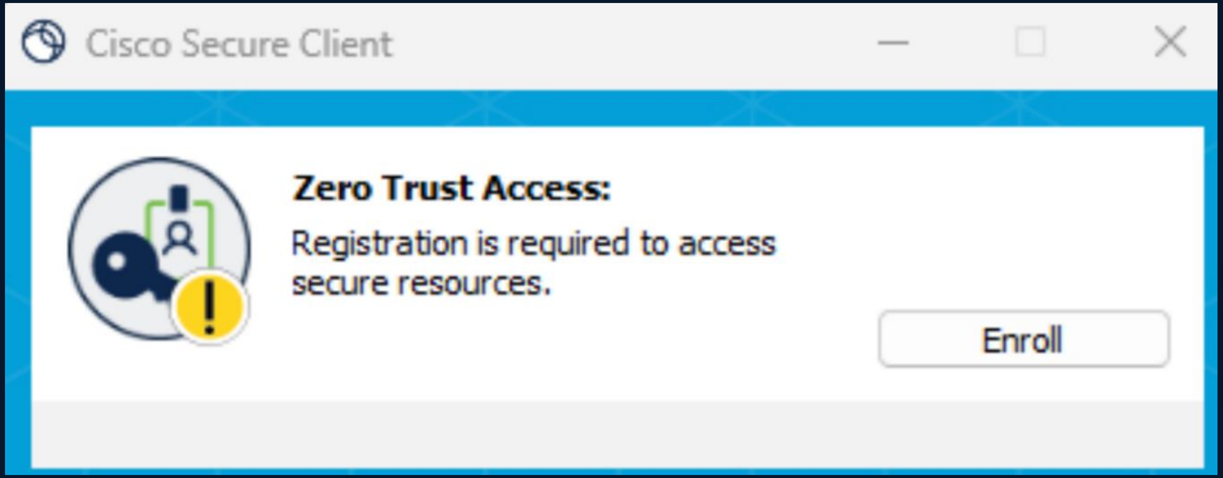
- ✓ Windows is up to date
- ✓ System password is set
- ! BitLocker is not enabled
- ! Firewall is not enabled

Login secured by DUO

ZTA Module

For Cisco Secure Access

- Manual Enrollment
  - Simply login, and it gets all the config
- Certificate Enrollment
  - Push configuration at time of deployment
- ZTA Module available in Cloud Management for deployment



Zero Trust Access:

Registration is required to access secure resources.

Cisco Zero Trust Access Options

	Secure Firewall	Cisco Secure Access
Hosting	Hardware or VM	
Type	Clientless	
Client	Web Browser	
Supported Traffic	Client-to-server	
Supported Apps	HTTPS	
Client Protocol(s)	TLS	
Device Posture	None (Use Duo)	
Per-App Controls	TLS Decrypt, IPS, Anti-Malware	

New Cisco Zero Trust Access Options

	Secure Firewall	Cisco Secure Access		
Hosting	Hardware or VM	SaaS		
Type	Clientless	Clientless	Client-Based	
Client	Web Browser	Web Browser	ZTA Module OS Native Clients	VPN Module
Supported Traffic	Client-to-server	Client-to-server	Client-to-server	Client-to-server, Client-to-client, Server-to-client
Supported Apps	HTTPS	HTTP, HTTPS	TCP & UDP, RDP, SSH	TCP, UDP & ICMP
Client Protocol(s)	TLS	TLS	MASQUE over QUIC or TLS	TLS, DTLS, IPSec
Device Posture	None (Use Duo)	Per-Rule	Per-Rule	On Connect
Per-App Controls	TLS Decrypt, IPS, Anti-Malware	User/Group-Based Access Control, TLS Decrypt, IPS		

...we pause for a shameless plug

Steven Chimes

Security Architect

Zero Trust Access (ZTA) Demystified – The Cisco Technologies That Make Frictionless Security Possible

BRKSEC-2079

On-Demand

(Las Vegas 2024)

Vinny Parla

Principal Architect

Deep Dive into Cisco's Use of QUIC, MASQUE and OS Native Capability to deliver frictionless Zero Trust Access

BRKSEC-3027

Tuesday, June 10

Jonny Noble

Technical Marketing

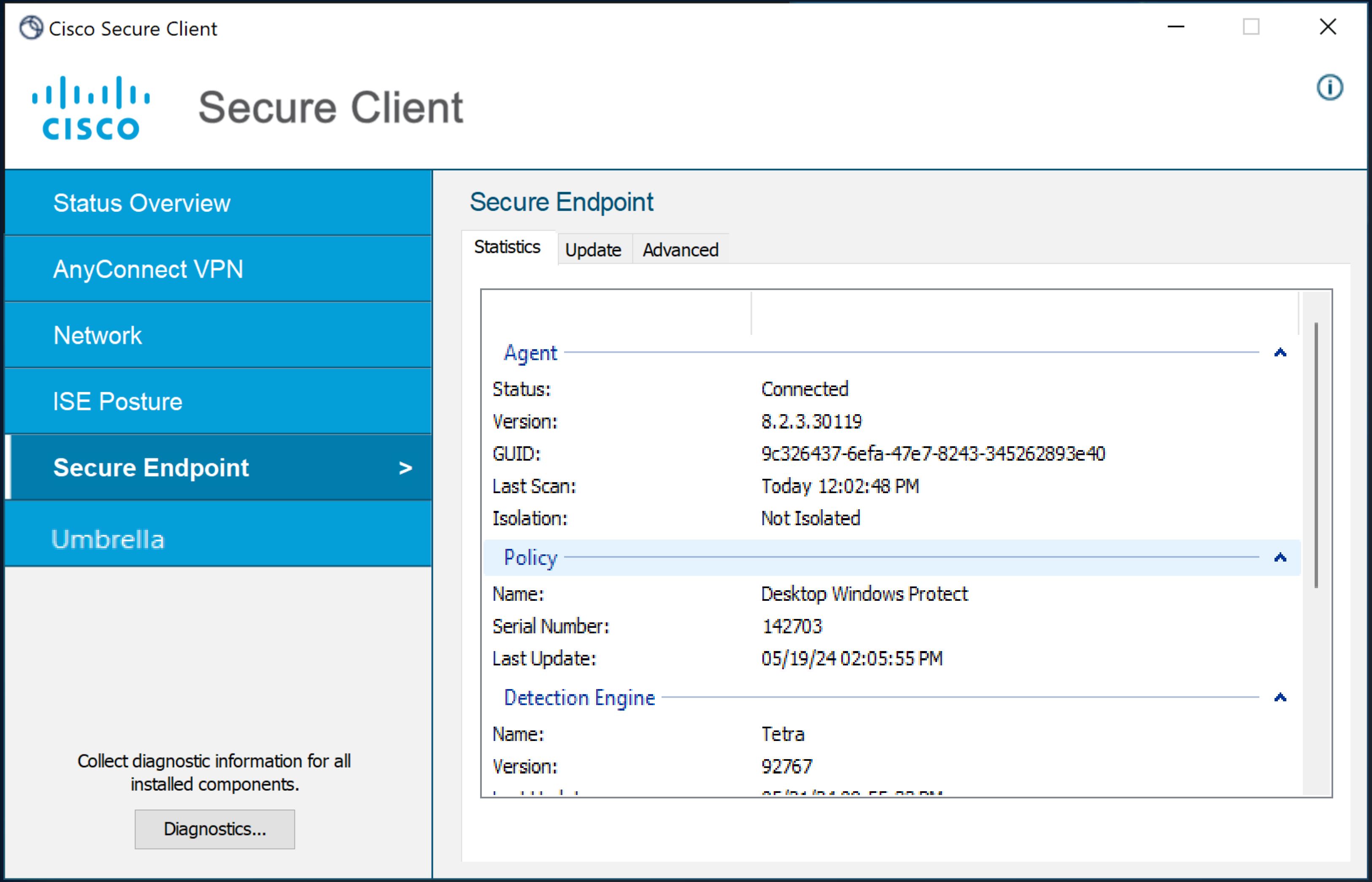
The Latest in Secure Access (SSE) Innovation

BRKSEC-2438

Monday, June 9

Secure Endpoint Module

- Follows the AnyConnect UI Framework
  - All the important status information from the old UI



Collect diagnostic information for all installed components.

Secure Endpoint

Agent

Status:	Connected
Version:	8.2.3.30119
GUID:	9c326437-6efa-47e7-8243-345262893e40
Last Scan:	Today 12:02:48 PM
Isolation:	Not Isolated

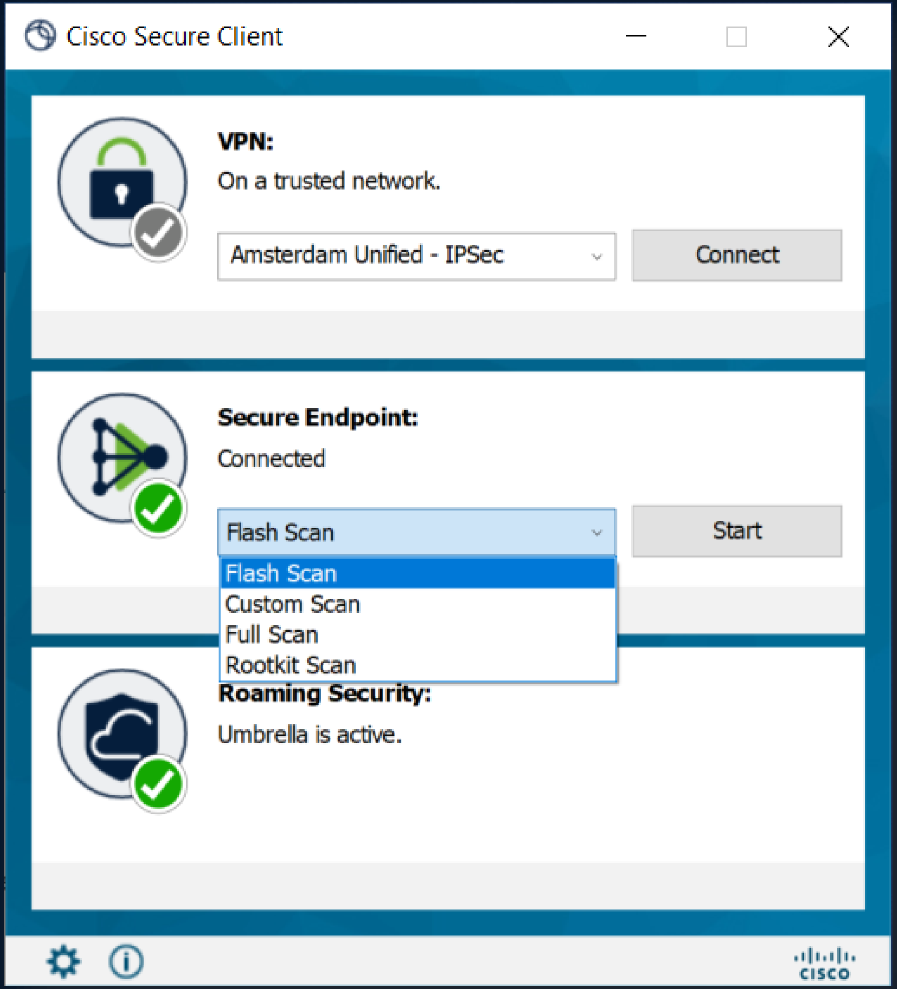
Policy

Name:	Desktop Windows Protect
Serial Number:	142703
Last Update:	05/19/24 02:05:55 PM

Detection Engine

Name:	Tetra
Version:	92767

More Secure Endpoint UI



Cisco Secure Client

VPN:
On a trusted network.

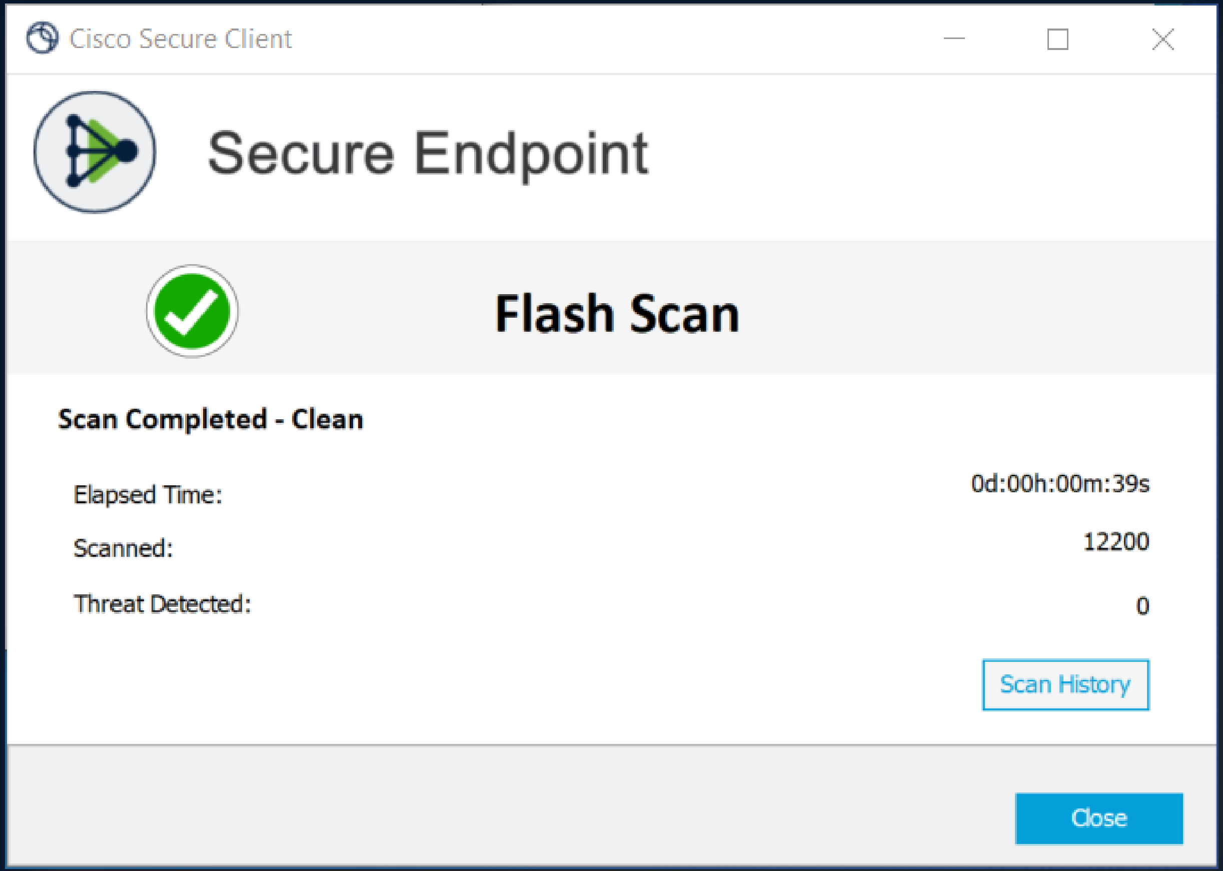
Amsterdam Unified - IPSec ⌄ | Connect

Secure Endpoint:
Connected

Flash Scan ⌄ | Start

- Flash Scan
- Custom Scan
- Full Scan
- Rootkit Scan

Roaming Security:
Umbrella is active.



Cisco Secure Client

Secure Endpoint

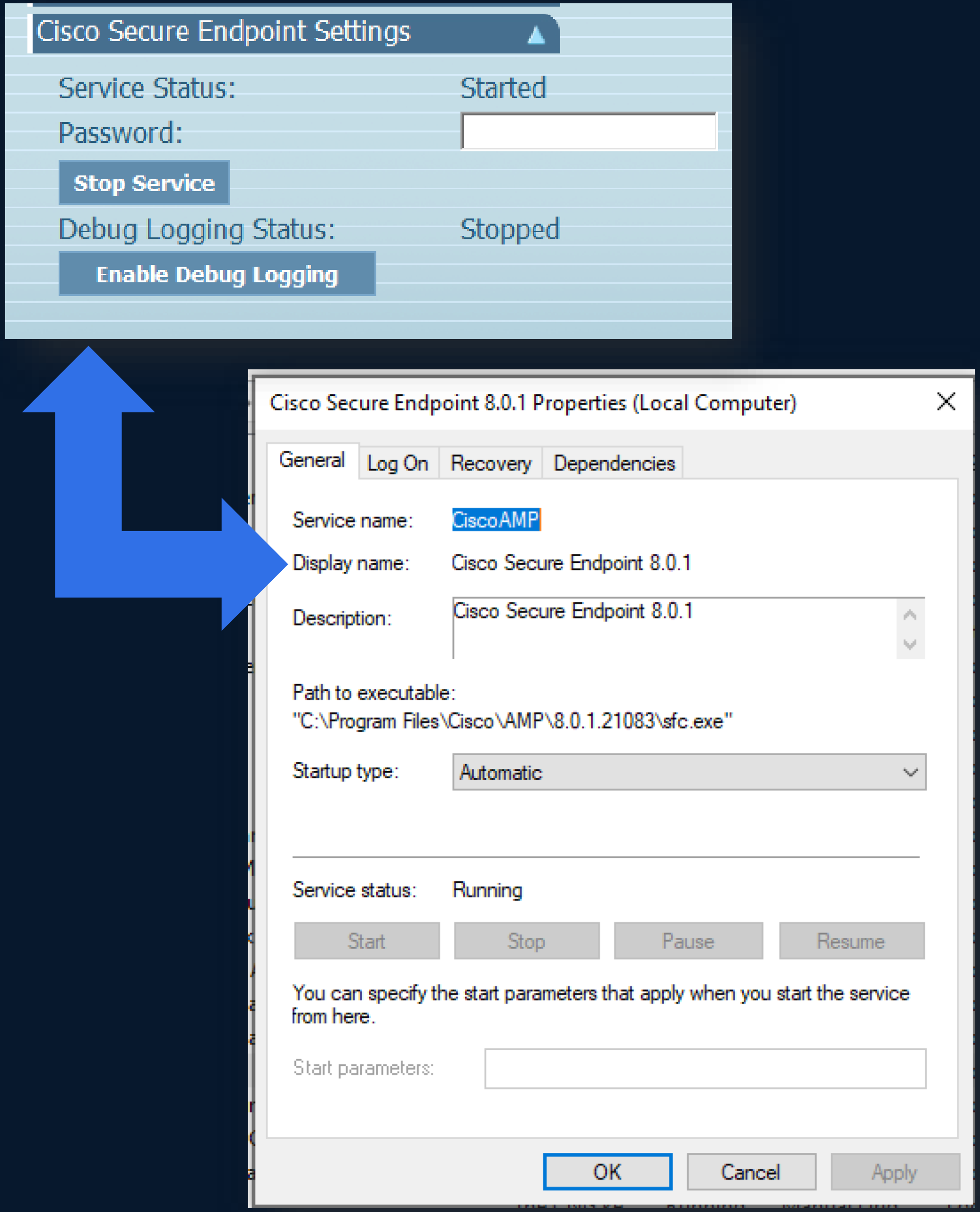
✓ Flash Scan

Scan Completed - Clean

Elapsed Time:	0d:00h:00m:39s
Scanned:	12200
Threat Detected:	0

More Secure Endpoint UI

- Removed the ability to control the service from the UI when the connector is protected mode.
  - For security reasons
  - CLI only



Cisco Secure Endpoint Settings

Service Status: Started

Password:

Debug Logging Status: Stopped

Cisco Secure Endpoint 8.0.1 Properties (Local Computer)

Service name: CiscoAMP

Display name: Cisco Secure Endpoint 8.0.1

Description: Cisco Secure Endpoint 8.0.1

Path to executable:
"C:\Program Files\Cisco\AMP\8.0.1.21083\sfc.exe"

Startup type: Automatic

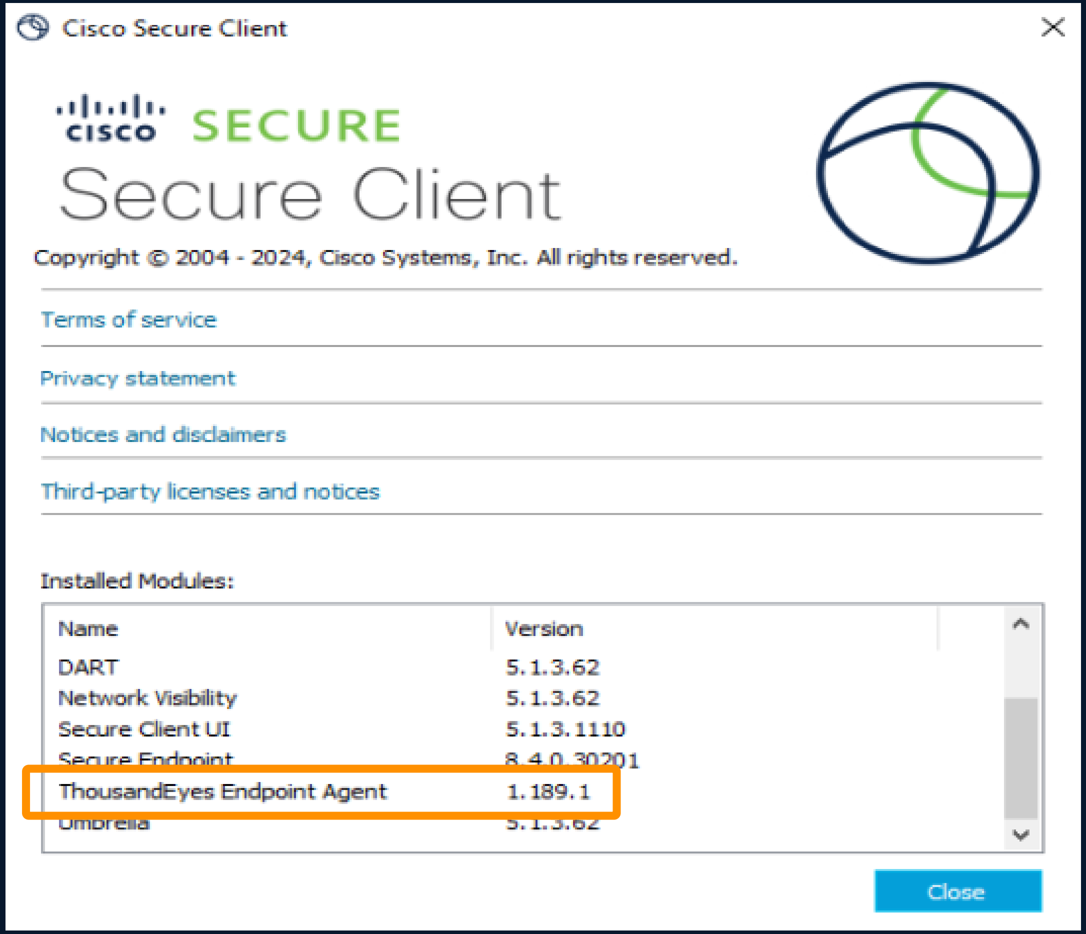
Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

ThousandEyes

- What is it?
  - End to end monitoring of connection statistics
- No UI Tile, No Cloud or Web Deployment.
- Windows & Mac Secure Client support
- Supports standalone ThousandEyes or Secure Access DEM



Cisco Secure Client

Secure Client

Copyright © 2004 - 2024, Cisco Systems, Inc. All rights reserved.

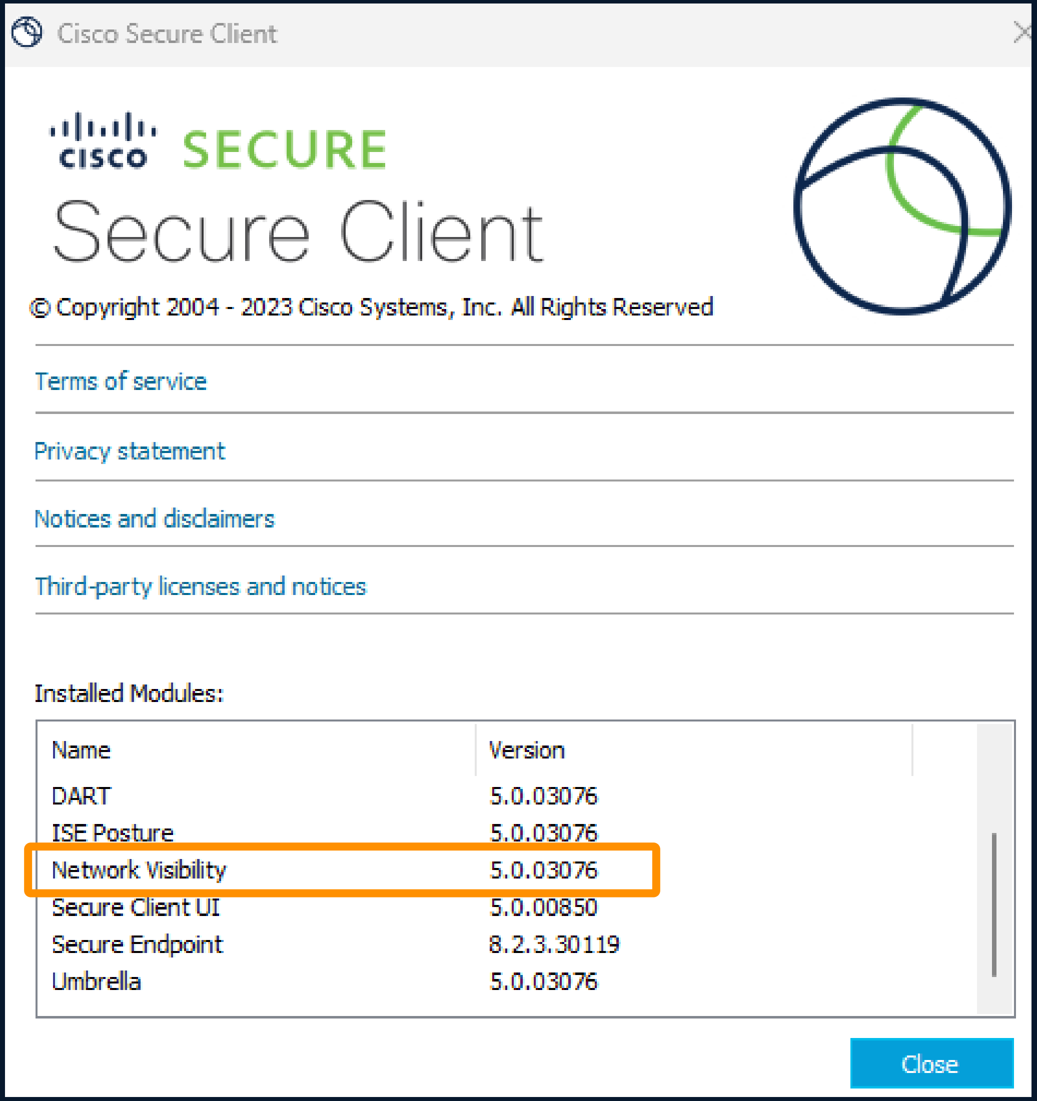
Installed Modules:

Name	Version
DART	5.1.3.62
Network Visibility	5.1.3.62
Secure Client UI	5.1.3.1110
Secure Endpoint	8.4.0.30201
ThousandEyes Endpoint Agent	1.189.1
Umbrella	5.1.3.62

https://docs.thousandeyes.com/product-documentation/global-vantage-points/endpoint-agents/secure-client-integration

Network Visibility Module (NVM)

- Network & Endpoint Visibility
  - Creates a flow record of every connection from endpoint
  - User/Process/Machine Information
  - No UI Tile
- Can send to Cloud **or** On-Premise
  - Cloud profile defaults to XDR



© Copyright 2004 - 2023 Cisco Systems, Inc. All Rights Reserved

Installed Modules:

Name	Version
DART	5.0.03076
ISE Posture	5.0.03076
Network Visibility	5.0.03076
Secure Client UI	5.0.00850
Secure Endpoint	8.2.3.30119
Umbrella	5.0.03076

...we pause for another plug

Paul Carco
Technical Marketing

Unified Endpoint Security: Cisco Secure Client & XDR Lab

LABSEC-2852

Walk-in Lab

Bernie Clairmont
Product Solution Architect

Getting Started with ThousandEyes in IT Operation

IBOBS-2013

Thursday, June 12

Fay-Ann Lee
Technical Marketing

Cisco's SASE Approach – Unifying Networking, Identity and Security

BRKSEC-2286

Thursday, June 12

TL;DR

- AnyConnect is now Secure Client
- CSC = Cisco Secure Client
- Yes, you can still do it.
- You can do a whole lot more.
- We’ve added Cloud Management
- We’ve added new modules

Agenda

01 CSC Overview

02 CSC Architecture

03 Cloud Deployment & Management

04 Upgrading to CSC

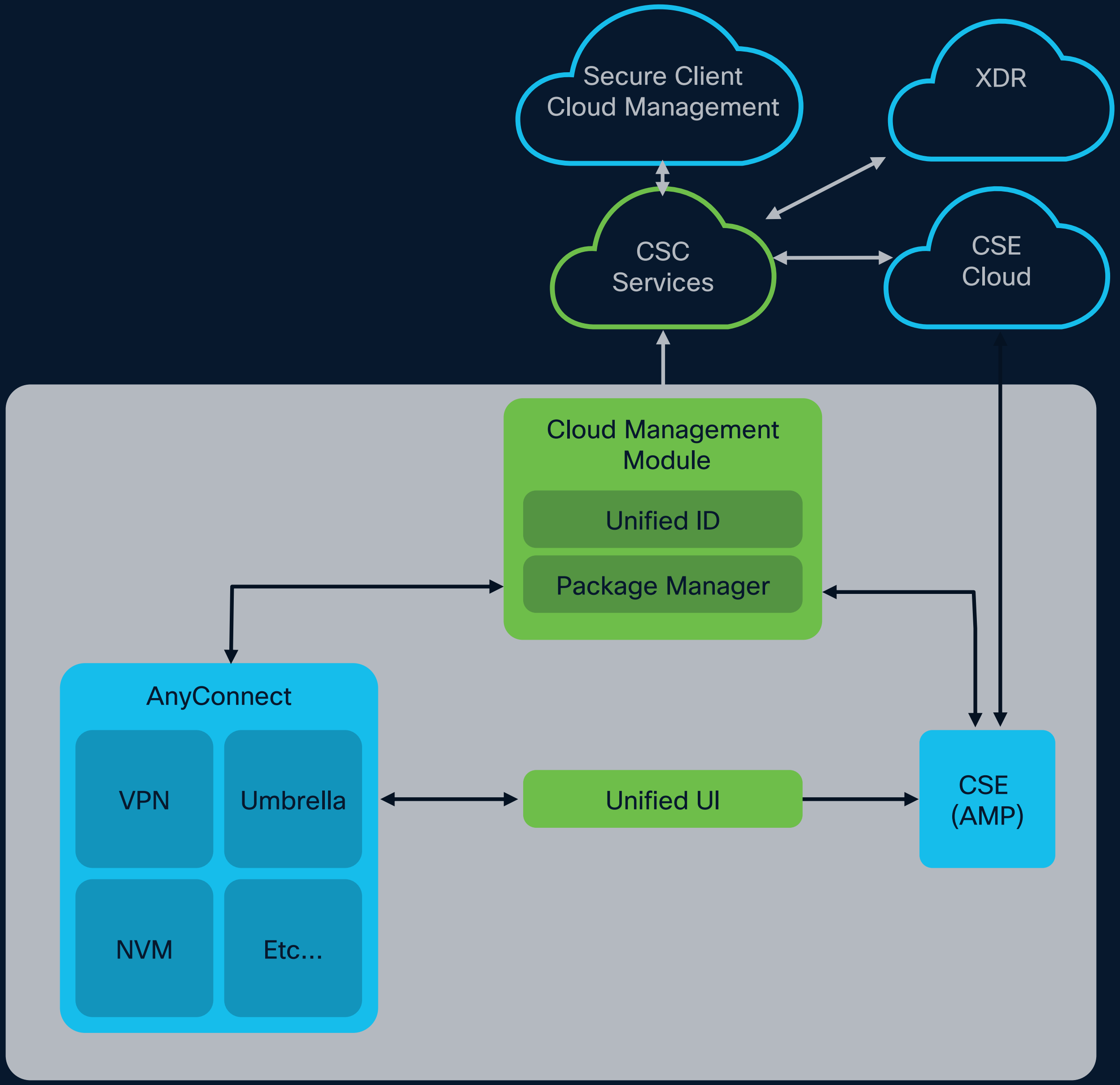
05 FAQs, Tips and Tricks

CSC Architecture

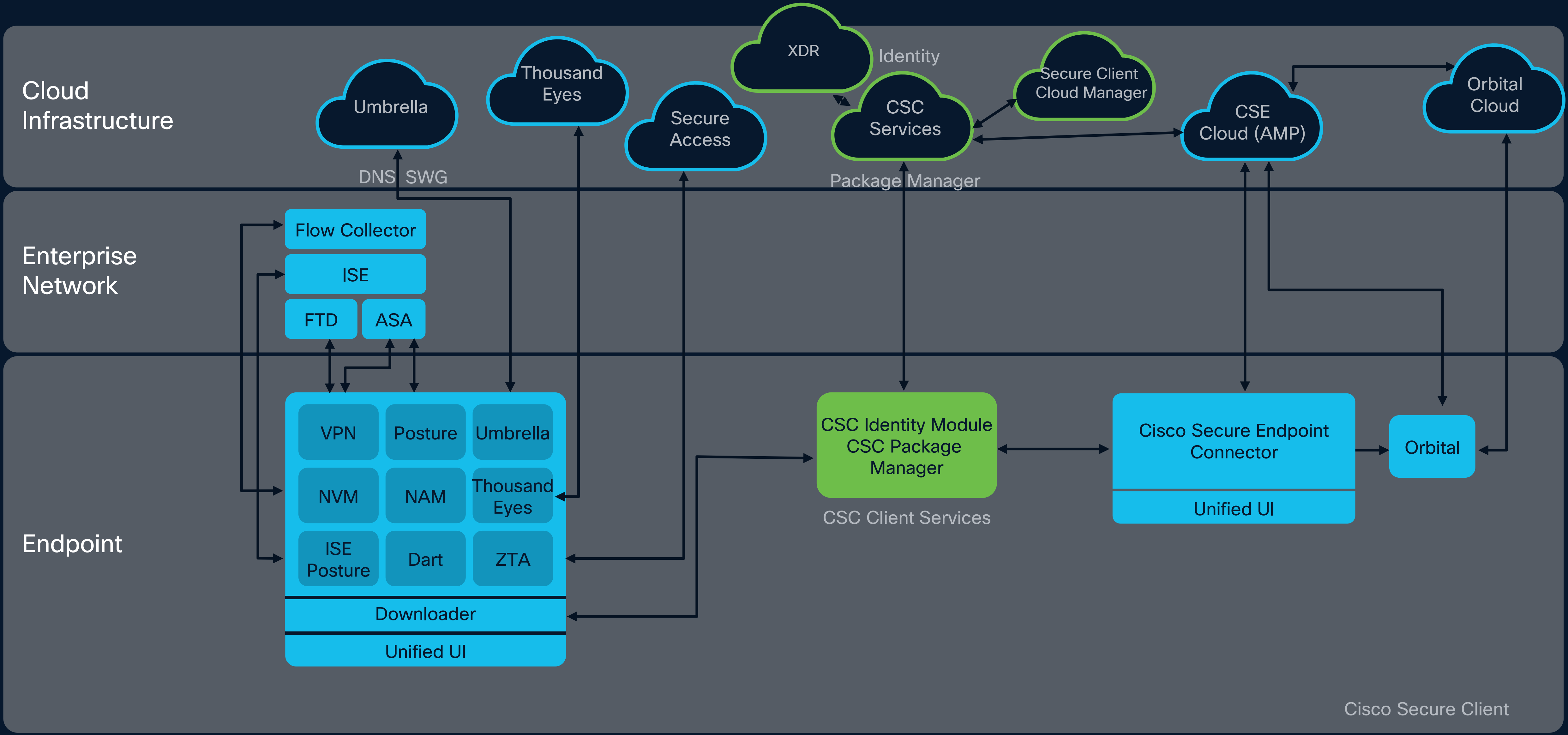
Cisco Secure Client

Architectural Overview

- Existing components that did not fundamentally change from AC
- New components
- Components that enable the Cisco Secure Client



Cisco Secure Client – Architecture



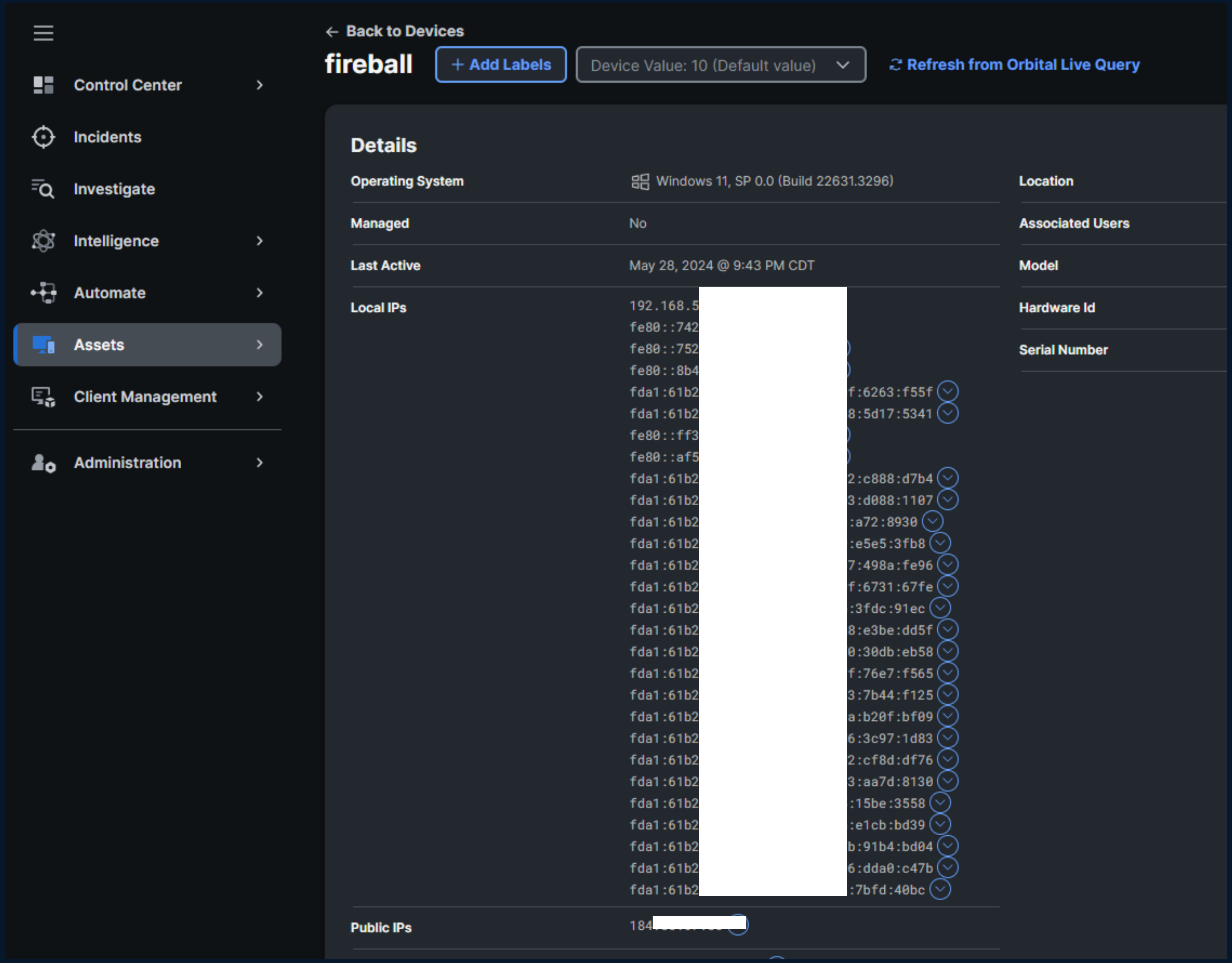
Cisco Secure Client

Identification madness

Unified ID – Device Insights

- AnyConnect Identifier (ACID)
- Secure Endpoint / Orbital UID
- Umbrella – Origin ID
- Hardware & Software Attributes

- Globally Unique Cloud Identifier
- Maintains on reinstall, etc



fireball

Details

Operating System	Windows 11, SP 0.0 (Build 22631.3296)
Managed	No
Last Active	May 28, 2024 @ 9:43 PM CDT
Local IPs	see below
Public IPs	184 [redacted]

```
192.168.5  [redacted]
fe80::742
fe80::752
fe80::8b4
fda1:61b2                    f:6263:f55f
fda1:61b2                    8:5d17:5341
fe80::ff3
fe80::af5
fda1:61b2                    2:c888:d7b4
fda1:61b2                    3:d088:1107
fda1:61b2                    :a72:8930
fda1:61b2                    :e5e5:3fb8
fda1:61b2                    7:498a:fe96
fda1:61b2                    f:6731:67fe
fda1:61b2                    :3fdc:91ec
fda1:61b2                    8:e3be:dd5f
fda1:61b2                    0:30db:eb58
fda1:61b2                    f:76e7:f565
fda1:61b2                    3:7b44:f125
fda1:61b2                    a:b20f:bf09
fda1:61b2                    6:3c97:1d83
fda1:61b2                    2:cf8d:df76
fda1:61b2                    3:aa7d:8130
fda1:61b2                    :15be:3558
fda1:61b2                    :e1cb:bd39
fda1:61b2                    b:91b4:bd04
fda1:61b2                    6:dda0:c47b
fda1:61b2                    :7bfd:40bc
```

Location

Associated Users

Model

Hardware Id

Serial Number

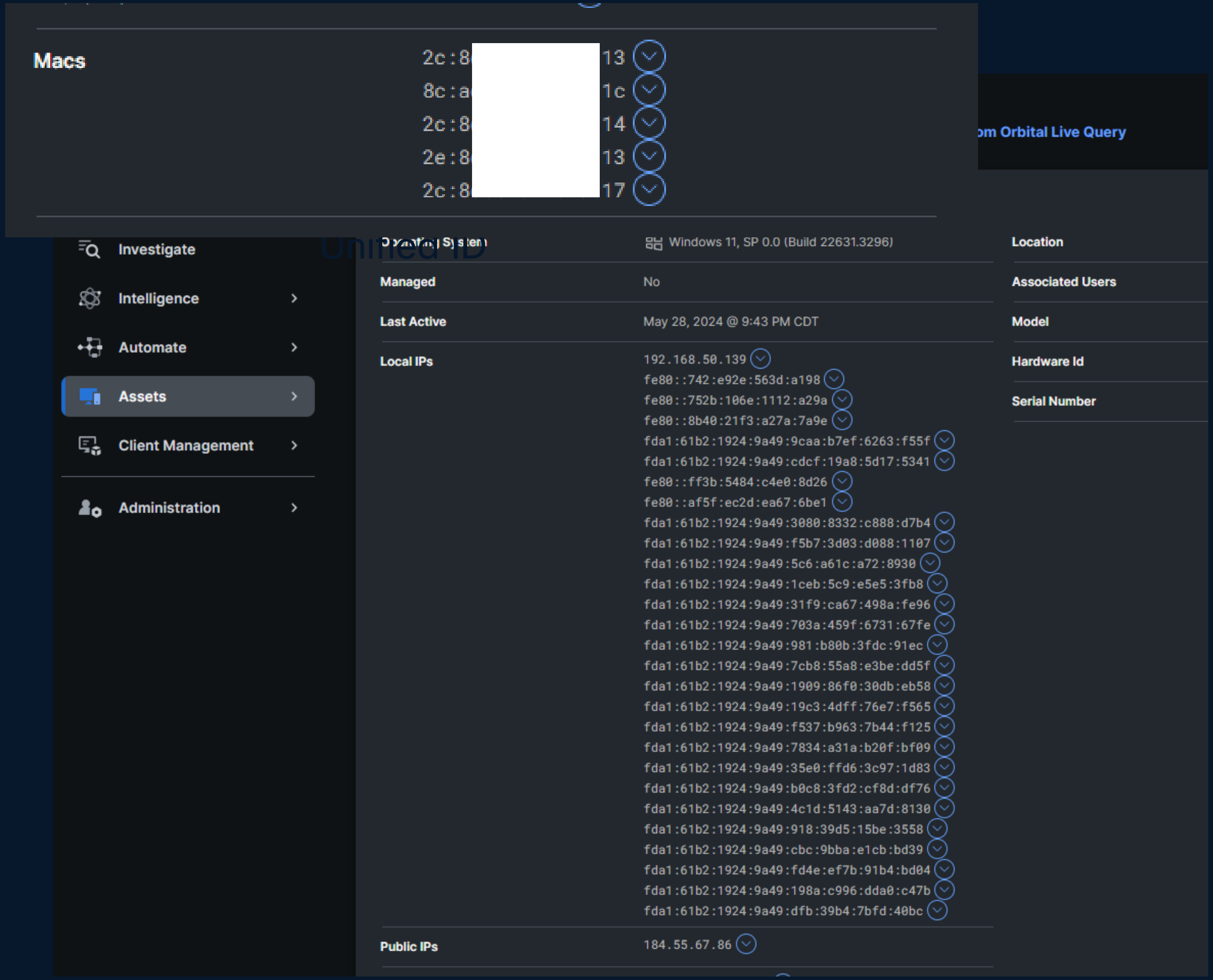
Cisco Secure Client

Identification madness

Unified ID – Device Insights

- AnyConnect Identifier (ACID)
- Secure Endpoint / Orbital UID
- Umbrella – Origin ID
- Hardware & Software Attributes

- Globally Unique Cloud Identifier
- Maintains on reinstall, etc



Macs

2c:8[redacted]13
8c:a[redacted]1c
2c:8[redacted]14
2e:8[redacted]13
2c:8[redacted]17

Operating System	Windows 11, SP 0.0 (Build 22631.3296)	**Location**
Managed	No	**Associated Users**
Last Active	May 28, 2024 @ 9:43 PM CDT	**Model**
Local IPs	192.168.50.139 fe80::742:e92e:563d:a198 fe80::752b:106e:1112:a29a fe80::8b40:21f3:a27a:7a9e fda1:61b2:1924:9a49:9caa:b7ef:6263:f55f fda1:61b2:1924:9a49:cdcf:19a8:5d17:5341 fe80::ff3b:5484:c4e0:8d26 fe80::af5f:ec2d:ea67:6be1 fda1:61b2:1924:9a49:3080:8332:c888:d7b4 fda1:61b2:1924:9a49:f5b7:3d03:d088:1107 fda1:61b2:1924:9a49:5c6:a61c:a72:8930 fda1:61b2:1924:9a49:1ceb:5c9:e5e5:3fb8 fda1:61b2:1924:9a49:31f9:ca67:498a:fe96 fda1:61b2:1924:9a49:703a:459f:6731:67fe fda1:61b2:1924:9a49:981:b80b:3fdc:91ec fda1:61b2:1924:9a49:7cb8:55a8:e3be:dd5f fda1:61b2:1924:9a49:1909:86f0:30db:eb58 fda1:61b2:1924:9a49:19c3:4dff:76e7:f565 fda1:61b2:1924:9a49:f537:b963:7b44:f125 fda1:61b2:1924:9a49:7834:a31a:b20f:bf09 fda1:61b2:1924:9a49:35e0:ffd6:3c97:1d83 fda1:61b2:1924:9a49:b0c8:3fd2:cf8d:df76 fda1:61b2:1924:9a49:4c1d:5143:aa7d:8130 fda1:61b2:1924:9a49:918:39d5:15be:3558 fda1:61b2:1924:9a49:cbc:9bba:e1cb:bd39 fda1:61b2:1924:9a49:fd4e:ef7b:91b4:bd04 fda1:61b2:1924:9a49:198a:c996:dda0:c47b fda1:61b2:1924:9a49:dfb:39b4:7bfd:40bc	**Hardware Id**
		Serial Number
Public IPs	184.55.67.86	

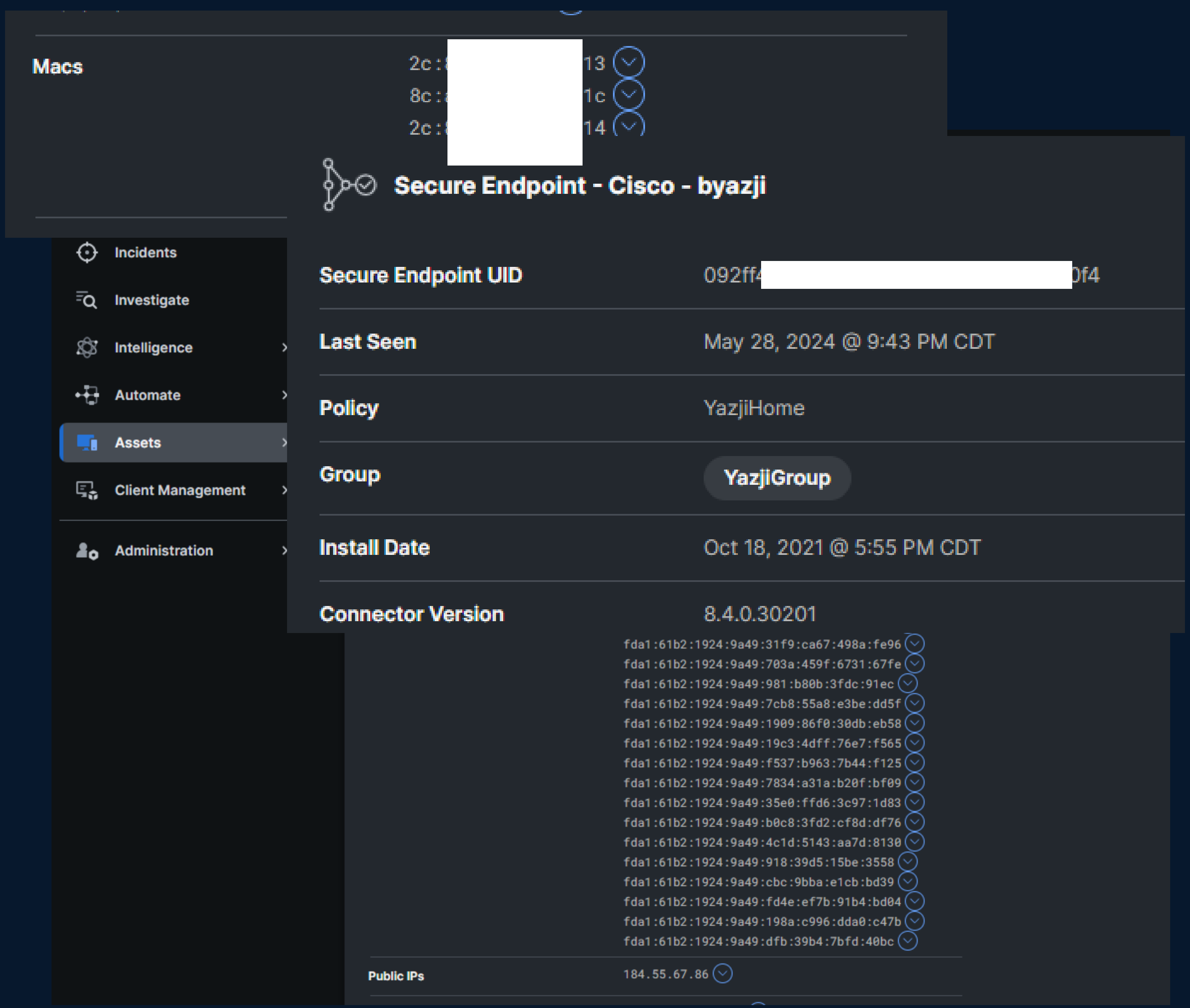
Cisco Secure Client

Identification madness

Unified ID – Device Insights

- AnyConnect Identifier (ACID)
- Secure Endpoint / Orbital UID
- Umbrella – Origin ID
- Hardware & Software Attributes

- Globally Unique Cloud Identifier
- Maintains on reinstall, etc



Macs
2c:[redacted]13
8c:1c
2c:14

Secure Endpoint - Cisco - byazji

Secure Endpoint UID	092ff4[redacted]0f4
Last Seen	May 28, 2024 @ 9:43 PM CDT
Policy	YazjiHome
Group	YazjiGroup
Install Date	Oct 18, 2021 @ 5:55 PM CDT
Connector Version	8.4.0.30201

```
fda1:61b2:1924:9a49:31f9:ca67:498a:fe96
fda1:61b2:1924:9a49:703a:459f:6731:67fe
fda1:61b2:1924:9a49:981:b80b:3fdc:91ec
fda1:61b2:1924:9a49:7cb8:55a8:e3be:dd5f
fda1:61b2:1924:9a49:1909:86f0:30db:eb58
fda1:61b2:1924:9a49:19c3:4dff:76e7:f565
fda1:61b2:1924:9a49:f537:b963:7b44:f125
fda1:61b2:1924:9a49:7834:a31a:b20f:bf09
fda1:61b2:1924:9a49:35e0:ffd6:3c97:1d83
fda1:61b2:1924:9a49:b0c8:3fd2:cf8d:df76
fda1:61b2:1924:9a49:4c1d:5143:aa7d:8130
fda1:61b2:1924:9a49:918:39d5:15be:3558
fda1:61b2:1924:9a49:cbc:9bba:e1cb:bd39
fda1:61b2:1924:9a49:fd4e:ef7b:91b4:bd04
fda1:61b2:1924:9a49:198a:c996:dda0:c47b
fda1:61b2:1924:9a49:dfb:39b4:7bfd:40bc
```

Public IPs 184.55.67.86

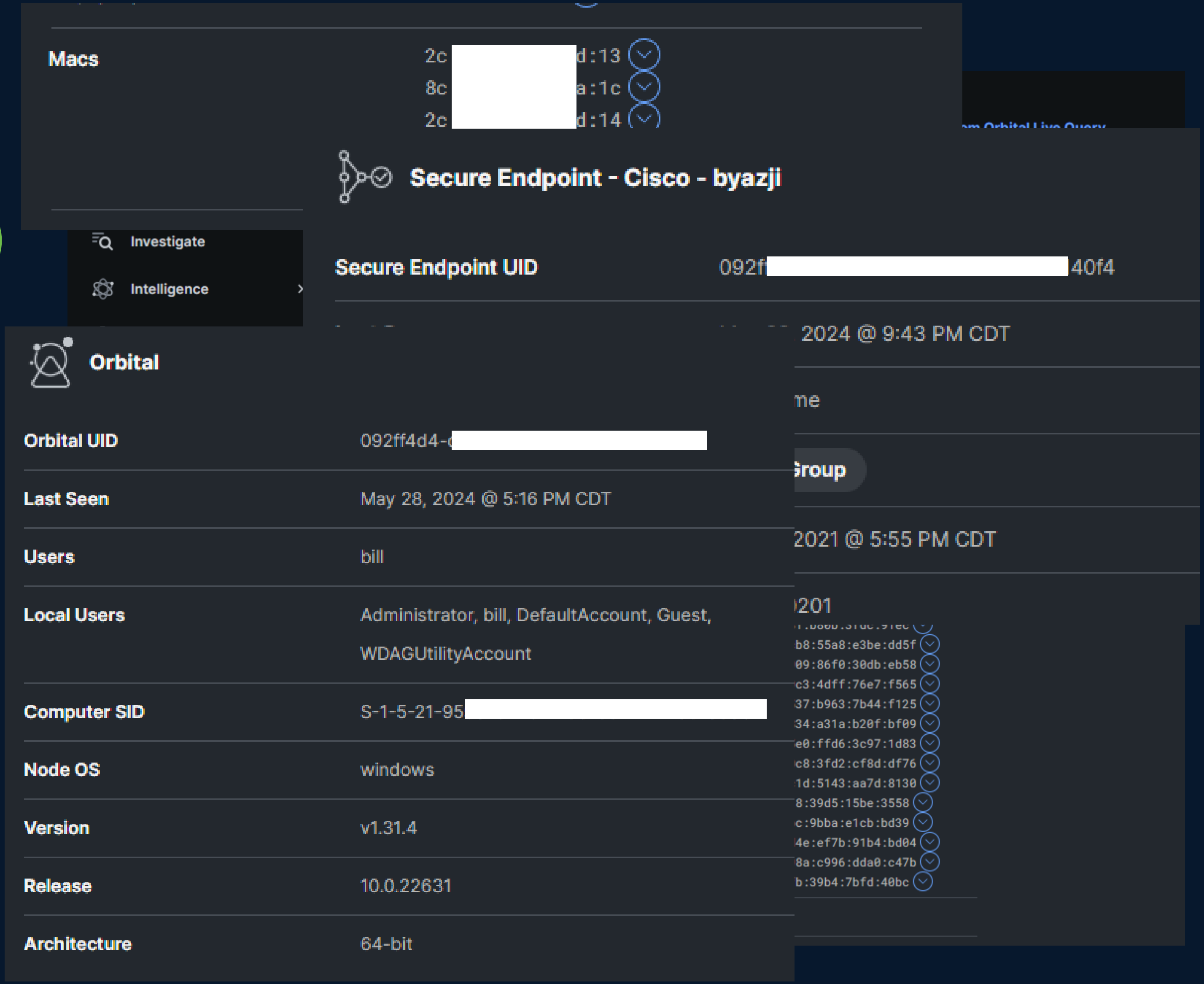
Cisco Secure Client

Identification madness

Unified ID – Device Insights

- AnyConnect Identifier (ACID)
- Secure Endpoint / Orbital UID
- Umbrella – Origin ID
- Hardware & Software Attributes

- Globally Unique Cloud Identifier
- Maintains on reinstall, etc



Macs: 2c[redacted]d:13, 8c[redacted]a:1c, 2c[redacted]d:14

Secure Endpoint - Cisco - byazji

Secure Endpoint UID: 092f[redacted]40f4

2024 @ 9:43 PM CDT

me

Group

2021 @ 5:55 PM CDT

201

```
b8:55a8:e3be:dd5f
09:86f0:30db:eb58
c3:4dff:76e7:f565
37:b963:7b44:f125
34:a31a:b20f:bf09
e0:ffd6:3c97:1d83
c8:3fd2:cf8d:df76
1d:5143:aa7d:8130
8:39d5:15be:3558
c:9bba:e1cb:bd39
4e:ef7b:91b4:bd04
8a:c996:dda0:c47b
b:39b4:7bfd:40bc
```

Orbital

Orbital UID	092ff4d4-[redacted]
Last Seen	May 28, 2024 @ 5:16 PM CDT
Users	bill
Local Users	Administrator, bill, DefaultAccount, Guest, WDAGUtilityAccount
Computer SID	S-1-5-21-95[redacted]
Node OS	windows
Version	v1.31.4
Release	10.0.22631
Architecture	64-bit

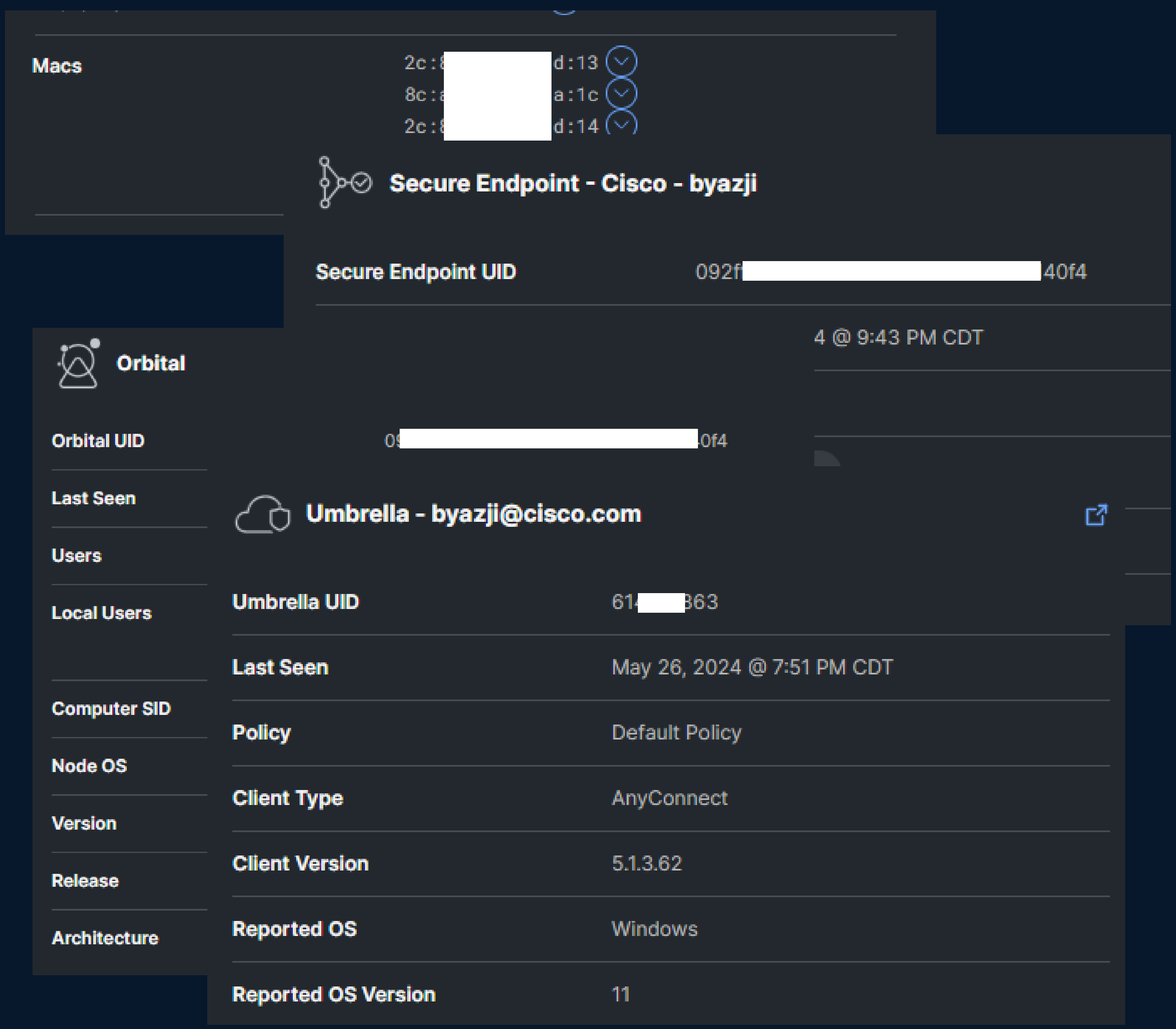
Cisco Secure Client

Identification madness

Unified ID – Device Insights

- AnyConnect Identifier (ACID)
- Secure Endpoint / Orbital UID
- Umbrella – Origin ID
- Hardware & Software Attributes

- Globally Unique Cloud Identifier
- Maintains on reinstall, etc



Macs
2c:[redacted]d:13
8c:[redacted]a:1c
2c:[redacted]d:14

Secure Endpoint - Cisco - byazji

Secure Endpoint UID	092f[redacted]40f4
	4 @ 9:43 PM CDT

Orbital

Orbital UID	0[redacted]0f4
Last Seen	
Users	
Local Users	
Computer SID	
Node OS	
Version	
Release	
Architecture	

Umbrella - byazji@cisco.com

Umbrella UID	61[redacted]363
Last Seen	May 26, 2024 @ 7:51 PM CDT
Policy	Default Policy
Client Type	AnyConnect
Client Version	5.1.3.62
Reported OS	Windows
Reported OS Version	11

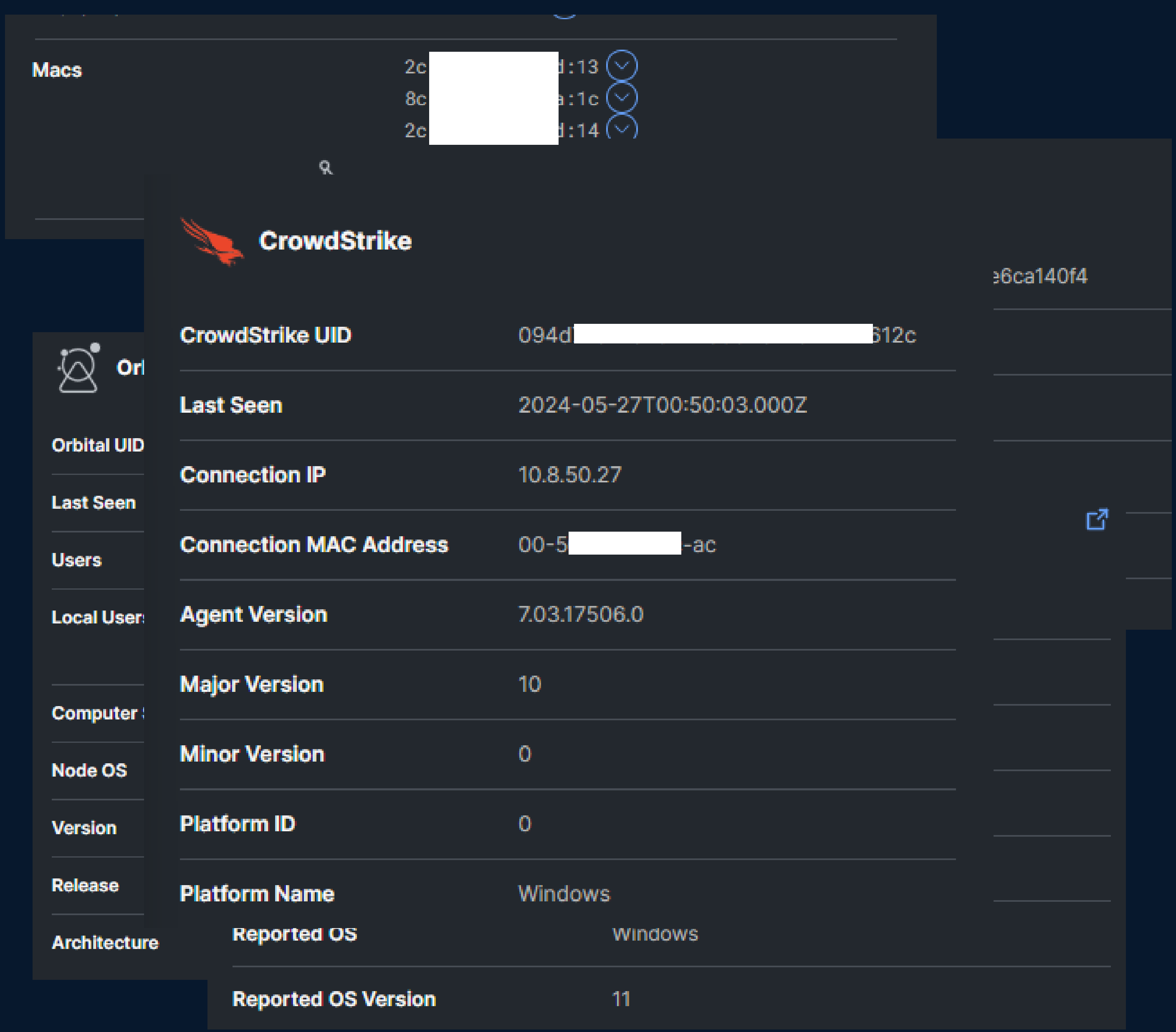
Cisco Secure Client

Identification madness

Unified ID – Device Insights

- AnyConnect Identifier (ACID)
- Secure Endpoint / Orbital UID
- Umbrella – Origin ID
- Hardware & Software Attributes

- Globally Unique Cloud Identifier
- Maintains on reinstall, etc



Macs 2c[redacted]d:13
8c[redacted]a:1c
2c[redacted]d:14

e6ca140f4

Orl

Orbital UID

Last Seen

Users

Local User

Computer

Node OS

Version

Release

Architecture

CrowdStrike

CrowdStrike UID	094d[redacted]612c
Last Seen	2024-05-27T00:50:03.000Z
Connection IP	10.8.50.27
Connection MAC Address	00-5[redacted]-ac
Agent Version	7.03.17506.0
Major Version	10
Minor Version	0
Platform ID	0
Platform Name	Windows
Reported OS	Windows
Reported OS Version	11

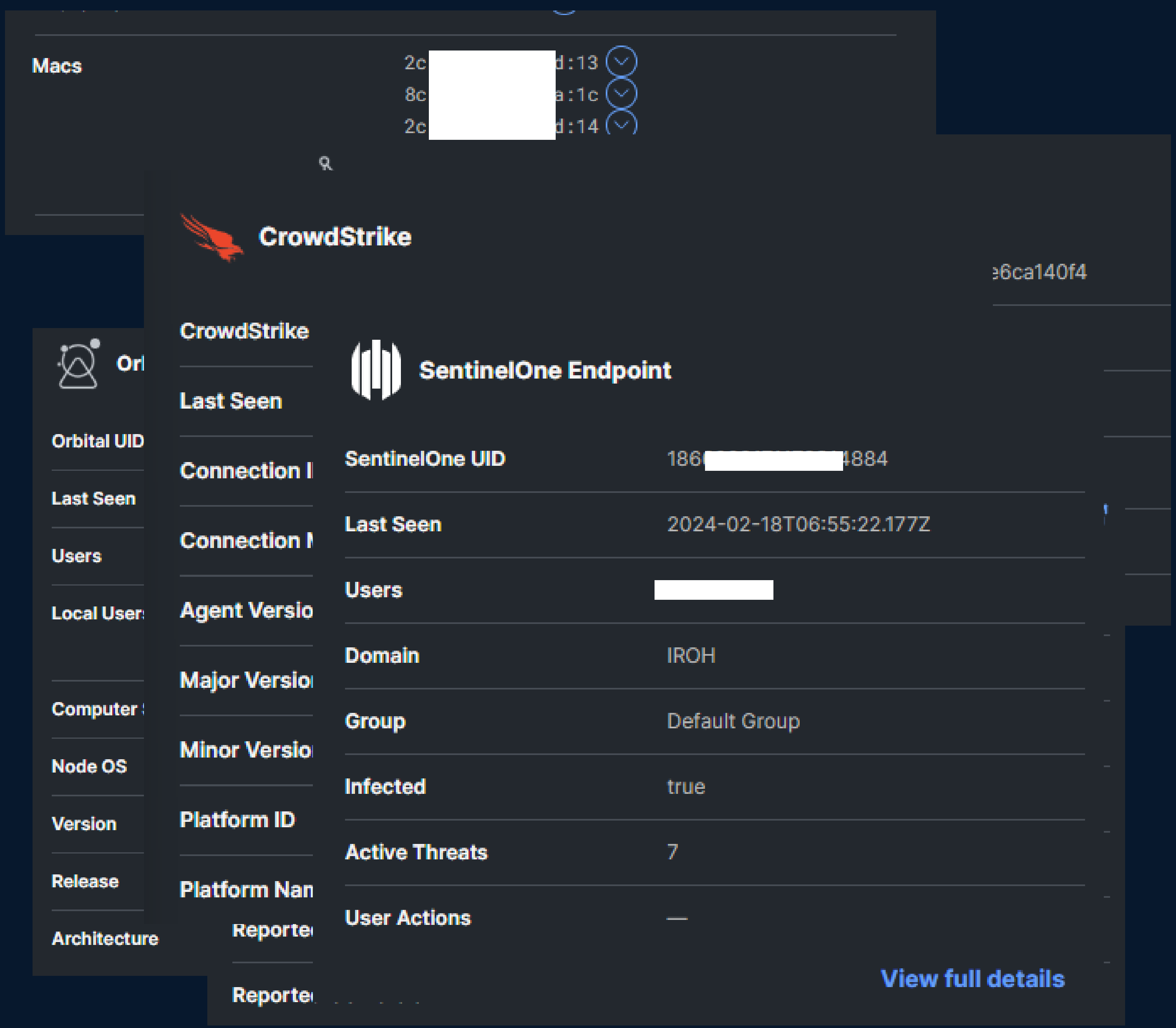
Cisco Secure Client

Identification madness

Unified ID – Device Insights

- AnyConnect Identifier (ACID)
- Secure Endpoint / Orbital UID
- Umbrella – Origin ID
- Hardware & Software Attributes

- Globally Unique Cloud Identifier
- Maintains on reinstall, etc



Macs 2c[redacted]d:13
8c[redacted]a:1c
2c[redacted]d:14

e6ca140f4

Orl

Orbital UID

Last Seen

Users

Local User

Computer

Node OS

Version

Release

Architecture

CrowdStrike

CrowdStrike

Last Seen

Connection I

Connection I

Agent Versio

Major Versio

Minor Versio

Platform ID

Platform Nan

Reporte

Reporte

SentinelOne Endpoint

SentinelOne UID	186[redacted]4884
Last Seen	2024-02-18T06:55:22.177Z
Users	[redacted]
Domain	IROH
Group	Default Group
Infected	true
Active Threats	7
User Actions	—

View full details

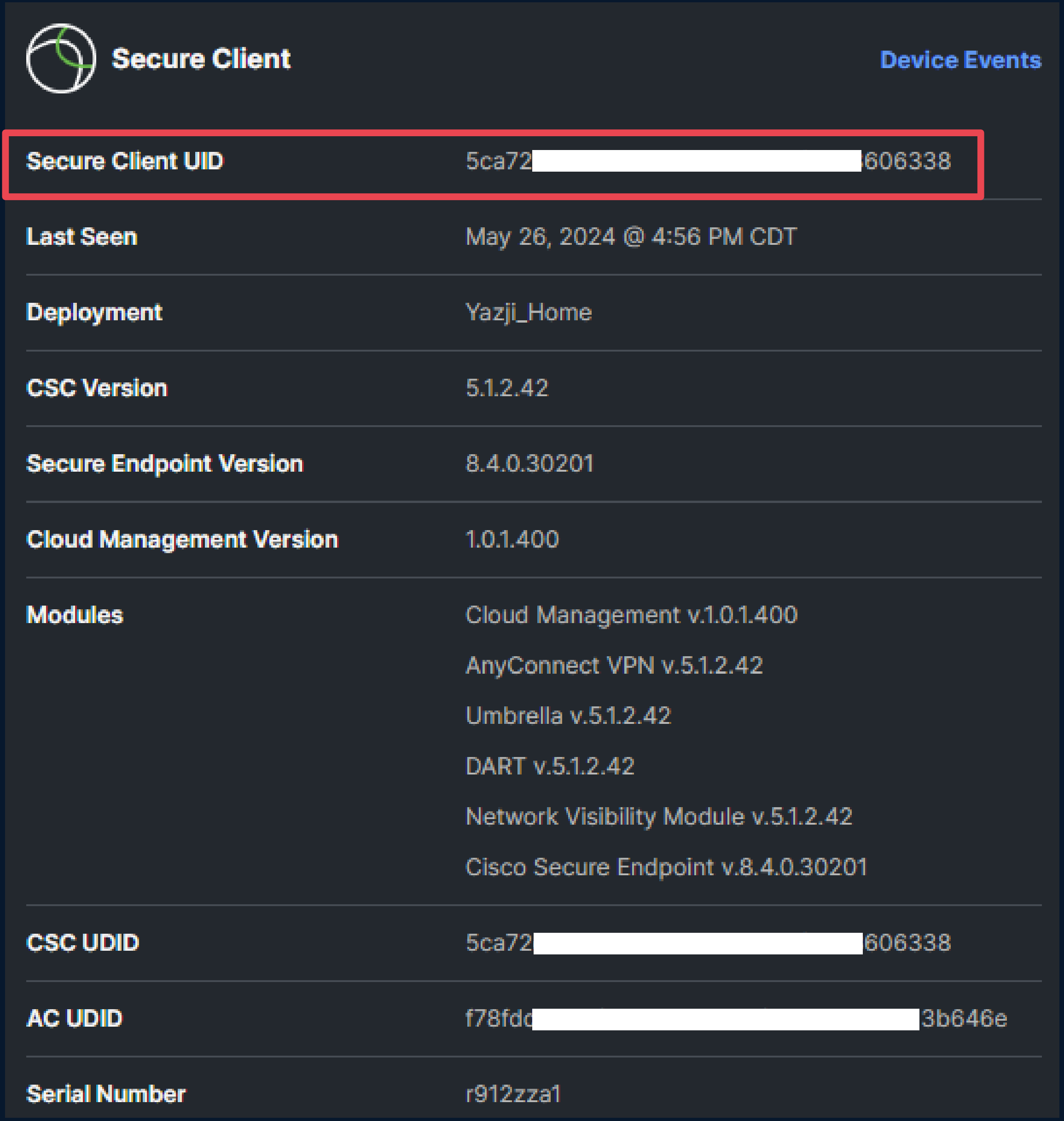
Cisco Secure Client

Secure Client UID

Unified ID – Device Insights

- AnyConnect Identifier (ACID)
- Secure Endpoint / Orbital UID
- Umbrella – Origin ID
- Hardware & Software Attributes

- Globally Unique Cloud Identifier
- Maintains on reinstall, etc



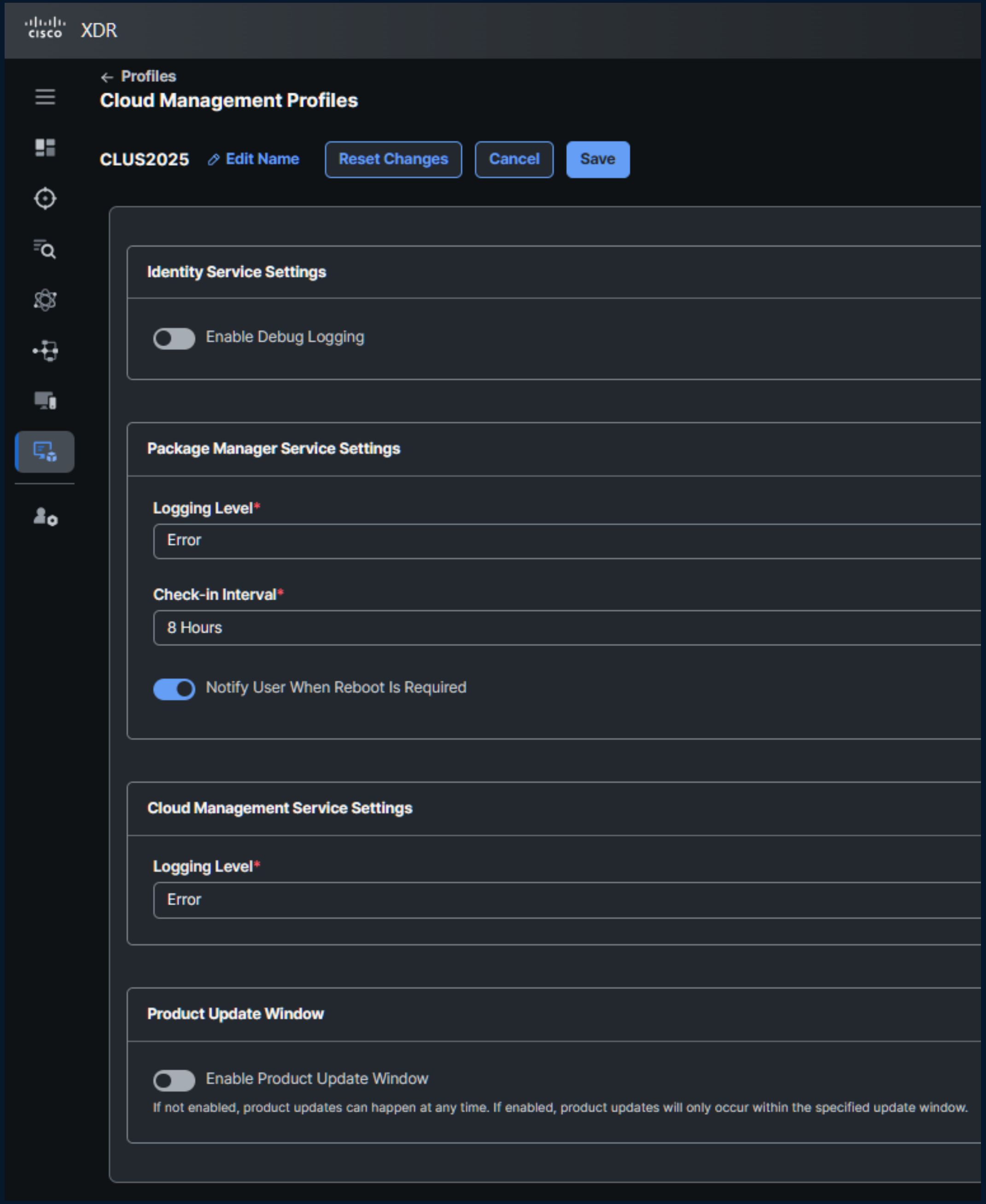
Secure Client UID	5ca72[redacted]606338
Last Seen	May 26, 2024 @ 4:56 PM CDT
Deployment	Yazji_Home
CSC Version	5.1.2.42
Secure Endpoint Version	8.4.0.30201
Cloud Management Version	1.0.1.400
Modules	Cloud Management v.1.0.1.400 AnyConnect VPN v.5.1.2.42 Umbrella v.5.1.2.42 DART v.5.1.2.42 Network Visibility Module v.5.1.2.42 Cisco Secure Endpoint v.8.4.0.30201
CSC UDID	5ca72[redacted]606338
AC UDID	f78fdd[redacted]3b646e
Serial Number	r912zza1

Cisco Secure Client

Client Management Module

Package Manager

- Check-in timer to cloud
- Looks for new manifest
- Installs based on cloud detail/configuration/update windows



Cloud Management Profiles

CLUS2025

Identity Service Settings

Enable Debug Logging

Package Manager Service Settings

Logging Level*: Error

Check-in Interval*: 8 Hours

Notify User When Reboot Is Required

Cloud Management Service Settings

Logging Level*: Error

Product Update Window

Enable Product Update Window

If not enabled, product updates can happen at any time. If enabled, product updates will only occur within the specified update window.

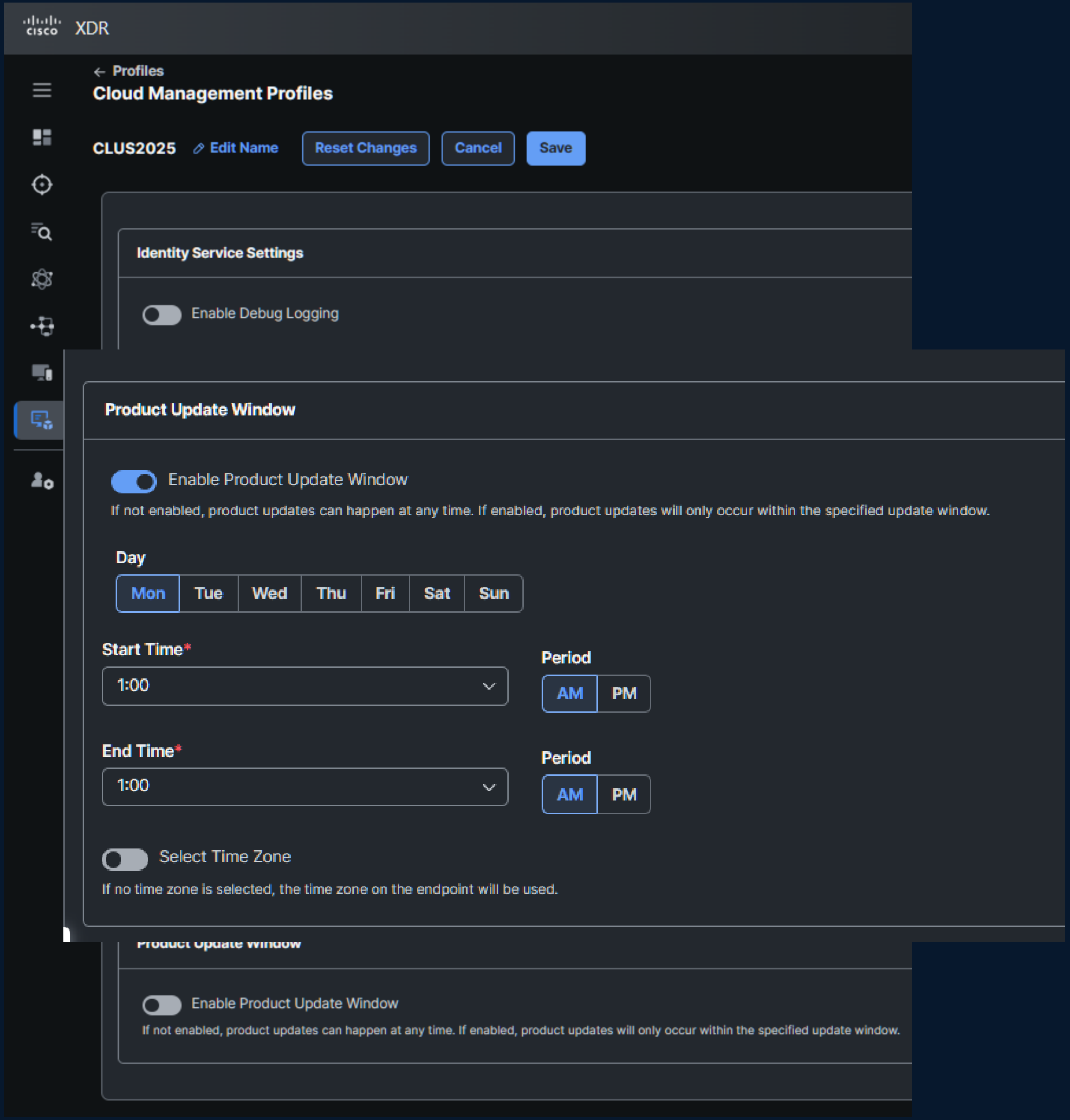
Cisco Secure Client

Client Management Module

Package Manager

- Check-in timer to cloud
- Looks for new manifest
- Installs based on cloud detail/configuration/update windows

- Update Window Configuration
  - Leveraged for **Installation Window** for Network Installer & Module updates
  - If CM checks in with the cloud within that time window, the updates will be pushed to the endpoint
  - All cloud controlled!



Identity Service Settings

Enable Debug Logging

Product Update Window

Enable Product Update Window

If not enabled, product updates can happen at any time. If enabled, product updates will only occur within the specified update window.

Day: [✓ Mon] Tue Wed Thu Fri Sat Sun

Start Time*: 1:00 — Period: [✓ AM] PM

End Time*: 1:00 — Period: [✓ AM] PM

Select Time Zone

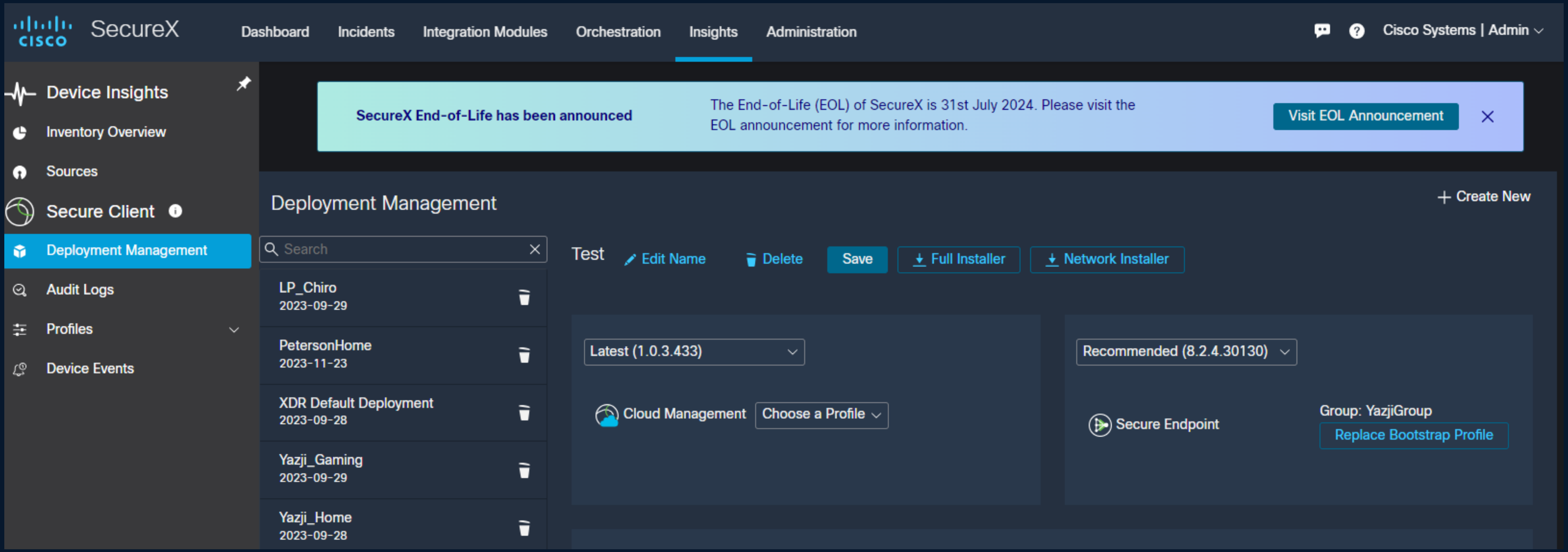
If no time zone is selected, the time zone on the endpoint will be used.

Product Update Window

Enable Product Update Window

If not enabled, product updates can happen at any time. If enabled, product updates will only occur within the specified update window.

SecureX Who? [EOL 2024, left for posterity]



SecureX End-of-Life has been announced

The End-of-Life (EOL) of SecureX is 31st July 2024. Please visit the EOL announcement for more information.

Test

LP_Chiro 2023-09-29

PetersonHome 2023-11-23

XDR Default Deployment 2023-09-28

Yazji_Gaming 2023-09-29

Yazji_Home 2023-09-28

Latest (1.0.3.433)

Cloud Management: Choose a Profile

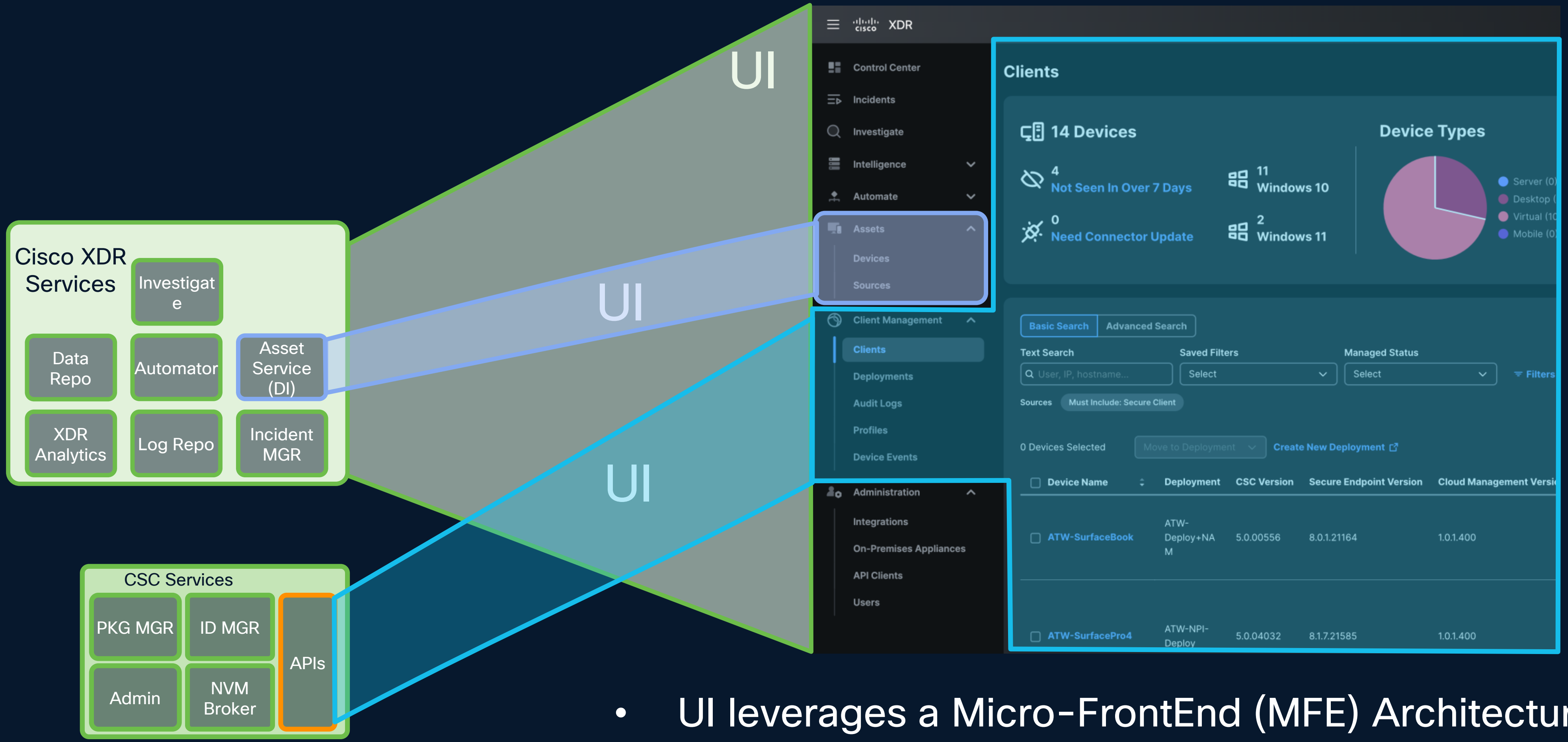
Recommended (8.2.4.30130)

Secure Endpoint

Group: YazjiGroup

- https://www.cisco.com/c/en/us/products/collateral/security/securex/securex-eol.html
- https://blogs.cisco.com/security/accessing-secure-client-cloud-management-after-the-securex-eol
- https://video.cisco.com/detail/video/6353048690112

Cloud Management Architecture



Clients

14 Devices

4 Not Seen In Over 7 Days

11 Windows 10

0 Need Connector Update

2 Windows 11

Text Search: User, IP, hostname...

Saved Filters: Select

Managed Status: Select

Sources: Must Include: Secure Client

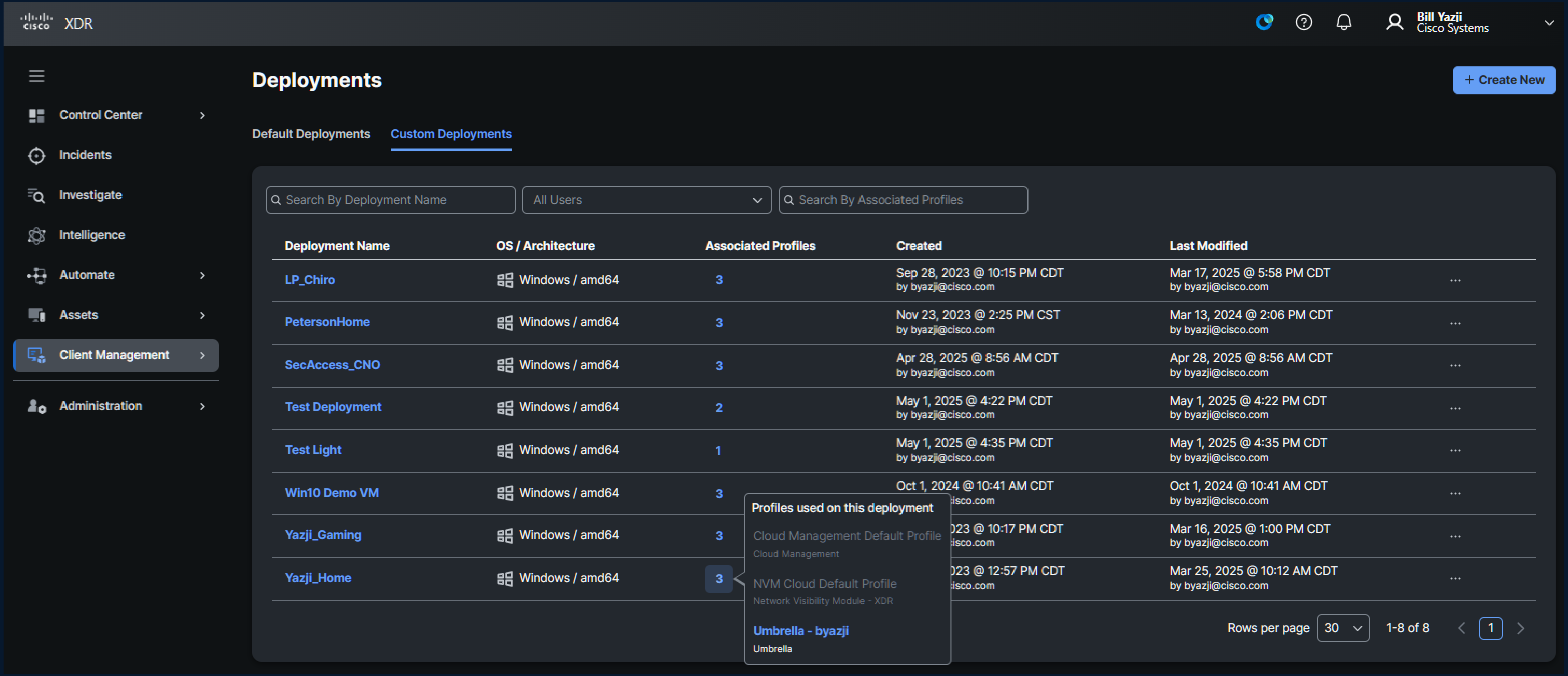
0 Devices Selected

□ Device Name	Deployment	CSC Version	Secure Endpoint Version	Cloud Management Versi
□ ATW-SurfaceBook	ATW-Deploy+NAM	5.0.00556	8.0.1.21164	1.0.1.400
□ ATW-SurfacePro4	ATW-NPI-Deploy	5.0.04032	8.1.7.21585	1.0.1.400

- UI leverages a Micro-FrontEnd (MFE) Architecture
- UI components may run from any service & be part of a single UI Experience

CSC Cloud Management

Today – In XDR



Deployments

Default Deployments | Custom Deployments

Deployment Name	OS / Architecture	Associated Profiles	Created	Last Modified
LP_Chiro	Windows / amd64	3	Sep 28, 2023 @ 10:15 PM CDT by byazji@cisco.com	Mar 17, 2025 @ 5:58 PM CDT by byazji@cisco.com
PetersonHome	Windows / amd64	3	Nov 23, 2023 @ 2:25 PM CST by byazji@cisco.com	Mar 13, 2024 @ 2:06 PM CDT by byazji@cisco.com
SecAccess_CNO	Windows / amd64	3	Apr 28, 2025 @ 8:56 AM CDT by byazji@cisco.com	Apr 28, 2025 @ 8:56 AM CDT by byazji@cisco.com
Test Deployment	Windows / amd64	2	May 1, 2025 @ 4:22 PM CDT by byazji@cisco.com	May 1, 2025 @ 4:22 PM CDT by byazji@cisco.com
Test Light	Windows / amd64	1	May 1, 2025 @ 4:35 PM CDT by byazji@cisco.com	May 1, 2025 @ 4:35 PM CDT by byazji@cisco.com
Win10 Demo VM	Windows / amd64	3	Oct 1, 2024 @ 10:41 AM CDT isco.com	Oct 1, 2024 @ 10:41 AM CDT by byazji@cisco.com
Yazji_Gaming	Windows / amd64	3	023 @ 10:17 PM CDT isco.com	Mar 16, 2025 @ 1:00 PM CDT by byazji@cisco.com
Yazji_Home	Windows / amd64	3	023 @ 12:57 PM CDT isco.com	Mar 25, 2025 @ 10:12 AM CDT by byazji@cisco.com

Profiles used on this deployment

Cloud Management Default Profile
Cloud Management

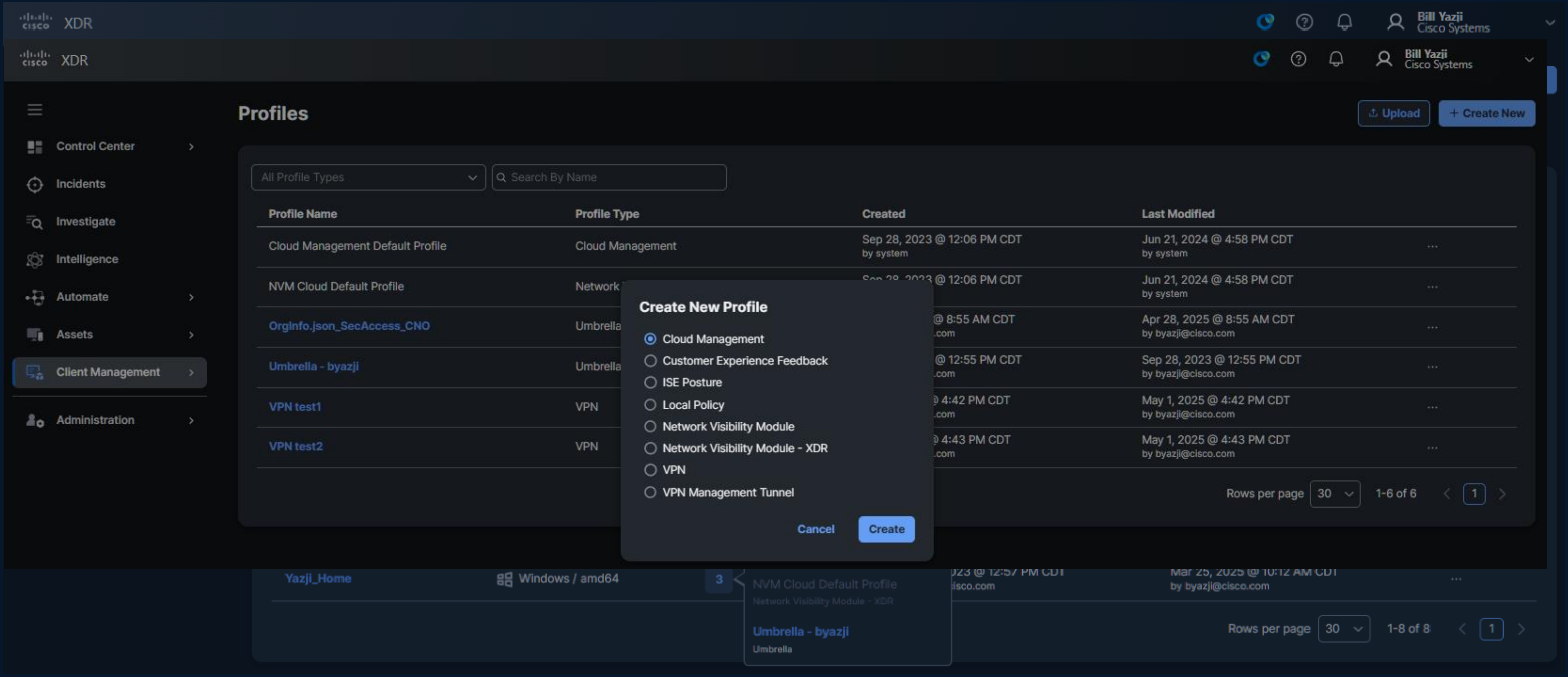
NVM Cloud Default Profile
Network Visibility Module - XDR

Umbrella - byazji
Umbrella

Rows per page 30 1-8 of 8 1

CSC Cloud Management

Today – In XDR



Profiles

Profile Name	Profile Type	Created	Last Modified
Cloud Management Default Profile	Cloud Management	Sep 28, 2023 @ 12:06 PM CDT by system	Jun 21, 2024 @ 4:58 PM CDT by system
NVM Cloud Default Profile	Network	Sep 28, 2023 @ 12:06 PM CDT	Jun 21, 2024 @ 4:58 PM CDT by system
OrgInfo.json_SecAccess_CNO	Umbrella	@ 8:55 AM CDT .com	Apr 28, 2025 @ 8:55 AM CDT by byazji@cisco.com
Umbrella - byazji	Umbrella	@ 12:55 PM CDT .com	Sep 28, 2023 @ 12:55 PM CDT by byazji@cisco.com
VPN test1	VPN	4:42 PM CDT .com	May 1, 2025 @ 4:42 PM CDT by byazji@cisco.com
VPN test2	VPN	4:43 PM CDT .com	May 1, 2025 @ 4:43 PM CDT by byazji@cisco.com

Rows per page 30 1-6 of 6 1

Create New Profile

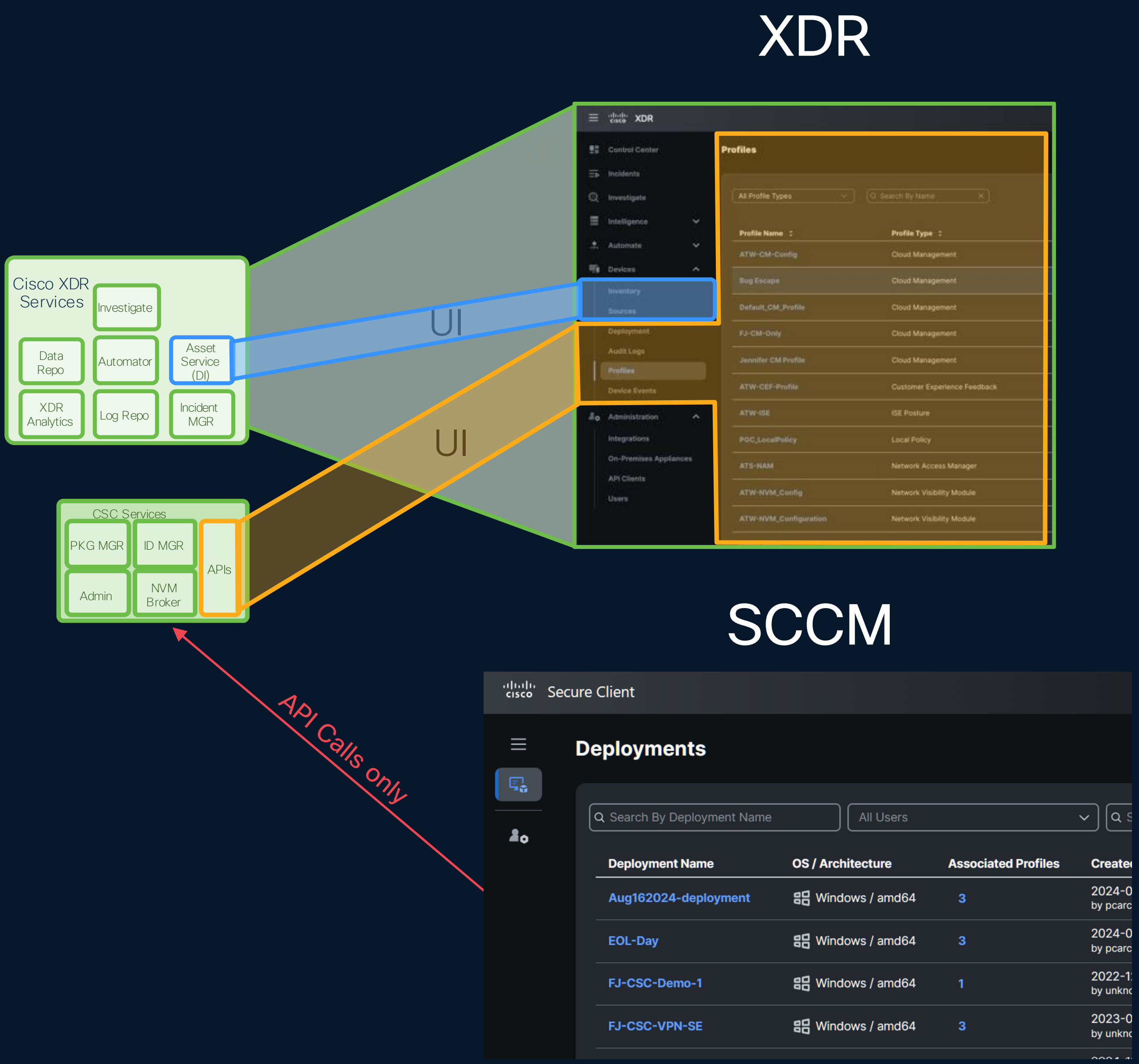
- ● Cloud Management
- ○ Customer Experience Feedback
- ○ ISE Posture
- ○ Local Policy
- ○ Network Visibility Module
- ○ Network Visibility Module - XDR
- ○ VPN
- ○ VPN Management Tunnel

Cancel Create

CSC Cloud Management

For **NON**-XDR users

- Standalone exists *today* in Secure Client Cloud Management (SCCM)
- Secure Access Customers are redirected to SCCM or XDR for CSC Management today.
- Our Micro-FrontEnd (MFE) UI Architecture will enable the CSC management to be pulled into other front-ends in future.



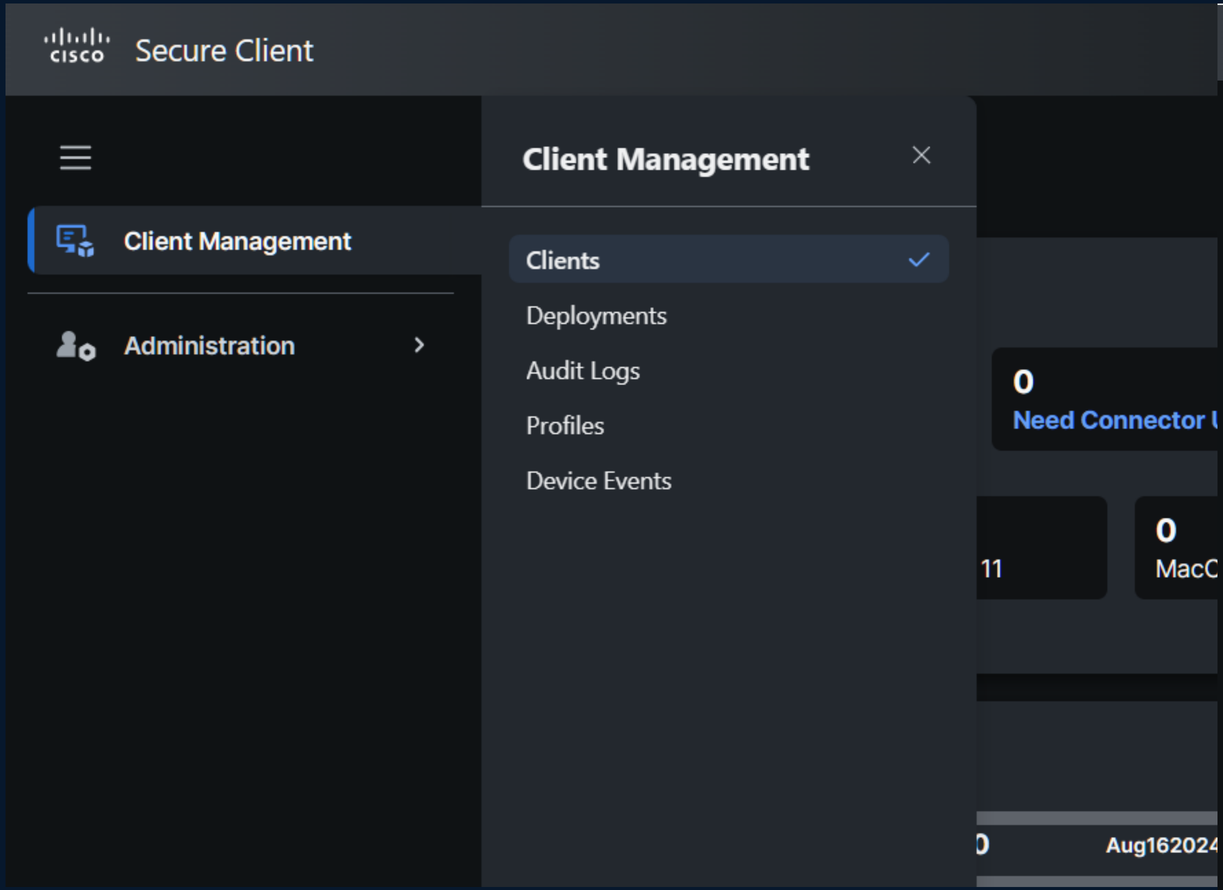
Profiles

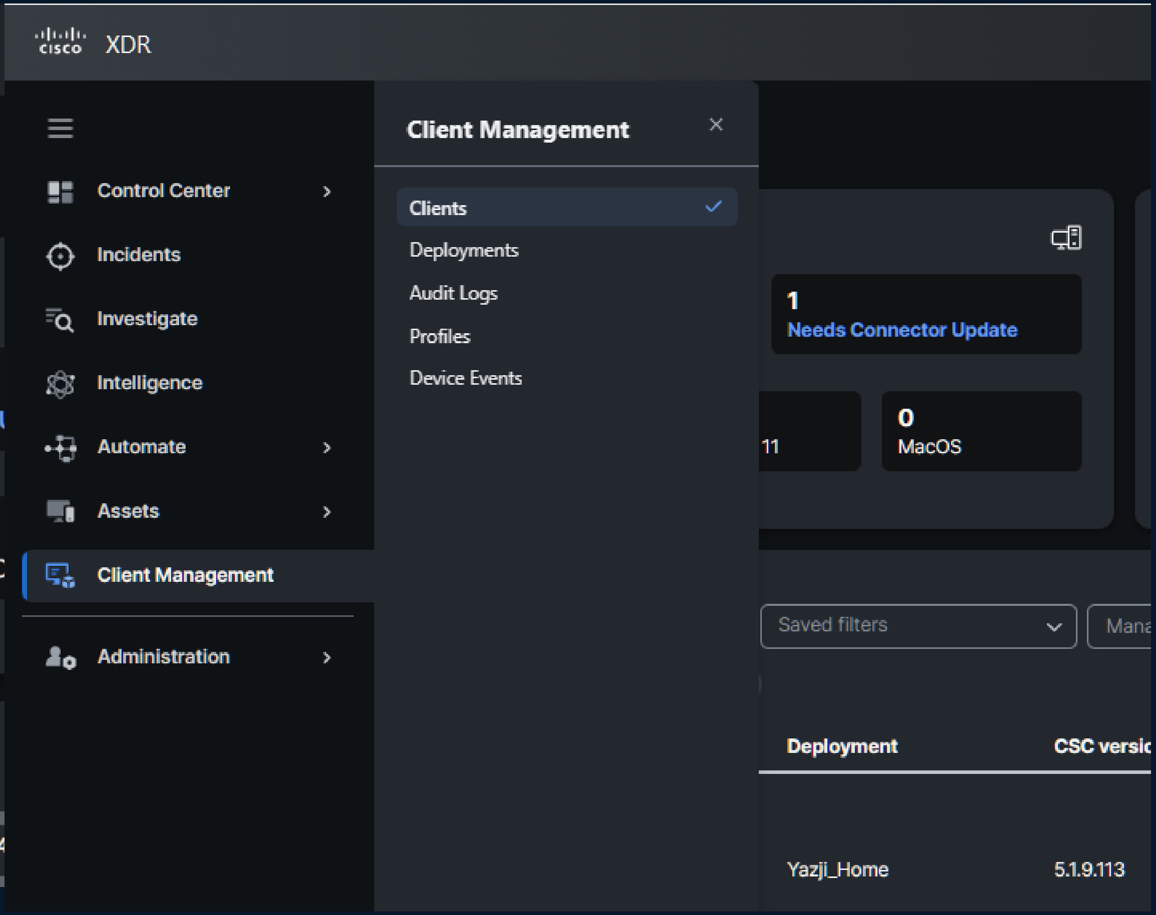
Profile Name	Profile Type
ATW-CM-Config	Cloud Management
Bug Escape	Cloud Management
Default_CM_Profile	Cloud Management
FJ-CM-Only	Cloud Management
Jennifer CM Profile	Cloud Management
ATW-CEF-Profile	Customer Experience Feedback
ATW-ISE	ISE Posture
PGC_LocalPolicy	Local Policy
ATS-NAM	Network Access Manager
ATW-NVM_Config	Network Visibility Module
ATW-NVM_Configuration	Network Visibility Module

Deployments

Deployment Name	OS / Architecture	Associated Profiles	Create
Aug162024-deployment	Windows / amd64	3	2024-0 by pcarc
EOL-Day	Windows / amd64	3	2024-0 by pcarc
FJ-CSC-Demo-1	Windows / amd64	1	2022-1 by unkn
FJ-CSC-VPN-SE	Windows / amd64	3	2023-0 by unkn

SCCM and XDR – Identical User Interfaces





https://secure-client.us.security.cisco.com/

https://xdr.us.security.cisco.com/

I ~~want~~ need Cloud Management... how do I get it?

- Do you have Cisco XDR already?
  - Client Management is included in XDR and must be managed within XDR
- Wait, we didn’t purchase XDR?!
  - Buy XDR
  - .... Or Client Management is also a no-cost entitlement for non-XDR customers
- How can I get standalone Cloud Management?
  - https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/request-scm-tenant.pdf

Open a TAC Case

Product: XDR - Administration

Request a Secure Client Cloud Management tenant be provisioned

Agenda

01 CSC Overview

02 CSC Architecture

03 Cloud Deployment & Management

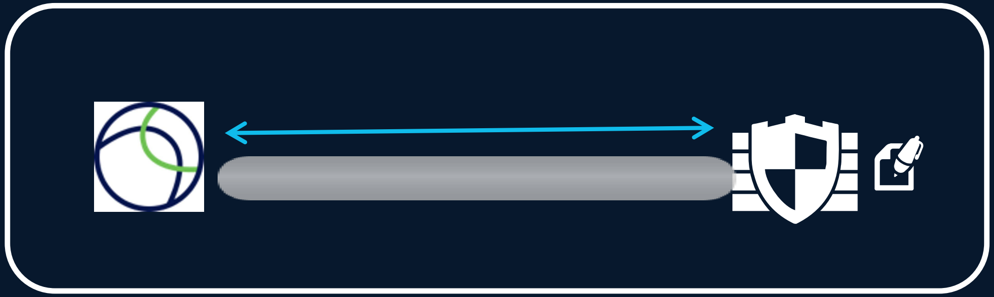
04 Upgrading to CSC

05 FAQs, Tips and Tricks

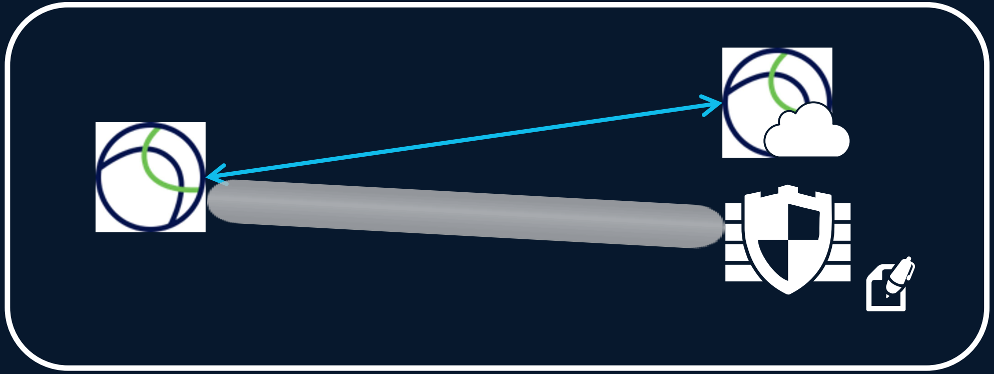
Deploying / Managing from Cloud

Deployment Models

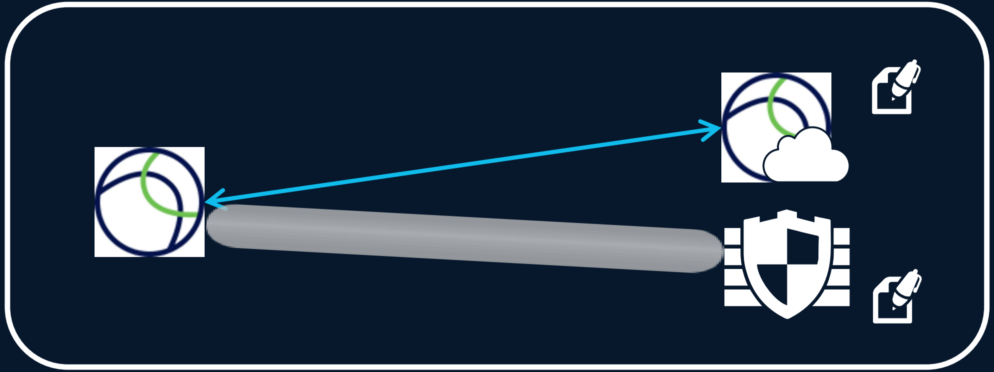
- No Cloud Management
  - Note: No XDR NVM!



- Cloud Registration – no Package Management

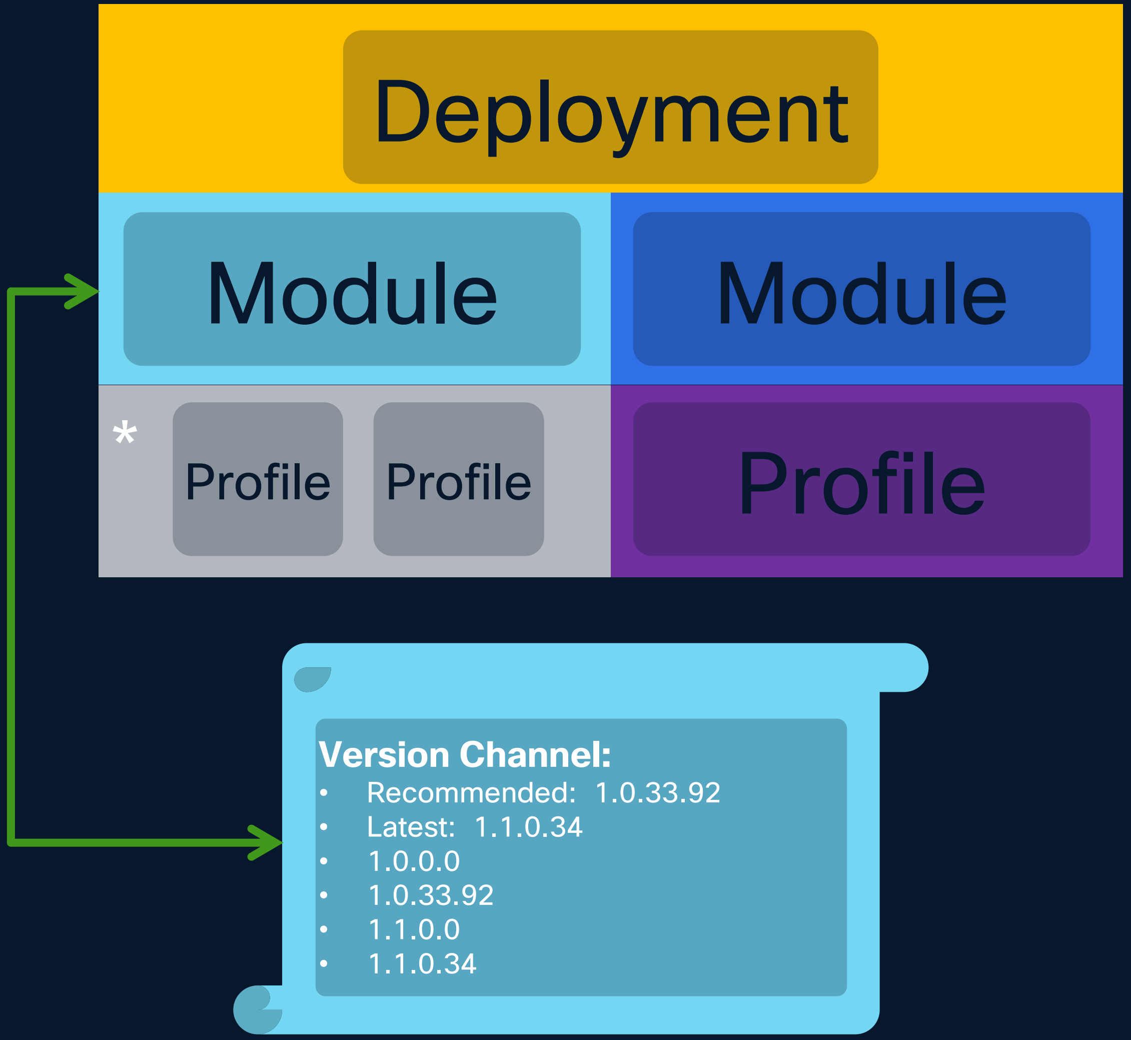


- Cloud Registration – Partial or Full Management



Glossary

- New & Old Terminology
  - Profile: Configuration for a module
  - Module: Software component that provides client-side of a security service
  - Version: Software version to be deployed
  - Channel: Cisco ‘assigned’ version
  - Deployment: Binds together modules, versions and profiles to create packages



Version Channel:

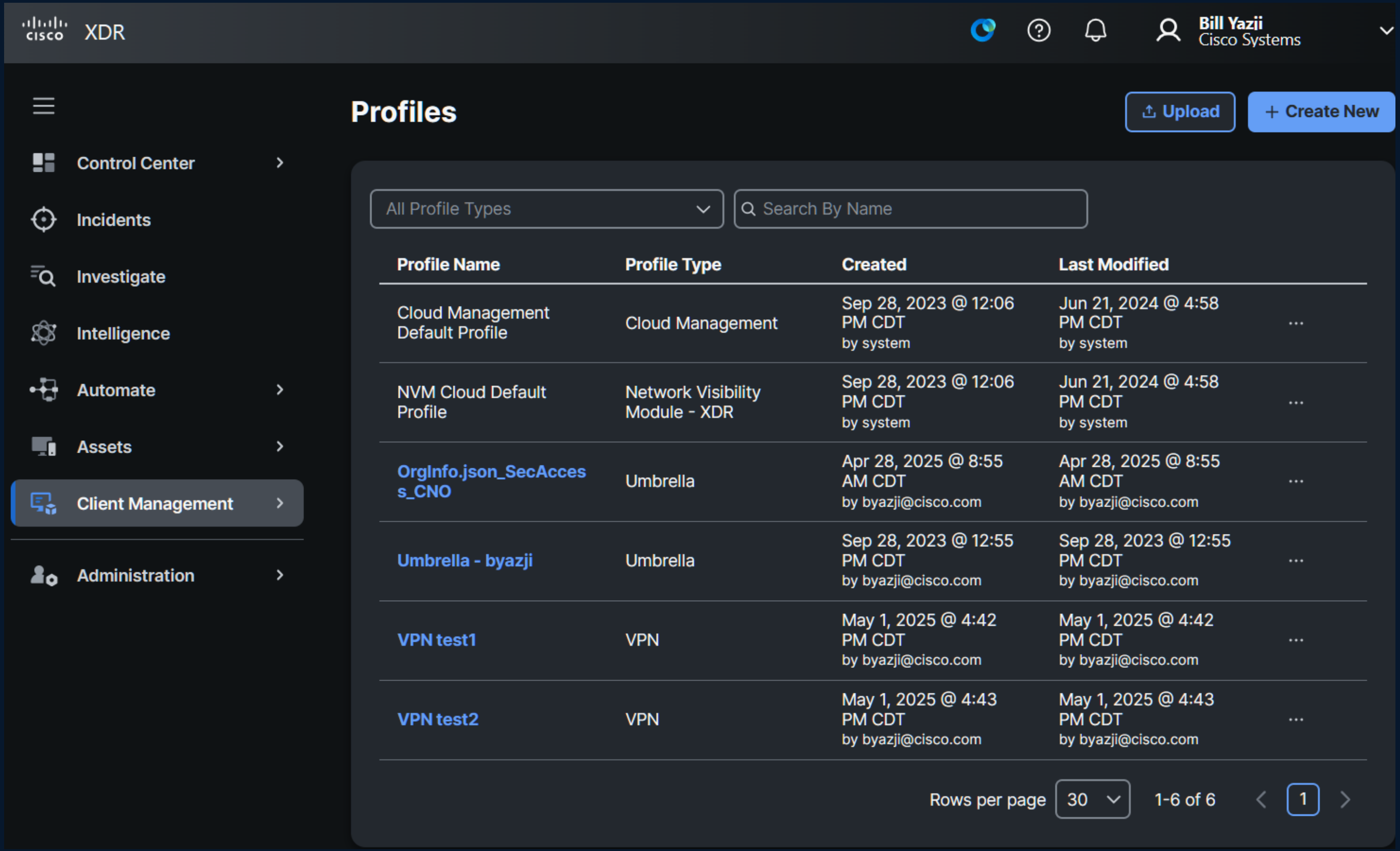
- Recommended: 1.0.33.92
- Latest: 1.1.0.34
- 1.0.0.0
- 1.0.33.92
- 1.1.0.0
- 1.1.0.34

* When module supports >1

Secure Client Cloud Management

Profile

- Each module has a profile for its “configuration”
- Similar to standalone Windows-only configuration tool



Profiles

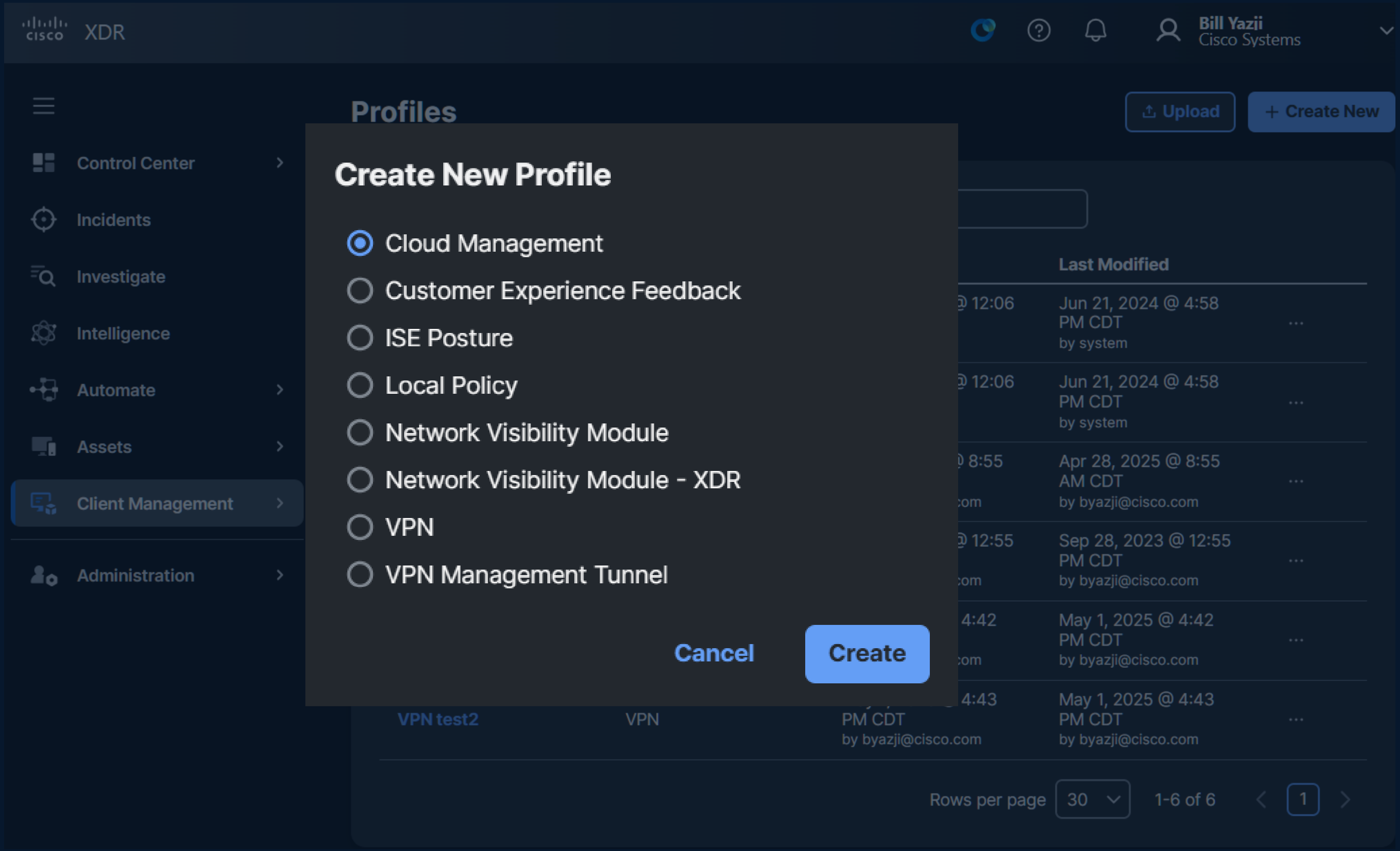
Profile Name	Profile Type	Created	Last Modified
Cloud Management Default Profile	Cloud Management	Sep 28, 2023 @ 12:06 PM CDT by system	Jun 21, 2024 @ 4:58 PM CDT by system
NVM Cloud Default Profile	Network Visibility Module - XDR	Sep 28, 2023 @ 12:06 PM CDT by system	Jun 21, 2024 @ 4:58 PM CDT by system
OrgInfo.json_SecAccess_CNO	Umbrella	Apr 28, 2025 @ 8:55 AM CDT by byazji@cisco.com	Apr 28, 2025 @ 8:55 AM CDT by byazji@cisco.com
Umbrella - byazji	Umbrella	Sep 28, 2023 @ 12:55 PM CDT by byazji@cisco.com	Sep 28, 2023 @ 12:55 PM CDT by byazji@cisco.com
VPN test1	VPN	May 1, 2025 @ 4:42 PM CDT by byazji@cisco.com	May 1, 2025 @ 4:42 PM CDT by byazji@cisco.com
VPN test2	VPN	May 1, 2025 @ 4:43 PM CDT by byazji@cisco.com	May 1, 2025 @ 4:43 PM CDT by byazji@cisco.com

Rows per page 30 1-6 of 6 1

Secure Client Cloud Management

Profile

- Each module has a profile for its “configuration”
- Similar to standalone Windows-only configuration tool
- Create new profile in SCCM....



XDR
Bill Yazii
Cisco Systems
Control Center
Incidents
Investigate
Intelligence
Automate
Assets
Client Management
Administration
Profiles
Upload
+ Create New
Last Modified
Jun 21, 2024 @ 4:58 PM CDT by system
Jun 21, 2024 @ 4:58 PM CDT by system
Apr 28, 2025 @ 8:55 AM CDT by byazji@cisco.com
Sep 28, 2023 @ 12:55 PM CDT by byazji@cisco.com
May 1, 2025 @ 4:42 PM CDT by byazji@cisco.com
VPN test2
VPN
PM CDT by byazji@cisco.com
May 1, 2025 @ 4:43 PM CDT by byazji@cisco.com
Rows per page
30
1-6 of 6
1

Create New Profile

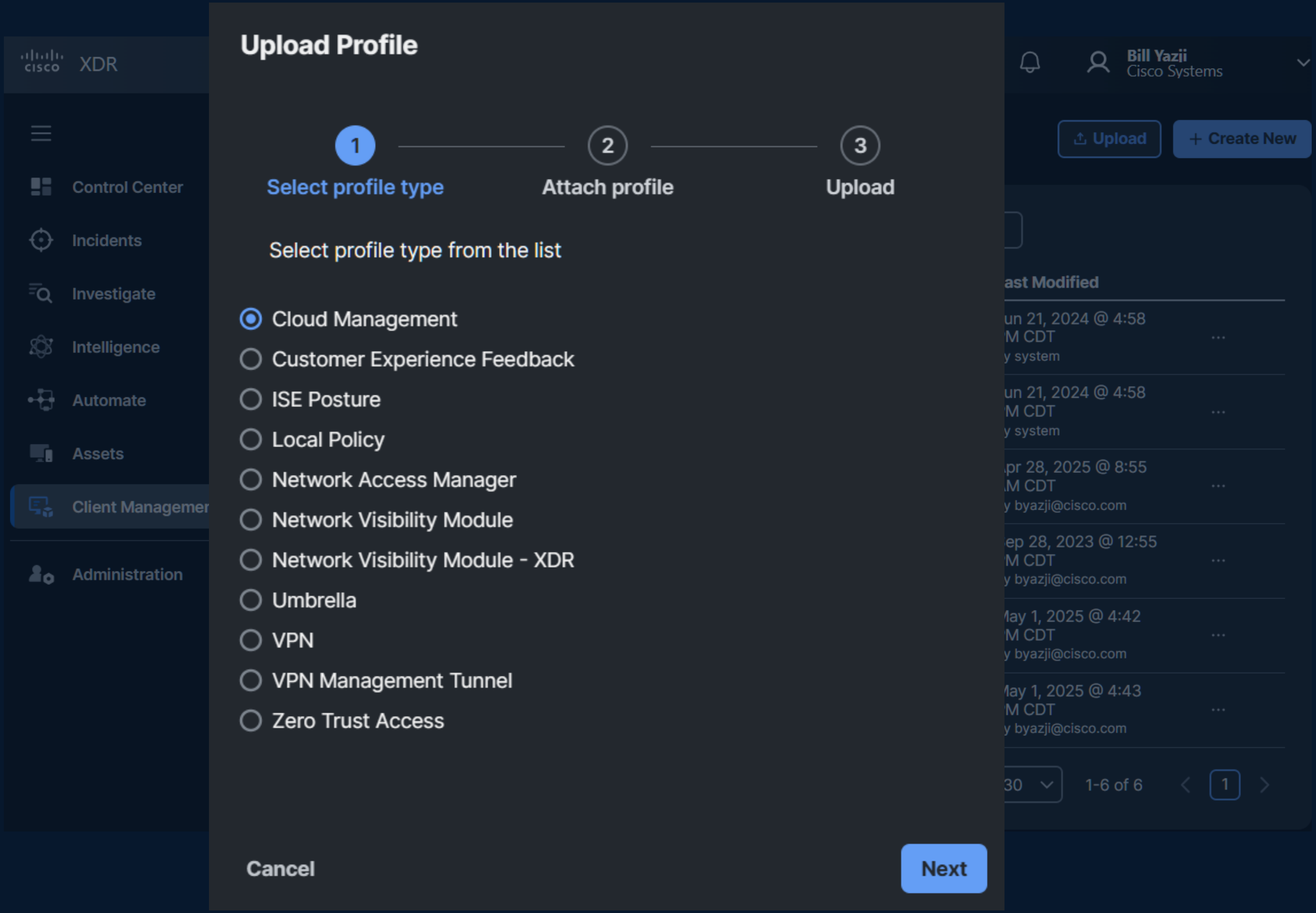
- ● Cloud Management
- ○ Customer Experience Feedback
- ○ ISE Posture
- ○ Local Policy
- ○ Network Visibility Module
- ○ Network Visibility Module - XDR
- ○ VPN
- ○ VPN Management Tunnel

Cancel Create

Secure Client Cloud Management

Profile

- Each module has a profile for its “configuration”
- Similar to standalone Windows-only configuration tool
- Create new profile in SCCM….
- ….or upload/import existing one.



Upload Profile

1 Select profile type — 2 Attach profile — 3 Upload

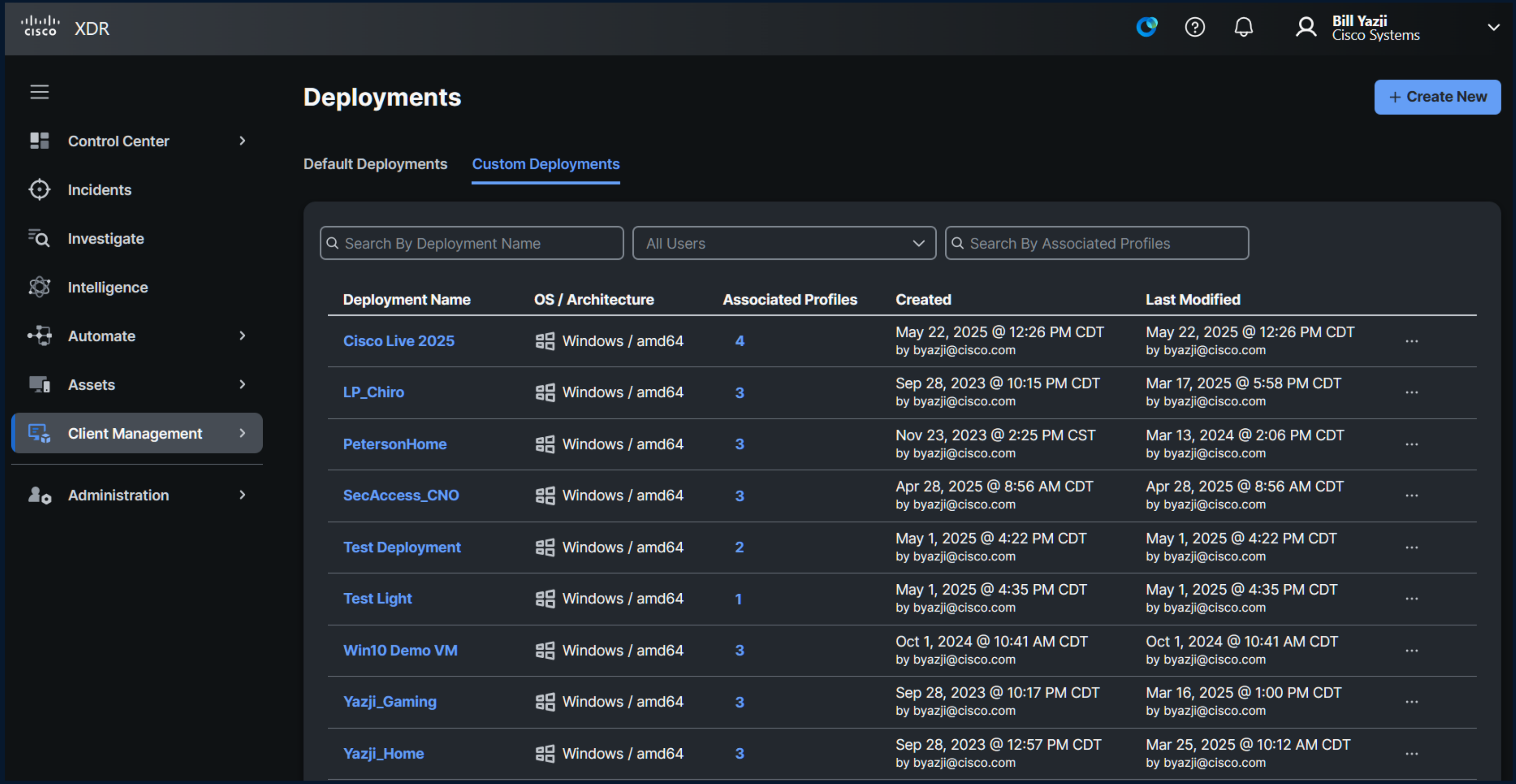
Select profile type from the list

● Cloud Management
○ Customer Experience Feedback
○ ISE Posture
○ Local Policy
○ Network Access Manager
○ Network Visibility Module
○ Network Visibility Module - XDR
○ Umbrella
○ VPN
○ VPN Management Tunnel
○ Zero Trust Access

Secure Client Cloud Management

Deployments

- Combining modules and profiles
- “Groups” are coming in future version & can assign entire groups to a Deployment
- Builds the installer dynamically per deployment



Deployments

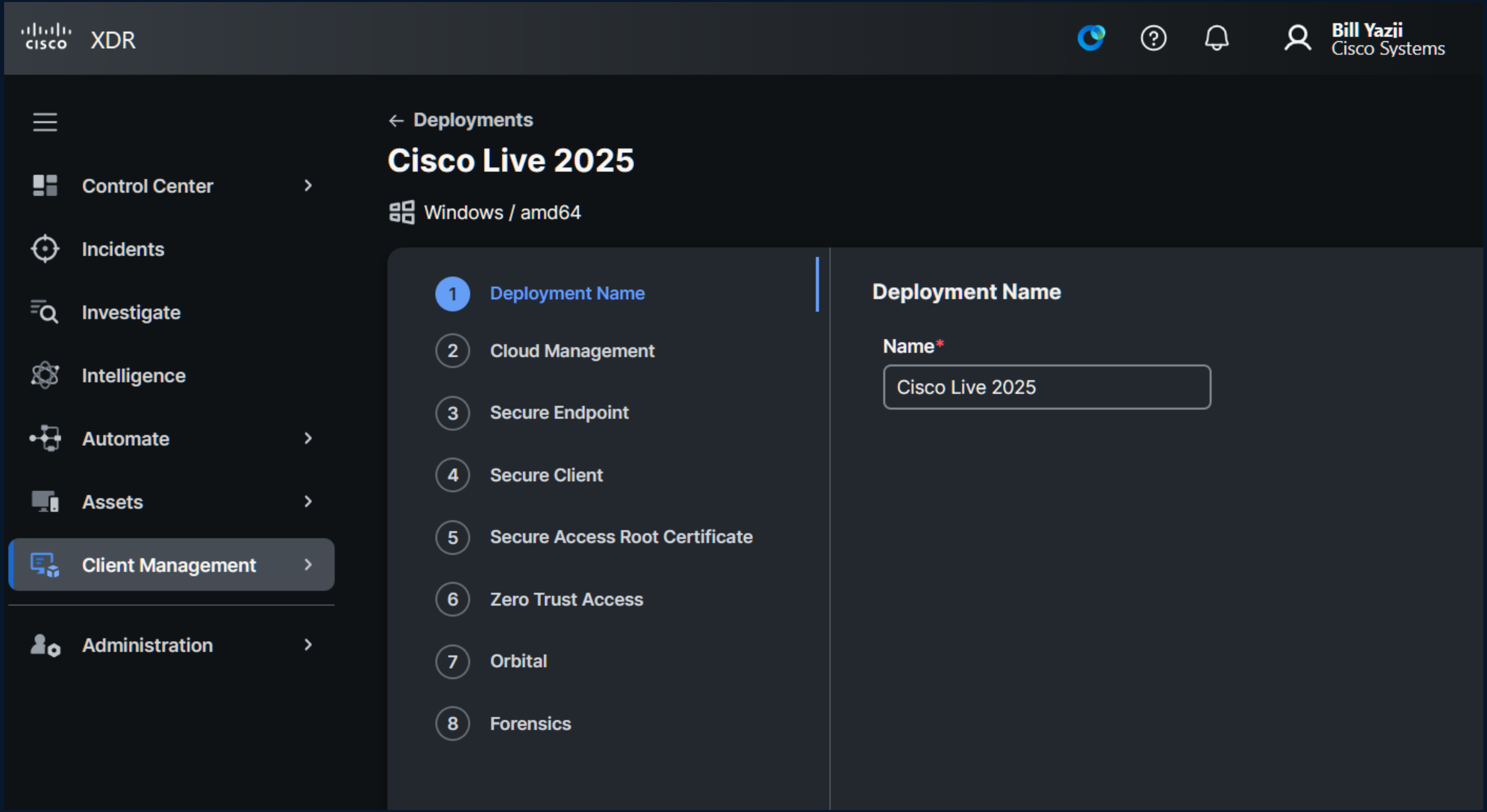
Default Deployments | Custom Deployments

Deployment Name	OS / Architecture	Associated Profiles	Created	Last Modified	
Cisco Live 2025	Windows / amd64	4	May 22, 2025 @ 12:26 PM CDT by byazji@cisco.com	May 22, 2025 @ 12:26 PM CDT by byazji@cisco.com	...
LP_Chiro	Windows / amd64	3	Sep 28, 2023 @ 10:15 PM CDT by byazji@cisco.com	Mar 17, 2025 @ 5:58 PM CDT by byazji@cisco.com	...
PetersonHome	Windows / amd64	3	Nov 23, 2023 @ 2:25 PM CST by byazji@cisco.com	Mar 13, 2024 @ 2:06 PM CDT by byazji@cisco.com	...
SecAccess_CNO	Windows / amd64	3	Apr 28, 2025 @ 8:56 AM CDT by byazji@cisco.com	Apr 28, 2025 @ 8:56 AM CDT by byazji@cisco.com	...
Test Deployment	Windows / amd64	2	May 1, 2025 @ 4:22 PM CDT by byazji@cisco.com	May 1, 2025 @ 4:22 PM CDT by byazji@cisco.com	...
Test Light	Windows / amd64	1	May 1, 2025 @ 4:35 PM CDT by byazji@cisco.com	May 1, 2025 @ 4:35 PM CDT by byazji@cisco.com	...
Win10 Demo VM	Windows / amd64	3	Oct 1, 2024 @ 10:41 AM CDT by byazji@cisco.com	Oct 1, 2024 @ 10:41 AM CDT by byazji@cisco.com	...
Yazji_Gaming	Windows / amd64	3	Sep 28, 2023 @ 10:17 PM CDT by byazji@cisco.com	Mar 16, 2025 @ 1:00 PM CDT by byazji@cisco.com	...
Yazji_Home	Windows / amd64	3	Sep 28, 2023 @ 12:57 PM CDT by byazji@cisco.com	Mar 25, 2025 @ 10:12 AM CDT by byazji@cisco.com	...

Secure Client Cloud Management

Deployment creation

- Combining modules and profiles
- “Groups” are coming in future version & can assign entire groups to a Deployment
- Builds the installer dynamically per deployment



← Deployments

Cisco Live 2025

Windows / amd64

1 Deployment Name
2 Cloud Management
3 Secure Endpoint
4 Secure Client
5 Secure Access Root Certificate
6 Zero Trust Access
7 Orbital
8 Forensics

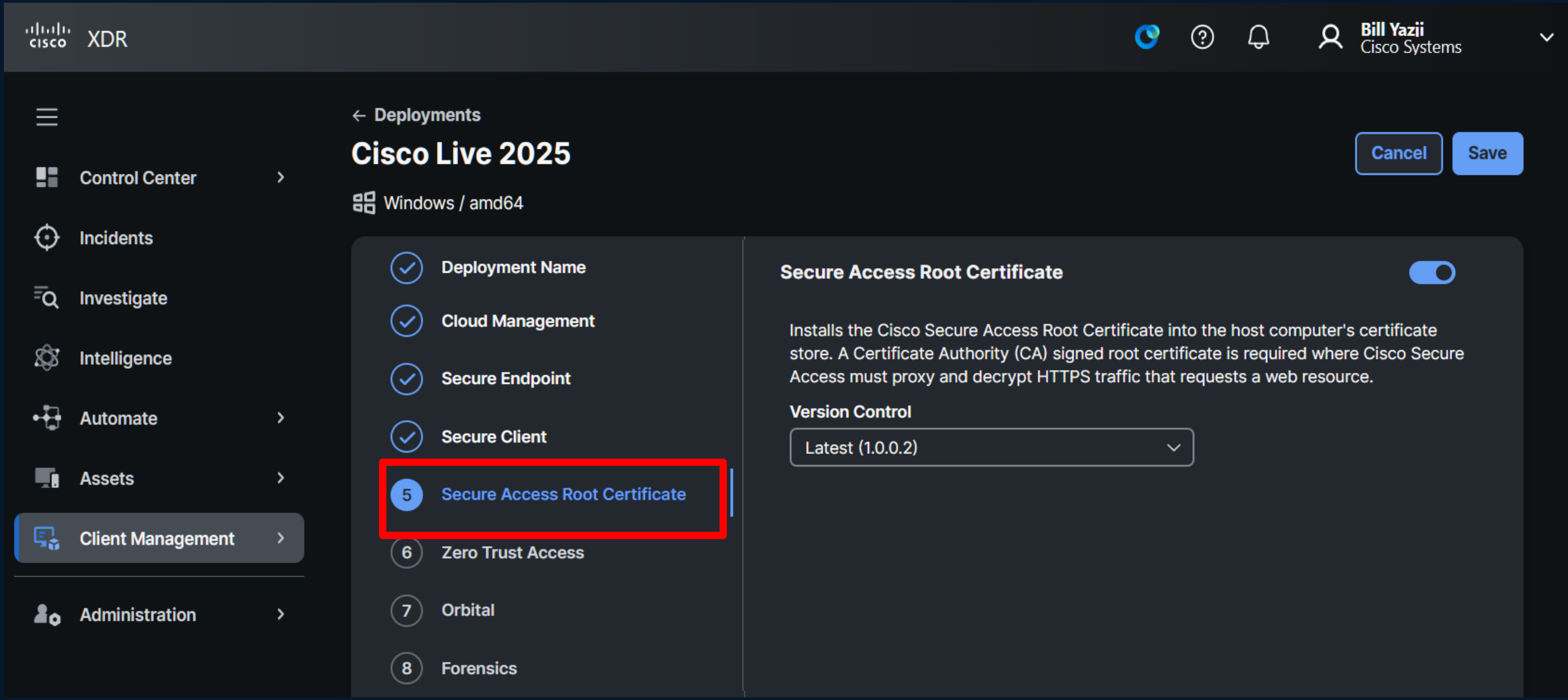
Deployment Name

Name*: Cisco Live 2025

Secure Client Cloud Management

New for 2025

- Secure Access Root Certificate



Cisco Live 2025

Windows / amd64

1. Deployment Name
2. Cloud Management
3. Secure Endpoint
4. Secure Client
5. Secure Access Root Certificate
6. Zero Trust Access
7. Orbital
8. Forensics

Secure Access Root Certificate

Installs the Cisco Secure Access Root Certificate into the host computer's certificate store. A Certificate Authority (CA) signed root certificate is required where Cisco Secure Access must proxy and decrypt HTTPS traffic that requests a web resource.

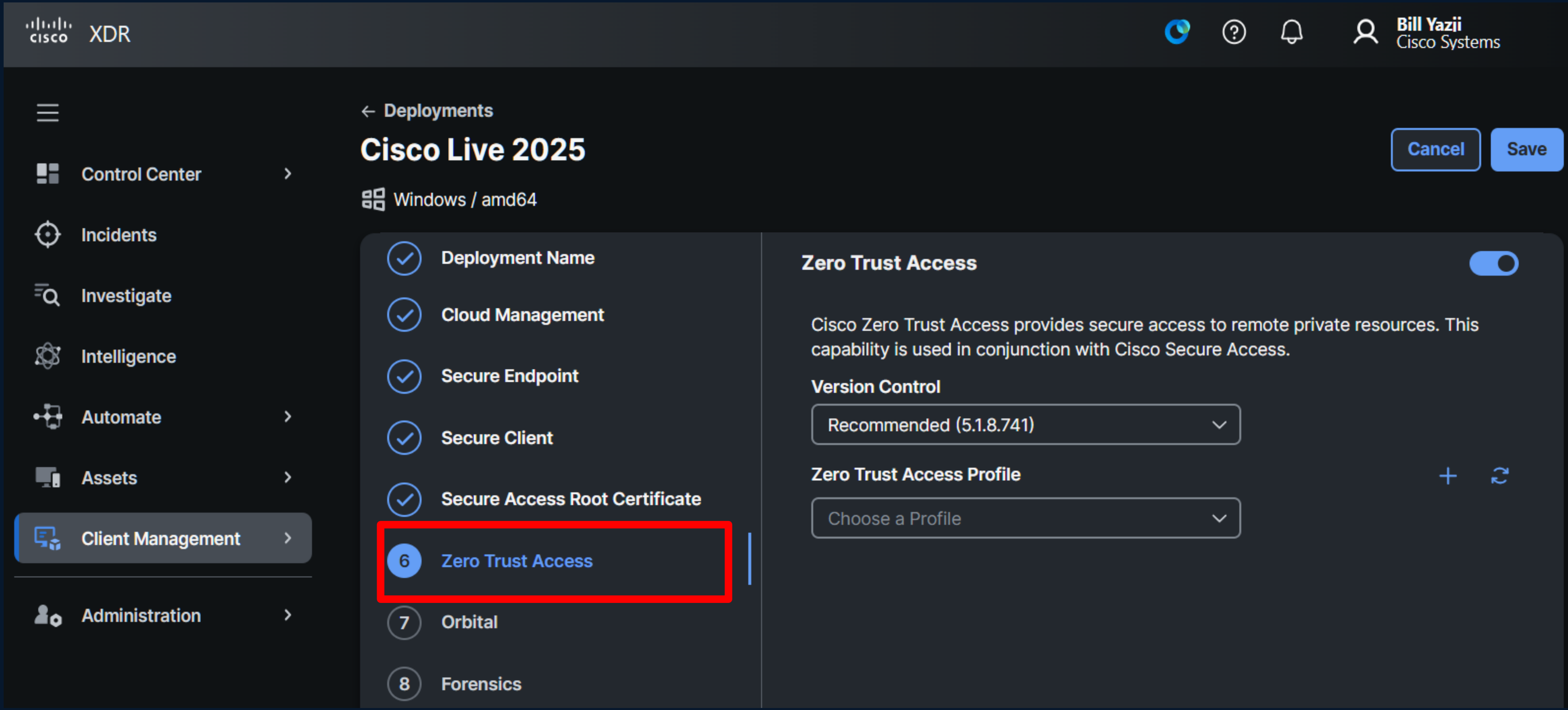
Version Control

Latest (1.0.0.2)

Secure Client Cloud Management

New for 2025

- Zero Trust Access
- ZTA Cert Enrollment
  - Requires 5.1.9
  - Win/Mac
  - TPM/Secure Enclave
- ZTA TND GA in June
  - Requires 5.1.10



Cisco Live 2025

Windows / amd64

Zero Trust Access

Cisco Zero Trust Access provides secure access to remote private resources. This capability is used in conjunction with Cisco Secure Access.

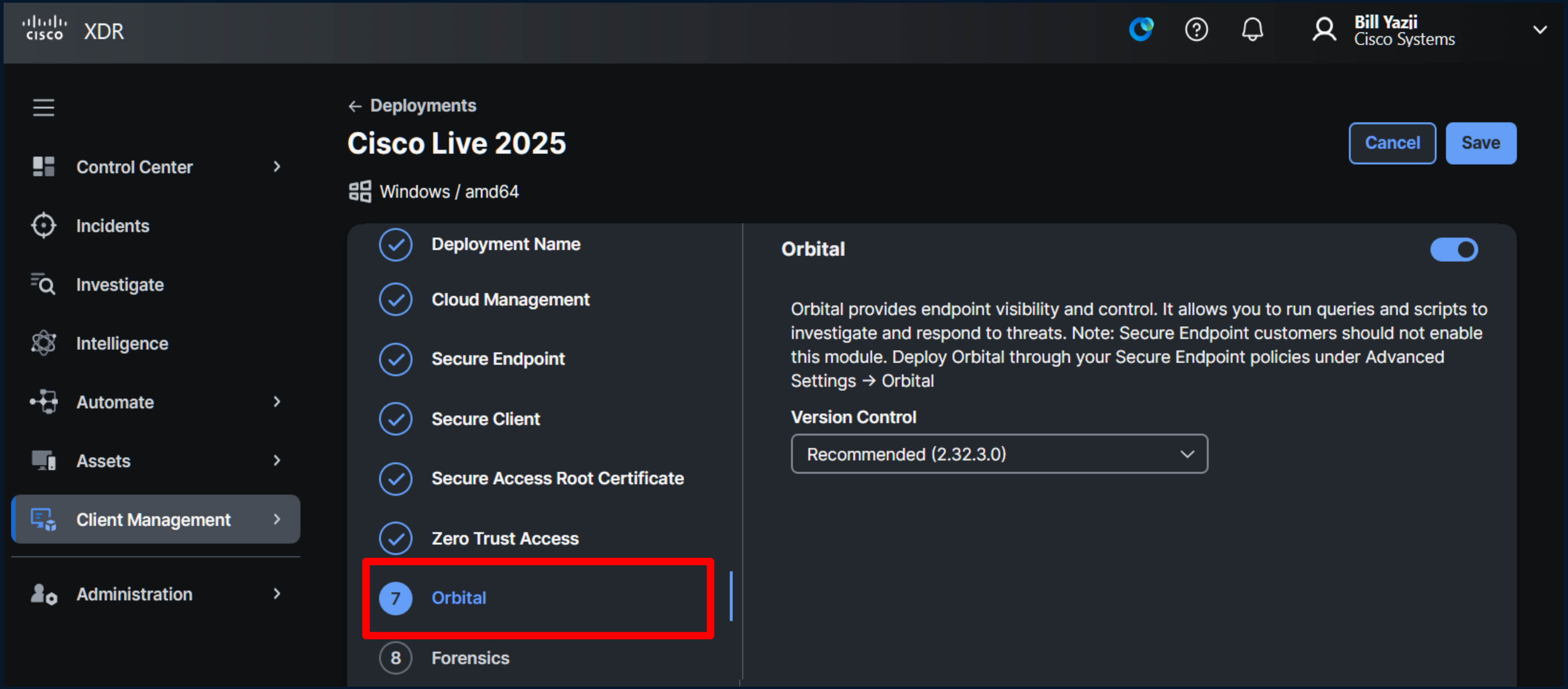
Version Control: Recommended (5.1.8.741)

Zero Trust Access Profile: Choose a Profile

Secure Client Cloud Management

New for 2025

- Orbital Standalone
  - XDR customers only
  - Windows today
  - Mac expected Q3
  - All XDR tiers are entitled



Cisco Live 2025

Windows / amd64

1. Deployment Name
2. Cloud Management
3. Secure Endpoint
4. Secure Client
5. Secure Access Root Certificate
6. Zero Trust Access
7. Orbital
8. Forensics

Orbital

Orbital provides endpoint visibility and control. It allows you to run queries and scripts to investigate and respond to threats. Note: Secure Endpoint customers should not enable this module. Deploy Orbital through your Secure Endpoint policies under Advanced Settings → Orbital

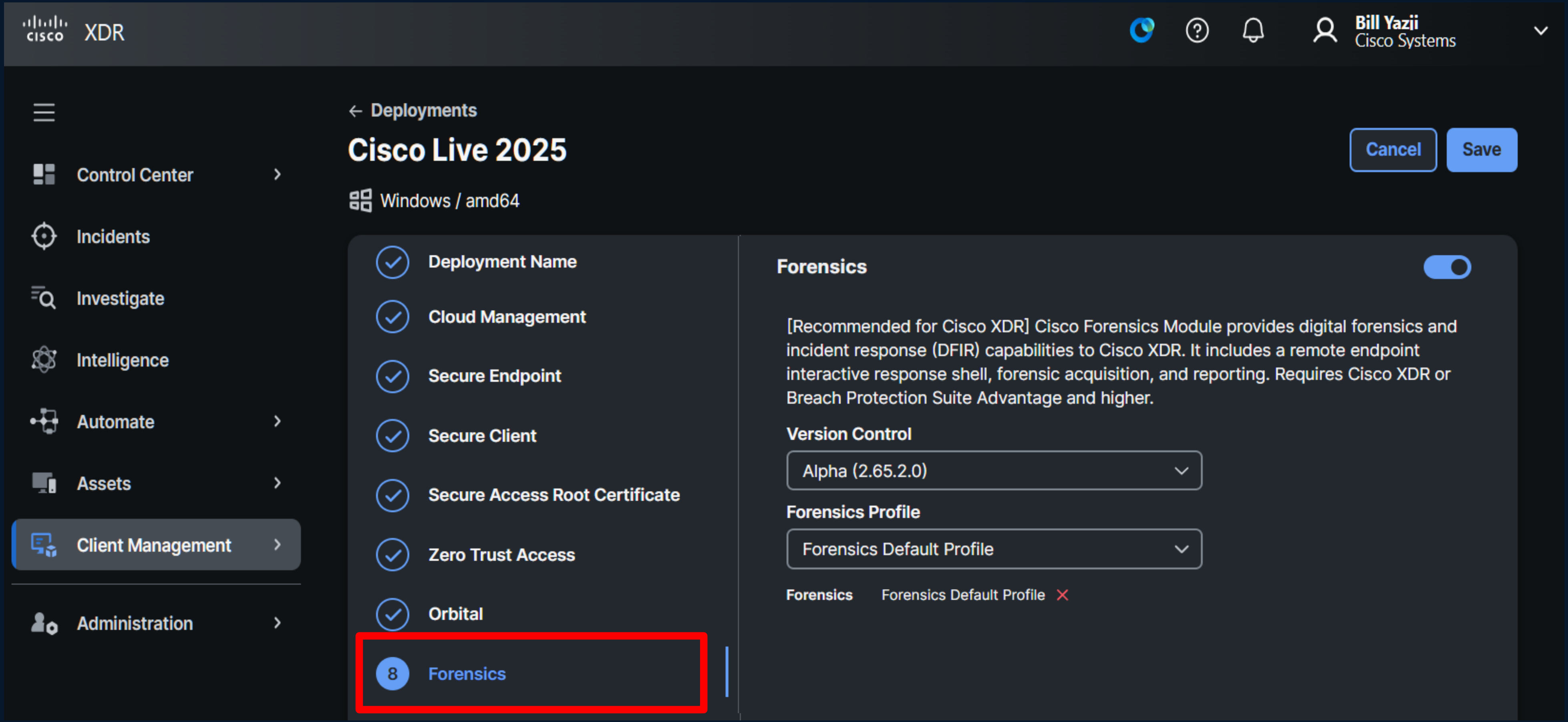
Version Control

Recommended (2.32.3.0)

Secure Client Cloud Management

New for 2025

- XDR Forensics
  - Coming soon
  - Windows & Mac
  - XDR Adv/Premier



Cisco Live 2025

Windows / amd64

- Deployment Name
- Cloud Management
- Secure Endpoint
- Secure Client
- Secure Access Root Certificate
- Zero Trust Access
- Orbital
- 8 Forensics

Forensics

[Recommended for Cisco XDR] Cisco Forensics Module provides digital forensics and incident response (DFIR) capabilities to Cisco XDR. It includes a remote endpoint interactive response shell, forensic acquisition, and reporting. Requires Cisco XDR or Breach Protection Suite Advantage and higher.

Version Control: Alpha (2.65.2.0)

Forensics Profile: Forensics Default Profile

Forensics   Forensics Default Profile ✕

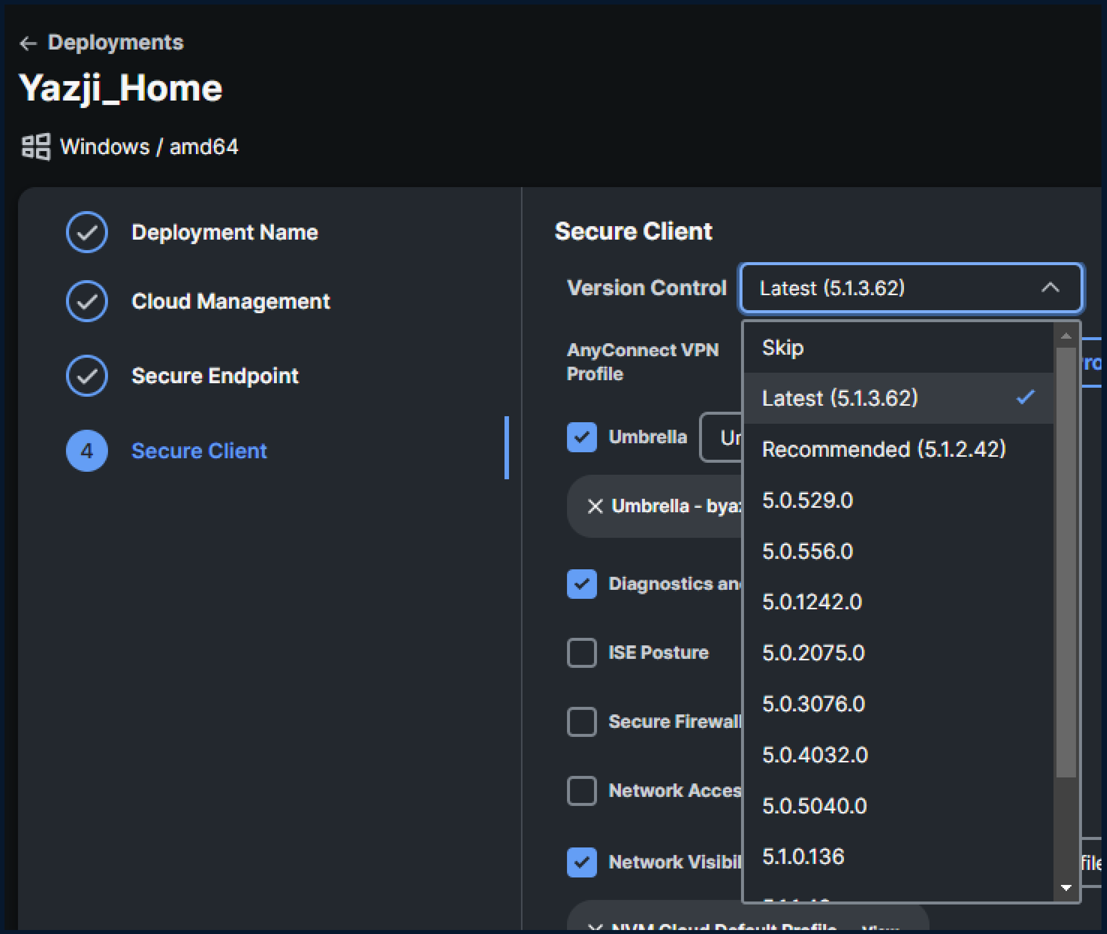
Learn more about the new Forensics capabilities of XDR at the Showcase Zone

Version Catalog

- For each deployment:
  - Controllable channel for software versioning:
    - Hard-Code the specific version (version lock)
    - Skip (never upgrade version)
    - Recommended
    - Latest
    - Beta
    - Alpha

Auto upgraded when Cisco publishes a new version to channel

  - Allows you to have an “early testers” set of endpoints, etc..



← Deployments

Yazji_Home

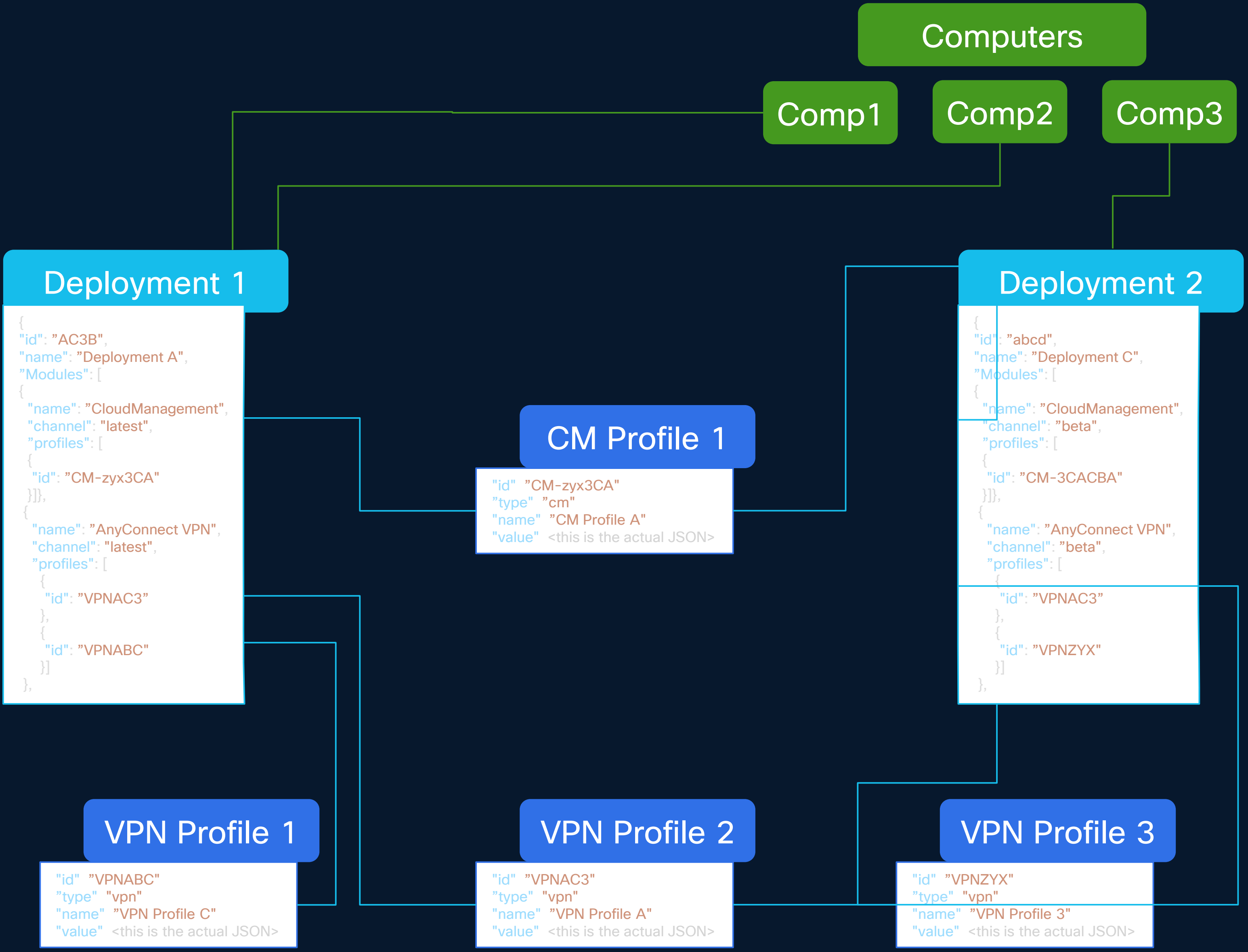
Windows / amd64

Secure Client

Version Control: Latest (5.1.3.62)

Deployment Hierarchy

- Computers assigned to 1 Deployment at a time!
- Able to move computers to different Deployments
- Deployment ties together:
  - Chosen Modules
    - Module Software Versions
    - Software “Channel” for updates / versions
  - Profiles (Module Configs)
    - Each Profile can be in up to 45 Deployments (increasing in future)
- Installers are created dynamically based on the Deployment



Deployment 1

```
{
"id": ”AC3B",
"name": ”Deployment A",
”Modules": [
{
  "name": ”CloudManagement",
  "channel": "latest",
  ”profiles": [
  {
   "id": ”CM-zyx3CA"
  }]},
 {
   "name": ”AnyConnect VPN",
   "channel": "latest",
   ”profiles": [
     {
      "id": ”VPNAC3”
     },
     {
      "id": ”VPNABC"
     }]
 },
```

Deployment 2

```
{
"id": ”abcd",
"name": ”Deployment C",
”Modules": [
{
  "name": ”CloudManagement",
  "channel": ”beta",
  ”profiles": [
  {
   "id": ”CM-3CACBA"
  }]},
 {
   "name": ”AnyConnect VPN",
   "channel": ”beta",
   ”profiles": [
     {
      "id": ”VPNAC3”
     },
     {
      "id": ”VPNZYX"
     }]
 },
```

CM Profile 1

```
"id"  ”CM-zyx3CA"
"type"  ”cm"
"name"  ”CM Profile A"
"value"  <this is the actual JSON>
```

VPN Profile 1

```
"id"  ”VPNABC"
"type"  ”vpn"
"name"  ”VPN Profile C"
"value"  <this is the actual JSON>
```

VPN Profile 2

```
"id"  ”VPNAC3"
"type"  ”vpn"
"name"  ”VPN Profile A"
"value"  <this is the actual JSON>
```

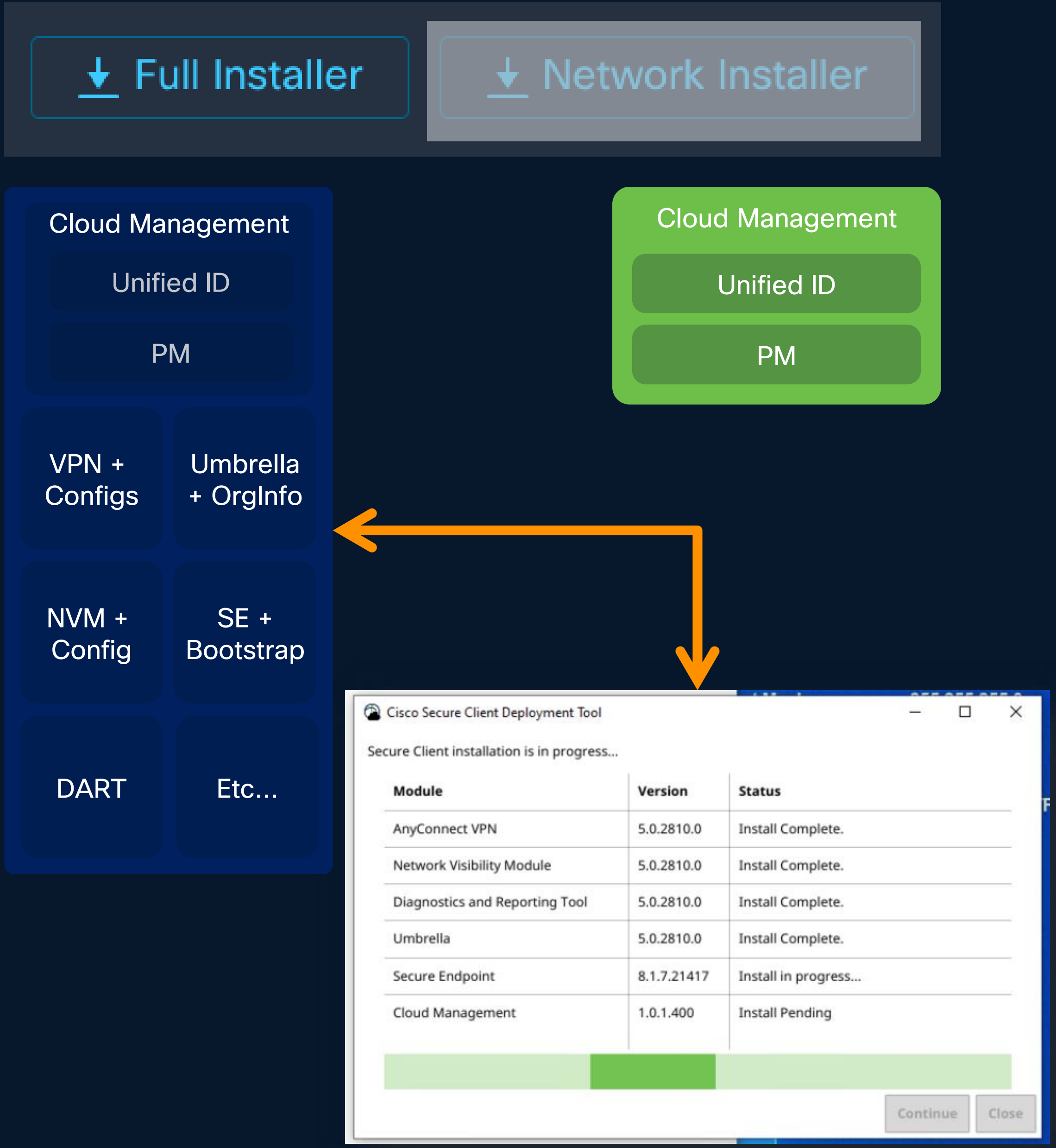
VPN Profile 3

```
"id"  ”VPNZYX"
"type"  ”vpn"
"name"  ”VPN Profile 3"
"value"  <this is the actual JSON>
```

Installing CSC

Full & Network Installer Options

- Full Installer:
  - All selected Modules & their configurations.



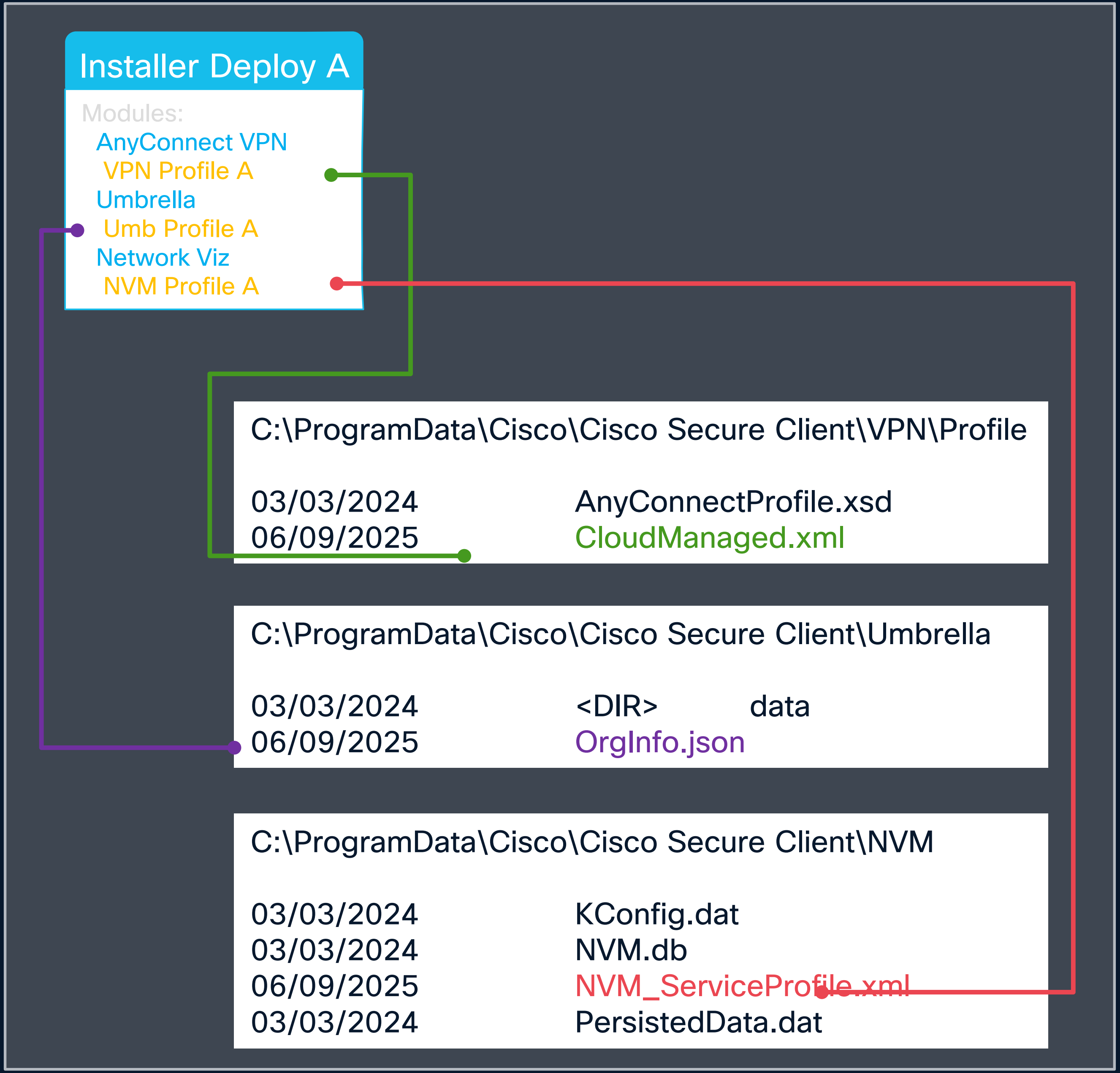
Secure Client installation is in progress...

Module	Version	Status
AnyConnect VPN	5.0.2810.0	Install Complete.
Network Visibility Module	5.0.2810.0	Install Complete.
Diagnostics and Reporting Tool	5.0.2810.0	Install Complete.
Umbrella	5.0.2810.0	Install Complete.
Secure Endpoint	8.1.7.21417	Install in progress...
Cloud Management	1.0.1.400	Install Pending

Installing CSC

Full Installer Option

- Contains packages for modules + profiles
- Places the profiles in the correct place
- Renames profile from the ‘friendly name’ in Cloud Management to the required name (if applicable)



Installer Deploy A

Modules:
- AnyConnect VPN
  - VPN Profile A
- Umbrella
  - Umb Profile A
- Network Viz
  - NVM Profile A

```
C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

03/03/2024          AnyConnectProfile.xsd
06/09/2025          CloudManaged.xml
```

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella

03/03/2024          <DIR>       data
06/09/2025          OrgInfo.json
```

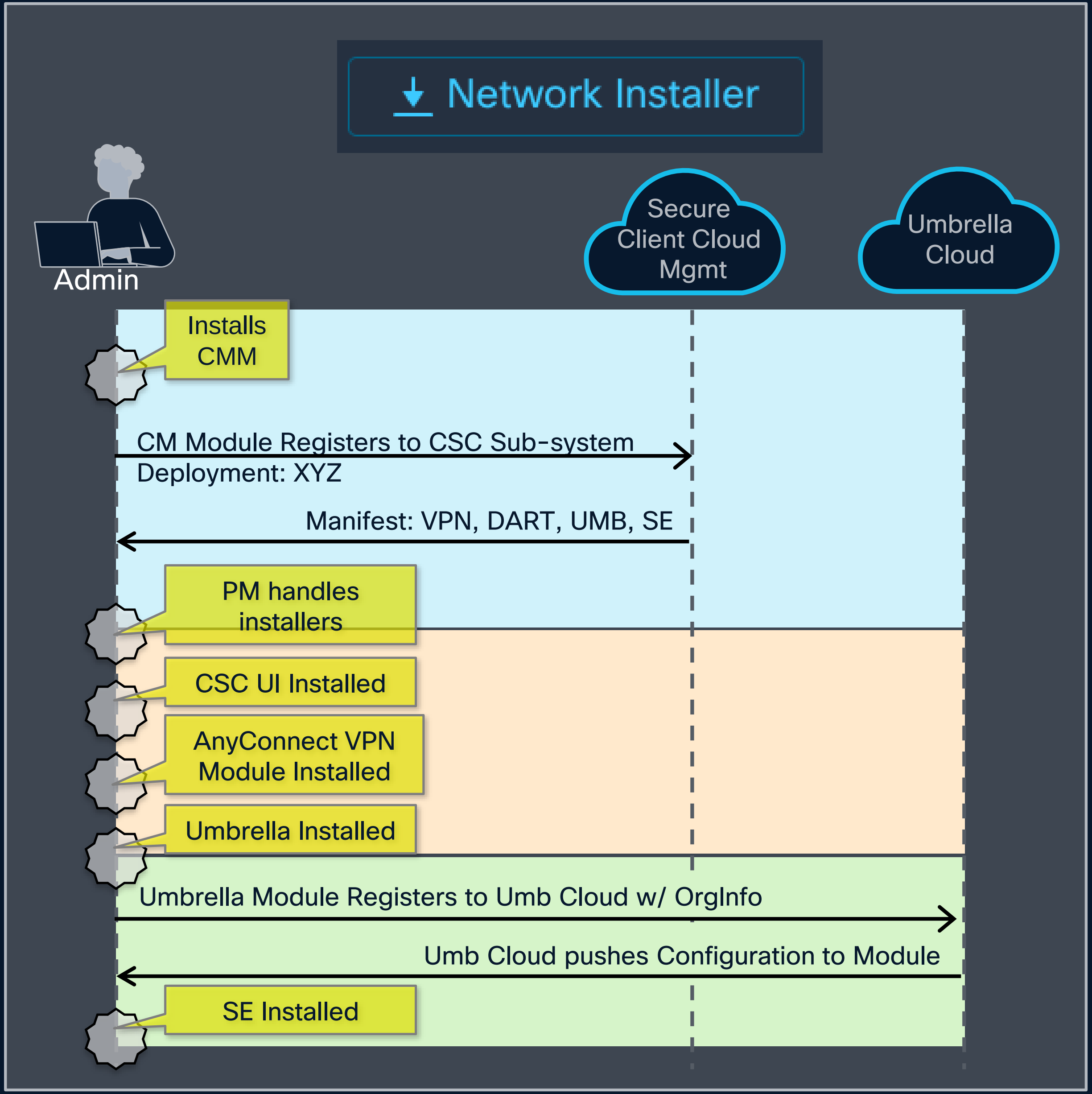
```
C:\ProgramData\Cisco\Cisco Secure Client\NVM

03/03/2024          KConfig.dat
03/03/2024          NVM.db
06/09/2025          NVM_ServiceProfile.xml
03/03/2024          PersistedData.dat
```

Installing CSC

Network Installer

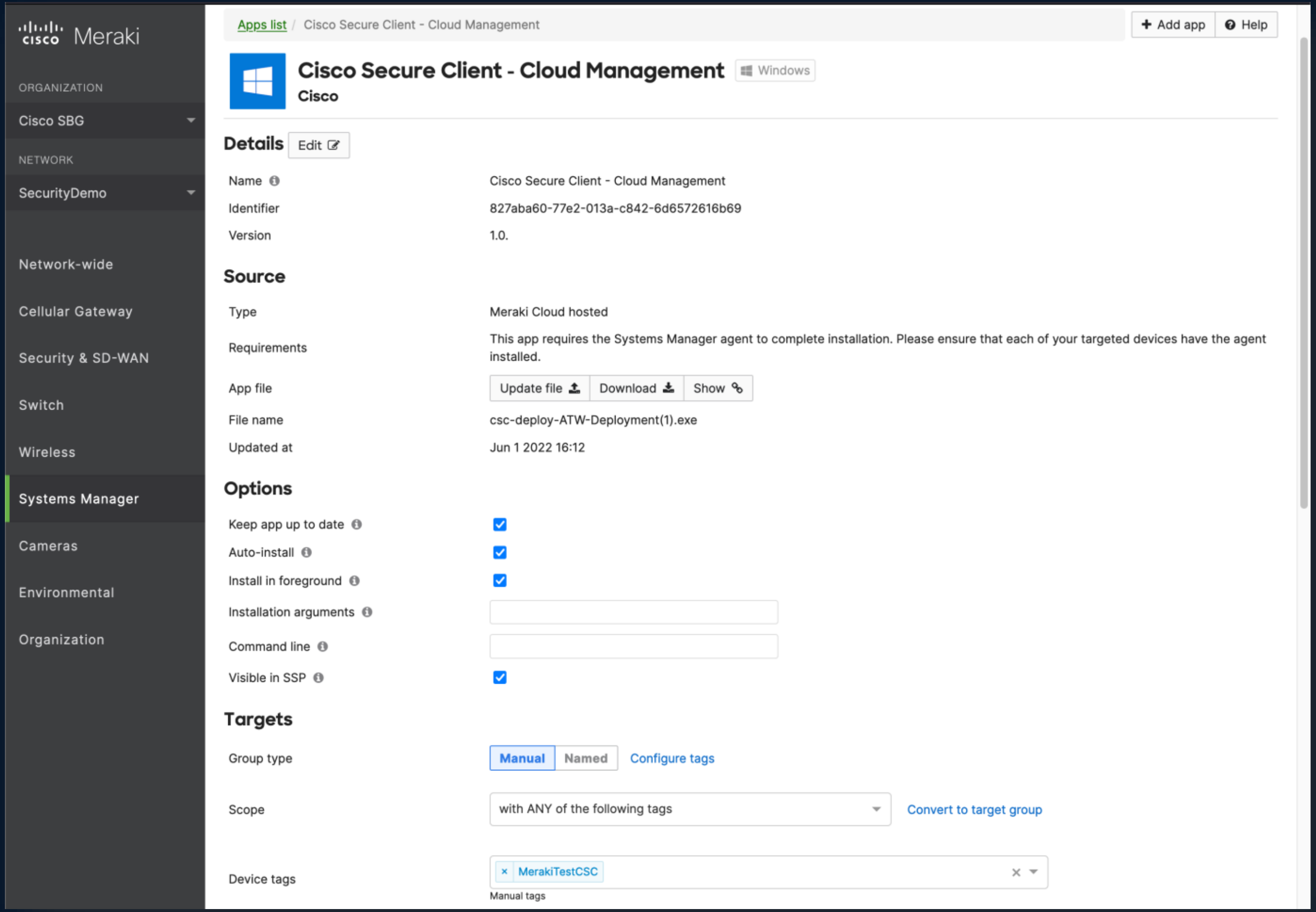
- Lightweight installer
  - Installs the Cloud Management Module with its config only & Cloud Diagnostic tool
  - Package Manager pulls the manifest from cloud deployment and installs each module and configuration.
  - Size Comparison Example
    - Identical module/profile configuration
    - Network Installer: ~37M
    - Full Deploy Installer: ~196M


Network Installer
Admin
Secure Client Cloud Mgmt
Umbrella Cloud
Installs CMM
CM Module Registers to CSC Sub-system
Deployment: XYZ
Manifest: VPN, DART, UMB, SE
PM handles installers
CSC UI Installed
AnyConnect VPN Module Installed
Umbrella Installed
Umbrella Module Registers to Umb Cloud w/ OrgInfo
Umb Cloud pushes Configuration to Module
SE Installed

Installing CSC

Using MDM of choice

- Either Full or Network Installer
  - Using a Device Manager
  - Using your own endpoint software manager
  - However your company normally pushes software



Cisco Secure Client - Cloud Management
Cisco

Details

Name	Cisco Secure Client - Cloud Management
Identifier	827aba60-77e2-013a-c842-6d6572616b69
Version	1.0.

Source

Type	Meraki Cloud hosted
Requirements	This app requires the Systems Manager agent to complete installation. Please ensure that each of your targeted devices have the agent installed.
App file	Update file / Download / Show
File name	csc-deploy-ATW-Deployment(1).exe
Updated at	Jun 1 2022 16:12

Options

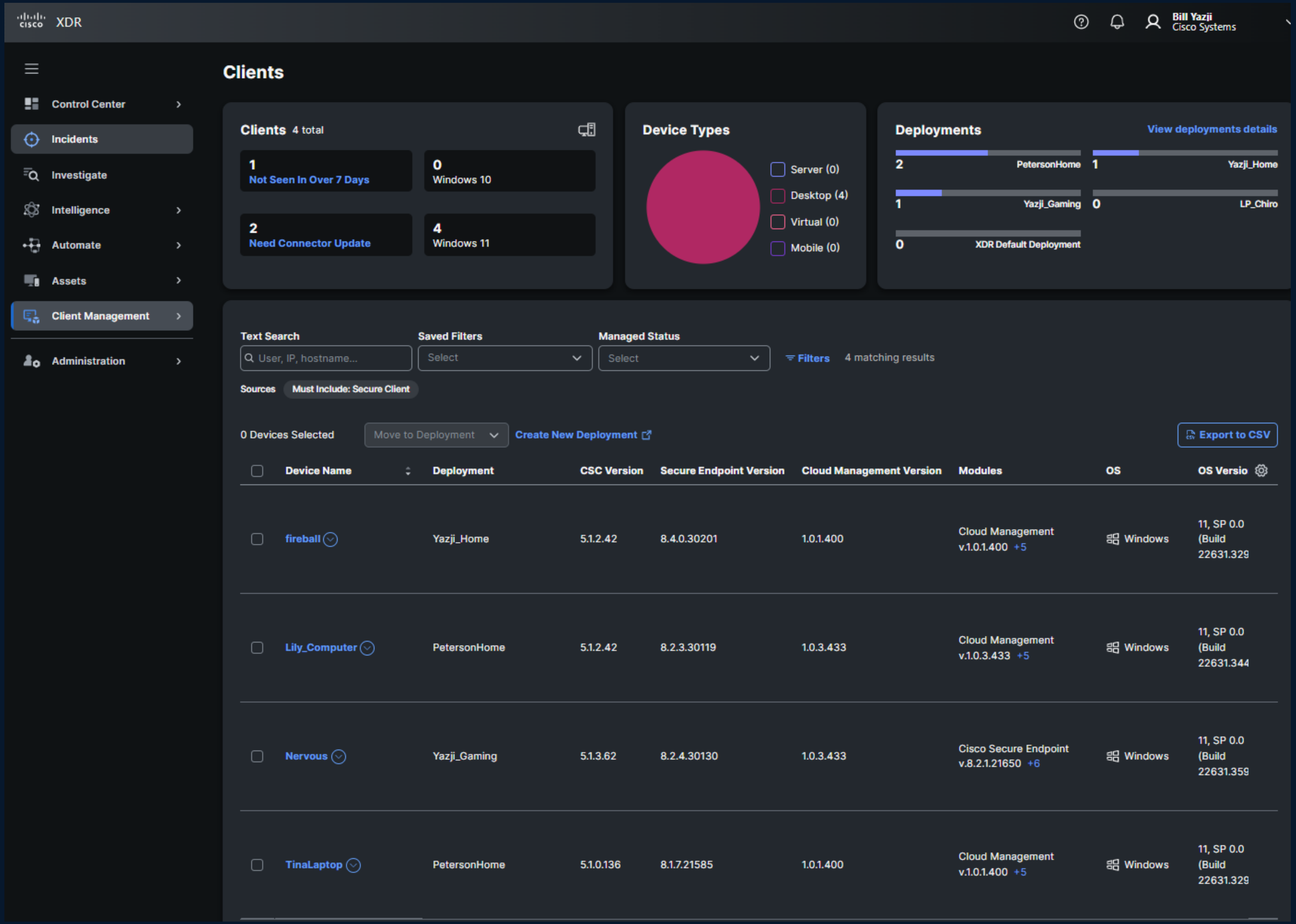
Keep app up to date	☑
Auto-install	☑
Install in foreground	☑
Installation arguments	
Command line	
Visible in SSP	☑

Targets

Group type	[✓ Manual] Named
Scope	with ANY of the following tags
Device tags	× MerakiTestCSC Manual tags

Client Management

- Clients
  - Device Names
  - Deployments
  - Versioning
  - Audit Logs
  - Device Events



Clients

Clients 4 total

1 Not Seen In Over 7 Days	0 Windows 10
2 Need Connector Update	4 Windows 11

Device Types

- □ Server (0)
- □ Desktop (4)
- □ Virtual (0)
- □ Mobile (0)

Deployments View deployments details

2	PetersonHome	1	Yazji_Home
1	Yazji_Gaming	0	LP_Chiro
0	XDR Default Deployment		

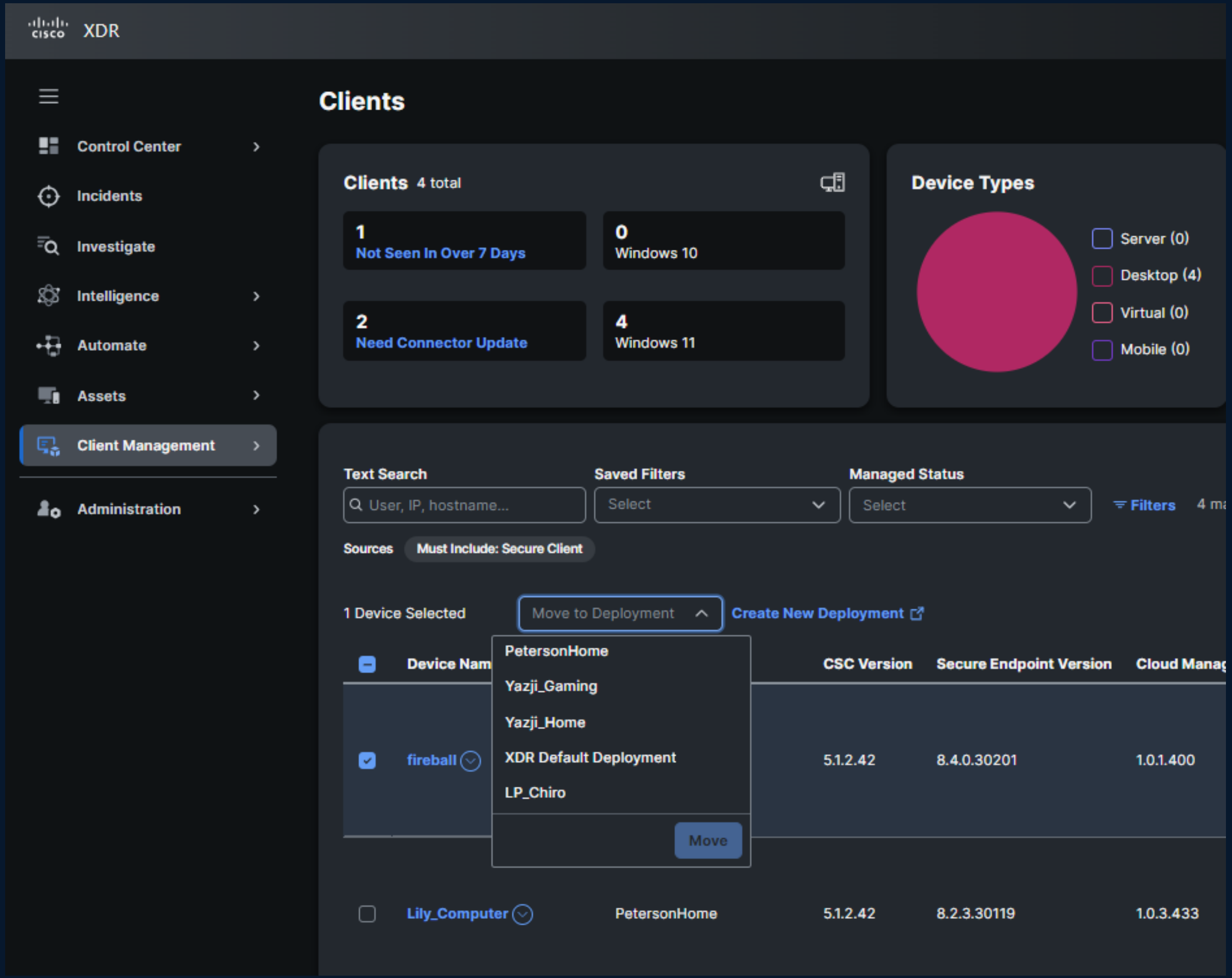
Text Search: User, IP, hostname...
Saved Filters: Select
Managed Status: Select
Filters 4 matching results
Sources Must Include: Secure Client

0 Devices Selected | Move to Deployment | Create New Deployment | Export to CSV

□	Device Name	Deployment	CSC Version	Secure Endpoint Version	Cloud Management Version	Modules	OS	OS Versio
□	fireball	Yazji_Home	5.1.2.42	8.4.0.30201	1.0.1.400	Cloud Management v.1.0.1.400 +5	Windows	11, SP 0.0 (Build 22631.329
□	Lily_Computer	PetersonHome	5.1.2.42	8.2.3.30119	1.0.3.433	Cloud Management v.1.0.3.433 +5	Windows	11, SP 0.0 (Build 22631.344
□	Nervous	Yazji_Gaming	5.1.3.62	8.2.4.30130	1.0.3.433	Cisco Secure Endpoint v.8.2.1.21650 +6	Windows	11, SP 0.0 (Build 22631.359
□	TinaLaptop	PetersonHome	5.1.0.136	8.1.7.21585	1.0.1.400	Cloud Management v.1.0.1.400 +5	Windows	11, SP 0.0 (Build 22631.329

Moving Deployments

- Admin role only
- “Desired Deployment”
  - The move will not happen until the endpoint checks in with the cloud again.
  - But the UI may show that it is already in that target deployment.



Clients

Clients 4 total

1 Not Seen In Over 7 Days

0 Windows 10

2 Need Connector Update

4 Windows 11

Device Types

☐ Server (0)
☐ Desktop (4)
☐ Virtual (0)
☐ Mobile (0)

Text Search: User, IP, hostname...
Saved Filters: Select
Managed Status: Select
Filters 4 ma

Sources: Must Include: Secure Client

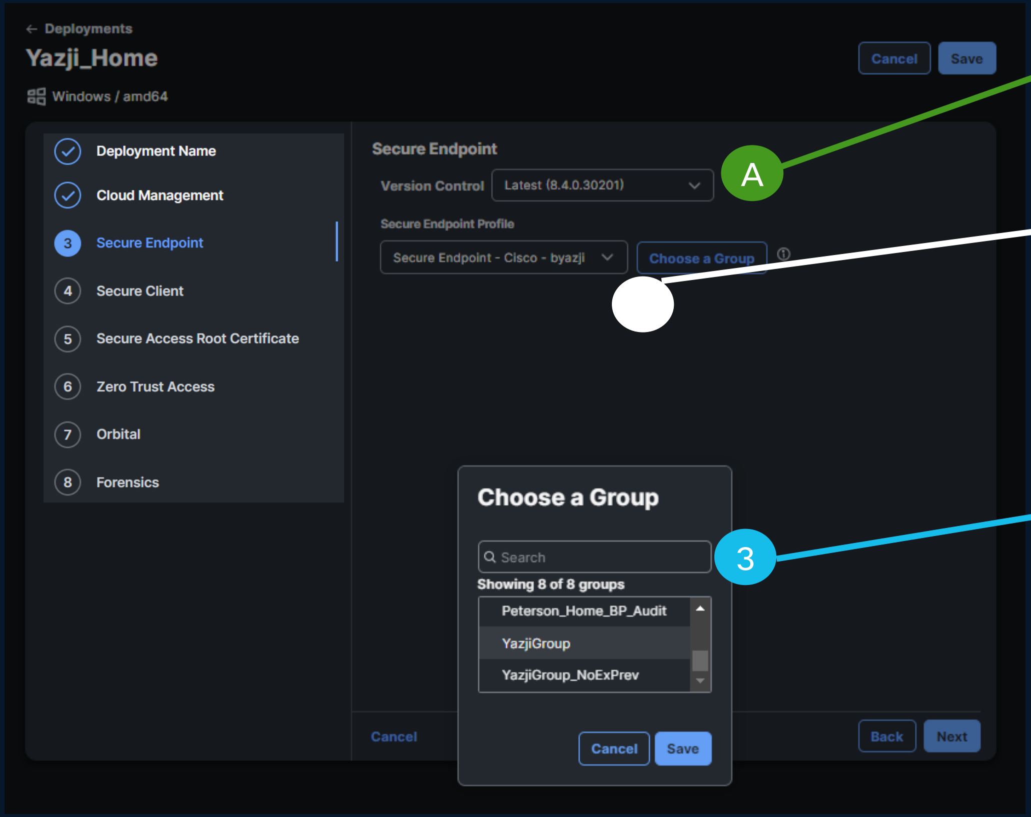
1 Device Selected — Move to Deployment

- PetersonHome
- Yazji_Gaming
- Yazji_Home
- XDR Default Deployment
- LP_Chiro

	Device Nam		CSC Version	Secure Endpoint Version	Cloud Manag
☑	fireball		5.1.2.42	8.4.0.30201	1.0.1.400
☐	Lily_Computer	PetersonHome	5.1.2.42	8.2.3.30119	1.0.3.433

Deployments w/ Secure Endpoint and Orbital

Configuring Secure Endpoint



← Deployments

Yazji_Home

Cancel Save

Windows / amd64

1. Deployment Name
2. Cloud Management
3. Secure Endpoint
4. Secure Client
5. Secure Access Root Certificate
6. Zero Trust Access
7. Orbital
8. Forensics

Secure Endpoint

Version Control: Latest (8.4.0.30201)

Secure Endpoint Profile: Secure Endpoint - Cisco - byazji | Choose a Group

Choose a Group

Search

Showing 8 of 8 groups

- Peterson_Home_BP_Audit
- YazjiGroup
- YazjiGroup_NoExPrev

Cancel Save

Cancel | Back Next

Select Desired SE Version

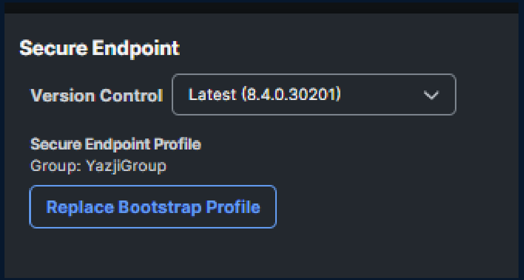
Select your SE Organization

There *can* be more than one

Choose the SE Group

Endpoints who ‘net new’ install the module via this deployment, will be assigned to this group, when the CSE module registers with the CSE cloud.

The bootstrap file configures new installs of SE to join that Secure Endpoint org and that group



Secure Endpoint

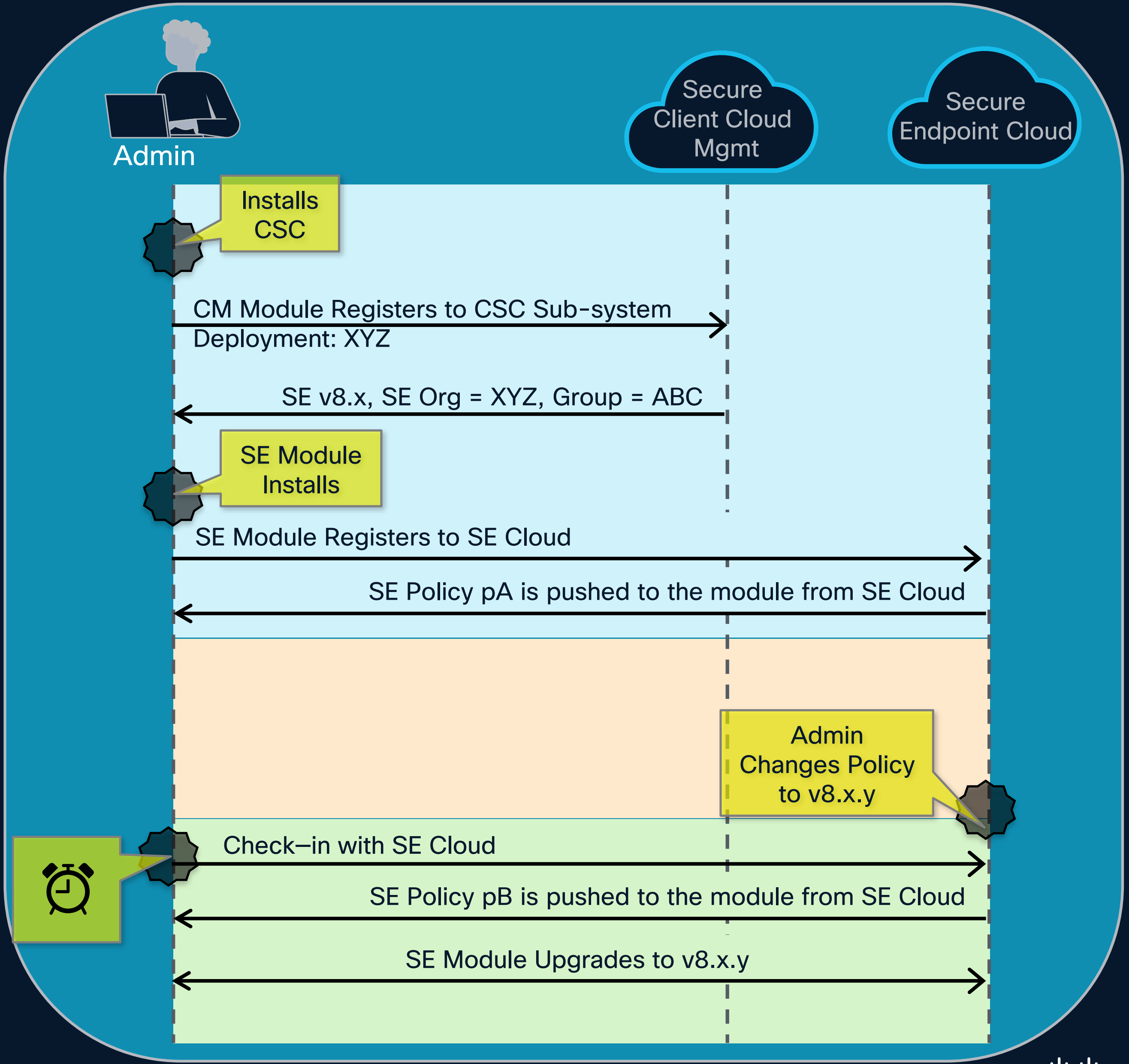
Version Control: Latest (8.4.0.30201)

Secure Endpoint Profile
Group: YazjiGroup

Replace Bootstrap Profile

Bootstrap?

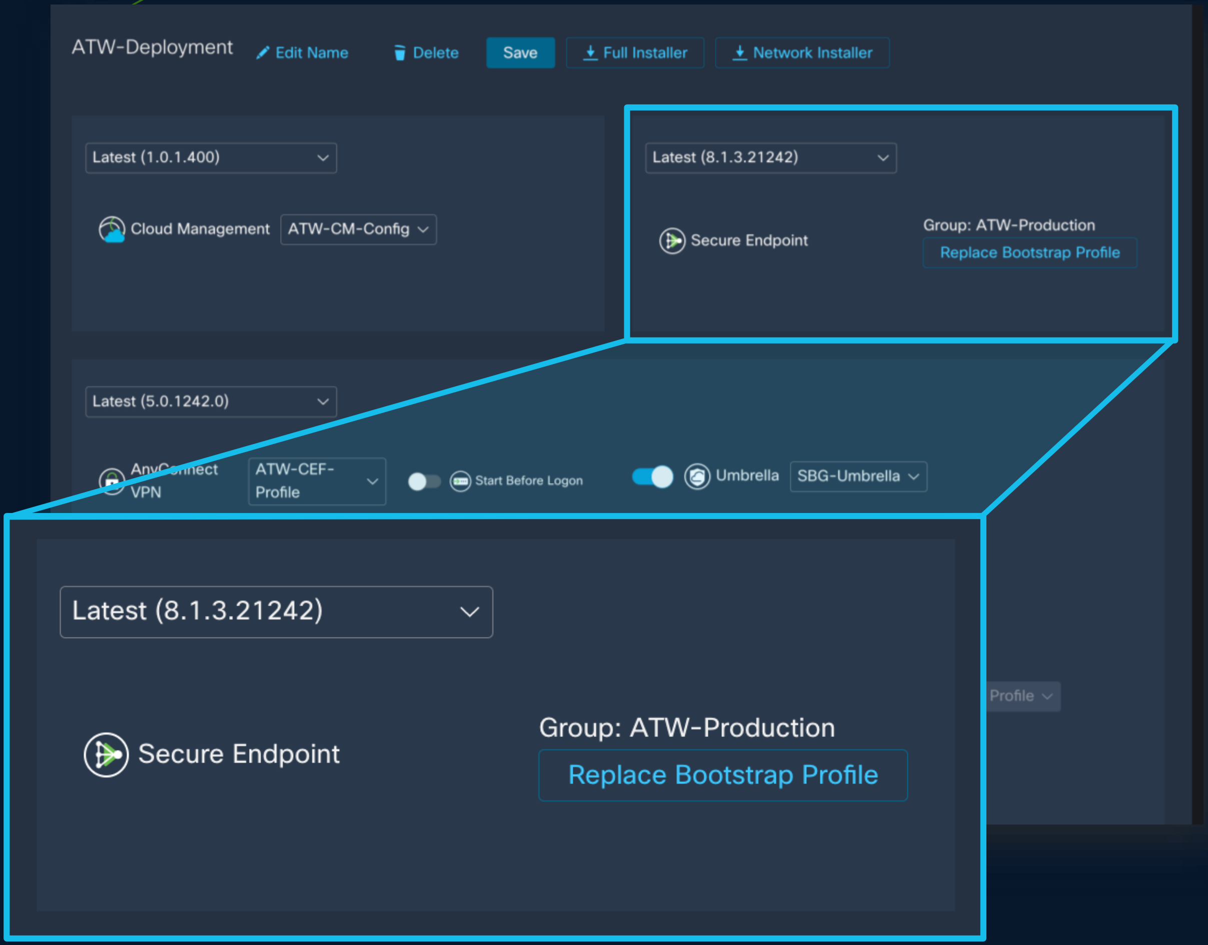
- Secure Client config is just to get the SE module to install & register to SE Cloud.
  - Then: ALL group & policy control of the SE module comes from SE Cloud.
  - SE group changes, software updates, etc...
  - Cloud Management can still update software versions through deployment.



Admin
Secure Client Cloud Mgmt
Secure Endpoint Cloud
Installs CSC
CM Module Registers to CSC Sub-system Deployment: XYZ
SE v8.x, SE Org = XYZ, Group = ABC
SE Module Installs
SE Module Registers to SE Cloud
SE Policy pA is pushed to the module from SE Cloud
Admin Changes Policy to v8.x.y
Check–in with SE Cloud
SE Policy pB is pushed to the module from SE Cloud
SE Module Upgrades to v8.x.y

Secure Endpoint Version Updates

Highest Version Wins!



ATW-Deployment · Edit Name · Delete · Save · Full Installer · Network Installer

Latest (1.0.1.400)

Cloud Management: ATW-CM-Config

Latest (8.1.3.21242)

Secure Endpoint

Group: ATW-Production

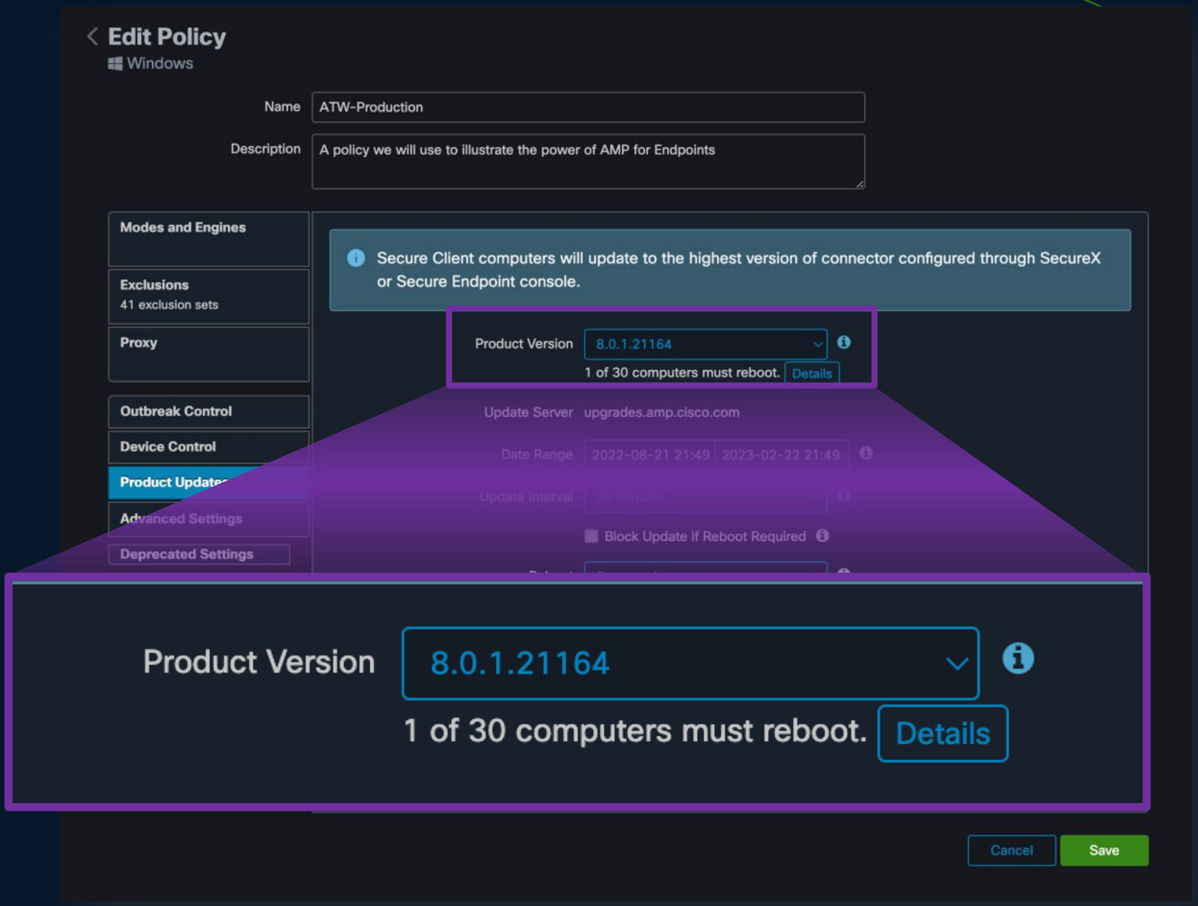
Replace Bootstrap Profile

Latest (5.0.1242.0)

AnyConnect VPN: ATW-CEF-Profile

Start Before Logon

Umbrella: SBG-Umbrella



Edit Policy

Windows

Name: ATW-Production

Description: A policy we will use to illustrate the power of AMP for Endpoints

Secure Client computers will update to the highest version of connector configured through SecureX or Secure Endpoint console.

Product Version: 8.0.1.21164

1 of 30 computers must reboot. Details

Update Server: upgrades.amp.cisco.com

Date Range: 2022-08-21 21:49 – 2023-02-22 21:49

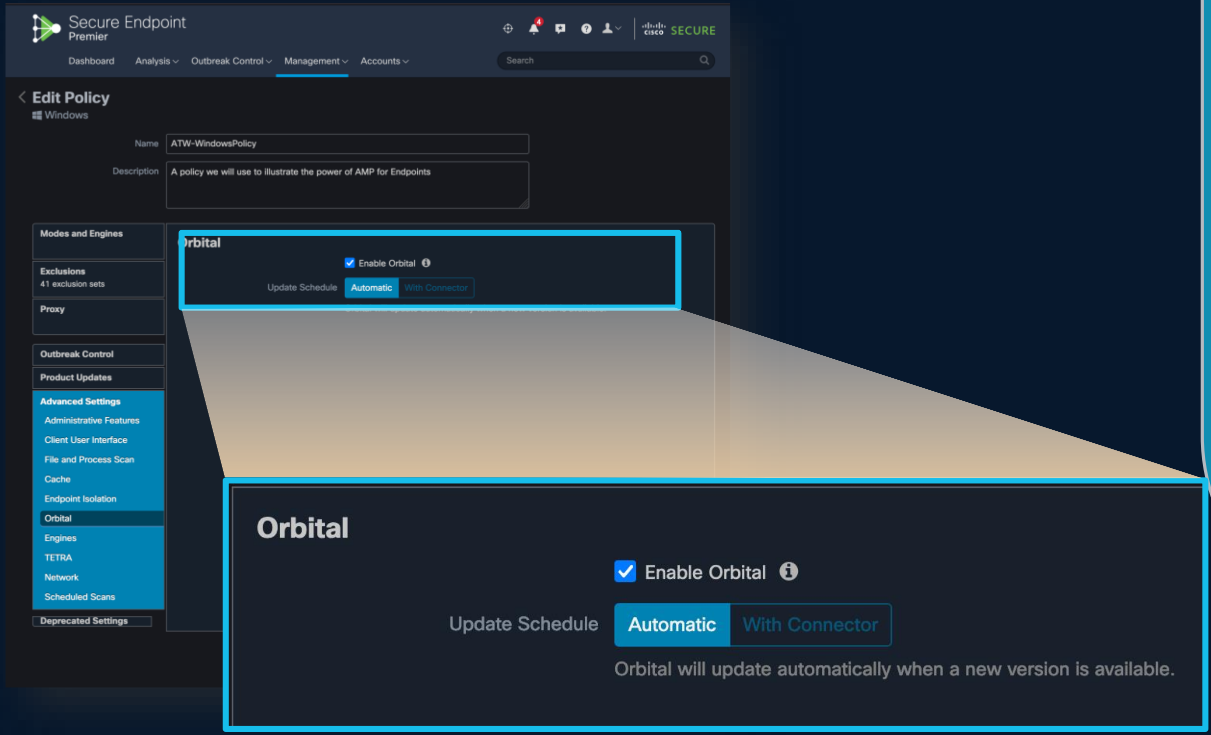
Update Interval

☐ Block Update if Reboot Required

Cancel · Save

Deploying Orbital – Option A

- Install Orbital as part of Secure Endpoint
  - Updates with SE Connector or when published on Orbital Cloud
- Controlled in Secure Endpoint UI



Edit Policy
Windows

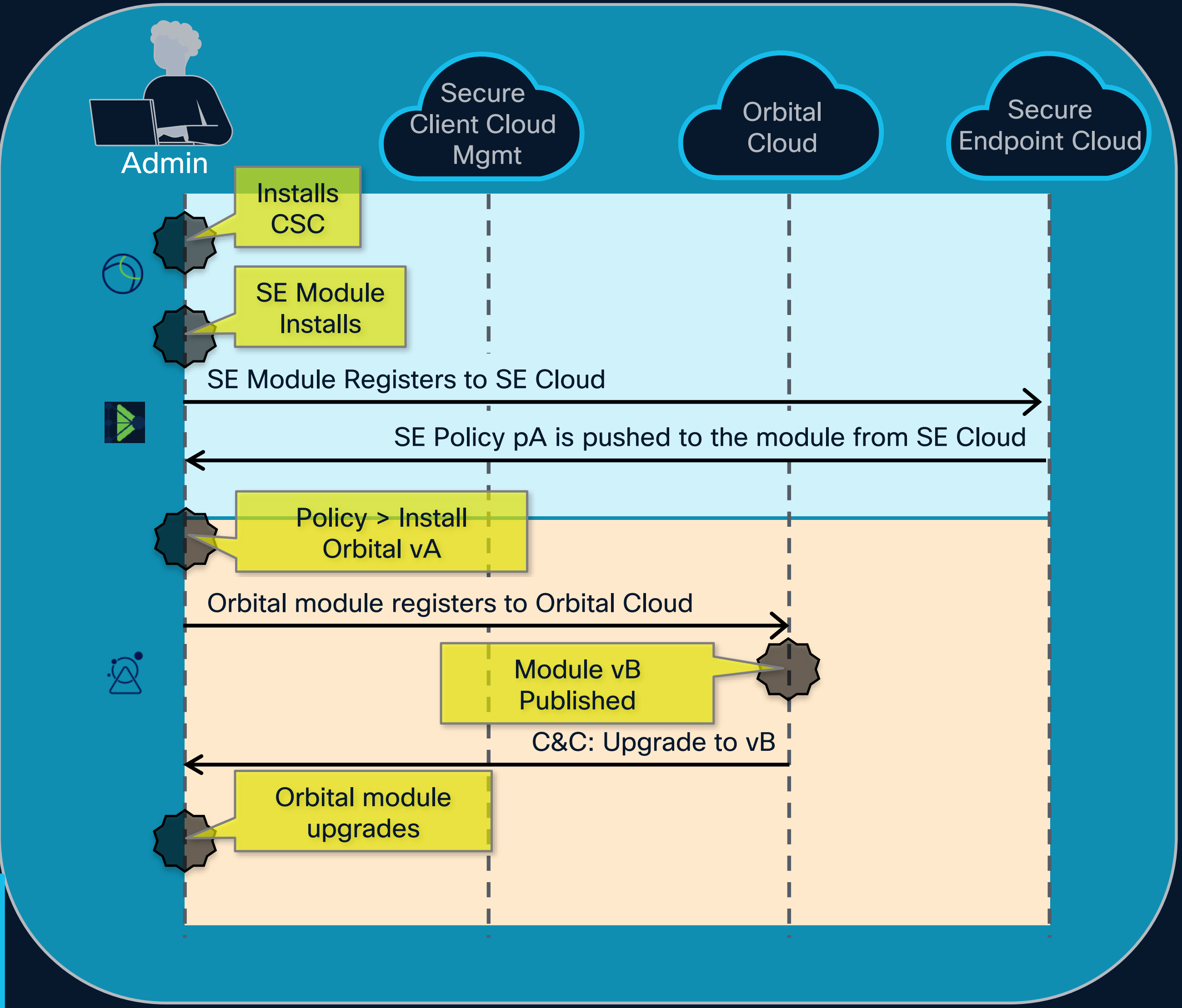
Name: ATW-WindowsPolicy
Description: A policy we will use to illustrate the power of AMP for Endpoints

Orbital

☑ Enable Orbital

Update Schedule: Automatic | With Connector

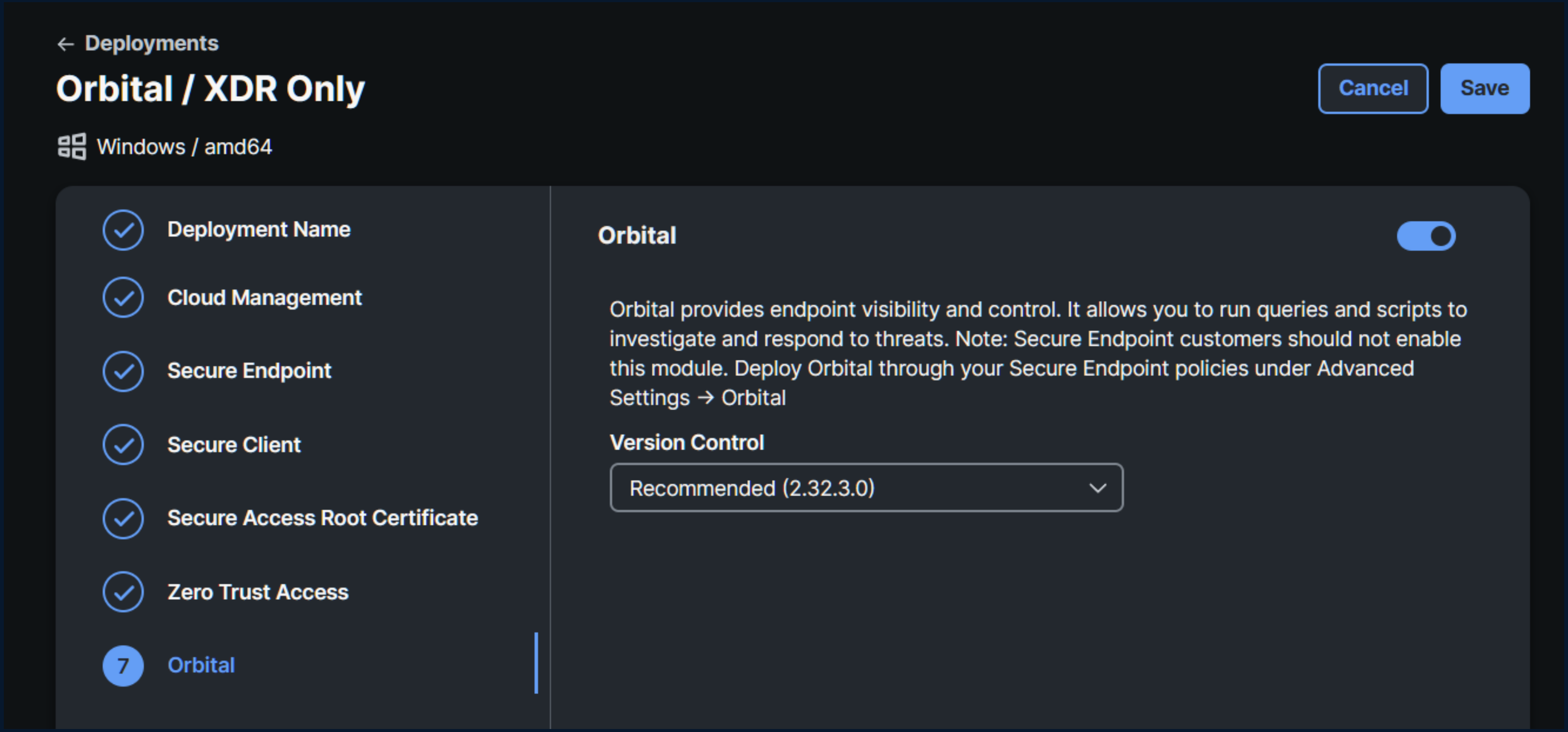
Orbital will update automatically when a new version is available.



Deploying Orbital – Option B

New Stuff!

- Install Orbital Standalone (XDR customers only)
  - Cloud Management controlled



Orbital / XDR Only

Windows / amd64

- ✓ Deployment Name
- ✓ Cloud Management
- ✓ Secure Endpoint
- ✓ Secure Client
- ✓ Secure Access Root Certificate
- ✓ Zero Trust Access
- 7 Orbital

Orbital ●

Orbital provides endpoint visibility and control. It allows you to run queries and scripts to investigate and respond to threats. Note: Secure Endpoint customers should not enable this module. Deploy Orbital through your Secure Endpoint policies under Advanced Settings → Orbital

Version Control

Recommended (2.32.3.0)

Agenda

01 CSC Overview

02 CSC Architecture

03 Cloud Deployment & Management

04 Upgrading to CSC

05 FAQs, Tips and Tricks

Upgrading

Upgrading

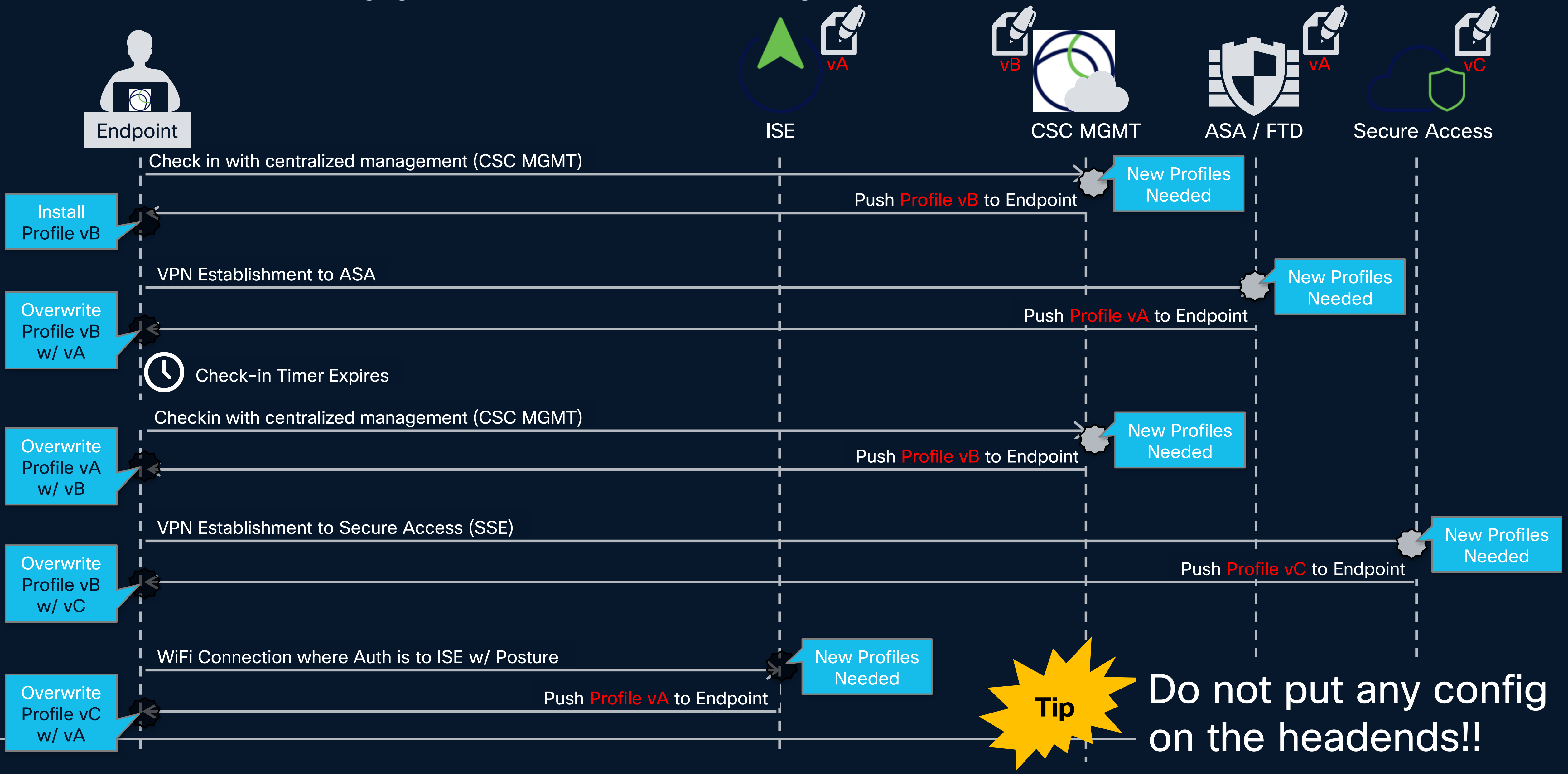
- Cisco Secure Client WILL uninstall the old versions when it is installed.
  - Cloud Install from Secure Endpoint
  - Inline upgrade from AnyConnect

  - Secure Endpoint Group behavior
    - Fresh install vs. upgrade
    - Secure Endpoint management nuances

Overwriting from other Headends

- Scenario: mismatched profiles
  - CSC deployment in cloud has a Profile vC
  - ASA group policy pushes Profile vA
    - Upon connecting to the ASA Headend, the Profile will be replaced with vA.
    - CSC Cloud Management update occurs (say C hours later), it will replace vA w/ vC.
  - This cycle will continue until the ASA and CSC deployment in Cloud Management are aligned.
- Pro Tip: Do not put any config on the headends!!

The Epic Struggle of Competing Control Points



Endpoint

ISE (vA)

CSC MGMT (vB)

ASA / FTD (vA)

Secure Access (vC)

Check in with centralized management (CSC MGMT)

New Profiles Needed

Push Profile vB to Endpoint

Install Profile vB

VPN Establishment to ASA

New Profiles Needed

Push Profile vA to Endpoint

Overwrite Profile vB w/ vA

Check-in Timer Expires

Checkin with centralized management (CSC MGMT)

New Profiles Needed

Push Profile vB to Endpoint

Overwrite Profile vA w/ vB

VPN Establishment to Secure Access (SSE)

New Profiles Needed

Push Profile vC to Endpoint

Overwrite Profile vB w/ vC

WiFi Connection where Auth is to ISE w/ Posture

New Profiles Needed

Push Profile vA to Endpoint

Overwrite Profile vC w/ vA

Tip

Do not put any config on the headends!!

Details on Profile Merges

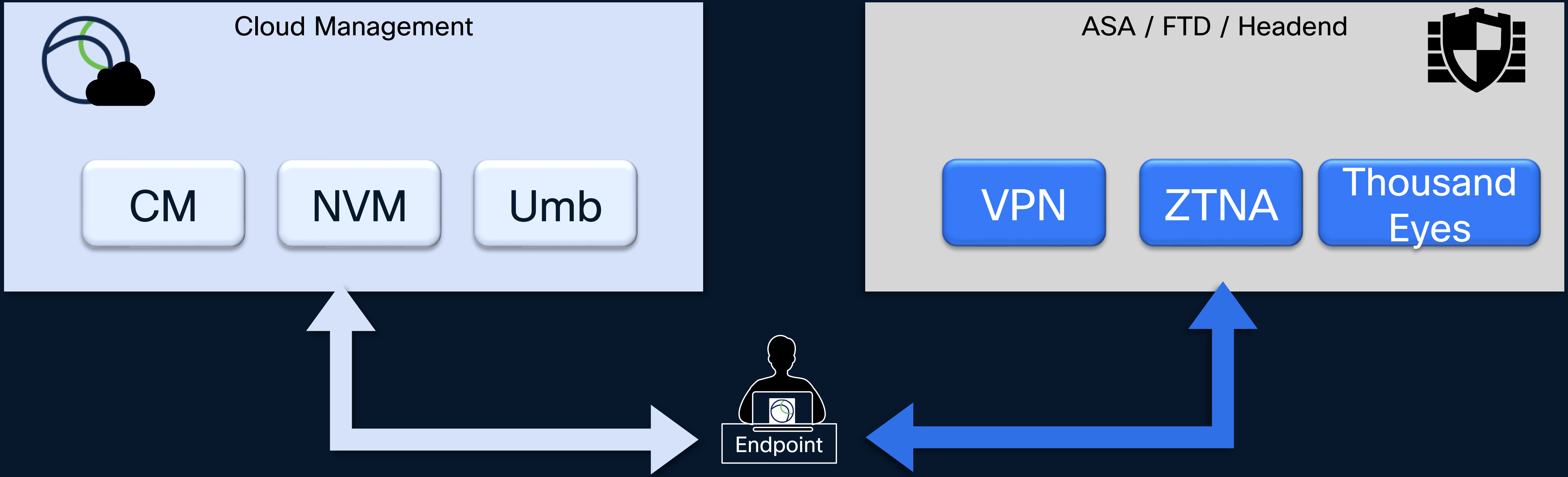
- If filenames match: ASA will overwrite the profile
- If filenames don't match: both profiles will be detected by VPN and behavior might be a little wonky... Some settings get merged from all detected profiles

- Recommendation: load the Cloud Profile immediately on the ASA with same Filename

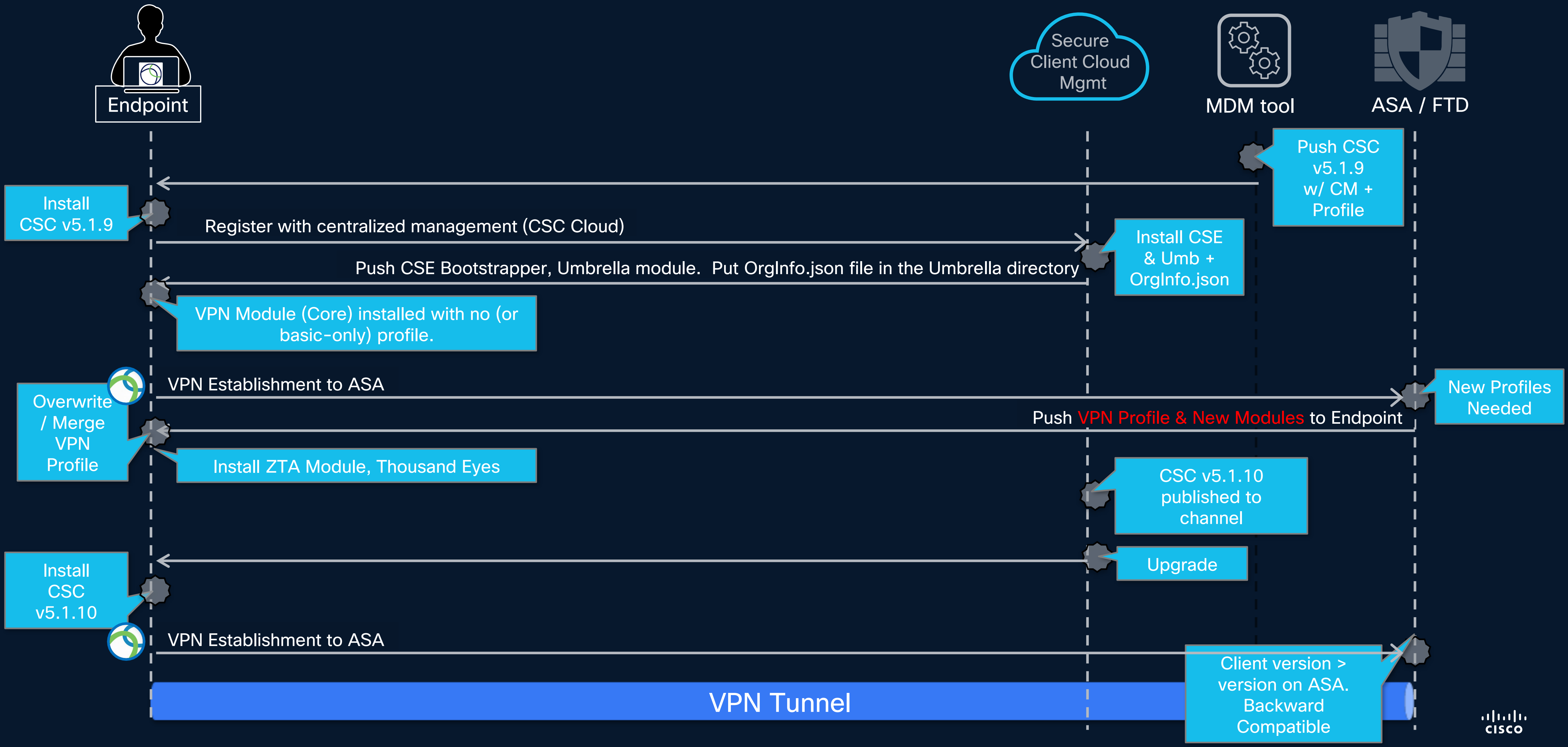
Do not put any config on the headends!!

Hybrid (Headend & Cloud)

- Cloud management **does not** have to manage all modules
- Cloud Management **can not** manage all modules (yet...)
  - The profiles (configs) can come from either place
  - Recommended to not host the same module profiles in multiple locations



Hybrid (Headend & Cloud)



Endpoint

Secure Client Cloud Mgmt

MDM tool

ASA / FTD

Push CSC v5.1.9 w/ CM + Profile

Install CSC v5.1.9

Register with centralized management (CSC Cloud)

Install CSE & Umb + OrgInfo.json

Push CSE Bootstrapper, Umbrella module. Put OrgInfo.json file in the Umbrella directory

VPN Module (Core) installed with no (or basic-only) profile.

VPN Establishment to ASA

New Profiles Needed

Push VPN Profile & New Modules to Endpoint

Overwrite / Merge VPN Profile

Install ZTA Module, Thousand Eyes

CSC v5.1.10 published to channel

Upgrade

Install CSC v5.1.10

VPN Establishment to ASA

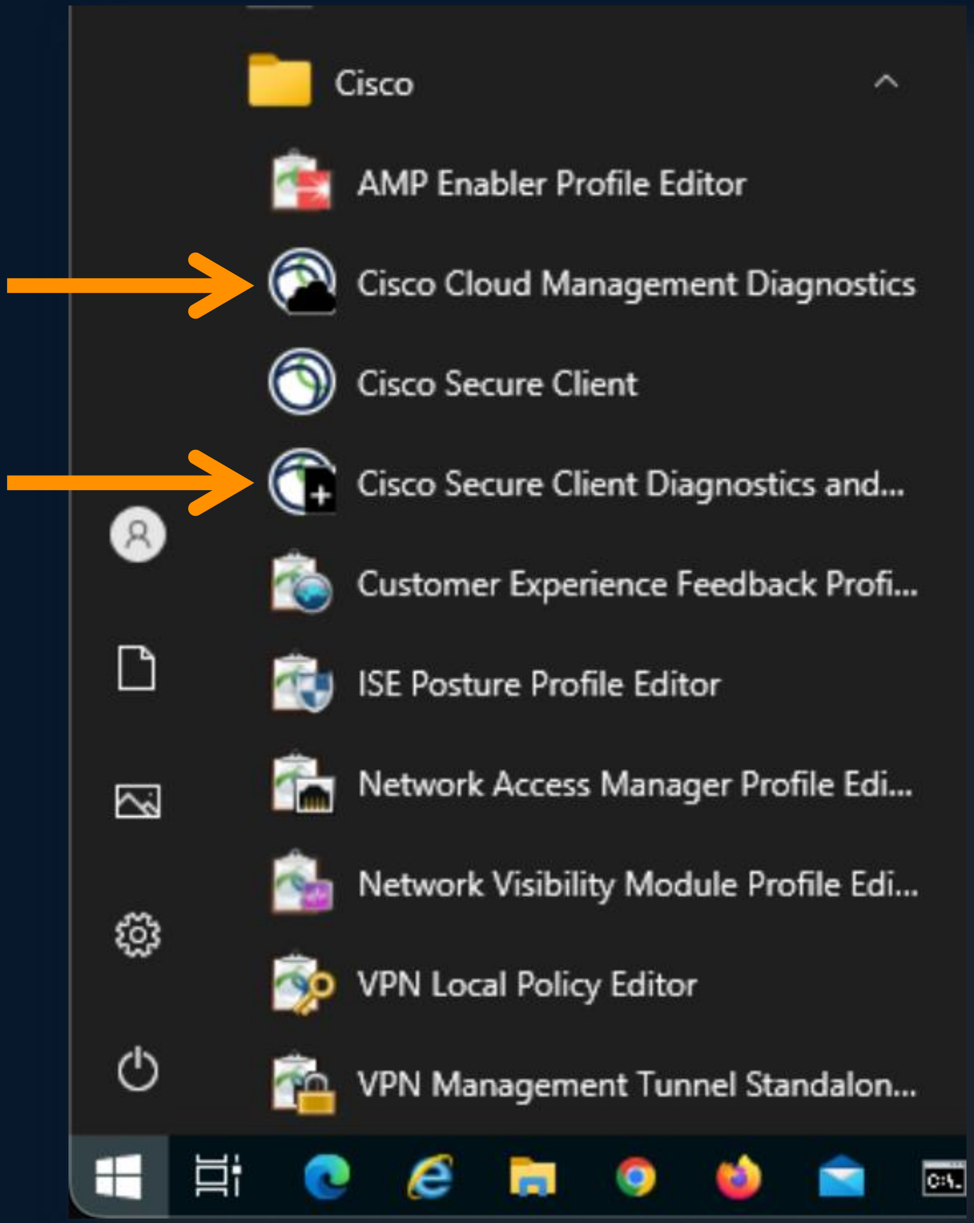
Client version > version on ASA. Backward Compatible

VPN Tunnel

Secure Client Diagnostics

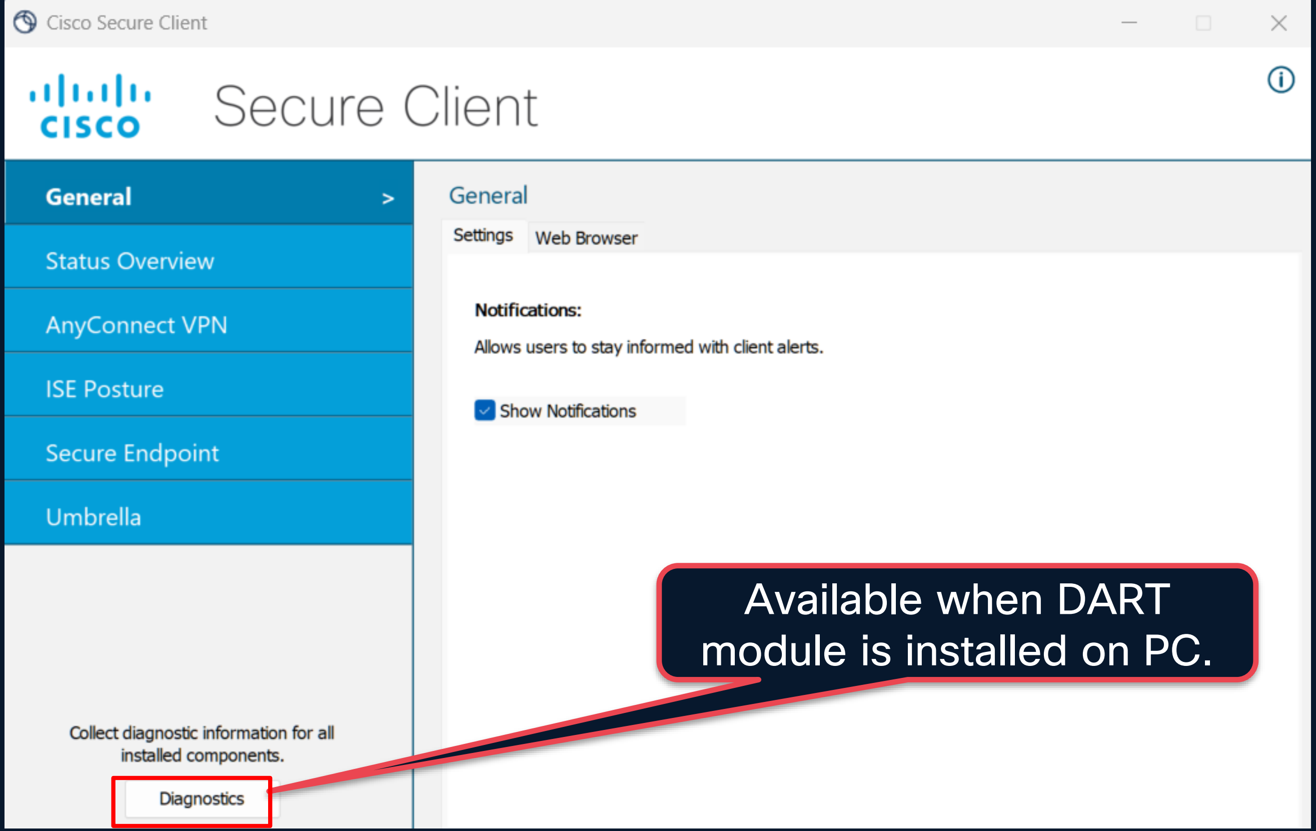
- *“Dart or it Didn’t Happen”*
- DART is still the perfect endpoint troubleshooting bundling tool.
- Only available if you install it.

- What about for troubleshooting Cloud Management only?
  - Cloud Management Diagnostics


Cisco
AMP Enabler Profile Editor
Cisco Cloud Management Diagnostics
Cisco Secure Client
Cisco Secure Client Diagnostics and...
Customer Experience Feedback Profi...
ISE Posture Profile Editor
Network Access Manager Profile Edi...
Network Visibility Module Profile Edi...
VPN Local Policy Editor
VPN Management Tunnel Standalon...

The DART “Bundle”

- DART is the Secure Client tool to collect data for troubleshooting installation and connection problems.



Notifications:

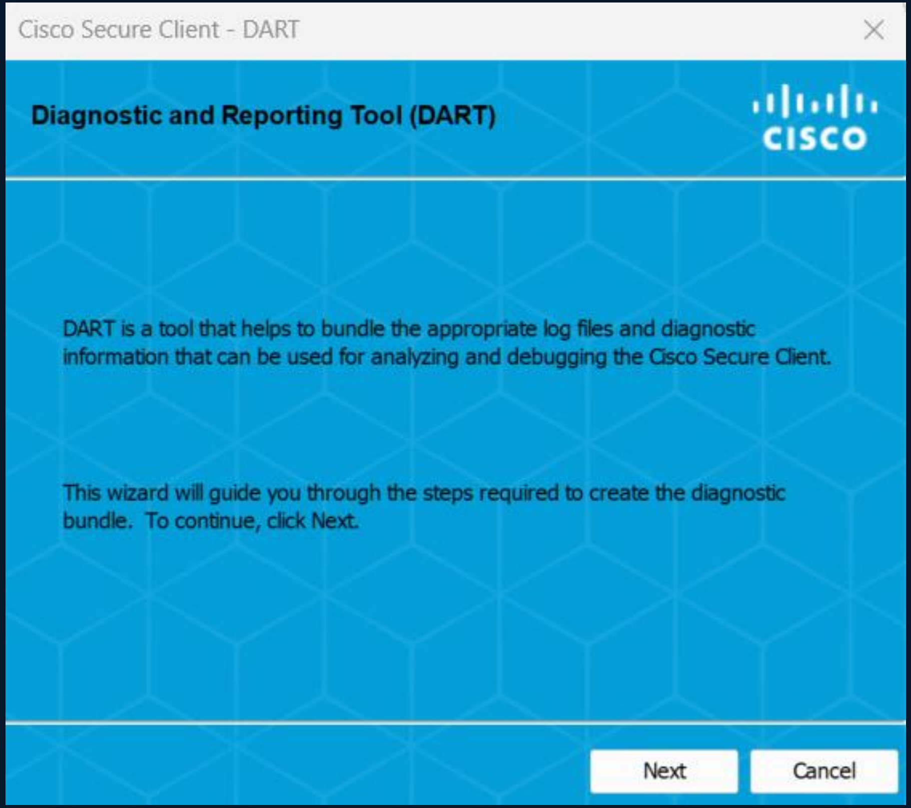
Allows users to stay informed with client alerts.

☑ Show Notifications

Collect diagnostic information for all installed components.

Diagnostics

Available when DART module is installed on PC.



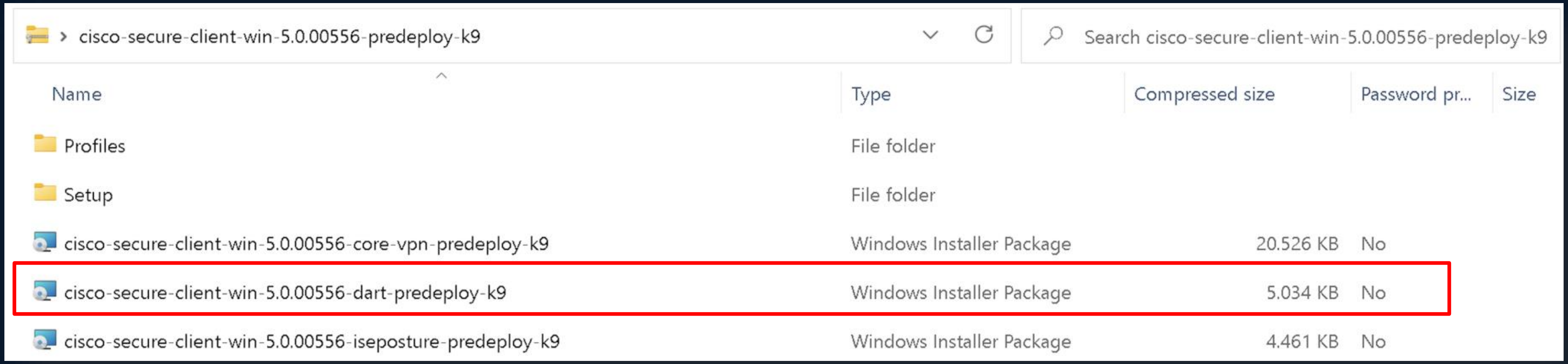
Diagnostic and Reporting Tool (DART)

DART is a tool that helps to bundle the appropriate log files and diagnostic information that can be used for analyzing and debugging the Cisco Secure Client.

This wizard will guide you through the steps required to create the diagnostic bundle. To continue, click Next.

DART Module Installation

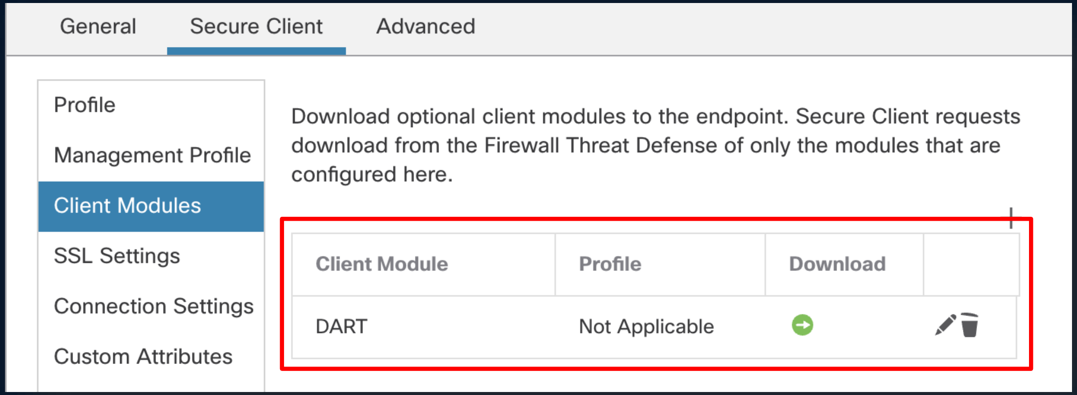
- The DART can be installed manually using the **msi** file included in the the pre-deploy package:



cisco-secure-client-win-5.0.00556-predeploy-k9
Search cisco-secure-client-win-5.0.00556-predeploy-k9

Name	Type	Compressed size	Password pr...	Size
Profiles	File folder			
Setup	File folder			
cisco-secure-client-win-5.0.00556-core-vpn-predeploy-k9	Windows Installer Package	20.526 KB	No	
cisco-secure-client-win-5.0.00556-dart-predeploy-k9	Windows Installer Package	5.034 KB	No	
cisco-secure-client-win-5.0.00556-iseposture-predeploy-k9	Windows Installer Package	4.461 KB	No	

- Another option is enabling DART module configuration under the Group Policy:



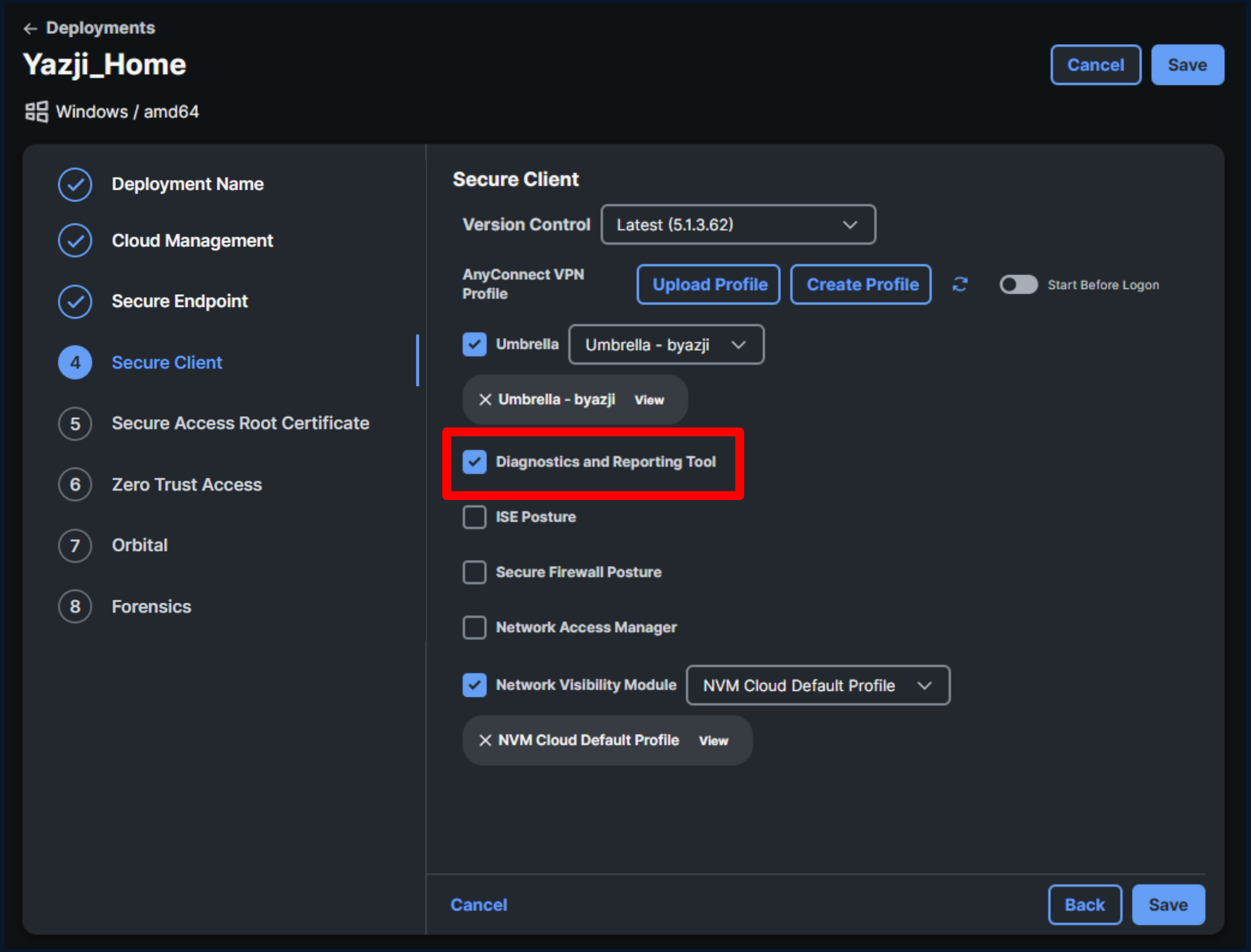
Download optional client modules to the endpoint. Secure Client requests download from the Firewall Threat Defense of only the modules that are configured here.

Client Module	Profile	Download	
DART	Not Applicable	●	

```
ASA# show run group-policy GPA
group-policy GPA attributes
 [..]
 webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
```

DART Module Installation

- Enabled in Cloud Management



← Deployments

Yazji_Home

Windows / amd64

Cancel Save

1. Deployment Name
2. Cloud Management
3. Secure Endpoint
4. Secure Client
5. Secure Access Root Certificate
6. Zero Trust Access
7. Orbital
8. Forensics

Secure Client

Version Control: Latest (5.1.3.62)

AnyConnect VPN Profile: Upload Profile | Create Profile | Start Before Logon

☑ Umbrella: Umbrella - byazji

× Umbrella - byazji View

☑ Diagnostics and Reporting Tool

□ ISE Posture

□ Secure Firewall Posture

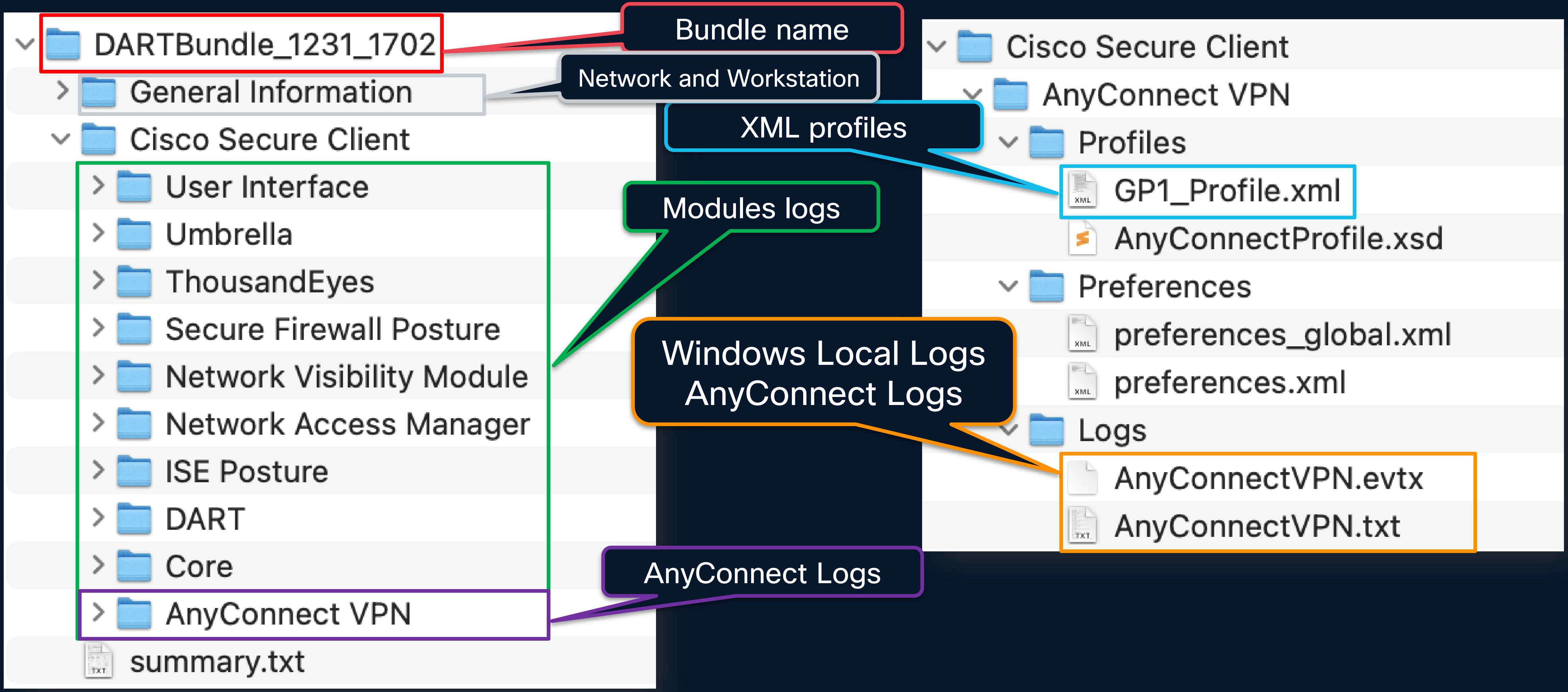
□ Network Access Manager

☑ Network Visibility Module: NVM Cloud Default Profile

× NVM Cloud Default Profile View

Cancel | Back | Save

Reviewing DART Bundle Content



DARTBundle_1231_1702
- General Information
- Cisco Secure Client
  - User Interface
  - Umbrella
  - ThousandEyes
  - Secure Firewall Posture
  - Network Visibility Module
  - Network Access Manager
  - ISE Posture
  - DART
  - Core
  - AnyConnect VPN
- summary.txt

Cisco Secure Client
- AnyConnect VPN
  - Profiles
    - GP1_Profile.xml
    - AnyConnectProfile.xsd
  - Preferences
    - preferences_global.xml
    - preferences.xml
  - Logs
    - AnyConnectVPN.evtx
    - AnyConnectVPN.txt

Bundle name

Network and Workstation

XML profiles

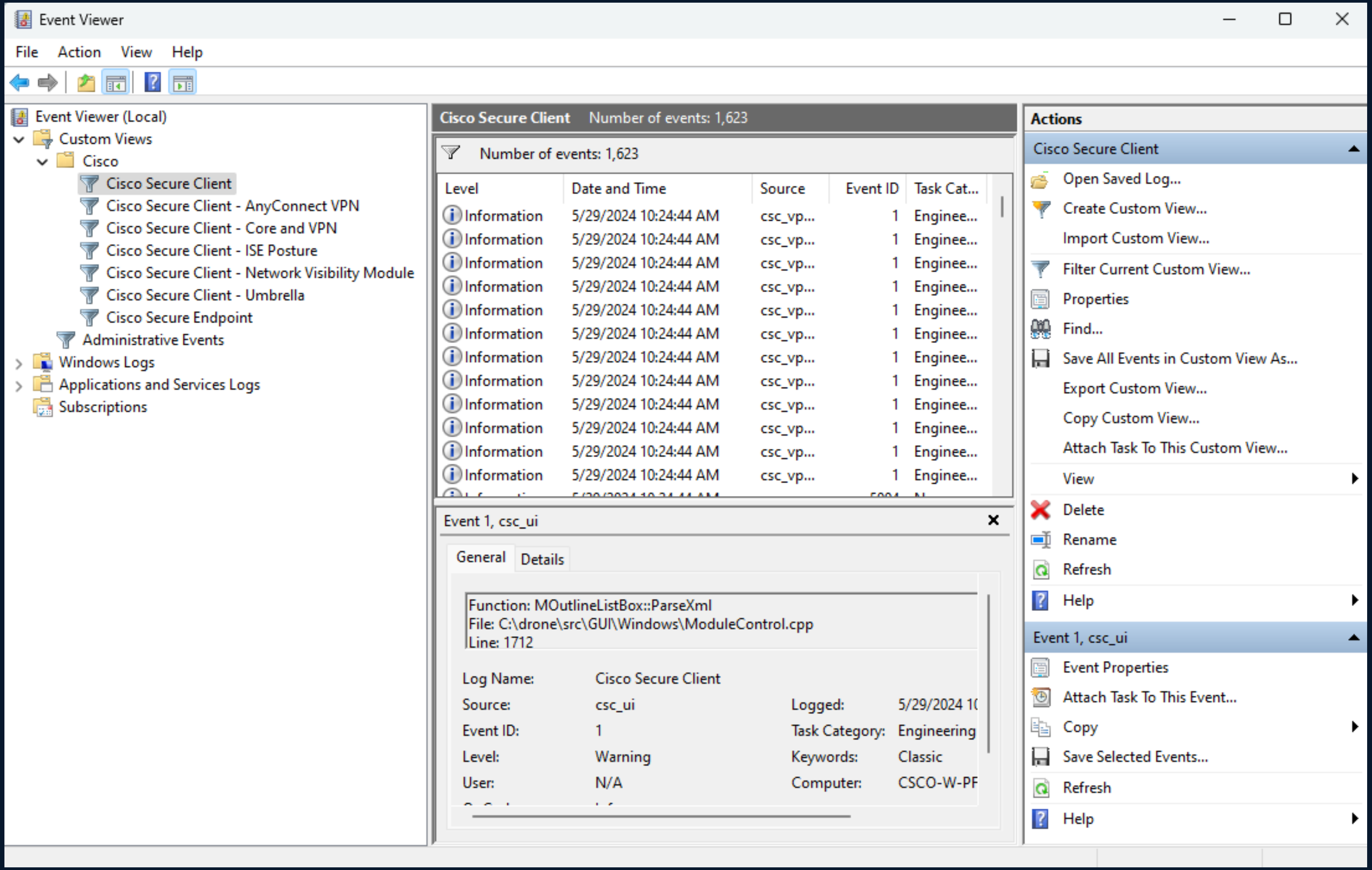
Modules logs

Windows Local Logs
AnyConnect Logs

AnyConnect Logs

Secure Client Events / Logs

- All client-side logs for CSC are in the Windows Event Log
  - Secure Endpoint
  - All Secure Client Modules



Cisco Secure Client Number of events: 1,623

Number of events: 1,623

Level	Date and Time	Source	Event ID	Task Cat...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...
Information	5/29/2024 10:24:44 AM	csc_vp...	1	Enginee...

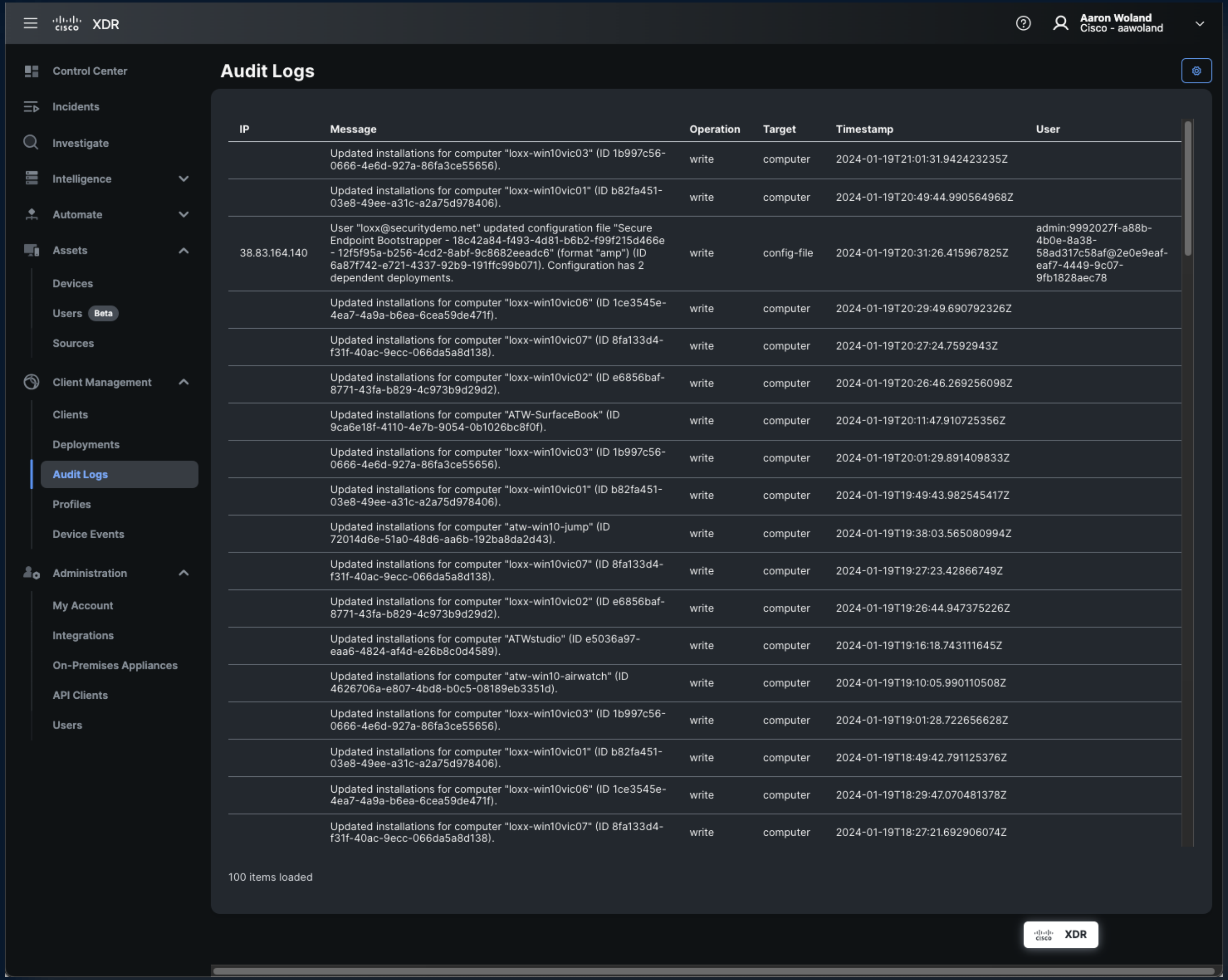
Event 1, csc_ui

```
Function: MOutlineListBox::ParseXml
File: C:\drone\src\GUI\Windows\ModuleControl.cpp
Line: 1712
```

Log Name:	Cisco Secure Client		
Source:	csc_ui	Logged:	5/29/2024 1(
Event ID:	1	Task Category:	Engineering
Level:	Warning	Keywords:	Classic
User:	N/A	Computer:	CSCO-W-PF

Cloud Audit Logging

- An audit trail for all activity related to the management of CSC.
    - Deployment Updates
    - Profile Uploads / Creations
    - Deletions
    - Etc.
- 6 month retention



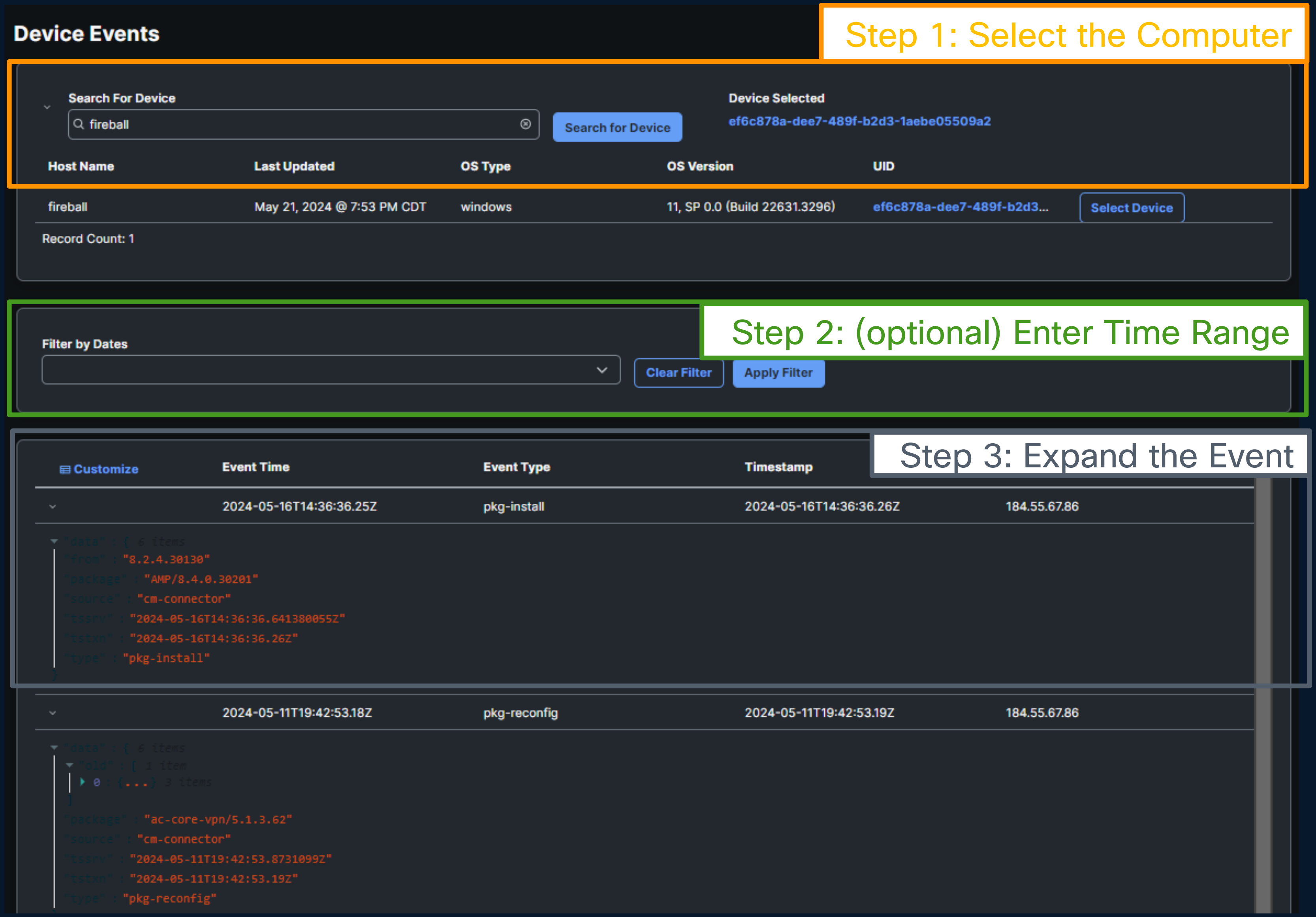
Audit Logs

IP	Message	Operation	Target	Timestamp	User
	Updated installations for computer "loxx-win10vic03" (ID 1b997c56-0666-4e6d-927a-86fa3ce55656).	write	computer	2024-01-19T21:01:31.942423235Z	
	Updated installations for computer "loxx-win10vic01" (ID b82fa451-03e8-49ee-a31c-a2a75d978406).	write	computer	2024-01-19T20:49:44.990564968Z	
38.83.164.140	User "loxx@securitydemo.net" updated configuration file "Secure Endpoint Bootstrapper - 18c42a84-f493-4d81-b6b2-f99f215d466e - 12f5f95a-b256-4cd2-8abf-9c8682eeadc6" (format "amp") (ID 6a87f742-e721-4337-92b9-191ffc99b071). Configuration has 2 dependent deployments.	write	config-file	2024-01-19T20:31:26.415967825Z	admin:9992027f-a88b-4b0e-8a38-58ad317c58af@2e0e9eaf-eaf7-4449-9c07-9fb1828aec78
	Updated installations for computer "loxx-win10vic06" (ID 1ce3545e-4ea7-4a9a-b6ea-6cea59de471f).	write	computer	2024-01-19T20:29:49.690792326Z	
	Updated installations for computer "loxx-win10vic07" (ID 8fa133d4-f31f-40ac-9ecc-066da5a8d138).	write	computer	2024-01-19T20:27:24.7592943Z	
	Updated installations for computer "loxx-win10vic02" (ID e6856baf-8771-43fa-b829-4c973b9d29d2).	write	computer	2024-01-19T20:26:46.269256098Z	
	Updated installations for computer "ATW-SurfaceBook" (ID 9ca6e18f-4110-4e7b-9054-0b1026bc8f0f).	write	computer	2024-01-19T20:11:47.910725356Z	
	Updated installations for computer "loxx-win10vic03" (ID 1b997c56-0666-4e6d-927a-86fa3ce55656).	write	computer	2024-01-19T20:01:29.891409833Z	
	Updated installations for computer "loxx-win10vic01" (ID b82fa451-03e8-49ee-a31c-a2a75d978406).	write	computer	2024-01-19T19:49:43.982545417Z	
	Updated installations for computer "atw-win10-jump" (ID 72014d6e-51a0-48d6-aa6b-192ba8da2d43).	write	computer	2024-01-19T19:38:03.565080994Z	
	Updated installations for computer "loxx-win10vic07" (ID 8fa133d4-f31f-40ac-9ecc-066da5a8d138).	write	computer	2024-01-19T19:27:23.42866749Z	
	Updated installations for computer "loxx-win10vic02" (ID e6856baf-8771-43fa-b829-4c973b9d29d2).	write	computer	2024-01-19T19:26:44.947375226Z	
	Updated installations for computer "ATWstudio" (ID e5036a97-eaa6-4824-af4d-e26b8c0d4589).	write	computer	2024-01-19T19:16:18.743111645Z	
	Updated installations for computer "atw-win10-airwatch" (ID 4626706a-e807-4bd8-b0c5-08189eb3351d).	write	computer	2024-01-19T19:10:05.990110508Z	
	Updated installations for computer "loxx-win10vic03" (ID 1b997c56-0666-4e6d-927a-86fa3ce55656).	write	computer	2024-01-19T19:01:28.722656628Z	
	Updated installations for computer "loxx-win10vic01" (ID b82fa451-03e8-49ee-a31c-a2a75d978406).	write	computer	2024-01-19T18:49:42.791125376Z	
	Updated installations for computer "loxx-win10vic06" (ID 1ce3545e-4ea7-4a9a-b6ea-6cea59de471f).	write	computer	2024-01-19T18:29:47.070481378Z	
	Updated installations for computer "loxx-win10vic07" (ID 8fa133d4-f31f-40ac-9ecc-066da5a8d138).	write	computer	2024-01-19T18:27:21.692906074Z	

100 items loaded

Device Event Logging

- Events where client interacts with cloud:
  - Installations
  - Failures
  - Cloud Related errors
- NOT local logs from device
- 12 month retention



Step 1: Select the Computer

Step 2: (optional) Enter Time Range

Step 3: Expand the Event

Device Events

Search For Device: fireball

Device Selected
ef6c878a-dee7-489f-b2d3-1aebe05509a2

Host Name	Last Updated	OS Type	OS Version	UID	
fireball	May 21, 2024 @ 7:53 PM CDT	windows	11, SP 0.0 (Build 22631.3296)	ef6c878a-dee7-489f-b2d3...	Select Device

Record Count: 1

Filter by Dates

Event Time	Event Type	Timestamp	
2024-05-16T14:36:36.25Z	pkg-install	2024-05-16T14:36:36.26Z	184.55.67.86

```
"data" : { 6 items
  "from" : "8.2.4.30130"
  "package" : "AMP/8.4.0.30201"
  "source" : "cm-connector"
  "tssrv" : "2024-05-16T14:36:36.641380055Z"
  "tstxn" : "2024-05-16T14:36:36.26Z"
  "type" : "pkg-install"
}
```

Event Time	Event Type	Timestamp	
2024-05-11T19:42:53.18Z	pkg-reconfig	2024-05-11T19:42:53.19Z	184.55.67.86

```
"data" : { 6 items
  "old" : [ 1 item
    0 : {...} 3 items
  ]
  "package" : "ac-core-vpn/5.1.3.62"
  "source" : "cm-connector"
  "tssrv" : "2024-05-11T19:42:53.8731099Z"
  "tstxn" : "2024-05-11T19:42:53.19Z"
  "type" : "pkg-reconfig"
```

Agenda

01 CSC Overview

02 CSC Architecture

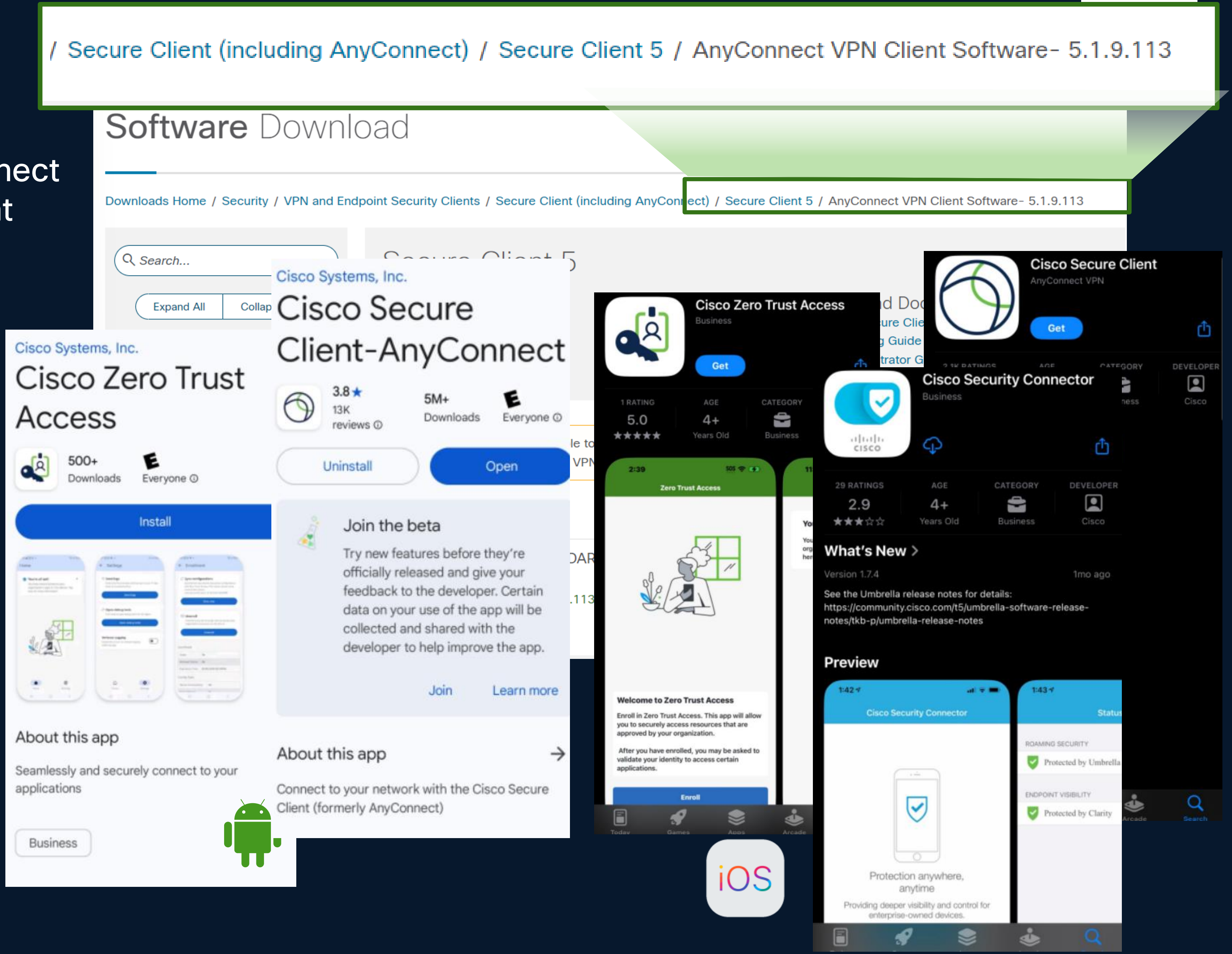
03 Cloud Deployment & Management

04 Upgrading to CSC

05 FAQs, Tips and Tricks

CSC for non-Windows/Mac

- Windows, Mac and Linux Cisco AnyConnect has been **rebranded** Cisco Secure Client
- Linux and mobile apps - No additional features compared to Secure Client
  - Not cloud managed
  - Not integrated with Secure Endpoint (yet)
  - Purpose built apps



/ Secure Client (including AnyConnect) / Secure Client 5 / AnyConnect VPN Client Software- 5.1.9.113

Software Download

Downloads Home / Security / VPN and Endpoint Security Clients / Secure Client (including AnyConnect) / Secure Client 5 / AnyConnect VPN Client Software- 5.1.9.113

Cisco Systems, Inc.

Cisco Zero Trust Access

500+ Downloads · Everyone

About this app

Seamlessly and securely connect to your applications

Cisco Systems, Inc.

Cisco Secure Client-AnyConnect

3.8★ 13K reviews · 5M+ Downloads · Everyone

Join the beta

Try new features before they're officially released and give your feedback to the developer. Certain data on your use of the app will be collected and shared with the developer to help improve the app.

About this app

Connect to your network with the Cisco Secure Client (formerly AnyConnect)

Cisco Zero Trust Access

Business

1 RATING	AGE	CATEGORY
5.0 ★★★★★	4+ Years Old	Business

Zero Trust Access

Welcome to Zero Trust Access

Enroll in Zero Trust Access. This app will allow you to securely access resources that are approved by your organization.

After you have enrolled, you may be asked to validate your identity to access certain applications.

Cisco Secure Client

AnyConnect VPN

Cisco Security Connector

Business

29 RATINGS	AGE	CATEGORY	DEVELOPER
2.9 ★★★☆☆	4+ Years Old	Business	Cisco

What's New >

Version 1.7.4 · 1mo ago

See the Umbrella release notes for details: https://community.cisco.com/t5/umbrella-software-release-notes/tkb-p/umbrella-release-notes

Preview

Cisco Security Connector

Protection anywhere, anytime

Providing deeper visibility and control for enterprise-owned devices.

Frequently Asked Questions

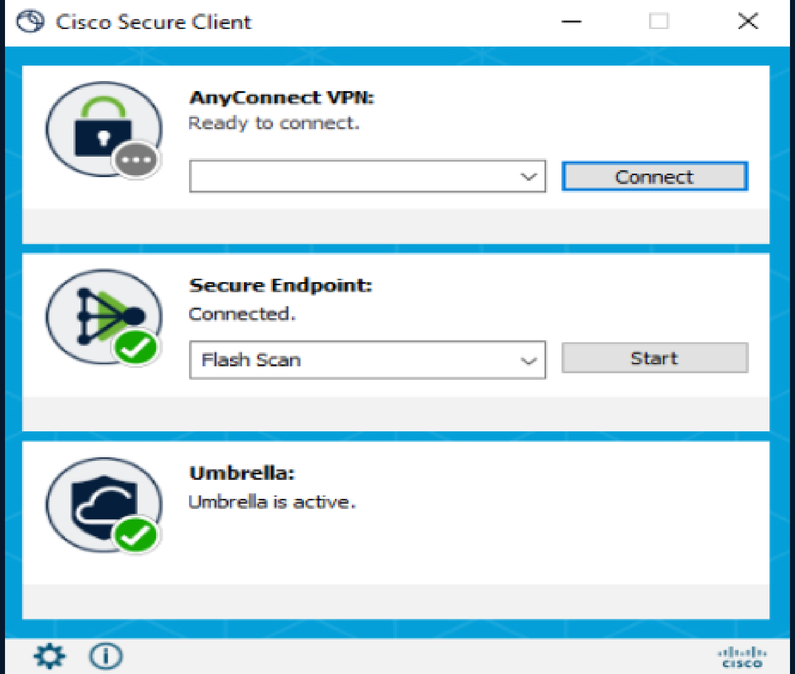
- Traditional Secure Client modules are still version locked together
- Duo is not in Secure Client yet
- Win/macOS Cloud Mgmt
- Linux – no firm dates

- A profile may only be in up to 45 deployments
  - TAC case to extend it
- Secure Client may be used with or without the Cloud Management, except XDR
- No “web-deploy” package for the Cloud-Management Module

Common Ask:
Hide that VPN Module

“I just have Umbrella or Secure Endpoint, I don’t want to confuse my users”

“We do not use AnyConnect, why is it there?”



Cisco Secure Client

AnyConnect VPN:
Ready to connect.

Secure Endpoint:
Connected.

Flash Scan

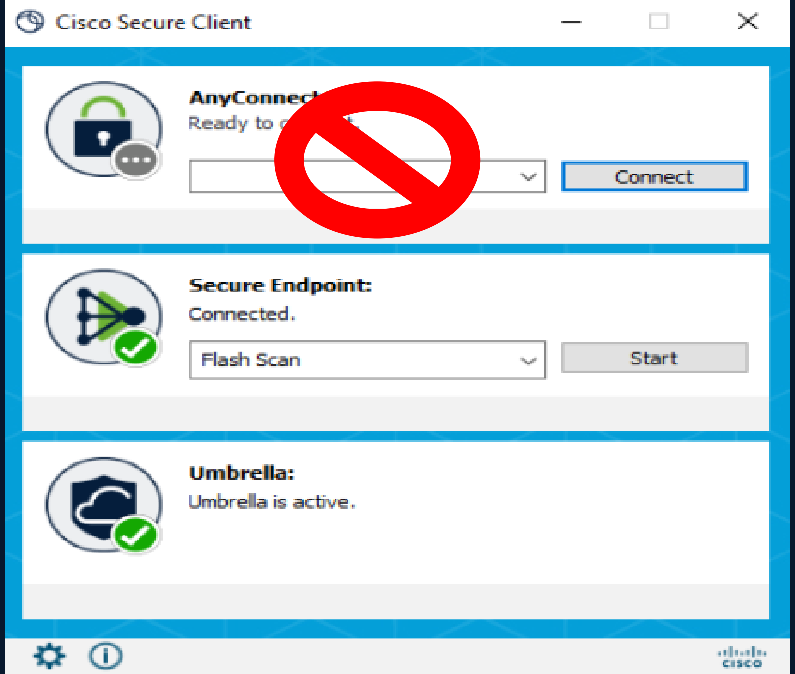
Umbrella:
Umbrella is active.

https://support.umbrella.com/hc/en-us/articles/18211951038740-How-to-hide-the-VPN-module-in-Cisco-Secure-Client-Windows

Common Ask:
Hide that VPN Module

“I just have Umbrella or Secure Endpoint, I don’t want to confuse my users”

“We do not use AnyConnect, why is it there?”



Cisco Secure Client

AnyConnect

Ready to c

Secure Endpoint:

Connected.

Flash Scan

Umbrella:

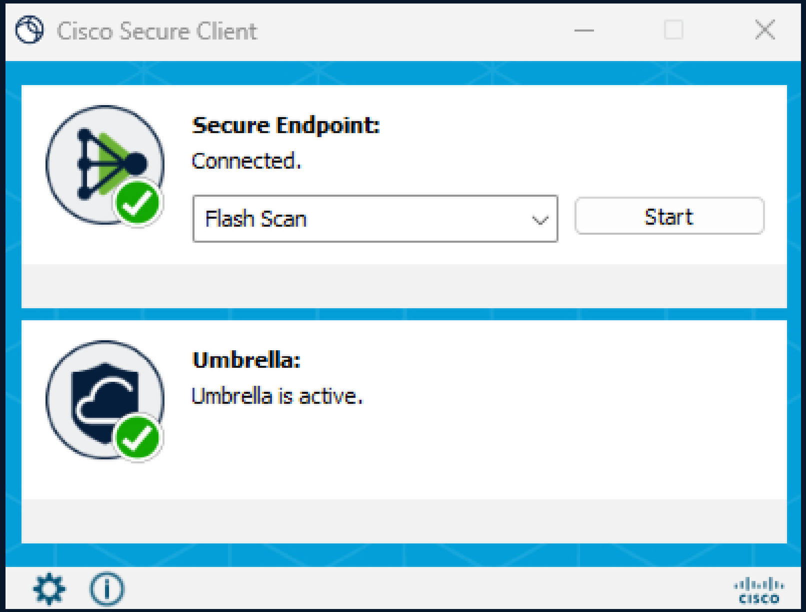
Umbrella is active.

https://support.umbrella.com/hc/en-us/articles/18211951038740-How-to-hide-the-VPN-module-in-Cisco-Secure-Client-Windows

Common Ask:
Hide that VPN Module

“I just have Umbrella or Secure Endpoint, I don’t want to confuse my users”

“We do not use AnyConnect, why is it there?”



Cisco Secure Client

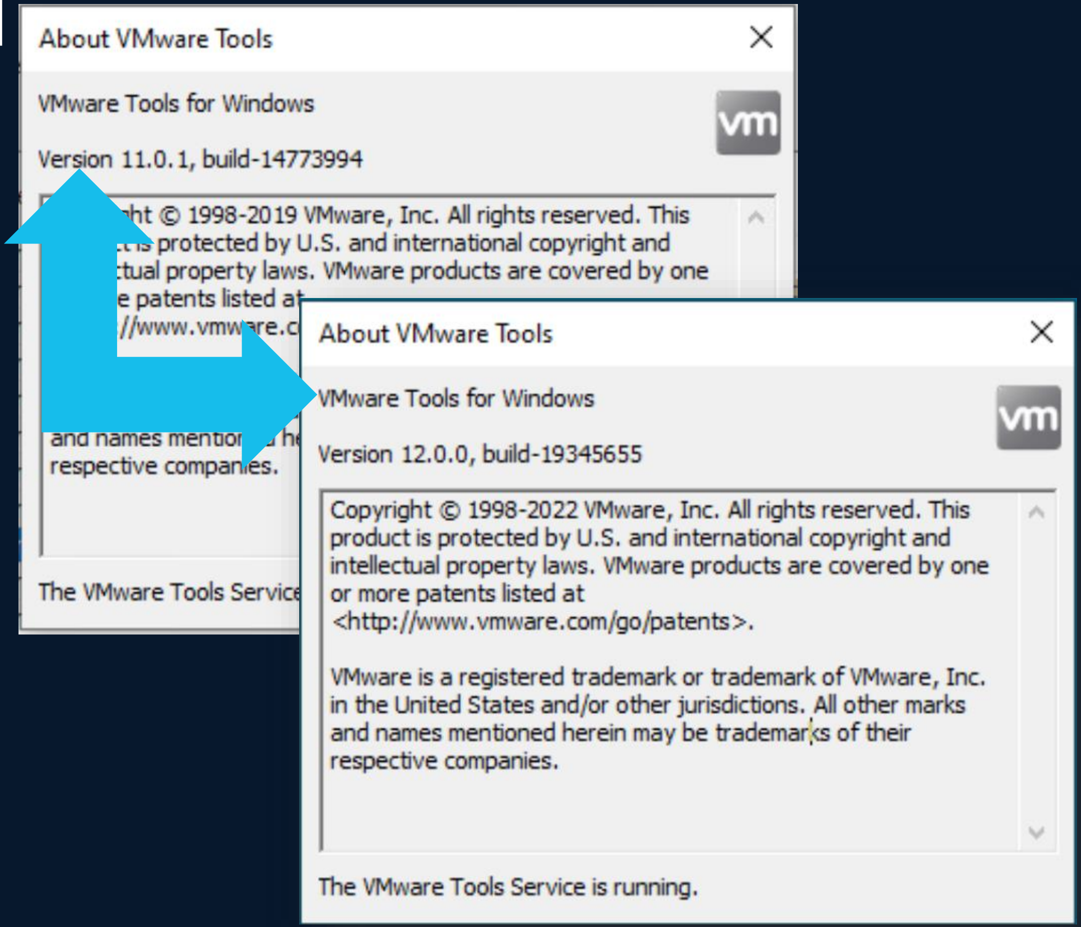
Secure Endpoint:
Connected.

Umbrella:
Umbrella is active.

https://support.umbrella.com/hc/en-us/articles/18211951038740-How-to-hide-the-VPN-module-in-Cisco-Secure-Client-Windows

Common Issue: Installing on VM

- Fyne error: window creation error
- CSC will not install on VMWare Virtual Machine
  - **Cause**: VMTools is outdated / Missing Open GL drivers
  - **Solution**: Upgrade to latest VMTools, install Mesa OpenGL or do command line
    - CLI install with a -q option



About VMware Tools

VMware Tools for Windows

Version 11.0.1, build-14773994

ght © 1998-2019 VMware, Inc. All rights reserved. This
t is protected by U.S. and international copyright and
ctual property laws. VMware products are covered by one
e patents listed at
//www.vmware.c

and names mentio he
respective companies.

The VMware Tools Servic

About VMware Tools

VMware Tools for Windows

Version 12.0.0, build-19345655

Copyright © 1998-2022 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

The VMware Tools Service is running.

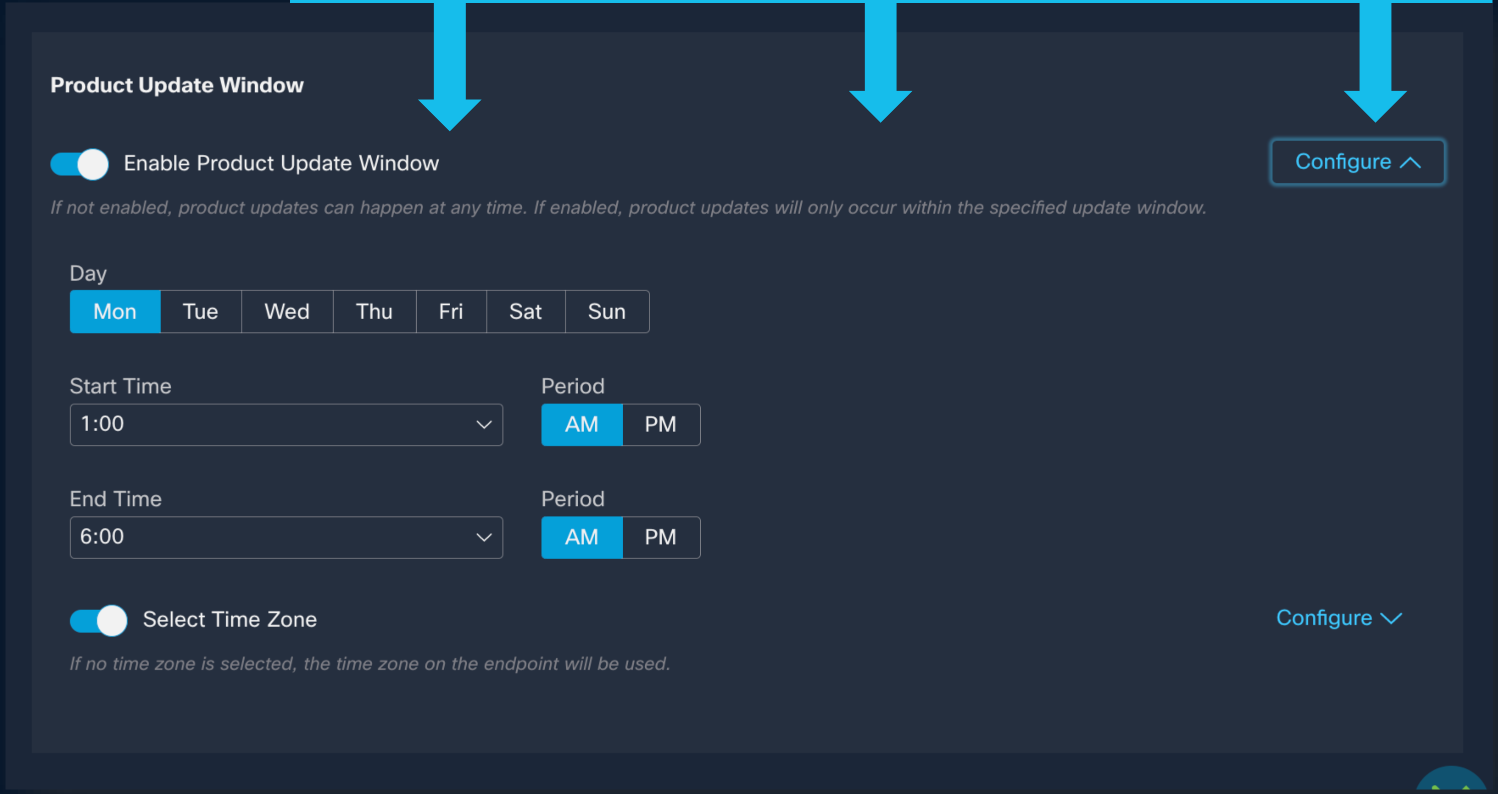
```
C:\Users\x\Downloads>".\csc-deploy-ATW-Deployment.exe"
C0CC/05/A7 A3:A3:C9 Fyne error:  window creation error
C0CC/05/A7 A3:A3:C9   Cause: APIUnavailable: WGL: The driver does not appear to support OpenGL
C0CC/05/A7 A3:A3:C9   At: E:/workspace/workspace/maine3a9eCe0/source/vendor/fyne.io/fyne/vC/internal/driver/glfw/driver.go:AC3
```

Common Issue: Installation updates

“I installed the Network Installer, but nothing is getting installed”

“I changed profile / software version in the deployment & it is not updating”

Check the Product Update Window



Product Update Window

Enable Product Update Window

If not enabled, product updates can happen at any time. If enabled, product updates will only occur within the specified update window.

Day: Mon (selected) | Tue | Wed | Thu | Fri | Sat | Sun

Start Time: 1:00 — Period: AM (selected) | PM

End Time: 6:00 — Period: AM (selected) | PM

Select Time Zone

If no time zone is selected, the time zone on the endpoint will be used.

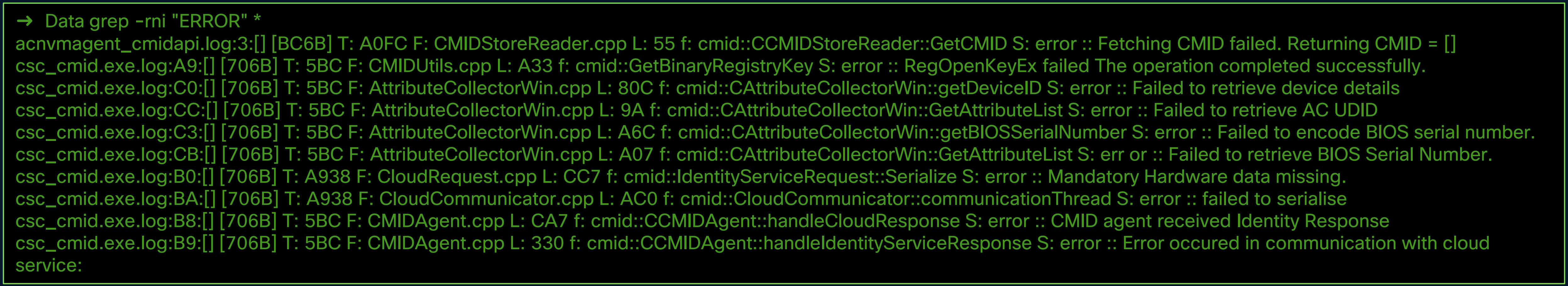
Client Management > Profiles > Cloud Management > [Profile]

Virtual Machine Troubleshooting

- Cloning a VM:
  - CMID is dependent on BIOS serial number and BIOS UUID
  - Need to make sure either one of them are changed when a VM is cloned
  - Usually, VMware generates different BIOS UUID if the user selects “copied” option when cloned VM boots the first time.
  - If not, that can be changed in cloned VM. VMware article about changing BIOS UUID: https://kb.vmware.com/s/article/1002403
- Platform support:
  - Any hypervisors which supports BIOS serial number and BIOS UUID is supported
- VM Secure Client Troubleshooting
  - Same as what would be followed for desktop/laptop

Another Example – Virtual Machines

- *“Help, I’m not getting NVM data to show up…”*
  - Step A: Get me a DART. Didn’t even bother with troubleshooting before DART.
  - Step C: Jumped to the Cloud Management Module Logs:
    - Why? Because CM is REQUIRED for NVM to the Cloud to work.
- What was seen in the logs?



```
➜  Data grep -rni "ERROR" *
acnvmagent_cmidapi.log:3:[] [BC6B] T: A0FC F: CMIDStoreReader.cpp L: 55 f: cmid::CCMIDStoreReader::GetCMID S: error :: Fetching CMID failed. Returning CMID = []
csc_cmid.exe.log:A9:[] [706B] T: 5BC F: CMIDUtils.cpp L: A33 f: cmid::GetBinaryRegistryKey S: error :: RegOpenKeyEx failed The operation completed successfully.
csc_cmid.exe.log:C0:[] [706B] T: 5BC F: AttributeCollectorWin.cpp L: 80C f: cmid::CAttributeCollectorWin::getDeviceID S: error :: Failed to retrieve device details
csc_cmid.exe.log:CC:[] [706B] T: 5BC F: AttributeCollectorWin.cpp L: 9A f: cmid::CAttributeCollectorWin::GetAttributeList S: error :: Failed to retrieve AC UDID
csc_cmid.exe.log:C3:[] [706B] T: 5BC F: AttributeCollectorWin.cpp L: A6C f: cmid::CAttributeCollectorWin::getBIOSSerialNumber S: error :: Failed to encode BIOS serial number.
csc_cmid.exe.log:CB:[] [706B] T: 5BC F: AttributeCollectorWin.cpp L: A07 f: cmid::CAttributeCollectorWin::GetAttributeList S: err or :: Failed to retrieve BIOS Serial Number.
csc_cmid.exe.log:B0:[] [706B] T: A938 F: CloudRequest.cpp L: CC7 f: cmid::IdentityServiceRequest::Serialize S: error :: Mandatory Hardware data missing.
csc_cmid.exe.log:BA:[] [706B] T: A938 F: CloudCommunicator.cpp L: AC0 f: cmid::CloudCommunicator::communicationThread S: error :: failed to serialise
csc_cmid.exe.log:B8:[] [706B] T: 5BC F: CMIDAgent.cpp L: CA7 f: cmid::CCMIDAgent::handleCloudResponse S: error :: CMID agent received Identity Response
csc_cmid.exe.log:B9:[] [706B] T: 5BC F: CMIDAgent.cpp L: 330 f: cmid::CCMIDAgent::handleIdentityServiceResponse S: error :: Error occured in communication with cloud
service:
```

- Result: was using QEMU hypervisor & it didn’t have usable hardware to generate the CMID.

QEMU & KVM Hypervisors

- QEMU & KVM need to add these lines to the VM’s XML to pass BIOS arguments to the Guest-OS.
  - To see whether the BIOS serial number is passed:
    - Windows and type 'wmic bios get serialnumber'
    - Linux 'dmidecode -s system-serial-number’
    - Example only.
      - Replace the values with unique values

```
<sysinfo type='smbios'>
    <bios>
      <entry name='vendor'>LENOVO</entry>
      <entry name='version'>A.C5</entry>
      <entry name='date'>06/CA/CC</entry>
    </bios>
    <system>
      <entry name='manufacturer'>LENOVO</entry>
      <entry name='product'>Virt-Manager</entry>
      <entry name='version'>0.9.B</entry>
      <entry name='serial'>WB6AAAA6A006A</entry>
      <entry name='uuid'>337eC7d5-9AbC-BA08-79cb-07ebc7dbaf9B</entry>
    </system>
  </sysinfo>
<smbios mode='sysinfo'/>
```

Check the NVM Directory

- %programdata%\Cisco\Cisco Secure Client\NVM\
- 2 files need to be there:

```
06/03/2025  03:00 PM                 311 NVM_BootstrapProfile.xml
06/03/2025  03:C5 PM               1,019 NVM_ServiceProfile.xml
```

- Make sure the BootstrapProfile.xml shows the Cloud Collector
- Ensure the ServiceProfile includes the default collection policy
  - *See hidden slides for the contents expected of these files.*
- If either of these files is missing, we start troubleshooting cloud management of Cisco Secure Client (CSC).

NVM_BootstrapProfile.xml

```
<?xml version="A.0" encoding="UTF-8"?>
<NVMBootstrapProfile xsi:noNamespaceSchemaLocation="NVMBootstrapProfile.xsd"
xmlns:xsi="http://www.w3.org/C00A/XMLSchema-instance">
<Cloud>
   <CloudServer>intake.prod.[region].tmc.nvmc.csc.cisco.com</CloudServer>
   <CloudPort>BB3</CloudPort>
</Cloud>
</NVMBootstrapProfile>
```

NVM_ServiceProfile.xml

```
<NVMProfile xsi:noNamespaceSchemaLocation="NVMProfile.xsd" xmlns:xsi="http://www.w3.org/C00A/XMLSchema-instance">
        <ProfileVersion>3</ProfileVersion>
        <CollectorConfiguration>
                <ExportTo>Cloud</ExportTo>
                <PingInterval>5</PingInterval>
        </CollectorConfiguration>
        <TemplateReportInterval>60</TemplateReportInterval>
        <AggInterval>5</AggInterval>
        <ThrottleRate>500</ThrottleRate>
        <CollectionMode>all</CollectionMode>
        <CollectionCriteria>
                <Broadcast>false</Broadcast>
                <Multicast>false</Multicast>
        </CollectionCriteria>
        <DataCollectionPolicy>
                <Policy>
                        <PolicyName>Default DCP for Cloud</PolicyName>
                        <NetworkType>VPN,Trusted,Untrusted</NetworkType>
                        <Type>include</Type>

<Fields>350,AC333,AC33B,AC335,AC336,AC337,AC338,AC339,AC3B0,AC3BA,AC3BC,AC3B3,AC3BB,AC3B5,AC3B6,AC3B7,AC35A,AC35C,AC353,AC3
56,AC357,AC358,AC360,AC36A,AC36C,AC363,AC365,AC366,AC367,AC368,AC369,AC370,AC37A,AC37C,AC373,AC359A,AC359C</Fields>
                </Policy>
        </DataCollectionPolicy>
</NVMProfile>
```

Do we see traffic?

- Traffic is NOT in the older IPFIX (netflow) format.
- It is inside TLS tunnel to the intake endpoint

intake.prod.apjc.tmc.nvmc.csc.cisco.com

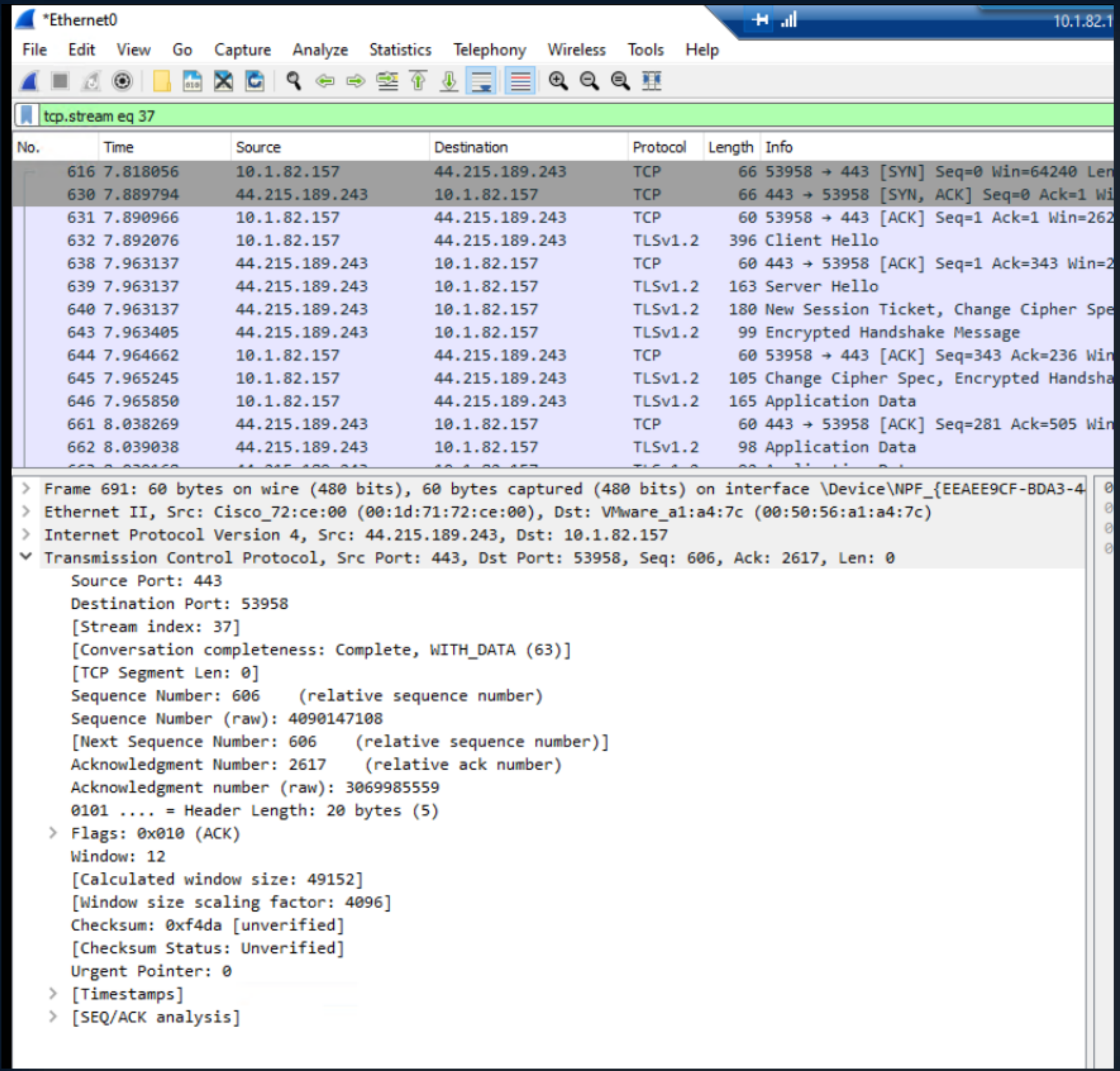
13.238.113.132
3.104.86.153
3.105.255.219

intake.prod.eu.tmc.nvmc.csc.cisco.com

3.68.136.100
3.73.201.90
18.158.108.76

intake.prod.nam.tmc.nvmc.csc.cisco.com

3.228.155.179
34.193.26.136
44.197.148.29



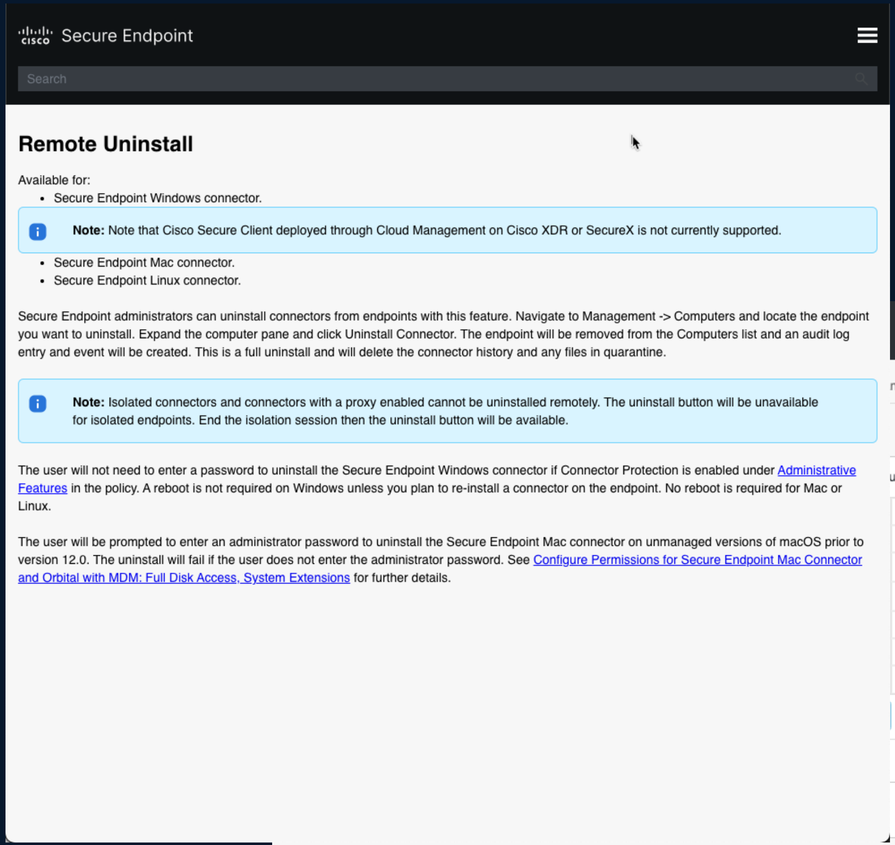
tcp.stream eq 37

```
No.  Time      Source          Destination     Protocol Length Info
 616 7.818056  10.1.82.157     44.215.189.243  TCP       66 53958 → 443 [SYN] Seq=0 Win=64240 Len
 630 7.889794  44.215.189.243  10.1.82.157     TCP       66 443 → 53958 [SYN, ACK] Seq=0 Ack=1 Wi
 631 7.890966  10.1.82.157     44.215.189.243  TCP       60 53958 → 443 [ACK] Seq=1 Ack=1 Win=262
 632 7.892076  10.1.82.157     44.215.189.243  TLSv1.2  396 Client Hello
 638 7.963137  44.215.189.243  10.1.82.157     TCP       60 443 → 53958 [ACK] Seq=1 Ack=343 Win=2
 639 7.963137  44.215.189.243  10.1.82.157     TLSv1.2  163 Server Hello
 640 7.963137  44.215.189.243  10.1.82.157     TLSv1.2  180 New Session Ticket, Change Cipher Spe
 643 7.963405  44.215.189.243  10.1.82.157     TLSv1.2   99 Encrypted Handshake Message
 644 7.964662  10.1.82.157     44.215.189.243  TCP       60 53958 → 443 [ACK] Seq=343 Ack=236 Win
 645 7.965245  10.1.82.157     44.215.189.243  TLSv1.2  105 Change Cipher Spec, Encrypted Handsha
 646 7.965850  10.1.82.157     44.215.189.243  TLSv1.2  165 Application Data
 661 8.038269  44.215.189.243  10.1.82.157     TCP       60 443 → 53958 [ACK] Seq=281 Ack=505 Win
 662 8.039038  44.215.189.243  10.1.82.157     TLSv1.2   98 Application Data
```

```
> Frame 691: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{EEAEE9CF-BDA3-4
> Ethernet II, Src: Cisco_72:ce:00 (00:1d:71:72:ce:00), Dst: VMware_a1:a4:7c (00:50:56:a1:a4:7c)
> Internet Protocol Version 4, Src: 44.215.189.243, Dst: 10.1.82.157
v Transmission Control Protocol, Src Port: 443, Dst Port: 53958, Seq: 606, Ack: 2617, Len: 0
    Source Port: 443
    Destination Port: 53958
    [Stream index: 37]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 606    (relative sequence number)
    Sequence Number (raw): 4090147108
    [Next Sequence Number: 606    (relative sequence number)]
    Acknowledgment Number: 2617    (relative ack number)
    Acknowledgment number (raw): 3069985559
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 12
    [Calculated window size: 49152]
    [Window size scaling factor: 4096]
    Checksum: 0xf4da [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
```

Cisco Secure Endpoint Remote Uninstall

- Cisco Secure Endpoint added Remote Uninstall
- Only supports standalone CSE
- No Remote Uninstall Support with CSC (yet)



Remote Uninstall

Available for:

- Secure Endpoint Windows connector.

Note: Note that Cisco Secure Client deployed through Cloud Management on Cisco XDR or SecureX is not currently supported.

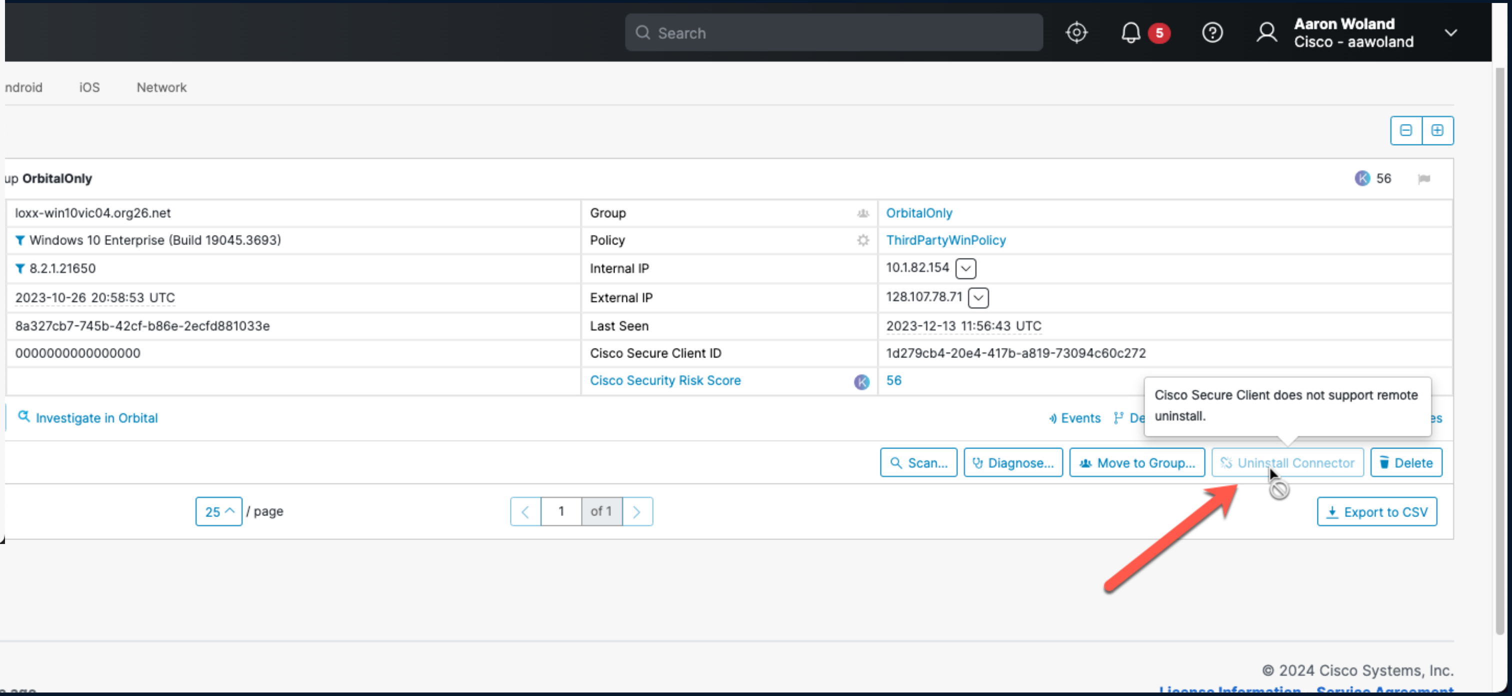
- Secure Endpoint Mac connector.
- Secure Endpoint Linux connector.

Secure Endpoint administrators can uninstall connectors from endpoints with this feature. Navigate to Management -> Computers and locate the endpoint you want to uninstall. Expand the computer pane and click Uninstall Connector. The endpoint will be removed from the Computers list and an audit log entry and event will be created. This is a full uninstall and will delete the connector history and any files in quarantine.

Note: Isolated connectors and connectors with a proxy enabled cannot be uninstalled remotely. The uninstall button will be unavailable for isolated endpoints. End the isolation session then the uninstall button will be available.

The user will not need to enter a password to uninstall the Secure Endpoint Windows connector if Connector Protection is enabled under Administrative Features in the policy. A reboot is not required on Windows unless you plan to re-install a connector on the endpoint. No reboot is required for Mac or Linux.

The user will be prompted to enter an administrator password to uninstall the Secure Endpoint Mac connector on unmanaged versions of macOS prior to version 12.0. The uninstall will fail if the user does not enter the administrator password. See Configure Permissions for Secure Endpoint Mac Connector and Orbital with MDM: Full Disk Access, System Extensions for further details.



loxx-win10vic04.org26.net	Group	OrbitalOnly
Windows 10 Enterprise (Build 19045.3693)	Policy	ThirdPartyWinPolicy
8.2.1.21650	Internal IP	10.1.82.154
2023-10-26 20:58:53 UTC	External IP	128.107.78.71
8a327cb7-745b-42cf-b86e-2ecfd881033e	Last Seen	2023-12-13 11:56:43 UTC
0000000000000000	Cisco Secure Client ID	1d279cb4-20e4-417b-a819-73094c60c272
	Cisco Security Risk Score	56

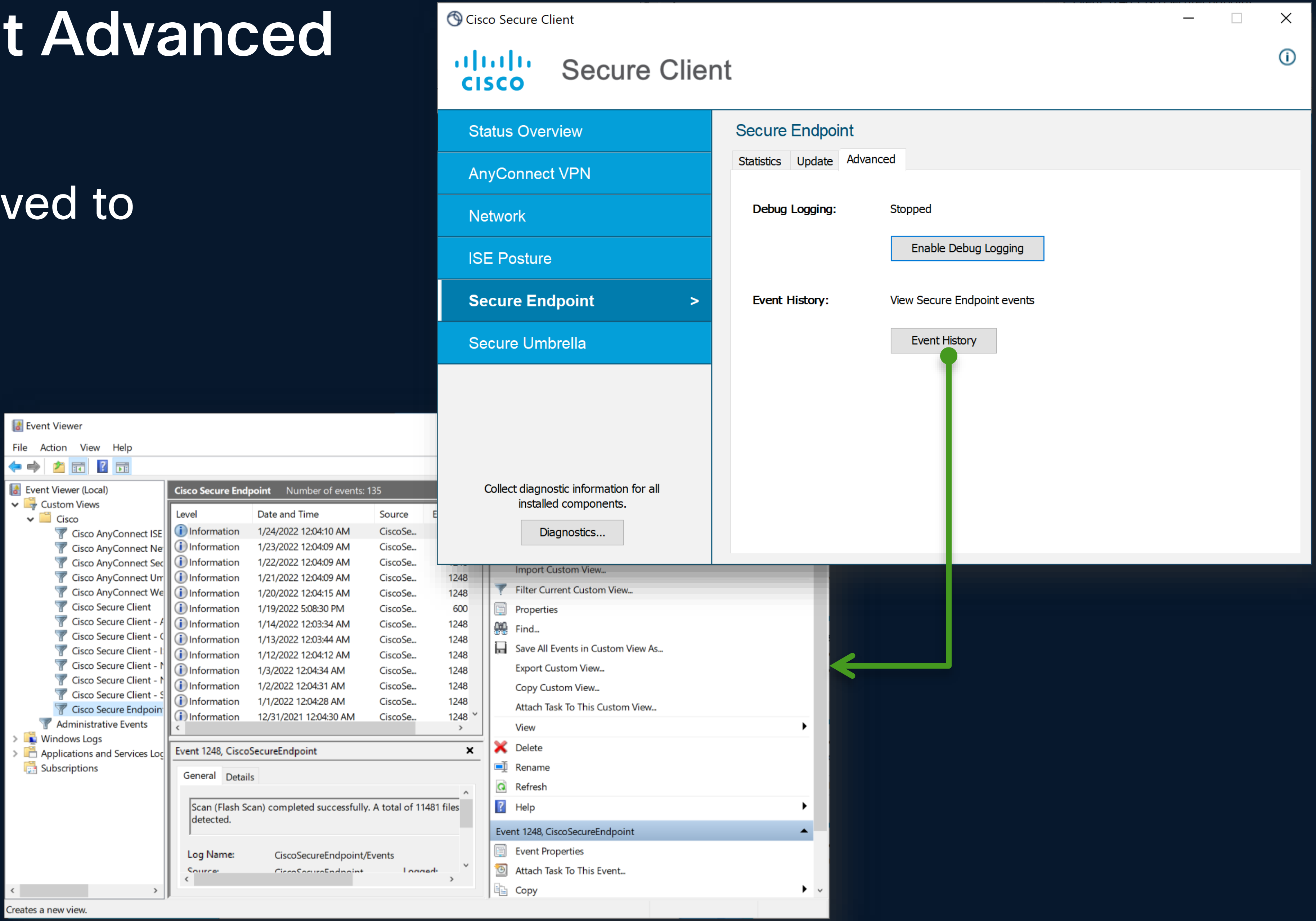
Cisco Secure Client does not support remote uninstall.

Last login 2 days ago from 38.83.164.227

© 2024 Cisco Systems, Inc.

Secure Endpoint Advanced

- Scan History moved to Advanced Tab



Debug Logging: Stopped

Event History: View Secure Endpoint events

Cisco Secure Endpoint Number of events: 135

Level	Date and Time	Source	E
Information	1/24/2022 12:04:10 AM	CiscoSe...	
Information	1/23/2022 12:04:09 AM	CiscoSe...	
Information	1/22/2022 12:04:09 AM	CiscoSe...	
Information	1/21/2022 12:04:09 AM	CiscoSe...	1248
Information	1/20/2022 12:04:15 AM	CiscoSe...	1248
Information	1/19/2022 5:08:30 PM	CiscoSe...	600
Information	1/14/2022 12:03:34 AM	CiscoSe...	1248
Information	1/13/2022 12:03:44 AM	CiscoSe...	1248
Information	1/12/2022 12:04:12 AM	CiscoSe...	1248
Information	1/3/2022 12:04:34 AM	CiscoSe...	1248
Information	1/2/2022 12:04:31 AM	CiscoSe...	1248
Information	1/1/2022 12:04:28 AM	CiscoSe...	1248
Information	12/31/2021 12:04:30 AM	CiscoSe...	1248

Event 1248, CiscoSecureEndpoint

General | Details

Scan (Flash Scan) completed successfully. A total of 11481 files detected.

Log Name: CiscoSecureEndpoint/Events

Helpful Links

- 2025 Cisco Live Webex Space: https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2834
- Endpoint Bar Webex Space (Secure Client/AnyConnect): https://eurl.io/#TmrReXaEj
- AnyConnect EOL: https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/anyconnect-secure-mobility-client-v4x-eol.html
- On-Demand Library: https://www.ciscolive.com/on-demand/on-demand-library.html?zid=pp#/
- Secure Client v5.x Release notes: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/release/notes/release-notes-cisco-secure-client-5-1.html
- Latest Secure Client Downloads : https://software.cisco.com/download/home/286330811/type/282364313/release/5.1.9.113
- Secure Client Order Guide: https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/secure-client-og.html
- DART Details: https://www.cisco.com/c/en/us/support/docs/security/secure-client/221919-collect-dart-bundle-for-secure-client.html
- Request Secure Client Cloud Management Tenant: https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/request-scm-tenant.pdf

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: byazji@cisco.com on in the Endpoint Bar

Thank you