



The bridge to possible

# Cisco Secure Client

## Technical Deep Dive

Bill Yazji – Technical Security Architect

byazji@cisco.com |  @BillYazji |  billyazji

BRKSEC-2834

**CISCO** *Live!*

#CiscoLive

# Abstract

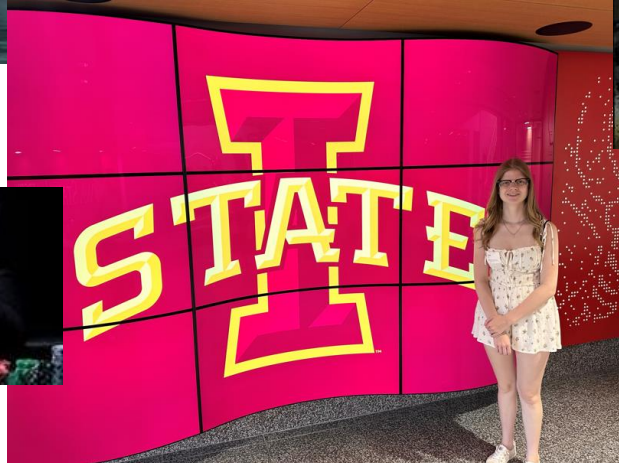
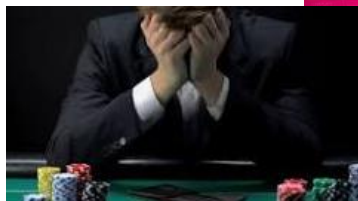
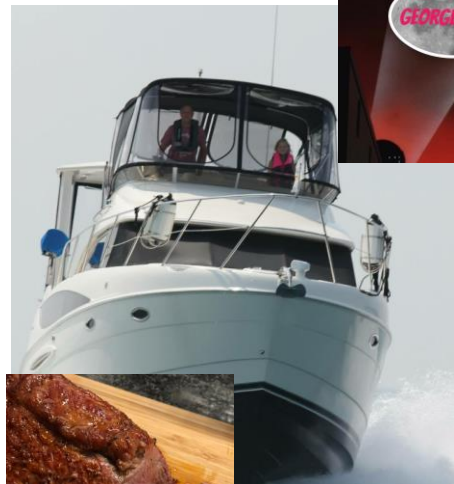
- We have all heard the complaints or did the complaining ourselves: "Cisco has too many agents". Come learn from Bill Yazji, while he shows you that Cisco has listened to the complaints and delivered a unified security agent called Cisco Secure Client.
- Cisco Secure Client (CSC) provides a modular 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 ~~Security~~ Solutions Architect
- Over 14 years with Cisco and nearly 25 years of security, cloud and networking experience
- Global lead for Secure Client Technical Advisory Group
- Prior to Cisco...
  - Cisco competitor in Web Security space
  - Network and Security Consultant on the customer side
  - Large design, deployment, integration and troubleshooting focus



# The “not” work...



cisco *Live!*



# Cisco Webex App

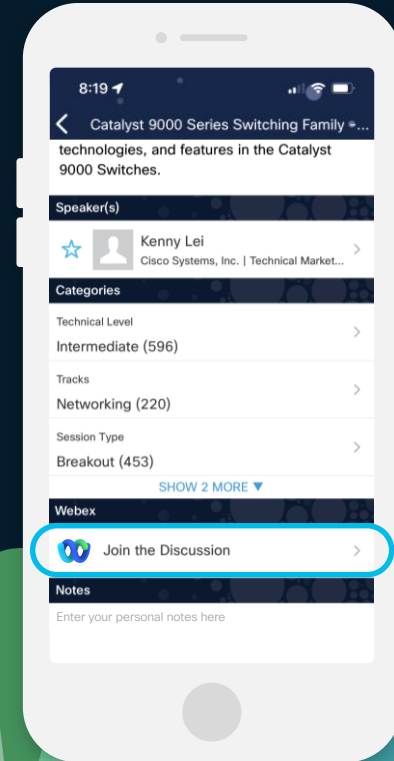
## Questions?

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

## How

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

Webex spaces will be moderated by the speaker until June 7, 2024.



# Surveys are important...



Drop your email in the comments – I WILL respond!

# Important: Hidden Slide Alert



There are hidden slides with additional information, for you to use later!



For Your  
Reference



# Agenda

- CSC Overview
- CSC Architecture
- Deploying / Managing from Cloud
- Upgrading to CSC
- FAQs and Nuggets

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

- No one, ever...



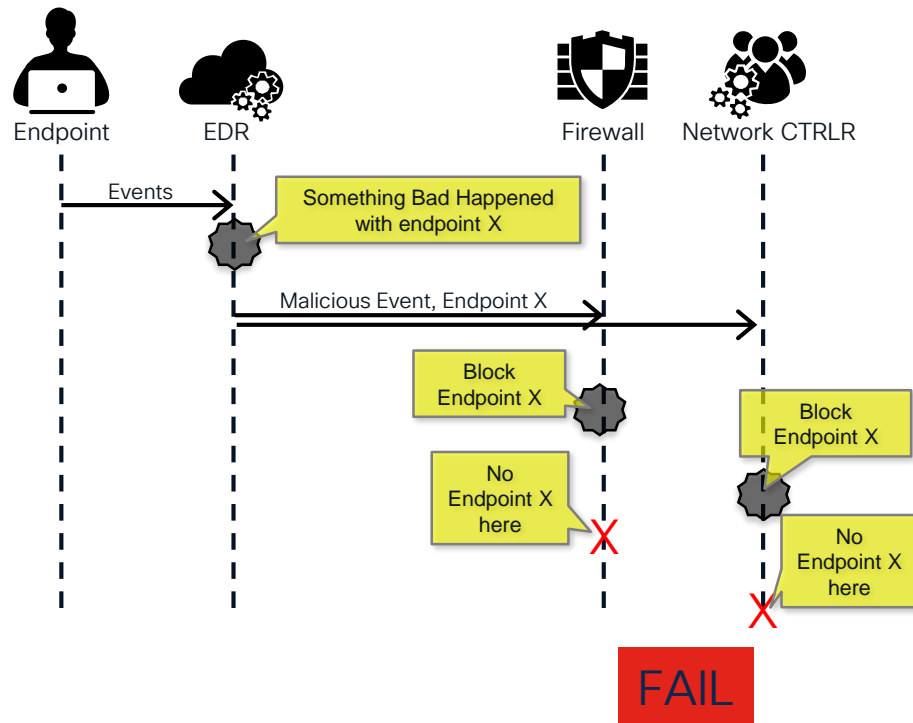
# Why build a unified security agent?

- Our customers have identified **operational challenges** with **deploying multiple endpoint agents** (e.g., AnyConnect, AMP4E, 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	AMP4E / Tetration Agent	AMP4E	AMP4E	-	AMP4E / Tetration Agent
Visibility / Telemetry	AnyConnect NVM / Tetration Agent / 1KEyes	AnyConnect NVM / Tetration Agent / 1KEyes	AnyConnect NVM (Knox)	Cisco Security Connector (CSC)	AnyConnect NVM / Tetration Agent / 1KEyes
Posture	AnyConnect / Duo Health	AnyConnect / 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

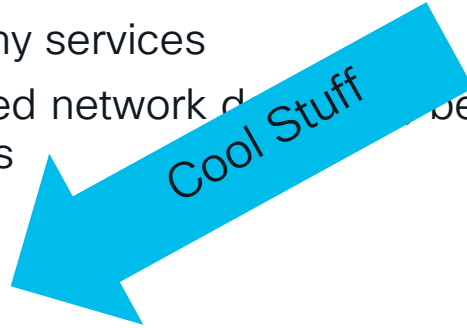


- Initial “unified agent” release was Windows only
- Seamless upgrade from existing AnyConnect & Secure Endpoint [AMP for Endpoint] Clients to Cisco Secure Client
- Leverages Existing AnyConnect (AC) Framework
  - AC UI is starting point for new shared UI
  - AC already had modules for many services
  - Core AC services, such as trusted network detection, become available as common services for all modules
  - Configurable UI
- Cloud management released!
  - Hosted in SecureX and XDR and soon to Secure Client Cloud Management

# Some basics/history



- Initial “unified agent” release was Windows only
- 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
  - Configurable UI
- Cloud management released!
  - Hosted in SecureX and XDR and soon to Secure Client Cloud Management





We used to go around the world stating:



AnyConnect

is  
more  
than



VPN

# End of Life Announcement

## AnyConnect 4.x

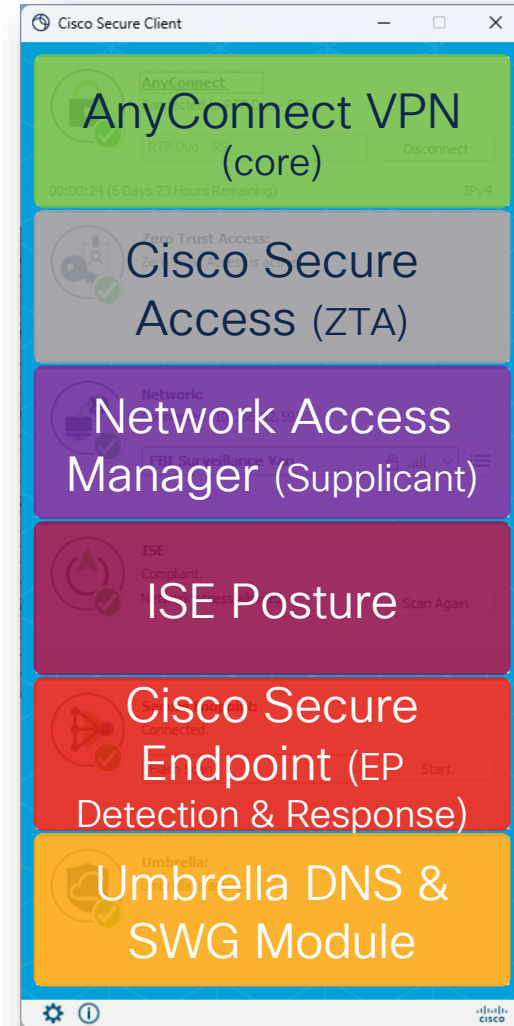
- Software maintenance for 4.x software releases ended **March 31, 2024**. No patches or maintenance releases will be provided for AnyConnect 4.x releases after this date.
- Application software support will not be available beyond **March 31, 2027**.
- Software maintenance and application software support 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>

# 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)

**CISCO** *Live!*

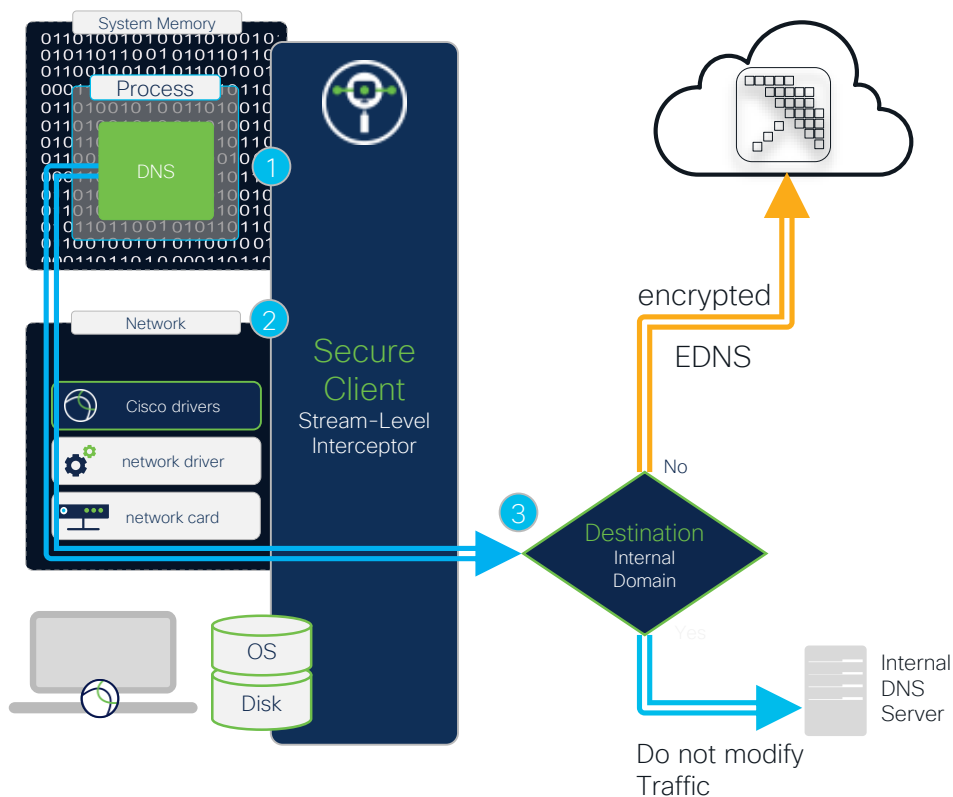


**CISCO** *Live!*



- CISCO** *Live!*

# Stream Level Interceptor



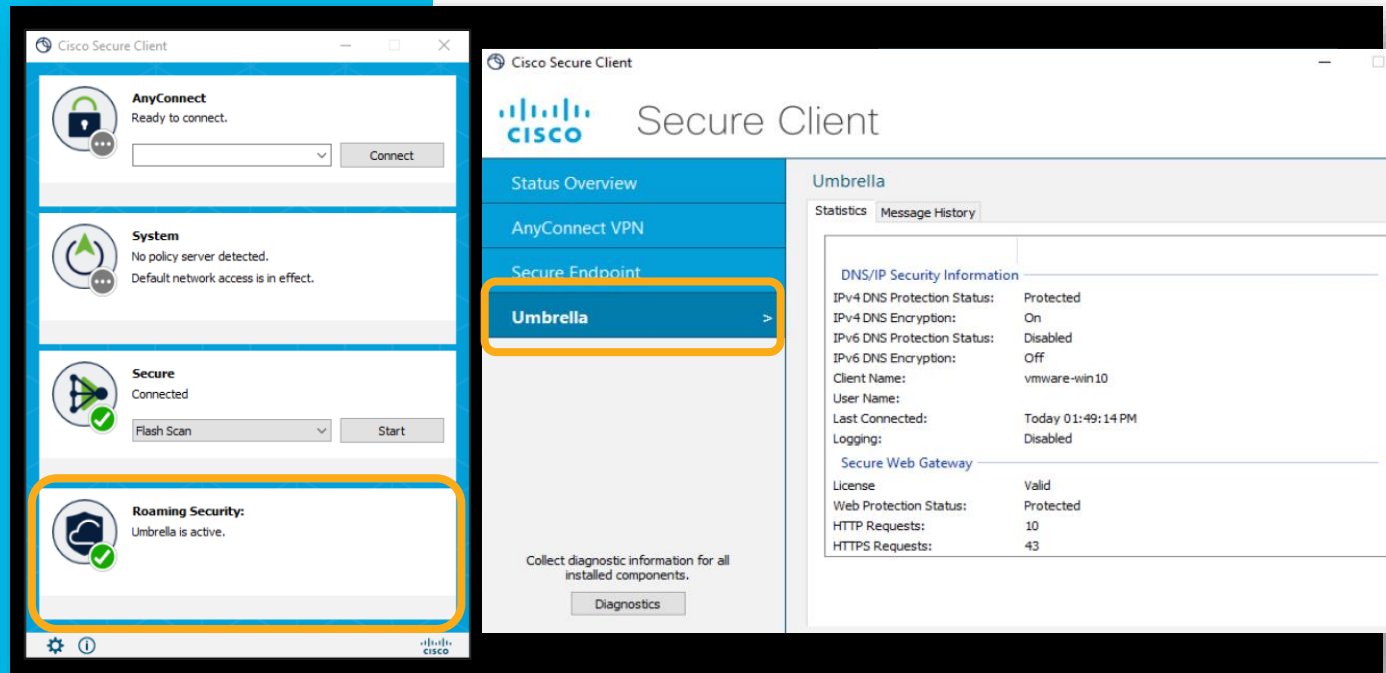
## • Umbrella (DNS) Example:

- 1 DNS Request Sent Down the Stack:
- 2 DNS identified in the stream
  - From Chrome
  - User was Lee (employee)
- 3 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

Same Umbrella  
Roaming from  
AnyConnect:

- Umbrella DNS
- Secure Web Gateway

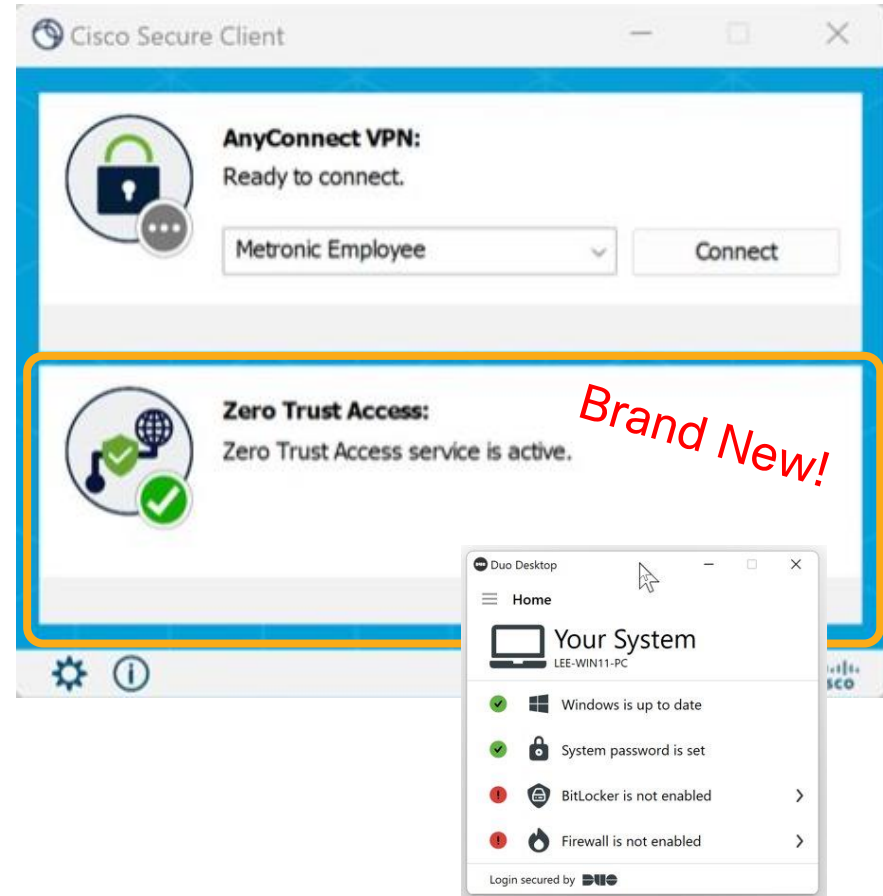




# ZTA Module

## For Cisco “Secure Access”

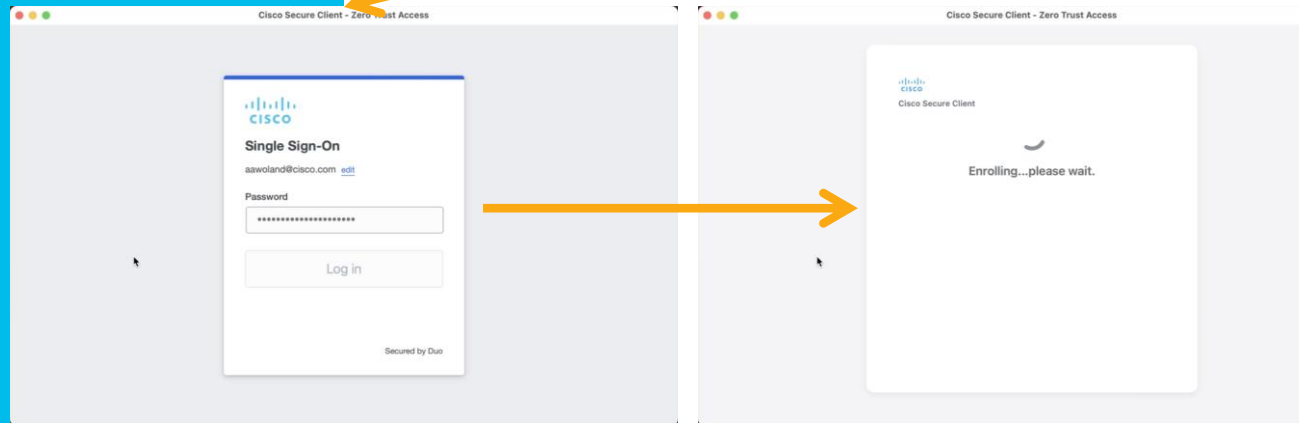
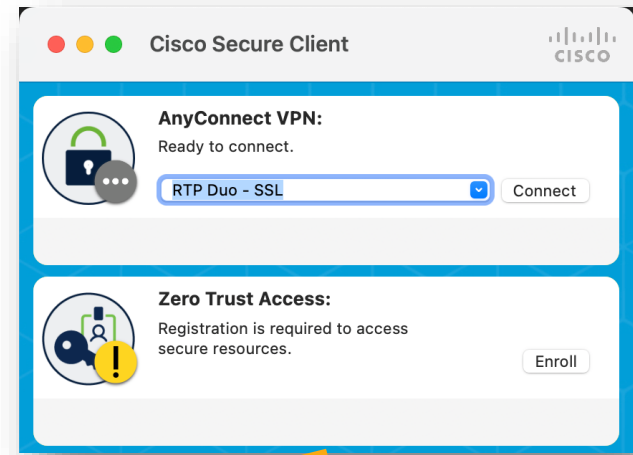
- Brand-New Module dedicated for Cisco Secure Access
- Side-loads the Duo Desktop
  - (formerly Duo Health Agent)
- Uses MASQUE + QUIC for seamless transport



# ZTA Module

## For Cisco “Secure Access”

- Simply login, and it gets all the config
- Currently not in Cloud Management, but coming soon



# 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	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 another plug



Steven Chimes  
Security Architect

---

(ZTNA) Demystified - What It Is, Why You Need It and the New Cisco Technologies That Make Frictionless Security Possible

---

BRKSEC-2079

On-Demand



Neil Patel  
Product Manager

---

The Latest In Secure Access (SSE) Innovation

---

BRKSEC-2285

Monday, June 3



Jonny Noble  
Technical Marketing

---

Cisco Secure Access: Stepping Behind the Curtain

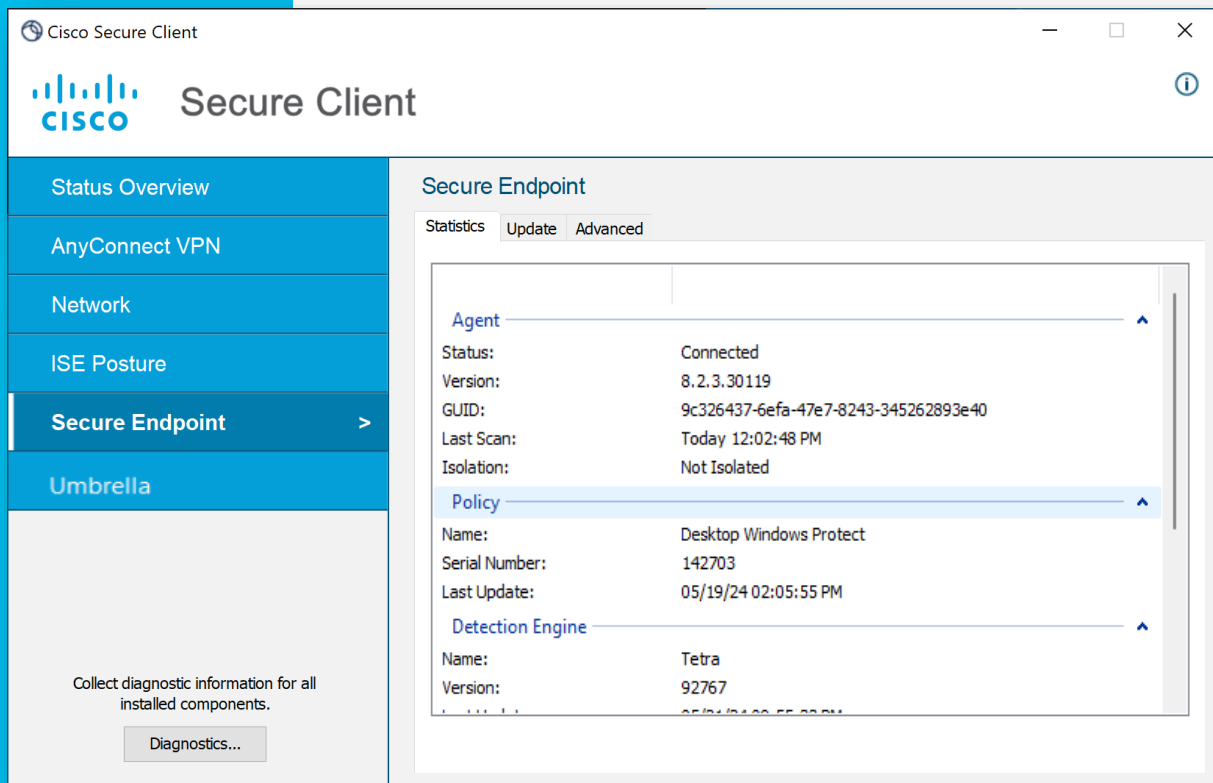
---

BRKSEC-2438

Monday, June 3

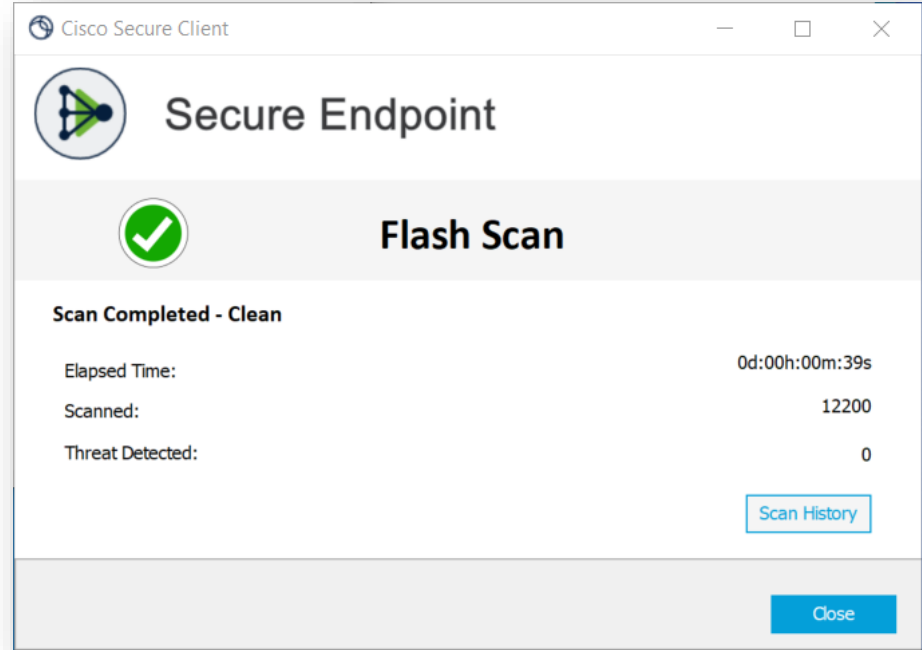
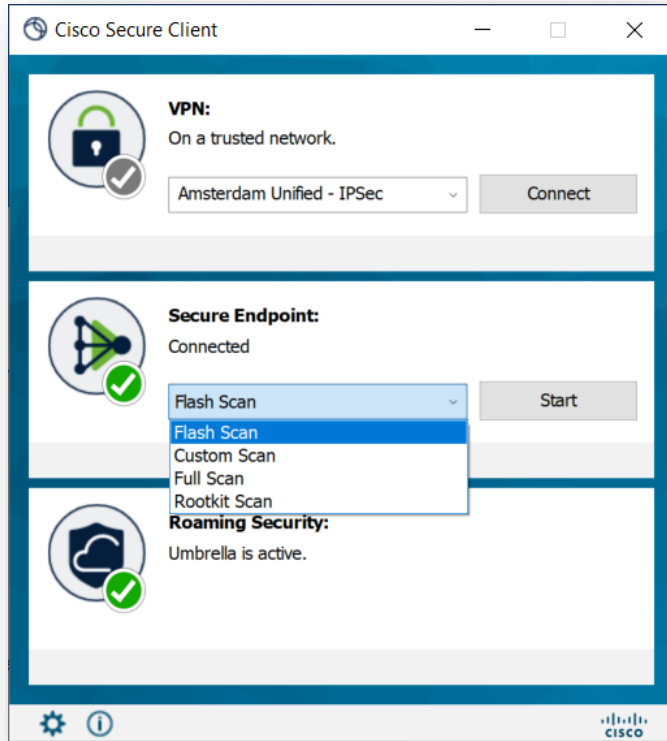
# Secure Endpoint Statistics

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



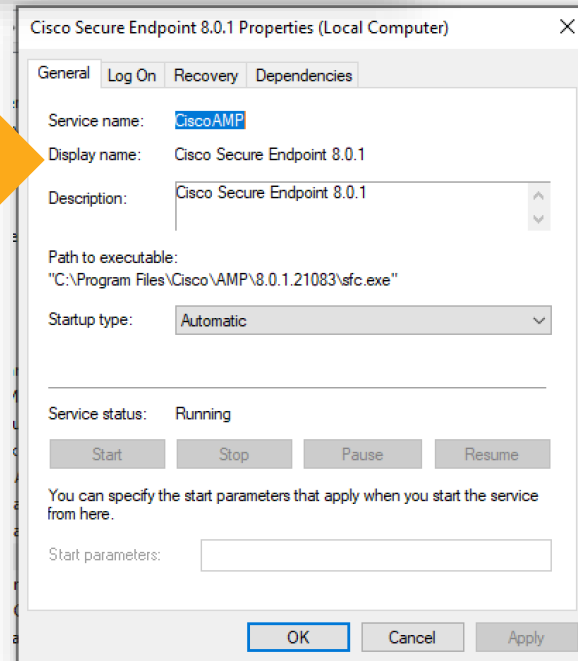
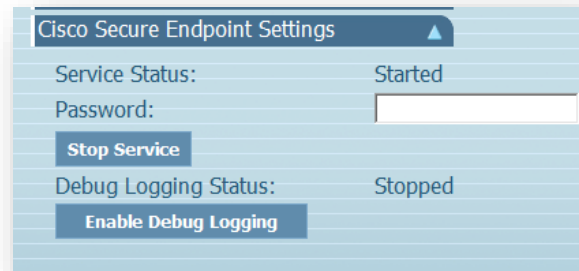


# More Secure Endpoint UI



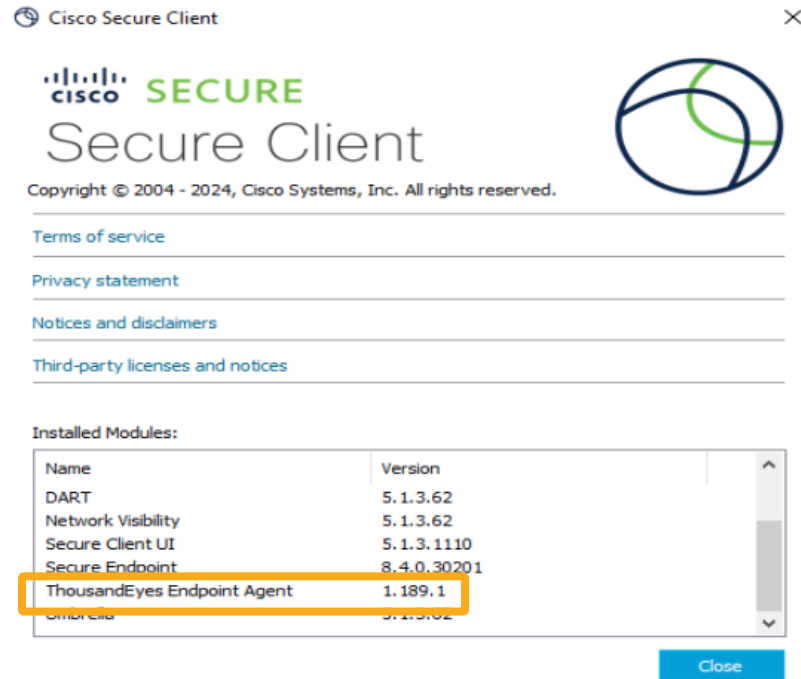
# More Secure Endpoint UI

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



# ThousandEyes

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



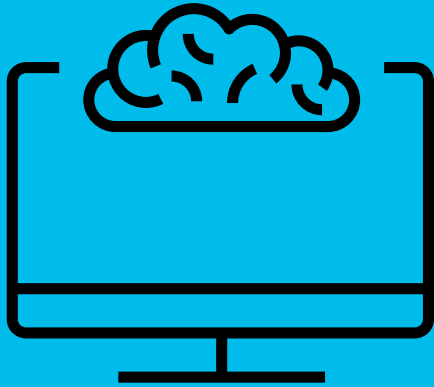
<https://docs.thousandeyes.com/product-documentation/global-vantage-points/endpoint-agents/secure-client-integration>

# 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-Prem – not both (today)
  - Cloud profile defaults to XDR



# TL;DR



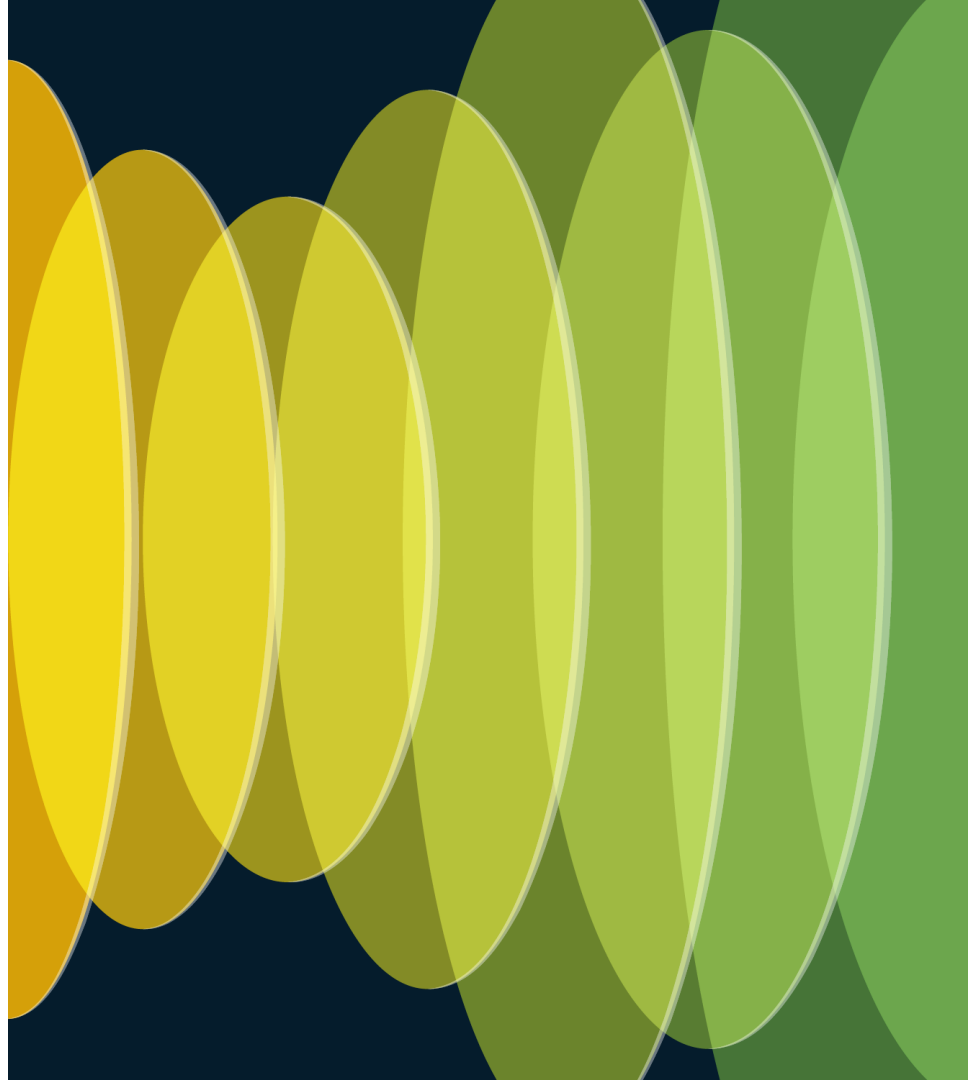
- AnyConnect is now Secure Client
- CSC = Cisco Secure Client
- Yes, you can still do it.
- You can do a whole lot more.
- We've added Cloud Management



# Agenda

- CSC Overview
- CSC Architecture
- Cloud Deployment & Management
- Upgrading to CSC
- FAQs and Nuggets

# The Architecture



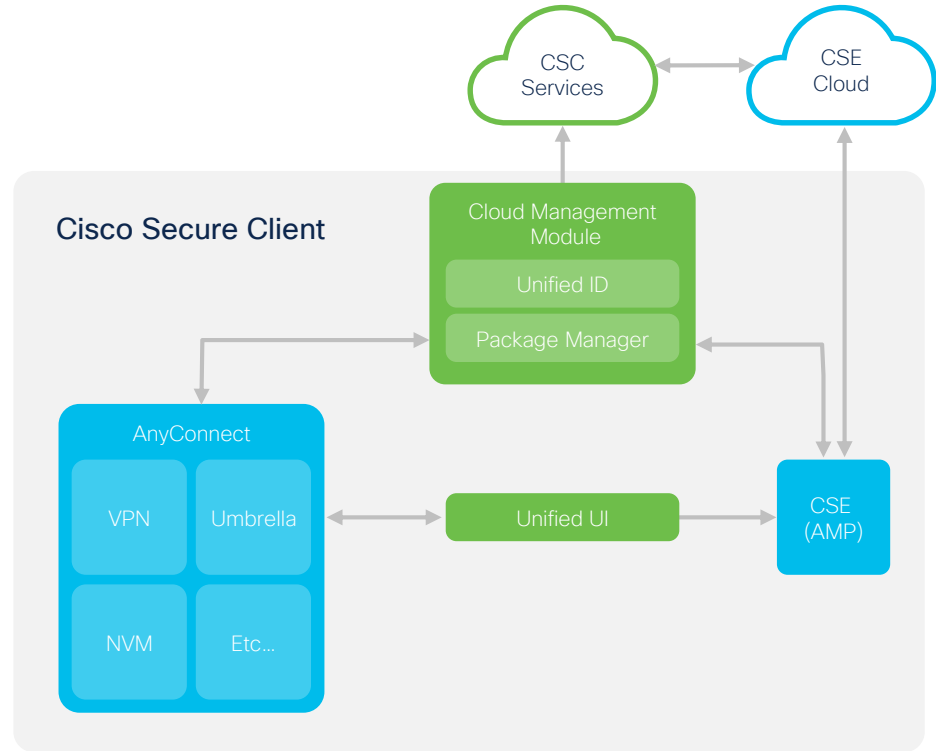
# Cisco Secure Client

## Architectural Overview

► Existing components that are not fundamentally changing

► New components

► Components that form the Cisco Secure Client





# Cisco Secure Client Cloud Management Module

## 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

## Package Manager

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

The screenshot displays the Cisco Secure Client Cloud Management Module interface. The left sidebar contains navigation options: Control Center, Incidents, Investigate, Intelligence, Automate, Assets (highlighted), Client Management, and Administration. The main content area shows details for a device named 'fireball'. At the top, there's a 'Back to Devices' link, a '+ Add Labels' button, a 'Device Value: 10 (Default value)' dropdown, and a 'Refresh from Orbital Live Query' button. The 'Details' section is divided into three columns: Operating System (Windows 11, SP 0.0 (Build 22631.3296)), Managed (No), Last Active (May 28, 2024 @ 9:43 PM CDT), Location, Associated Users, Model, Hardware Id, and Serial Number. The 'Local IPs' section lists 20 IP addresses, each with a status icon (a circle with a checkmark). The 'Public IPs' section shows 184 IP addresses.

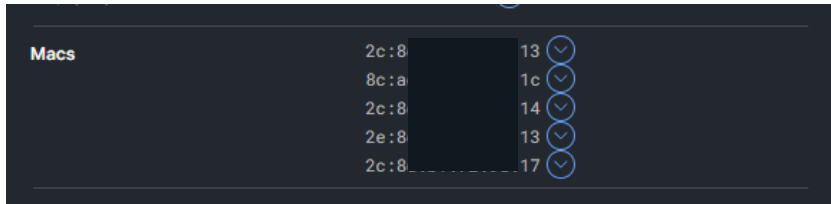
# Cisco Secure Client Cloud Management Module

## 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

## Package Manager

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



# Cisco Secure Client Cloud Management Module

## 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

## Package Manager

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

The screenshot displays the 'Secure Endpoint - Cisco - byazji' interface. At the top, there's a section for 'Macs' with a list of MAC addresses and their corresponding counts: 2c:11:11:11:11:11 (13), 8c:11:11:11:11:11 (1c), and 2c:11:11:11:11:11 (14). Below this, the main section shows the 'Secure Endpoint UID' as 092ff4...0f4. The 'Last Seen' timestamp is May 28, 2024 @ 9:43 PM CDT. The 'Policy' is set to 'YazjiHome'. The 'Group' is 'YazjiGroup'. The 'Install Date' is Oct 18, 2021 @ 5:55 PM CDT. The 'Connector Version' is 8.4.0.30201.

Property	Value
Secure Endpoint UID	092ff4...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

# Cisco Secure Client Cloud Management Module

## 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

## Package Manager

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

The screenshot displays the Cisco Secure Client Cloud Management Module interface. At the top, there's a section for 'Macs' with a list of MAC addresses and their corresponding device IDs. Below this, the 'Secure Endpoint - Cisco - byazji' section shows the 'Secure Endpoint UID' as '092f' followed by a truncated string ending in '40f4'. The 'Orbital' section shows the 'Orbital UID' as '092ff' followed by a truncated string ending in '140f4'. The 'Last Seen' timestamp is 'May 28, 2024 @ 5:16 PM CDT'. The 'Users' section lists 'bill' with a timestamp of '@ 5:55 PM CDT'. The 'Local Users' section lists 'Administrator, bill, DefaultAccount, Guest, WDAGUtilityAccount'. The 'Computer SID' is 'S-1-5-2' followed by a truncated string ending in '387'. The 'Node OS' is 'windows', the 'Version' is 'v1.31.4', the 'Release' is '10.0.22631', and the 'Architecture' is '64-bit'.

Category	Value
Secure Endpoint UID	092f...40f4
Orbital UID	092ff...140f4
Last Seen	May 28, 2024 @ 5:16 PM CDT
Users	bill @ 5:55 PM CDT
Local Users	Administrator, bill, DefaultAccount, Guest, WDAGUtilityAccount
Computer SID	S-1-5-2...387
Node OS	windows
Version	v1.31.4
Release	10.0.22631
Architecture	64-bit

# Cisco Secure Client Cloud Management Module

## 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

## Package Manager

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

The screenshot displays the Cisco Secure Client Cloud Management Module interface. At the top, there's a section for 'Macs' with a list of MAC addresses and their corresponding device IDs. Below this, the 'Secure Endpoint - Cisco - byazji' section shows the 'Secure Endpoint UID' as '092f...40f4'. The 'Orbital' section shows the 'Orbital UID' as '0f...0f4'. The 'Umbrella - byazji@cisco.com' section shows the 'Umbrella UID' as '61...363'. The 'Last Seen' timestamp is 'May 26, 2024 @ 7:51 PM CDT'. The 'Policy' is 'Default Policy'. The 'Client Type' is 'AnyConnect'. The 'Client Version' is '5.1.3.62'. The 'Reported OS' is 'Windows'. The 'Reported OS Version' is '11'.

Section	Value
Macs	2c:f...d:13 8c:f...a:1c 2c:f...d:14
Secure Endpoint - Cisco - byazji	Secure Endpoint UID: 092f...40f4
Orbital	Orbital UID: 0f...0f4
Umbrella - byazji@cisco.com	Umbrella UID: 61...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 Cloud Management Module

## 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

## Package Manager

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

The screenshot displays the Cisco Secure Client Cloud Management Module interface. The top section shows a list of devices under the 'Macs' tab, with columns for MAC address and IP address. Below this, the 'CrowdStrike' section is visible, showing a list of devices with columns for 'CrowdStrike UID', 'Last Seen', 'Connection IP', 'Connection MAC Address', 'Agent Version', 'Major Version', 'Minor Version', 'Platform ID', 'Platform Name', 'Reported OS', and 'Reported OS Version'. The 'Orbital UID' section is also visible, showing a list of devices with columns for 'Orbital UID', 'Last Seen', 'Users', 'Local User', 'Computer', 'Node OS', 'Version', 'Release', and 'Architecture'.

Mac	MAC Address	IP Address
2c	1:13	
8c	1:1c	
2c	1:14	

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

Orbital UID	Last Seen	Users	Local User	Computer	Node OS	Version	Release	Architecture
-------------	-----------	-------	------------	----------	---------	---------	---------	--------------

# Cisco Secure Client Cloud Management Module

## 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

## Package Manager

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

The screenshot displays the Cisco Secure Client Cloud Management Module interface. At the top, there's a section for 'Macs' with a list of MAC addresses and their corresponding device IDs. Below this, the 'CrowdStrike' logo is visible. The main content area is divided into two panels. The left panel shows a sidebar with navigation options: 'Orbital UID', 'Last Seen', 'Users', 'Local Users', 'Computer', 'Node OS', 'Version', 'Release', and 'Architecture'. The right panel displays the 'SentinelOne Endpoint' details, including 'Last Seen' (2024-02-18T06:55:22.177Z), 'Users', 'Domain' (IROH), 'Group' (Default Group), 'Infected' (true), 'Active Threats' (7), and 'User Actions'. A 'View full details' link is at the bottom right.

Category	Value
Orbital UID	1861...
Last Seen	2024-02-18T06:55:22.177Z
Users	...
Local Users	...
Computer	...
Node OS	...
Version	...
Release	...
Architecture	...

# Cisco Secure Client Cloud Management Module

## 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

## Package Manager

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



Secure Client			Device Events
Secure Client UID	5ca72	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	606338	
AC UDID	f78fdc	3b646e	
Serial Number	r912zza1		



# Cisco Secure Client

## Cloud Management Module

### Package Manager

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

The screenshot shows the 'Cloud Management Profiles' configuration page in the Cisco Secure Client. The page has a dark theme and includes a top navigation bar with a back arrow and the title 'Profiles'. Below the title, the main heading is 'Cloud Management Profiles'. A row of action buttons is located at the top right: 'New Profile', 'Edit Name', 'Delete', 'Reset Changes', 'Cancel', 'Make A Copy', 'Save', and 'Download'. The configuration is organized into four sections, each with a title and a set of controls:

- Identity Service Settings:** Contains a toggle switch for 'Enable Debug Logging', which is currently turned off.
- Package Manager Service Settings:** Contains two text input fields: 'Logging Level\*' with the value 'Error', and 'Check-in Interval\*' with the value '2 Hours'. Below these is a toggle switch for 'Notify User When Reboot Is Required', which is currently turned on.
- Cloud Management Service Settings:** Contains a text input field for 'Logging Level\*' with the value 'Error'.
- Product Update Window:** Contains a toggle switch for 'Enable Product Update Window', which is currently turned off. Below the toggle is a note: 'If not enabled, product updates can happen at any time. If enabled, product updates will only occur within the specified update window.'

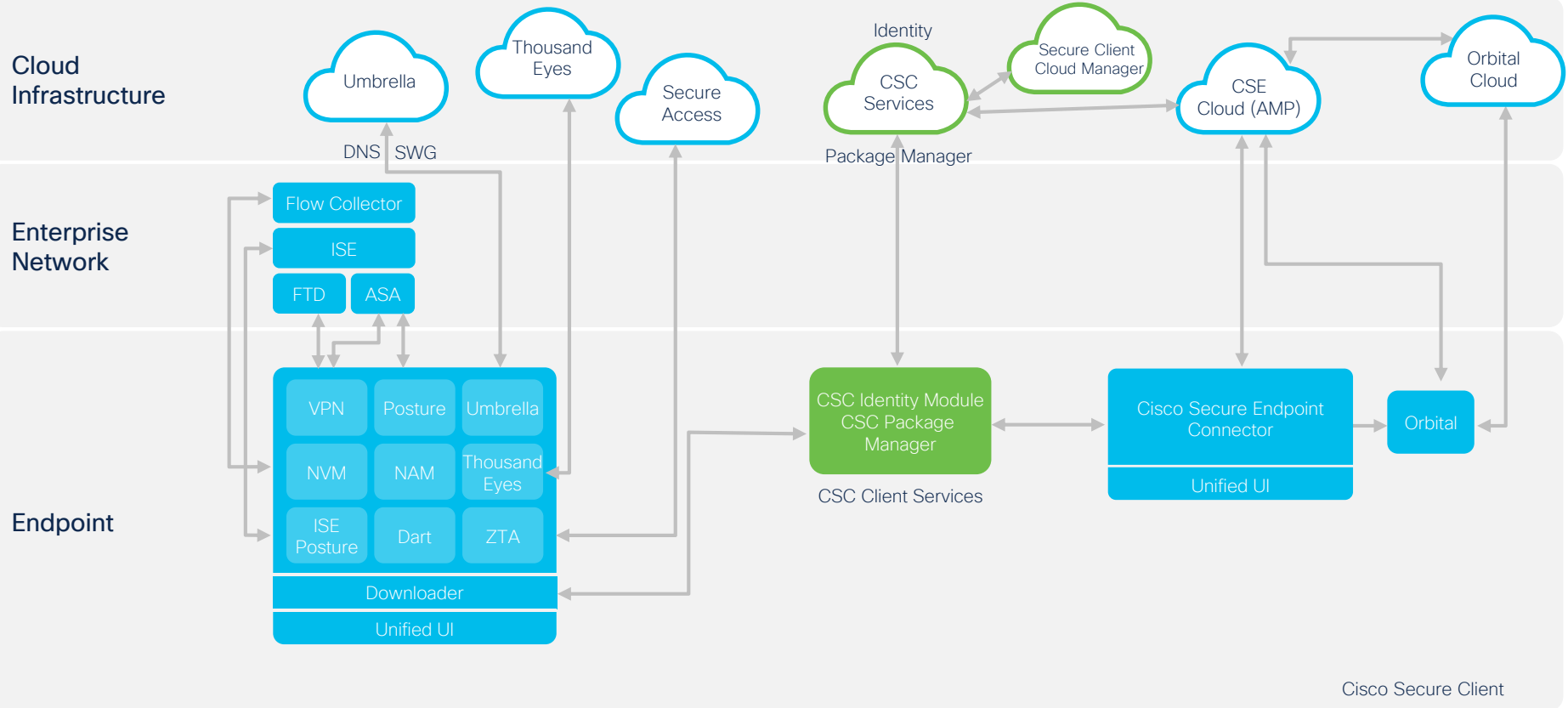
# Cisco Secure Client Cloud Management Module

## 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
  - CM has no idea what this window is, it's all controlled at the cloud

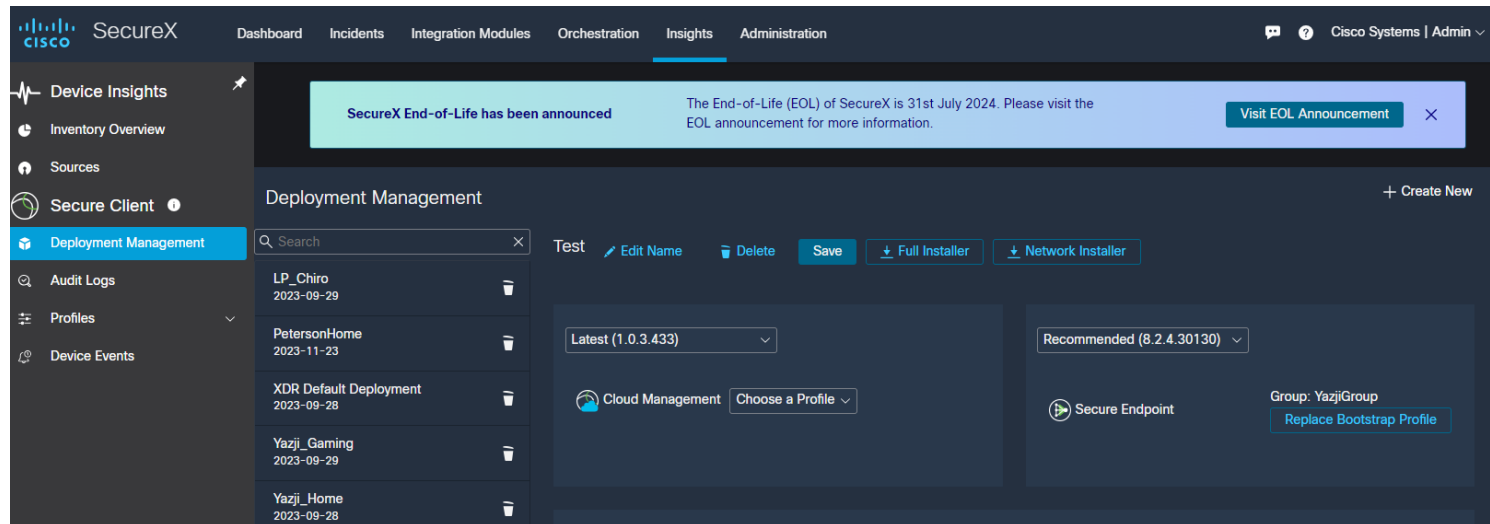
The screenshot displays the 'Cloud Management Profiles' configuration interface. At the top, there are navigation buttons: 'New Profile', 'Edit Name', 'Delete', 'Reset Changes', 'Cancel', 'Make A Copy', 'Save', and 'Download'. Below this is the 'Identity Service Settings' section with a toggle for 'Enable Debug Logging'. The main section is 'Product Update Window', which includes a toggle for 'Enable Product Update Window'. A descriptive text states: 'If not enabled, product updates can happen at any time. If enabled, product updates will only occur within the specified update window.' There is a 'Configure' link with an upward arrow. The configuration options include a 'Day' selector (Mon, Tue, Wed, Thu, Fri, Sat, Sun), 'Start Time' and 'End Time' dropdowns (both set to 1:00), and 'AM'/'PM' period selectors. A 'Select Time Zone' toggle is also present, with a note: 'If no time zone is selected, the time zone on the endpoint will be used.' The bottom of the image shows a partial view of the same configuration page.

# Cisco Secure Client – Architecture



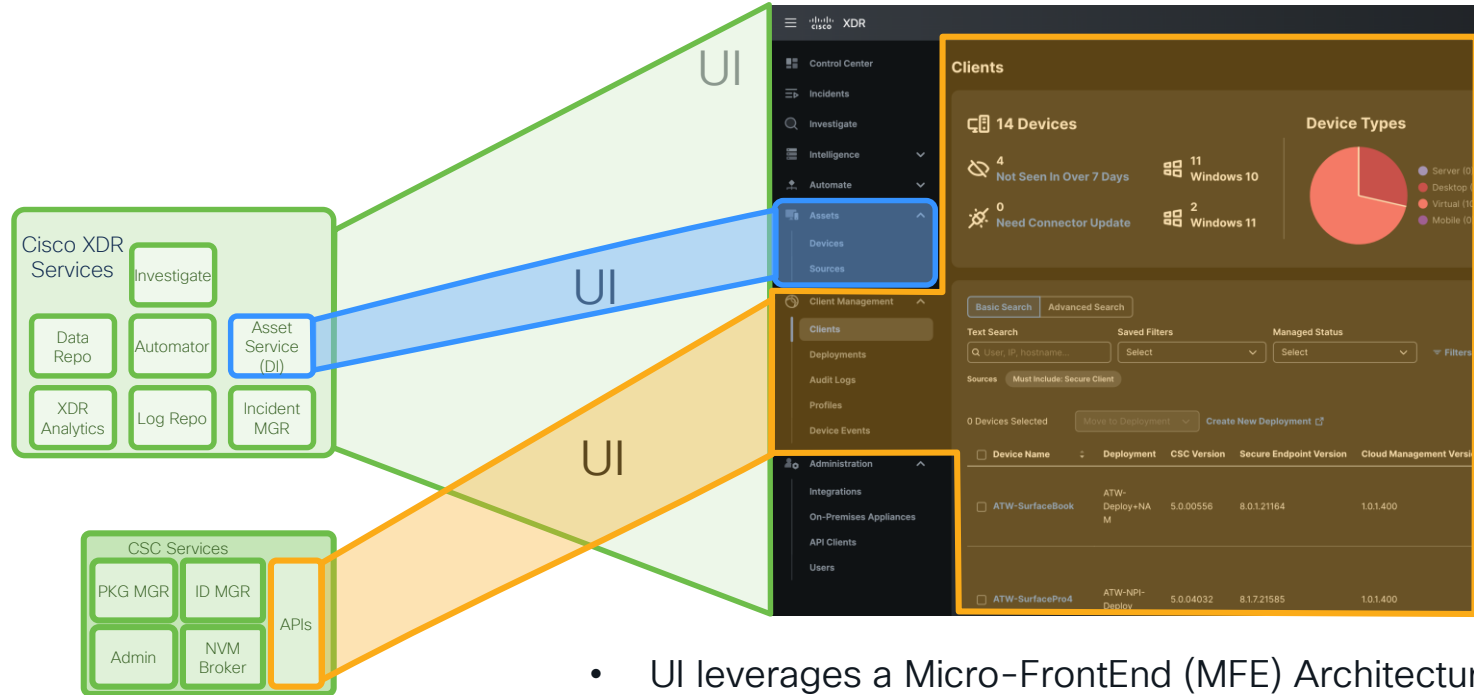
Cisco Secure Client

# SecureX Who?



- <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>

# Wait, it's in XDR too?



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

# Today – in SecureX

The screenshot displays the Cisco SecureX dashboard. At the top, a navigation bar includes links for Dashboard, Incidents, Integration Modules, Orchestration, Insights, and Administration. A user profile for 'Cisco Systems | Admin' is visible on the right. A prominent banner at the top center states: '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.' with a 'Visit EOL Announcement' button.

The left sidebar contains a menu with the following items: Device Insights, Inventory Overview, Sources, Secure Client, Deployment Management (highlighted), Audit Logs, Profiles, Cloud Management, Customer Experience Feedback, ISE Posture, Local Policy, Network Access Manager, Network Visibility Module, Umbrella, VPN, VPN Management Tunnel, and Device Events.

The main content area is titled 'Deployment Management' and features a '+ Create New' button. It displays a list of deployment profiles:

- 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) - This profile is selected and highlighted.

Below the list, the configuration for the 'Yazji\_Home' profile is shown. It includes a search bar, a version dropdown set to 'Latest (1.0.3.433)', and buttons for 'Edit Name', 'Delete', 'Save', 'Full Installer', and 'Network Installer'. The configuration is divided into three sections:

- Cloud Management:** Includes a dropdown for 'Cloud Management Default Profile'.
- Secure Endpoint:** Includes a 'Group' dropdown set to 'Replace Bootstrap Profile'.
- AnyConnect VPN:** Includes a 'Create Profile' button, a 'Start Before Logon' toggle, and an 'Umbrella' dropdown set to 'Umbrella - byazji'.

At the bottom, there are additional configuration options:

- Diagnostics and Reporting Tool:** Includes a 'Create Profile' button.
- ISE Posture:** Includes a 'Create Profile' button.
- Secure Firewall Posture:** Includes a 'Create Profile' button.
- Network Access Manager:** Includes a 'Create Profile' button.

# Today – In XDR

**Deployments** [+ Create New](#)

Search By Deployment Name All Users Search By Associated Profiles

Deployment Name	OS / Architecture	Associated Profiles	Created	Last Modified
<a href="#">XDR Default Deployment</a>	Windows / amd64	2	September 28, 2023 at 12:06:43 PM system	March 13, 2024 at 02:06:02 PM system
<a href="#">LP_Chiro</a>	Windows / amd64	3	September 28, 2023 at 10:15:20 PM byazji@cisico.com	March 13, 2024 at 02:06:02 PM byazji@cisico.com
<a href="#">PetersonHome</a>	Windows / amd64	3	November 23, 2023 at 02:25:57 PM byazji@cisico.com	March 13, 2024 at 02:06:02 PM byazji@cisico.com
<a href="#">Yazji_Gaming</a>	Windows / amd64	3	March 13, 2024 at 10:17:19 PM byazji@cisico.com	May 16, 2024 at 10:14:50 AM byazji@cisico.com
<a href="#">Yazji_Home</a>	Windows / amd64	3	March 13, 2024 at 12:57:40 PM byazji@cisico.com	May 16, 2024 at 10:16:57 AM byazji@cisico.com

**Profiles used on this deployment**

- Cloud Management Default Profile
- Cloud Management
- NVM Cloud Default Profile
- Network Visibility Module - XDR
- Umbrella - byazji**
- Umbrella

15 per page 1-5 of 5 1 / 1

# Today – In XDR

The screenshot displays the Cisco XDR web interface. The top navigation bar includes the Cisco logo, 'XDR', and user information for 'Bill Yazji, Cisco Systems'. The left sidebar contains a menu with options: Control Center, Incidents, Investigate, Intelligence, Automate, Assets, Client Management (highlighted), and Administration. The main content area is titled 'Profiles' and features a table of existing profiles. A modal window titled 'Create New Profile' is open, showing a list of profile types with 'Cloud Management' selected. The table below lists several profiles, including 'Cloud Management Default Profile', 'NVM Cloud Default Profile', 'New Profile', 'NVM\_CLUS', and 'Umbrella - byazji'. The bottom of the interface shows pagination controls indicating 15 items per page, 1-5 of 5, and page 1 of 1.

Profile Name	Profile Type	Created	Last Modified
Cloud Management Default Profile	Cloud Management	September 28, 2023 at 12:06:43 PM	September 28, 2023 at 12:06:43 PM system
NVM Cloud Default Profile	NVM Cloud	September 28, 2023 at 12:06:43 PM	September 28, 2023 at 12:06:43 PM system
New Profile	Customer Experience Feedback	May 22, 2024 at 06:26:25 PM	May 22, 2024 at 06:26:25 PM byazji@cisico.com
NVM_CLUS	ISE Posture	May 22, 2024 at 06:27:55 PM	May 22, 2024 at 06:28:13 PM byazji@cisico.com
Umbrella - byazji	Local Policy	September 28, 2023 at 12:55:15 PM	September 28, 2023 at 12:55:15 PM byazji@cisico.com

**Create New Profile**

- ☒ Cloud Management
- ☐ Customer Experience Feedback
- ☐ ISE Posture
- ☐ Local Policy
- ☐ Network Visibility Module
- ☐ VPN
- ☐ VPN Management Tunnel

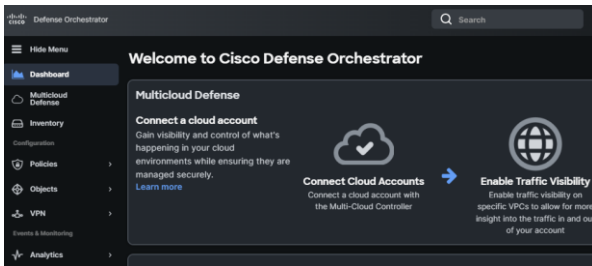
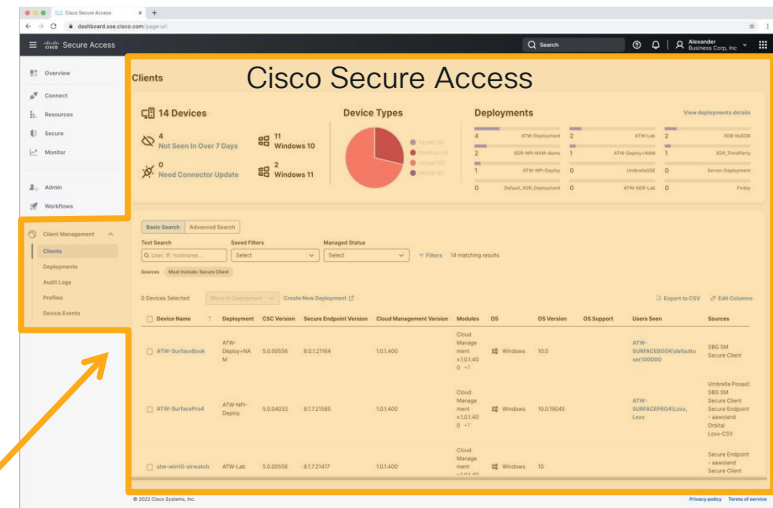
Cancel Create



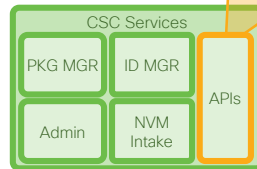
- For NON-XDR users
  - Exists \*today\* in SecureX
  - Secure Access Customers are redirected to SecureX / XDR for CSC Management today.
  - Micro-FrontEnd (MFE) UI Architecture will enable the CSC management to be pulled into other front-ends in future.



# Micro Front End *Potential*



Same UI from CSC Service



Common Services



cisco *Live!*

# I want this... how do I get it?

(..and I don't have XDR)

- Yes, you need SecureX today.
- Yes, SecureX is EOL.
- Yes, after EOL you'll still have Cloud Management access.
- Yes, it will have a new name.
- Yes, it will ultimately move to Cisco Security Cloud, and you'll have an entitlement.



Open a TAC Case



Product: Cisco Secure Client



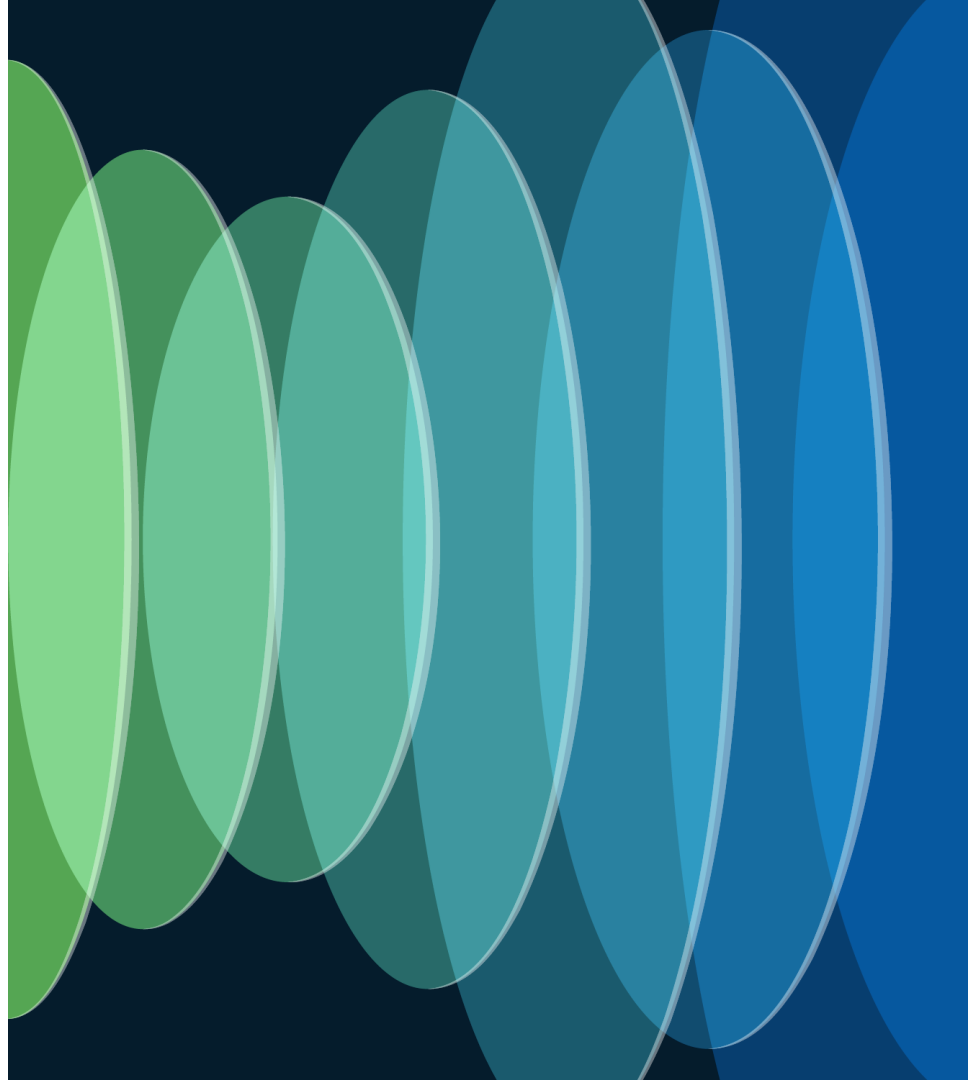
Request a SecureX tenant be provisioned for Cloud Management of CSC



# Agenda

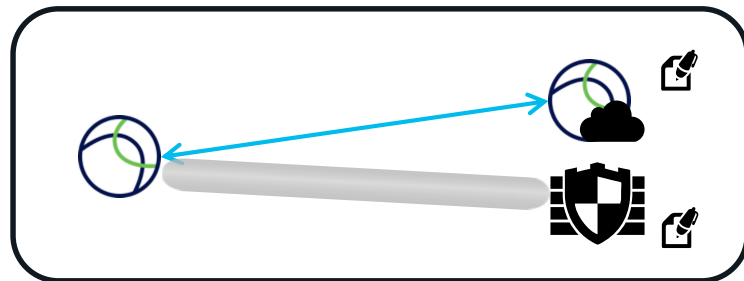
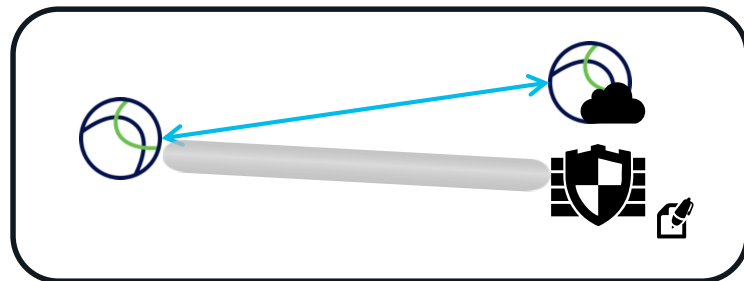
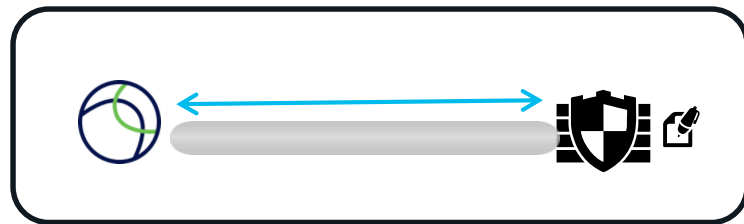
- CSC Overview
- CSC Architecture
- Cloud Deployment & Management
- Upgrading to CSC
- FAQs and Nuggets

# Deploying / Managing from Cloud



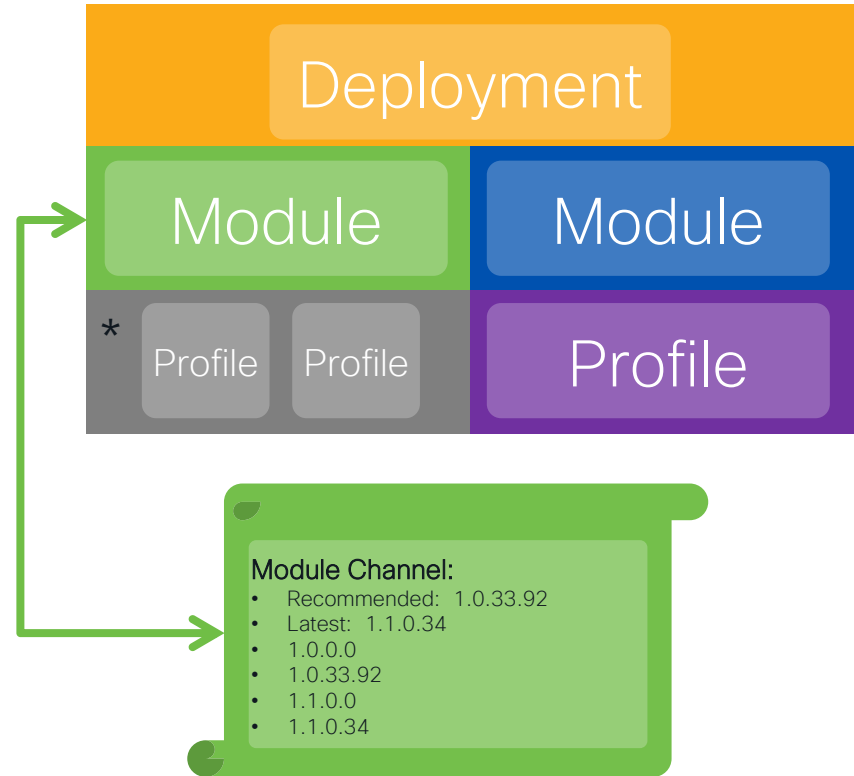
# Deployment Models

- No Cloud Management
- Cloud Registration – no Package Management
- Cloud Registration – Full Management



# Glossary

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

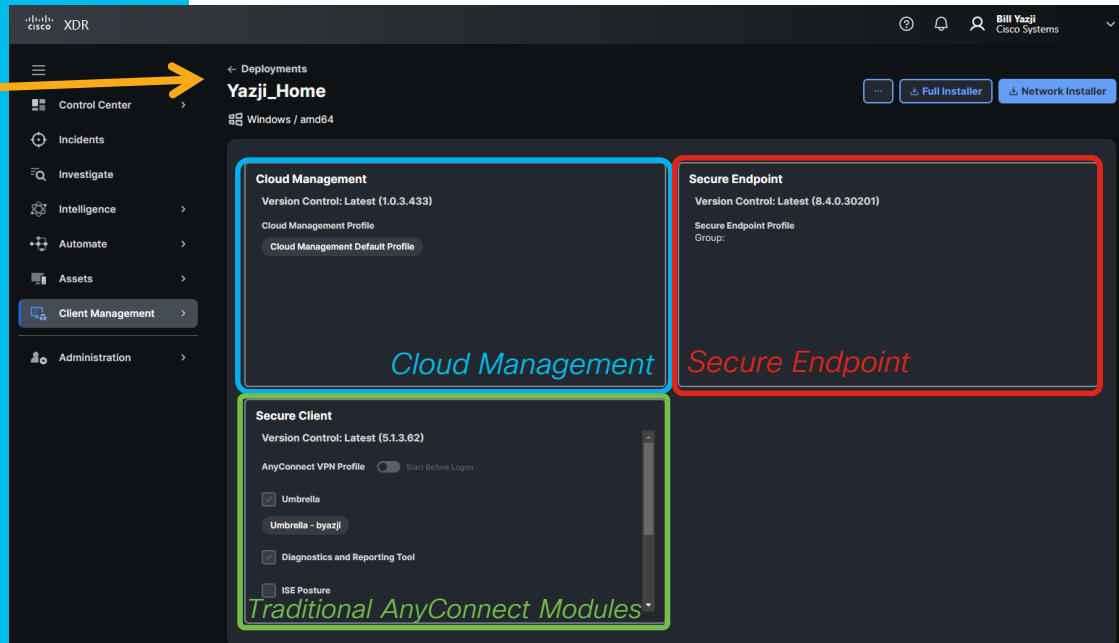


\* When module supports >1

# Managed from XDR or SecureX UI

## Deployments

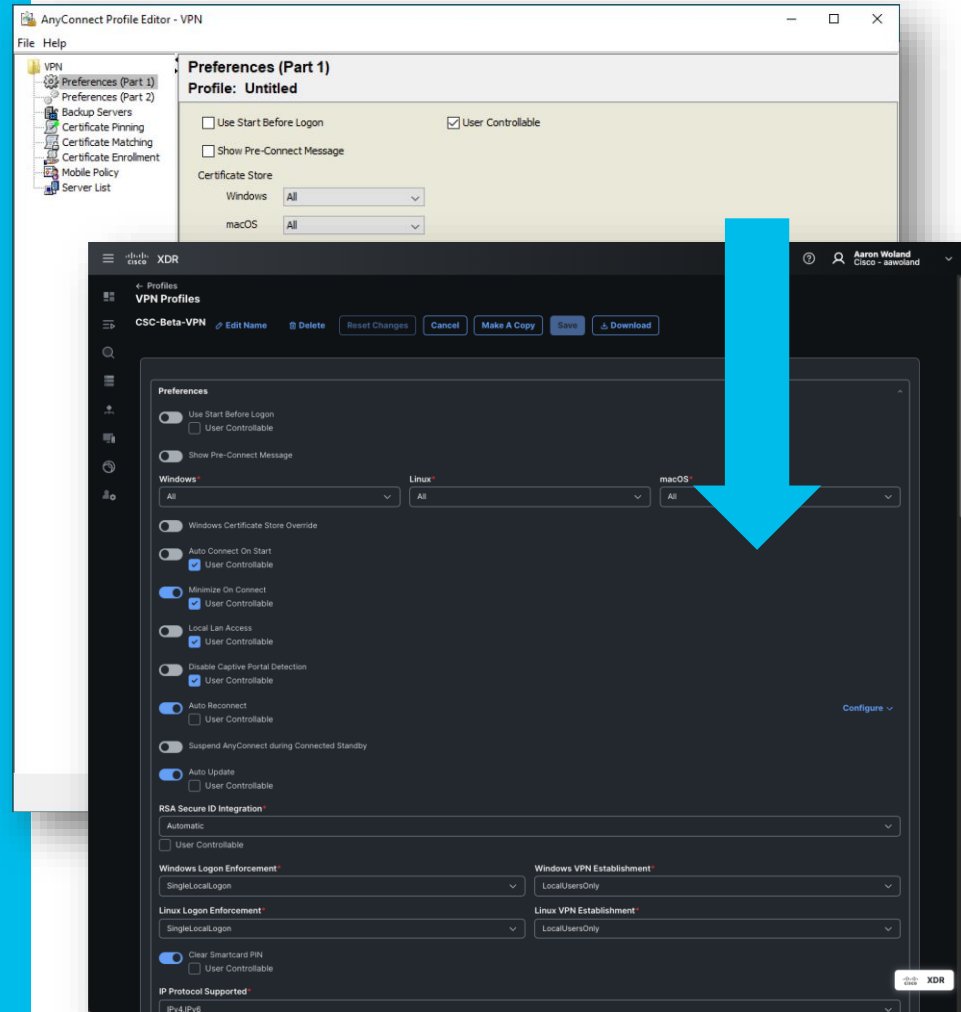
- The glue of all the profiles
- “Groups” are coming in future version & can assign entire groups to a Deployment
- Builds the installer dynamically





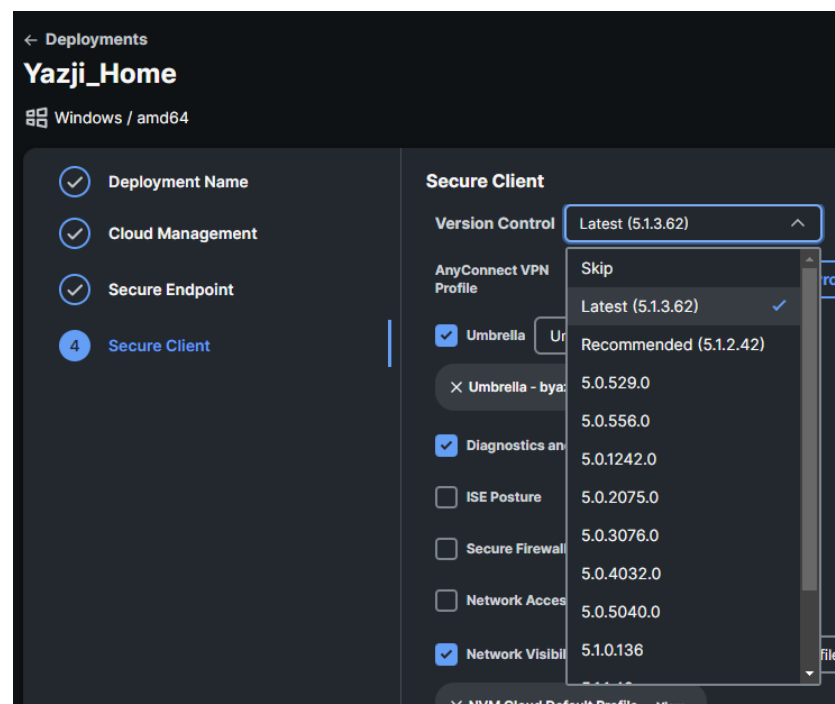
# Managed from XDR / SecureX UI

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



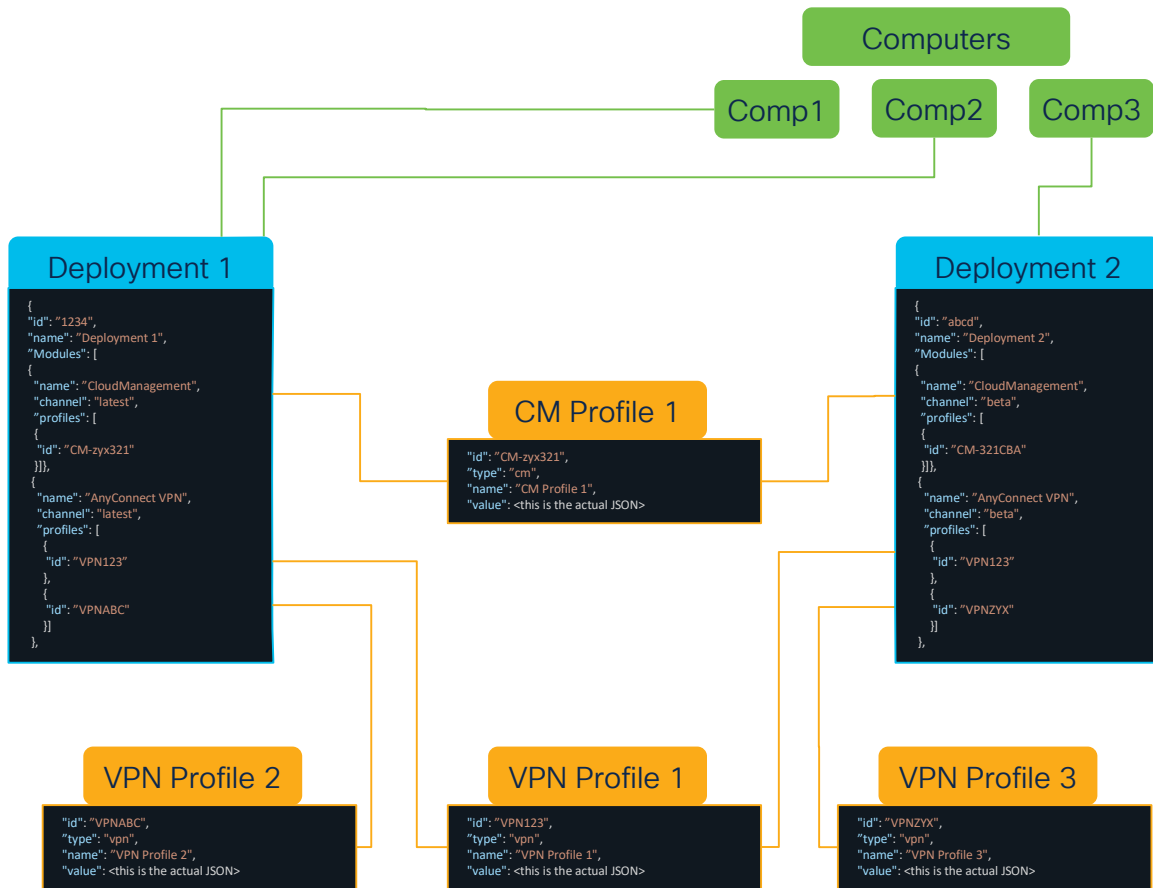
# Version Catalogs

- For Each Deployment:
  - Specify which channel you want the software to update from:
    - Hard-Code the specific version (version lock)
    - Skip (never upgrade version)
    - Recommended Auto Upgraded whenever Cisco publishes a new version to channel
    - Latest publishes a new version to channel
  - Allows you to have an “early testers” set of endpoints, etc..



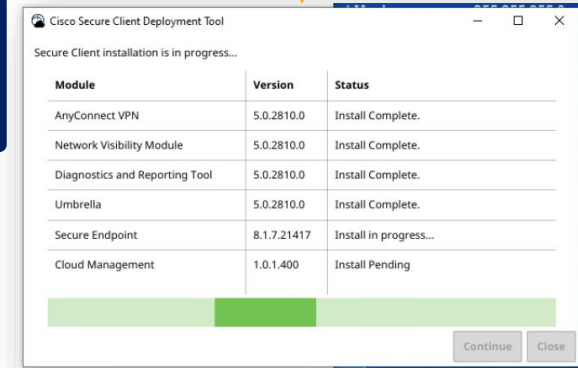
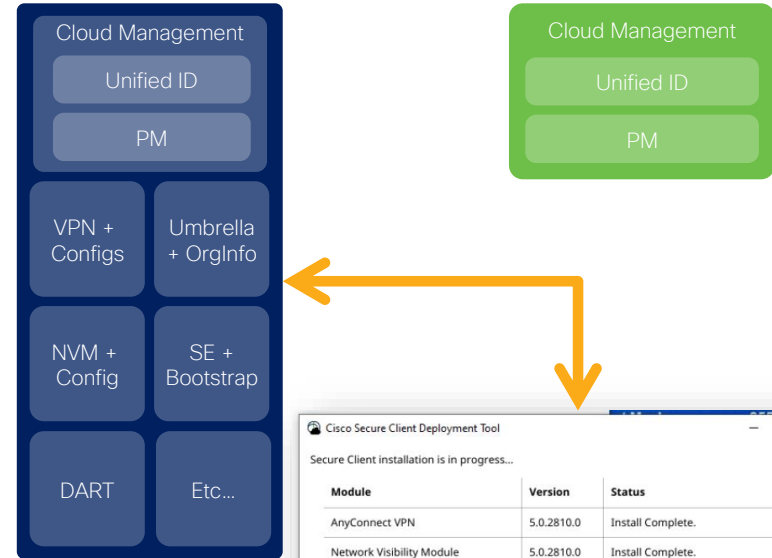
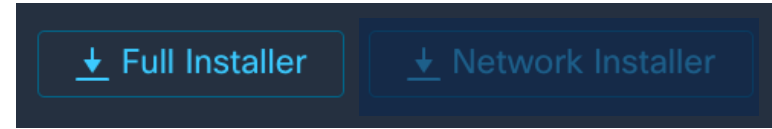
# Deployment Hierarchy

- 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 maybe in up to 45 Deployments (increasing in future)
- Installers are created dynamically based on the Deployment



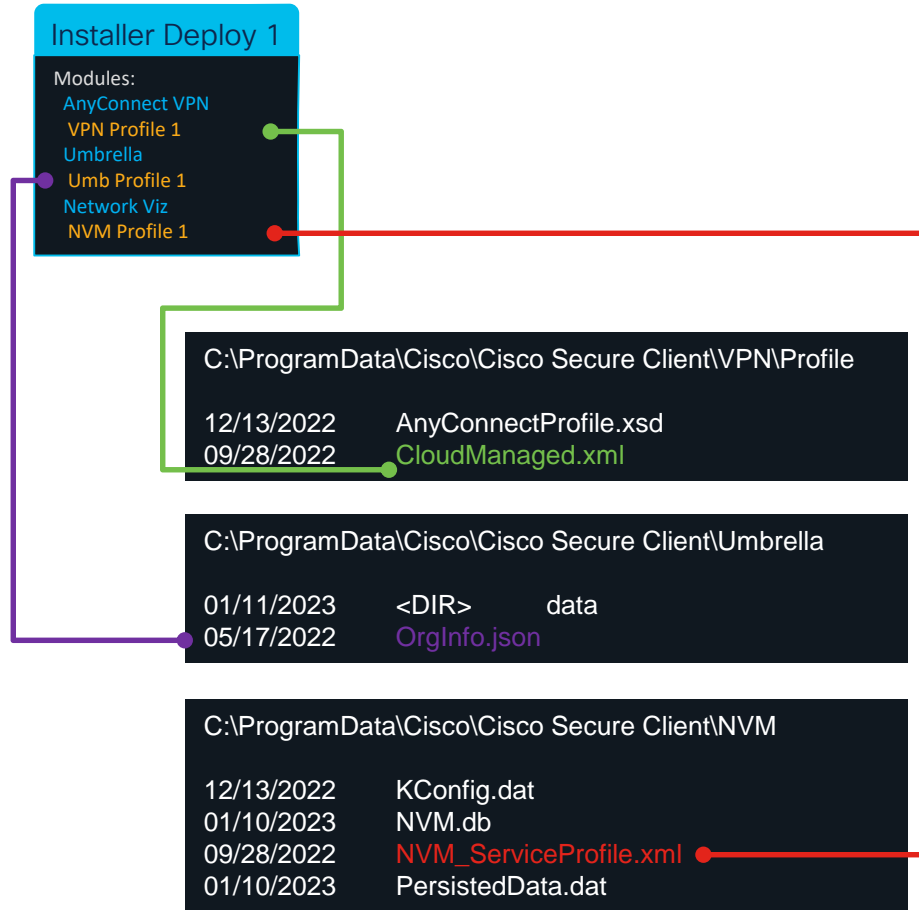
# Installing CSC

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



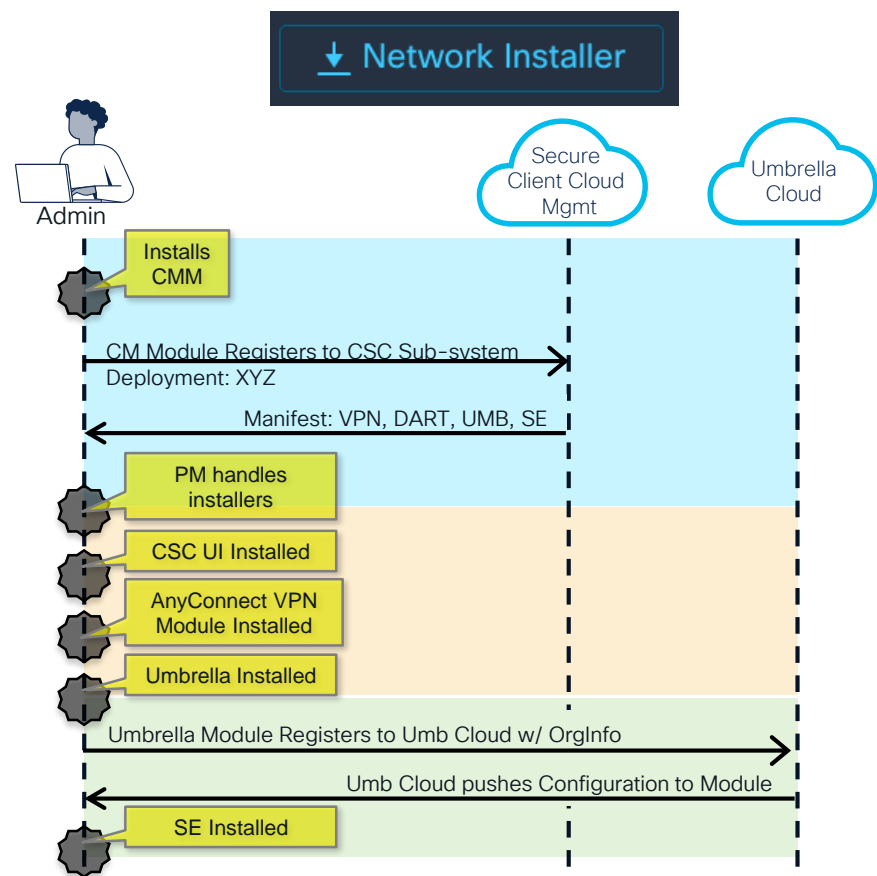
# Full Installer from Deployment

- 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)



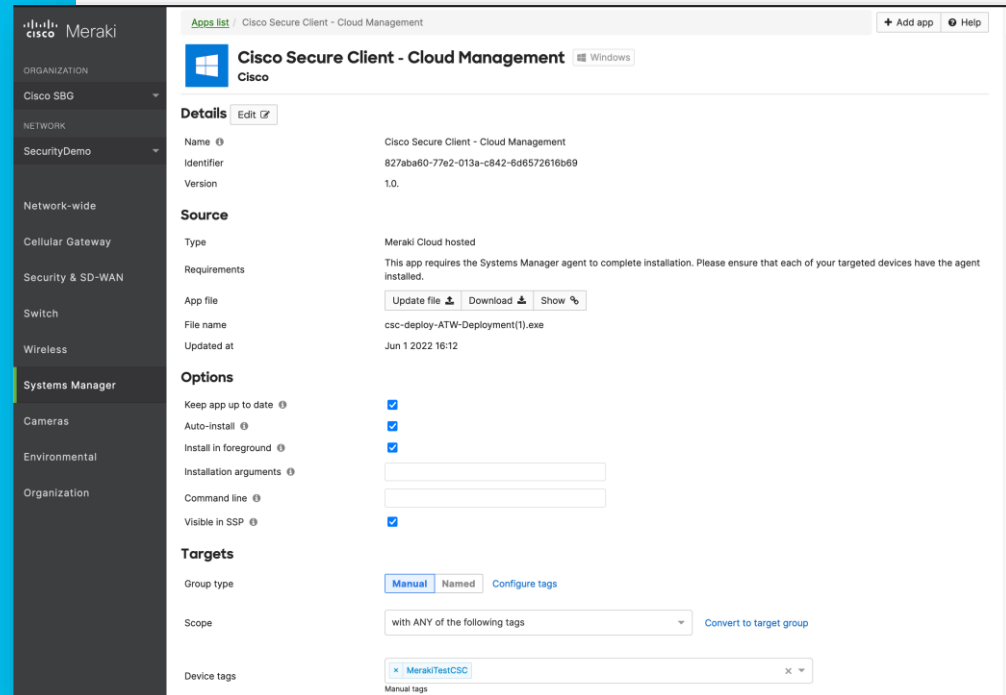
# Network Installer

- Lightweight installer
  - Installs the Cloud Management Module with its config only & Cloud Diagnostic tool
  - Package Manager pulls the manifest from deployment and installs each module and configuration.



# Installing CSC -MDM

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



# Client Management

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

The screenshot displays the Cisco XDR Client Management dashboard. The left sidebar contains navigation options: Control Center, Incidents, Investigate, Intelligence, Automate, Assets, Client Management (selected), and Administration. The main content area is titled 'Clients' and shows a summary of 4 total clients. It includes a 'Device Types' section with a pie chart and a 'Deployments' section with a bar chart. Below these is a table of clients with columns for Device Name, Deployment, CSC Version, Secure Endpoint Version, Cloud Management Version, Modules, OS, and OS Version. The table lists five clients: fireball, Lily\_Computer, Nervous, and TinaLaptop, each with their respective deployment and version information.

**Clients** 4 total

**Device Types**

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

**Deployments**

- PetersonHome: 2
- Yazji\_Home: 1
- Yazji\_Gaming: 1
- LP\_Chino: 0
- XDR Default Deployment: 0

**Text Search** Saved Filters Managed Status

Q User, IP, hostname... Select 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 Version
fireball	Yazji_Home	5.1.2.42	8.4.0.30201	1.0.1.400	Cloud Management v1.0.1.400 +5	Windows	11, SP 0.0 (Build 22631.326)
Lily_Computer	PetersonHome	5.1.2.42	8.2.3.30119	1.0.3.433	Cloud Management v1.0.3.433 +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 v8.2.1.21650 +6	Windows	11, SP 0.0 (Build 22631.356)
TinaLaptop	PetersonHome	5.1.0.136	8.1.7.21585	1.0.1.400	Cloud Management v1.0.1.400 +5	Windows	11, SP 0.0 (Build 22631.326)



# Moving Deployments – Admin Only

**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**

**Saved Filters**

**Managed Status**

**Sources**

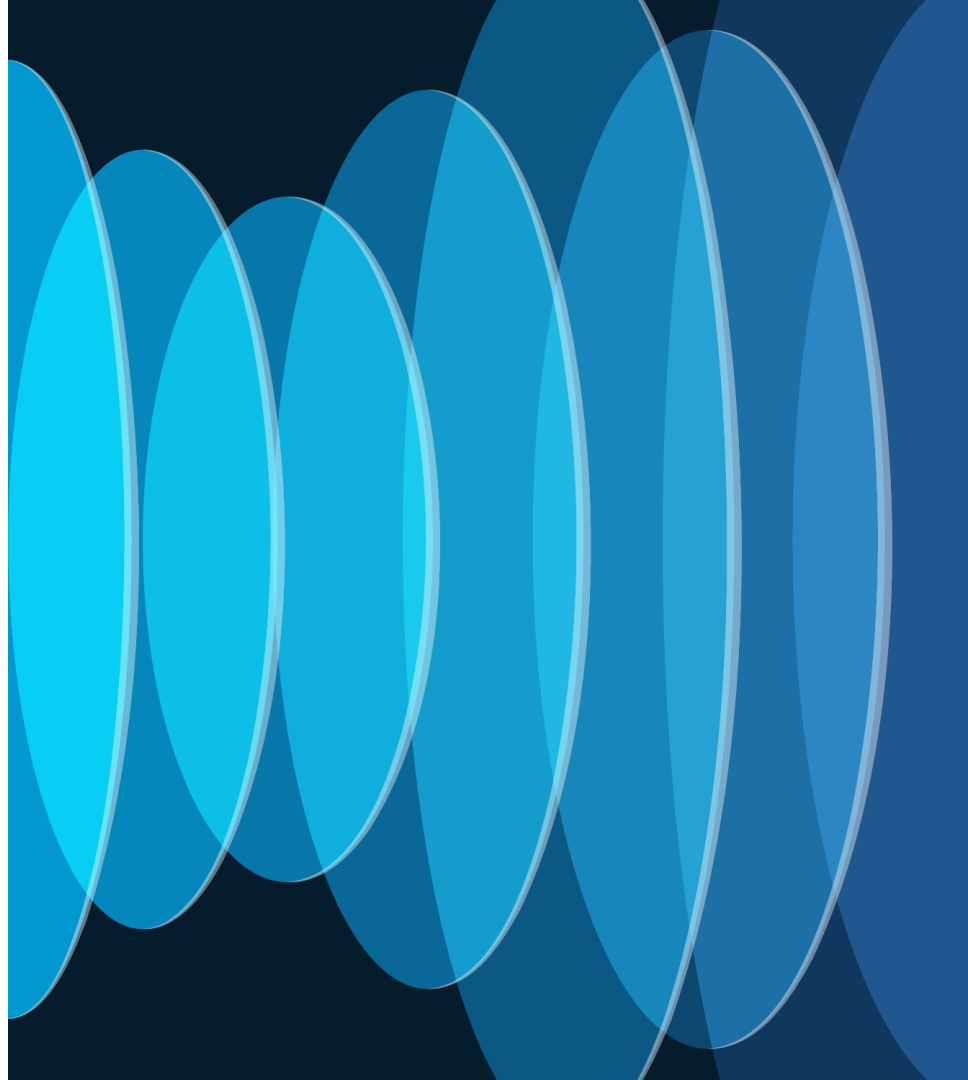
1 Device Selected

Device Name	CSC Version	Secure Endpoint Version	Cloud Managed	
<input checked="" type="checkbox"/> fireball	XDR Default Deployment	5.1.2.42	8.4.0.30201	1.0.1.400
<input type="checkbox"/> Lily_Computer	PetersonHome	5.1.2.42	8.2.3.30119	1.0.3.433

# Moving endpoints between deployments

- The UI tells the cloud backend that the “desired deployment” is XYZ.
- 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.

# Deployments w/ Secure Endpoint and Orbital



# Configuring Secure Endpoint

The screenshot shows the 'Secure Endpoint' configuration page in the 'Yazji\_Home' deployment. On the left, a sidebar lists 'Deployment Name', 'Cloud Management', 'Secure Endpoint' (highlighted with a blue circle), and 'Secure Client'. The main area has a 'Secure Endpoint' section with a 'Version Control' dropdown set to 'Latest (8.4.0.30201)' (callout 1). Below it, the 'Secure Endpoint Profile' section shows 'Secure Endpoint - Cisco - byazji' and a 'Choose a Group' button (callout 2). A modal window titled 'Choose a Group' is open, showing a search bar and a list of groups: 'Peterson\_Home\_BP\_Audit', 'YazjiGroup', and 'YazjiGroup\_NoExPrev' (callout 3). The modal has 'Cancel', 'Save', 'Back', and 'Next' buttons.

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

Select Desired SE Version

Select your SE Organization

There *can* be more than one

Choose the SE Group

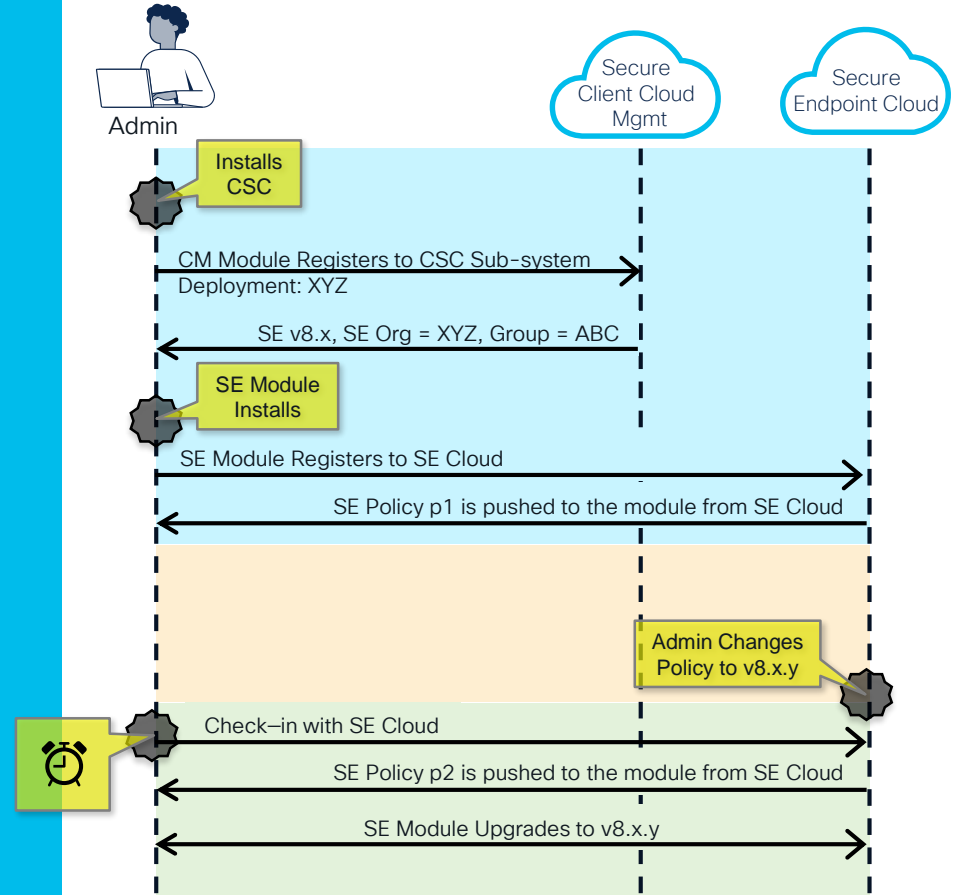
All endpoints who install the module via this deployment, will be assigned to this group, when the CSE module registers with the CSE cloud.

4

This screenshot shows the 'Secure Endpoint' configuration page with the 'Version Control' dropdown set to 'Latest (8.4.0.30201)'. The 'Secure Endpoint Profile' section shows 'Group: YazjiGroup' and a 'Replace Bootstrap Profile' button.

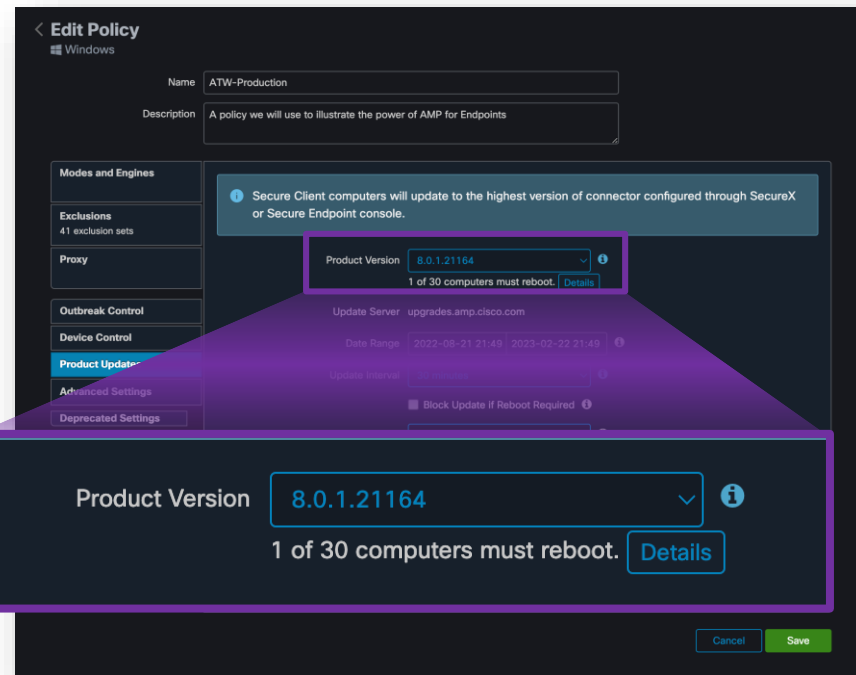
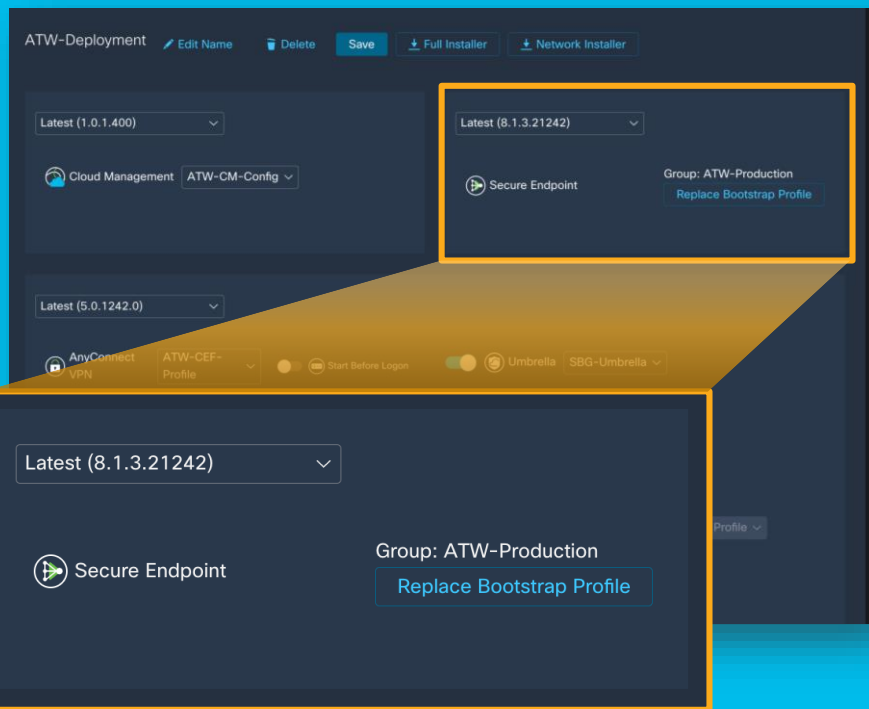
# Bootstrap?

- 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.



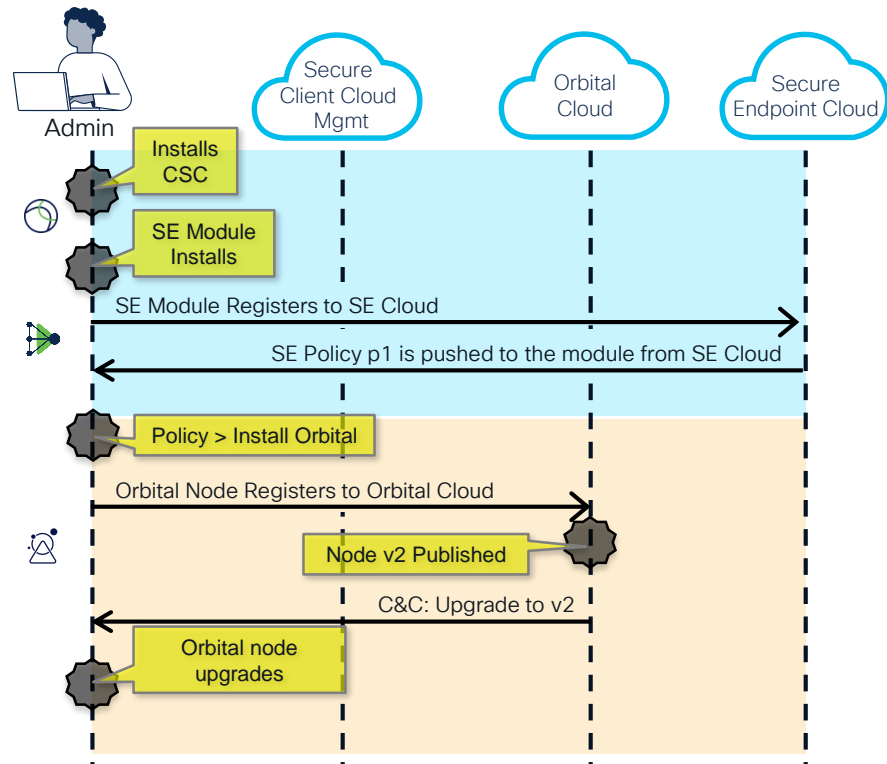
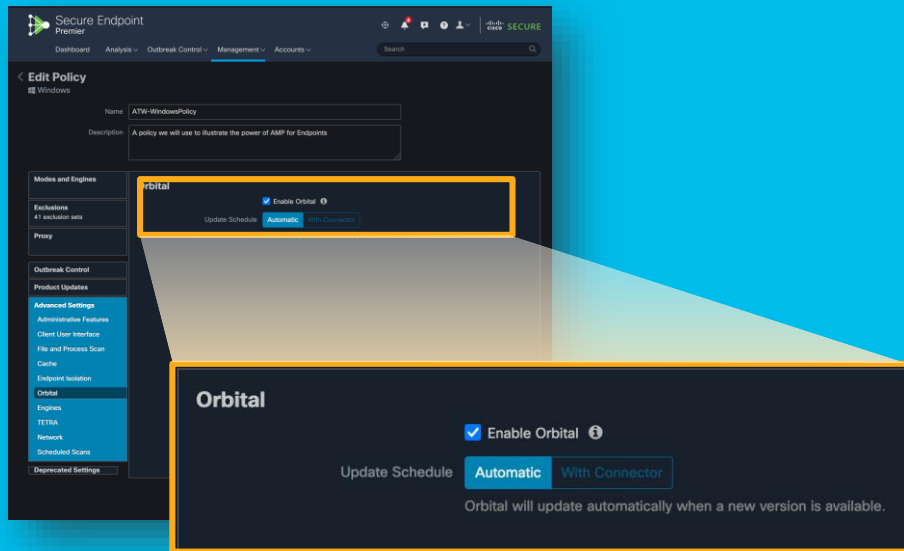
# SE Version Updates

Highest Version Wins!



# Deploying Orbital

- Orbital is still controlled by Secure Endpoint
- Updates with SE Connector or
- When published on Orbital Cloud



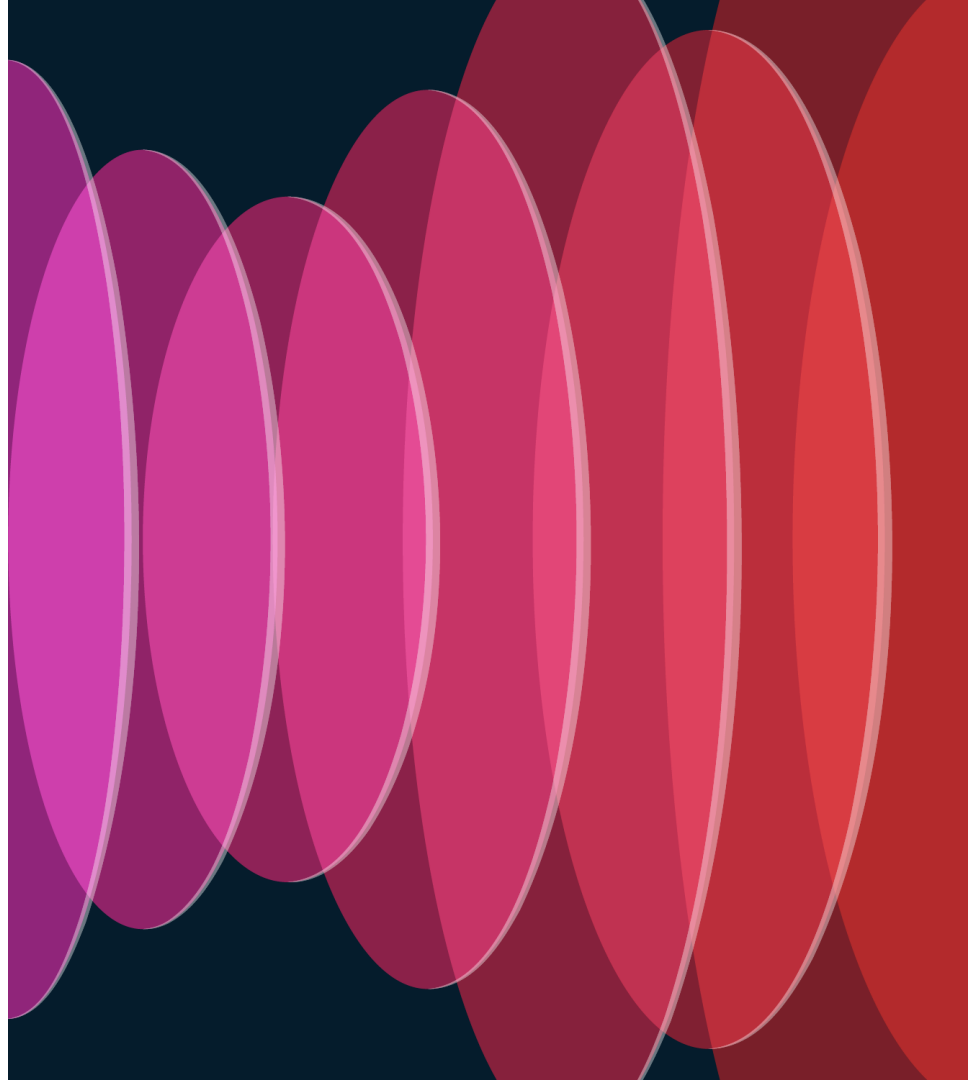


# Agenda

- CSC Overview
- CSC Architecture
- Cloud Deployment & Management
- Upgrading to CSC
- FAQs and Nuggets



# Upgrading



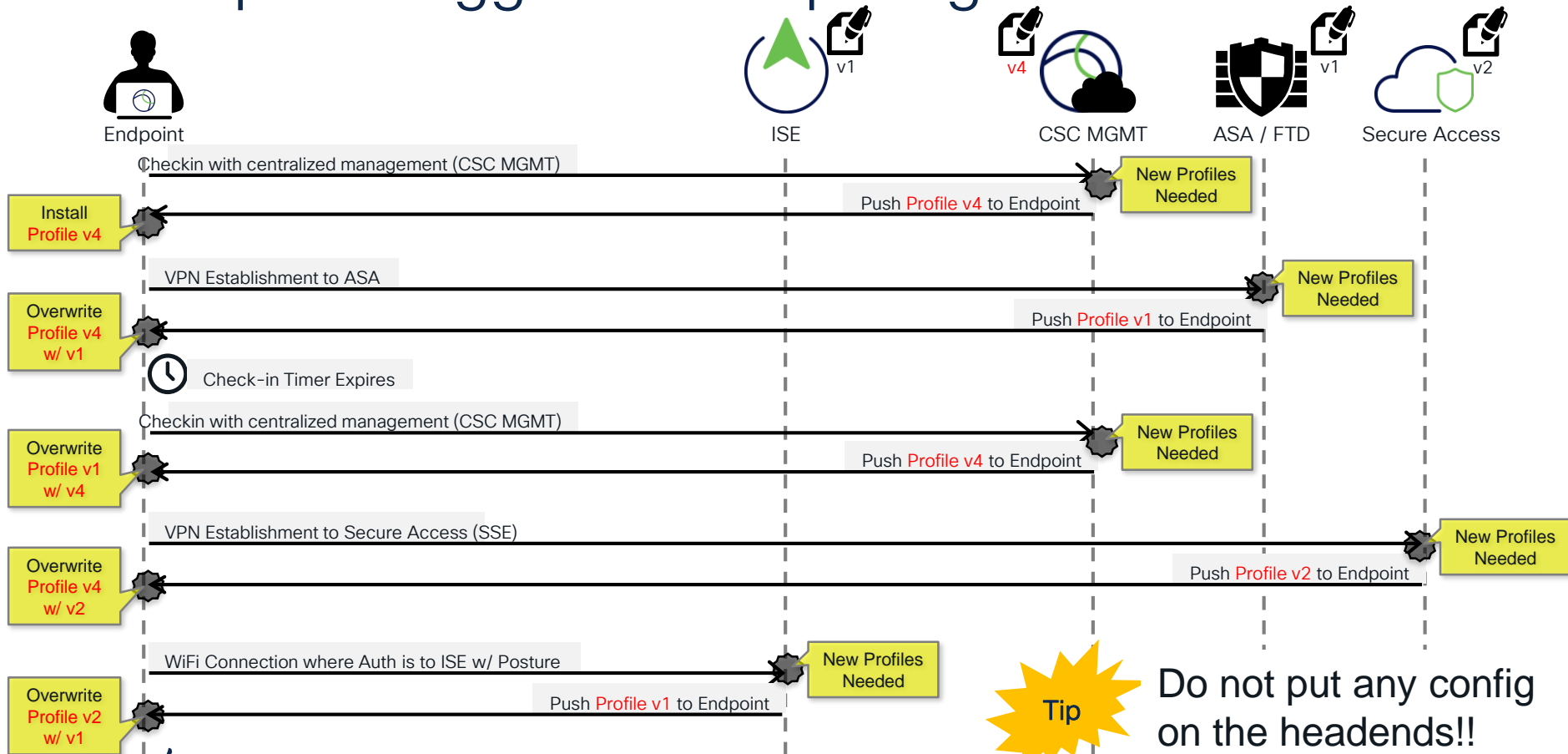
# Upgrading

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

# Overwriting from other Headends

- Scenario: mismatched profiles
  - CSC deployment in SecureX has a Profile v2
  - ASA group policy pushes Profile v1
    - Upon connecting to the ASA Headend, the Profile will be replaced with v1.
    - CSC Cloud Management update occurs (say 2 hours later), it will replace v1 w/ v2.
  - This cycle will continue until the ASA and CSC deployment in SecureX are aligned.
- Tip: Do not put any config on the headends!!

# The Epic Struggle of Competing Control Points



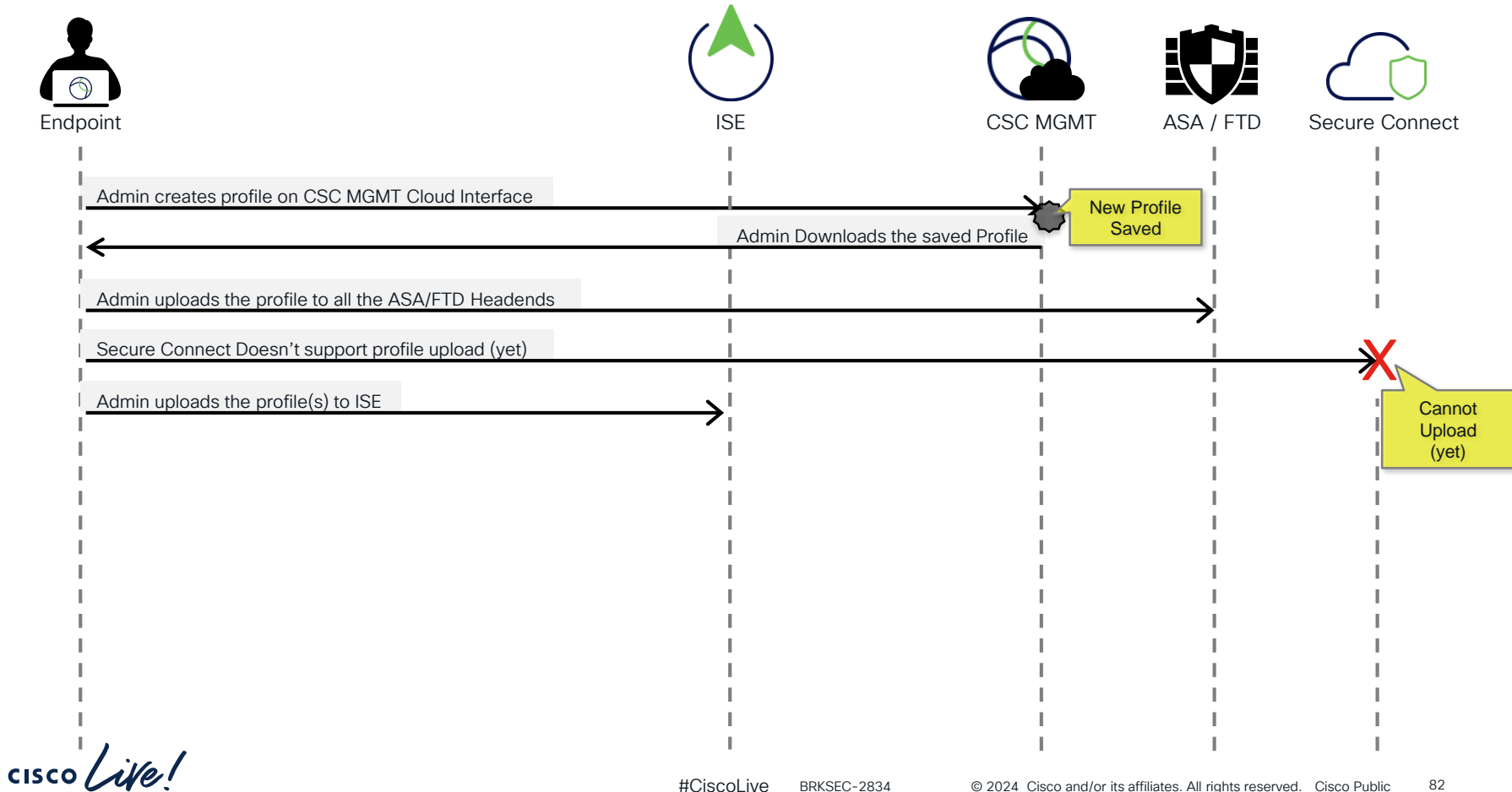
# Details on Profile Merges

- 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 SecureX Profile immediately on the ASA with same Filename

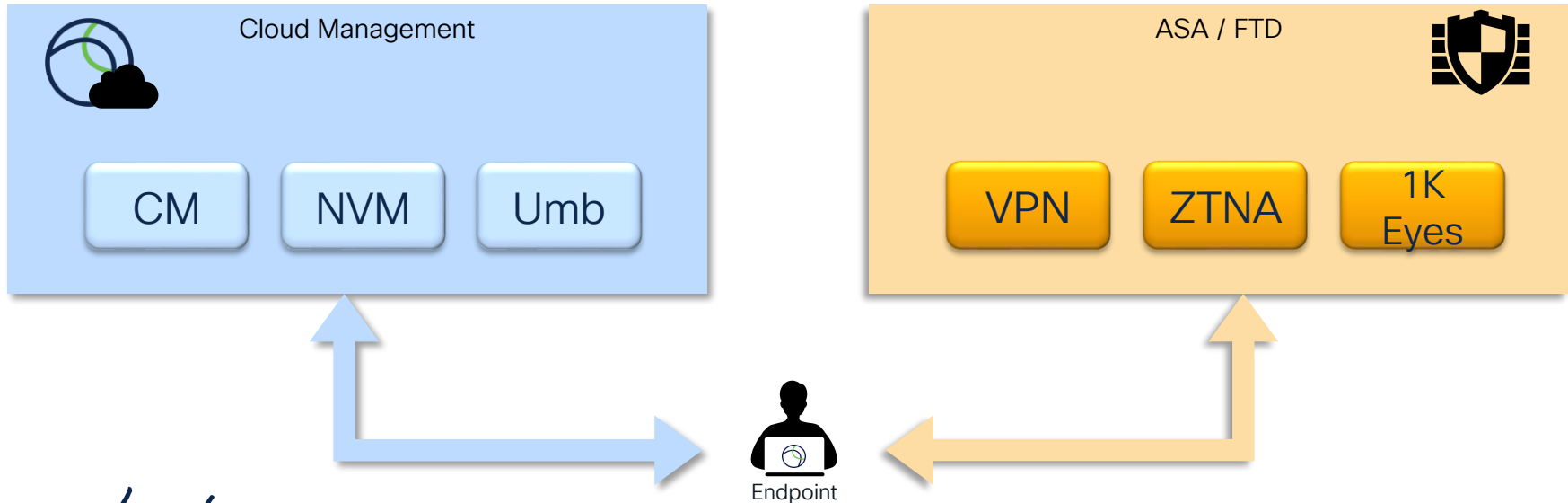
Do not put any config on the headends!!

# Download and Push to Head-ends

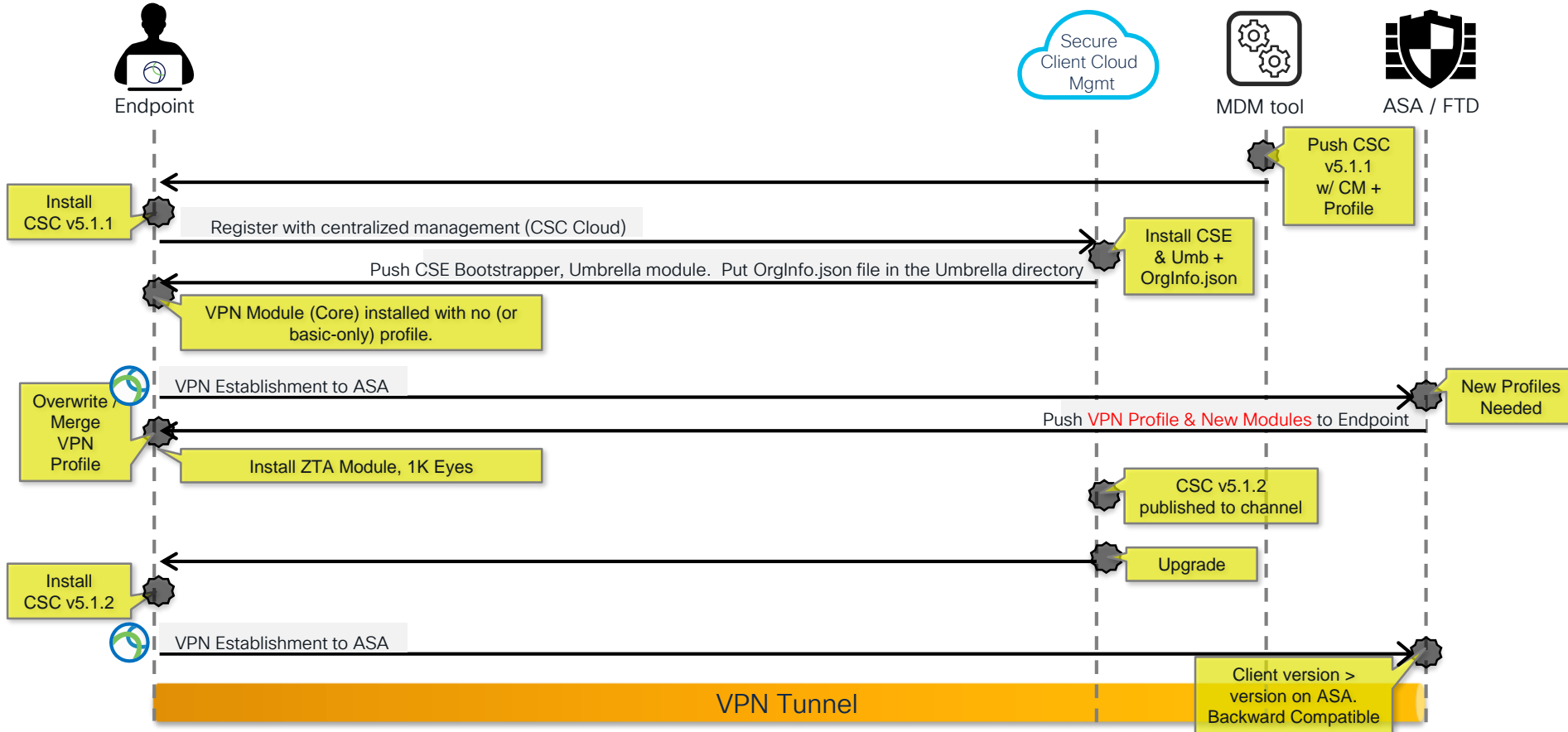


# Hybrid (Headend & Cloud)

- 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



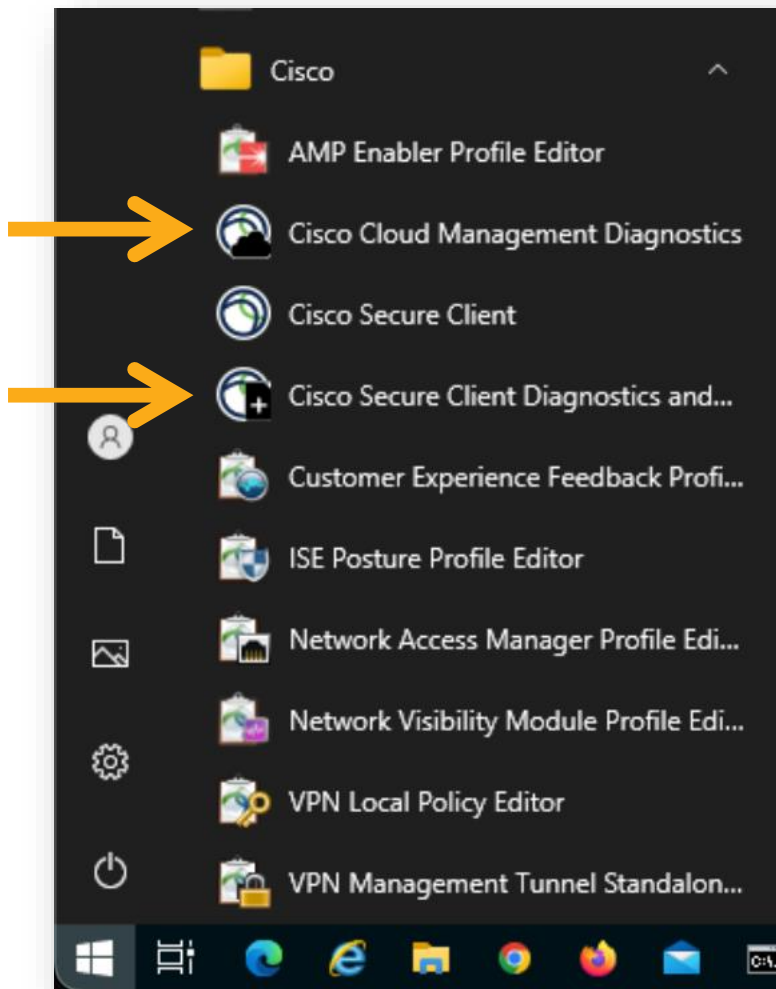
# Hybrid (Headend & Cloud)





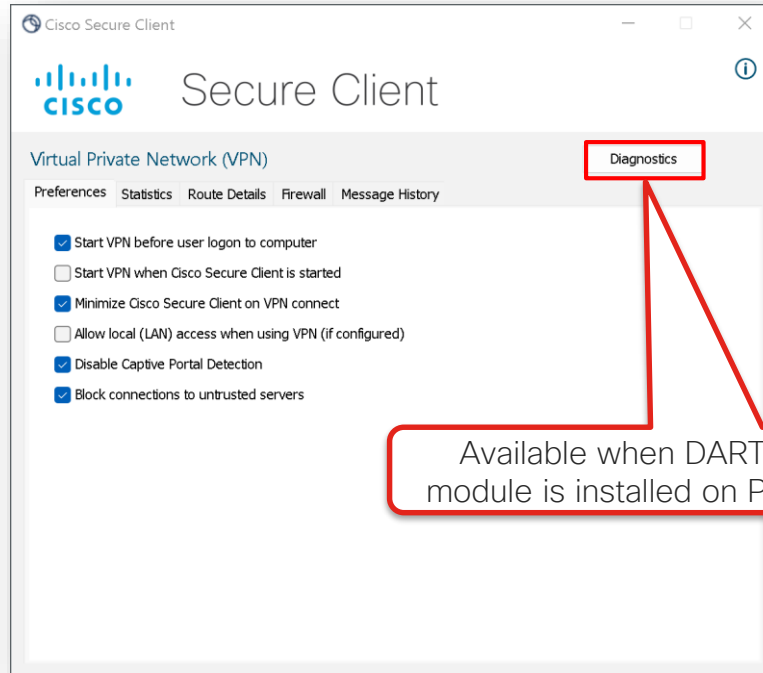
# DART & CM Diagnostics

- *“Dart or it Didn’t Happen”*
- DART is still the perfect endpoint troubleshooting bundling tool.
- Only available when you install it.
  - What about for troubleshooting Cloud Management only?

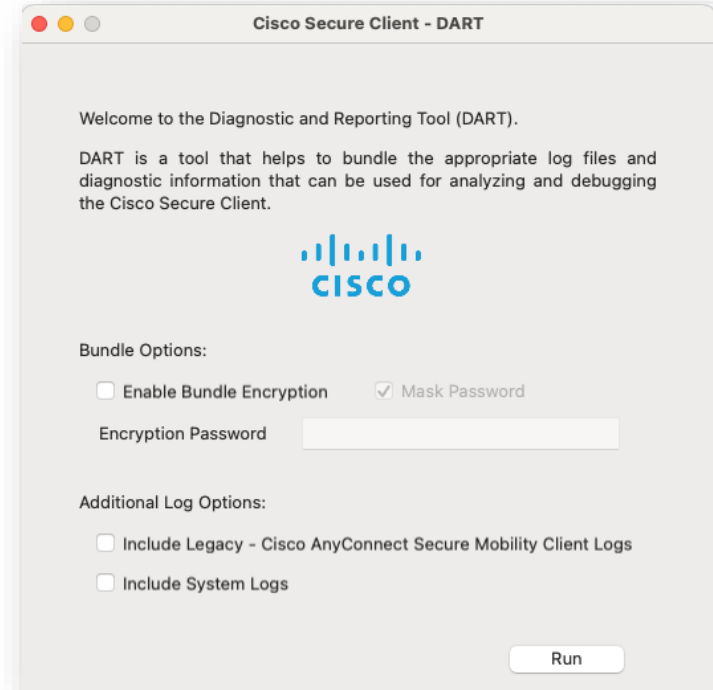


# The DART “Bundle”

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

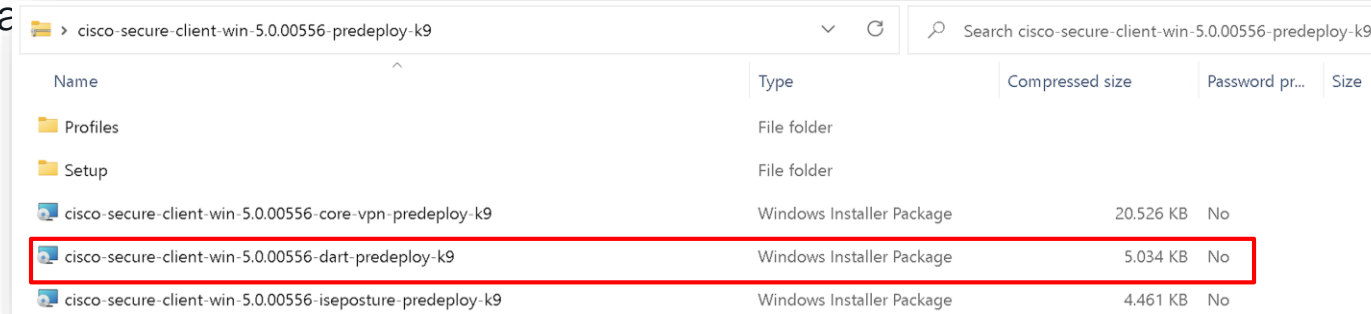


Available when DART module is installed on PC.



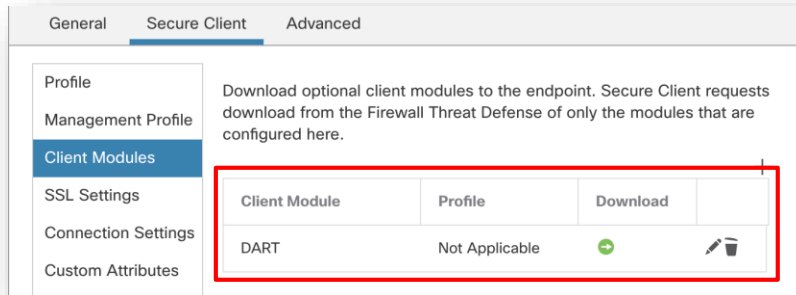
# DART Module Installation

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



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:



Client Module	Profile	Download	
DART	Not Applicable	➡	🗑️

```
ASA# show run group-policy GP1
group-policy GP1 attributes
[...]
```

webvpn

```
anyconnect keep-installer none
anyconnect modules value dart
```

# DART Module Installation

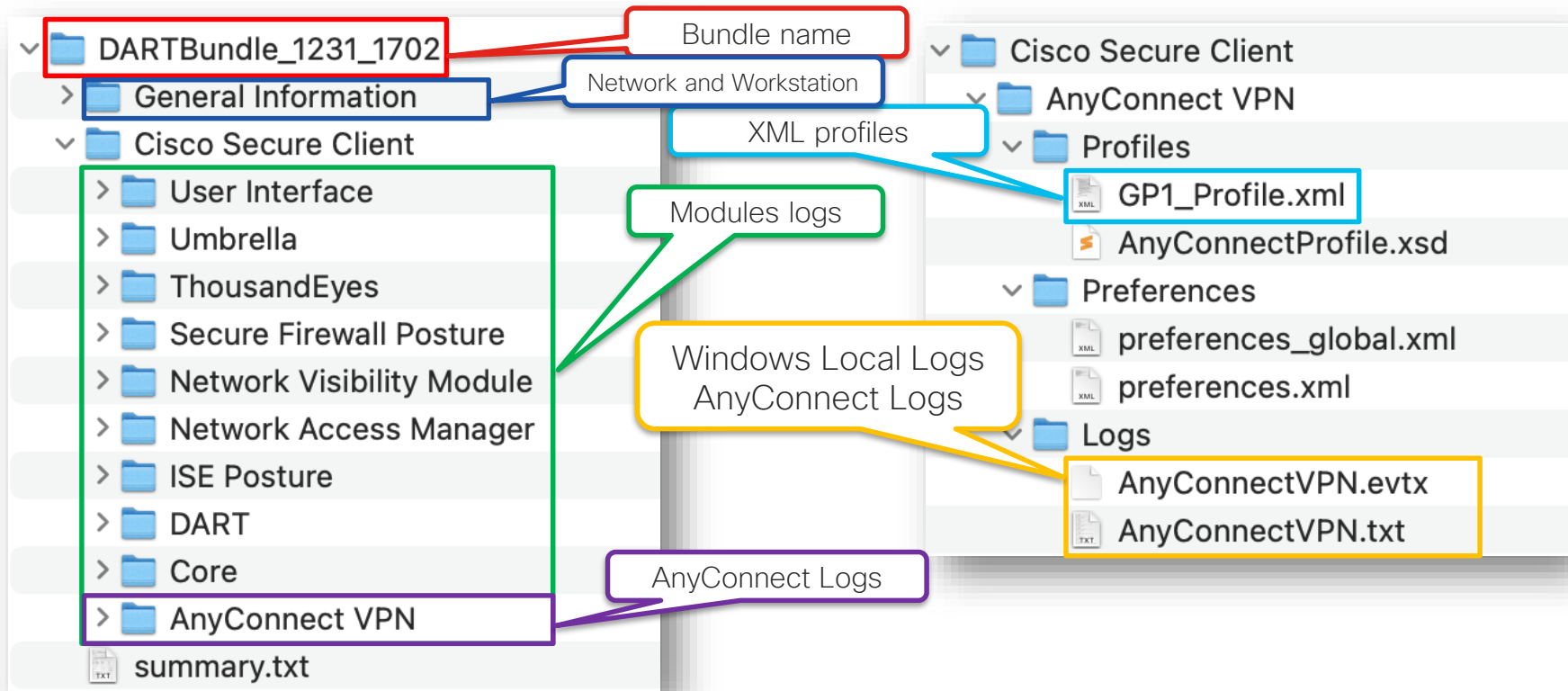
- Enabled in Cloud Management

The screenshot shows the 'Secure Client' configuration page for a deployment named 'Yazji\_Home'. The left sidebar lists the configuration steps: Deployment Name, Cloud Management, Secure Endpoint, and Secure Client (which is currently selected and highlighted with a blue circle and the number 4). The main content area is titled 'Secure Client' and contains several settings:

- Version Control:** A dropdown menu set to 'Latest (5.1.3.62)'.
- AnyConnect VPN Profile:** Two buttons, 'Upload Profile' and 'Create Profile', followed by a refresh icon and a toggle switch labeled 'Start Before Logon' which is currently turned off.
- Umbrella:** A checked checkbox, a dropdown menu set to 'Umbrella - byazji', and a button to 'View' the profile.
- Diagnostics and Reporting Tool:** A checked checkbox, which is highlighted with a red rectangle.
- ISE Posture:** An unchecked checkbox.
- Secure Firewall Posture:** An unchecked checkbox.
- Network Access Manager:** An unchecked checkbox.
- Network Visibility Module:** A checked checkbox, a dropdown menu set to 'NVM Cloud Default Profile', and a button to 'View' the profile.

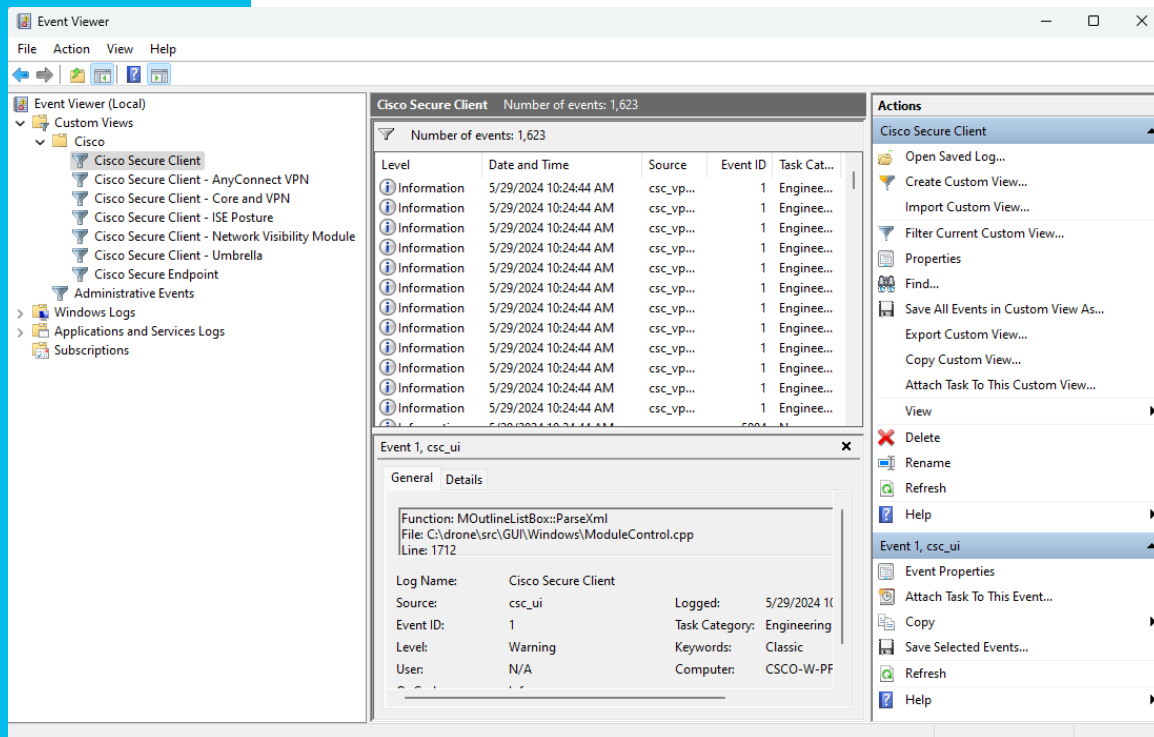
At the bottom of the page, there are 'Cancel', 'Back', and 'Save' buttons.

# Reviewing DART Bundle Content



# Secure Client Events / Logs

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



# Audit Logging

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

IP	Message	Operation	Target	Timestamp	User
	Updated installations for computer "loxx-win10vic03" (ID b997c56-0666-4e6d-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 - 18c42a84-4493-4d81-bb2-199f215d4d6e - 12f5f95a-b256-4cd2-8abf-9c8682eadc6" (format "amp") (ID 6a87742-e721-4337-92b9-191fc99b071). Configuration has 2 dependent deployments.	write	config-file	2024-01-19T20:31:26.415967825Z	admin@992027f-a88b-4b0e-8a38-58ad317c58af@ze0e9eaf-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-cb1026cbf0f).	write	computer	2024-01-19T20:11:47.910725356Z	
	Updated installations for computer "loxx-win10vic03" (ID b997c56-0666-4e6d-927a-86fa3ce55656).	write	computer	2024-01-19T20:01:29.891409833Z	
	Updated installations for computer "loxx-win10vic01" (ID b82fa451-03e8-49ee-a31c-a2a75d978406).	write	computer	2024-01-19T19:49:43.382545417Z	
	Updated installations for computer "atw-win10-jump" (ID 72014d6e-51a0-48d6-a6b6-192ba8da2d43).	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-ea66-4824-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 b997c56-0666-4e6d-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

The screenshot displays the Cisco Device Events management interface. It is divided into several sections with annotations:

- Step 1: Select the Computer**: This section includes a search bar labeled "Search For Device" with the text "fireball" entered. To the right, the "Device Selected" field shows the ID "ef6c878a-dee7-489f-b2d3-1a055c92". Below these is a table with columns: Host Name, Last Updated, OS Type, OS Version, and UID. The first row shows "fireball", "May 21, 2024 @ 7:53 PM CDT", "windows", "11, SP 0.0 (Build 22631.3296)", and the selected device ID. A "Select Device" button is next to the ID.
- Step 2: (optional) Enter Time Range**: This section shows a "Filter by Dates" area with a date range selector and a "Clear Filter" button.
- Step 3: Expand the Event**: This section shows a list of events. The first event is expanded, showing details for a "pkg-install" event at timestamp "2024-05-16T14:36:36.25Z" from IP "184.55.67.86". The expanded view shows a JSON-like log entry with fields like "type", "timestamp", "source", and "data".





# Agenda

- CSC Overview
- CSC Architecture
- Cloud Deployment & Management
- Upgrading to CSC
- FAQs and Nuggets

# CSC for non-Windows

- Cisco AnyConnect has been **rebranded** Cisco Secure Client
- No additional features compared to Cisco AnyConnect
  - Not cloud managed
  - Not integrated with Secure Endpoint (yet)

cisco *Live!*



/ Secure Client (including AnyConnect) / Secure Client 5 / AnyConnect VPN Client Software- 5.0.01242

The screenshot displays the Cisco Software Download page for Secure Client 5.0.01242. The page is titled "Software Download" and includes a search bar and navigation links. The main content area shows the "Secure Client 5" release information, including the release date (19-Dec-2022) and size (7.32 MB). A table lists various download packages for different operating systems and architectures, such as Linux 64-bit, Android, and Mac OS. The page also includes a "Related Links and Documentation" section with links to the Secure Client Ordering Guide, Release Notes, and Administrator Guide. In the bottom right corner, there is a mobile app interface showing the "Cisco Secure Client" app with an "OPEN" button and a "Cisco Security Connector" app with a download button.

# Frequently Asked Questions

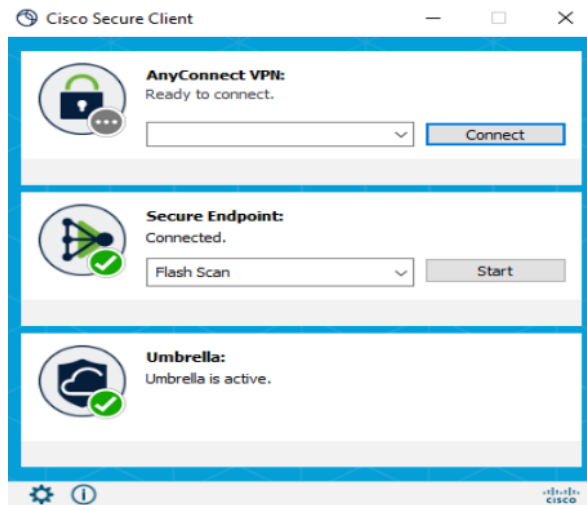
- Traditional Secure Client modules are still version locked together
- Duo is not in Secure Client yet
- macOS Cloud Mgmt – Fiscal Q4
- Linux: no date yet
- A profile may only be in up to 45 deployments
  - TAC case to extend it
- Secure Client may be used with or without the Cloud Management, except 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?”*

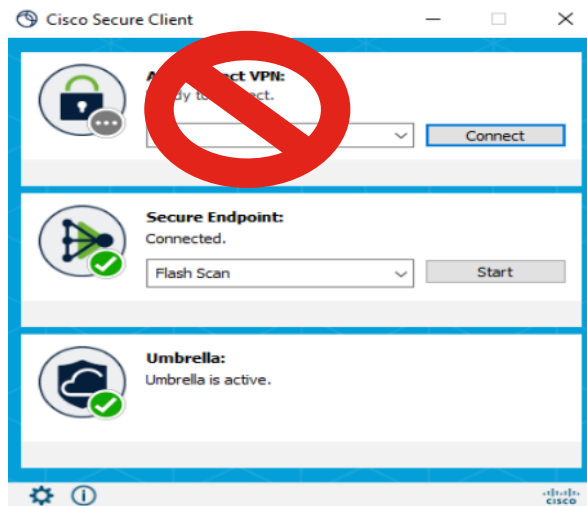
<https://support.umbrella.com/hc/en-us/articles/18211951038740-How-to-hide-the-VPN-module-in-Cisco-Secure-Client-Windows>



# 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?”*



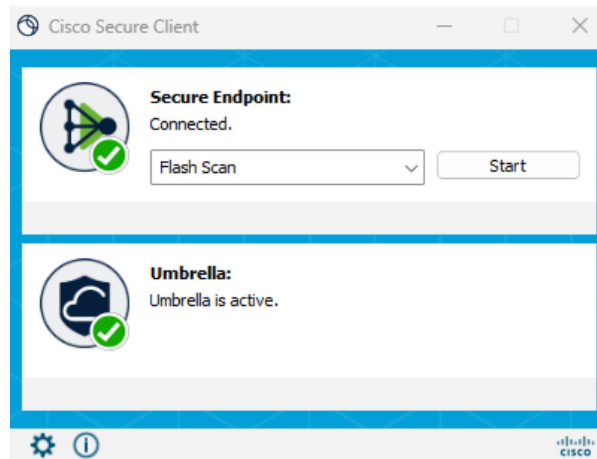
<https://support.umbrella.com/hc/en-us/articles/18211951038740-How-to-hide-the-VPN-module-in-Cisco-Secure-Client-Windows>

# 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?”*

<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

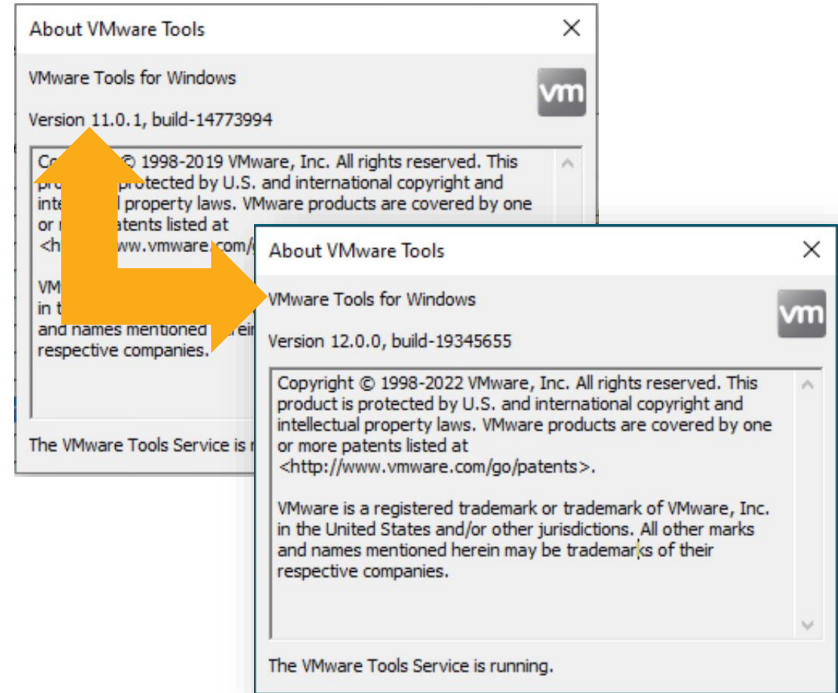
- Fyne error: window creation error
- CSC will not install on VMWare Virtual Machine
  - **Cause:** VMTools is outdated / Missing Open GL drivers
  - **Solution:** Upgrade to latest VMTools, install Mesa OpenGL or do command line

```
C:\Users\x\Downloads>".\csc-deploy-ATW-Deployment.exe"
```

```
2022/05/17 13:13:29 Fyne error: window creation error
```

```
2022/05/17 13:13:29 Cause: APIUnavailable: WGL: The driver does not appear to support OpenGL
```

```
2022/05/17 13:13:29 At: E:/workspace/workspace/maine3a9e2e0/source/vendor/fyne.io/fyne/v2/internal/driver/glfw/driver.go:123
```



CLI Install w/ a -q option

# Common Issue: Installation

*“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

The screenshot shows the 'Product Update Window' configuration page. It features a toggle for 'Enable Product Update Window', a 'Day' selector with 'Mon' highlighted, 'Start Time' and 'End Time' dropdowns set to '1:00' and '6:00' respectively, and 'AM' selected for both periods. A 'Select Time Zone' toggle is also present. Arrows from the title above point to the 'Enable Product Update Window' toggle, the 'Day' selector, and the 'Select Time Zone' toggle. 'Configure' buttons are visible in the top right and bottom right corners.

**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

6:00

Period

AM PM

☒ Select Time Zone

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

Configure ^

Configure v

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 1: Get me a DART. Didn’t even bother with troubleshooting before DART.
- Step 2: 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_cmldapi.log:3:[] [4264] T: 10FC F: CMIDStoreReader.cpp L: 55 f: cmdid::CCMIDStoreReader::GetCMID S: error :: Fetching CMID failed. Returning CMID = []
csc_cmld.exe.log:19:[] [7064] T: 54C F: CMIDUtils.cpp L: 133 f: cmdid::GetBinaryRegistryKey S: error :: RegOpenKeyEx failed The operation completed successfully.
csc_cmld.exe.log:20:[] [7064] T: 54C F: AttributeCollectorWin.cpp L: 802 f: cmdid::CAttributeCollectorWin::getDeviceID S: error :: Failed to retrieve device details
csc_cmld.exe.log:22:[] [7064] T: 54C F: AttributeCollectorWin.cpp L: 91 f: cmdid::CAttributeCollectorWin::GetAttributeList S: error :: Failed to retrieve AC UDID
csc_cmld.exe.log:23:[] [7064] T: 54C F: AttributeCollectorWin.cpp L: 162 f: cmdid::CAttributeCollectorWin::getBIOSSerialNumber S: error :: Failed to encode BIOS serial number.
csc_cmld.exe.log:24:[] [7064] T: 54C F: AttributeCollectorWin.cpp L: 107 f: cmdid::CAttributeCollectorWin::GetAttributeList S: error :: Failed to retrieve BIOS Serial Number.
csc_cmld.exe.log:40:[] [7064] T: 1938 F: CloudRequest.cpp L: 227 f: cmdid::IdentityServiceRequest::Serialize S: error :: Mandatory Hardware data missing.
csc_cmld.exe.log:41:[] [7064] T: 1938 F: CloudCommunicator.cpp L: 120 f: cmdid::CloudCommunicator::communicationThread S: error :: failed to serialise
csc_cmld.exe.log:48:[] [7064] T: 54C F: CMIDAgent.cpp L: 217 f: cmdid::CCMIDAgent::handleCloudResponse S: error :: CMID agent received Identity Response
csc_cmld.exe.log:49:[] [7064] T: 54C F: CMIDAgent.cpp L: 330 f: cmdid::CCMIDAgent::handleIdentityServiceResponse S: error :: Error occurred 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'>1.25</entry>
    <entry name='date'>06/21/22</entry>
  </bios>
  <system>
    <entry name='manufacturer'>LENOVO</entry>
    <entry name='product'>Virt-Manager</entry>
    <entry name='version'>0.9.4</entry>
    <entry name='serial'>WB61111610061</entry>
    <entry name='uuid'>337e27d5-91b2-4108-79cb-07ebc7dbaf94</entry>
  </system>
</sysinfo>
<smbios mode='sysinfo'>
```

# Check the NVM Directory

- %programdata%\Cisco\Cisco Secure Client\NVM\

- 2 files need to be there:

06/04/2023 03:00 PM

311 NVM\_BootstrapProfile.xml

06/04/2023 03:25 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="1.0" encoding="UTF-8"?>
<NVMBootstrapProfile xsi:noNamespaceSchemaLocation="NVMBootstrapProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Cloud>
    <CloudServer>intake.prod.[region].tmc.nvmc.csc.cisco.com</CloudServer>
    <CloudPort>443</CloudPort>
  </Cloud>
</NVMBootstrapProfile>
```

# NVM\_ServiceProfile.xml

```
<NVMProfile xsi:noNamespaceSchemaLocation="NVMProfile.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ProfileVersion>3</ProfileVersion>
  <CollectorConfiguration>
    <ExportTo>Cloud</ExportTo>
    <PingInterval>5</PingInterval>
  </CollectorConfiguration>
  <TemplateReportInterval>60</TemplateReportInterval>
  <AgglInterval>5</AgglInterval>
  <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>
    </Policy>
  </DataCollectionPolicy>
  <Fields>350,12333,12334,12335,12336,12337,12338,12339,12340,12341,12342,12343,12344,12345,12346,12347,12351,12352,12353,12356,12357,12358,12360,
  12361,12362,12363,12365,12366,12367,12368,12369,12370,12371,12372,12373,123591,123592</Fields>
</NVMProfile>
```

# Do we see traffic?

- Traffic is NOT in the older IPFIX (netflow) format.
- It is inside TLS1.2 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

The image shows a Wireshark packet capture of a TLS1.2 handshake. The top pane displays a list of packets, with packet 691 selected. The middle pane shows the details of the selected packet, which is a TLSv1.2 Handshake Message (Type 1). The bottom pane shows the raw data of the packet, which is a TLSv1.2 Handshake Message (Type 1). The handshake is between a client (Source: 10.1.82.157) and a server (Destination: 44.215.189.243). The handshake is initiated by the client with a 'Client Hello' message (Sequence Number: 606). The server responds with a 'Server Hello' message (Sequence Number: 606). The handshake is completed with a 'Finished' message (Sequence Number: 606) from the client and an 'Acknowledgment' message (Sequence Number: 606) from the server. The handshake is encrypted with a cipher suite of TLSv1.2.

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=0
630	7.889794	44.215.189.243	10.1.82.157	TCP	66	443 → 53958 [SYN, ACK] Seq=0 Ack=1 Win=0
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 Spec
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=0
645	7.965245	10.1.82.157	44.215.189.243	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake
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=0
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\_{EAE9CF-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

> 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 adds 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.

Search

Android iOS Network

group **OrbitalOnly** 56

loxx-win10vic04.org26.net	Group	OrbitalOnly
Windows 10 Enterprise (Build 19045.3693)	Policy	ThirdPartyWinPolicy
8.2.1.21650	Internal IP	10.182.154
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
000000000000000000	Cisco Secure Client ID	1d279cb4-20e4-417b-a819-73094c60c272
	Cisco Security Risk Score	56

Investigate in Orbital

Events | Diagnostics | Move to Group... | **Uninstall Connector** | Delete

25 / page

1 of 1

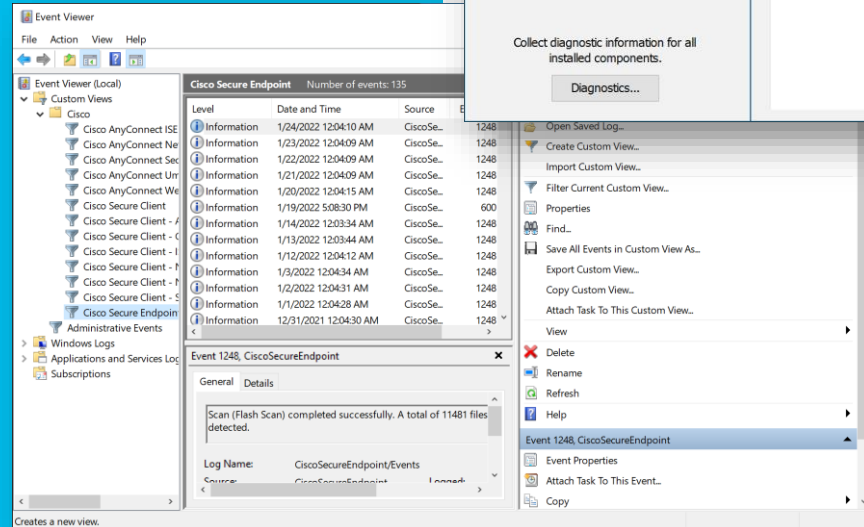
Export to CSV

Cisco Secure Client does not support remote uninstall.



# Secure Endpoint Advanced

- Scan History moved to Advanced Tab

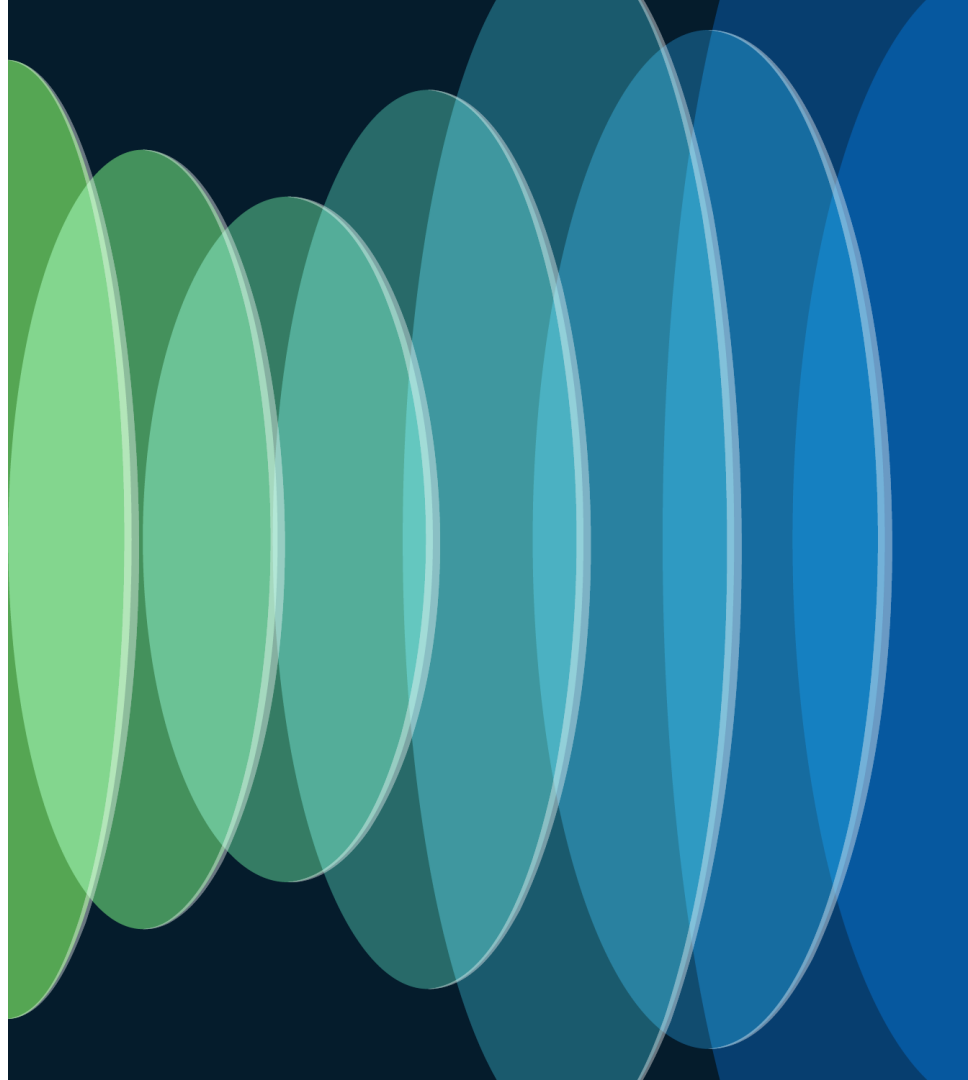


# Helpful Links

- Cisco Live Teams Space:  
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2834>
- Endpoint Bar (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#/>

Continue your  
education

CISCO *Live!*



# 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 2025.

---



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

---



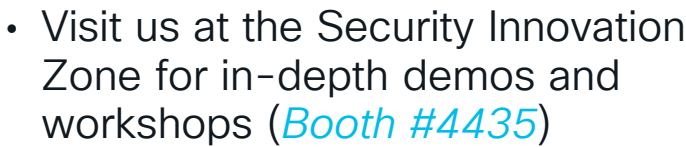
Level up and earn **exclusive prizes!**

---



Complete your surveys in the **Cisco Live mobile app**.





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

- Contact me at: [byazji@cisco.com](mailto:byazji@cisco.com)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive