

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Cisco Secure Client

Technical Deep Dive

Aaron T Woland, CCIE #20113

Distinguished Engineer, Threat Detection & Response

loxx@cisco.com | @aaronwoland

BRKSEC-2834

CISCO *Live!*

#CiscoLiveAPJC

\$ whoami



Cisco role: Distinguished Engineer,
Threat Detection & Response

Unofficial title:
“Cisco History Professor”

Experience: Old enough to wonder
how I have been doing this for ~30
years

Fun fact 1: Father of 5 daughters

Fun fact 2: Oldest works for Cisco
now! Youngest is 18 months!

Fun fact 3: Working through his
Cyber Security Master’s Degree
from SANS Institute (~04/24)

Sarcasm

*“If we can’t laugh
at ourselves,
Then we cannot
laugh at anything
at all”*



Disclaimer: “All Comments are my own, and are not representative of Cisco... Any correlation to real live persons or situations was completely unintentional... Blah Blah Blah...”

Important: Hidden Slide Alert



Look for this “For Your Reference”
Symbol in your PDF’s

There is a tremendous amount of
hidden content, for you to use later!



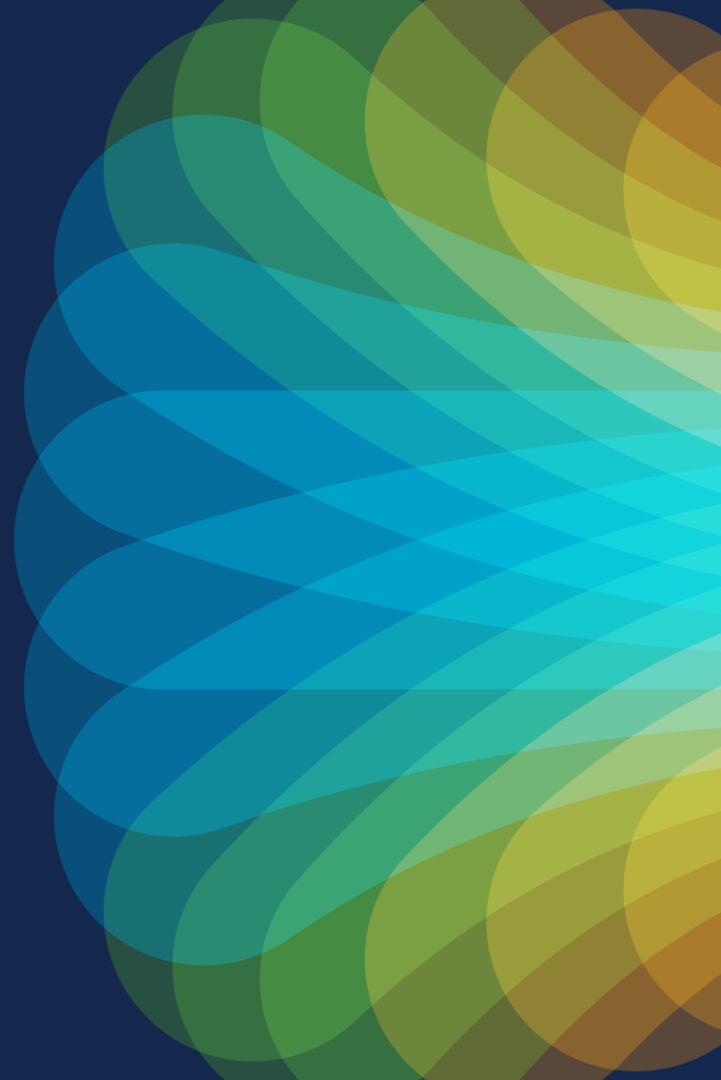
For Your Reference

Please fill out the survey



Drop your email in the comments – I WILL respond!

Let's get this
road on the
show...





“You cannot put another agent on
our endpoints unless it replaces
two”

Chris H., CISO Global Bank

Agenda

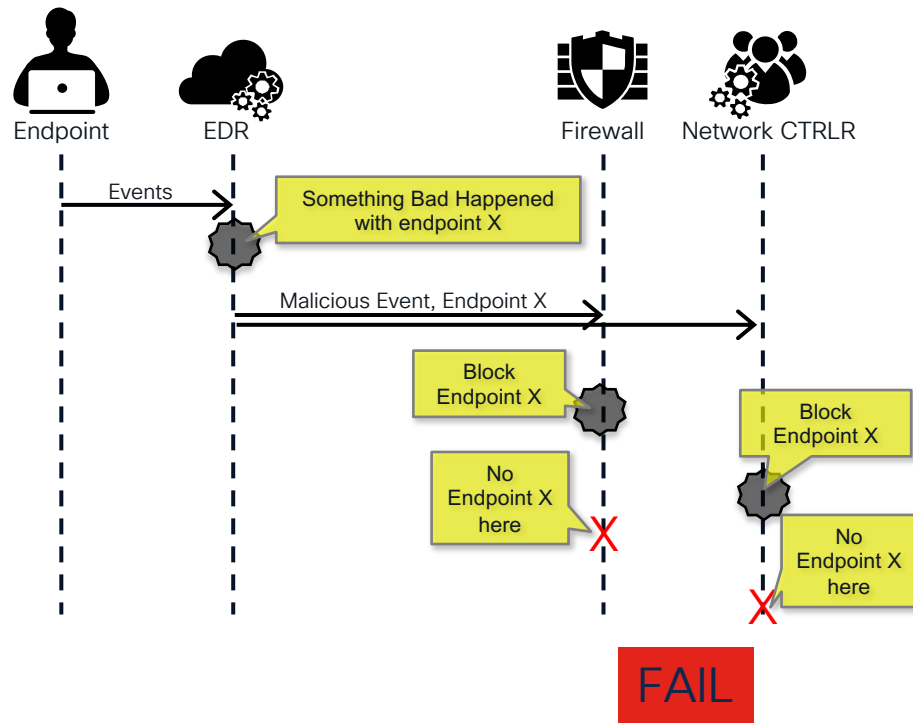
- CSC Overview
- CSC Architecture
- Deploying / Managing from Cloud
- Upgrading to CSC
- FAQs

Why build a unified security agent?

- Our customers have identified **operational challenges** with **deploying multiple endpoint agents** (e.g., AnyConnect, AMP4E, Orbital, Umbrella, Duo, Meraki SM, 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...

- You have seen this with SIEM & SOAR
- 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)
- Making the products work together is a challenge



We need a common endpoint “object”

We are doing two things about this

1. Device Insights

- Creates a common endpoint object from integrated sources

2. Cisco Secure Client

- Creates a common, immutable identity available for all integrated services of the unified agent



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

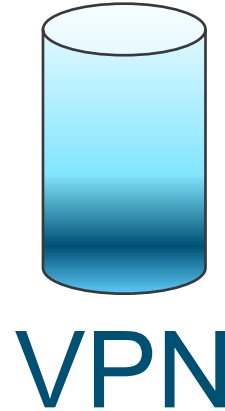


- Initial “unified agent” release is Windows only
- Seamless upgrade to new unified agent from existing AnyConnect & Secure Endpoint Clients
- Leverages Existing AnyConnect Framework
 - AC already has modules for many services
 - AC UI is starting point for new shared UI
 - Core AC services, such as trusted network detection, become available as common services for all modules
 - UI represents only installed functions
- Introduces a new Cloud Management System inside SecureX

We used to go around the world stating:



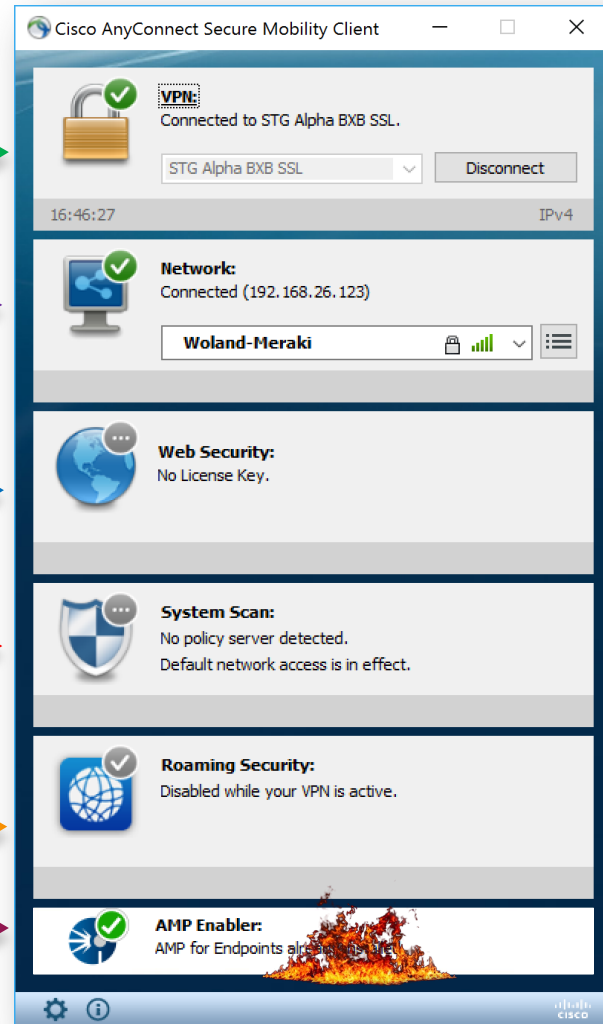
is
more
than



Cisco AnyConnect

Suite of security service enablement modules

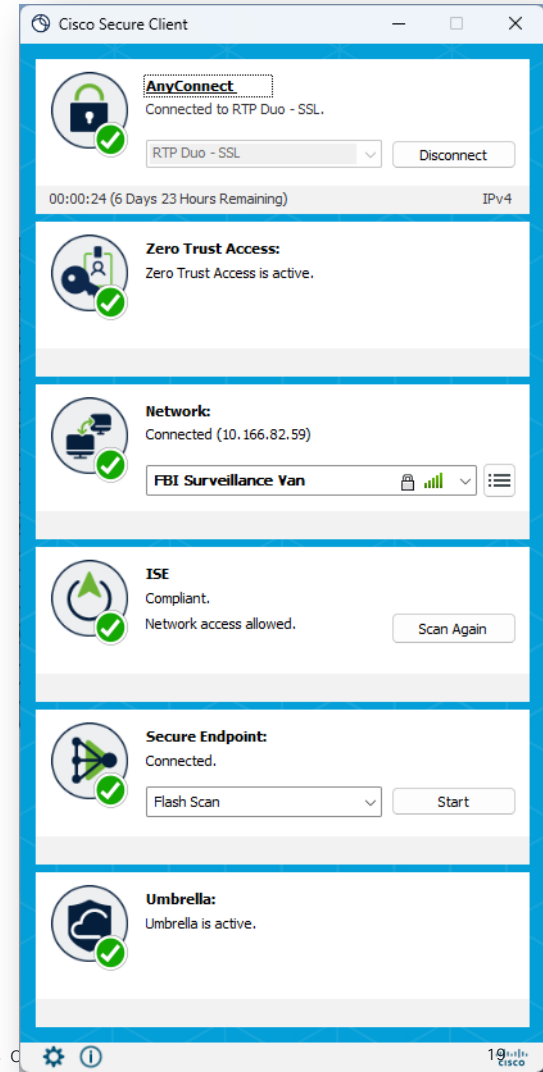
- VPN Module (Core)
- Network Access Manager (NAM)
- ~~Web Security (CWS)~~
- Posture
- Umbrella Module
- HostScan (aka: ASA posture) (No UI)
- Network Visibility Module (NVM) (No UI)
- ~~AMP Enabler Module~~
- Diagnostics and Reporting Tool (DART)



Cisco Secure Client

Suite of security service enablement modules

- AnyConnect VPN (Core)
- Zero Trust Access (Cisco Secure Access)
- Network Access Manager (NAM)
- ISE Posture
- Secure Firewall Posture (aka: HostScan) (No UI)
- Secure Endpoint (AMP)
- Umbrella Module
- Cloud Management Module (No UI)
- Network Visibility Module (NVM) (No UI)
- Diagnostics and Reporting Tool (DART)
- Thousand Eyes (new) (No UI)



Secure Endpoint Statistics

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

The screenshot displays the Cisco Secure Client application window. The title bar reads "Cisco Secure Client". The interface features a left-hand navigation pane with the following items: "Status Overview", "AnyConnect VPN", "Network", "ISE Posture", "Secure Endpoint" (which is highlighted with a right-pointing arrow), and "Secure Umbrella". Below this pane, a button labeled "Diagnostics..." is present with the text "Collect diagnostic information for all installed components." above it. The main content area is titled "Secure Endpoint" and contains three tabs: "Statistics", "Update", and "Advanced". The "Statistics" tab is active, showing a scrollable list of system details. These details are organized into three sections: "Agent", "Policy", and "Detection Engine".

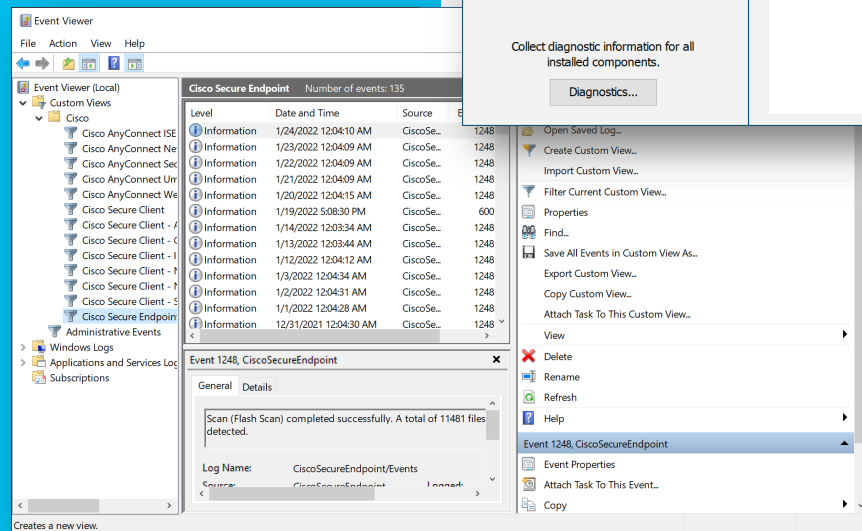
Agent	
Status	Connected
Version	8.0.1.20840
GUID	b2a7d93b-aac4-40a6-a0fe-06eac90f9677
Last Scan	Never
Isolation	Not Isolated

Policy	
Name	ATW-WindowsPolicy
Serial Number	409
Last Update	09/30/21 12:33:51 PM

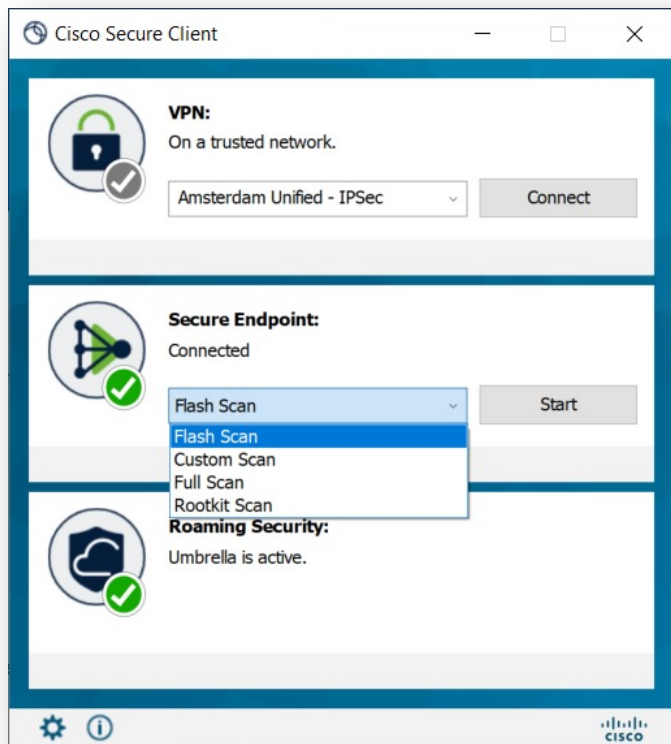
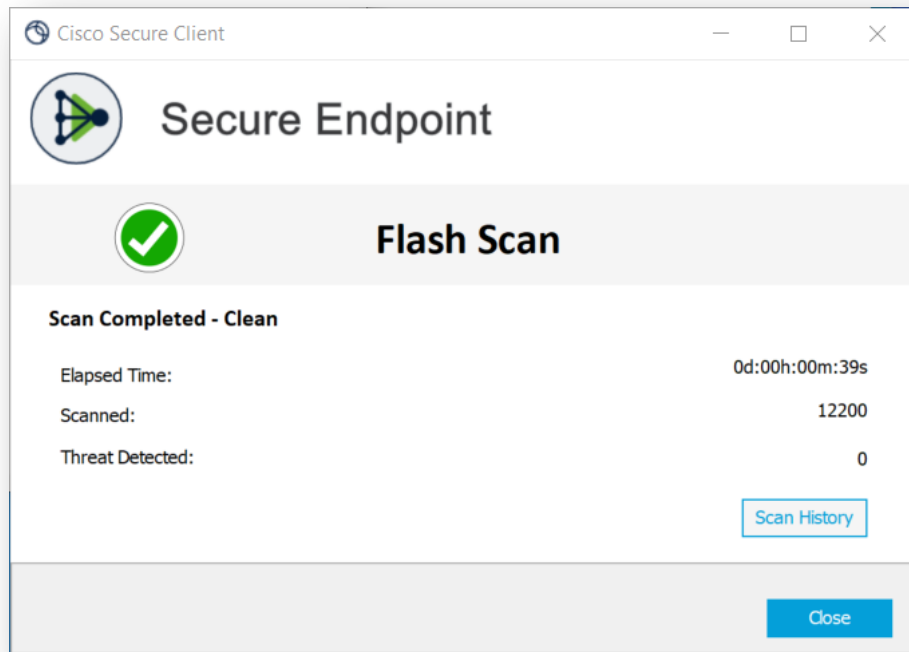
Detection Engine	
Name	Tetra
Version	87000
Last Update	Today 05:13:59 AM

Secure Endpoint Advanced

- Scan History moved to Advanced Tab

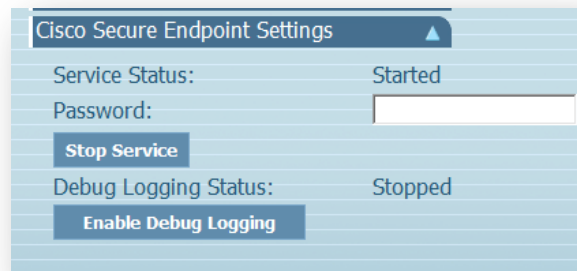
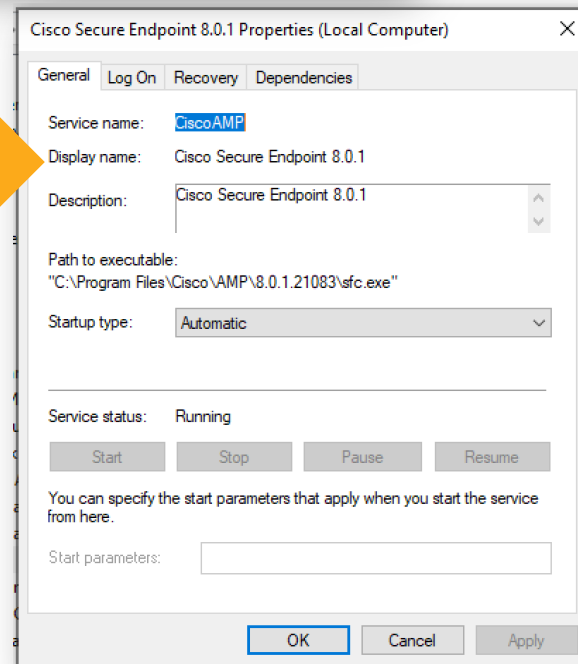


More Secure Endpoint UI



More Secure Endpoint UI

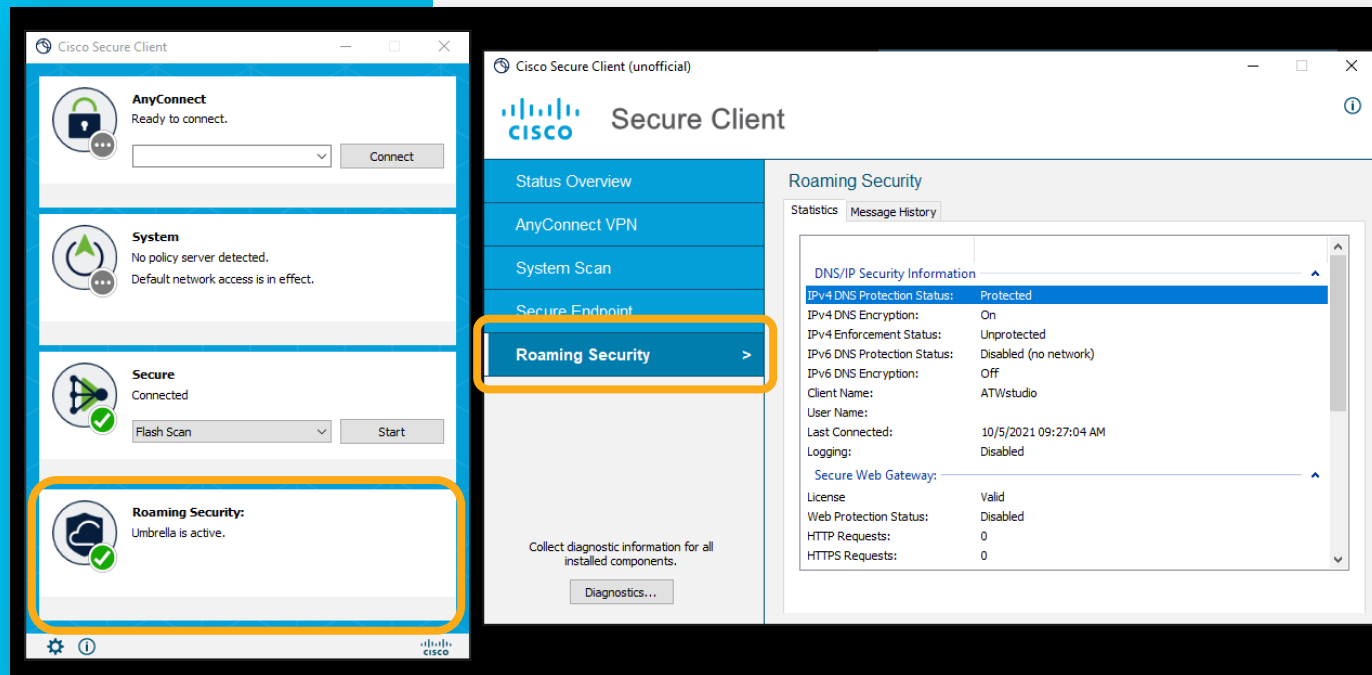
- Removed the ability to control the service from the UI when the connector is protected mode.
 - For security reasons
 - CLI only



Secure Umbrella

Same Umbrella
Roaming from
AnyConnect:

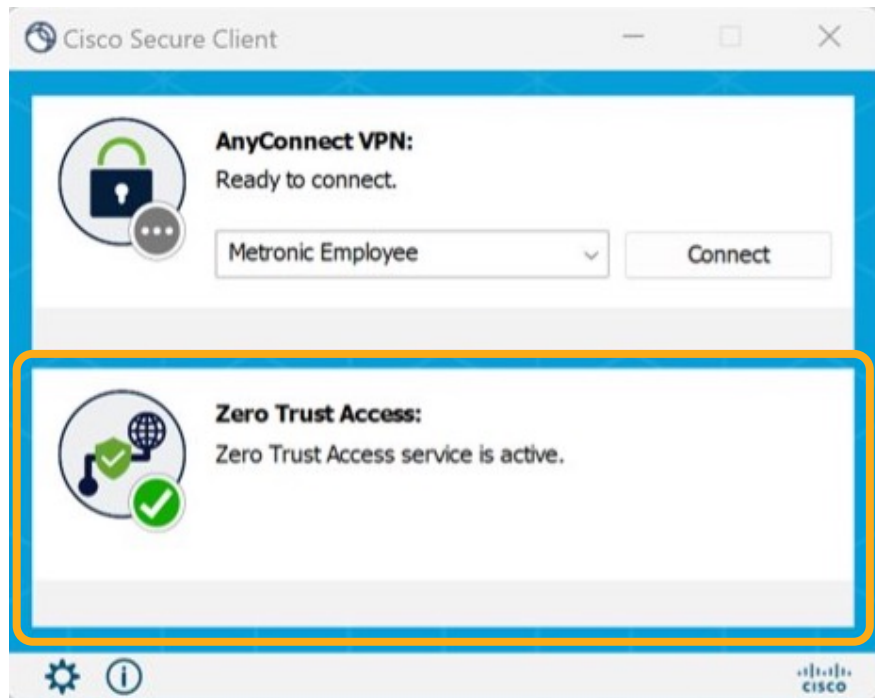
- Umbrella DNS
- Secure Web Gateway



ZTNA Module

For Cisco “Secure Access”

- Brand-New Module
- Dedicated for Cisco Secure Access
- Side-loads the Duo Health Agent (DHA)
- Uses MASQUE & QUIC for seamless transport



Putting it Simply

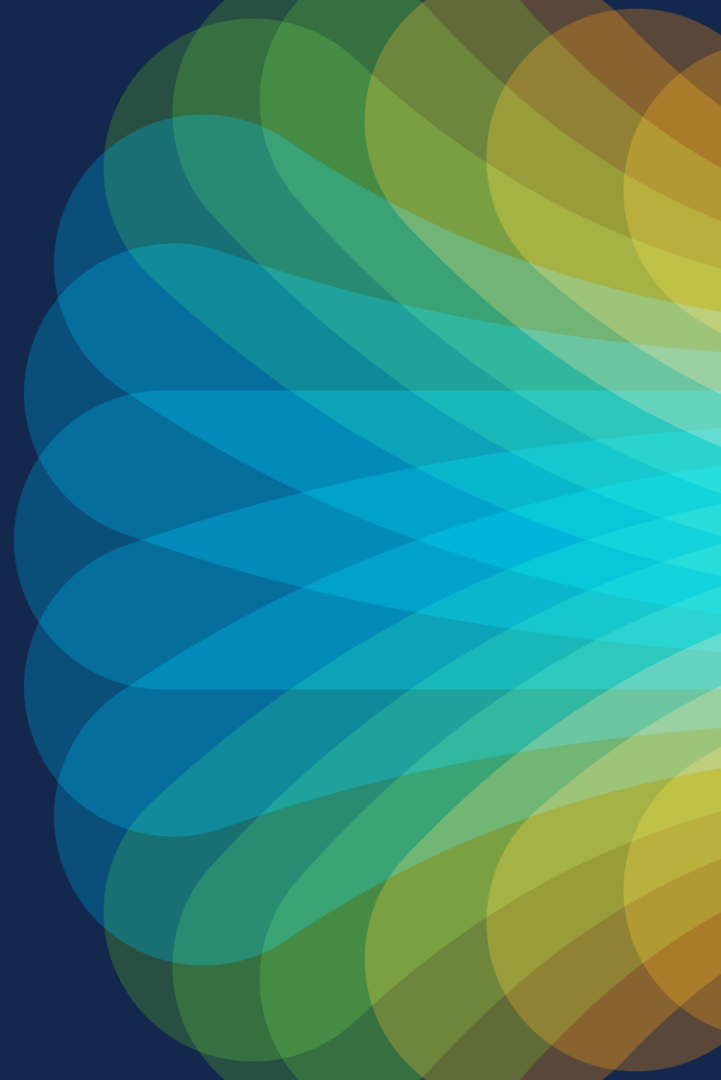
CSC = (rebranded)
AnyConnect 5.x

If you could do it in
AnyConnect 4.x, you can do it
in CSC 5.x



- Installed on headend's
- Not even using the cloud management
- Install just CORE + Umbrella
- It all works!!!

The Architecture



Agenda

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

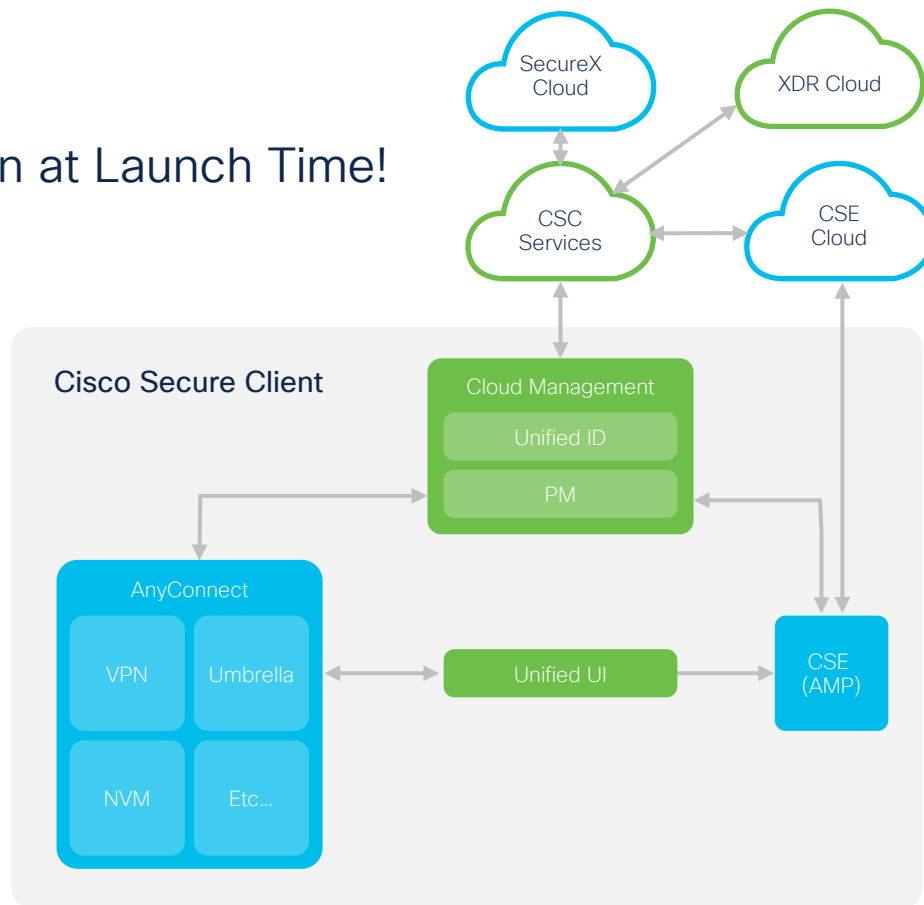
Cisco Secure Client

Architectural Overview – Yes, even at Launch Time!

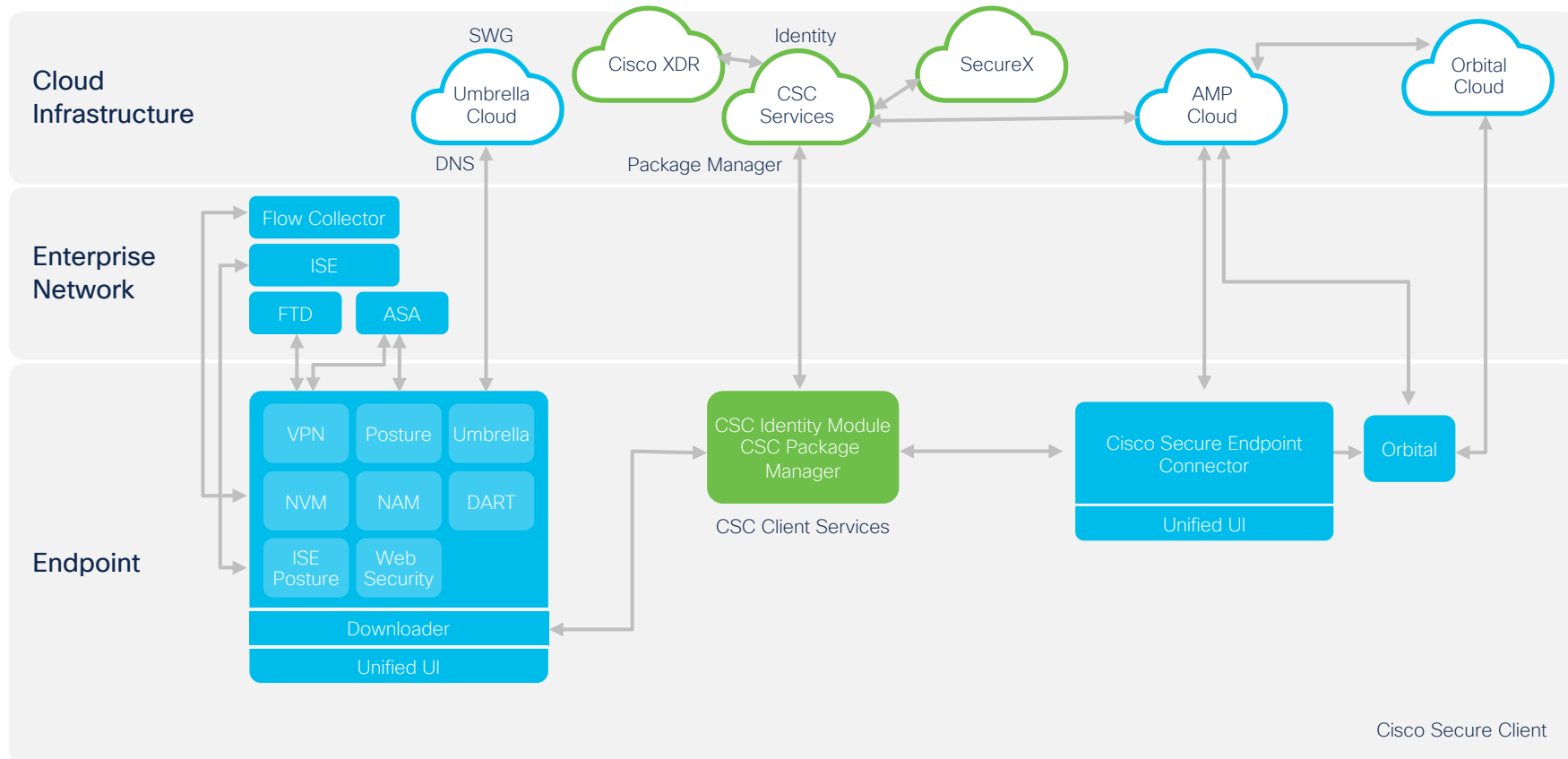
► Existing components that are not fundamentally changing

► New components

► Components that form the Cisco Secure Client

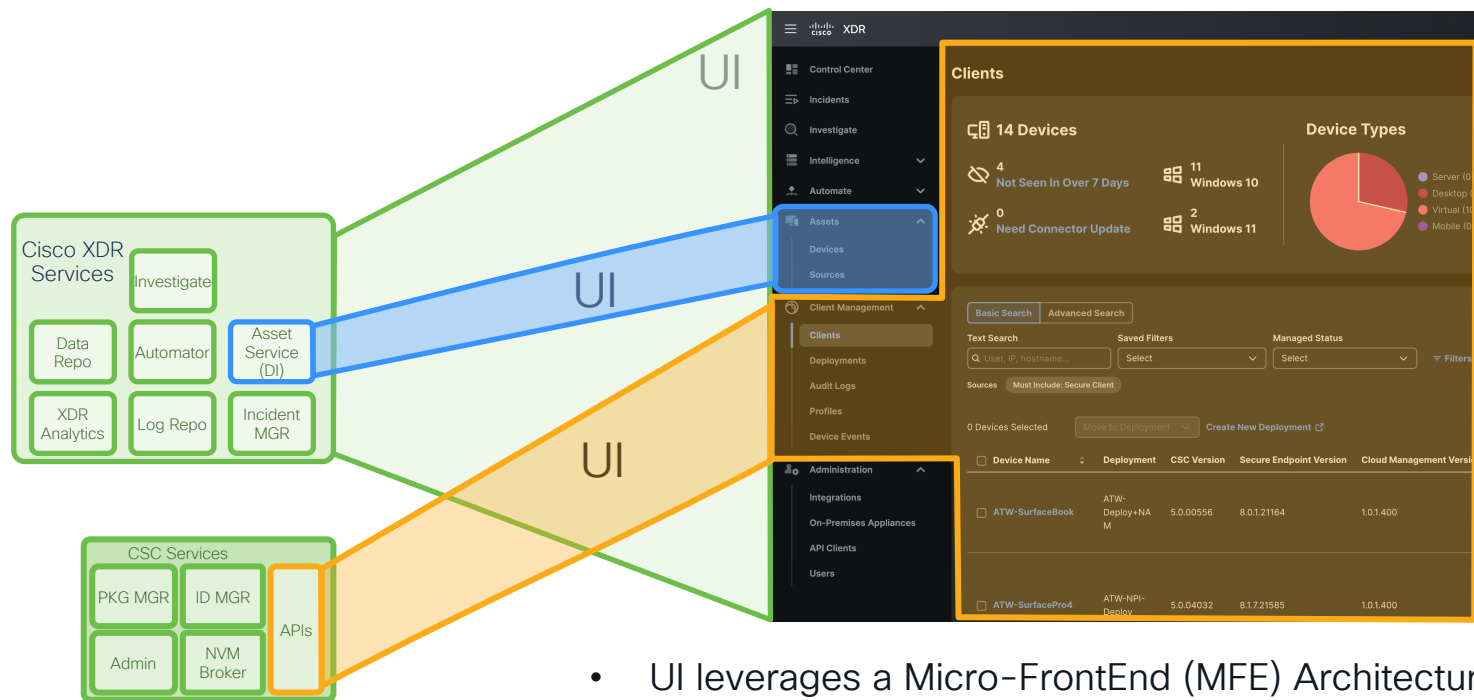


Cisco Secure Client – Architecture



Cisco Secure Client

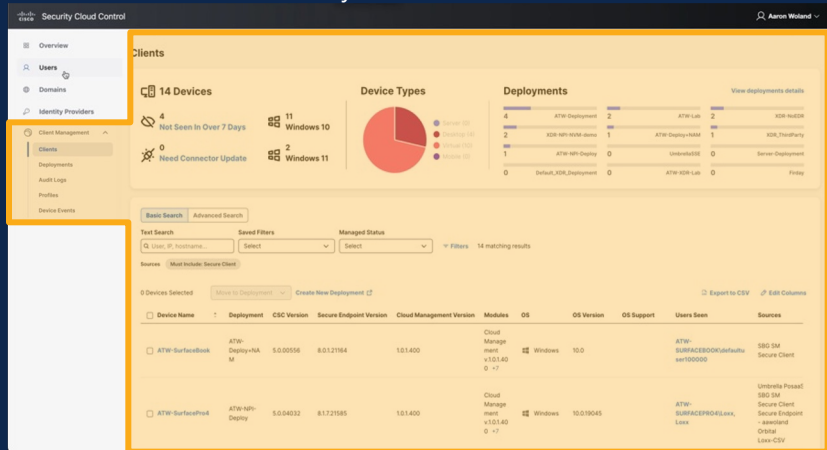
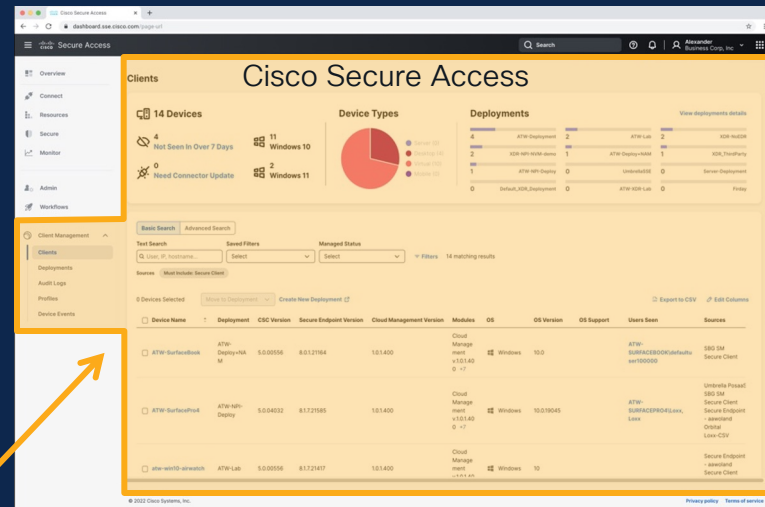
What Happens w/ CSC Management & XDR?



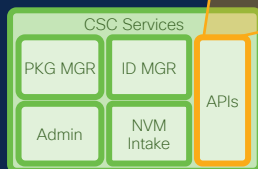
- UI leverages a Micro-FrontEnd (MFE) Architecture
- UI components may run from any service & be part of a single UI Experience

Micro Front End Illustrated

Security Cloud Control



Same UI from CSC Service

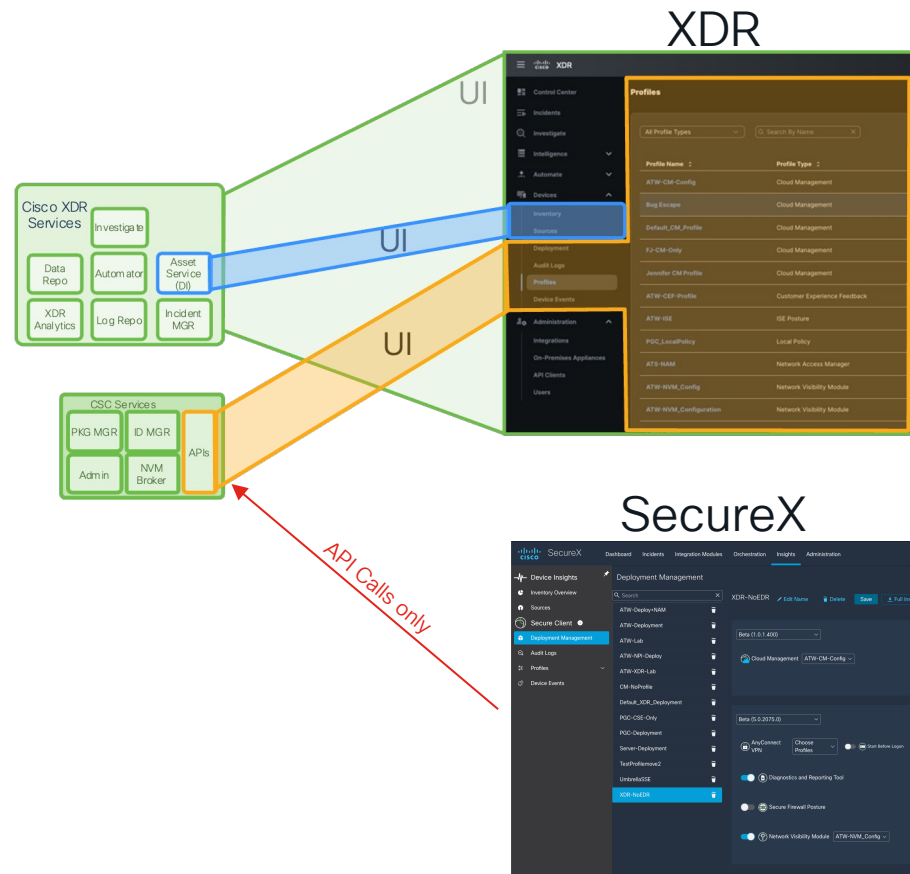


Common Services



CSC Management

- Still exists in SecureX
 - For non-XDR users
 - SSE Customers are redirected to SecureX / XDR for CSC Management today.
 - Micro-FrontEnd (MFE) UI Architecture will enable the CSC UI to be pulled into other front-ends in future.
 - Expected EoL – July 2024



CSC – SecureX

- The process to request a SecureX tenant be provisioned is.....

- Open a TAC Case
- Product: Cisco Secure Client
- Request a SecureX tenant be provisioned for Cloud Management of CSC

Deploying / Managing from Cloud

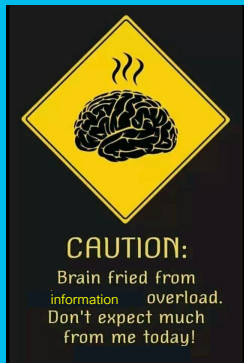
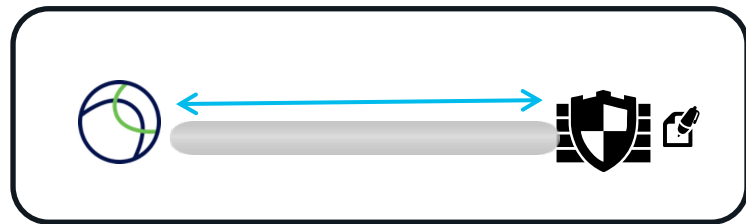
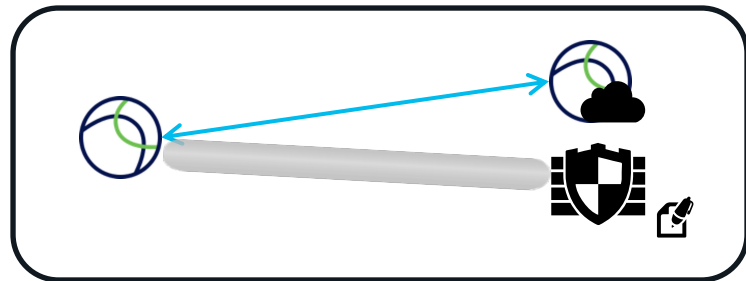
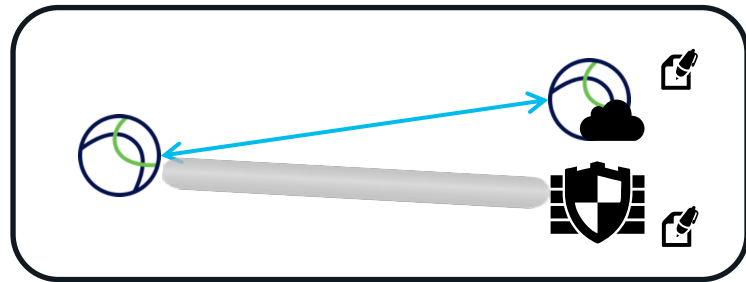


Agenda

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

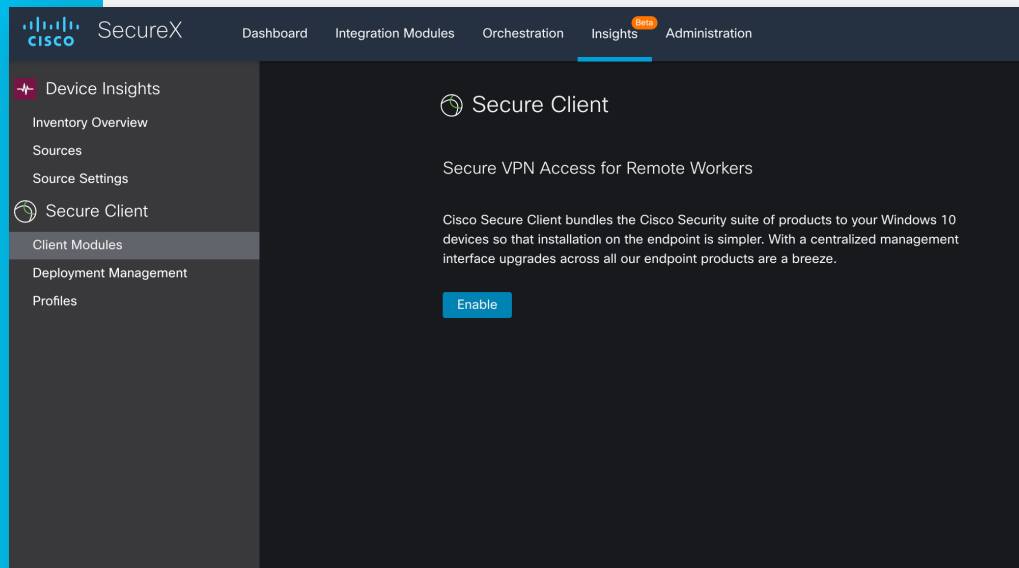
Deployment Models

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



Enable Secure Client

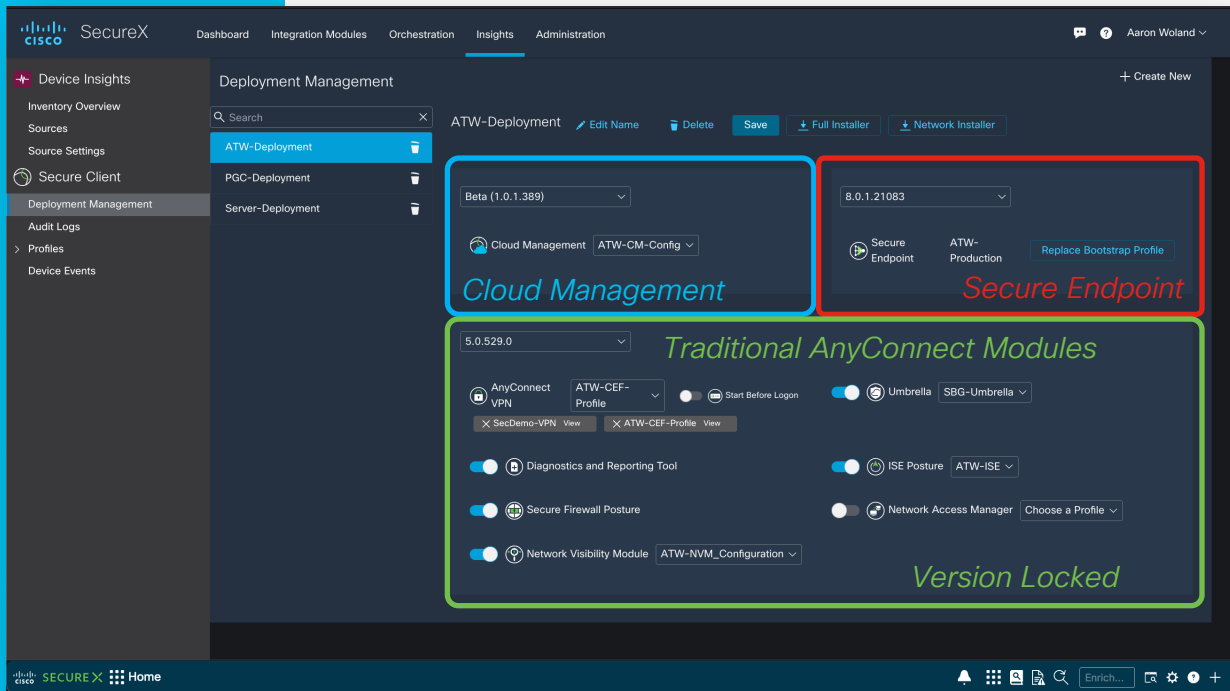
- Currently within Device Insights
 - Click **Enable**
 - This starts the process of spinning up your CSC Sub-system
- **Enabled by default in XDR



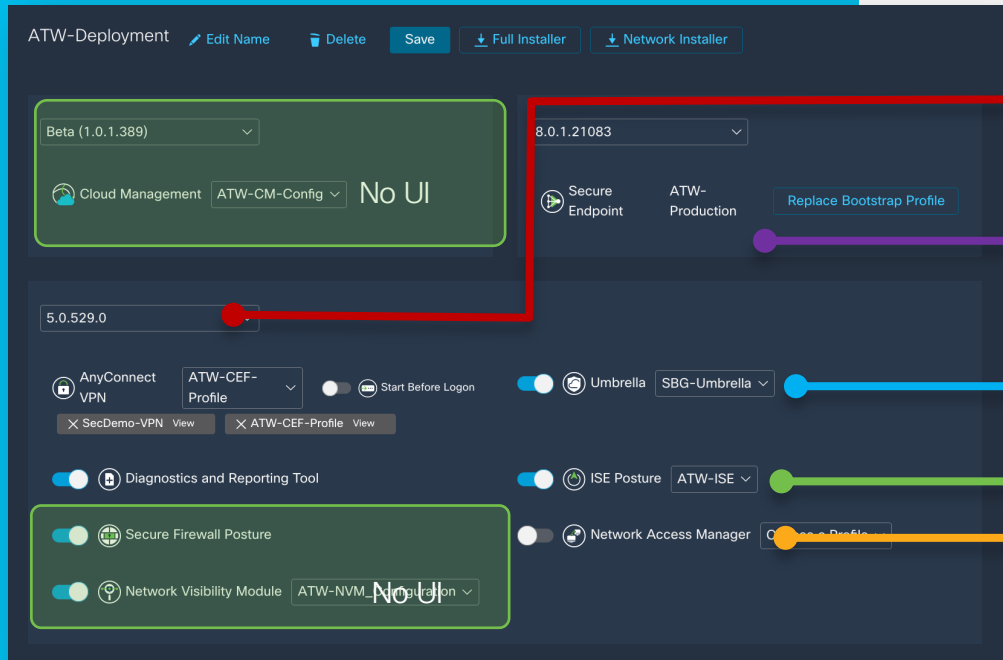
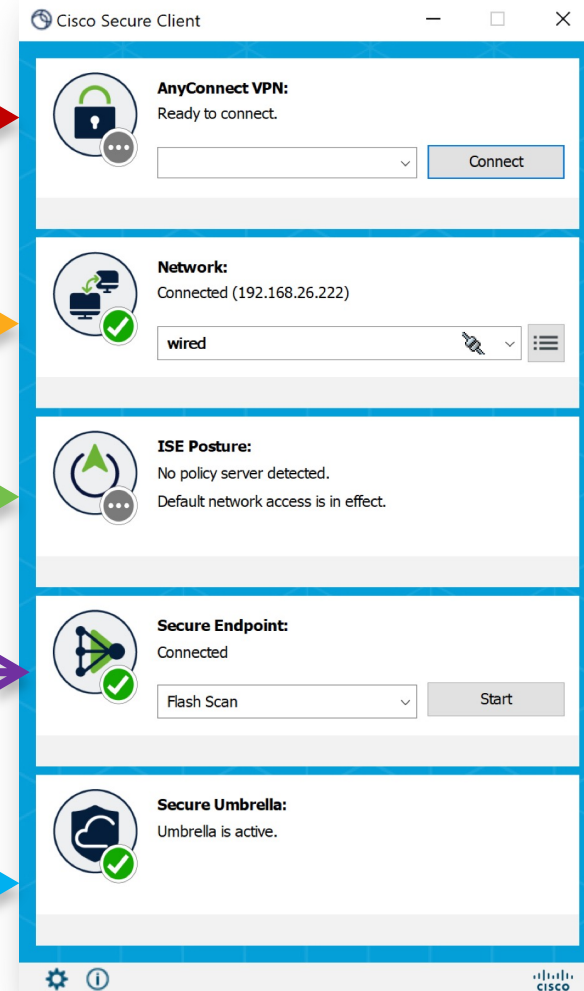
Managed from XDR or SecureX UI

Deployments

- Links endpoints to get specific modules + configs
- “Groups” are coming in future version & can assign entire groups to a Deployment
- Builds the installer dynamically



Managed from XDR or SecureX UI



Managed from XDR / SecureX UI

- Profiles

- Cloud Management (UC) module
- Includes package manager

- Check-in timer

- Update Window:

- *Also leveraged for Installation Window for Network Installer*

- 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

ATW CM Profile [Edit Name](#) [Delete](#) [Cancel](#) [Save As](#) [Save](#) [Download](#)

Identity Service Settings

☒ Enable Debug Logging

Package Manager Service Settings

Logging Level:

Check-in Interval:

☒ Notify User When Reboot Is Required

Cloud Management Service Settings

Logging Level:

Product Update Window

☒ Enable Product Update Window [Configure ^](#)

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

Day:

Start Time: Period:

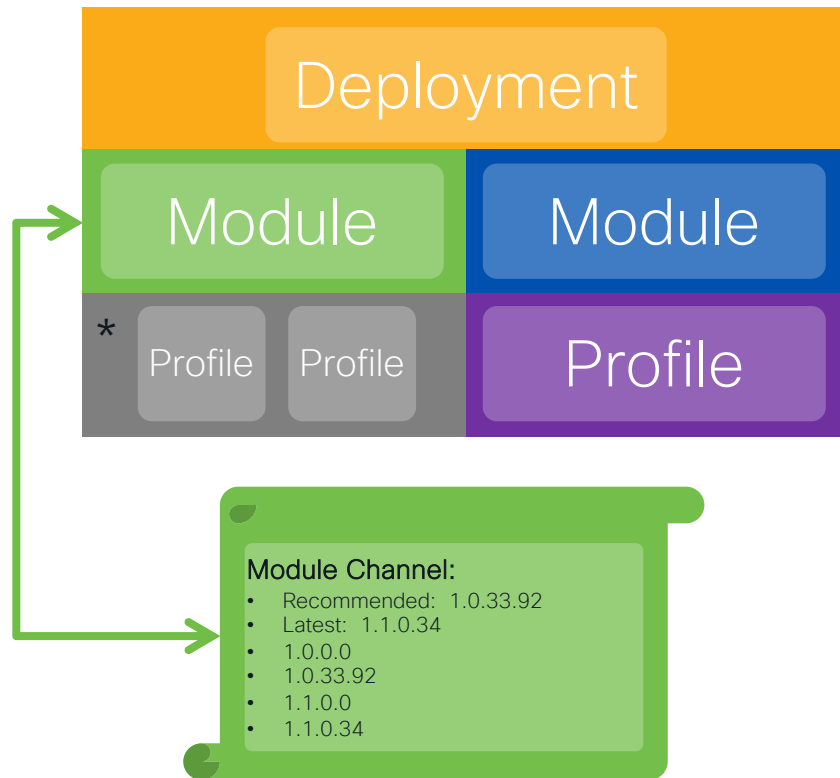
End Time: Period:

☐ Select Time Zone

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

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

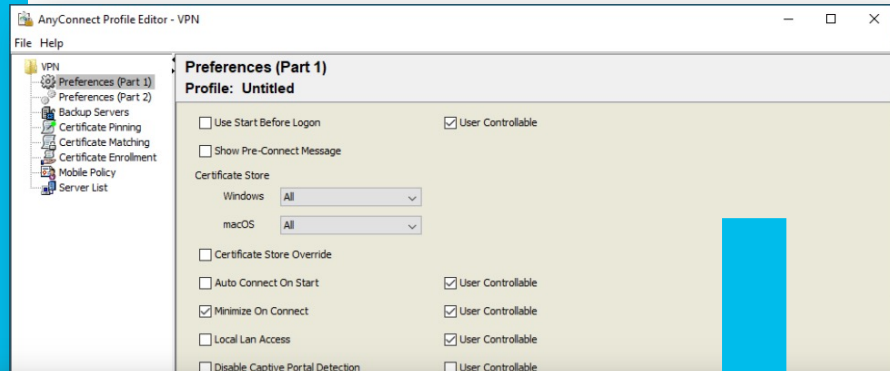
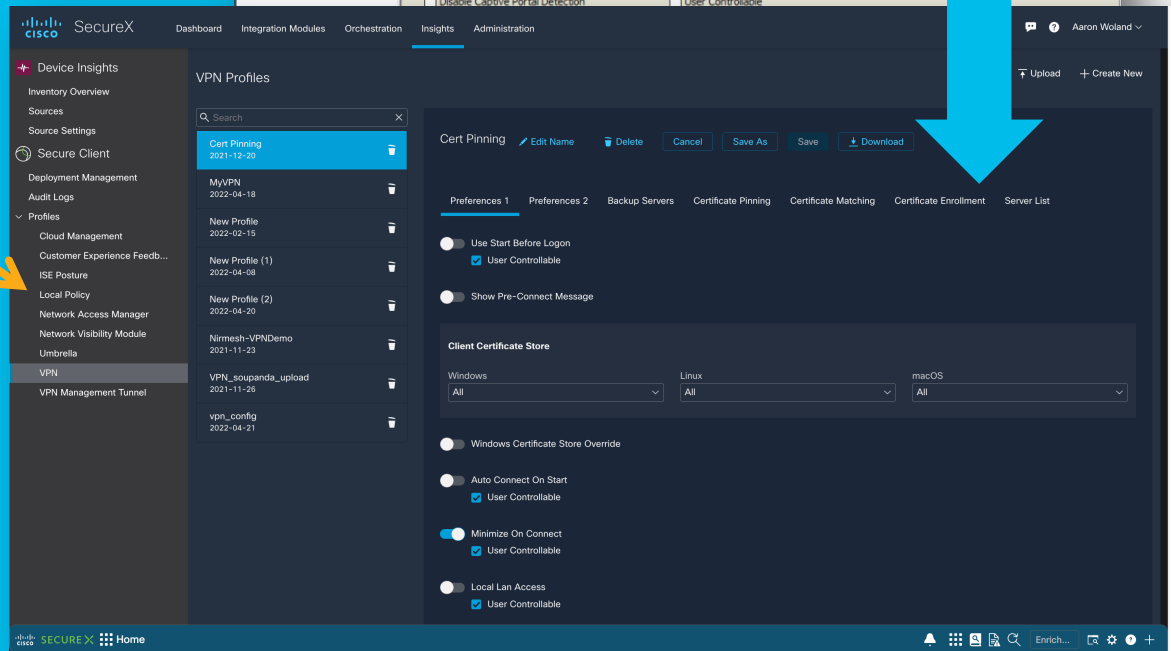


* When module supports >1

Managed from XDR / SecureX UI

- Profiles

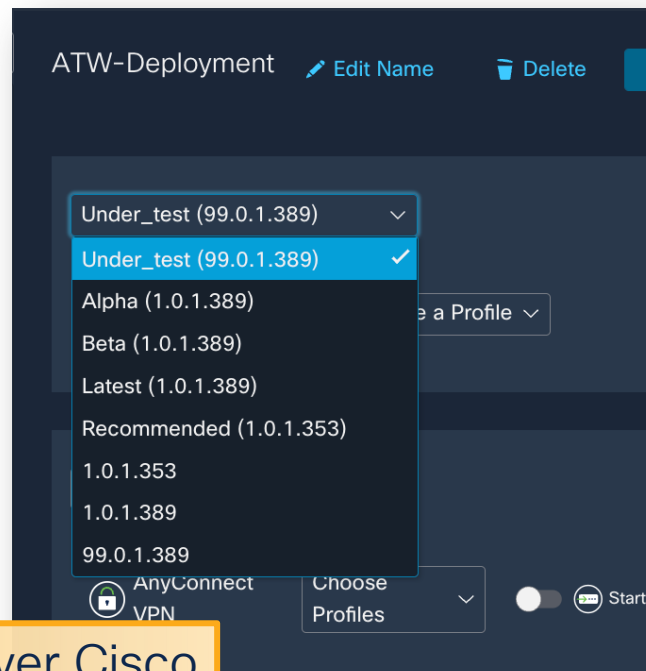
- Each module has a profile for its “configuration”
- Used to be standalone Windows-only configuration tool



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

Auto Upgraded whenever Cisco publishes a new version to channel

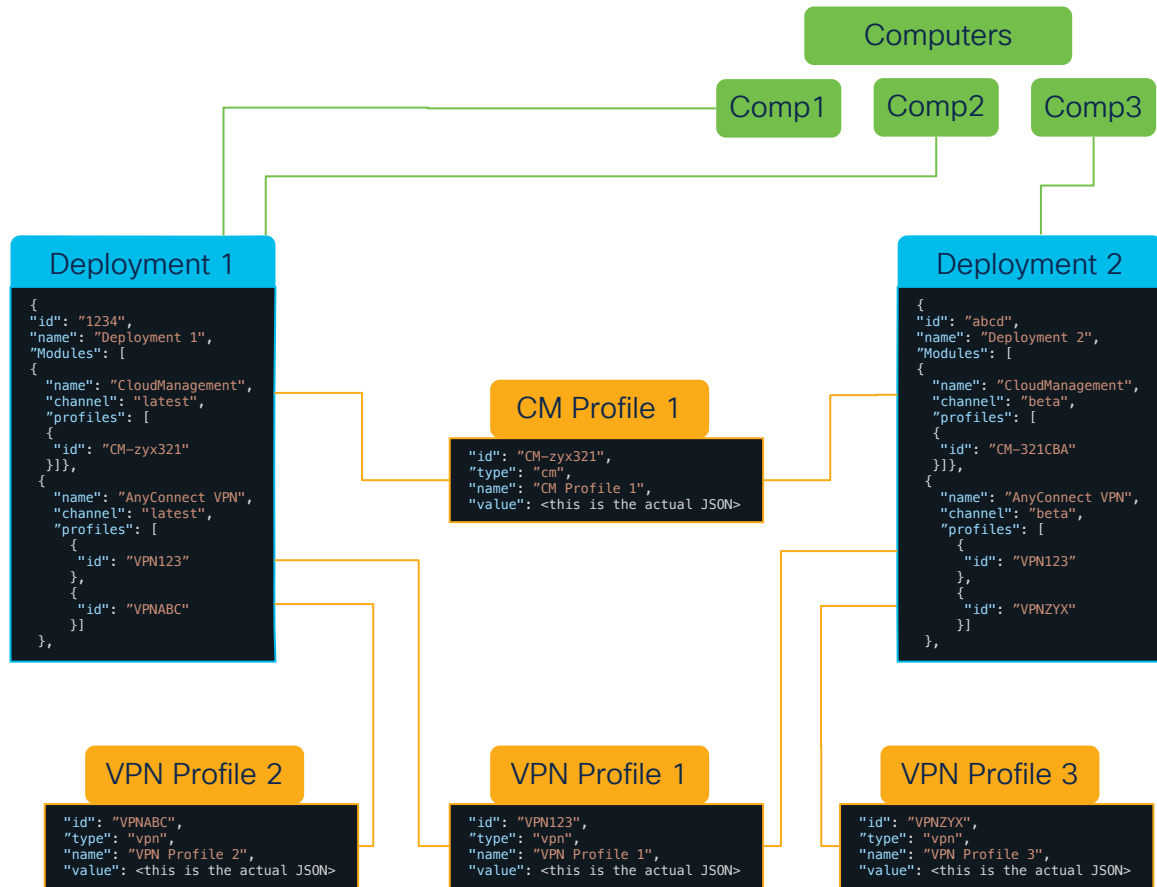


For CM and “AnyConnect” modules
SE module will use latest for bootstrap*

*SE upgrades handled by SE Cloud

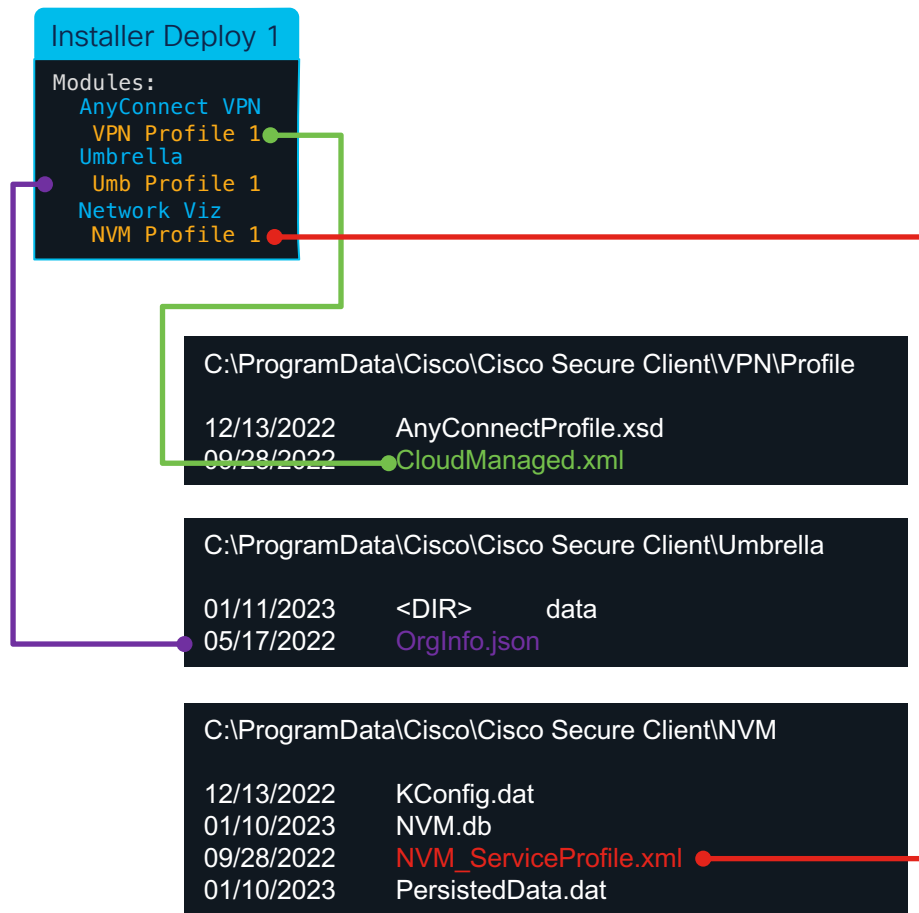
Deployment Hierarchy

- Computers assigned to 1 Deployment at a time!
- Deployment ties together:
 - Chosen Modules
 - Module Software Versions
 - Software “Channel” for updates / versions
 - Profiles (Module Configs)
 - Each Profile maybe in up to 11 Deployments (increasing in future)
- Installers are created dynamically based on the deployment



Installer from Deployment

- Contains packages for modules + profiles
- Places the profiles in the correct place
- Renames the profile from the friendly name in cloud management to the required name (if applicable)



Inventory of endpoints is part of Device Insights

- SxDI has a “mode” for CSC inventory management
- Changes Columns
- Changes Dashboard Elements
- Move devices between deployments, etc.

Device View: All Devices **Secure Client Devices**

5 Devices | 0/5 Devices Not Seen In Over 7 Days | 4 Devices Need Connector Update | 5 Windows 10 / 0 Windows 11 | 3 Deployments

Basic Search: Select Saved Filter | Switch to Advanced Search

Text Search: User, IP, hostname... | Managed Status: Select | Operating System: Select | OS Support: Select | Type: Select | Sources: 1 Selected | Policies: Select

Deployment Configurations: Select | ☐ Not Seen In Over 7 Days (0) | ☐ Need Connector Update (4) | ☐ Has Faults (0) | ☐ AV Definitions out of date (1) | Clear Filters | Save Filters

Must Include: Secure Client

5 Devices found | 0 Devices Selected | Move to Deployment | Move | Create New Deployment | Export to CSV | Edit Columns

Device Name	Deployment	CSC Version	Secure Endpoint Version	Cloud Management Version	Modules	OS	OS Version	OS Support	Users Seen	Sources	Managed	Compromised
C6385286146	PGC-Deployment	5.0.00117	8.0.1.20940	1.0.1.331	Cloud Management v.1.0.1.331 Cisco Secure Endpoint v.8.0.1.20940 AnyConnect VPN v.5.0.00117 DART v.5.0.00117	Windows	10 Pro			Secure Endpoint - Cisco - aawoland Orbital Secure Client	No	
lox-surfacepro	ATW-Deployment	5.0.00117	8.0.1.20940	1.0.1.353	Cloud Management v.1.0.1.353 Cisco Secure Endpoint v.8.0.1.20940 AnyConnect VPN v.5.0.00117 Umbrella v.5.0.00117 DART v.5.0.00117 ISE Posture v.5.0.00117 Secure Firewall Posture v.5.0.00117 Network Visibility Module v.5.0.00117 Cloud Management v.1.0.1.389	Windows	10.0	lox, lox-surfacepro/Aaron, lox@securitydemo.net, Aaron, eden, nyah	Umbrella PosaaS SBC SM Dao Secure Endpoint - Cisco - aawoland Orbital Secure Client	Yes		

Moving Deployments – Admin Only

Device View | All Devices | **Secure Client Devices** | **Admin**

7 Devices

0/7
Devices Not Seen
In Over 7 Days

0
Devices Need
Connector Update

Basic Search | Select Saved Filter | Switch to Advanced Search

Text Search: User, IP, hostname... | Managed Status: Select | Operating System: Select

Policies: Select | Deployment Configurations: Select | ☐ Not Seen In Over 7 Days (0)

Must Include: Secure Client

7 Devices found | 0 Devices Selected | Move to Deployment | Move | Create New Deployment

☐ Device Name ↑	Deployment	CSC Version	Secure Endpoint Version	Cloud
☐ ATW-SURFACEPRO4	ATW-Deployment	5.0.00529	8.0.1.21083	1.0.1.3

Device View | All Devices | **Secure Client Devices** | **Non-Admin**

7 Devices

0/7
Devices Not Seen
In Over 7 Days

0
Devices Need
Connector Update

Basic Search | Select Saved Filter | Switch to Advanced Search

Text Search: User, IP, hostname... | Managed Status: Select | Operating System: Select

Policies: Select | Deployment Configurations: Select | ☐ Not Seen In Over 7 Days (0)

Must Include: Secure Client

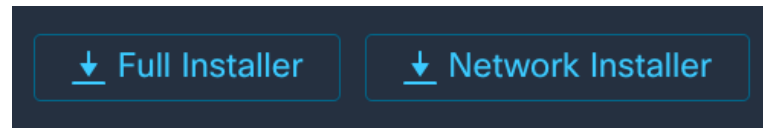
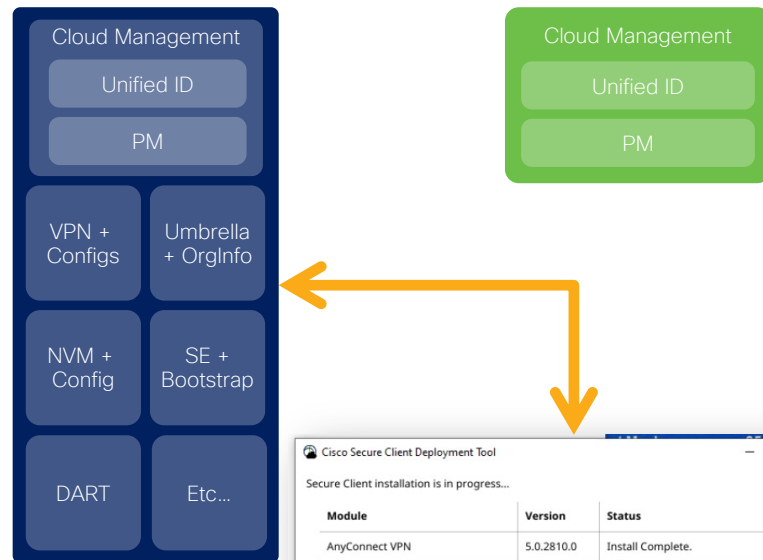
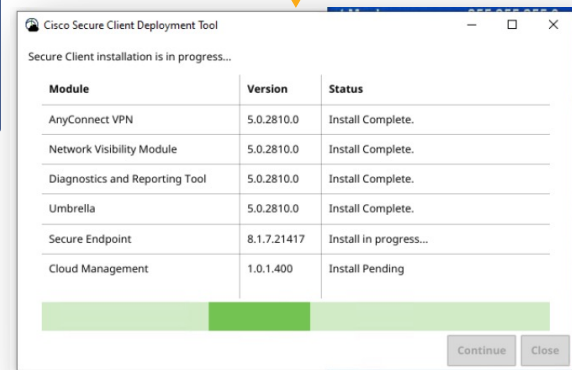
7 Devices found

Device Name ↑	Deployment	CSC Version	Secure Endpoint Version	Cloud
ATW-SURFACEPRO4	ATW-Deployment	5.0.00529	8.0.1.21083	1.0

Installing

Installing CSC

- Full Installer:
 - All selected Modules & their configurations.
- Network Installer:
 - Installs Cloud Management first, then PM pulls the manifest from deployment and installs each module and configuration one at a time.



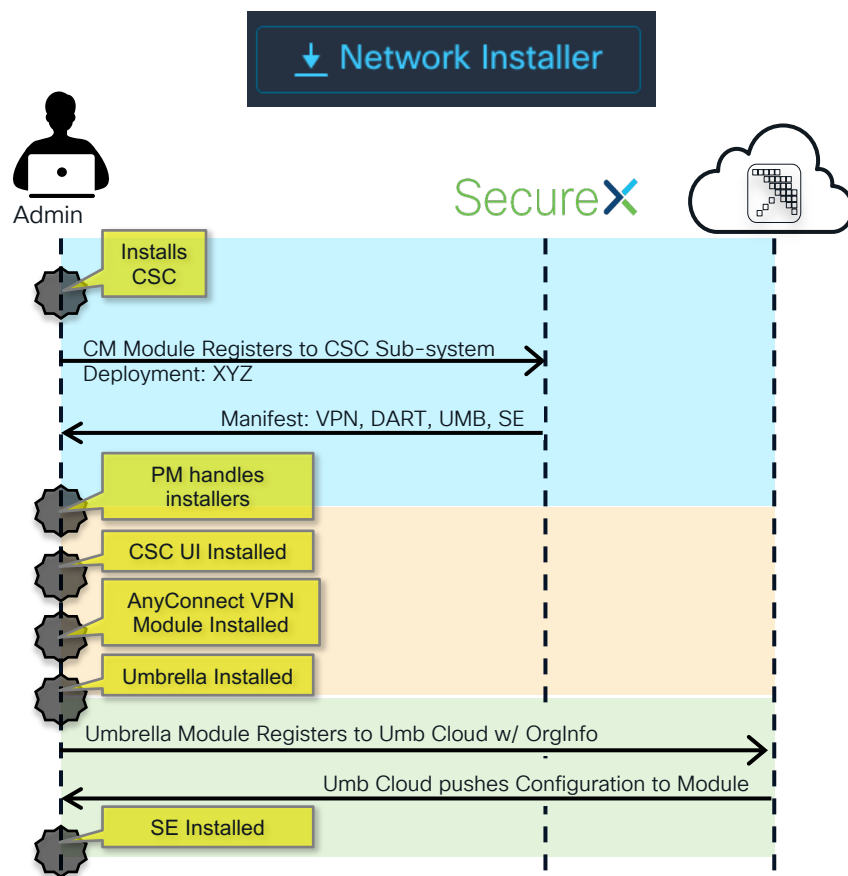
The screenshot shows the 'Cisco Secure Client Deployment Tool' window. The title bar reads 'Cisco Secure Client Deployment Tool'. The main text says 'Secure Client installation is in progress...'. Below this is a table with three columns: 'Module', 'Version', and 'Status'. The table lists the following modules and their installation status:

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

At the bottom right of the window are 'Continue' and 'Close' buttons.

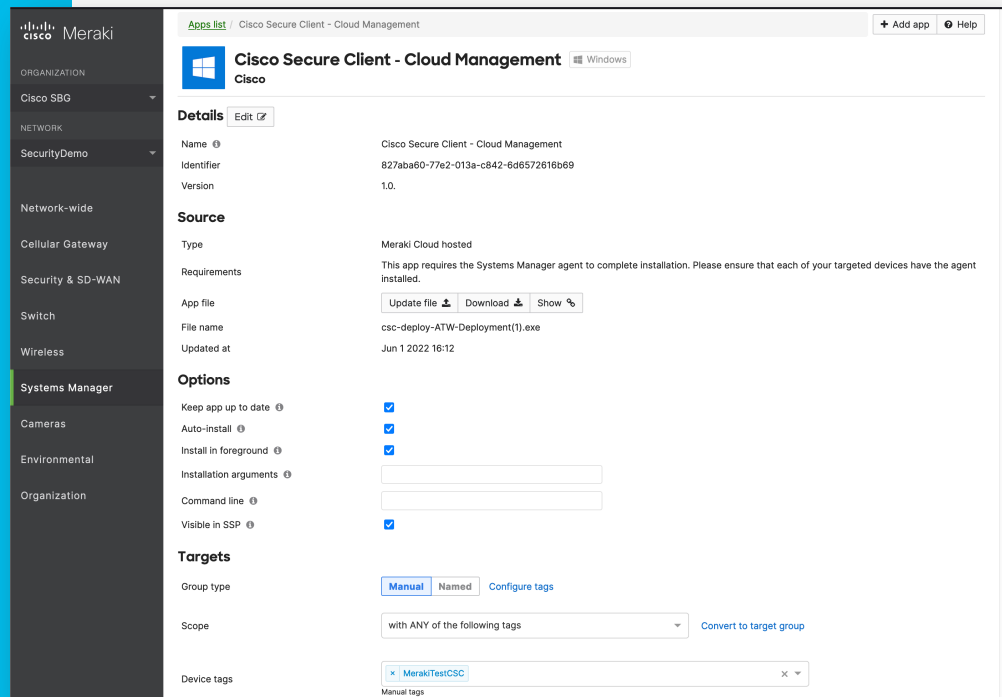
Network Installer

- Lightweight installer
- Installs the Cloud Management Module with its config only
- After CM registers to SecureX, the Manifest directs the rest of the installations with their configs



Installing CSC

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



Deployments w/ Secure Endpoint and Orbital



Configuring Secure Endpoint

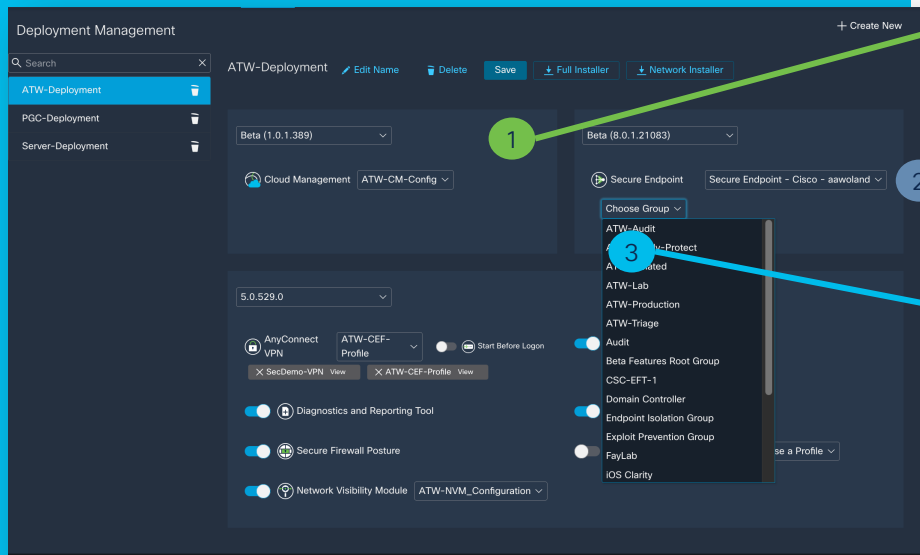
Select Desired SE Version

Select your SE Integration

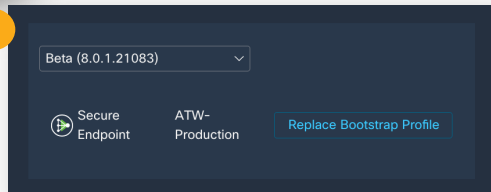
There *can* be more than one

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.

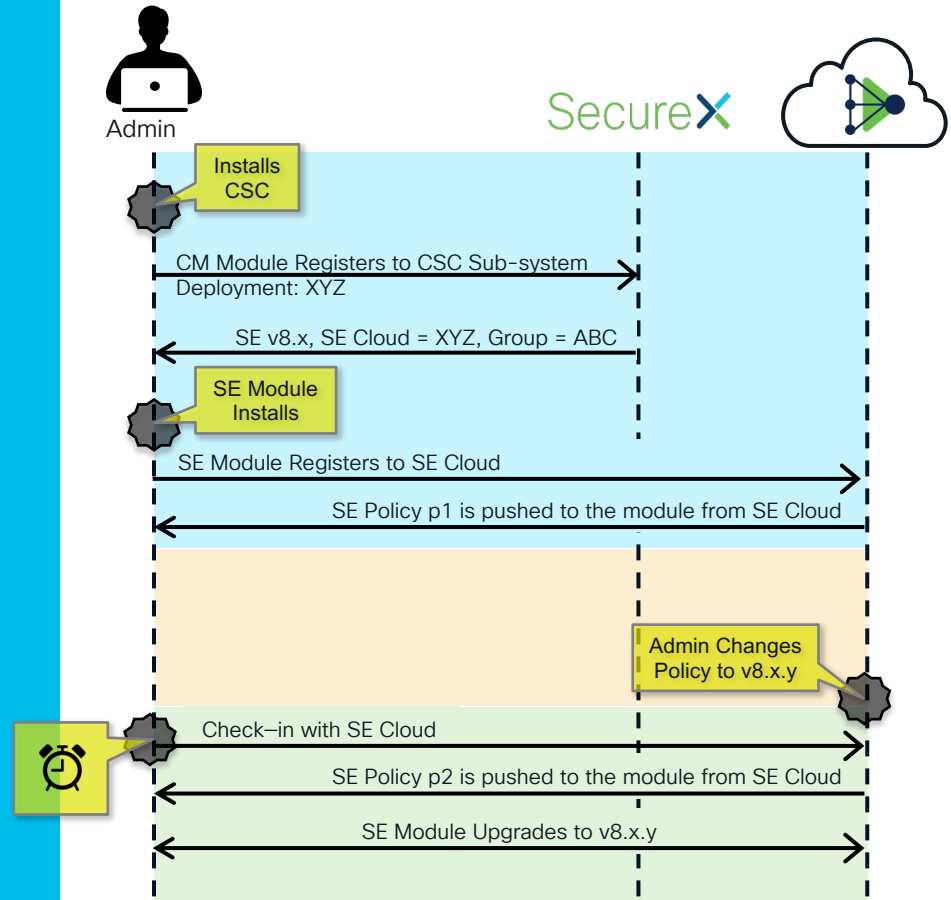


The bootstrap file configures new installs of SE to join that Secure Endpoint tenant and that group



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...
- SecureX can still update software versions through deployment.



SE Version Updates

Highest Version Wins!

ATW-Deployment [Edit Name](#) [Delete](#) [Save](#) [Full Installer](#) [Network Installer](#) **SECURE X**

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 Login](#) [Umbrella](#) [SBG-Umbrella](#)

Latest (8.1.3.21242) [Secure Endpoint](#) Group: ATW-Production [Replace Bootstrap Profile](#)

Edit Policy [Windows](#)

Name: ATW-Production

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

Modes and Engines

Exclusions: 41 exclusion sets

Proxy

Outbreak Control

Device Control

Product Updates

Advanced Settings

Deprecated Settings

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

Product Version: 8.0.1.21164 [Details](#)
1 of 30 computers must reboot.

Update Server: upgrades.amp.cisco.com

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

Update Interval: 144 hours

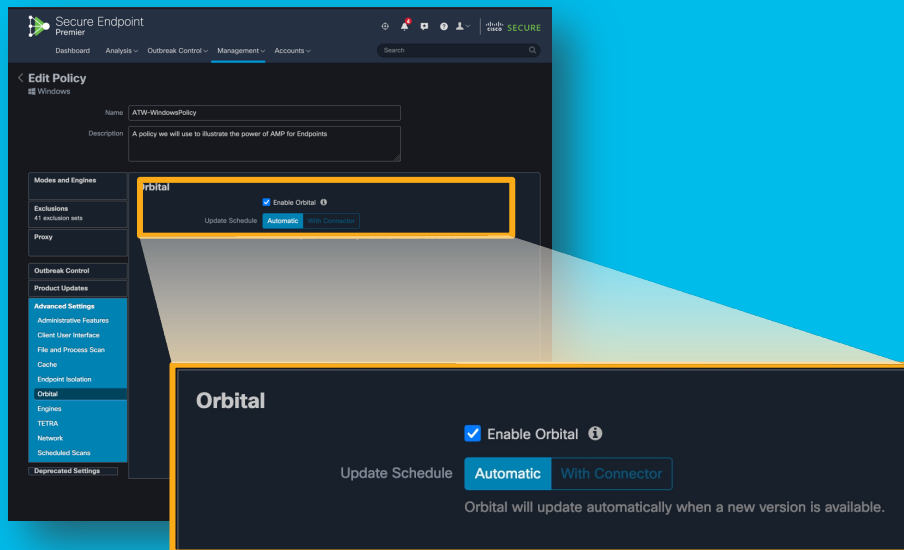
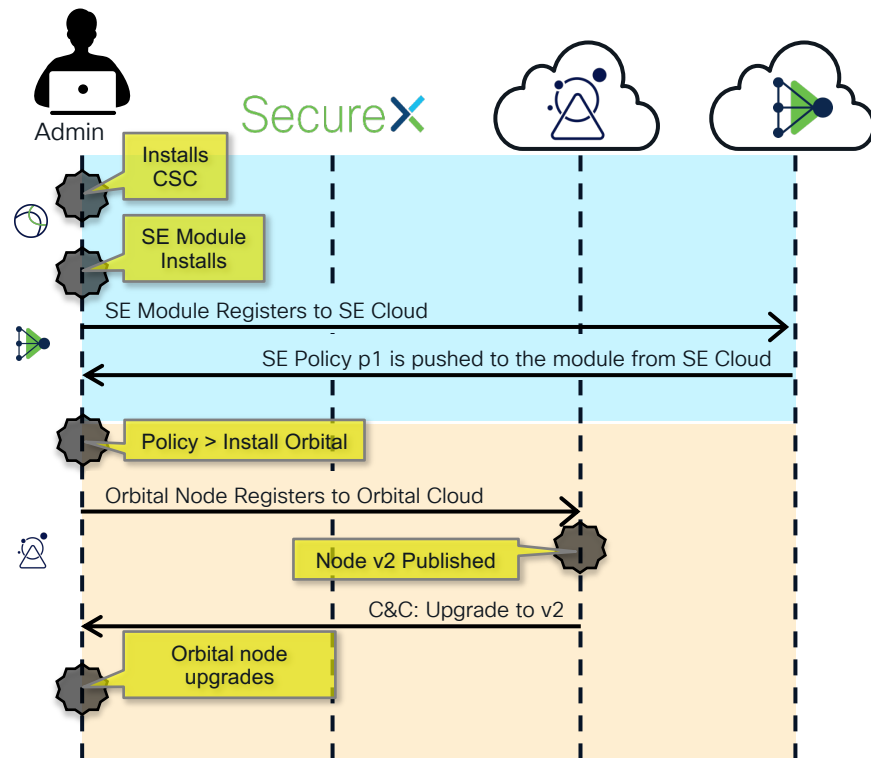
☐ Block Update if Reboot Required

Cancel Save

Product Version: 8.0.1.21164 [Details](#)
1 of 30 computers must reboot.

Deploying Orbital

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





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.

Upgrading

Agenda

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

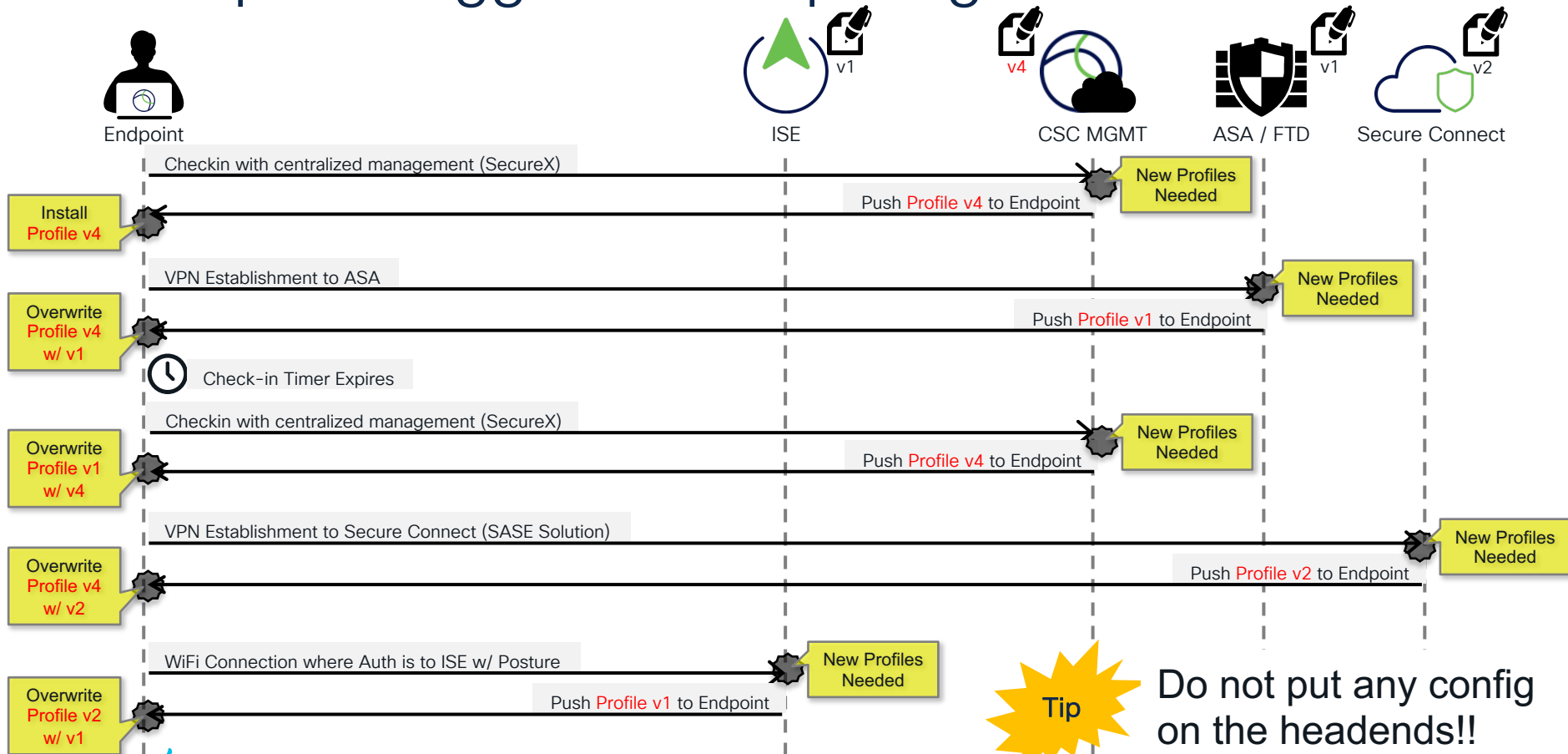
Upgrading

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

AnyConnect Upgrades

- Through the upgrade to secure client, AnyConnect customers would not just have cloud management
- But also full access to SecureX and hence also device insights.

The Epic Struggle of Competing Control Points

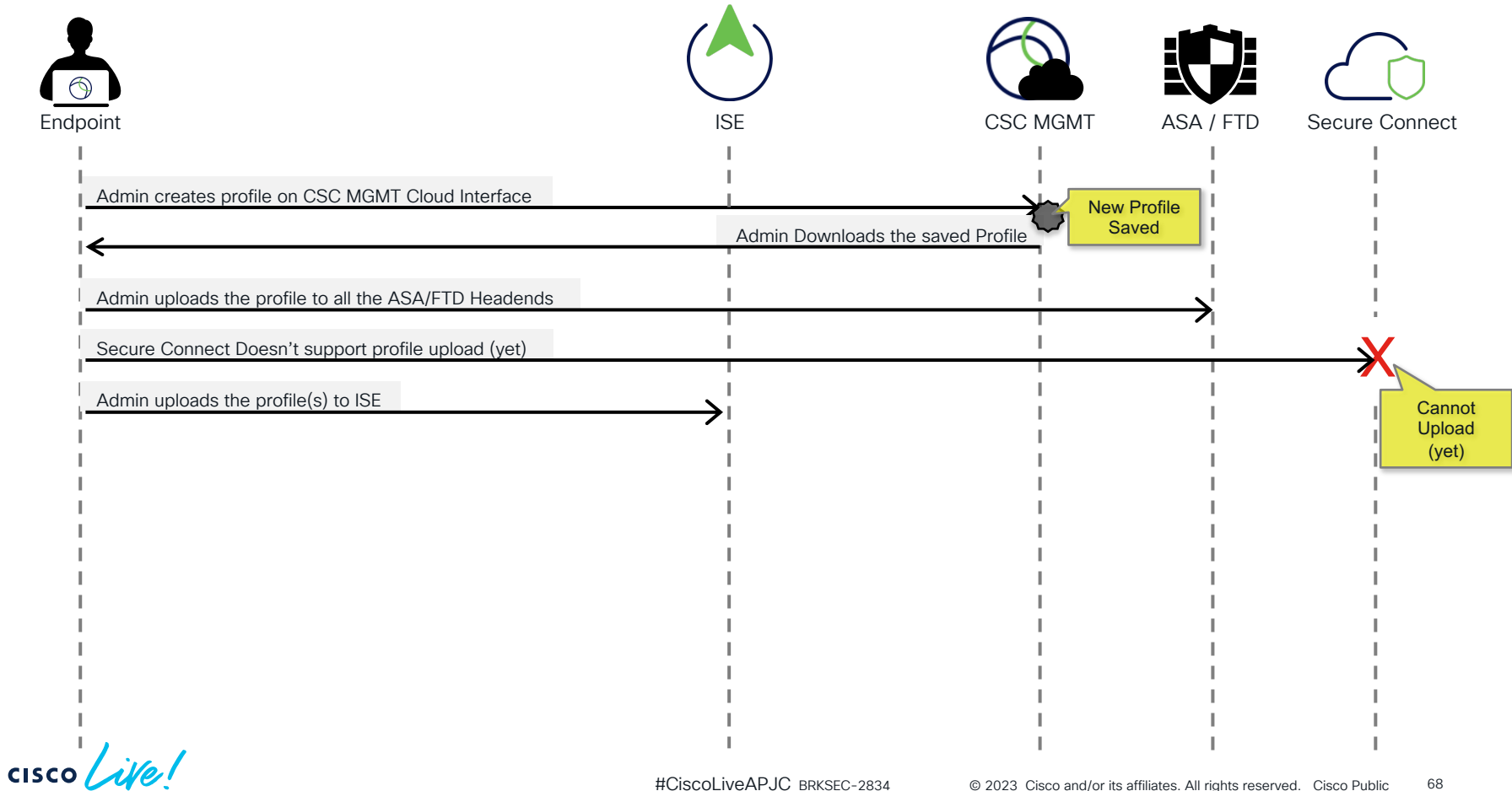


Details on Profile Merges

- Recommendation: load the SecureX Profile immediately on the ASA with same Filename
- Or: Do not put any config on the headends!!

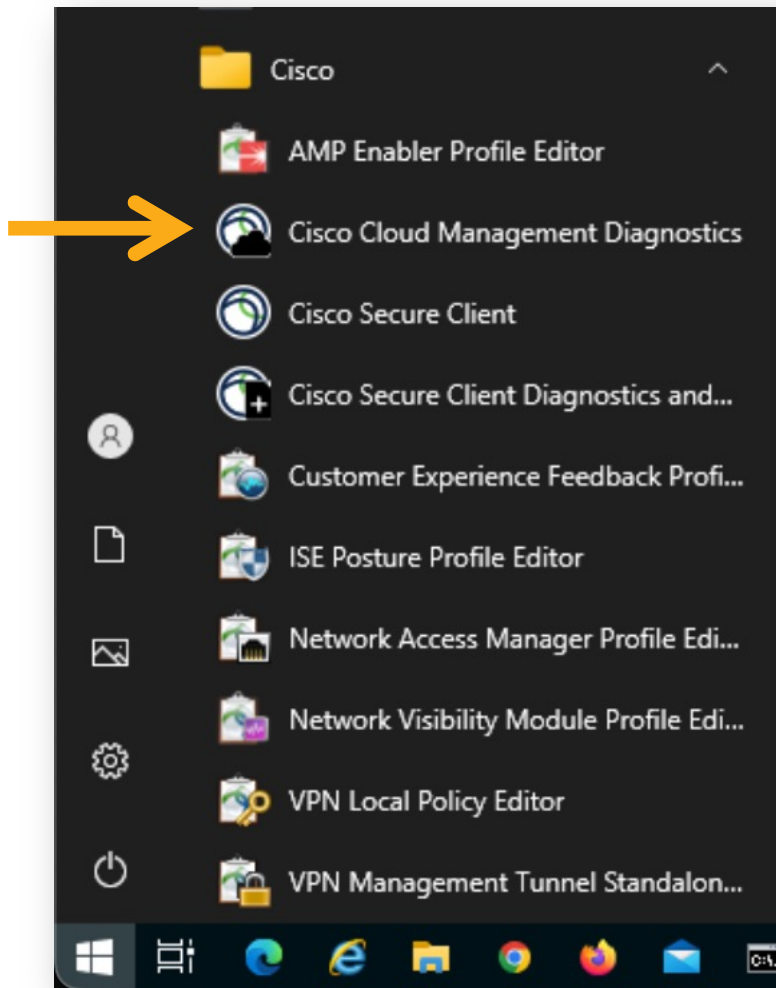
- If filenames match: ASA will overwrite the profile
- If filenames don't match: both profiles will be detected by VPN and behavior might be a little wonky... Some settings get merged from all detected profiles

Download and Push to Head-ends



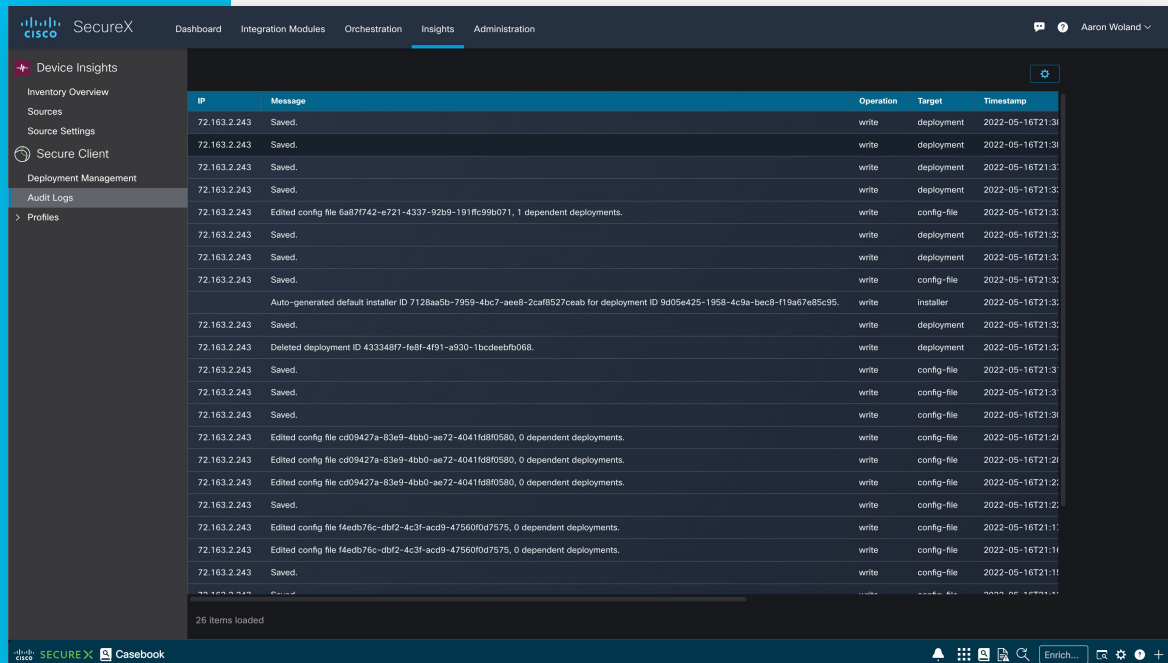
DART & CM Diagnostics

- *“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?



Placeholder: Audit Logging

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



The screenshot displays the Cisco SecureX Audit Logs interface. The left sidebar contains navigation options: Device Insights, Inventory Overview, Sources, Source Settings, Secure Client, Deployment Management, Audit Logs (selected), and Profiles. The main content area shows a table of audit events with columns for IP, Message, Operation, Target, and Timestamp. The table lists various system actions such as saving configurations, editing config files, deleting deployments, and writing config files, all with timestamps from May 16, 2022. At the bottom, it indicates '26 items loaded'.

IP	Message	Operation	Target	Timestamp
72.163.2.243	Saved.	write	deployment	2022-05-16T21:31
72.163.2.243	Saved.	write	deployment	2022-05-16T21:31
72.163.2.243	Saved.	write	deployment	2022-05-16T21:31
72.163.2.243	Saved.	write	deployment	2022-05-16T21:31
72.163.2.243	Edited config file 6a87f742-e721-4337-92b9-191fc99b071, 1 dependent deployments.	write	config-file	2022-05-16T21:31
72.163.2.243	Saved.	write	deployment	2022-05-16T21:31
72.163.2.243	Saved.	write	deployment	2022-05-16T21:31
72.163.2.243	Saved.	write	config-file	2022-05-16T21:31
	Auto-generated default installer ID 712baa5b-7959-4bc7-ae68-2caf6527ceab for deployment ID 9d05e425-1958-4c9a-bec8-f19a67e85c95.	write	installer	2022-05-16T21:31
72.163.2.243	Saved.	write	deployment	2022-05-16T21:31
72.163.2.243	Deleted deployment ID 433348b7-fe8f-4f91-a930-1bcdeebf068.	write	deployment	2022-05-16T21:31
72.163.2.243	Saved.	write	config-file	2022-05-16T21:31
72.163.2.243	Saved.	write	config-file	2022-05-16T21:31
72.163.2.243	Saved.	write	config-file	2022-05-16T21:31
72.163.2.243	Edited config file cd09427a-83e9-4bb0-ae72-4041f68f0580, 0 dependent deployments.	write	config-file	2022-05-16T21:21
72.163.2.243	Edited config file cd09427a-83e9-4bb0-ae72-4041f68f0580, 0 dependent deployments.	write	config-file	2022-05-16T21:21
72.163.2.243	Edited config file cd09427a-83e9-4bb0-ae72-4041f68f0580, 0 dependent deployments.	write	config-file	2022-05-16T21:21
72.163.2.243	Saved.	write	config-file	2022-05-16T21:21
72.163.2.243	Edited config file f4edb76c-dbf2-4c3f-acd9-47560fd07575, 0 dependent deployments.	write	config-file	2022-05-16T21:11
72.163.2.243	Edited config file f4edb76c-dbf2-4c3f-acd9-47560fd07575, 0 dependent deployments.	write	config-file	2022-05-16T21:11
72.163.2.243	Saved.	write	config-file	2022-05-16T21:11

Cloud Event Logging

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

The screenshot displays the Cisco Cloud Event Logging interface with three highlighted steps:

- Step 1: Select the Computer**: A search bar labeled "Search For Device" with a dropdown arrow and a search button. The "Device Selected" field shows "09a43288-ebc7-467c-a1ed-bb8c-1b2b-1b2b-1b2b".
- Step 2: (optional) Enter Time Range**: A "Filter by Dates" dropdown menu and an "Apply Filter" button.
- Step 3: Expand the Event**: A table with columns "Event Time", "Timestamp", and "IP Address". The first row is expanded, showing a JSON event log entry.

The expanded event log entry shows:

```
{
  "data": {
    "new": [
      {
        "type": "pkg-reconfig"
      }
    ],
    "old": [
      {
        "type": "pkg-reconfig"
      }
    ]
  },
  "package": "AMD/8.0.1.21083",
  "tsrx": "2022-06-08T16:55:31.050840692",
  "tstxn": "2022-06-08T16:55:31.05071752",
  "type": "pkg-reconfig"
}
```

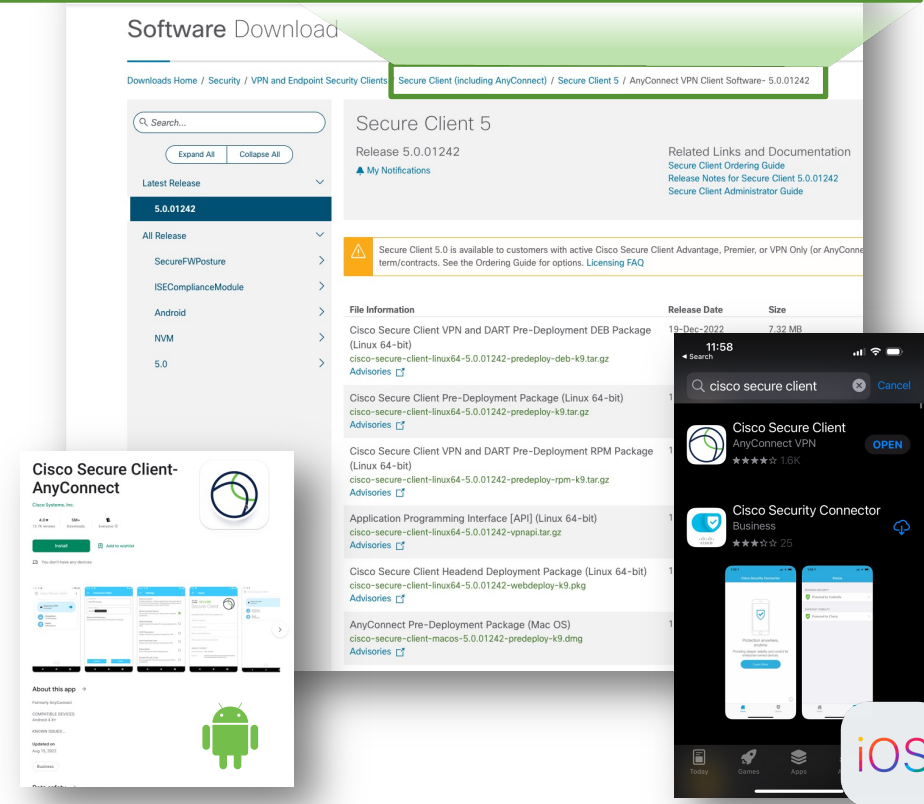
Event Time	Timestamp	IP Address
2022-06-08T16:55:31.06-05:00	2022-06-08T16:55:31.16-05:00	70.60.206.37
2022-06-01T22:55:19.05-05:00	2022-06-01T22:55:19.05-05:00	70.60.206.37
2022-06-01T14:54:59.62-05:00	2022-06-01T14:54:59.63-05:00	70.60.206.37
2022-06-01T12:54:54.71-05:00	2022-06-01T12:54:54.71-05:00	70.60.206.37
2022-06-01T12:54:54.51-05:00	2022-06-01T12:54:54.51-05:00	70.60.206.37
2022-06-01T12:54:54.28-05:00	2022-06-01T12:54:54.28-05:00	70.60.206.37

Agenda

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

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)



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, expand/collapse buttons, and a list of release versions. The "Latest Release" is 5.0.01242. The page also features a "Secure Client 5" section with a release date of 5.0.01242 and a "My Notifications" link. A table lists the download links for various operating systems, including Linux 64-bit, Android, and Mac OS. The table includes columns for "File Information", "Release Date", and "Size".

File Information	Release Date	Size
Cisco Secure Client VPN and DART Pre-Deployment DEB Package (Linux 64-bit)	19-Dec-2022	7.32 MB
cisco-secure-client-linux64-5.0.01242-predeploy-deb-k9.tar.gz		
Advisories		
Cisco Secure Client VPN and DART Pre-Deployment RPM Package (Linux 64-bit)		
cisco-secure-client-linux64-5.0.01242-predeploy-rpm-k9.tar.gz		
Advisories		
Application Programming Interface [API] (Linux 64-bit)		
cisco-secure-client-linux64-5.0.01242-vpnapi.tar.gz		
Advisories		
Cisco Secure Client Headend Deployment Package (Linux 64-bit)		
cisco-secure-client-linux64-5.0.01242-webdeploy-k9.pkg		
Advisories		
AnyConnect Pre-Deployment Package (Mac OS)		
cisco-secure-client-macos-5.0.01242-predeploy-k9.dmg		
Advisories		

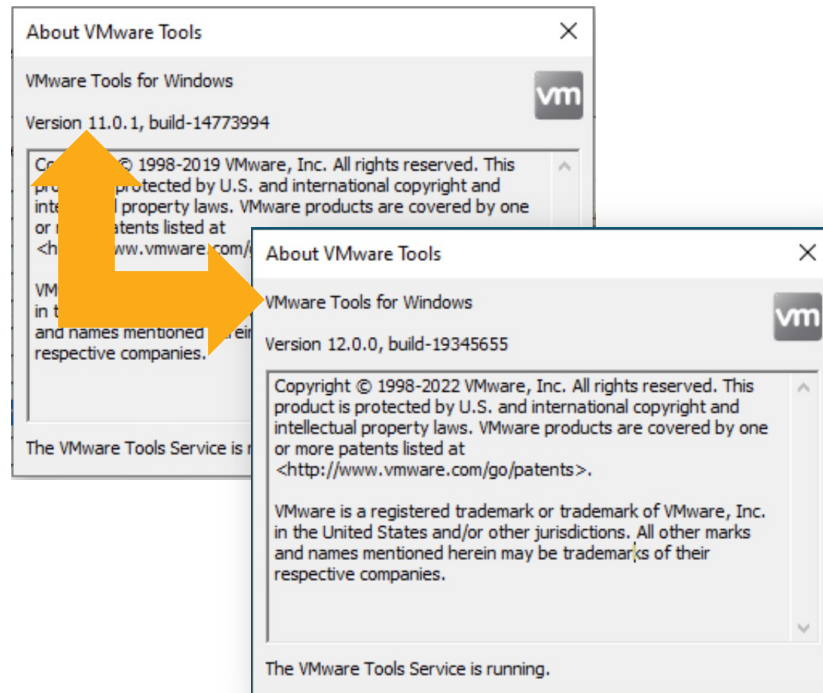
The mobile app interface shows the "Cisco Secure Client" app with a rating of 1.0K and the "Cisco Security Connector" app with a rating of 25. The app interface includes a search bar, a list of apps, and a "Today" tab.

Frequently Asked Questions

- Traditional AnyConnect modules are still version locked together
- No, Duo & 1000 Eyes are not part of this release either
- macOS and Linux on “fast- follow” roadmap
- Future version of CSC will have module independence
- No “web-deploy” package for the Cloud-Management Module
- A profile may only be in up-to 10 deployments
 - 90 Deployments targeted to be released Summer 2023
- CSC is Windows 10/11 Only
- AnyConnect 4.x still exists for customers who don't want/need to upgrade
- CSC may be used with or without the Cloud Management

Common Issue: Installing on VM

- Fyne error: window creation error
- CSC will not install on VMWare Virtual Machine
 - Cause: VMTools is outdated
 - Solution: Upgrade to latest VMTools



```
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 it's nothing is getting installed"

"I changed profile / software version in the deployment & it's 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' period buttons. A 'Select Time Zone' toggle is at the bottom. Three green arrows point to the 'Enable Product Update Window' toggle, the 'Day' selector, and the 'Select Time Zone' toggle. 'Configure' buttons with up/down arrows are 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

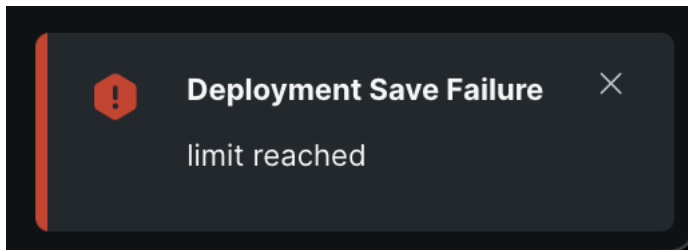
SecureX > Insights > Profiles > Cloud Management > [Profile]

Common Issue: Profile Limits

*“I have used this profile
in 10 deployments, but
get an error on the 11th”*

A single profile may only
be used in 10
deployments as of June
4, 2023.

Limit expanding to 90
deployments ~Summer
2023



Please fill out the survey



Drop your email in the comments – I WILL respond!

Other XDR sessions



Matthew Robertson
Distinguished TME

Extended Detection with
Cisco XDR: Security
analytics across the
enterprise

BRKSEC-2178

Wednesday @ 4:00 PM



Aaron Woland
Distinguished TME

Cisco's Unified Agent:
Cisco Secure Client.
Bringing AMP,
AnyConnect, Orbital &
Umbrella together

BRKSEC-2834

Thursday @ 9:00 AM



Aaron Woland
Distinguished TME

Cisco XDR - Making sense
of the Solution and how it's
a Security Productivity Tool

BRKSEC-2113

Friday @ 1:30 PM



<https://cisco.com/go/xdr>

Participating in user research gives you a place to share your thoughts and experiences to influence the future of Cisco Secure products.

- You'll hear from us at most once every 90 days.
- Participation is completely optional, and you can opt out at any time.





Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Capture the Flag

The Hub in the World of Solutions

Tuesday	9:00 a.m. – 5:30 p.m.
Wednesday	8:00 a.m. – 5:30 p.m.
Thursday	8:00 a.m. – 5:30 p.m.
Friday	9:00 a.m. – 1:30 p.m.

Learn Technology using your problem-solving skills and ignite your competitive spirit with our immersive and educational Capture the Flag – Gamified Hands-on Labs!

Now you can earn **Cisco Continuing Education Credits** by playing select Capture the Flag Missions at Cisco Live. Redeem them to renew your Cisco Certifications!



Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC